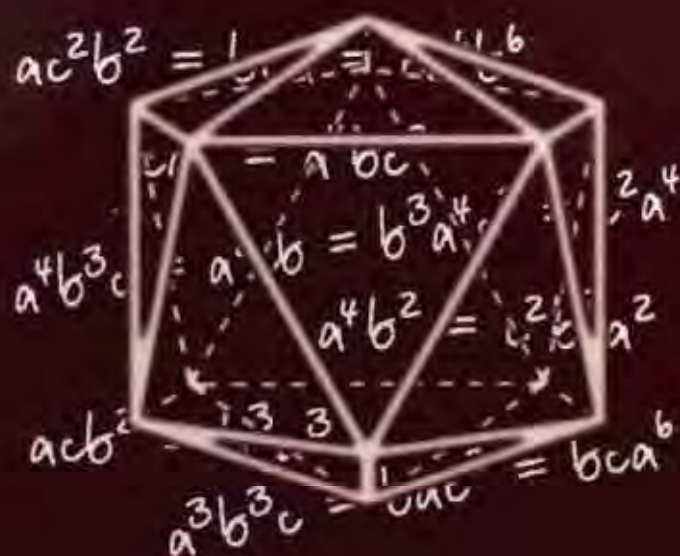


54
А39

О. Е. АКИМОВ

ДИСКРЕТНАЯ МАТЕМАТИКА

ЛОГИКА, ГРУППЫ,
ГРАФЫ



О. Е. АКИМОВ

ДИСКРЕТНАЯ МАТЕМАТИКА

ЛОГИКА, ГРУППЫ,
ГРАФЫ



Москва
Лаборатория Базовых Знаний
2001

УДК 681.5.01:512

ББК 22

А 39

Акимов О. Е. Дискретная математика: логика, группы, графы. — М.:
А 39 Лаборатория Базовых Знаний, 2001 — 352 с.: ил.

В книге излагаются основные разделы курса дискретной математики, имеющей большое значение для информатики и электроники. При подготовке книги использовался конструктивный подход, особое внимание автор уделил доступности материала. Текст снабжен большим количеством примеров.

Книга предназначена для студентов и преподавателей высших учебных заведений.

САЙТ АВТОРА: <http://sceptic-ratio.narod.ru/index.htm>

По вопросам приобретения обращаться:

В Москве

«Лаборатория Базовых Знаний» (095) 955-03-98, e-mail: lbz@aha.ru

В Санкт-Петербурге

«Диалект» (812) 247-93-01, e-mail: dialect@ndict.ioffe.rssi.ru

ISBN 5-93208-053-1

© Акимов О. Е., 2001

© Лаборатория Базовых Знаний, 2001

Предисловие

Эта книга закладывает прочный фундамент для изучения практически всех специализированных курсов, читаемых в технических вузах, университетах и академиях. Ее непосредственная цель — дать математическое обеспечение для современных компьютерных и информационных технологий. Материал книги составляет базу для таких важнейших на сегодняшний день узко специализированных дисциплин как «Теоретическая информатика», «Методы и алгоритмы принятия решений», «Функциональное и логическое программирование», «Структуры и организация данных для компьютеров», «Конструирование программ», «Системный анализ и моделирование», «Теория искусственного интеллекта» и т.п. Все эти курсы держатся на трех китах — логике, алгебре и графах. В результате систематического и добросовестного изучения материала читатель узнает базовые математические модели и алгоритмы, которые в дальнейшем позволяют ему профессионально формулировать и решать множество задач в конкретных областях информатики и вычислительной техники. Он сможет грамотно применять полученные знания для абстрактного проектирования логических структур и вычислительных процессов на графах. Книга дает представления о новейших тенденциях в развитии математического инструментария. Если ваш выбор пал на получение действительно серьезного образования в области информатики, вычислительной техники и коммуникационных сетей, то настоящая книга как раз и служит краеугольным камнем такого образования.

Автор

1. Логика

Введение. САЙТ АВТОРА: <http://sceptic-ratio.narod.ru/index.htm>

Логика, которая здесь излагается, можно назвать либо *формальной*, либо *математической*. Из-за последнего названия читатель вправе потребовать от нас анализа сложных гносеологических проблем, а именно: раскрытия природы математического доказательства и рассмотрения вопросов взаимоотношения логики с основаниями математики. Кое-что об этом сказано будет, но в общем мы намерены заняться логической «техникой».

Формальная логика делится у нас на три подраздела: *логику Буля*, *логику высказываний* и *логику предикатов*. «Логика Буля» основывается на *отношении эквивалентности*, при котором правая часть равенства всегда содержит ровно столько же «истины», сколько и левая. Строго говоря, в этом случае не происходит приращение нового знания. Два последующих подраздела, «Логика высказываний» и «Логика предикатов», базируются уже на *отношении порядка*, при котором правая часть выражения (*заключение*) содержит больше «истины», чем левая (*посылки*), т.е. «истинность» заключения оказывается выше «истинности» посылок, о чем можно судить, в частности, по количеству единиц в *таблицах истинности*. Именно это обстоятельство, по нашему мнению, создает *субъективный эффект объяснения* и вносит асимметрию во всякое *объективное причинно-следственное отношение*.

С самого начала мы обращаем внимание на *конструктивный* и *аксиоматический* подходы в получении какого-либо знания. Первый из этих подходов состоит в поиске адекватной *конструктивной модели*. Родоначальником такого подхода можно считать немецкого мыслителя Лейбница (1646–1716). В ряде своих работ, посвященных логике, он неизменно пытался реализовать идею разложения того или иного понятия на простые составляющие. Приведем его главную идею так, как она изложена в самом начале одной из первых его работ «Элементы универсального характера»¹:

Правило построения характеров следующее: всякому термину (т.е. субъекту или предикату предложения) приписывается какое-нибудь число при соблюдении одного условия — чтобы термину, составленному из каких-либо других терминов, соответствовало число, образованное из чисел этих терминов, умноженных друг на друга. Например, если представить, что термин «животное» выражается числом 2 (или, в более общем виде, *a*), термин «разумное» — через число 3 (или, в более общем виде, *r*), то термин «человек» будет выражен через число 2×3 , т.е. 6, образованное из умноженных друг на друга 2 и 3 (либо, в более общем виде, числом *ar*).

¹ Лейбниц Г.В. Соч. в 4-х томах. Т. 3. — М., 1984, с. 506

Лейбницу не удалось найти подходящую математическую структуру, которая бы адекватным образом воспроизводила логические соотношения; его «правило построения характеров» в современной логике не используется. Но от самого конструктивного подхода современные логики не отказались. В качестве явно выраженных *конструктов* широко используются *таблицы истинности* и *диаграммы Эйлера — Венна*. Заметим, по-настоящему новое знание в науке или в общественной жизни человека возникает благодаря *индукции*, находящейся в рамках конструктивного подхода, при этом мысль развивается от частного к общему.

В противовес к конструктивному выступает *аксиоматический* подход. Он уже относится к *дедуктивному* методу доказательства, при котором осуществляется движение мысли от общего к частному. Этот подход таит в себе ряд спекулятивных, схоластических или софистических ловушек; в частности, без иерархической модели последовательная манипуляция словами может привести к *логическим парадоксам*. Главное отличие аксиоматического подхода от конструктивного состоит в степени наглядности или образности исходных логических приемов: дедуктивно-аксиоматический подход гораздо в большей степени опирается на формализм знаков, чем на структуру модели. Ярчайшим представителем символического формализма был Аристотель (384—322 гг. до Р.Х.). Чтобы проиллюстрировать его способ мышления, приведем вторую главу первой книги «Первой аналитики»:

Всякая же посылка есть посылка или о том, что присуще, или о том, что необходимо присуще, или о том, что возможно присуще; и из них в соответствии с каждым способом сказанного одни утвердительные, другие отрицательные; и далее, из утвердительных и отрицательных одни — общие, другие — частные, третьи — неопределенные. Посылка о присущем, если она общеотрицательная, необходимо обратима в отношении своих терминов; например, если никакое удовольствие не есть благо, то и никакое благо не есть удовольствие. Общеутвердительная же посылка хотя и необходимо обратима, однако не в общую, а в частную; например, если всякое удовольствие есть благо, то какое-нибудь благо есть удовольствие; из частных посылок утвердительная необходимо обратима в частную же (ибо если какое-нибудь благо будет удовольствием), отрицательная же необходимо не обратима, ибо если некоторым живым существам не присуще быть человеком, то отсюда не следует, что какому-то человеку не присуще быть живым существом.

Итак, пусть сперва посылка *АБ* будет общеотрицательной. Если *А* не присуще ни одному *Б*, то и *Б* не будет присуще ни одному *А*. Ибо если бы *Б* было присуще какому-то *А*, например *В*, то было бы неправильно, что *А* не присуще ни одному *Б*, так как *В* есть какое-то *Б*. Если же *А* присуще всем *Б*, то и *Б* будет присуще некоторым *А*, ибо если *Б* не было бы присуще ни одному *А*, то и *А* не было бы присуще ни одному *Б*; но ведь было предположено, что *А* присуще всем *Б*. Точно так же, если посылка частная. В самом деле, если *А* присуще некоторым *Б*, то и *Б* необходимо присуще некоторым *А*. Если *Б* не было бы присуще ни одному *А*, то и *А* не было бы присуще ни одному *Б*. Наконец, если бы *А* некоторым *Б* не присуще, то не необходимо, чтобы и *Б* не было присуще некоторым *А*, как, например, если *Б* есть живое существо, а *А* — человек; ведь не всякому существу присуще быть человеком, однако всякому человеку присуще быть живым существом¹.

Подобными символическими приемами будем пользоваться и мы, хотя подача материала в аристотелевской логике существенно отличается от предлагаемой нами. Приведенный отрывок отчасти касается действий с *кванторами общности*

¹ Аристотель. Соч. в 4-х томах. Т. 2. — М., 1978, с. 120 — 121.

и существования, которые тоже рассматриваются нами, но с заметными элементами конструктивизма.

Цель первого раздела: надежно овладеть элементарным аппаратом формальной логики. Здесь мы не претендуем на раскрытие каких-то тонких психологических и философских характеристик теории познания и т.д., в частности, мы оставляем в стороне анализ таких гносеологических категорий, как «понятие» и «суждение». Инструмент, которым мы надеемся вооружить прилежного читателя, конечно, поможет ему правильно мыслить, но ровно настолько, насколько этому учит, скажем, элементарная геометрия: оба предмета дисциплинируют ум, однако не дают гарантированных алгоритмов проникновения в неизведанную реальность. Логика, как и геометрия, разумеется, имеет отношение к практике (исчисление предикатов в рамках языка ПРОЛОГ, действия над множествами чисел и высказываниями), однако подлинная ценность логики, как, впрочем, и любой другой базовой науки, все же содержится в ней самой, без применения ее к каким-либо другим сферам человеческого знания: языку, математике, гносеологии и психологии.

1.1. Операции логики Буля

Операции булевой логики удобно ввести через понятие «множество». Под *множеством* мы будем понимать совокупность элементов любой природы, поддающихся счету. Счет может продолжаться бесконечно долго или, начавшись, тут же и кончиться ввиду отсутствия элементов. Тем не менее, *процедура счета*, смысл которой состоит в установлении взаимно однозначного соответствия между элементами и числами натурального ряда, для множеств является определяющей. Вопросы, связанные с несчетными множествами, нами рассматриваться не будут.

Пусть дана некоторая совокупность предметов, которую после пересчета можно было бы обозначить как

$$V = \{1, 2, \dots, 11\}.$$

Предположим далее, что часть предметов, а именно: 1, 2, 4 и 6, имеет круглую форму, а часть — 2, 3, 4, 8 и 9 — окрашена в белый цвет. В этом случае говорят, что множество V имеет два *подмножества*

$$A = \{1, 2, 4, 6\} \text{ и } B = \{2, 3, 4, 8, 9\}$$

круглых и белых предметов. Можно говорить иначе: исходное множество называть *фундаментальным*, а подмножества A и B — просто множествами.

В результате мы получим четыре класса элементов:

$C_0 = \{5, 7, 10, 11\}$ — элементы, которые не обладают ни одним из названных свойств,

$C_1 = \{1, 6\}$ — элементы, обладающие только свойством A (быть круглыми),

$C_2 = \{3, 8, 9\}$ — элементы, обладающие только свойством B (быть белыми),

$C_3 = \{2, 4\}$ — элементы, которые обладают одновременно двумя названными свойствами.

Эти классы изображены на графической диаграмме Эйлера — Венна (рис. 1.1).

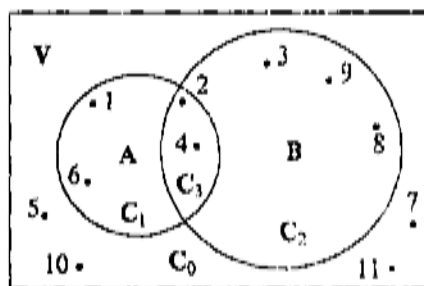


Рис. 1.1

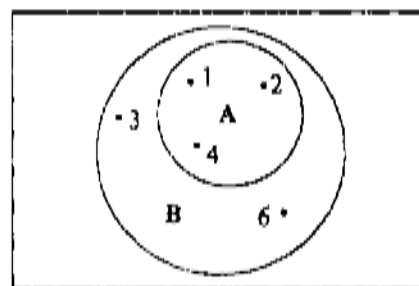


Рис. 1.2

Часто диаграммы не имеют всей полноты общности, напримерта, что изображена на рис. 1.2. На ней уже множество A полностью включено в B . Для такого случая используется специальный символ *включения* ($\subset$):

$$A \subset B = \{1, 2, 4\} \subset \{1, 2, 3, 4, 6\}.$$

Если одновременно выполняются два условия:

$$A \subset B \text{ и } B \subset A, \text{ то } A = B.$$

в этом случае говорят, что множества A и B *полностью эквивалентны*.

После того, как определены четыре класса элементов и даны необходимые сведения о диаграммах Эйлера — Венна, введем операции на множествах. В качестве первой рассмотрим операцию объединения.

Объединением множеств

$$A = \{1, 2, 4, 6\} \text{ и } B = \{2, 3, 4, 8, 9\}$$

назовем множество

$$A \cup B = \{1, 2, 3, 4, 6, 8, 9\}.$$

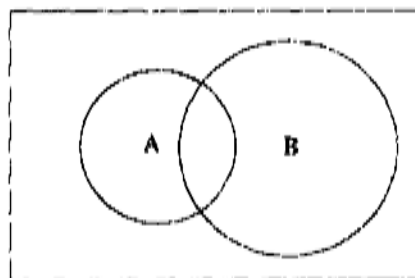


Рис. 1.3

где $\cup$ — символ объединения множеств. Таким образом, объединением охватываются три класса элементов — C_1 , C_2 и C_3 , которые на диаграмме (рис. 1.3) заштрихованы.

Логически операцию объединения двух множеств можно охарактеризовать словами: элемент x *принадлежит* множеству A или множеству B . При этом связка «или» одновременно означает и связку «и». Факт принадлежности элемента x множеству A обозначается как $x \in A$. Поэтому то, что x

принадлежит A или/и B , выражается формулой:

$$x \in A \cup B = (x \in A) \vee (x \in B),$$

где $\vee$ — символ логической связки *или*, которая называется *дизъюнкцией*.

С точки зрения логики, вместо одной *предметной* переменной x удобно ввести две *логические* переменные x_1 и x_2 . Областью определения x_1 и x_2 будут уже не числа натурального ряда, а только два логических значения: 1 для *истинного* значения и 0 для *ложного*.

Допустим, что $x = 7$. Поскольку это число не принадлежит ни множеству A , ни множеству B , то и логические значения переменных будут: $x_1 = 0, x_2 = 0$. Эта комбинация переменных отвечает классу C_0 . Теперь предположим, что выбрано число 4. Оно входит как в A , так и в B . Следовательно, $x_1 = 1, x_2 = 1$, что соответствует классу C_3 . Существуют еще два варианта, например для числа $x = 6$ имеем $x_1 = 1, x_2 = 0$, и для $x = 8$ — значения $x_1 = 0, x_2 = 1$, которые отвечают классам C_1 и C_2 .

Переменные x_1 и x_2 определяют некоторую логическую функцию:

$$y = f(x_1, x_2).$$

которая в случае дизъюнкции может быть записана как пропозиционная связка:

$$y = x_1 \vee x_2.$$

Легко усматривается, что число 7 не входит в объединенное множество $A \cup B$, поэтому при $x_1 = 0, x_2 = 0$ значение логической функции y равно нулю. Когда же выбираются числа 4, 6 или 8, то все они непременно попадут в заштрихованную область диаграммы, следовательно, при этих значениях функция y равна единице. Все это удобно оформить таблицей (табл. 1.1), которую называют *таблицей истинности*.

Таблица 1.1

x_1	x_2	$y = x_1 \vee x_2$
0	0	0
1	0	1
0	1	1
1	1	1

Между таблицей истинности и диаграммой Эйлера — Венна существует взаимно однозначное соответствие. Поэтому число единиц для y всегда будет совпадать с числом заштрихованных областей на диаграмме. Четыре комбинации аргументов x_1 и x_2 будут отвечать четырем областям C_i . Кроме того, нетрудно подсчитать, что число комбинаций нулей и единиц для функции y равно 16, значит и общее число возможных операций на двух множествах тоже равно этому же числу.

Пересечением множеств A и B называется множество $A \cap B$, содержащее те элементы из A и B , которые входят одновременно в оба множества. Для нашего числового примера будем иметь:

$$A \cap B = \{1, 2, 4, 6\} \cap \{2, 3, 4, 8, 9\} = \{2, 4\} = C_3.$$

Диаграмма Эйлера — Венна для пересечения изображена на рис. 1.4.

То, что x принадлежит одновременно двум множествам A и B , можно представить выражением:

$$x \in A \cap B \quad (x \in A) \wedge (x \in B),$$

где $\wedge$ — символ логической связки «и», которая называется *конъюнкцией*. Если в таблице истинности для дизъюнкции (табл. 1.2) все нули заменить единицами, а все единицы — нулями, то в итоге получим табл. 1.1.

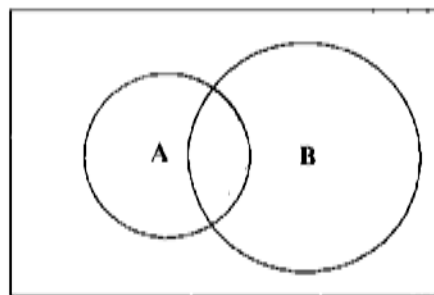


Рис. 1.4

Этот факт определяет взаимную *двойственность* конъюнкции и дизъюнкции. Для любой логической операции можно найти двойственную. Представим себе операцию, в результате которой окажутся заштрихованными области C_1 и C_3 , образующие множество A (рис. 1.5). Затем еще одну операцию, которая охватит две другие области C_0 и C_2 , не входящие в A , что обозначается как $\bar{A}$ (рис. 1.6). Если объединить заштрихованные области на обеих диаграммах, то получим все заштрихованное множество I ; пересечение же A и $\bar{A}$ даст пустое множество 0 , в котором не содержится ни одного элемента:

$$A \cup \bar{A} = I, \quad A \cap \bar{A} = 0.$$

Таблица 1.2

x_1	x_2	$y = x_1 \wedge x_2$
0	0	0
1	0	0
0	1	0
1	1	1

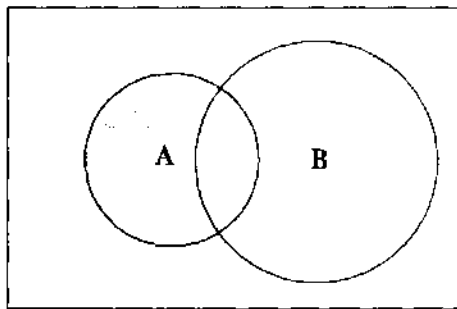


Рис. 1.5

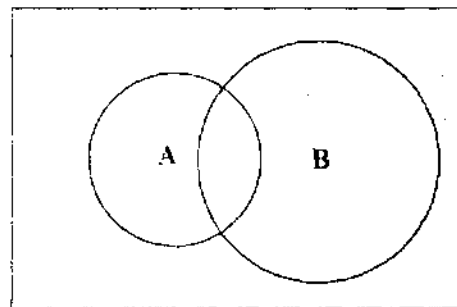


Рис. 1.6

Аналогичные равенства выполняются и для логических функций, которые имеют соответствующие названия:

$$y = x \vee \bar{x} = 1 \text{ — тавтология,}$$

$$y = x \wedge \bar{x} = 0 \text{ — противоречие.}$$

Тавтология — это всегда истинное логическое выражение, какое бы при этом значение не принимала переменная x . *Противоречие*, напротив, всегда ложное выражение.

Множество $\bar{A}$ *дополняет* множество A до фундаментального множества V (или I); отсюда название: *дополнительное* множество $\bar{A}$ или *дополнение* как операция. Дополнение к логической переменной x , т.е. $\bar{x}$ (*не- x*), называется в логике чаще всего *отрицанием x* .

После введения операций пересечения и дополнения все четыре области C_i на диаграмме Эйлера — Венна можно выразить следующим образом:

$$C_0 = \bar{A} \cap \bar{B}, \quad C_1 = A \cap \bar{B}, \quad C_2 = \bar{A} \cap B, \quad C_3 = A \cap B.$$

Путем объединения соответствующих областей C_i можно представить любую множественную операцию, в том числе и само объединение:

$$A \cup B = (A \cap \bar{B}) \cup (\bar{A} \cap B) \cup (A \cap B).$$

Все это распространяется и на логику:

$$y = x_1 \vee x_2 = (x_1 \wedge \bar{x}_2) \vee (\bar{x}_1 \wedge x_2) \vee (x_1 \wedge x_2).$$

На рис. 1.7 и рис. 1.8 приведены диаграммы двух новых операций, которые называются соответственно *стрелка Пирса* и *штрих Шеффера*. Эти диаграммы дополняют объединение и пересечение до фундаментального множества V .

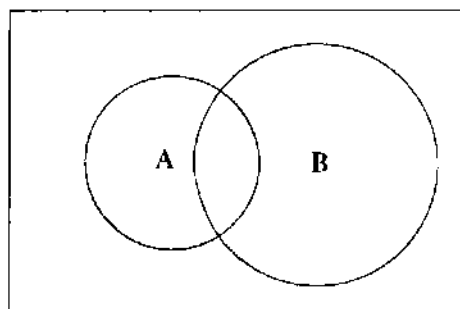


Рис. 1.7

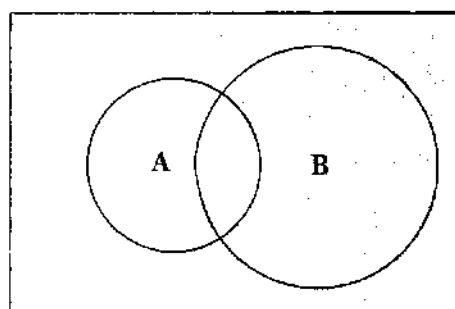


Рис. 1.8

На языке логических формул этот факт выражается следующим образом: для стрелки Пирса —

$$(x_1 \vee x_2) \vee (x_1 \downarrow x_2) = 1, \quad (x_1 \vee x_2) \wedge (x_1 \downarrow x_2) = 0,$$

для штриха Шеффера

$$(x_1 \vee x_2) \vee (x_1 | x_2) = 1, \quad (x_1 \vee x_2) \wedge (x_1 | x_2) = 0.$$

Из таблицы истинности для этих операций (табл. 1.3 и табл. 1.4) видно, что

$$y = x_1 \downarrow x_2 = \overline{x_1 \vee x_2} = \bar{x}_1 \wedge \bar{x}_2 = (x_1 \vee x_2) \wedge (\bar{x}_1 \vee \bar{x}_2) \wedge (\bar{x}_1 \vee \bar{x}_2),$$

$$y = x_1 | x_2 = \overline{x_1 \wedge x_2} = \bar{x}_1 \vee \bar{x}_2 = (x_1 \wedge \bar{x}_2) \vee (\bar{x}_1 \wedge x_2) \vee (\bar{x}_1 \wedge \bar{x}_2),$$

Таблица 1.3

x_1	x_2	$y = x_1 \downarrow x_2$
0	0	1
1	0	0
0	1	0
1	1	0

Таблица 1.4

x_1	x_2	$y = x_1 x_2$
0	0	1
1	0	1
0	1	1
1	1	0

Разностью между множествами A и B называется совокупность тех элементов множества A , которые не вошли в множество B :

$$A - B = \{1, 2, 4, 6\} - \{2, 3, 4, 8, 9\} = \{1, 6\} = C_1.$$

Диаграмма Эйлера — Венна для нее приведена на рис. 1.9.

Дополнением к разности служит *импликация*. Таблицы истинности для разности и импликации представлены табл. 1.5 и табл. 1.6.

$$y = x_1 \rightarrow x_2 = \overline{x_1 - x_2} = \bar{x}_1 \vee x_2 = (x_1 \wedge \bar{x}_2) \vee (\bar{x}_1 \wedge x_2) \vee (\bar{x}_1 \wedge \bar{x}_2),$$

$$(x_1 - x_2) \vee (x_1 \rightarrow x_2) = 1, \quad (x_1 - x_2) \wedge (x_1 \rightarrow x_2) = 0.$$

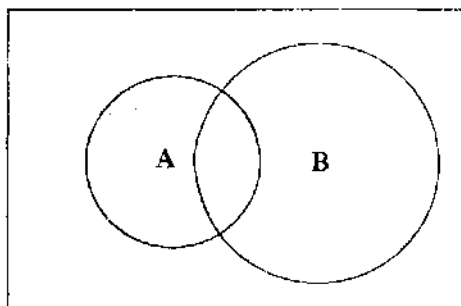


Рис. 1.9

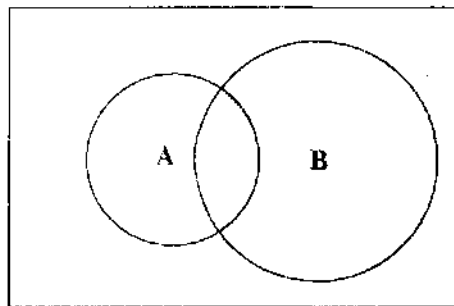


Рис. 1.10

Таблица 1.5

x_1	x_2	$y = x_1 \rightarrow x_2$
0	0	0
1	0	1
0	1	0
1	1	0

Таблица 1.6

x_1	x_2	$y = x_1 \rightarrow x_2$
0	0	1
1	0	0
0	1	1
1	1	1

На диаграмме Эйлера — Венна для импликации (рис. 1.10) показано *частичное* включение множества A в множество B , которое нужно отличать от *полного* включения (рис. 1.2).

Если утверждается, что «элементы множества A включены в множество B », то область C_3 обязательно должна быть заштрихована, так как она соответствует истине, а область C_1 с такой же необходимостью должна быть оставлена белой, поскольку ей отвечает прямо противоположное утверждение. Относительно областей C_0 и C_2 , находящихся в A , заметим следующее. Мы не имеем права оставлять их белыми, поскольку они прямо не противоречат первому утверждению; но, так как логика *двузначная*, мы обязаны все же области, попадающие в A , заштриховать. В *трехзначной* логике эти области должны быть заштрихованы как-то иначе, а в таблице истинности для импликации (табл. 1.6) на месте первой и третьей строк для y должны стоять не 1, а $1/2$, что отвечает состоянию *неопределенности*. Однако *трехзначная* и другие *неклассические* логики нами рассматриваться не будут, впрочем, к этому вопросу мы еще вернемся в разделе, который посвящен *логике высказываний*. Сейчас лишь отметим, что в *классической двузначной логике* импликация передается словами «если A , то B ».

Остается привести еще две взаимно дополняющих операции — симметрическую разность и эквивалентность.

Симметрическая разность двух множеств A и B есть объединение двух разностей:

$$A + B = (A - B) \cup (B - A) = \{1, 3, 6, 8, 9\} = C_1 \cup C_2 = \{1, 6\} \cup \{3, 8, 9\}.$$

Эквивалентность определяется теми элементами множеств A и B , которые для них являются общими. Однако элементы, не входящие ни в A , ни в B , также считаются эквивалентными:

$$A \sim B = (A \cap B) \cup (\bar{A} \cap \bar{B}) = C_0 \cup C_3 = \{2, 4, 5, 7, 10, 11\}.$$

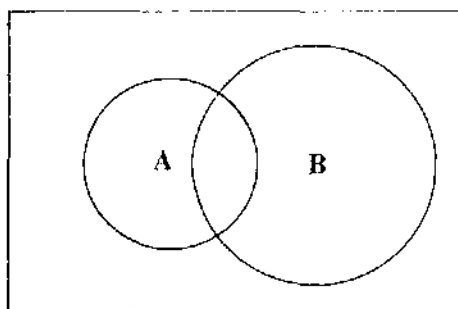


Рис. 1.11

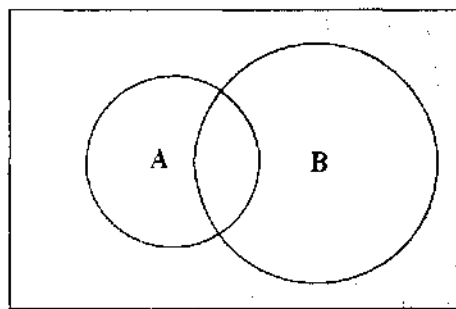


Рис. 1.12

На рис. 1.11 и рис. 1.12 показана штриховка диаграмм Эйлера — Венна, а табл. 1.7 и табл. 1.8 представляют таблицы истинности соответствующих операций. Из условия дополнительности операций вытекают следующие соотношения:

$$(x_1 + x_2) \vee (x_1 \sim x_2) = 1, \quad (x_1 + x_2) \wedge (x_1 \sim x_2) = 0,$$

$$y = x_1 \sim x_2 = \overline{x_1 + x_2} = (x_1 \wedge x_2) \vee (\overline{x_1} \wedge \overline{x_2}) = (x_1 \wedge \overline{x_2}) \wedge (\overline{x_1} \wedge x_2) \wedge (\overline{x_1} \wedge \overline{x_2}).$$

Таблица 1.7

x_1	x_2	$y = x_1 \cdot x_2$
0	0	0
1	0	1
0	1	1
1	1	0

Таблица 1.8

x_1	x_2	$y = x_1 \sim x_2$
0	0	1
1	0	0
0	1	0
1	1	1

В заключение отметим, что *симметрическая разность* имеет несколько названий: *строгая дизъюнкция*, *исключающая альтернатива*, *сумма по модулю два*. Эту операцию можно передать словами — «либо А, либо В», т. е. это логическая связка «или», но без включенной в нее связки «и».

1.2. Формы представления булевых функций

Любую булеву функцию $y = f(a, b)$ можно представить как некоторую комбинацию областей:

$$C_0 = \overline{a} \wedge \overline{b}, \quad C_1 = a \wedge \overline{b}, \quad C_2 = \overline{a} \wedge b, \quad C_3 = a \wedge b.$$

Тогда, в зависимости от значения функции и заданных C_i , которые в этом случае мы будем именовать *конституентами*, получим шестнадцать логических операций:

$$y = [\overline{a} \wedge \overline{b} \wedge f(0, 0)] \vee [a \wedge \overline{b} \wedge f(1, 0)] \vee [\overline{a} \wedge b \wedge f(0, 1)] \vee [a \wedge b \wedge f(1, 1)].$$

Подобная форма представления логических функций называется *совершенной дизъюнктивной нормальной формой* (СДНФ).

В логике Буля действует *принцип двойственности*, который гласит: при одновременной замене символов $\wedge \Leftrightarrow \vee$ и $1 \Leftrightarrow 0$ все логические равенства остаются в силе. Поэтому нашу СДНФ можно представить несколько иначе:

$$y = [\bar{a} \vee \bar{b} \vee f(1, 1)] \wedge [a \vee \bar{b} \vee f(0, 1)] \wedge [\bar{a} \vee b \vee f(1, 0)] \wedge [a \vee b \vee f(0, 0)].$$

Эта форма представления называется *совершенной конъюнктивной нормальной формой* (СКНФ). Здесь уже конститутенты представлены не в виде конъюнктов, как в СДНФ, а в виде дизъюнктов. Соединены же эти дизъюнкты конъюнкцией, отсюда и название — СКНФ.

Существует еще и третья форма — *совершенная полиномиальная нормальная форма* (СПНФ). Ее легко получить из СДНФ путем замены:

$$a \vee b = a + b + ab, \quad \bar{a} = 1 + a.$$

Поскольку конститутенты не пересекаются ($C_i C_j = 0$), мы можем сразу же записать (в СПНФ символ конъюнкции опускается):

$$y = [(1+a)(1+b)f(0,0)] + [a(1+b)f(1,0)] + [(1+a)b f(0,1)] + [ab f(1,1)] = \\ = f(0,0) + a[f(0,0)+f(1,0)] + b[f(0,0)+f(0,1)] + ab[f(0,0)+f(1,0)+f(0,1)+f(1,1)].$$

В табл. 1.9 приведен полный список *элементарных логических функций* от двух аргументов и в трех *совершенных формах* — СДНФ, СКНФ и СПНФ. Совершенные формы представлений позволяют выразить аналитической формулой любую функцию, если известна ее таблица истинности.

Таблица 1.9

$y = f(a, b)$	СДНФ = СКНФ = СПНФ
$y_0 = 0$	$= (a \vee b) \wedge (\bar{a} \vee b) \wedge (a \vee \bar{b}) \wedge (\bar{a} \vee \bar{b}) = 0$
$y_1 = a \wedge b$	$= (a \vee b) \wedge (\bar{a} \vee b) \wedge (a \vee \bar{b}) = ab$
$y_2 = b - a$	$= \bar{a} \wedge b = (a \vee b) \wedge (\bar{a} \vee b) \wedge (\bar{a} \vee \bar{b}) = b + ab$
$y_3 = b$	$= (\bar{a} \wedge b) \vee (a \wedge b) = (a \vee b) \wedge (a \vee \bar{b}) = b$
$y_4 = a - b$	$= a \wedge \bar{b} = (a \vee b) \wedge (\bar{a} \vee \bar{b}) \wedge (\bar{a} \vee b) = a + ab$
$y_5 = a$	$= (a \wedge \bar{b}) \vee (a \wedge b) = (a \vee b) \wedge (\bar{a} \vee \bar{b}) = a$
$y_6 = a + b$	$= (a \wedge \bar{b}) \vee (\bar{a} \wedge b) = (a \vee b) \wedge (\bar{a} \vee \bar{b}) = a + b$
$y_7 = a \vee b$	$= (a \wedge \bar{b}) \vee (\bar{a} \wedge b) \vee (a \wedge b) = (a \vee b) + a + b + ab$
$y_8 = a \downarrow b$	$= \bar{a} \wedge \bar{b} = (a \vee b) \wedge (\bar{a} \vee b) \wedge (\bar{a} \vee \bar{b}) = 1 + a + b + ab$
$y_9 = a \sim b$	$= (\bar{a} \wedge \bar{b}) \vee (a \wedge b) = (\bar{a} \vee b) \wedge (a \vee \bar{b}) = 1 + a + b$
$y_{10} = \bar{a}$	$= (\bar{a} \wedge \bar{b}) \vee (\bar{a} \wedge b) = (\bar{a} \vee b) \wedge (\bar{a} \vee \bar{b}) = 1 + a$
$y_{11} = a \rightarrow b$	$= (\bar{a} \wedge \bar{b}) \vee (\bar{a} \wedge b) \vee (a \wedge b) = 1 + a + ab$
$y_{12} = \bar{b}$	$= (\bar{a} \wedge \bar{b}) \vee (a \wedge \bar{b}) = (a \vee \bar{b}) \wedge (\bar{a} \vee \bar{b}) = 1 + b$
$y_{13} = b \rightarrow a$	$= (\bar{a} \wedge \bar{b}) \vee (a \wedge \bar{b}) \vee (a \wedge b) = a \vee \bar{b} = 1 + b + ab$
$y_{14} = a \uparrow b$	$= (\bar{a} \wedge \bar{b}) \vee (a \wedge \bar{b}) \vee (\bar{a} \wedge b) = 1 + ab$
$y_{15} = 1$	$= (\bar{a} \wedge \bar{b}) \vee (a \wedge \bar{b}) \vee (\bar{a} \wedge b) \vee (a \wedge b) = 1$

Пусть задана конкретная таблица истинности (табл. 1.10) для функции, зависящей от трех аргументов. Тогда, выпишывая соответствующие конъюнкты против единичных значений y , мы получим СДНФ. Если же мы выпишем дизъюнкты против нулевых значений y , то в результате уже получим СКНФ. Наконец, СПНФ образуется путем замены в СДНФ: $\vee$ на $+$ и $\bar{x}$ на $1+x$.

$$Y_{\text{СДНФ}} = (\bar{x}_3 \wedge \bar{x}_2 \wedge x_1) \vee (\bar{x}_3 \wedge x_2 \wedge x_1) \vee (x_3 \wedge \bar{x}_2 \wedge \bar{x}_1) \vee (x_3 \wedge x_2 \wedge x_1),$$

$$Y_{\text{СКНФ}} = (x_3 \vee x_2 \vee x_1) \wedge (x_3 \vee \bar{x}_2 \vee x_1) \wedge (\bar{x}_3 \vee x_2 \vee \bar{x}_1) \wedge (\bar{x}_3 \vee \bar{x}_2 \vee x_1),$$

$$Y_{\text{СПНФ}} = (x_3 + 1)(x_2 + 1)x_1 + x_3x_2x_1 + (x_3 + 1)x_2x_1 + x_3(x_2 + 1)(x_1 + 1).$$

В последнем случае выражение для $Y_{\text{СПНФ}}$ легко можно упростить, если раскрыть скобки и взаимно сократить все одинаковые слагаемые, входящие в формулу четное число раз:

$$Y_{\text{СПНФ}} = x_1 + x_2 + x_3.$$

Подобное упрощение, которое называется *минимизацией логической функции*, можно осуществить и по отношению к СДНФ и СКНФ.

Таблица 1.10

x_1	x_2	x_3	y
0	0	0	0
1	0	0	1
0	1	0	0
1	1	0	1
0	0	1	1
1	0	1	0
0	1	1	0
1	1	1	1

В логике Буля действует *закон склеивания*:

$$(a \wedge \bar{b}) \vee (a \wedge b) = a, \quad (a \vee \bar{b}) \wedge (a \vee b) = a.$$

Применение этих законов позволяет найти более компактные аналитические выражения для заданной функции y , т.е. *минимальную дизъюнктивную нормальную форму* $Y_{\text{МДНФ}}$. Приведем соответствующие формы представления функции y , заданной табл. 1.10:

$$Y_{\text{МДНФ}} = (\bar{x}_3 \wedge x_1) \vee (x_2 \wedge x_1) \vee (x_3 \wedge \bar{x}_2 \wedge \bar{x}_1),$$

и для СКНФ, т.е. *минимальную КНФ*:

$$Y_{\text{МКНФ}} = (x_3 \vee x_1) \wedge (\bar{x}_3 \vee x_2 \vee \bar{x}_1) \wedge (\bar{x}_2 \vee x_1).$$

После того, как найдены *минимальные нормальные формы* (МНФ), их рекомендуется проверить на всех наборах аргументов x_i . Переменные x_i или $\bar{x}_i$ часто называют *термами*. Именно полный набор из n термов образует *конституенту*. В процессе же минимизации некоторые термы из конституент пропадают. Тогда оставшаяся часть дизъюнкта или конъюнкта называют *импликантой*.

Как мы только что убедились на примере, импликанты появляются в результате склейки *смежных* конституент, различающихся одним термом. Однако для функций, зависящих от многих переменных, неконтролируемый процесс

склейки неизбежно приводит к лишним импликантам. Требуемое число импликант может оказаться гораздо меньше возможного числа смежных склеек. В таких случаях истинную МНФ получают с помощью специальных методов минимизации, три из которых мы сейчас разберем. При этом следует помнить, что рассматриваемые далее методы минимизации касаются только СДНФ. Эти методы на основании принципа двойственности легко могут быть распространены и на СКНФ.

Пусть будут заданы номера наборов четырех переменных, на которых логическая функция принимает единичное значение:

$$f(2, 5, 6, 7, 10, 12, 13, 14) = 1.$$

Выразим эту логическую функцию в СДНФ (символ конъюнкции писать не будем):

$$f(0010, 0101, 0110, 0111, 1010, 1100, 1101, 1110) = \bar{x}_4\bar{x}_3x_2\bar{x}_1 \vee \bar{x}_4x_3\bar{x}_2x_1 \vee \bar{x}_4x_3x_2\bar{x}_1 \vee \bar{x}_4x_3x_2x_1 \vee x_4\bar{x}_3x_2\bar{x}_1 \vee x_4x_3\bar{x}_2\bar{x}_1 \vee x_4x_3\bar{x}_2x_1 \vee x_4x_3x_2x_1.$$

На первом этапе минимизации исходную СДНФ можно упростить за счет использования закона склеивания, тогда получим:

$$f = x_2\bar{x}_1 \vee \bar{x}_4x_3x_1 \vee \bar{x}_4x_3x_2 \vee x_3\bar{x}_2x_1 \vee x_4x_3\bar{x}_2 \vee x_4x_3\bar{x}_1.$$

Обращаем внимание на то, что одну и ту же конституенту (импликанту) можно склеивать с другими конституентами (импликантами) многократно, так как в логике Буля действует *закон идемпотентности*:

$$a = a \vee a = a \vee a \vee a = \dots, \quad a = a \wedge a = a \wedge a \wedge a = \dots,$$

поэтому любую конституенту можно размножить.

На втором этапе воспользуемся *таблицей Куайна* (табл. 1.11), в соответствии с которой данный метод минимизации получил свое наименование — *метод Куайна*. В таблице по вертикали перечислены все полученные на первом этапе упрощения импликанты, а по горизонтали — исходные конституенты. Единица в табл. 1.11 стоит там, где импликанта «накрывает» конституенту. Дело в том, что конституента всегда может быть заменена импликантой или даже отдельным термом по *закону поглощения*:

$$a = a \vee (a \wedge b) = a \vee (a \wedge abc) = \dots,$$

$$a = a \wedge (a \vee b) = a \wedge (a \vee abc) = \dots$$

Таблица 1.11

$x_4x_3x_2x_1$	0010	0101	0110	0111	1010	1100	1101	1110
$\bar{x}_4\bar{x}_3x_2\bar{x}_1$	1	0	1	0	1	0	0	1
$\bar{x}_4x_3\bar{x}_2x_1$	0	1	0	1	0	0	0	0
$\bar{x}_4x_3x_2\bar{x}_1$	0	0	1	1	0	0	0	0
$\bar{x}_4x_3x_2x_1$	0	1	0	0	0	0	1	0
$x_4\bar{x}_3x_2\bar{x}_1$	0	0	0	0	0	1	1	0
$x_4x_3\bar{x}_2\bar{x}_1$	0	0	0	0	0	1	0	1

После заполнения таблицы Куайна у нас получилось так, что почти в каждой графе оказалось по две единицы; между тем достаточно иметь одну единицу в графе. Поэтому, по возможности, нужно исключить избыточные единицы. Выбор единиц производится из соображений минимальности числа термов (выбранные единицы затемнены). В итоге оказалось, что можно обойтись только тремя импликантами вместо шести:

$$f = x_2\bar{x}_1 \vee \bar{x}_1x_3x_1 \vee x_1x_3\bar{x}_2.$$

С помощью таблиц истинности легко проверить, что полученная в МНФ функция воспроизводит все значения исходной функции. Отметим, что в общем случае решений по критерию минимума термов может быть несколько.

Не менее эффективным способом минимизации логических функций является *метод сочетания индексов*. Для его изложения составим табл. 1.12, в графах которой записаны возможные сочетания индексов. В последней графе выписаны значения функции. Анализ таблицы начинается слева по столбцам. Принцип исключения i, j -кода следующий. На пересечении i -столбца, например с сочетанием индексов 23, и j -строки, например 3-ей, находится код 10, что соответствует импликанте x_2x_3 . Следовательно, в этом столбце везде, где встречается код 10, т.е. в строках 2, 3, 10 и 11, эти коды исключаются, поскольку значение функции в 3-ей строке равно нулю. Теперь возьмем столбец с сочетанием индексов 124. Здесь во 2-ой и 6-ой строках оставлены коды 010, а в 10-ой и 14-ой строках — код 011. Сделано это потому, что эти коды встречаются только на строках со значением функции, равным единице. Напротив, код 110 этого же столбца встречается как при единичных значениях функции, так и при нулевых.

Таблица 1.12

n	1	2	3	4	12	13	14	23	24	34	123	124	134	234	1234	y
0	0	0	0	0	00	00	00	00	00	00	000	000	000	000	0000	0
1	1	0	0	0	10	10	10	00	00	00	100	100	100	000	1000	0
2	0	1	0	0	01	00	00	10	10	00	010	010	000	100	0100	1
3	1	1	0	0	11	10	10	10	10	00	110	110	100	100	1100	0
4	0	0	1	0	00	01	00	01	00	10	001	000	010	010	0010	0
5	1	0	1	0	10	11	10	01	00	10	101	100	110	010	1010	1
6	0	1	1	0	01	01	00	11	10	10	011	010	010	110	0110	1
7	1	1	1	0	11	11	10	11	10	10	111	110	110	110	1110	1
8	0	0	0	1	00	00	01	00	01	01	000	001	001	001	0001	0
9	1	0	0	1	10	10	11	00	01	01	100	101	101	001	1001	0
10	0	1	0	1	01	00	01	10	11	01	010	011	001	101	0101	1
11	1	1	0	1	11	10	11	10	11	01	110	111	101	101	1101	0
12	0	0	1	1	00	01	01	01	01	11	001	001	011	011	0011	1
13	1	0	1	1	10	11	11	01	01	11	101	101	111	011	1011	1
14	0	1	1	1	01	01	01	11	11	11	011	011	011	111	0111	1
15	1	1	1	1	11	11	11	11	11	11	111	111	111	111	1111	1

Итак, все коды на строках, заканчивающихся нулевыми значениями функции, исключаются автоматически. Если эти коды попадают на строки, заканчивающиеся единичным значением функции, то они также не учитываются. Остаются только те коды, которые расположены на строках с единичным значением функции (эти коды затемнены).

Далее руководствуются следующим правилом. Для того чтобы функция приняла значение, равное единице, достаточно того, чтобы только какая-нибудь одна импликанта на строке приняла единичное значение. Прежде всего оставляем минимальную импликанту $x_2\bar{x}_1$, которая перекрывает единицы в строках 2, 6, 10 и 14. Затем, естественно, обращаемся к 12-ой строке. Здесь оставляем единственный на строке код 011, что отвечает импликанте $x_4x_3\bar{x}_2$. Эта же импликанта ответственна за 13-ую строку, оканчивающуюся тоже единицей. Осталось рассмотреть 5-ую и 7-ую строки. Общей для них является импликанта $\bar{x}_4x_3x_1$. Таким образом, тремя импликантами мы перекрыли все единичные значения функции, что совпадает с результатом, полученным на основе таблиц Куайна.

Хотя табл. 1.12 более громоздка, чем табл. 1.11, метод сочетания индексов не считается более сложным, чем метод Куайна, если помнить, что до составления таблиц Куайна необходимо произвести многочисленные склейки конституент и импликант. Реализация на компьютере алгоритма метода сочетания индексов оказывается сравнительно простой. И напротив, внешняя простота и наглядность *третьего метода* минимизации логических функций с помощью карт Карно оборачивается сложной программой при реализации алгоритма на компьютере.

Таблица 1.13

	x_1	x_1	x_1	$\bar{x}_1$	
x_2	1100	1110	0110	0100	x_4
x_2	1101	1111	0111	0101	x_4
$\bar{x}_2$	1001	1011	0011	0001	x_4
$\bar{x}_2$	1000	1010	0010	0000	x_4
	$\bar{x}_3$	x_3	x_3	$\bar{x}_3$	

Таблица 1.14

	0	1	1	1	
	0	1	1	0	$x_2\bar{x}_1$
$\bar{x}_4x_3x_1$	0	1	1	0	
	0	1	0	0	$x_4x_3\bar{x}_2$

Карта Карно для четырех переменных представлена в виде табл. 1.13. Каждая клетка карты соответствует конституенте. Заполненная карта представлена табл. 1.14 (функция взята та же, что и в первых двух методах). Согласно *закону склеивания*, две смежные конституенты с единичными значениями всегда можно объединить для получения соответствующей импликанты. Причем смежными счи-

таются и те, которые лежат на границах карты. Какие именно единицы требуется объединить для получения подходящей импликанты, легко определить визуально. Следует также помнить, что в соответствии с *законом идемпотентности* одна и та же единица табл. 1.14 может склеиваться с двумя или тремя смежными единицами.

Рассмотренные здесь три метода используются для сравнительно небольшого числа переменных. Если же число их становится слишком большим, требуются более изощренные приемы отбора импликант.

Представление функций в СДНФ и СКНФ образовано тремя операциями — дизъюнкцией, конъюнкцией и отрицанием, а СПНФ — сложением по модулю два, конъюнкцией и единицей как операцией. В логике Буля действует *принцип суперпозиции*, который гласит: любая сложная функция может быть представлена в виде совокупности элементарных функций двух аргументов, например:

$$F(x_1, x_2, x_3, x_4) = ((x_1 \cdot x_2) \rightarrow (x_2 \vee x_3)) \downarrow (\bar{x}_3 + x_4) = \\ = f_8 \{f_1, [f_{14}(x_1, x_2), f_7(x_3, x_3)], f_6[f_{10}(x_3, x_4), x_4]\}.$$

Табл. 1.15 является таблицей истинности для нашей сложной функции $F(x_1, x_2, x_3, x_4)$. На всех наборах аргументов, кроме двух, эта функция равна нулю. Поэтому ее можно представить в виде одного конъюнкта, который выражается через операцию вычитания:

$$F(x_1, x_2, x_3, x_4) = \bar{x}_2 \wedge \bar{x}_3 \wedge x_4 = (x_4 - x_3) - x_2.$$

Таблица 1.15

x_1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
$f_4 = x_1 \cdot x_2$	1	1	1	0	1	1	1	0	1	1	1	0	1	1	1	0
$f_7 = x_2 \vee x_3$	0	0	1	1	1	1	1	1	0	0	1	1	1	1	1	1
$f_{10} = \bar{x}_3$	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
$f_6 = f_{10} + x_4$	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1
$f_{11} = f_4 \rightarrow f_7$	0	0	1	1	1	1	1	1	0	0	1	1	1	1	1	1
$f_8 = f_{11} \downarrow f_6$	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0

Зададимся вопросом: через какие еще системы логических операций можно выразить произвольно взятую булеву функцию? В связи с этим вопросом определим пять *классов функций*.

Функция, сохраняющая нулевое значение на нулевом наборе термов: $f(0, 0) = 0$, определяет 0-класс. К этому классу относятся все элементарные функции с 0 по 7 (см. табл. 1.9).

Аналогично определяется 1-класс, *сохраняющий константу 1* на единичном наборе: $f(1, 1) = 1$. К 1-классу относятся нечетные функции.

Класс *линейных функций* (2-класс) определяется линейностью полиномиальной формы. Так, например, эквивалентность является линейной функцией, так как $f_9 = 1 - a + b$, а стрелка Пирса за счет нелинейного слагаемого ab уже не будет являться таковой: $f_3 = 1 + a + b - ab$.

Класс *самодвойственных функций* (3 класс) описывается формулой: $f(a, b) = \bar{f}(\bar{a}, \bar{b})$. Таких элементарных функций всего четыре.

Наконец, класс *монотонных функций* (4-класс) определяется неравенством: $f(a, b) \leq f'(a', b')$, при $a \leq a'$, и $b \leq b'$. Например, пусть $a=0$, $a'=1$, $b=1$ и $b'=1$, тогда для дизъюнкции будем иметь:

$$(f_7 = a \vee b = 1) \leq (f_7' = a' \vee b' = 1).$$

И какие бы наборы a, a', b и b' мы не брали, если выполняются условия $a \leq a'$ и $b \leq b'$, всегда будет иметь место $f_7 \leq f_7'$; значит, дизъюнкция является монотонной функцией.

Принадлежность элементарной функции к тому или иному классу (K) отмечена единицей в табл. 1.16. По этой таблице уже легко можно определить систему базисных функций.

Таблица 1.16

K	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
2	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1
3	0	0	0	1	0	1	0	0	0	0	1	0	1	0	0	0
4	1	1	0	1	0	1	0	1	0	0	0	0	0	0	0	1

Система функций является базисной, если она перекрывает нулями все строки 0-, 1-, 2-, 3-, 4-классов. Например, СПНФ образована функциями f_1, f_6, f_{15} . Для этих трех функций нули стоят во всех пяти столбцах табл. 1.16. Следовательно, в СПНФ может быть представлена любая сколь угодно сложная функция.

СДНФ и СКНФ образованы функциями f_1, f_7, f_{10} . Перекрытие нулями всех пяти классов достигается уже двумя функциями: либо f_1 и f_{10} , либо f_7 и f_{10} , т.е. в этих формах имеется некоторая избыточность функций.

Итогом теории пяти классов функций является *теорема Поста*, которая гласит: для того чтобы система функций была базисной, необходимо и достаточно чтобы она включала в себя хотя бы одну функцию, не принадлежащую 0-, 1-, 2-, 3- и 4-классам (условие наличия нулей на всех строках табл. 1.16). Однако для установления базисной системы функций вовсе не обязательно вводить пять классов функций: достаточно знать взаимосвязь между операциями. Коль скоро было установлено, что всякая логическая операция представима через три булевых, требуется лишь выразить эти три через все остальные. На основе таблиц истинности можно убедиться в справедливости следующих равенств:

$$\begin{aligned}
 a \rightarrow b &= \overline{a - b}, \\
 \bar{a} &= 1 - a - a \rightarrow 0 = 1 - a - a \sim 0 = a | a - a \downarrow a, \\
 a \wedge b &= a - \bar{b} = (a | b) : (a | b) - (a \downarrow a) \downarrow (b \downarrow b), \\
 a \vee b &= \bar{a} \rightarrow b = (a | a) | (b | b) - (a \downarrow b) \downarrow (a \downarrow b), \\
 a + b &= \bar{a} + \bar{b} = \bar{a} \sim b = a \sim \bar{b} = \overline{a - b}, \\
 1 &= a \rightarrow a - \bar{a} \vee a = a \sim a, \\
 0 &= a - a = \bar{a} \wedge a = a \downarrow a.
 \end{aligned}$$

1.3. Методы доказательства в логике Буля

В качестве основных законов логики Буля чаще других называют:

1) *законы идемпотентности*:

$$a = a \wedge a, \quad a = a \vee a;$$

2) *законы коммутативности*:

$$a \wedge b = b \wedge a, \quad a \vee b = b \vee a;$$

3) *законы ассоциативности*:

$$a \wedge (b \wedge c) = (a \wedge b) \wedge c, \quad a \vee (b \vee c) = (a \vee b) \vee c;$$

4) *законы дистрибутивности*:

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c),$$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c);$$

5) *законы нуля и единицы*:

$$a \wedge \bar{a} = 0, \quad a \wedge 1 = a, \quad a \vee \bar{a} = 1, \quad a \vee 0 = a;$$

6) *законы поглощения*:

$$a \vee (a \wedge b) = a, \quad a \wedge (a \vee b) = a;$$

7) *законы де Моргана*:

$$\overline{a \vee b} = \bar{a} \wedge \bar{b}, \quad \overline{a \wedge b} = \bar{a} \vee \bar{b};$$

8) *законы склеивания*:

$$(a \vee \bar{b}) \wedge (a \vee b) = a, \quad (a \wedge \bar{b}) \vee (a \wedge b) = a.$$

Не все восемь законов независимы друг от друга. Так, например, закон идемпотентности можно получить из закона поглощения с использованием закона дистрибутивности:

$$a = a \vee (a \wedge b) = (a \vee a) \wedge (a \vee b) = (a \wedge (a \vee b)) \vee (a \wedge (a \vee b)) = a \vee a.$$

Закон поглощения может быть выведен из закона нуля и единицы:

$$a \vee (a \wedge b) = (a \wedge 1) \vee (a \wedge b) = a \wedge (1 \vee b) = a \wedge 1 = a.$$

Закон идемпотентности относительно дизъюнкции непосредственно выводится из законов нуля и единицы:

$$a \vee a = (a \vee a) \wedge 1 = (a \vee a) \wedge (\bar{a} \vee a) = a \vee (a \wedge \bar{a}) = a \vee 0 = a.$$

При доказательствах логических выражений мы должны всегда иметь в виду принцип двойственности. Так, вышеприведенная цепочка равенств для закона поглощения может быть представлена следующим образом:

$$a \wedge (a \vee b) = (a \vee 0) \wedge (a \vee b) = a \vee (0 \wedge b) = a \vee 0 = a.$$

Итак, в качестве *независимой системы законов* можно выбрать законы: *коммутативности, ассоциативности, дистрибутивности, нуля и единицы*.

В логике широко используются два подхода — *аксиоматический* и *конструктивный*. При аксиоматическом доказательстве используется жесткая *система аксиом*, состоящая, например, из четырех только что названных. Все остальные тождества необходимо представлять через эти законы. При конструктивном же доказательстве мы должны будем воспользоваться *системой конструктов*, при-

мерами которых являются диаграмма Эйлера — Венна и таблица истинности. Продемонстрируем различие этих двух подходов.

Для доказательства простого тождества $(a \wedge 0 = 0)$ приверженец аксиоматического подхода приведет примерно такую цепочку преобразований:

$$\begin{aligned} a \wedge 0 &= a \wedge (a \wedge \bar{a}) = (a \wedge a) \wedge \bar{a} = ((a \wedge a) \vee 0) \wedge \bar{a} = \\ &= ((a \wedge a) \vee (a \wedge \bar{a})) \wedge \bar{a} = (a \wedge (a \vee \bar{a})) \wedge \bar{a} = (a \wedge 1) \wedge \bar{a} = a \wedge \bar{a} = 0. \end{aligned}$$

И сделает он это только ради того, чтобы формально привязаться к провозглашенной выше системе аксиом. Вместе с тем для конструктивиста исходное тождество практически не потребует никаких доказательств.

Картина выглядит противоположным образом в отношении, например, закона дистрибутивности. Аксиоматик в данном случае не предпримет никаких действий, а сторонник конструктивного подхода обязан продемонстрировать эквивалентность левой и правой частей тождества:

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

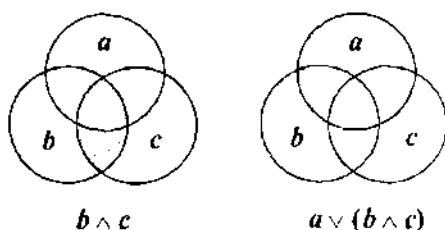


Рис. 1.13

Проведем доказательство с помощью диаграмм Эйлера — Венна. С этой целью построим две диаграммы, изображенные на рис. 1.13, которые отвечают двум операциям левой части тождества.

Теперь построим еще три диаграммы (рис. 1.14), соответствующие трем операциям, фигурирующим в правой части закона дистрибутивности.

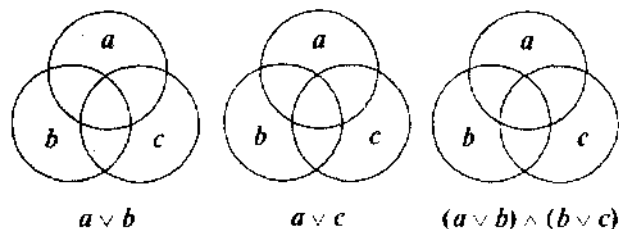


Рис. 1.14

Как видно из диаграмм, результаты построения логических операций левой и правой части закона дистрибутивности полностью совпали.

Докажем с помощью диаграмм Эйлера — Венна справедливость более сложного тождества:

$$a + b + c + d = ((a \sim b) \rightarrow (c \sim d)) \wedge ((a + b) \sim (c \sim d)).$$

На рис. 1.15 изображены две операции — $a + b$ и $c + d$, — фигурирующие в левой части приведенного тождества. Следует заметить, что диаграмма Эйлера — Венна, нарисованная с помощью кругов, для четырех переменных a , b , c и d не является полной, поскольку она содержит только 14 областей, а необходимо 16. Поэтому в роли исходных областей выбраны эллипсы.

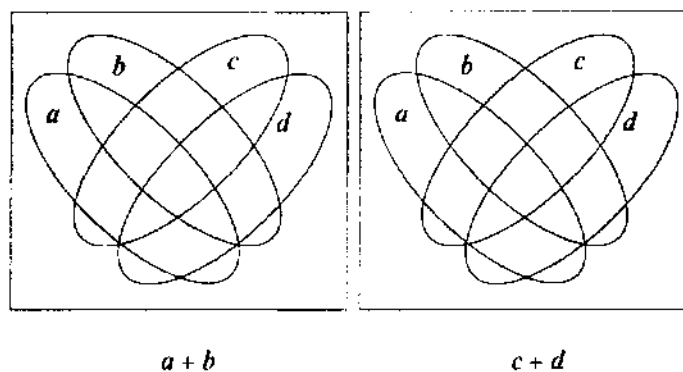


Рис. 1.15

На рис. 1.16 изображены четыре диаграммы, соответствующие операциям правой части тождества; последняя из них является результирующей. Но точно такая же результирующая диаграмма получится при сложении по mod (2) двух первых диаграмм: $(a + b) + (c + d)$. Так как результирующие диаграммы левой и правой части одинаковые, приведенное нами тождество является верным.

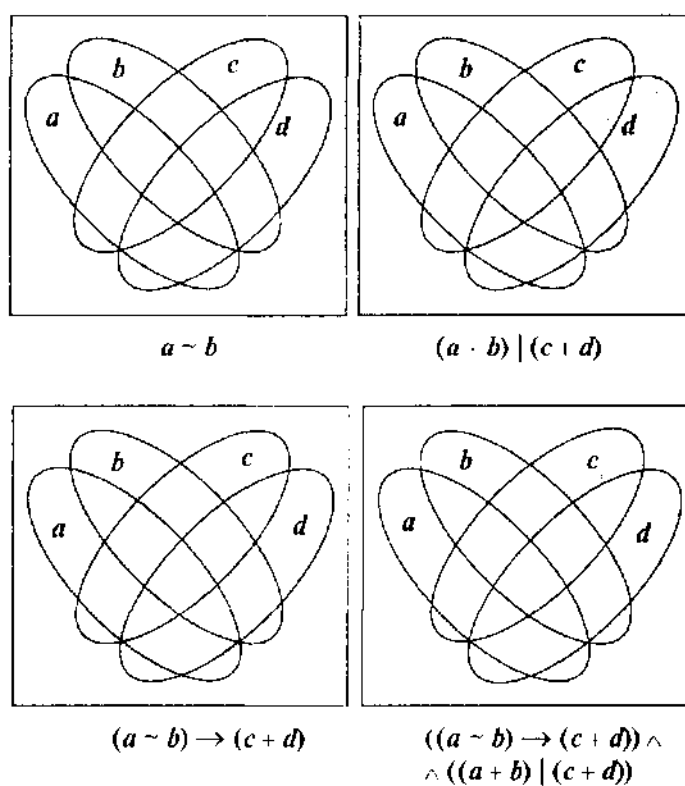


Рис. 1.16

В правильности тождества можно убедиться с помощью таблицы истинности (табл. 1.17). Она показывает, что наборы значений из нулей и единиц для левой части (f_L) совпали с наборами правой части (f_R), значит, исходное тождество верно.

Таблица 1.17

a	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
b	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
c	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
d	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
$f_1 = a + b$	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
$f_2 = c + d$	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0
$f_3 = f_1 + f_2$	0	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0
$f_4 = a \sim b$	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1
$f_4 = f_3 \rightarrow f_2$	0	1	1	0	1	1	1	1	1	1	1	1	0	1	1	0
$f_5 = f_1 f_2$	1	1	1	1	1	0	0	1	1	0	0	1	1	1	1	1
$f_R = f_4 \wedge f_5$	0	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0

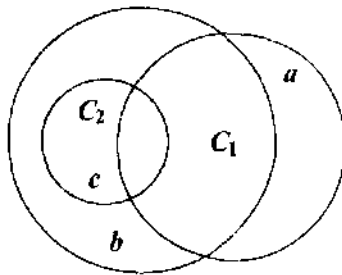


Рис. 1.17

Можно ставить обратную задачу, т.е. по известной диаграмме находить отвечающее ей компактное аналитическое выражение. Пусть дана диаграмма, изображенная на рис. 1.17. Найдем соответствующее ей аналитическое выражение. Для этого заштрихованные области представим в виде конъюнктов:

$$C_1 = a \wedge b \wedge \bar{c}, \quad C_2 = \bar{a} \wedge b \wedge c.$$

Искомое выражение получается при объединении этих конъюнктов:

$$x = C_1 \vee C_2 = b \wedge ((a \wedge \bar{c}) \vee (\bar{a} \wedge c)) = b \wedge (a + c).$$

Требуется выяснить, будет ли выполняться закон ассоциативности относительно штриха Шеффера:

$$(a | b) | c = a | (b | c) ?$$

Здесь можно не прибегать к таблицам истинности или диаграммам Эйлера — Венна. Достаточно знать связь между операциями, чтобы показать ложность этого закона:

$$a | (b | c) = 1 + a(1 + bc) = 1 + a - abc;$$

$$(a | b) | c = 1 + (1 + ab)c = 1 + c + abc.$$

Позиция конструктивистов состоит в том, чтобы любое тождество в математической логике получило свое убедительное обоснование, будь то закон дистрибутивности для дизъюнкции и конъюнкции или закон ассоциативности для этих операций — ничто не должно браться в качестве «аксиом», т.е. утверждений без доказательств. Аналогичный конструктивный прием можно использовать для доказательства тавтологии:

$$(a \wedge a(a \rightarrow b)) \rightarrow b = 1.$$

Доказательство:

$$a(1 + a + ab) \rightarrow b \quad ab \rightarrow b = 1 \cdot ab + abb = 1.$$

В следующем примере полиномальная форма уже не используется, а доказательство ведется посредством булевых операций. Требуется доказать:

$$((a + b) \rightarrow (a \vee b)) \wedge ((a \vee b) \rightarrow (a + b)) = a + b.$$

Доказательство:

$$\begin{aligned} ((a + b) \rightarrow (a \vee b)) \wedge ((a \vee b) \rightarrow (a + b)) &= ((\bar{a} \vee \bar{b}) \wedge (a \vee b)) \rightarrow (a \vee b) \wedge \\ &\wedge ((\bar{a} \vee \bar{b}) \vee (\bar{a} \vee \bar{b}) \wedge (a \vee b)) = ((a \wedge b) \vee (\bar{a} \vee \bar{b}) \vee (a \vee b)) \wedge ((\bar{a} \vee \bar{b}) \vee \\ &\vee (\bar{a} \vee \bar{b})) = 1 \wedge ((\bar{a} \wedge \bar{b}) \vee (\bar{a} \vee \bar{b})) = \bar{a} \vee \bar{b} = a + b. \end{aligned}$$

Часто встречаются доказательства смешанного характера. Например, требуется установить, что

$$\bar{A} \cup B = 1, \quad \text{если } A \subseteq B.$$

Когда встречается символ включения, его лучше всего перевести в тождество. Если A полностью включено в B , то с помощью диаграмм Эйлера — Венна легко проверить, что

$$A \cap B = A \quad \text{или} \quad A \cup B = B.$$

Далее, используя последнее равенство и аксиомы булевой логики, получим:

$$\bar{A} \cup B = \bar{A} \cup (A \cup B) = (\bar{A} \cup A) \cup B = 1 \cup B = 1.$$

Предположим, требуется доказать тождество

$$A \cap B = B \quad \text{или} \quad A \cup B = A.$$

В данном случае доказательство можно провести, по крайней мере, двумя способами. Первый способ:

$$\begin{aligned} B &= B \cup 0 = B \cup (A \cap \bar{A}) = (A \cup B) \cap (\bar{A} \cup B) = A \cap (\bar{A} \cup B) = \\ &= (A \cap \bar{A}) \cup (A \cap B) = 0 \cup (A \cap B) = A \cap B. \end{aligned}$$

Второй способ:

$$A \cap B = (A \cup B) \cap B = B.$$

При втором способе доказательства использовался закон поглощения, который, вообще говоря, не входит в систему провозглашенных ранее аксиом, но справедливость которого, тем не менее, легко установить отдельно. Отсюда вывод: всякое доказательство зависит от тех средств, которыми мы располагаем.

Закон де Моргана можно доказать следующим образом. «Умножив» тождество слева и справа на скобку $(a \vee b)$, получим:

$$(\bar{a} \vee \bar{b}) \wedge (a \vee b) = (\bar{a} \wedge \bar{b}) \wedge (a \vee b).$$

Так как $a \wedge a = 0$, то левая часть тождества равна нулю. Раскрывая скобки в правой части, убеждаемся, что и она также равна нулю.

По аналогии с этим доказательством кажется вполне правдоподобным и такое доказательство закона поглощения:

$$a = a \wedge (a \vee b).$$

Обе части тождества «умножаем» на скобку $(a \vee b)$:

$$a \wedge (a \vee b) = a \wedge (a \vee b) \wedge (a \vee b).$$

Используя закон идемпотентности, приходим к тождеству:

$$a \wedge (a \vee b) = a \wedge (a \vee b).$$

Однако такое доказательство является ошибочным, поскольку произвольное «умножение» в логике недопустимо. Возможно лишь такое «умножение» и «сложение», которое отвечает законам нуля и единицы, т.е. $a \wedge \bar{a} = 0$, $a \vee \bar{a} = 1$. Для иллюстрации сказанного возьмем заведомо ложное тождество:

$$(a \wedge b) \vee (\bar{a} \wedge c) \vee (a \wedge c) = (a \wedge b) \vee (\bar{a} \wedge c).$$

Воспользуемся законом поглощения в виде:

$$a = a \vee (a \wedge c).$$

«Сложив» его с исходным выражением, получим:

$$(a \wedge b) \vee (\bar{a} \wedge c) \vee (a \wedge c) \vee a = (a \wedge b) \vee (\bar{a} \wedge c) \vee (a \wedge c) \vee a,$$

что должно доказывать справедливость исходного выражения. Однако с помощью таблиц истинности (табл. 1.18) легко устанавливаем, что это не так. Две самые нижние строки, соответствующие правой (f_R) и левой (f_L) частям исходного выражения, отличаются друг от друга. Следовательно, тождество записано ошибочно. Истинным тождеством является:

$$(a \wedge b) \vee (\bar{a} \wedge c) \vee (b \wedge c) = (a \wedge b) \vee (\bar{a} \wedge c).$$

Таблица 1.18

a	0	1	0	1	0	1	0	1
b	0	0	1	1	0	0	1	1
c	0	0	0	0	1	1	1	1
$f_1 = a \wedge b$	0	0	0	1	0	0	0	1
$f_2 = \bar{a} \wedge c$	0	0	0	0	1	0	1	0
$f_3 = a \wedge c$	0	0	0	0	0	1	0	1
$f_R = f_1 \vee f_2$	0	0	0	1	1	0	1	1
$f_L = f_1 \vee f_2 \vee f_3$	0	0	0	1	1	1	1	1

Закончим этот подраздел различными примерами решения задач.

1) Доказать тождество:

$$a \rightarrow (b \wedge c) = a \mid (b \mid c).$$

Доказательство: $a \rightarrow (b \wedge c) = \bar{a} \vee (b \wedge c) = \bar{a} \vee (\overline{b \mid c}) = a \mid (b \mid c).$

2) Доказать тождество:

$$a + (b \wedge c) = (a \rightarrow b) \sim ((a + c) \wedge b).$$

Доказательство: $(a \rightarrow b) \sim ((a + c) \wedge b) = (1 + a + ab) \sim (ab + bc) =$
 $= 1 + (1 + a + ab) + (ab + bc) = a + (b \wedge c).$

3) Доказать тождество:

$$(a \wedge b \wedge c) \rightarrow (a \vee b \vee c) = (a \rightarrow b) \vee (b \rightarrow c) \vee (c \rightarrow a).$$

Доказательство:

$$(\bar{a} \wedge \bar{b} \wedge \bar{c}) \vee (a \vee b \vee c) = (\bar{a} \vee \bar{b} \vee \bar{c}) \vee (a \vee b \vee c) =$$

$$= (\bar{a} \vee b) \vee (\bar{b} \vee c) \vee (\bar{c} \vee a) = (a \rightarrow b) \vee (b \rightarrow c) \vee (c \rightarrow a).$$

4) Доказать тождество:

$$((a \downarrow b) \rightarrow (a + b)) \wedge ((a - b) \rightarrow (a \uparrow b)) = a \vee b.$$

Доказательство:

$$\begin{aligned} & ((a \downarrow b) \rightarrow (a + b)) \wedge ((a - b) \rightarrow (a \uparrow b)) = ((a \vee b) \vee ((a \wedge b) \vee (a \wedge \bar{b}))) \wedge \\ & \wedge ((\bar{a} \vee b) \vee (\bar{a} \vee \bar{b})) = ((a \vee b) \wedge ((a \vee b) \vee (\bar{a} \vee \bar{b}))) \wedge (a \vee 1) = \\ & = (x \wedge (x \vee y)) \wedge 1 = x, \quad \text{где } x = a \vee b, \quad y = \bar{a} \vee \bar{b}. \end{aligned}$$

5) Доказать тождество:

$$(A \cup \bar{C}) \cap (\bar{A} \cup \bar{B}) \cap (\bar{B} \cup C) \cap (\bar{A} \cup B) \cap (B \cup C) = 0.$$

Доказательство:

$$\bar{A} \cap C \cap (A \cup \bar{C}) = X \cap \bar{X} = 0, \quad \text{где } X = \bar{A} \cap C.$$

6) Доказать тождество:

$$(A \cup B \cup C) + (A \cap B \cap C) = (A \cup B \cup C) - (A \cap B \cap C).$$

Доказательство:

$$\begin{aligned} & (A \cup B \cup C) + (A \cap B \cap C) = ((\bar{A} \cap \bar{B} \cap \bar{C}) \cap (A \cap B \cap C)) \cup ((A \cup B \cup C) \cap \\ & \cup (\bar{A} \cup \bar{B} \cup \bar{C})) = 0 \cup ((A \cup B \cup C) \cap (\bar{A} \cup \bar{B} \cup \bar{C})) = (A \cup B \cup C) - (A \cap B \cap C). \end{aligned}$$

7) Доказать тождество:

$$((\bar{A} \cup B) \cap (B \cup C)) \cup ((A \cup \bar{C}) \cap (\bar{B} \cup C) \cap (\bar{A} \cup \bar{B})) = 1.$$

Доказательство:

$$\begin{aligned} & ((\bar{A} \cup B) \cap (B \cup C)) \cup ((A \cup \bar{C}) \cap (\bar{B} \cup C) \cap (\bar{A} \cup \bar{B})) = \\ & = (B \cup (\bar{A} \cap C)) \cup ((A \cup \bar{C}) \cap (\bar{B} \cup (\bar{A} \cap C))) = (B \cup X) \cup (\bar{X} \cap (\bar{B} \cup X)) = \\ & = (B \cup X) \cup (\bar{X} \cap \bar{B}) = (B \cup X) \cup (\bar{B} \cup \bar{X}) = 1, \quad \text{где } X = (\bar{A} \cap C). \end{aligned}$$

8) Преобразовать в СДНФ функцию:

$$f = (x + \bar{z}) \rightarrow (x \rightarrow y).$$

$$\begin{aligned} \text{Решение: } f_{\text{СДНФ}} = (x + \bar{z}) \rightarrow (x \rightarrow y) &= (x \vee \bar{z}) \wedge (\bar{x} \vee y) \wedge x \wedge \bar{y} = \\ &= (\bar{x} \vee \bar{z}) \wedge x \wedge \bar{y} = x \wedge \bar{y} \wedge \bar{z}. \end{aligned}$$

Правильность нахождения $f_{\text{СДНФ}}$ проверим с помощью таблицы истинности (табл. 1.19).

Таблица 1.19

x	y	z	$x + z$	$x \rightarrow y$	f
0	0	0	1	1	0
0	0	1	0	1	0
0	1	0	1	1	0
0	1	1	0	1	0
1	0	0	0	0	0
1	0	1	1	0	1
1	1	0	0	1	0
1	1	1	1	1	0

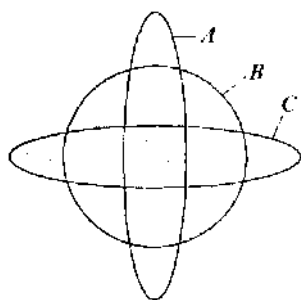


Рис. 1.18

9) Используя операции над множествами, представить заштрихованные области рис. 1.18 в виде компактного аналитического выражения.

Заштрихованные области можно представить четырьмя конституентами:

$$\begin{aligned} & (A \cap \bar{B} \cap \bar{C}) \cup (\bar{A} \cap \bar{B} \cap C) \cup (A \cap B \cap C) \cup (\bar{A} \cap B \cap \bar{C}) = \\ & = (A \cap ((\bar{B} \cap \bar{C}) \cup (B \cap C))) \cup (\bar{A} \cap ((\bar{B} \cap C) \cup (B \cap \bar{C}))) = \\ & = (A \cap (B \sim C)) \cup (\bar{A} \cap (B \sim C)) = \\ & = (A \cap (B \sim C)) \cup (\bar{A} \cap (B \sim C)) = A \sim (B \sim C). \end{aligned}$$

1.4. Задания на практическую работу по логике Буля

1) В табл. 1.20 заданы номера наборов аргументов, на которых логическая функция принимает значение, равное единице. Необходимо записать эту функцию в СДНФ и произвести ее минимизацию методом Куайна, методом сочетания индексов и методом Карно (результаты минимизации для всех трех случаев должны совпасть).

Таблица 1.20

№	Номера конституент							
1	4	6	8	9	10	11	15	-
2	2	3	6	7	8	14	15	-
3	0	2	4	5	6	7	9	11
4	1	3	5	7	8	12	14	-
5	1	2	5	6	10	12	13	14
6	0	3	7	9	10	12	13	14
7	0	2	5	8	10	11	14	15
8	0	1	2	4	7	10	11	12
9	0	5	7	8	9	12	13	15
10	0	1	2	3	9	12	14	15
11	0	1	4	6	7	8	9	15
12	0	3	4	5	7	8	10	11
13	0	2	3	7	8	12	14	15
14	0	2	9	10	11	12	13	15
15	1	2	5	6	8	9	10	14
16	1	3	6	7	9	11	13	-
17	1	6	7	9	12	13	14	15
18	1	2	4	10	11	13	14	-
19	1	5	6	7	9	13	14	15
20	1	2	3	4	9	12	15	-
21	2	3	4	7	10	12	13	14
22	2	3	5	8	10	11	12	14
23	3	4	5	7	8	9	10	11
24	4	5	7	9	10	11	12	15

2) Логическую функцию вашего варианта из предыдущего задания запишите в СКНФ. Как нужно модифицировать метод Куайна, метод сочетания индексов и метод Карно, чтобы приспособить их к СКНФ? Произведите минимизацию вашей функции, записанной в СКНФ, всеми тремя методами.

3) Ниже приведены логические выражения. Максимально упростите выражение своего варианта, воспользовавшись законами логики Буля. Затем с помощью таблиц истинности сравните ваше упрощенное выражение с исходным.

1. $(a \vee (\bar{d} \wedge b)) \wedge ((\bar{a} \wedge (\bar{b} \vee d)) \vee c) \vee \bar{c} \vee (a \vee (b \wedge \bar{d})),$
2. $((a \vee c) \wedge (a \vee d)) \wedge ((c \vee (c \wedge b)) \wedge \bar{c}) \vee \bar{a},$
3. $(\bar{b} \vee d) \wedge ((\bar{d} \wedge c) \vee (a \wedge c) \vee (\bar{d} \wedge \bar{c}) \vee (a \wedge \bar{c})) \wedge (b \vee d),$
4. $(a \vee \bar{c}) \wedge (\bar{a} \vee \bar{b}) \wedge (\bar{b} \vee c) \wedge (\bar{a} \vee b) \wedge (b \vee c),$
5. $(a \wedge c) \vee ((b \vee \bar{d}) \wedge (\bar{a} \vee \bar{d}) \wedge (d \vee b) \wedge (\bar{a} \vee d)) \vee (a \wedge \bar{c}),$
6. $((\bar{b} \vee \bar{c}) \wedge (a \vee b)) \vee (d \wedge c) \vee ((\bar{b} \wedge a) \vee c) \wedge (a \vee b),$
7. $(a \wedge \bar{c}) \vee (\bar{a} \wedge \bar{b}) \vee (b \wedge c) \vee (\bar{a} \wedge b) \vee (c \wedge \bar{b}),$
8. $((a \vee (c \vee (b \wedge c))) \wedge (\bar{c} \wedge \bar{d}) \wedge (c \wedge \bar{d})) \wedge (c \vee (\bar{d} \wedge \bar{c}) \vee d),$
9. $((a \vee \bar{a}) \wedge (\bar{b} \vee \bar{d}) \wedge (\bar{b} \vee \bar{c}) \wedge (\bar{c} \vee d)) \vee ((\bar{b} \vee c) \wedge (c \vee d)),$
10. $(a \vee \bar{c}) \wedge ((\bar{a} \wedge d) \vee (b \wedge d) \vee (\bar{a} \wedge \bar{d}) \vee (b \wedge \bar{d})) \wedge (a \vee c),$
11. $((d \wedge \bar{c}) \vee (\bar{d} \wedge \bar{b}) \vee (c \wedge \bar{b})) \wedge ((\bar{d} \wedge b) \vee (c \wedge b)) \wedge (\bar{a} \vee a),$
12. $((\bar{c} \wedge \bar{d}) \vee (b \wedge c)) \wedge (\bar{a} \vee \bar{d}) \wedge ((\bar{c} \vee \bar{b}) \wedge d) \vee (c \wedge b),$
13. $((a \vee b) \wedge (\bar{b} \wedge c \wedge d) \vee (\bar{a} \wedge \bar{b} \wedge c \wedge d) \vee \bar{b} \vee \bar{c} \vee d),$
14. $((a \wedge b) \vee (a \wedge \bar{b})) \vee ((\bar{a} \vee b) \wedge (c \vee \bar{d}) \wedge (\bar{a} \vee \bar{b}) \wedge (d \vee c)),$
15. $((\bar{b} \wedge c) \vee (\bar{c} \vee d) \vee \bar{a}) \wedge (\bar{a} \vee b \vee \bar{c} \vee d) \wedge (\bar{c} \vee d) \wedge a,$
16. $((b \vee c) \wedge (d \vee (\bar{b} \wedge \bar{c}))) \vee (\bar{d} \wedge \bar{a}) \vee ((c \vee b) \wedge (\bar{d} \vee \bar{c})),$
17. $(b \wedge d) \vee ((c \vee \bar{d}) \wedge (a \vee c) \wedge (\bar{d} \vee \bar{c}) \wedge (a \vee \bar{c})) \vee (\bar{b} \wedge d),$
18. $((\bar{c} \vee d) \wedge (d \vee a)) \vee ((b \vee \bar{b}) \wedge (\bar{c} \vee \bar{a}) \wedge (\bar{c} \vee \bar{d}) \wedge (\bar{d} \vee a)),$
19. $(a \wedge \bar{d}) \vee (((\bar{c} \wedge \bar{b}) \vee d) \wedge (c \vee b)) \vee ((\bar{d} \vee \bar{c}) \wedge (c \vee b)),$
20. $((d \vee (d \wedge c)) \wedge d) \vee \bar{b} \wedge ((b \vee d) \wedge (b \vee a)),$
21. $((\bar{b} \wedge (\bar{c} \vee a)) \vee d) \vee \bar{d} \vee (b \vee (c \wedge \bar{a})) \wedge (b \vee (\bar{a} \wedge c)),$
22. $((c \vee \bar{a}) \wedge (\bar{a} \vee \bar{b}) \wedge (a \vee c) \wedge (\bar{b} \vee a)) \vee (b \wedge \bar{d}) \vee (b \wedge d),$
23. $(d \vee (\bar{a} \wedge \bar{d}) \vee a) \wedge ((b \vee (\bar{d} \vee (d \wedge c))) \wedge (\bar{c} \wedge \bar{a}) \wedge (d \wedge \bar{a})),$
24. $(c \wedge \bar{b}) \vee (d \wedge c) \vee (\bar{b} \wedge c) \vee (\bar{d} \wedge \bar{c}) \vee (b \wedge \bar{d}).$

4) Аналитическим способом, т.е. на основе формул взаимосвязи между логическими операциями, докажите справедливость нижеприведенных тождеств. Затем с помощью диаграмм Эйлера — Венна подтвердите справедливость этого доказательства. Представьте одно из выражений (предварительно его упростив) в базисе элементарных функций. В наборе номеров базисных функций должны фигурировать цифры вашего варианта. Например, для варианта 12 могут быть взяты следующие функции: f_1, f_2, f_{12} . Недостающие функции отбираются на основе теории классов.

1. $((a \mid b) \mid (a \sim b)) \mid ((c \vdash d) \vdash (d \sim c)) = ((b \rightarrow c) \rightarrow (a \sim c)) \downarrow ((a \mid d) \mid (d \rightarrow \bar{b}))$,
2. $((a \wedge \bar{c}) \downarrow (b \sim c)) \wedge ((a \mid d) \sim (b \wedge d)) = ((a \mid b) \sim (a + \bar{b})) \rightarrow ((c + d) \wedge (d \rightarrow c))$,
3. $((a \downarrow b) \vee (a + b)) \sim ((c \sim d) \downarrow (c \sim d)) = ((c \rightarrow a) \wedge (c \rightarrow b)) \rightarrow ((a \downarrow d) \vee (b \downarrow d))$,
4. $((a \sim b) \sim (a \downarrow b)) \downarrow ((c \sim d) \downarrow (c \sim d)) = ((c \sim a) \downarrow (c \sim b)) \mid ((a \downarrow d) \downarrow (b \downarrow d))$,
5. $((a \wedge b) \vee (a + b)) \sim ((d \sim c) \downarrow (d \sim c)) = ((a \rightarrow c) \wedge (b \rightarrow c)) \rightarrow ((a \mid d) \mid (b \mid d))$,
6. $((a \vee b) \sim (a + b)) \vee ((c \sim d) \downarrow (c \sim d)) = ((c \sim a) \downarrow (c \sim b)) \wedge ((a \vee d) \sim (b \downarrow d))$,
7. $((d \rightarrow b) \rightarrow (\bar{c} \sim b)) \downarrow ((c \vee a) \mid (d \rightarrow a)) = ((\bar{c} \mid d) \sim (c + d)) \mid ((a \sim b) \rightarrow (\bar{a} \sim b))$,
8. $((a \mid b) \sim (\bar{a} + \bar{b})) \vee ((d \sim c) \downarrow (c \sim d)) = ((\bar{a} \downarrow \bar{d}) \downarrow (b \sim \bar{d})) \wedge ((a \rightarrow c) \sim (b \sim c))$,
9. $((c \sim a) \vee (c \sim a)) \sim ((d \sim b) \downarrow (d \sim b)) = ((a \vee b) \wedge (c \rightarrow b)) \rightarrow ((d \sim a) \vee (c \wedge d))$,
10. $((c \sim b) \sim (b \downarrow c)) \downarrow ((\bar{a} \sim \bar{d}) \downarrow (a \sim d)) = ((b \downarrow d) \downarrow (c \downarrow d)) \mid ((a \sim b) \downarrow (a \sim c))$,
11. $((a \sim d) \vee (a \sim d)) \sim ((b \sim c) \downarrow (b \sim c)) = ((b \rightarrow d) \wedge (a \sim b)) \rightarrow ((c \vee d) \mid (a \rightarrow c))$,
12. $((b \downarrow d) \downarrow (c \downarrow d)) \wedge ((a \rightarrow b) \sim (a \sim c)) = ((b \vee c) \sim (b + c)) \vee ((a \sim d) \downarrow (a \sim d))$,
13. $((c \rightarrow d) \mid (c + d)) \mid ((a \sim b) \rightarrow (a \wedge b)) = ((a \rightarrow \bar{c}) \rightarrow (a \sim d)) \downarrow ((b \rightarrow d) \mid (b \rightarrow \bar{c}))$,
14. $((b \wedge d) \downarrow (b \wedge c)) \wedge ((d \rightarrow a) \sim (c \sim a)) = ((c \mid d) \mid (\bar{c} \sim \bar{d})) \rightarrow ((a + b) \wedge (b \rightarrow a))$,
15. $((d \sim a) \vee (d \sim a)) \sim ((c \sim b) \downarrow (\bar{c} + \bar{b})) = ((a \vee b) \wedge (d \rightarrow b)) \rightarrow ((c \wedge d) \vee (c \sim a))$,
16. $((c \rightarrow d) \sim (c \sim d)) \vee ((a \wedge b) \downarrow (a + b)) = ((b \wedge c) \downarrow (b \sim d)) \wedge ((a \mid c) \sim (a \sim d))$,
17. $((\bar{c} \rightarrow b) \rightarrow (d \downarrow b)) \downarrow ((a \rightarrow d) \mid (a \rightarrow c)) = ((c \vee d) \mid (c \sim d)) \mid ((\bar{a} + \bar{b}) \rightarrow (a \sim b))$,
18. $((a \wedge c) \downarrow (b \sim \bar{a})) \wedge ((c \rightarrow d) \sim (b \sim d)) = ((b \mid c) \mid (b \sim c)) \rightarrow ((a + d) \wedge (a \rightarrow d))$,
19. $((b \downarrow \bar{d}) \vee (\bar{b} + d)) \sim ((a \sim c) \downarrow (a \sim c)) = ((\bar{c} \rightarrow b) \wedge (d \rightarrow c)) \rightarrow ((a \sim b) \vee (a \wedge d))$,
20. $((d \wedge a) \downarrow (b \wedge d)) \mid ((a \sim c) \downarrow (b \sim c)) = ((a + \bar{b}) \sim (b \wedge a)) \downarrow ((\bar{c} \sim \bar{d}) \downarrow (d \sim c))$,
21. $((a \downarrow b) \vee (\bar{a} \sim b)) \sim ((c \sim d) \downarrow (c \sim d)) = ((\bar{a} \rightarrow d) \wedge (\bar{d} \rightarrow b)) \rightarrow ((c \rightarrow a) \mid (c \rightarrow b))$,
22. $((c \rightarrow a) \sim (a + \bar{c})) \vee ((d \sim b) \downarrow (b \sim d)) = ((a \downarrow b) \downarrow (c \sim b)) \wedge ((d \rightarrow a) \sim (c \wedge d))$,
23. $((c \mid \bar{b}) \mid (c \sim \bar{b})) \mid ((\bar{a} + \bar{d}) \rightarrow (\bar{a} \sim \bar{d})) = ((c \rightarrow \bar{d}) \rightarrow (\bar{b} \sim \bar{d})) \downarrow ((\bar{b} \mid \bar{a}) \mid (\bar{a} \rightarrow c))$,
24. $((c \downarrow \bar{b}) \vee (c \sim \bar{b})) \sim ((\bar{d} \sim \bar{a}) \downarrow (\bar{d} \sim \bar{a})) = ((\bar{d} \rightarrow \bar{b}) \wedge (\bar{d} \rightarrow c)) \rightarrow ((\bar{b} \downarrow \bar{a}) \vee (c \downarrow \bar{a}))$.

5) Воспользовавшись таблицами истинности, представьте логические выражения вашего варианта двух последних заданий в СПНФ. Затем произведите минимизацию (результаты расчета проверьте с помощью таблиц истинности). Наконец, определите, к каким классам (0, 1, 2, 3 или 4) относятся ваши логические выражения.

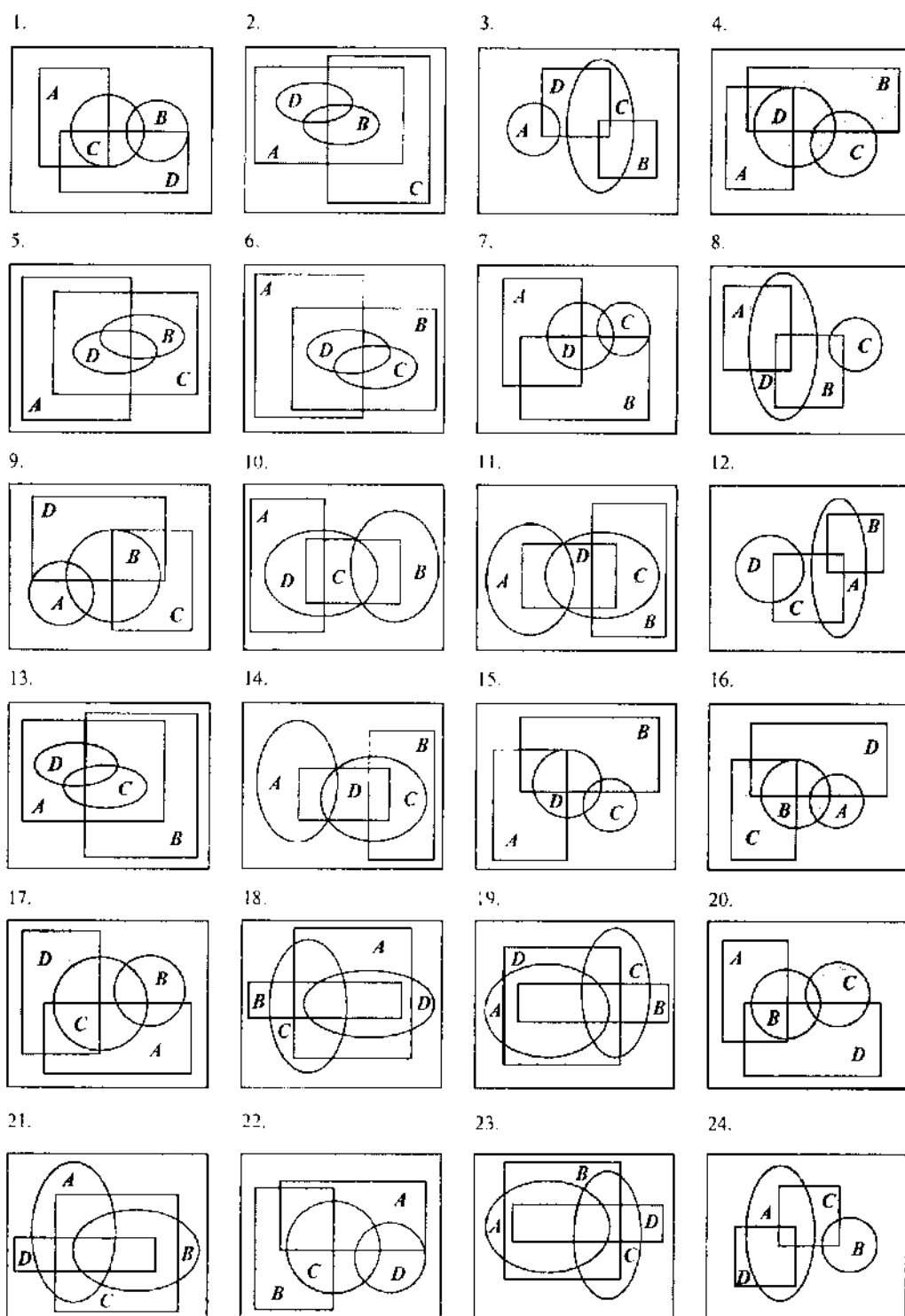
6) Докажите аналитическим путем справедливость трех предложенных вам выражений.

1. $(A \sim B) + (C \sim D) = A + C$, если $A \cap B = C \cap D$;
 $A \cup B \cup (\bar{A} \cap \bar{B} \cap C) \cup (\bar{A} \cap \bar{B} \cap \bar{C}) = 1$;
 $(a \sim b) \sim (a \mid b) = a \wedge b$.
2. $(A \sim B) + (B \sim C) + (B \sim A) + (C \sim B) = A + C$;
 $((A \cup B) \cap (B \cup C)) \cup ((\bar{A} \cup \bar{B}) \cap (\bar{B} \cup \bar{C})) = 1$;
 $a \rightarrow b = (a + b) \sim (b \sim a)$.

3. $(A - B) + (B - C) + (C - A) = (B - A) + (C - B) + (A - C)$;
 $((A \cup B) - C) \subset (A \cup (B - C))$;
 $((a \downarrow b) \downarrow (a \downarrow b)) + ((a \downarrow a) \downarrow (b \downarrow b)) = a + b$.
4. $(A \cup B) - (C \cup D) = B + C$, если $A \cap B = D$, $C \cap D = A$;
 $((B \cap \bar{C}) \cup (A \cap \bar{C})) \cap ((\bar{B} \cap C) \cup (A \cap C)) = \emptyset$;
 $a \rightarrow c = (a \vee (b \wedge c)) \rightarrow (a \vee b) \wedge c$.
5. $(A - (B - C)) - ((A - B) - C) = A \cap C$;
 $(\bar{A} \cup \bar{B}) \cap (\bar{B} \cup C) \cup ((\bar{A} \cup B) \cap (B \cup \bar{C})) = 1$;
 $(b \vee (c \wedge a)) \vee (a \vee (b \wedge c)) = a \vee b$.
6. $(A \cap B \cap C) \cup (A \cap \bar{B}) \cup (A \cap \bar{C}) = A$;
 $A \cap B = A$, если $\bar{A} \cup B = 1$;
 $(a | (b - c)) + (b | (a | c)) + (c - (a | b)) = (a \rightarrow (b \vee c)) \wedge (b \rightarrow (a \vee c)) \wedge (c \rightarrow (a \vee b))$.
7. $(A \cup B) + (A \cup C) + (B \cup C) = (A \cap B) + (A \cap C) + (B \cap C)$;
 $((A \cup B) - C) \subset ((A - C) \cup (B - A))$;
 $((a \downarrow b) \vee (a | b)) \rightarrow ((a \wedge b) | (a + b)) = 1$.
8. $((A \cup B) \cap C) \cup (\bar{A} \cap (\bar{B} \cup \bar{C})) = \bar{A} \cup C$;
 $(A - (B - C)) \subset ((A - B) \cup (B \cap C))$;
 $a \vee ((b - a) - b) = \emptyset$.
9. $(A \cap B) - (C \cup D) = (A - C) \cap (B - D)$;
 $(A \cap (B \cup C)) \subset ((A \cap B) \cup C)$;
 $a \sim (b | c) = ((a + b) \wedge c) + (a - c)$.
10. $(A - B) + (B - A) = A + B$;
 $P - Q = A \cap C$, если $P = A - (B - C)$, $Q = (A - B) - C$;
 $(a \sim b) - (a | b) = (a \downarrow a) \downarrow (b \downarrow b)$.
11. $((A \cap \bar{B}) \cup (\bar{B} \cap C)) \cap ((\bar{A} \cap B) \cup (B \cap \bar{C})) = \emptyset$;
 $(A - (B - C)) \subset (A \cup (B \cap C))$;
 $(b \vee (a \wedge c)) \supset (b \vee c) \wedge a = b \supset a$.
12. $(A \cup B) + (C \cup D) = A + B + C + D$, если $A \cap B = C \cap D$;
 $(A - B) - C = (A - C) - (B - C)$;
 $(a \wedge (\bar{b} \wedge c)) \vee ((a \vee c) \wedge b) = a \vee b$.
13. $((A \cap C) + (B \cap D)) \subset ((A + B) \cap (C + D))$;
 $(A + B) - C = (A - (B \cup C)) \cup (B - (A \cup C))$;
 $(a | b) \rightarrow (b \vee c) = b \vee c$.
14. $((\bar{B} \cap C) \cup (\bar{A} \cap \bar{B}) \cup (A \cap \bar{C})) \cap ((\bar{A} \cap B) \cup (B \cap C)) = \emptyset$;
 $(A - B) \cup (B - A) = (B - A) + (A - B)$;
 $(a \downarrow b) + (b \downarrow c) = (a + c) - b$.
15. $P = (A - B) - C$, $Q = A - (B - C)$, если $P \subset Q$;
 $(A - B) \cup (B - C) \cup (C - A) = (A \cup B \cup C) + (A \cap B \cap C)$;
 $(a \vee b \vee c) \sim (a \wedge b \wedge c) = (a \supset b) \wedge (b \supset c) \wedge (c \rightarrow a)$.

16. $((A \cup C) + (B \cup D)) \subseteq ((A + B) \cup (C + D))$;
 $((B \cap A) \cup C) \cap ((\overline{A \cup C}) \cup B) = B \cap C$;
 $((a + b) - c) \mid ((a - b) + c) = a \rightarrow (b \vee c)$.
17. $(C \cap B) \cup (\overline{B} \cap \overline{A}) \cup (\overline{B} \cap C) \cup (\overline{A} \cap B) \cup (A \cap \overline{C}) = 1$;
 $(A \cap B) \cup C = A \cap (B \cup C)$, если $C \subseteq A$;
 $(a \sim b) \vee ((a \downarrow c) \rightarrow (c \wedge d)) = (b - a) - c$.
18. $A - (B \cup C) = (A - B) \cap (A - C)$;
 $P \subseteq Q$, если $P = (A - B) - C$, $Q = A - (B - C)$;
 $((a \mid b) \rightarrow (b \vee c)) \downarrow (c \sim d) = (d - c) - b$.
19. $(A - (B \cup C)) \cup (B - (A \cup C)) \cup (C - (A \cup B)) = A + B + C + (A \cap B \cap C)$;
 $((A \cup B) - C) \subseteq ((A \cup B \cup C) - (A \cap B \cap C))$;
 $(a - b) - c = (a \sim b) \downarrow (b \vee c)$.
20. $A + B = (\overline{A} \cup B) + (A \cup \overline{B})$;
 $(A \cap B) \cup (B \cap C) \cup (A \cap C) = (A \cup B) \cap (B \cup C) \cap (A \cup C)$;
 $(a - b) + (a + c) \wedge b = \overline{a} + (b + c)$.
21. $(\overline{A} \cup B) + (\overline{B} \cup A) = (A \cap B) + (A \cup B)$;
 $(\overline{A} \cup B) \cap (B \cup C) \subseteq (\overline{A} \cup C)$;
 $a + (c - b) = (a \sim c) + (b \mid c)$.
22. $A + B = (A - B) + (B - A)$;
 $C \supseteq (A \cup B)$, если $C \supseteq A$, $C \supseteq B$;
 $(a \downarrow b) \downarrow ((\overline{a} \mid c) \downarrow (\overline{b} \mid d)) = a \vee b$.
23. $(A - B) + ((A + C) \cap B) = (A - C) + ((A + B) \cap C)$;
 $(A \cup B) \cap C = A \cup (B \cap C)$, если $A \subseteq C$;
 $((a \mid b) \rightarrow (b \vee c)) \vee (c \sim d) = d \rightarrow (c \vee b)$.
24. $(A + (A - B)) \cap (1 - B) = 0$;
 $((A - C) \cup (B - A)) \subseteq (A \cup B)$;
 $a \sim (b \mid c) = (a \rightarrow b) \sim (a + c) \wedge b$.

7) Ниже приведены диаграммы Эйлера — Венна. Представьте заштрихованные и отдельно незаштрихованные области максимально компактными аналитическими выражениями, в которых бы использовалось минимальное количество логических операций и букв. С этой целью сначала выразите все заштрихованные области через конститuenty-конъюнкты, а незаштрихованные — через конститuenty-дизъюнкты, и только после этого приступайте к упрощению полученных форм (результаты проверьте на таблицах истинности).



Под *высказыванием* мы будем понимать грамматически правильное повествовательное предложение, про которое можно сказать, что оно либо истинно, либо ложно, например:

«Киев — столица Украины»,
«Париж — столица России».

Первое высказывание является *истинным*, второе — *ложным*.

Возьмем два *простых* высказывания:

A = «На улице идет дождь»,
 B = «Над моей головой раскрыт зонтик».

С помощью пяти логических связок можно образовать следующие *сложные* высказывания:

1) *отрицание*: $\bar{A}$ = «На улице *не* идет дождь»;

2) *дизъюнкция*:

$\bar{A} \vee B$ = «На улице *не* идет дождь *или* над моей головой раскрыт зонтик»;

3) *конъюнкция*:

$A \wedge \bar{B}$ = «На улице идет дождь *и* над моей головой *не* раскрыт зонтик»;

4) *импликация*:

$A \rightarrow B$ = «Если на улице идет дождь, *то* над моей головой раскрыт зонтик»;

5) *эквивалентность*:

$B \sim A$ = «Над моей головой раскрыт зонтик *тогда и только тогда*, когда на улице идет дождь».

Другие логические связки, известные нам по логике Буля, в логике высказывания не используются. Теперь сделаем по поводу каждой из пяти указанных связок небольшие замечания.

Отрицание. Высказывание A по-другому можно прочесть так:

«*Истинно* то, что на улице идет дождь».

Поэтому, если $A = 0$, то это означает, что на улице не идет дождь. Дополняющее высказывание $\bar{A}$ также ориентируется на истинное высказывание, т.е. его следует понимать как

«*Истинно* то, что на улице *не* идет дождь».

Тогда $\bar{\bar{A}} = 1$ будет обозначать ту же самую ситуацию, что и в предыдущем случае, т.е. отсутствие дождя.

Дизъюнкция. В нашем конкретном примере дизъюнкция двух высказываний $\bar{A}$ и B , в принципе, может подразумевать и конъюнкцию этих же высказываний. Однако часто грамматический союз *или* не включает в себя союз *и*. Например, пусть будут даны два других высказывания:

P = «Петр находится в кинотеатре»,

Q = «Петр находится в бассейне».

Если для нас не столь важно, где находится Петр, то мы, конечно, можем использовать союз *или* с включенным в него союзом *и*, формально записав:

$P \vee Q$ = «Петр находится в кинотеатре *или/и* в бассейне».

Но если нам нужно точно установить, где находится Петр, то мы обязаны исключить случай одновременного присутствия Петра в кинотеатре и бассейне, т.е. формально записать:

$$(P \vee Q) \wedge (\overline{P \wedge Q}) .$$

Подобные высказывания называются *строгой дизъюнкцией*, которая означает «*либо P, либо Q, но не P и Q одновременно*». И хотя, с точки зрения логики Буля, эта логическая операция равносильна операции *симметрической разности*:

$$P \dot{+} Q = (P \vee Q) \wedge (\overline{P \wedge Q}),$$

исторически сложилось так, что символ «+» в логике высказываний не используется.

Конъюнкция. Логический союз *и* необязательно должен представляться через грамматический союз *и*. В частности, выше приведенное выражение можно прочитать несколько иначе:

$A \wedge \overline{B}$ = «На улице идет дождь, *а* над моей головой *не* раскрыт зонтик».

Союзы *а* и *но* по смыслу часто совпадают с союзом *и*, поэтому они используются в сложных конъюнктивных предложениях.

Однако языковая ситуация может стать такой, что союз *и* перестает играть роль *конъюнкции*; приведем два сложных предложения:

«Ему стало страшно *и* он убил человека.»

«Он убил человека *и* ему стало страшно.»

Здесь некоммутативность двух простых предложений очевидна, поскольку мы имеем дело со скрытой *импликацией*, когда одно простое предложение обуславливает другое.

Импликация. Высказывание типа «*если A, то B*» носит *объясняющий* характер. Оно как бы разъясняет нам, почему имеет место событие **B** — потому что имело место событие **A**. Это свойство импликации особенно ценно для логики высказываний, о чем мы подробно остановимся в следующем подразделе.

Объясняющий характер импликации тесно связан с *причинно-следственным отношением*, при котором **A** выступает в роли причины, а **B** — следствия. Причинно-следственная связь между **A** и **B** грамматически может быть оформлена предложениями: «**A** является достаточным основанием для **B**», «**B**, потому что **A**», «**B** при условии выполнения **A**» и т.д. Если под **A** и **B** понимать прежние высказывания, то результат причинно-следственного отношения можно оформить следующей таблицей истинности (табл. 1.21). Вторая строка таблицы говорит об отсутствии причинно-следственного отношения между событиями **A** и **B**.

Таблица 1.21

A	B	A → B	Результаты
0	0	1	Останусь сухим
1	0	0	Вымокну
0	1	1	Останусь сухим
1	1	1	Останусь сухим

Эквивалентность. Высказывание «**A** эквивалентно **B**» может быть с успехом заменено на «**A** равно **B**», «**A** тождественно **B**», «**A** равносильно **B**», «**A** тогда и только тогда, когда **B**» и т.д. Так как эквивалентность выражается через конъюнкцию двух импликаций:

$$A \sim B = (A \rightarrow B) \wedge (B \rightarrow A),$$

то это отношение часто возникает при одновременном выполнении двух условий: «из **A** следует **B**» и «из **B** следует **A**». Таким образом, при эквивалентности двух событий невозможно одному из них приписать роль только причины, а другому — только следствия. Например, два события:

R = «Нарастание анархии в обществе»,

S = «Падение авторитета власти»,

являются вполне равнопорядковыми событиями, поскольку причиной нарастания анархии в обществе является падение авторитета власти; и наоборот, падение авторитета власти происходит из-за нарастания анархии в обществе. В данной ситуации бессмысленно обвинять только власть в слабости и некомпетентности или обвинять народ в несознательности и недисциплинированности.

События **R** и **S** образуют *логический круг*; их будем называть сильно связанными событиями и выражать следующими тождественными формами:

$$R \sim S = (R \wedge S) \sim (R \vee S) = (R \vee S) \rightarrow (R \wedge S).$$

Понятие «сильной связанности» совпадает с понятием «эквивалентности», если речь идет о двух событиях. Но возьмем, к примеру, хорошо известное объяснение, на чем держится Земля:

Земля (X) держится на трех китах (Y), киты (Y) держатся на водах океана (Z), океан (Z) держится на Земле (X).

Последовательность, куда входят три названных объекта **X**, **Y** и **Z**, тоже образуют логический круг:

$$(X \rightarrow Y) \wedge (Y \rightarrow Z) \wedge (Z \rightarrow X).$$

Однако отношение эквивалентности (быть взаимной опорой друг для друга) между всеми тремя объектами, т.е.

$$X \sim Y \sim Z,$$

здесь не возникает, да и не могло возникнуть, так как мы ведь не утверждаем, что Земля является непосредственной опорой для китов ($X \sim Y$), или что киты являются непосредственной опорой для вод океана ($Y \sim Z$). Поэтому эквивалентность в данном случае проявляется в весьма своеобразной форме:

$$(X \wedge Y \wedge Z) \sim (X \vee Y \vee Z) \quad \text{или} \quad (X \vee Y \vee Z) \rightarrow (X \wedge Y \wedge Z),$$

что можно истолковать в случае операции эквивалентности как: одновременное появление всех трех опор произойдет *тогда и только тогда, когда* возникнет хотя бы одна из опор, и наоборот; для операции импликации: *если* возникнет какая-нибудь одна из опор, *то* это приведет к появлению всех трех опор. Таким образом, *сильная связанность* или *логический круг* есть нечто промежуточное между *причинно-следственным отношением* и *отношением эквивалентности*. Подобные отношения возникают очень часто, например между членами преступной организации, где все связаны круговой порукой и невозможно найти крайнего.

В заключение этого вводного подраздела хотелось бы подчеркнуть важность различия между *языком* и *метаязыком*, между *объектными* и *субъектными* высказываниями. Пренебрегая этим различием, мы рискуем впасть в противоречие, которое называется *логическим парадоксом*.

С древних времен известен так называемый «Парадокс лжеца». Изложим его суть.

«Я лжец», — сказал лжец.

Итак, некий лжец сообщает о себе, что он лжец. Следовательно, здесь он выступает в своем противоположном качестве, а именно — *нелжеца*. Поэтому приведенное высказывание на самом деле нужно понимать иначе:

«Я лжец», — сказал нелжец.

Теперь получается, что правдивый человек сообщает о себе, что он лжец. Правдивому человеку мы, естественно, должны верить. Поэтому второе высказывание следует понимать все-таки так, как это отражено в первом высказывании. Таким образом, возникает неопределенность, заключающаяся в том, что непонятно, как квалифицировать говорящего — как лжеца или как нелжеца, т.е. непонятно, как идентифицировать высказывание — как истинное или как ложное.

Парадокс возник потому, что в приведенных высказываниях не делается разграничения между двумя принципиально различными логическими уровнями. Помимо «лжеца» или «нелжеца» в данной логической ситуации участвует субъект (метанаблюдатель). Если провести четкое синтаксическое отделение смыслового содержания, которое должно относиться к нам, как метанаблюдателям, от прочей семантики объектных персонажей, то логическое противоречие будет снято. Ситуацию с лжецом необходимо представлять следующим образом:

«Я лжец», — сказал лжец.

«Это истинно», — сказал метанаблюдатель.

«Я лжец», — сказал нелжец.

«Это ложно», — сказал метанаблюдатель.

«Я нелжец», — сказал лжец.

«Это ложно», — сказал метанаблюдатель.

«Я нелжец», — сказал нелжец.

«Это истинно», — сказал метанаблюдатель.

*ложно * ложно = истинно,*

*истинно * ложно = ложно,*

*ложно * истинно = ложно,*

*истинно * истинно = истинно.*

Если приведенные четыре конструкции записать через два слова *истинно* и *ложно*, то получим обыкновенную таблицу умножения для группы из двух элементов типа *плюс* и *минус* единицы. Однако источником противоречий в логике высказываний необязательно является смещение именно *объектного* и *субъектного* уровней. Неопределенность может возникнуть между различными объектными уровнями. В качестве примера приведем следующую фразу: «*Нет правил без исключений*». Но фраза, стоящая здесь в кавычках сама является правилом. Так какое исключение должно следовать из него? Разберем это противоречие, несколько изменив его семантику. Пусть имеется высказывание:

$A =$ «Любое высказывание является ложным».

Так как A является высказыванием, на него должно распространяться сказанное в предложении A . Рассмотрим два случая:

- 1) Пусть $A = 1$. Это означает, что $A = \langle A = 0 \rangle = 1$, т.е. $A = 0$.
- 2) Пусть $A = 0$. Это означает, что $A = \langle A = 0 \rangle = 0$, т.е. $A = 1$.

Таким образом, в обоих случаях имеем противоречие. Чтобы его избежать, нужно произвести логическое разграничение всего множества высказываний на два принципиально различных класса — A и B . В этом случае формальная запись первоначальной фразы будет иметь вид: $A = \langle B = 0 \rangle$; тогда при $A = 1$, $B = 0$ и при $A = 0$, $B = 1$.

Приведем еще один пример известного парадокса. Английский логик Бертран Рассел поведал такую притчу:

В одной из деревень жил парикмахер. Он брил всех тех жителей деревни, кто не брился сам.

Рассел задался вопросом: *может ли парикмахер побрить самого себя?* Начинаем рассуждать: если парикмахер захочет побрить самого себя, то как житель этого селения, который бреется сам, он не вправе это сделать; но если парикмахер не станет бриться, то уже как житель селения, который не бреется сам, он обязан будет себя побрить.

Выразим семантику этого противоречия формальным языком. Обозначим через A парикмахера и пусть $P(A, B)$ означает высказывание « A бреет B ». Тогда ситуацию, которую мы имеем в селении, можно описать двумя метавысказываниями:

- 1) Если $P(B, B) = 0$, то $P(A, B) = 1$.
- 2) Если $P(B, B) = 1$, то $P(A, B) = 0$.

Когда парикмахер рассматривается в качестве рядового жителя селения ($A = B$), оба метавысказывания становятся внутренне противоречивыми:

- 1) Если $P(A, A) = 0$, то $P(A, A) = 1$.
- 2) Если $P(A, A) = 1$, то $P(A, A) = 0$.

Выражение $P(A, B)$ может означать « A учит B », « A развлекает B » и т.д. При этом под A понимается учитель, юморист и т.д. И хотя A , наряду с B , формально является объектной переменной, ее нельзя ставить на один уровень с B , так как именно относительно A сформулированы метавысказывания.

Логика — это наука о способах доказательства. Выясним, в чем, собственно, состоит различие в построении доказательств в логике высказываний и логике Буля.

В булевой логике все доказательства строились на *отношении эквивалентности*. Даже если в множественных выражениях и фигурировало отношение включения, что является частным случаем *отношения порядка*, то его мы переводили в тождество. Две логические функции считались эквивалентными, если они давали на соответствующих наборах аргументов абсолютно одинаковые значения нулей и единиц. При использовании формальной записи логических выражений отдельные звенья цепи любого доказательства там были связаны через символ равенства «=». Отношение эквивалентности удовлетворяет трем законам —

рефлексивности: $A = A$;
 симметричности: если $A = B$, то $B = A$;
 транзитивности: если $A = B$ и $B = C$, то $A = C$.

В логике высказываний все доказательства строятся на *отношении порядка*, т.е. на отношении, которое существует между причиной и следствием. Здесь уже отдельные звенья цепи доказательства связаны символом импликации. Однако символ импликации « $\rightarrow$ » при логическом выводе мы будем заменять на символ « $\Rightarrow$ », подобно тому, как в логике Буля используются два символа эквивалентности — « $\sim$ » и « $=$ ». Символ « $\sim$ » является *объективным*, а « $=$ » — *субъективным*. Таким образом, следует различать язык логики высказываний и *метаязык* исследователя. Во избежание путаницы введем еще два *метасимвола*: вместо *объективной конъюнкции* « $\wedge$ » будем использовать *субъективный символ метаконъюнкции* — « $,$ », а вместо *объективной дизъюнкции* « $\vee$ » — *субъективную метадизъюнкцию* « $;$ ». Тогда утверждение, которое требуется доказать, в логике высказываний оформляется в виде следующего *причинно-следственного отношения*:

$$P_1, P_2, \dots, P_{n-1}, P_n \Rightarrow C, \quad (1.1)$$

где P_i — *посылка (причина)*, C — *заключение (следствие)*. Читается: «Если посылки $P_1, P_2, \dots, P_{n-1}, P_n$ истинны, то заключение C тоже истинно» или, по-другому: «Если причины $P_1, P_2, \dots, P_{n-1}, P_n$ имели место, то будет иметь место и следствие C ».

Чтобы не спутать *объективное высказывание* (предложение) с *субъективным высказыванием*, справедливость которого мы намереваемся установить, условимся предложения типа (1.1) называть *клаузой (clause)*.

Клауза — это *метапредложение*, в котором использовано *отношение порядка*, оформленное через символ *метaimпликации* « $\Rightarrow$ ». Как и отношение эквивалентности, отношение порядка удовлетворяет трем законам —

рефлексивности: $A \Rightarrow A$;
 антисимметричности: если $A \Rightarrow B$, то $\bar{B} \Rightarrow \bar{A}$;
 транзитивности: если $A \Rightarrow B$ и $B \Rightarrow C$, то $A \Rightarrow C$.

В отличие от эквивалентности отношение порядка предполагает выполнение закона антисимметричности, который можно записать так:

$$\text{если } A \rightarrow B \text{ и } B \Rightarrow A, \text{ то } A \equiv B.$$

Клауза есть именно формальная запись доказываемого предложения. Вместо букв в ней можно подставить объектные высказывания, и тогда клауза наполняется конкретным содержанием, которое уже именуется *семантикой* или *легендой*. Пример клаузы:

$$A \rightarrow B, A \rightarrow B.$$

Если принять, что

$$A = \text{сверкнула молния}, B = \text{грянул гром},$$

то можно составить следующую легенду:

Известно, что если сверкнула молния, то после этого грянет гром. Молния сверкнула. Следовательно, должен и грянуть гром.

Над субъектом, который формулирует метаясуждение, может стоять другой субъект, для которого уже предложения первого субъекта окажутся объектными. Тогда клаузу (1.1) второй субъект или метасубъект запишет для себя следующим логическим выражением:

$$(P_1 \wedge P_2 \wedge \dots \wedge P_{n-1} \wedge P_n) \rightarrow C.$$

Преобразовав это выражение в дизъюнкт, получим:

$$\bar{P}_1 \vee \bar{P}_2 \vee \dots \vee \bar{P}_{n-1} \vee \bar{P}_n \vee C.$$

Отсюда легко находим:

$$(P_1 \wedge P_2 \wedge \dots \wedge P_{n-1}) \rightarrow (\bar{P}_n \vee C).$$

Поэтому клауза (1.1) может быть представлена в другой эквивалентной форме:

$$P_1, P_2, \dots, P_{n-1} \rightarrow \bar{P}_n; C. \quad (1.2)$$

В силу коммутативности конъюнкции на месте посылки P_n может оказаться любая другая, причем не одна. Например, клауза:

$$P_1, P_2, P_3, P_4 \Rightarrow C_1; C_2; C_3$$

может быть преобразована в другую эквивалентную форму:

$$P_4, \bar{C}_2, P_1, \bar{C}_1 \Rightarrow \bar{P}_1; C_3; \bar{P}_2. \quad (1.3)$$

Однако клауза (1.1) по сравнению с (1.2) и другими подобными формами, типа (1.3), имеет определенные преимущества и, в частности, используется в языке логического программирования ПРОЛОГ. Ее называют *хорновской*. Произвольную клаузу всегда можно свести путем эквивалентных преобразований к хорновскому виду.

Если символ импликаций « $\Rightarrow$ » клаузы (1.2) сместить в крайнее левое положение, то она превратится в *тавтологию*; если же это сместить в крайнее правое положение, то — в *противоречие*:

$$1 \Rightarrow \bar{P}_1; \bar{P}_2; \dots; \bar{P}_{n-1}; \bar{P}_n; C \text{ — тавтология,}$$

$$P_1, P_2, \dots, P_{n-1}, P_n, P_n, \bar{C} \Rightarrow 0 \text{ — противоречие.}$$

Ниже мы рассмотрим пять конкретных методов доказательства справедливости логических клауз — *аксиоматический метод, метод таблиц истинности, метод резолюций, метод Вонга и метод натурального исчисления*. Как и в логике Буля, в логике высказываний существуют *аксиоматический и конструктивный* подходы доказательств логических выражений. Два первых из только что названных пяти как раз являются яркими представителями таких подходов, остальные три метода — смешанной стратегии. Аксиоматическое построение логики высказываний состоит в том, чтобы попытаться вычлени из бесконечного числа истинных клауз *независимую систему аксиом*, с помощью которой можно было бы установить справедливость любых других клауз.

Мы уже сказали, что доказательство в логике высказываний строится на отношении порядка, которое является *более общим случаем* отношения эквивалентности. В самом деле, закон симметричности:

$$\text{если } A = B, \text{ то } B = A$$

всегда можно представить в антисимметричной форме:

$$\text{если } A = B, \text{ то } \bar{B} = \bar{A},$$

но не наоборот. Следовательно, логика высказывания является *расширением* логики Буля. Поэтому все истинные тождества логики Буля *автоматически* становятся справедливыми клаузами логики высказываний. Например, *закон склеивания*:

$$(A \vee B) \wedge (A \vee \bar{B}) = A$$

можно представить следующими справедливыми клаузами:

$$(A \vee B), (A \vee \bar{B}) \Rightarrow A, \quad A \Rightarrow (A \vee B) \wedge (A \vee \bar{B}),$$

$$1 \Rightarrow ((A \vee B) \wedge (A \vee \bar{B})) \sim A, \quad A \vee B \Rightarrow (A \vee \bar{B}) \rightarrow A.$$

Таким образом, независимая система аксиом логики Буля, которая состоит из четырех законов — *коммутативности, ассоциативности, дистрибутивности, нуля и единицы* — автоматически становится системой аксиом и логики высказываний. Для выражения же *отношения порядка*, в принципе, требуется лишь какое-то одно *элементарное* высказывание, к которому можно было бы сводить все остальные более сложные высказывания. Сейчас мы его и введем.

Очевидная сентенция:

Истину может изречь всякий.

На формальном языке логики высказываний эту сентенцию можно представить следующей клаузой:

$$A \rightarrow B \rightarrow A.$$

Она означает: «если *A* истинно, то источником этой истинности может быть что угодно, например *B*». Если произвести эквивалентное преобразование этой клаузы

$$A, B \Rightarrow A, \tag{1.4}$$

то семантика ее тоже изменится, и станет примерно такой: «если ранее было установлено, что *A* истинно, то истинность *B* не может проявиться так, что *A* станет ложным» или «истинность одного высказывания (*B*) не может повлиять на истинность другого высказывания (*A*)». Путем эквивалентных преобразований

клаузу (1.4) всегда можно преобразовать к другим формам:

$$\bar{A} \Rightarrow \overline{A \wedge B}, \quad A \Rightarrow A; B, \quad I \Rightarrow (A \wedge B) \rightarrow A, \dots$$

Однако в качестве основной аксиомы логики высказываний, выражающей отношение порядка, мы возьмем клаузу (1.4).

Теперь на первом нашем примере, который был приведен выше, выясним, как производится доказательство справедливости логической клаузы. Исходная клауза имела вид:

$$A, A \rightarrow B \Rightarrow B. \quad (1.5)$$

Преобразуем ее к несколько иному виду:

$$A \wedge (\bar{A} \vee B) \Rightarrow B.$$

После раскрытия скобок и упрощения сразу же приходим к аксиоме порядка (1.4). Доказанная элементарная клауза (1.5) известна с времен Аристотеля и играет исключительно важную роль в логике высказываний. Она имеет даже специальное латинское название — *modus ponens* — *правило отделения*. Если в процессе доказательства справедливости какой-либо сложной клаузы удалось свести ее к клаузе (1.5), будем считать, что доказательство состоялось.

Закон антисимметричности по существу определяет правила действия по переносу объектных высказываний относительно символа метампликации « $\Rightarrow$ ». Что же касается двух других законов отношения порядка, то они, в принципе, сводятся к аксиоме порядка. Так закон *рефлексивности* путем использования закона о единице может быть записан как:

$$A, I \Rightarrow A,$$

что является частным случаем аксиомы порядка. Закон *транзитивности* также может быть представлен в несколько иной форме:

$$A \rightarrow B, B \rightarrow C \Rightarrow A \rightarrow C,$$

а эту клаузу уже можно доказывать путем сведения ее к аксиоме порядка. Доказательство проведем в три этапа:

1) перенесем A влево за знак метампликации —

$$A, A \rightarrow B, B \rightarrow C \Rightarrow C;$$

2) воспользуемся правилом отделения, которое нами уже доказано, для первых двух посылок —

$$B, B \rightarrow C \Rightarrow C;$$

3) затем еще раз воспользуемся этим же правилом, но для третьей посылки и вновь полученной, что приведет нас к аксиоме порядка в форме —

$$B, C \Rightarrow C.$$

Таким образом, закон транзитивности доказан.

Убедимся в истинности тавтологии:

$$I \Rightarrow (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)).$$

Доказательство:

1) произведем эквивалентные преобразования —

$$A \rightarrow (B \rightarrow C), A \rightarrow B, A \Rightarrow C;$$

2) воспользуемся правилом отделения —

$$B \rightarrow C, B \rightarrow C ;$$

3) воспользовавшись еще раз правилом отделения, приходим к аксиоме порядка в форме предыдущего примера.

Докажем справедливость клаузы, которая построена на основе тождественного закона склеивания:

$$1 \Rightarrow (\bar{A} \rightarrow B) \rightarrow ((\bar{A} \rightarrow \bar{B}) \rightarrow A) .$$

После эквивалентных преобразований:

$$(A \vee B) \wedge (A \vee \bar{B}) \rightarrow A$$

она сводится к закону рефлексивности, т.е. к частному случаю аксиомы порядка, рассмотренному выше.

Исторически первой системой аксиом классической логики была система, предложенная Г. Фреге:

1. $1 \rightarrow A \rightarrow (B \rightarrow A) ,$
2. $1 \Rightarrow (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)) ,$
3. $1 \Rightarrow (A \rightarrow (B \rightarrow C)) \rightarrow (B \rightarrow (A \rightarrow C)) ,$
4. $1 \Rightarrow (A \rightarrow B) \rightarrow (\bar{B} \rightarrow \bar{A}) ,$
5. $1 \rightarrow A \rightarrow \bar{\bar{A}} , \quad 1 \rightarrow \bar{\bar{A}} \rightarrow A .$

Первая из аксиом Фреге является нашей аксиомой порядка. Вторая «аксиома» нами доказана выше. Остальные «аксиомы» представляют собой тождества логики Буля, записанные в форме клауз.

Позднее Я. Лукасевич (1878–1956) уменьшил число аксиом в системе Фреге с пяти до трех —

1. $1 \Rightarrow A \rightarrow (B \rightarrow A) ,$
2. $1 \Rightarrow (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)) ,$
3. $1 \Rightarrow (A \rightarrow B) \rightarrow (\bar{B} \rightarrow \bar{A}) .$

Вместо третьей «аксиомы» в современной логике часто используют «аксиому» вида:

$$1 \Rightarrow (\bar{A} \rightarrow B) \rightarrow ((\bar{A} \rightarrow \bar{B}) \rightarrow A) ,$$

вытекающую из тождественного закона склеивания. Однако, по нашему мнению, в процессе доказательств истинности клауз без аксиом булевой логики обойтись невозможно. Поэтому есть смысл говорить о *пяти* основополагающих законах логики высказываний: *закона отношения порядка*, а также законов *коммутативности*, *ассоциативности*, *дистрибутивности*, *нуля* и *единицы*.

Теперь вспомним о *логическом круге*, который возникал у нас в связи с «объяснением» опоры Земли. Тогда мы пришли к логическому соотношению вида:

$$(X \vee Y \vee Z) \rightarrow (X \wedge Y \wedge Z) .$$

Если перейти на метаязык, то получим клаузу:

$$X; Y; Z \Rightarrow X, Y, Z .$$

Данное выражение противоречит аксиоме порядка. Это говорит об ошибке в объяснении. Сказав, что Земля держится на трех китах, киты — на водах океана, а океан — на Земле, мы нарушили естественный порядок вещей — причину обусловили следствием. В связи с чем математический аппарат логики высказываний сразу же дал сбой. В приведенной клаузе уже нельзя будет переносить посылки через символ метaimпликации, так как

$$(X \vee Y \vee Z) \cdot \rightarrow (X \wedge Y \wedge Z) \neq (X \vee Y) \rightarrow (\bar{Z} \wedge X \wedge Y \wedge Z).$$

Отсюда вывод: *метадизъюнкция* « $\cdot \rightarrow$ » не может разделять две различные посылки, а *метаконъюнкция* « $\cdot$ » — два различных заключения; это приводит к невозможности использовать аппарат логики высказываний.

Противоположным к *аксиоматическому* является *конструктивный* метод доказательства, основанный на *таблицах истинности*. Чтобы понять его, достаточно составить таблицу истинности для какого-нибудь одного примера. Пусть дана следующая легенда:

Кассир Сидорова сказала, что она видела водителя контейнеровоза Иванова в комнате отдыха. Эта комната по ее словам находится рядом с помещением склада готовой продукции. Стреляли в складе. Водитель заявил, что он никаких выстрелов не слышал. Вывод следователя: если кассир говорит правду, то водитель вводит следствие в заблуждение; не могут кассир и водитель одновременно говорить правду.

Введем обозначения для высказываний:

- A = «Кассир сказала правду»,
- B = «Водитель находился в комнате отдыха»,
- C = «Комната отдыха находится вблизи склада»,
- D = «Водитель слышал выстрелы»,
- E = «Водитель сказал правду».

Посылки следователя:

Если кассир сказала правду, то водитель находился в комнате отдыха —

$$P_1 = A \rightarrow B.$$

Если водитель находился в комнате отдыха, то он должен был слышать все, что делается на складе —

$$P_2 = B \rightarrow C.$$

Если он имел возможность слышать, что делается на складе, то он слышал и выстрелы —

$$P_3 = C \rightarrow D.$$

Если верить водителю, то он не слышал выстрелов —

$$P_4 = E \rightarrow \bar{D}.$$

Заключение следователя:

Водитель меня обманывает при условии, что кассир говорит правду —

$$C_1 = A \rightarrow \bar{E}.$$

Кассир и водитель одновременно говорят правду —

$$C_2 = A \wedge E.$$

Формальная запись легенды:

$$A \rightarrow B, B \rightarrow C, C \rightarrow D, E \rightarrow \bar{D} \rightarrow C_1.$$

Доказать истинность следствия C_1 аксиоматическим методом не составит труда. Для этого нужно воспользоваться тождеством:

$$E \rightarrow \bar{D} \rightarrow D \rightarrow \bar{E},$$

и затем трижды применить закон транзитивности. Заключение C_2 ошибочно, так как

$$A \rightarrow \bar{E} \Rightarrow A \wedge E,$$

что означает

$$\bar{A} \vee \bar{E} \Rightarrow A \wedge E \quad \text{или} \quad \bar{A} \wedge \bar{E} \rightarrow A \wedge E,$$

а это противоречит аксиоме порядка.

Теперь составим таблицу истинности (табл. 1.22), в которой под P понимается обобщенная причина, т.е. конъюнкция всех P_i .

Таблица 1.22

n	A	B	C	D	E	P	P_1	P_2	P_3	P_4	P	C_1	C_2	C_3	C_4
0	0	0	0	0	0	1	1	1	1	1	1	1	0	1	1
1	1	0	0	0	0	0	1	1	1	1	0	1	0	0	0
2	0	1	0	0	0	1	0	1	1	1	0	1	0	1	0
3	1	1	0	0	0	1	0	1	1	1	0	1	0	0	0
4	0	0	1	0	0	1	1	0	1	1	0	1	0	1	1
5	1	0	1	0	0	0	1	0	1	1	0	1	0	0	0
6	0	1	1	0	0	1	1	0	1	1	0	1	0	1	0
7	1	1	1	0	0	1	1	0	1	1	0	1	0	1	0
8	0	0	0	1	0	1	1	1	1	1	1	1	0	0	1
9	1	0	0	1	0	0	1	1	1	1	0	1	0	0	0
10	0	1	0	1	0	1	0	1	1	1	0	1	0	0	0
11	1	1	0	1	0	1	0	1	1	1	0	1	0	0	0
12	0	0	1	1	0	1	1	1	1	1	1	1	0	0	1
13	1	0	1	1	0	0	1	1	1	1	0	1	0	0	1
14	0	1	1	1	0	1	1	1	1	1	1	1	0	1	1
15	1	1	1	1	0	1	1	1	1	1	1	1	0	1	1
16	0	0	0	0	1	1	1	1	1	1	1	1	0	1	1
17	1	0	0	0	1	0	1	1	1	1	0	0	1	0	0
18	0	1	0	0	1	1	0	1	1	1	0	1	0	1	0
19	1	1	0	0	1	1	0	1	1	1	0	0	1	0	0
20	0	0	1	0	1	1	1	0	1	1	0	1	0	1	1
21	1	0	1	0	1	0	1	0	1	1	0	0	1	0	0
22	0	1	1	0	1	1	1	0	1	1	0	1	0	1	0
23	1	1	1	0	1	1	1	0	1	1	0	0	1	0	0
24	0	0	0	1	1	1	1	1	0	0	0	1	0	0	1
25	1	0	0	1	1	0	1	1	0	0	0	0	1	0	0
26	0	1	0	1	1	1	0	1	0	0	0	1	0	0	0
27	1	1	0	1	1	1	0	1	0	0	0	0	1	0	0
28	0	0	1	1	1	1	1	1	1	0	0	1	0	0	1
29	1	0	1	1	1	0	1	1	0	0	0	0	1	0	0
30	0	1	1	1	1	1	1	1	1	0	0	1	0	0	0
31	1	1	1	1	1	1	1	1	1	0	0	0	1	0	0

Клауза считается *истинной*, если единицы следствия (*C*) *накрывают* все единицы обобщенной причины (*P*), т.е. единицы обобщенной причины образуют подмножество единиц следствия. Это требование выполняется для следствия C_1 , так как

$$P = \{0, 8, 12, 14, 15, 16\} \subset \{0, \dots, 16, \dots\} = C_1,$$

но не для C_2 ($C_1 \neq C_2$), так как

$$P = \{0, 8, 12, 14, 15, 16\} \not\subset \{18, 20, 22, 24, 26, 28, 30\} = C_2.$$

С помощью скорректированной табл. 1.22 нетрудно установить справедливость тавтологии, составленной из этих же посылок, —

$$1 \Rightarrow \bar{P}_1; \bar{P}_2; \bar{P}_3; \bar{P}_4; C_1,$$

и противоречия —

$$P_1, P_2, P_3, P_4, \bar{C}_1 \Rightarrow 0,$$

а также любых других клауз, полученных из первоначальной путем эквивалентных преобразований, например:

$$P_2, P_4 \Rightarrow \bar{P}_1; C_1; \bar{P}_3.$$

Если C_1 заменить на C_2 , то во всех указанных случаях условие причинно-следственного отношения нарушится и клаузы обратятся в ложные метавысказывания.

Заключения C_1 и C_2 , настолько очевидны, что никакой следователь в этом случае не стал бы прибегать к таблицам истинности. Но трудно найти такого следователя, который только путем одних рассуждений смог бы правильно выбрать из двух нижепредставленных заключений истинное:

Водитель обманывает, он находился в комнате отдыха, а комната отдыха действительно расположена рядом со складом — все это так, но при условии, что кассир сказала правду или что водитель слышал выстрелы —

$$C_3 = (A \vee D) \rightarrow (\bar{E} \wedge B \wedge C).$$

Водитель обманывает, он слышал выстрелы, а комната отдыха действительно расположена рядом со складом — все это так, но при условии, что кассир сказала правду или что водитель находился в комнате отдыха —

$$C_4 = (A \vee B) \rightarrow (\bar{E} \wedge D \wedge C).$$

Единичные наборы для заключений C_3 и C_4 тоже приведены в табл. 1.22. Для заключения C_3 в строках 8 и 12 стоят нули, следовательно, условие причинно-следственного отношения не выполняется, и поэтому C_3 является ложным заключением. Для заключения C_4 все его единицы накрывают единицы обобщенной посылки P . Следовательно, C_4 является истинным заключением:

$$P = \{0, 8, 12, 14, 15, 16\} \subset \{0, 2, 4, 6, 7, 14, 15, 16, 18, 20, 22\} = C_3,$$

$$P = \{0, 8, 12, 14, 15, 16\} \subset \{0, 4, 8, 12, 13, 14, 15, 16, 20, 24, 28\} = C_4.$$

Истинность заключения тем очевиднее, чем большим числом его единиц накрываются единицы обобщенной причины. Отсюда можно составить объективный критерий для оценки логических способностей человека.

Вообще, опытный логик прежде всего должен построить все совместимые ряды событий. В нашем случае таких рядов 6 (они соответствуют 0, 8, 12, 14, 15, 16 строкам табл. 1.22). Их объединение даст предельный случай условия выпол-

нения причинно-следственного отношения:

$$\begin{aligned} &\bar{A}, \bar{B}, \bar{C}, \bar{D}, \bar{E}; \quad \bar{A}, \bar{B}, \bar{C}, D, \bar{E}; \quad \bar{A}, \bar{B}, C, D, \bar{E}; \\ &\bar{A}, B, C, D, \bar{E}; \quad A, B, C, D, \bar{E}; \quad \bar{A}, \bar{B}, \bar{C}, \bar{D}, E. \end{aligned}$$

Перед нами не что иное как СДНФ, отвечающая нашей конкретной причине Р. Всевозможные покрытия шести конститuent дают множество истинных следствий. Так, заключения ---

$$C_1 = \bar{A}; E, \quad C_4 = (A, \bar{B}); (C, D, \bar{E})$$

покрывают все шесть конститuent; они — истинные. Что касается двух других заключений

$$C_2 = A, E, \quad C_3 = (\bar{A}, \bar{D}); (C, B, \bar{E}),$$

то они не покрывают все или отдельные конститuent, значит являются ложными следствиями.

Не надо знать комбинаторный анализ, чтобы ощутить все многообразие возможных покрытий, т.е. истинных следствий из заданных причин. Однако опытный следователь должен уметь определять три вещи — минимальную нормальную форму (МНФ), минимальное и трансверсальное покрытия.

Нахождением точных МНФ по известной СДНФ мы занимались в первом разделе. Минимизируя одним из известных способов нашу СДНФ, получим следующую МНФ:

$$\bar{A}, \bar{B}, \bar{C}, \bar{D}; \quad \bar{A}, \bar{B}, D, \bar{E}; \quad B, C, D, \bar{E};$$

Минимальное покрытие — это покрытие с наименьшим числом термов. Мы его уже знаем — это заключение C_1 . В него входят два *решающих* высказывания, связанные с правдивостью кассира (А) и правдивостью водителя (Е). Все остальные утверждения (В, С, D) являются *второстепенными* и могут выступать в результирующем заключении совместно с А и Е.

Трансверсальное покрытие должно включать все имеющиеся термы. Для нашего конкретного примера существуют четыре трансверсальных покрытия:

$$\begin{aligned} &\bar{A}; B, C, D, \bar{E} \quad \bar{A}, \bar{B}; C, D, \bar{E} \\ &\bar{A}, B, \bar{C}; D, \bar{E} \quad A, \bar{B}, C, \bar{D}; E. \end{aligned}$$

Как видим, среди выписанных покрытий находится и заключение C_4 , которое мы уже проинтерпретировали в имплицативной форме. Интерпретация заключений через ДНФ может показаться более предпочтительной. Возьмем для примера заключение

$$C_5 = \bar{A}, \bar{B}, \bar{C}; D, \bar{E}.$$

Оно предполагает три исхода истинного значения при совместном действии всех пяти факторов:

$$\begin{aligned} &\bar{A}, B, \bar{C} = 1 \quad D, \bar{E} = 0, \\ &\bar{A}, \bar{B}, \bar{C} = 0 \quad D, \bar{E} = 1, \\ &\bar{A}, \bar{B}, \bar{C} = 1 \quad D, \bar{E} = 1. \end{aligned}$$

Именно трансверсальные покрытия дают наиболее полную картину возможных следствий из сформулированных посылок.

Рассмотрим еще один *полуконструктивный* метод доказательства истинности логических клауз, в котором используется так называемый *принцип резолюций*. Этот принцип играет роль *аксиомы порядка* и вместе с тем порождает очень эффективную *конструктивную процедуру*. Суть его сводится к тому, что два посылочных дизъюнкта с противоположными термами всегда можно склеить в один заключительный дизъюнкт, в котором уже не будет противоположных термов:

$$X \vee A, Y \vee \bar{A} \Rightarrow X \vee Y,$$

где X и Y — произвольные термы или целые дизъюнкты с любым набором термов, включая ноль; A и $\bar{A}$ — произвольные термы.

При последовательном применении принципа резолюций происходит уменьшение числа букв, вплоть до их полного исчезновения. При этом исходная клауза *конструируется* в форме *конъюнктивного противоречия*:

$$P_1, P_2, \dots, P_n \Rightarrow 0.$$

Докажем с помощью метода резолюций справедливость *правила отделения*:

$$A, A \rightarrow B \rightarrow B \text{ или } 0 \vee A, \bar{A} \vee B, \bar{B} \vee 0 \Rightarrow 0.$$

Здесь имеются три дизъюнкта. Склеивая их последовательно, получаем в результате ноль, который говорит о несовместимости заключения и посылок. Это как раз и свидетельствует о справедливости исходной клаузы.

Принцип резолюций целиком заменяет *аксиому порядка*, поскольку сама эта аксиома может быть доказана в рамках метода резолюций. Действительно,

$$A, B \Rightarrow A, \quad A, B, \bar{A} \Rightarrow 0, \quad 0, B \Rightarrow 0.$$

Обращаем внимание на то, что посылка B здесь вообще не используется. Это необходимо иметь в виду: необязательно использовать все посылки (их число часто бывает избыточным) — главное получить ноль.

Пусть дана клауза:

$$\bar{A} \rightarrow B, C \vee A, B \rightarrow \bar{C} \Rightarrow A.$$

Доказательство ее справедливости следует начать с приведения ее в *нормальную конъюнктивную форму*:

$$A \vee B, C \vee A, \bar{B} \vee \bar{C}, \bar{A} \Rightarrow 0.$$

Выпишем по порядку все посылки и далее начнем их склеивать согласно очередности. Справа от каждого нового дизъюнкта будем писать номера используемых дизъюнктов, получим:

1. $A \vee B$,	8. C ,	(2,4)
2. $C \vee A$,	9. A ,	(2,5)
3. $\bar{B} \vee \bar{C}$,	10. $\bar{C}$,	(3,6)
4. $\bar{A}$,	11. $\bar{B}$,	(3,8)
5. $A \vee \bar{C}$,	12. $\bar{C}$,	(4,5)
6. B ,	13. $\bar{B}$,	(4,7)
7. $A \vee \bar{B}$,	14. 0 .	(4,9)

Близким к методу резолюций является *метод Вонга*, в котором тоже используется сконструированная *конъюнктивно-дизъюнктивная нормальная форма* представления исходной клаузы, а *аксиому порядка* заменяет *клауза Вонга*:

$$X, L \Rightarrow X; R,$$

здесь X пробегает некоторые буквы, входящие в клаузу, а L и R — определенные комбинации дизъюнктов и конъюнктов.

Конструктивная процедура доказательства сводится к последовательному разбиению дизъюнктов или конъюнктов таким образом, чтобы слева и справа от метаимпликации появилась одна и та же буква X . Если в результате такого разбиения все конечные клаузы приобретают вид клаузы Вонга, то и исходная клауза была составлена верно. Разберем метод Вонга на примере доказательства справедливости *правила отделения*:

$$A, A \rightarrow B \Rightarrow B \text{ или } A, \bar{A} \vee B \Rightarrow B.$$

Здесь имеется только один дизъюнкт, который можно подвергнуть разбиению. После его разбиения получим две новых клаузы:

$$A, \bar{A} \Rightarrow B \text{ и } A, B \Rightarrow B.$$

Вторая клауза удовлетворяет аксиоме порядка и клаузе Вонга. В качестве X в ней выступает B , а $L = A$ и $R = \emptyset$. Первая же клауза тоже будет удовлетворять необходимым требованиям, но только после того, как терм A из левой части клаузы с противоположным знаком перенести в правую часть. Тогда будем иметь:

$$A \rightarrow A; B \text{ где } X = A, L = 1 \text{ и } R = B.$$

При большом числе букв в исходной клаузе прибегают к специальной нумерации производных клауз, чтобы не запутаться. Пусть требуется установить справедливость следующей клаузы:

$$X \vee Y, (X \rightarrow Y) \vee U, Z \rightarrow (Y \rightarrow W) \Rightarrow (W \rightarrow X) \rightarrow (Z \rightarrow X).$$

Приведем ее в соответствующую конъюнктивно-дизъюнктивную нормальную форму:

$$X \vee Y, \bar{X} \vee Y \vee U, \bar{Z} \vee \bar{Y} \vee W \Rightarrow W \wedge \bar{X}; \bar{Z}; X.$$

Далее произведем разбиение первого дизъюнкта, в результате получим две производные клаузы:

1. $X, \bar{X} \vee Y \vee U, \bar{Z} \vee \bar{Y} \vee W \Rightarrow W \wedge \bar{X}; \bar{Z}; X,$
2. $Y, \bar{X} \vee Y \vee U, \bar{Z} \vee \bar{Y} \vee W \Rightarrow W \wedge \bar{X}; \bar{Z}; X.$

Клауза (1) отбрасывается, так как она удовлетворяет клаузе Вонга. Разбивая следующий дизъюнкт клаузы (2), получаем еще три новых клаузы:

- 2.1. $Y, \bar{X}, \bar{Z} \vee \bar{Y} \vee W \Rightarrow W \wedge \bar{X}; \bar{Z}; X,$
- 2.2. $Y, Y, \bar{Z} \vee \bar{Y} \vee W \Rightarrow W \wedge \bar{X}; \bar{Z}; X,$
- 2.3. $Y, U, \bar{Z} \vee \bar{Y} \vee W \Rightarrow W \wedge \bar{X}; \bar{Z}; X.$

Клаузы (2. 1) и (2. 2) сводятся к одной клаузе —

$$2.1. Y, \bar{Z} \vee \bar{Y} \vee W \Rightarrow W \wedge \bar{X}; \bar{Z}; X.$$

Произведем ее разбиение:

$$2.1.1. Y, \bar{Z} \Rightarrow W \wedge \bar{X}; \bar{Z}; X,$$

$$2.1.2. Y, \bar{Y} \Rightarrow W \wedge \bar{X}; \bar{Z}; X,$$

$$2.1.3. Y, W \Rightarrow W \wedge \bar{X}; \bar{Z}; X.$$

Первые две клаузы удовлетворяют клаузе Вонга. У клаузы (2.1.3) нужно разбивать конъюнкт:

$$2.1.3.1. Y, W \Rightarrow W; \bar{Z}; X, \quad 2.1.3.2. Y, W \Rightarrow \bar{X}; \bar{Z}; X.$$

Теперь обе клаузы имеют вид клаузы Вонга.

Но у нас осталась еще ветвь (2.3). Она отличается от рассмотренной ветви (2.1) наличием непарного термина U , который, однако, не может повлиять на конечный результат, т.е. разбиение клаузы (2.3) практически полностью совпадает с разбиением клаузы (2.1). Следовательно, исходная клауза была записана верно.

Недостатком метода Вонга, как и метода резолюций, является то, что исходная клауза обязательно должна иметь нормальную дизъюнктивную или конъюнктивную форму. Этот недостаток преодолен в *методе натурального исчисления*, к которому мы переходим.

Доказательный вывод в натуральном исчислении строится как упорядоченная цепь преобразований, связанных с удалением или введением логических связок на основе следующих десяти правил:

1) правило введения конъюнкции (ВК) —

$$(\Rightarrow A) \& (\Rightarrow B) // \Rightarrow A \wedge B;$$

2) правило удаления конъюнкции (УК) —

$$\Rightarrow A \wedge B // \Rightarrow A;$$

3) правило введения импликации (ВИ) —

$$\Rightarrow B // \Rightarrow A \rightarrow B, \quad A \Rightarrow B // \Rightarrow A \rightarrow B;$$

4) правило удаления импликации (УИ) —

$$(\Rightarrow A) \& (\Rightarrow A \rightarrow B) // \Rightarrow B, \quad \Rightarrow A \rightarrow B // A \Rightarrow B;$$

5) правило введения дизъюнкции (ВД) —

$$\Rightarrow A // \Rightarrow A \vee B;$$

6) правило удаления дизъюнкции (УД) —

$$(\Rightarrow A \vee B) \& (A \Rightarrow C) \& (B \Rightarrow C) // \Rightarrow C;$$

7) правило введения отрицания (ВО) —

$$A, B \Rightarrow 0 // A \Rightarrow \bar{B};$$

8) правило удаления отрицания (УО) —

$$(A \Rightarrow \bar{B}) \& (A \Rightarrow B) // A \Rightarrow 0;$$

9) правило введения эквивалентности (ВЭ)

$$(A \Rightarrow B) \& (B \Rightarrow A) // \Rightarrow A \sim B;$$

10) правило удаления эквивалентности (УЭ) —

$$\Rightarrow A \sim B // (A \rightarrow B) \& (B \rightarrow A).$$

Эти правила надо понимать так: если слева от символа «//» стоят истинные клаузы, то справа от символа «//» тоже будут стоять истинные клаузы. Напри-

мер, первое правило *введения конъюнкции* можно прочитать следующим образом: если высказывания **A** и **B** (связка «и» передается знаком «&») порознь истинны (о чем говорят рядом стоящие с этими буквами символы метаимпликации « $\Rightarrow$ »), то будет истинной и их конъюнкция $A \wedge B$. При этом надо помнить, что во всех десяти правилах перед символом метаимпликации « $\Rightarrow$ » может стоять любой перечень посылок **P**. Так, десятое правило может выглядеть следующим образом:

$$P \Rightarrow A \sim B // (P, A \Rightarrow B) \& (P, B \Rightarrow A) .$$

Кроме перечисленных десяти правил, имеется еще одно — *базовое правило* (БП), которое сначала сформулируем словами: во-первых, любая посылка может выступать в роли следствия, т.е.

$$A, B, C \Rightarrow A, \quad A, B, C \Rightarrow B \quad \text{и} \quad A, B, C \Rightarrow C$$

будут всегда истинными и не требуют доказательства, т.к. удовлетворяют *аксиоме порядка*; во-вторых, в перечень посылок истинной клаузы всегда можно добавить новые посылки, т.е. если клауза

$$A, B, C \Rightarrow X$$

верна, то будут истинными и все клаузы, построенные на ее основе —

$$A, B, C, D \Rightarrow X, \quad A, B, C, \dots \Rightarrow X .$$

В обобщенной форме базовое правило можно записать так:

$$P \Rightarrow X // P, Y \Rightarrow X ,$$

где **X** — любая посылка из **P**, а **Y** — произвольная посылка.

Действенность метода натурального исчисления продемонстрируем на примере следующей тавтологии:

$$1 \Rightarrow (A \rightarrow B) \rightarrow ((A \rightarrow \bar{B}) \rightarrow \bar{A}) .$$

Доказательство:

- | | |
|--|------------|
| 1. $A, A \rightarrow B \Rightarrow B ,$ | (УИ) |
| 2. $A, A \rightarrow \bar{B} \Rightarrow \bar{B} ,$ | (УИ) |
| 3. $A, A \rightarrow B, A \rightarrow \bar{B} \Rightarrow B ,$ | (1, БП) |
| 4. $A, A \rightarrow \bar{B}, A \rightarrow B \Rightarrow \bar{B} ,$ | (2, БП) |
| 5. $A, A \rightarrow B, A \rightarrow \bar{B} \Rightarrow 0 ,$ | (3, 4, УО) |
| 6. $A \rightarrow B, A \rightarrow \bar{B} \rightarrow \bar{A} ,$ | (5, ВО) |
| 7. $A \rightarrow B \Rightarrow (A \rightarrow \bar{B}) \rightarrow \bar{A} ,$ | (6, ВИ) |
| 8. $1 \Rightarrow (A \rightarrow B) \rightarrow ((A \rightarrow \bar{B}) \rightarrow \bar{A}) .$ | (7, ВИ) |

Справа в круглых скобках указан номер строки, из которой получена данная клауза, а также начальные буквы используемого правила. Приведем доказательство еще одной клаузы:

$$1 \Rightarrow (A \rightarrow B) \rightarrow ((C \rightarrow D) \rightarrow ((A \vee C) \rightarrow (B \vee D))) .$$

Доказательство:

- | | |
|--|---------|
| 1. $A \rightarrow B \Rightarrow (C \rightarrow D) \rightarrow ((A \vee C) \rightarrow (B \vee D)) ,$ | (УИ) |
| 2. $A \rightarrow B, C \rightarrow D \Rightarrow (A \vee C) \rightarrow (B \vee D) ,$ | (1, УИ) |

3. $A \rightarrow B, C \rightarrow D, A \vee C \Rightarrow B \vee D$. (2, УИ)
4. $P_1, P_2, P_3 \rightarrow B \vee D$. (3)
5. $P \Rightarrow A \rightarrow B$, (P₁, БП)
6. $P, A \Rightarrow B$, (5, УИ)
7. $P, A \Rightarrow B \vee D$, (6, ВД)
8. $P \Rightarrow C \rightarrow D$, (P₂, БП)
9. $P, C \Rightarrow D$, (8, УИ)
10. $P, C \Rightarrow D \vee B$, (9, ВД)
11. $P \rightarrow A \vee C$, (P₃, БП)
12. $P \rightarrow B \vee D$. (7, 10, 11, УД)

1.7. Задания на практическую работу по логике высказываний

1) Ниже приведены по три клаузы в одном варианте. Каждую клаузу необходимо доказать следующими методами: аксиоматическим, натурального исчисления, резолюций и Вонга.

1. $(A \rightarrow C) \rightarrow (\bar{A} \wedge B) \Rightarrow A \vee B$,
 $A \vee D, B \vee E, D \rightarrow C, D \vee C \rightarrow A \wedge C; E \wedge D; B$,
 $A \rightarrow B, C \rightarrow D, A \vee C, A \rightarrow \bar{D}, C \rightarrow \bar{B} \Rightarrow (A \vee B) \rightarrow (A \wedge B)$.
2. $C \rightarrow A, B \vee C, B \rightarrow D, D \rightarrow A \Rightarrow A$,
 $D \rightarrow E, E \rightarrow C, A \sim D, B \sim C \Rightarrow A \rightarrow B$,
 $A \vee B, A \rightarrow B, B \rightarrow (C \rightarrow \bar{D}), A \rightarrow D \rightarrow \overline{A \wedge C}$.
3. $(A \wedge B) \rightarrow C \Rightarrow A \rightarrow (B \rightarrow C)$,
 $A \rightarrow (B \rightarrow C), (C \wedge D) \rightarrow E, \bar{F} \rightarrow (D \wedge \bar{E}) \Rightarrow A \rightarrow (B \rightarrow F)$,
 $(A \wedge (B \rightarrow C)) \sim D, E \sim (A \wedge (\bar{B} \vee \bar{C})) \Rightarrow (D \wedge \bar{E}) \sim (A \wedge C)$.
4. $A \rightarrow (B \rightarrow \bar{C}), \bar{A} \rightarrow B, \bar{A} \rightarrow (\bar{B} \rightarrow C) \Rightarrow C; B$,
 $A, \bar{B} \rightarrow (A \rightarrow D), C \rightarrow (B \rightarrow E), D \rightarrow (E \vee \bar{C}) \Rightarrow C \rightarrow E$,
 $\bar{C}, D \rightarrow C, A \rightarrow (\bar{B} \rightarrow D), B \Rightarrow A \rightarrow C$.
5. $(A \vee C) \sim (\bar{B} \vee \bar{D}) \Rightarrow \bar{A} \sim B; \bar{C} \sim D$,
 $A \rightarrow B, C \rightarrow D, B \rightarrow E, D \rightarrow F, \bar{E} \wedge \bar{F}, A \rightarrow C \rightarrow \bar{A}$,
 $C \rightarrow (B \rightarrow A), \bar{B} \rightarrow D, C \Rightarrow A \vee D$.
6. $\bar{C}, A \vee B \Rightarrow (B \rightarrow C) \rightarrow A$,
 $A \rightarrow C, D \rightarrow F, B \rightarrow E, \bar{D} \rightarrow \bar{C}, A \rightarrow B \Rightarrow A \rightarrow (E \wedge F)$,
 $A, B \vee C, C \sim D \Rightarrow (B \rightarrow \bar{A}) \rightarrow (B \rightarrow D)$.
7. $A \rightarrow (C \rightarrow B), D \rightarrow A, C \Rightarrow D \rightarrow B$,
 $E \rightarrow F, C \rightarrow (D \rightarrow E), (A \rightarrow B) \rightarrow C \Rightarrow D \rightarrow (A \vee F)$,
 $\bar{A} \sim B, B \rightarrow C, \bar{C} \sim D \Rightarrow (C \rightarrow B) \rightarrow (D \rightarrow A)$.

8. $A \sim B, C \sim D \rightarrow (A \vee C) \sim (B \vee D)$,
 $A \rightarrow (B \rightarrow C), C \rightarrow (B \rightarrow \bar{A}), D \rightarrow A, A \rightarrow B \rightarrow \bar{D}$,
 $A \rightarrow B, B \rightarrow D, D \rightarrow A, B \vee C, C \rightarrow D \Rightarrow D$.
9. $A, B \vee C \Rightarrow A \wedge B; C$,
 $C, (A \rightarrow B) \rightarrow (C \rightarrow A) \Rightarrow A$,
 $A \rightarrow (B \vee C), B \rightarrow (D \rightarrow A), C \rightarrow (B \rightarrow A), A \rightarrow (B \rightarrow C),$
 $D \rightarrow (A \vee B), D \rightarrow (A \rightarrow B), C \rightarrow (B \vee D), A \vee C \vee D,$
 $C \rightarrow (A \rightarrow B) \Rightarrow A \wedge B \wedge C; A \wedge B \wedge D$.
10. $A, B \rightarrow C \rightarrow A \wedge \bar{B}; B \wedge C$,
 $A \rightarrow (B \wedge C), \bar{B} \vee D, (E \rightarrow \bar{F}) \rightarrow \bar{D}, \bar{B} \vee (A \wedge \bar{E}) \rightarrow B \rightarrow E,$
 $A \vee B, A \vee C, A \rightarrow C, C \rightarrow (A \rightarrow D) \Rightarrow B \vee D$.
11. $A, B \rightarrow C \Rightarrow (A \rightarrow \bar{C}) \rightarrow \bar{B}$,
 $A \rightarrow B, A \sim D, C \sim E \Rightarrow (B \rightarrow C) \rightarrow (D \rightarrow E)$,
 $A \rightarrow (C \rightarrow B), D \rightarrow A, C \Rightarrow D \rightarrow B$.
12. $A \rightarrow (B \rightarrow C), A \rightarrow (B \vee C) \rightarrow A \rightarrow C$,
 $A \sim \bar{B}, A \vee C, \bar{C} \wedge \bar{E}, B \rightarrow C, B \vee D, A \rightarrow E \Rightarrow D \sim E; \bar{C} \wedge \bar{D}$,
 $A, D \rightarrow C, B \vee (A \rightarrow D), B \rightarrow C \Rightarrow C$.
13. $A \sim B, C \sim D \rightarrow (A \rightarrow C) \rightarrow (B \rightarrow D)$,
 $A \vee C, C \rightarrow D, \bar{A} \wedge \bar{D}, \bar{B} \wedge \bar{C}, A \rightarrow B, A \vee B \rightarrow A \wedge B$,
 $E \rightarrow D, C \vee E, A \vee D, D \rightarrow \bar{B} \Rightarrow C \wedge D; (E \wedge B) \rightarrow (E \rightarrow A)$.
14. $A, B \rightarrow C \Rightarrow A \wedge \bar{B}; B \wedge C$,
 $C \rightarrow (D \rightarrow E), E \rightarrow F \Rightarrow ((A \rightarrow B) \rightarrow C) \rightarrow (D \rightarrow (\bar{A} \rightarrow F))$,
 $A \rightarrow B, A \sim C, D \sim E \Rightarrow (B \rightarrow D) \rightarrow (C \rightarrow E)$.
15. $(\bar{A} \vee \bar{C}) \sim (B \vee D), \bar{A} \sim B \Rightarrow C \rightarrow \bar{D}$,
 $A \rightarrow (B \vee C), A \vee B, B \rightarrow A, B \rightarrow D \Rightarrow C \vee D$,
 $E \rightarrow D, C \vee E, A \vee D, D \rightarrow B, E \Rightarrow A; B \wedge E; C \wedge D$.
16. $A \rightarrow B, B \vee C, C \rightarrow A, B \rightarrow C \rightarrow A \wedge B$,
 $E \rightarrow D, E \sim C, C \sim A, D \sim B \Rightarrow A \rightarrow B$.
 $A \vee B, B \sim C, C, D, A \sim D \Rightarrow A \wedge B$.
17. $A \rightarrow B, A \vee C, C \rightarrow B, D \rightarrow A \Rightarrow (B \rightarrow D) \rightarrow B$,
 $\bar{D}, E \Rightarrow ((A \wedge \bar{B}) \rightarrow C) \sim \bar{D}; E \sim (A \wedge (B \rightarrow C))$,
 $A \vee (B \rightarrow C), C \rightarrow (B \rightarrow A), A \rightarrow D \Rightarrow (A \vee B) \rightarrow D$.
18. $(\bar{A} \rightarrow \bar{C}) \sim (B \rightarrow D) \Rightarrow A \sim \bar{B}; \bar{C} \sim D$,
 $C \rightarrow (A \vee B), D \rightarrow (B \vee C) \Rightarrow A \vee B; \bar{D}$,
 $A \rightarrow D, A \vee C, D \vee E, D \rightarrow B \Rightarrow (A \wedge B) \rightarrow (A \rightarrow E); C \wedge D$.
19. $A \vee C, A \rightarrow B, C \rightarrow B \Rightarrow A \wedge B; B \wedge C$,
 $A \rightarrow B, A \rightarrow C, D \sim E, D \rightarrow A, E \rightarrow A, B \rightarrow E, C \rightarrow D \Rightarrow B \sim C,$
 $C \rightarrow (B \rightarrow A), C \vee D, D \rightarrow B, B \vee D \Rightarrow (D \rightarrow C) \rightarrow A$.

20. $A, B \vee C \Rightarrow A \wedge C; B \wedge \bar{C},$
 $A \rightarrow B, C \rightarrow D, (B \wedge D) \rightarrow E, E, A \Rightarrow C,$
 $A \rightarrow (B \rightarrow C), B \vee C \vee D \rightarrow (A \rightarrow C) \vee D.$
21. $A \vee B, A \rightarrow C \Rightarrow \bar{A} \wedge B; C,$
 $(A \rightarrow B) \rightarrow (C \rightarrow D), (D \rightarrow F) \rightarrow E \rightarrow A \vee E,$
 $A \vee C, C \rightarrow \bar{D}, A \rightarrow D, B \vee C \rightarrow D \rightarrow (B \wedge D).$
22. $A \vee B, C \rightarrow B, B \rightarrow A, A \rightarrow C \Rightarrow B \wedge C,$
 $A \rightarrow C, \bar{B} \sim C, B \vee D, B \rightarrow A \Rightarrow D; A \wedge C,$
 $A \vee B, D \vee E, D \vee C, D \rightarrow C \Rightarrow A \wedge D; B; C \wedge E.$
23. $A \rightarrow C, A \vee B, B \rightarrow D, D \rightarrow C \rightarrow C,$
 $B \vee D, D \rightarrow B, C \vee D, D \rightarrow C, C \rightarrow (B \rightarrow A) \Rightarrow A,$
 $A \rightarrow B, A \vee D, C \vee E, E \rightarrow A \Rightarrow (B \wedge E) \rightarrow (E \rightarrow D); A \wedge C.$
24. $(A \wedge B) \vee (C \wedge D), \bar{A} \rightarrow C,$
 $C \rightarrow A \Rightarrow ((A \wedge B) \vee C) \sim (A \wedge (B \vee C)),$
 $D \rightarrow F, A \rightarrow (E \rightarrow D), (C \rightarrow B) \rightarrow A \Rightarrow E \rightarrow (C \vee F).$

2) По вашему выбору для двух из трех клауз составьте легенды.

3) Ниже приведены легенды. Запишите с использованием 4–6 различных букв клаузу, отвечающую тексту или контексту вашей легенды, для чего сформулируйте необходимые посылки и два следствия: одно истинное, другое ложное. С помощью таблицы истинности найдите МНФ, минимальное и все трансверсальные покрытия.

1. В одной старой легенде рассказывается, что греческий драматург Софокл погиб при очень странных обстоятельствах. На его лысый череп орел сбросил камень, приняв его за яйцо. Если бы Софокл не сочинял трагедии, то он не уединился бы в горах и остался бы жить до своей естественной кончины. Он мог бы сочинять свои трагедии в горах при наличии волос на голове или при отсутствии там этих странных птиц.

2. «Ты меня уважаешь?» — «Да». — «Тогда дай мне денег». — «Дав тебе денег, я перестану тебя уважать». — «Разве ты меня уважаешь из-за денег?» — «Нет, как художника». — «Ну, тогда тем более ты должен дать их мне». — «Я даю деньги тем, у кого они в принципе водятся. Ты же мне долг не вернешь». — «Я открою свое дело. Через год у меня будет состояние. Займи под проценты». — «Я тебе не верю, но помогу организовать выставку твоих картин». — «Хорошо, идет».

3. Современный футбол — это надежная защита, хорошая скорость, напористая атака и убедительная результативность. Матвеев мне результативность обеспечит, но голы он забивает только по вдохновению, когда складывается игра. Без Федотова такой игры не получится. Он видит поле, чувствует, где надо находиться, но бегать не может. Скорость команде сообщит Комаров, хотя он может развалить всю защиту. Попробовать Петрова в обороне, но в паре с Матвеевым он не играет. Квасов умеет блокировать бомбардиров противника, но левой у него не получается. Надо ставить Земерова, чтобы левый край прикрыл. Однако Земеров в последнее время точный пас отдать не может. Ну нет команды! Завтра встречу точно проиграем.

4. Мотоцикл я сначала не заметил, так как его заслонил бензовоз, а «Волга» вывернула из-за угла, когда «Жигули» были уже вблизи светофора. «Иномарка» проскочила на красный свет и явилась, как мне кажется, причиной всей этой аварии. Из-за нее «Волга» резко затормозила и мотоциклист оказался на асфальте. «Жигули», чтобы не задавить мотоциклиста, свернули на тротуар, а бензовоз в это время врезался в «Волгу». Если бы не было мотоцикла, то опасной ситуации тоже могло и не быть. Хотя виноват и водитель «Волги», поскольку он явно превысил скорость.

5. Если облака — это горы в небе и горы — это облака на земле, то гроза — это вулкан на небе и вулкан — это гроза на земле. Вулкан извергает пепел, а гроза — воду. Вулканический пепел и дождевая вода одинаково хорошо сказываются на урожайности полей. Урожай — это благо. Все благо — от Бога. Значит, пепел и вода, вулкан и гроза, горы и облака — от Бога.

6. «Я вижу, у Вас поднялось давление». — «Это последствие рыбалки, доктор». — «Рыбалка, напротив, должна успокаивать и укреплять здоровье». — «Верно, доктор, но я переволновался, так как ловил рыбу в запрещенном месте». — «Ай-ай-ай! Зачем же Вы на это пошли?» — «Там, где разрешено, доктор, рыбы нет». — «В таком случае рыбы много в магазине. Я же Вам прописал отдых на свежем воздухе». — «Хорошо, доктор, тогда завтра я пойду охотиться». — «Только, пожалуйста, голубчик, не стреляйте в зоопарке».

7. Ваня и Петя — братья-близнецы. Ваня с огромной скоростью улетел на ракете в космос, а Петя остался на неподвижной Земле. Теория относительности утверждает, что если лететь на большой скорости, то время замедляется, поэтому Петя состарится, а Ваня — нет. Эта же теория учит, что движение относительно: если Ваня движется относительно Пети, то Петя движется относительно Вани. Однако по теории почему-то именно Ваня, вернувшись из полета, будет моложе Пети. Вывод: теория относительности не свободна от противоречий.

8. Если усложнить схему устройства, то возрастет его производительность, а если использовать новую элементную базу, то увеличится период эксплуатации. Устройство начнут хорошо раскупать только при одновременном росте его производительности и периода эксплуатации. Но устройство не пользуется спросом.

9. Увеличение денег в обращении влечет за собой инфляцию. Но рост денежной массы происходит по двум причинам: из-за денежной эмиссии или снижения товарооборота. Снижение товарооборота приводит к безработице и спаду производства. Из-за инфляции падает курс денежной единицы. Рекомендации экономиста Иванова: увеличить денежную эмиссию и поднять производство, тогда избежим безработицы и курс денежной единицы останется неизменным.

10. «Что собираешься делать, честолюбивый полководец?» — «Хочу завоевать Африку, мудрый философ». — «Предположим, Африку ты завоевал. Что дальше будешь делать?» — «Пойду походом на Индию». — «Допустим, и Индию ты покорил. Что потом?» — «Потом я уединюсь в своем саду и стану наслаждаться чтением книг. Хочу быть таким же мудрым как ты, философ». — «Почему бы тебе сразу же не отправиться в сад и не приняться за книги?» — «Так ведь ни Африки, ни Индии я еще не завоевал». — «Да, ты прав, полководец. Я рассуждаю немудро, поскольку не учитываю твое сегодняшнее честолюбие».

11. Чтобы сварить щи, нужны: капуста, свекла, картофель, лук, морковь и томаты. Свеклы и капусты в нашем магазине не оказалось. Все остальное я купила.

Однако ши уже не получатся. Хорошо, тогда куплю огурцы и сметану, сделаю салат из огурцов, томатов и лука. Поджарю котлетки, отварю картошечку — второе у меня есть. Что приготовить на первое? Пожалуй, на говяжьих косточках неплоха будет домашняя лапша. А морковку я сейчас помою и отдам детям — пусть червячка заморят.

12. Любый марксист — диалектик, но не всякий диалектик — марксист. Любый марксист — материалист, но не всякий материалист — марксист. Гегель был диалектик, но не материалист. Фейербах был материалист, но не диалектик. Итак, если бы Гегель и Фейербах могли объединиться в один кружок, то Маркс уже не понадобился бы.

13. Преступник изготовит партию фальшивых денег, если у него имеются соответствующие материалы и работает станок. Эти два условия, к сожалению, выполняются. Однако фальшивые деньги не появятся, если хорошо работает милиция. Милиция же работает хорошо тогда и только тогда, когда каждый милиционер получает высокую зарплату. Увы, пока такой зарплаты нет, но есть высокая сознательность всех работников милиции.

14. «Надо завести собаку», — сказал старик. «Она не даст жить моей копечке», — сказала старуха. «Если не будет собаки, то я не смогу результативно охотиться и приносить в дом дичь». — «А если не будет моей кошечки, то в доме разведутся мыши, которые уничтожат все наши продовольственные запасы». — «Согласен, старуха. Давай собаку я заведу, но держать ее буду во дворе». — «Копечку во двор я пускать не буду».

15. Существуют две теории возникновения человека на земле — теория эволюции Дарвина и теория сотворения человека Господом Богом. Если справедлива теория эволюции, то самопроизвольное возникновение человека без соответствующих превращений живых организмов невозможно. Как доказали ученые, такие превращения действительно имели место. По теории же сотворения человек был слеплен из простой глины, а жизнь в него вдохнул Господь. Глины всегда было много, а насчет дыхания Бога тоже сомневаться не приходится, поскольку есть на то свидетельство Библии. Отсюда вывод — две названные теории друг другу не противоречат.

16. Человек, который решил свести счеты со своей жизнью, вряд ли будет за час до этого просматривать статистические данные по зерну за прошлый год. Сломанная герань только подчеркивает кем-то хорошо скрытые следы борьбы и насилия. Очень, конечно, странно, что дверь оказалась заперта изнутри, а вахтер ничего не заметил. Как же преступнику удалось выйти из помещения? И каковы, собственно, мотивы преступления? Такой тихий, скромный человек, ничего кроме семьи и работы его не интересовало. Правда, жена сообщила, что она вчера вечером видела его в обществе двух подозрительных молодых людей. Да и вахтер утверждал, что примерно в течение получаса отлучался для обхода территории. Тем не менее не хватает какого-то звена в этой загадочной цепи событий, чтобы уверенно сказать — «самоубийство» кем-то старательно инсценировано.

17. Из утверждения «два плюс два равно пяти» следует, что я и папа римский — одно и то же лицо. В самом деле, если от обеих частей указанного равенства отнять по двойке, то будет справедливо равенство «два равно трем». Если от обеих частей нового равенства отнять по единице, то будет справедливо равенство

во — «один равен двум». Один — это я, а двойка — это я и папа римский. Поскольку верно, что «один равен двум», то я есть папа римский.

18. «Хочешь яблоко?» — «Яблоки я не ем после рыбы, а рыбу я не ем после борща. Борщ я сегодня не ел, но съел немного горохового супа. После него я съел кусочек жареного хека. Если я ем гороховый суп, то в этот день уже не буду отказываться от яблок, но при условии, что к столу не подавали салат. Итак, давай сюда яблоко».

19. Слепой и глухой пошли погулять. «Смотри, вдали озеро, значит, напьемся», — сказал глухой. «Ага», — сказал слепой. «Послушай, гремит гром, значит дождь собирается», — сказал слепой. «Ага», — сказал глухой. Глухой и слепой набрали воды и достали плащи. Все это видел и слышал немой. «Я им не компания», — подумал немой.

20. Сегодня посмотрю футбол, если трамвай не задержится. Трамвай не опоздал, но случилась другая беда: у меня не оказалось денег на билет. Рискну доехать «зайцем». В салоне оказался контролер, и я лихорадочно стал рыться по карманам. К моему счастью, нашелся один неиспользованный трамвайный талон. До компостера я добрался вовремя, хотя футбольный матч я так и не увидел: вместе с деньгами я дома оставил и билет на матч.

21. Если в одном месте что-то убудет, то в другом месте что-то прибудет — это истина, не требующая доказательств. Но есть такая теория, которая утверждает: где-то в далеком космосе существуют «черные дыры», куда все проваливается, но оттуда ничего не появляется. Эта теория ничего не говорит о существовании «белых дыр», которые действовали бы противоположно «черным». Один иностранный астрономический журнал сообщил координаты «черной дыры». Российский астроном Иванов направил туда свой мощный телескоп и ничего не обнаружил. «Так-так», — сказал Иванов, — но «белую дыру» я все же открою».

22. Если в цепи будет большой перепад напряжения, то сгорит предохранитель, что повлечет за собой необходимость его замены. При целом предохранителе телевизор, конечно, будет работать, но только если он включен в сеть питания. Если телевизор работает нормально, то я увижу сегодняшние «Новости». Итак, я смотрю телевизионные «Новости» при условии отсутствия перепада напряжения и подключения телевизора к сети питания.

23. «Иван Иванович, можно?» — «Входи, Петров. Ну, сделал, что я тебя просил?» — «Видите ли... Если бы Вы немного прибавили...» — «Ты что, Петров! Сидоров за эту же работу берет в два раза меньше». — «Сидоров и сделал бы се в два раза хуже. Я же работаю с личным клеймом. И потом, у меня семья — сами знаете». — «Ладно, проси что хочешь, но денег у меня нет». — «А как сделаю, на рыбалку отпустите?» — «Договорились, только ты моего Вовку с собой возьми, а то он тут с какой-то подозрительной компанией спутался». — «Если с Вовкой, то на Ваней лодке». — «Вот хитрец! Хорошо, поедем все вместе. Мне тоже не мешало бы проветриться. Ты дело только сделай».

24. Уменьшение температуры приводит к снижению давления и уменьшению объема. Увеличение объема приводит к росту скорости потока. Повышение давления приводит к падению уровня, если при этом уменьшать температуру. Снижение скорости приводит к уменьшению давления или росту температуры. Технолог Иванов рассудил так: «Мне надо повысить давление при одновременном снижении скорости потока, поэтому я должен увеличить объем и температуру».

25. «В эти брезентовые штаны не пытайся влезть — в них ты смотришься как маляр». — «Но и это шерстяное платье я тоже не надену — оно на мне как на вешалке». — «Как насчет кожаного пиджака и юбки с разрезом?» — «У юбки заело молнию, а пиджак вот здесь испачкал». — «Ну, это не беда; пятно прикроется сумкой». — «Да, пожалуй, ты права — сумку в любом случае брать нужно; она очень идет к моим любимым туфлям». — «Сломанную молнию заменит булавка, а ее прикроет пиджак». — «Хорошо, так и сделаем». — «Шерстяное платье одену я, если ты не возражаешь». — «Возражаю, надень уж лучше эти штаны».

1) Доказать методом натурального исчисления истинность следующей клаузы:

$$B \rightarrow (C \rightarrow A), \bar{B} \rightarrow D, C, \bar{D} \Rightarrow A.$$

Доказательство:

1. $P \Rightarrow \bar{B} \rightarrow D$, (P₂, БП)
2. $P, \bar{B} \Rightarrow D$, (1, УИ)
3. $P, \bar{B} \Rightarrow \bar{D}$, (P₄, БП)
4. $P, \bar{B} \Rightarrow 0$, (2, 3, УО)
5. $P \Rightarrow B \rightarrow (C \rightarrow A)$, (P₁, БП)
6. $P \Rightarrow C \rightarrow A$, (4, 5, УИ)
7. $P \Rightarrow A$, (6, P₃, БП, УИ).

2) Доказать аксиоматическим методом истинность клаузы:

$$A, B \rightarrow D, C \rightarrow D, A \rightarrow (B \vee C) \Rightarrow D.$$

Доказательство:

1. $B \rightarrow D, C \rightarrow D, B \vee C \Rightarrow D$,
2. $\bar{B} \vee D, \bar{C} \vee D, B \vee C \rightarrow D$,
3. $(\bar{B} \wedge \bar{C}) \vee D, B \vee C \rightarrow D$,
4. $(B \vee C) \rightarrow D, B \vee C \Rightarrow D$,
5. $B \vee C, D \rightarrow D$.

3) Доказать методом Вонга истинность следующей клаузы:

$$\bar{B} \rightarrow (D \rightarrow C), D, C \rightarrow (A \vee B) \Rightarrow A \vee B.$$

Доказательство:

1. $B \vee \bar{D} \vee C, D, \bar{C} \vee A \vee B \Rightarrow A \vee B$,
 1. 1. $B, D, \bar{C} \vee A \vee B, \bar{A} \Rightarrow B$,
 1. 2. $\bar{D}, D, \bar{C} \vee A \vee B, \bar{A} \rightarrow B$,
 1. 3. $C, D, \bar{C} \vee A \vee B \Rightarrow A \vee B$,
 - 1.3.1. $C, D, \bar{C} \Rightarrow A \vee B$,
 - 1.3.2. $C, D, A, \bar{A} \rightarrow B$,
 - 1.3.3. $C, D, B, \bar{A} \Rightarrow B$.

4) Доказать методом резолюций истинность следующей клаузы:

$$A \rightarrow B, C \rightarrow D, B \rightarrow E, D \rightarrow F, E \rightarrow \bar{F}, A \rightarrow C \Rightarrow \bar{A}.$$

Доказательство:

$$\bar{A} \vee B, \bar{C} \vee D, \bar{B} \vee E, \bar{D} \vee F, \bar{E} \vee \bar{F}, \bar{A} \vee C, A \Rightarrow 0.$$

- | | | | |
|----------------------------|--------------|----------------|------------|
| 1. $\bar{C} \vee F,$ | (P_2, P_4) | 4. $A \vee F,$ | $(1, P_6)$ |
| 2. $\bar{B} \vee \bar{F},$ | (P_3, P_5) | 5. $A,$ | $(3, 4)$ |
| 3. $\bar{A} \vee \bar{F},$ | $(2, P_1)$ | 6. $0.$ | $(6, P_7)$ |

5) Пусть задана система аксиом :

$$A1. I \Rightarrow A \rightarrow (B \rightarrow A),$$

$$A2. I \Rightarrow (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C)),$$

$$A3. I \Rightarrow (A \rightarrow B) \rightarrow ((A \rightarrow \bar{B}) \rightarrow \bar{A});$$

и правило отделения (modus ponens — MP):

$$A, A \rightarrow B \Rightarrow B.$$

С помощью этих аксиом и правила MP доказать справедливость закона рефлексивности:

$$I \Rightarrow A \rightarrow A.$$

Доказательство (символы « $I \Rightarrow$ » здесь и в следующем примере писать не будем):

- | | |
|---|--------------|
| 1. $A \rightarrow ((A \rightarrow A) \rightarrow A),$ | $(A1)$ |
| 2. $(A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)),$ | $(A2)$ |
| 3. $(A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A),$ | $(1, 2, MP)$ |
| 4. $A \rightarrow (A \rightarrow A),$ | $(A1)$ |
| 5. $A \rightarrow A.$ | $(3, 4, MP)$ |

6) С помощью средств предыдущего примера доказать клаузу:

$$\bar{X}, Y, Z \rightarrow X, S \rightarrow (Y \vee Z), (T \vee U) \rightarrow S \Rightarrow \bar{T}.$$

Доказательство:

- | | |
|---|----------------|
| 1. $(Z \rightarrow X) \rightarrow ((Z \rightarrow \bar{X}) \rightarrow \bar{Z}),$ | $(A1)$ |
| 2. $(Z \rightarrow \bar{X}) \rightarrow \bar{Z},$ | $(1, P_3, MP)$ |
| 3. $\bar{X} \rightarrow (Z \rightarrow \bar{X}),$ | $(A1)$ |
| 4. $Z \rightarrow \bar{X},$ | $(3, P_1, MP)$ |
| 5. $(S \rightarrow (\bar{Y} \rightarrow Z)) \rightarrow ((S \rightarrow \bar{Y}) \rightarrow (S \rightarrow Z)),$ | $(A2)$ |
| 6. $(S \rightarrow \bar{Y}) \rightarrow (S \rightarrow Z),$ | $(5, P_4, MP)$ |
| 7. $\bar{Y} \rightarrow (S \rightarrow \bar{Y}),$ | $(A1)$ |
| 8. $S \rightarrow \bar{Y},$ | $(7, P_2, MP)$ |
| 9. $S \rightarrow Z.$ | $(6, 8, MP)$ |
| 10. $(S \rightarrow Z) \rightarrow ((S \rightarrow \bar{Z}) \rightarrow \bar{S}).$ | $(A3)$ |
| 11. $(S \rightarrow \bar{Z}) \rightarrow \bar{S},$ | $(9, 10, MP)$ |

- | | |
|---|--------------------|
| 12. $\bar{Z} \rightarrow (S \rightarrow \bar{Z})$, | (A1) |
| 13. $\bar{Z}$, | (2, 4, MP) |
| 14. $S \rightarrow \bar{Z}$, | (12, 13, MP) |
| 15. $\bar{S}$. | (11, 14, MP) |
| 16. $(T \vee U) \rightarrow S \equiv T \rightarrow S, U \rightarrow S$. | (P ₅ .) |
| 17. $(T \rightarrow S) \rightarrow ((T \rightarrow \bar{S}) \rightarrow \bar{T})$. | (A3) |
| 18. $(T \rightarrow \bar{S}) \rightarrow \bar{T}$, | (16, 17, MP) |
| 19. $\bar{S} \rightarrow (T \rightarrow \bar{S})$. | (A1) |
| 20. $T \rightarrow \bar{S}$, | (15, 19, MP) |
| 21. $\bar{T}$. | (18, 20, MP) |

7) Составить легенды для приведенных ниже четырех клауз.

Клауза 1: $A \sim C, C \sim E, E \rightarrow D, D \rightarrow B \Rightarrow A \rightarrow B$.

A — Падение авторитета власти.

B — Политики, не способные управлять страной.

C — Нарастание анархии в обществе.

D — Высказывание абсурдных идей.

E — Появление безответственных политиков.

«Падение авторитета власти происходит тогда и только тогда, когда нарастает анархия в обществе ($A \sim C$). Нарастание анархии в обществе равносильно появлению на политической арене безответственных политиков ($C \sim E$). Появление подобных политиков приводит к тому, что они высказывают абсурдные идеи ($E \rightarrow D$). Высказывание политиками таких идей демонстрирует неспособность их управлять страной ($D \rightarrow B$). Итак, падение авторитета власти приводит к появлению политиков, не способных управлять страной ($A \rightarrow B$)».

Клауза 2: $A \rightarrow B, B \rightarrow E, A \rightarrow C, C \rightarrow D, D \rightarrow F, \bar{E} \wedge \bar{F} \Rightarrow \bar{A}$.

«Если человек занимается спортом (**A**), то он хочет быть здоровым (**B**). Хорошее здоровье (**B**) ведет к счастливой жизни (**E**). Кроме того, если человек занимается спортом (**A**), то он, как правило, стремится достичь высоких спортивных результатов (**C**). Наличие высоких результатов (**C**) позволяет одерживать победы на соревнованиях (**D**). Победы на соревнованиях (**D**) влекут за собой всеобщее признание (**F**). Однако, человек не хочет жить счастливо и иметь всеобщее признание ($\bar{E} \wedge \bar{F}$). Значит, он не станет заниматься и спортом ($\bar{A}$)».

Клауза 3: $J \rightarrow H, K \rightarrow H, I \rightarrow J, H \rightarrow I, \bar{H} \rightarrow \bar{J} \wedge \bar{K}$.

«Если знать язык программирования (**J**), то можно составить рабочую программу (**H**). Рабочую программу можно также получить (**H**) при условии наличия знакомого программиста (**K**). Овладеть языком программирования (**J**) можно, обучаясь в институте (**I**). Если программа работает (**H**), то ее написал выпускник такого института (**I**). Но программа не работает (**H**). Это говорит о том, что желающий получить правильный результат не знает языка программирования (**J**) и не имеет знакомых программистов (**K**)».

Клауза 4. $A \rightarrow B, C \rightarrow D, B \wedge D \rightarrow E, A, \bar{E} \Rightarrow \bar{C}$.

«Все живое способно чувствовать ($A \rightarrow B$). Всякое материальное тело занимает определенный объем ($C \rightarrow D$). Если нечто занимает пространственный объем и способно чувствовать, то это нечто есть ни что иное, как живой организм ($B \wedge D \rightarrow E$). Пусть существует нечто живое (A), но не являющееся организмом ($\bar{E}$). Тогда следует вывод, что это нечто нематериально ($\bar{C}$)».

8) Выше приведены легенды. Запишем клаузы, отвечающие тексту или контексту этих легенд, для чего сформулируем необходимые посылки и два следствия: одно истинное, другое ложное. С помощью таблицы истинности найдем МНФ, минимальное и все трансверсальные покрытия (последнее задание выполнено только для варианта 21).

Для варианта 21 можно предложить следующую клаузу:

$A \sim B, C \rightarrow A, D \rightarrow B, C \rightarrow E, E \rightarrow C \rightarrow B$.

A — Где-то что-то убыло.

B — Где-то что-то прибыло.

C — “Черная дыра” существует.

D — “Белая дыра” существует.

E — Невозможность ничего увидеть.

Исходную легенду допустимо трансформировать в близкую по смыслу и составить таблицу истинности (табл. 1.23):

«Если в одном месте что-то убудет, то в другом что-то непременно прибудет, и наоборот ($A \sim B$). Если существует “черная дыра”, то в нее все проваливается, то есть в ее окрестностях что-то убывает ($C \rightarrow A$). Если существует “белая дыра”, то из нее в окружающее пространство должно прибывать вещество ($D \rightarrow B$). Если существует “черная дыра”, то ее невозможно увидеть, так как она не излучает свет ($C \rightarrow E$). Астроном ничего не увидел (E). Итак, “белая дыра” существует (D).» Это — ложное умозаключение. Истинным же заключением является, например, следующее: «Если существует “черная дыра”, то где-то в пространстве вселенной должно непременно появляться вещество ($C \rightarrow B$)».

Из табл. 1.23 видно, что три единицы обобщенной посылки (P) не покрываются единицами ложного следствия (D); единицы же истинного следствия ($C \rightarrow B$) целиком накрывают единицы обобщенной посылки. По табл. 1.23 составим СДНФ:

$A, B, C, D, E; \quad A, B, \bar{C}, D, E; \quad A, B, C, \bar{D}, E;$

$A, B, \bar{C}, \bar{D}, E; \quad \bar{A}, \bar{B}, \bar{C}, \bar{D}, E.$

После преобразований получим следующую МДФ:

$A, B, D, E; \bar{A}, \bar{B}, \bar{C}, \bar{D}, E.$

Трансверсальные покрытия:

$\bar{A}; \bar{B}, \bar{C}, \bar{D}, E \quad A, B; \bar{C}, \bar{D}, E \quad A, B, E; \bar{C}, \bar{D}.$

Минимальное покрытие: $E.$

Таблица 1.23

A	B	C	D	E	A → B	C → A	D → B	C → E	F	D	C → B
1	1	1	1	1	1	1	1	1	1	1	1
0	1	1	1	1	0	0	1	1	0	1	1
1	0	1	1	1	0	1	0	1	0	1	0
0	0	1	1	1	1	0	0	1	0	1	0
1	1	0	1	1	1	1	1	1	1	1	1
0	1	0	1	1	0	1	1	1	0	1	1
1	0	0	1	1	0	1	0	1	0	1	1
0	0	0	1	1	1	1	0	1	0	1	1
1	1	1	0	1	1	1	1	1	1	0	1
0	1	1	0	1	0	0	1	1	0	0	1
1	0	1	0	1	0	1	1	1	0	0	0
0	0	1	0	1	1	0	1	1	0	0	0
1	1	0	0	1	1	1	1	1	1	0	1
0	1	0	0	1	0	1	1	1	0	0	1
1	0	0	0	1	0	1	1	1	0	0	1
0	0	0	0	1	1	1	1	1	1	0	1
1	1	1	1	0	1	1	1	0	0	1	1
0	1	1	1	0	0	0	1	0	0	1	1
1	0	1	1	0	0	1	0	0	0	1	0
0	0	1	1	0	1	0	0	0	0	1	0
1	1	0	1	0	1	1	1	1	0	1	1
0	1	0	1	0	0	1	1	1	0	1	1
1	0	0	1	0	0	1	0	1	0	1	1
0	0	0	1	0	1	1	0	1	0	1	1
1	1	1	0	0	1	1	1	0	0	0	1
0	1	1	0	0	0	0	1	0	0	0	1
1	0	1	0	0	0	1	1	0	0	0	0
0	0	1	0	0	1	0	1	0	0	0	0
1	1	0	0	0	1	1	1	1	0	0	1
0	1	0	0	0	0	1	1	1	0	0	1
1	0	0	0	0	0	1	1	1	0	0	1
0	0	0	0	0	1	1	1	1	0	0	1

Для варианта 22 можно составить следующую клаузу:

$$A \rightarrow B, B \rightarrow C, E \rightarrow (\bar{B} \rightarrow D), D \rightarrow F \rightarrow (\bar{B} \wedge \bar{A} \wedge E) \rightarrow F.$$

Введем следующие обозначения:

- A — Возникновение перепада напряжения в сети.
- B — Перегорание предохранителя.
- C — Необходимость замены предохранителя.
- D — Телевизор работает нормально.
- E — Телевизор подключен к сети питания.
- F — Я смотрю "Новости".

«Если в сети был большой перепад напряжения, то сгорит предохранитель ($A \rightarrow B$). Если предохранитель сгорел, необходима его замена ($B \rightarrow C$). Если телевизор включен в сеть, то телевизор работает нормально при условии целостности предохранителя ($E \rightarrow (B \rightarrow D)$). Если телевизор работает нормально, я увижу “Новости” ($D \rightarrow F$). Я увижу “Новости” при условии отсутствия перепада напряжения и подключения телевизора к сети питания ($(\bar{A} \wedge E) \rightarrow F$)». Данное следствие является *ложным*. Истинным же следствием будет: «Я увижу “Новости” при условии целостности предохранителя, отсутствия перепада напряжения в сети и подключения телевизора к сети питания ($(B \wedge \bar{A} \wedge E) \rightarrow F$)». Выделим ту строку табл. 1.24, для которой обобщенная посылка (P) и *истинное* следствие ($(B \wedge \bar{A} \wedge E) \rightarrow F$) принимают значения единицы, а *ложное* следствие ($(\bar{A} \wedge E) \rightarrow F$) — значение нуля.

Таблица 1.24

A	B	C	D	E	F	$A \rightarrow B$	$B \rightarrow C$	$E \rightarrow (B \rightarrow D)$	$D \rightarrow F$	P	$(\bar{A} \wedge E) \rightarrow F$	$(B \wedge \bar{A} \wedge E) \rightarrow F$
0	1	1	0	1	0	1	1	1	1	1	0	1

Для варианта 23 допустимо составить следующую простую клаузу:

$$A \rightarrow B, B \rightarrow C, C \rightarrow D, D \rightarrow E \Rightarrow A \rightarrow E.$$

A — Работа выполнена.

D — Рыбалку провести с лодкой.

B — Отпуск на рыбалку.

E — На рыбалку поедут все вместе.

C — Взять на рыбалку сына.

«Если работа выполнена, то начальство отпустит на рыбалку ($A \rightarrow B$). Если отпустят на рыбалку, то обязательно возьмут на нее и сына ($B \rightarrow C$). Если берут сына, значит надо брать лодку ($C \rightarrow D$). Если брать с собой лодку, то поедут все вместе ($D \rightarrow E$). Таким образом, если работа выполнена, то все вместе едут на рыбалку ($A \rightarrow E$)». Данное следствие является *истинным*. Ложным следствием является, очевидно, такое: «Если работа сделана, то все вместе на рыбалку не едут ($A \rightarrow \bar{E}$)».

Для варианта 24 составим следующую клаузу:

$$A \rightarrow (B \wedge C), \bar{C} \rightarrow \bar{D}, \bar{B} \rightarrow (A \rightarrow E), D \rightarrow (B \vee \bar{A}) \Rightarrow (\bar{A} \wedge B) \rightarrow C.$$

A — Уменьшение температуры.

B — Снижение давления.

D — Снижение скорости.

C — Уменьшение объема.

E — Падение уровня.

«Уменьшение температуры приводит к снижению давления и уменьшению объема ($A \rightarrow (B \wedge C)$). Увеличение объема приводит к росту скорости потока ($\bar{C} \rightarrow \bar{D}$). Повышение давления приводит к падению уровня, если при этом уменьшать температуру ($\bar{B} \rightarrow (A \rightarrow E)$). Снижение скорости приводит к уменьшению давления или росту температуры ($D \rightarrow (B \vee \bar{A})$). Технолог Иванов рассудил так: “Мне надо повысить давление при одновременном снижении скорости потока, поэтому я должен увеличить объем и температуру” ($(\bar{A} \wedge \bar{C}) \rightarrow (B \wedge D)$)». Данное умозаключение является *ложным*. Истинным рассуждением будет, например, такое: «Уменьшение температуры и увеличение давления ведут к уменьшению объема ($(\bar{A} \wedge B) \rightarrow C$)».

Для варианта 25 составим клаузу:

$$A \vee B \vee C, (C \wedge D) \rightarrow E, (A \vee B) \rightarrow \bar{E}, C \rightarrow D, \Rightarrow C \rightarrow E.$$

A — Надеть брезентовые штаны.

D — Взять с собой сумку.

B — Надеть шерстяное платье.

E — Великолепно смотрится.

C — Надеть пиджак и юбку с разрезом.

«Я могу надеть на себя брезентовые штаны или шерстяное платье или пиджак и юбку с разрезом ($A \vee B \vee C$). Я буду выглядеть великолепно, если надену пиджак и юбку с разрезом и при этом возьму с собой сумку ($(C \wedge D) \rightarrow E$). И наоборот, я буду выглядеть ужасно, если надену на себя брезентовые штаны или шерстяное платье ($(A \vee B) \rightarrow \bar{E}$). Однако сумку надо брать обязательно, если надеть пиджак и юбку с разрезом ($C \rightarrow D$). Итак, чтобы выглядеть великолепно я выберу последнее, т.е. надену на себя пиджак и юбку с разрезом ($C \rightarrow E$)». Данное заключение является истинным. Ложным может быть, например, такое: «Чтобы выглядеть великолепно, нужно надеть на себя брезентовые штаны ($A \rightarrow E$)».

1.9. Операции над предикатами и кванторами

Предикат — это функциональное высказывание, а высказывание — предикатная константа. *Логика предикатов* — это расширение логики высказываний за счет использования предикатов в роли логических функций. Эти функции несколько отличаются от функций, которые мы использовали в логике Буля. Булева функция *однородна*, т.е. для нее область значений функции и область изменений аргументов по типу одна и та же — *логическая* (либо истина, либо ложь). Для предикатов же область значений функции — *логическая*, а область изменений аргументов — *предметная*. Таким образом, эта функция — *неоднородна*. Приведем примеры предикатных функций. Пусть имеется ряд простых высказываний:

P_1 = «Иван читает Достоевского»,

P_2 = «Петр читает Достоевского»,

.....,

P_n = «Степан читает Достоевского».

Вместо высказываний $P_1, P_2, \dots, P_n$ мы могли бы ввести *одноместный предикат* $P(x)$, для которого переменная x принимала бы значения из предметной области —

$x = \{\text{Иван, Петр, } \dots, \text{Степан}\}$,

а сама предикатная функция передавалась бы словами:

$P(x)$ = « x читает Достоевского».

Теперь изменим исходный ряд высказываний на другой:

P_1 = «Иван читает Достоевского»,

P_2 = «Петр читает Толстого»,

.....,

P_n = «Степан читает Чехова».

Здесь можно было бы ввести уже *двухместный предикат* —

$$P(x, y) = \text{« } x \text{ читает } y \text{ »}$$

с дополнительной предметной областью —

$$y = \{\text{Достоевский, Толстой, ... , Чехов}\}.$$

Введем *трехместный предикат* $P(x, y, z)$, который означает, что « x есть сумма y и z ». Допустим, в процессе вычислений переменная x приняла конкретное значение, равное 5. Тогда трехместный предикат превратится в двухместный:

$$P(5, y, z) = P'(y, z) = \text{« } 5 \text{ есть сумма } y \text{ и } z \text{ »}.$$

При $x = 5$ и $y = 3$ получим одноместный предикат:

$$P(5, 3, z) = P'(3, z) = P''(z) = \text{« } 5 \text{ есть сумма } 3 \text{ и } z \text{ »}.$$

Наконец, если добавить условие $z = 2$, то исходный предикат становится *нульместным предикатом* (*константой* или *высказыванием*), который в данном случае принимает истинное значение:

$$P_1 = P(5, 3, 2) = \text{« } 5 \text{ есть сумма } 3 \text{ и } 2 \text{ »} = 1.$$

Но могло случиться, что $z = 1$ тогда имели бы ложное высказывание:

$$P_0 = P(5, 3, 1) = \text{« } 5 \text{ есть сумма } 3 \text{ и } 1 \text{ »} = 0.$$

Таким образом, при замещении переменной x_i предметной постоянной a_i происходит превращение n -местного предиката $P(x_1, \dots, x_i, \dots, x_n)$ в $(n-1)$ -местный — $P(x_1, \dots, a_i, \dots, x_n)$. Приписав конкретные значения всем аргументам предикатной функции — $P(a_1, \dots, a_i, \dots, a_n)$, мы тем самым получаем предикатную константу, к которой применимы все законы логики высказываний.

Функциональная природа предиката влечет за собой введение еще одного понятия — *квантора*. Роль его выясним на следующих двух примерах:

- 1) «Все люди смертны. Сократ человек.
Следовательно, Сократ смертен.»
- 2) «Некоторые люди гениальны. Сократ человек.
Следовательно, Сократ гениален.»

Во втором примере хорошо чувствуется ложность заключения, поскольку интуитивно мы понимаем, что Сократ мог и не попасть в число гениальных людей.

Итак, ключевыми словами в наших примерах являются «все» и «некоторые». Когда какое-нибудь правило распространяется на *всех* индивидуумов, оно, естественно, распространяется и на Сократа. Когда же правило касается только *некоторых*, оно может оказаться в отношении Сократа как раз и неверным.

Термин «*все x* » обозначается в логике предикатов $\forall x$ и называется *квантором общности* (символ $\forall$ есть перевернутая буква A , которая является начальной буквой английского слова All — «все»). Термин «*некоторые x* » или «*существует хотя бы одно значение x* » обозначается через $\exists x$ и называется *квантором существования* (символ $\exists$ есть перевернутая буква E , являющаяся первой буквой английского слова Exist — «существовать»).

Выставляя кванторы перед предикатами, мы как бы усиливаем или ослабляем их действие. Так, выражение

$$\forall x P(x)$$

означает «для всех без исключения x свойство P истинно», а выражение

$$\exists x P(x)$$

означает «существует по крайней мере одно значение x , для которого свойство P истинно». Мы не будем использовать так называемые *свободные переменные*, т.е. не будем рассматривать предикатные функции, аргументы которых не связаны ни квантором общности, ни квантором существования. Сказать «для всех x свойство P истинно» — это все равно, что сказать «конъюнкция всех значений предикатной функции равна единице»:

$$\forall x P(x) = P(a) \wedge P(b) \wedge P(c) \wedge \dots$$

Квантор существования означает дизъюнкцию всех значений предикатной функции:

$$\exists x P(x) = P(a) \vee P(b) \vee P(c) \vee \dots$$

Оба квантора можно отрицать и выражать один через другой на основе закона де Моргана:

$$\overline{\forall x P(x)} = \overline{P(a) \wedge P(b) \wedge P(c) \wedge \dots} = \overline{P(a)} \vee \overline{P(b)} \vee \overline{P(c)} \vee \dots = \exists x \overline{P(x)},$$

$$\exists x P(x) = \overline{\overline{P(a)} \vee \overline{P(b)} \vee \overline{P(c)} \vee \dots} = \overline{\overline{P(a)} \wedge \overline{P(b)} \wedge \overline{P(c)} \wedge \dots} = \forall x P(x).$$

Отсюда

$$\overline{\forall x \overline{P(x)}} = \exists x P(x), \quad \overline{\exists x \overline{P(x)}} = \forall x P(x).$$

Осмыслить формулы отрицания кванторов поможет следующий пример. Пусть предикат $P(x)$ означает, что « x является простым числом». Когда x будет пробегать ряд натуральных чисел —

$$x = \{1, 2, 3, 4, 5, 6, \dots\},$$

предикатная функция пробежит ряд истинных и ложных значений

$$P(1) = 0, \quad P(2) = 1, \quad P(3) = 1, \quad P(4) = 0,$$

$$P(5) = 1, \quad P(6) = 0, \quad P(7) = 1, \quad \dots$$

Убедимся в справедливости первой формулы для отрицания квантора общности:

$$\overline{\forall x P(x)} = \text{«не все } x \text{ простые числа»} = \text{«существуют такие } x, \text{ которые являются непростыми числами»} = \exists x \overline{P(x)} = 1.$$

Оба эти высказывания истинны. Теперь убедимся в справедливости второй формулы для отрицания квантора существования:

$$\overline{\exists x P(x)} = \text{«нет ни одного } x, \text{ которое было бы простым»} = \\ = \text{«все } x \text{ являются непростыми числами»} = \forall x \overline{P(x)} = 0.$$

Эти высказывания — ложны.

Пусть предметная область предиката $P(x)$ состоит всего из двух конкретных значений a и b . Учитывая, что

$$\forall x P(x) = P(a) \wedge P(b), \quad \exists x P(x) = P(a) \vee P(b),$$

составим табл. 1.25, из которой непосредственно вытекают три элементарных клаузы:

$$\forall x P(x) \Rightarrow P(a), \quad P(a) \Rightarrow \exists x P(x), \quad \forall x P(x) \Rightarrow \exists x P(x).$$

Вместо $P(a)$ в последних выражениях можно было бы взять $P(b)$ — семантика клаузы от этого не изменится, а она такова: если выражение «для всех x свойство P выполняется» является истинным, то для конкретного значения x , равного a , это свойство тоже будет выполняться. Первая клауза является предикатной формой выражения аксиомы порядка:

$$\forall x P(x) \rightarrow P(a), P(b) \rightarrow P(a) .$$

Таблица 1.25

$P(a)$	$P(b)$	$\forall x P(x)$	$\exists x P(x)$
0	0	0	0
1	0	0	1
0	1	0	1
1	1	1	1

Действие ее продемонстрируем на уже знакомом нам примере, который сейчас мы сформулируем более отчетливо:

Для всех x справедливо правило: если x — человек, то x смертен. Сократ человек. Следовательно, Сократ смертен.

Введем два предиката:

$$A(x) = \text{«}x \text{ — человек»} \text{ и } B(x) = \text{«}x \text{ смертен»}.$$

Примем также, что $a = \text{«Сократ»}$. Составим клаузу, соответствующую нашей легенде:

$$\forall x (A(x) \rightarrow B(x)), A(a) \rightarrow B(a) .$$

Для ее доказательства достаточно перенести вторую посылку вправо за знак метаимпликации, чтобы клауза сразу же удовлетворяла аксиоме порядка в предикатной форме:

$$\forall x (A(x) \rightarrow B(x)) \Rightarrow A(a) \rightarrow B(a) .$$

Ясно, что второй пример с заключением о гениальности Сократа является ложным выводом, поскольку приводит к клаузе, противоречащей аксиоме порядка:

$$\exists x (A(x) \rightarrow B(x)) \Rightarrow A(a) \rightarrow B(a) .$$

Конъюнктивная природа квантора общности и дизъюнктивная квантора существования с точки зрения *отношения эквивалентности* накладывают определенные ограничения при использовании их совместно с дизъюнкцией и конъюнкцией как логическими операциями.

Пусть для определенности предметная область состоит из двух элементов a и b (в общем случае для областей, состоящих из n элементов, все представленные здесь доказательства останутся теми же, только окажутся более громоздкими). Убедимся, что следующие два тождества выполняются:

$$\forall x (A(x) \wedge B(x)) = \forall x A(x) \wedge \forall x B(x) ,$$

$$\exists x (A(x) \vee B(x)) = \exists x A(x) \vee \exists x B(x) .$$

Действительно,

$$\forall x (A(x) \wedge B(x)) = (A(a) \wedge B(a)) \wedge (A(b) \wedge B(b)) =$$

$$= (A(a) \wedge B(b)) \wedge (A(a) \wedge B(b)) = \forall x A(x) \wedge \forall x B(x).$$

Аналогично расписывается второе равенство.

Однако ситуация изменится, если квантор общности использовать совместно с дизъюнкцией, а квантор существования — с конъюнкцией:

$$\exists x (A(x) \wedge B(x)) \rightarrow \exists x A(x) \wedge \exists x B(x).$$

В самом деле,

$$\exists x (A(x) \wedge B(x)) = (A(a) \wedge B(a)) \vee (A(b) \wedge B(b)) = R \wedge Q, \text{ где}$$

$$R = (A(a) \vee A(b)) \wedge (B(a) \vee B(b)) = \exists x A(x) \wedge \exists x B(x),$$

$$Q = (A(a) \vee B(b)) \wedge (A(b) \vee B(a)).$$

Первая клауза верна, так как она сводится к аксиоме порядка:

$$R, Q \rightarrow R.$$

Аналогично доказывается клауза —

$$\forall x A(x) \vee \forall x B(x) \rightarrow \forall x (A(x) \vee B(x)).$$

В логике предикатов, как и в логике высказываний или логике Буля, действует *принцип двойственности*. Клауза останется в силе, если ее посылки и заключения поменять местами, но при этом одновременно произвести замену:

$$\forall \leftrightarrow \exists, \quad \wedge \leftrightarrow \vee, \quad 0 \leftrightarrow 1.$$

Благодаря этому принципу последнюю клаузу можно не доказывать отдельно, а составить, исходя из истинности предыдущей.

Установленное свойство кванторов в отношении дизъюнкции отражается и на импликации, поскольку она может быть выражена через дизъюнкцию. Поэтому справедливы следующие выражения:

$$\exists x (A(x) \rightarrow B(x)) = \forall x A(x) \rightarrow \exists x B(x),$$

$$\exists x A(x) \rightarrow \forall x B(x) \Rightarrow \forall x (A(x) \rightarrow B(x)).$$

Но ситуация вновь изменится в пользу отношения эквивалентности, если любой из двух предикатов заменить высказыванием:

$$\forall x (A \vee B(x)) = A \vee \forall x B(x),$$

$$\exists x (A \wedge B(x)) = A \wedge \exists x B(x).$$

Действительно,

$$\begin{aligned} \forall x (A \vee B(x)) &= (A \vee B(a)) \wedge (A \vee B(b)) = \\ &= A \vee (A \wedge B(a)) \vee (A \wedge B(b)) \vee (B(a) \wedge B(b)) = \\ &= A \vee (B(a) \wedge B(b)) = A \vee \forall x B(x). \end{aligned}$$

Раскрывая скобки и используя закон идемпотентности и поглощения, или применяя вновь принцип двойственности, можно доказать второе равенство. Отсюда будут выполняться и равенства для импликации:

$$\forall x (A \rightarrow B(x)) = A \rightarrow \forall x B(x),$$

$$\forall x (A(x) \rightarrow B) = \exists x A(x) \rightarrow B,$$

$$\exists x (A \rightarrow B(x)) = A \rightarrow \exists x B(x),$$

$$\exists x (A(x) \rightarrow B) = \forall x A(x) \rightarrow B.$$

Чтобы сохранить отношение эквивалентности при вынесении за скобки квантора $\exists$ при конъюнкции и квантора $\forall$ при дизъюнкции, когда даны два различных предиката, прибегают к введению дополнительной переменной, например:

$$\begin{aligned}\exists x A(x) \wedge \exists x B(x) &= \exists x A(x) \wedge \exists y B(y) = \exists x \exists y (A(x) \wedge B(y)) = \\ &= (A(a) \vee A(b)) \wedge (B(a) \vee B(b)).\end{aligned}$$

Аналогично поступают в других случаях:

$$\begin{aligned}\forall x A(x) \vee \forall x B(x) &= \forall x \forall y (A(x) \vee B(y)) , \\ \exists x A(x) \rightarrow \forall x B(x) &= \forall x \forall y (A(x) \rightarrow B(y)) , \\ \exists x A(x) \vee \forall x B(x) &= \exists x \forall y (A(x) \vee B(y)) \rightarrow \\ &= \forall x \exists y (A(x) \vee B(y)) = \forall x \exists y (A(y) \vee B(x)) .\end{aligned}$$

Последний пример показывает, что кванторы $\forall$ и $\exists$ можно переставлять местами, если они независимы (в данном случае они относятся к независимым одноместным предикатам).

Рассмотрим всевозможные комбинации кванторов при двухместных предикатах. С помощью законов коммутативности и ассоциативности для конъюнкции и дизъюнкции доказывается справедливость двух тождеств:

$$\forall x \forall y P(x, y) = \forall y \forall x P(x, y) , \quad \exists x \exists y P(x, y) = \exists y \exists x P(x, y) ,$$

т.е. одинаковые кванторы при двухместных предикатах можно переставлять местами. Но перестановка кванторов $\exists$ и $\forall$ подчинена только отношению порядка:

$$\exists x \forall y P(x, y) \Rightarrow \forall y \exists x P(x, y) .$$

В самом деле,

$$\begin{aligned}\exists x \forall y P(x, y) &= \exists x (P(x, a) \wedge P(x, b)) = \\ &= (P(a, a) \wedge P(a, b)) \vee (P(b, a) \wedge P(b, b)) = R \wedge Q ,\end{aligned}$$

где

$$\begin{aligned}Q &= (P(a, a) \vee P(b, b)) \wedge (P(a, b) \vee P(b, a)) , \\ R &= (P(a, a) \vee P(b, a)) \wedge (P(a, b) \vee P(b, b)) = \\ &= \forall y (P(a, y) \vee P(b, y)) = \forall y \exists x P(x, y) .\end{aligned}$$

Таким образом, исходная клауза свелась к аксиоме порядка —

$$R, Q \Rightarrow R .$$

Справедливость последней клаузы можно установить и с помощью таблицы истинности (табл. 1.26), в которой приняты следующие сокращения:

$$\begin{aligned}\forall \forall P &= \forall x \forall y P(x, y) , \quad \exists \forall P = \exists x \forall y P(x, y) , \\ \forall \exists P &= \forall y \exists x P(x, y) , \quad \exists \exists P = \exists x \exists y P(x, y) .\end{aligned}$$

На основе этой же таблицы можно установить истинность множества других клауз (k и m принимают значения a или b):

1. $\forall x \forall y P(x, y) \Rightarrow \forall x \exists y P(x, y)$, 4. $\exists x \forall y P(x, y) \Rightarrow \exists x \exists y P(x, y)$,
2. $\forall x \forall y P(x, y) \Rightarrow \exists x \forall y P(x, y)$, 5. $\forall x \exists y P(x, y) \Rightarrow \exists x \exists y P(x, y)$,
3. $\forall x \forall y P(x, y) \Rightarrow \exists x \exists y P(x, y)$, 6. $\exists x \forall y P(x, y) \Rightarrow \forall y \exists x P(x, y)$,

7. $\forall x \forall y P(x, y) \rightarrow \forall x P(x, x)$, 13. $\forall x P(x, m) \Rightarrow \exists y \forall x P(x, y)$,
8. $\exists x P(x, x) \rightarrow \neg x \exists y P(x, y)$, 14. $\forall x P(x, m) \rightarrow \forall x \exists y P(x, y)$,
9. $\forall x \forall y P(x, y) \Rightarrow P(k, m)$, 15. $\forall x \exists y P(x, y) \Rightarrow \exists y P(k, y)$,
10. $P(k, m) \Rightarrow \exists x \exists y P(x, y)$, 16. $\exists y \forall x P(x, y) \Rightarrow \exists y P(k, y)$,
11. $\forall y P(k, y) \Rightarrow \forall y \exists x P(x, y)$, 17. $\exists x \forall y P(x, y) \Rightarrow \exists x P(x, m)$,
12. $\forall y P(k, y) \Rightarrow \exists x \forall y P(x, y)$, 18. $\forall y \exists x P(x, y) \rightarrow \exists x P(x, m)$.

Таблица 1.26

$P(a, a)$	$P(a, b)$	$P(b, a)$	$P(b, b)$	$\forall \forall P$	$\exists \forall P$	$\forall \exists P$	$\exists \exists P$
0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	1
0	1	0	0	0	0	0	1
1	1	0	0	0	1	1	1
0	0	1	0	0	0	0	1
1	0	1	0	0	0	0	1
0	1	1	0	0	0	1	1
1	1	1	0	0	1	1	1
0	0	0	1	0	0	0	1
1	0	0	1	0	0	1	1
0	1	0	1	0	0	0	1
1	1	0	1	0	1	1	1
0	0	1	1	0	1	1	1
1	0	1	1	0	1	1	1
0	1	1	1	0	1	1	1
1	1	1	1	1	1	1	1

Пять первых клауз из приведенного списка являются для нас сейчас особенно важными, так как они дают ключ к пониманию процедуры составления истинных клауз для многоместных предикатов с любым числом кванторов. Эту процедуру схематично можно пояснить следующим образом. Для одноместных предикатов справедливы три клаузы:

$$\forall P \Rightarrow \forall P, \quad \forall P \rightarrow \neg P, \quad \neg P \Rightarrow \exists P.$$

Клауза

$$\neg P \Rightarrow \forall P$$

является ошибочной. Для двухместных предикатов будут верны уже девять клауз, четыре из которых являются тождествами, а пять других как раз и возглавляют приведенный список:

$$\begin{aligned} \forall(\forall P) &\Rightarrow \forall(\forall P), & \forall(\forall P) &\Rightarrow \exists(\forall P), & \exists(\forall P) &\Rightarrow \exists(\forall P), \\ \forall(\forall P) &\Rightarrow \forall(\exists P), & \forall(\forall P) &\Rightarrow \exists(\exists P), & \exists(\forall P) &\Rightarrow \exists(\exists P), \\ \forall(\exists P) &\Rightarrow \forall(\exists P), & \forall(\exists P) &\Rightarrow \exists(\neg P), & \exists(\exists P) &\Rightarrow \exists(\neg P). \end{aligned}$$

Клаузы-тождества не следует отбрасывать, если мы хотим построить следующий ряд для трехместных предикатов, например:

$$\forall(\forall\forall P) \rightarrow \exists(\forall\forall P), \quad \forall(\forall\exists P) \rightarrow \exists(\forall\exists P).$$

Зная процедуру построения правильных клауз, легко распознать истинность клауз, в частности:

$$\exists\forall\exists\forall P \Rightarrow \exists\exists\forall\exists P \text{ — истинная, } \exists\forall\forall P \Rightarrow \exists\forall\forall\exists P \text{ — ложная.}$$

Соседние одинаковые кванторы в многоместных предикатах можно переставлять в любом направлении; что же касается различных кванторов, то здесь допустима лишь перестановка, описанная клаузой 6 в вышеприведенном списке:

$$\dots \exists u \forall v \dots P(\dots, u, v, \dots) \Rightarrow \dots \forall v \exists u \dots P(\dots, u, v, \dots).$$

Одинаковые кванторы могут быть объединены по схеме, продиктованной клаузами 7 и 8:

$$\dots \forall u \forall v \dots P(\dots, u, v, \dots) \rightarrow \dots \forall u \dots P(\dots, u, u, \dots),$$

$$\dots \exists v \dots P(\dots, v, v, \dots) \rightarrow \dots \exists u \exists v \dots P(\dots, u, v, \dots).$$

Законы конкретизации, представленные в списке следующими десятью клаузами (с 8 по 18) и являющиеся производными от первых шести клауз, естественно, распространяются и на многоместные предикаты.

В отношении дизъюнкции и конъюнкции двух многоместных предикатов действуют примерно те же законы эквивалентности, что и для одноместных. Если все кванторы соответствуют операции, то введение дополнительных переменных необязательно, например:

$$\forall x \forall y (A(x, y) \wedge B(x, y)) = \forall x \forall y A(x, y) \wedge \forall x \forall y B(x, y).$$

Во всех остальных случаях необходимо вводить переменные:

$$\forall x \exists y \forall z \exists u \forall v \forall w (A(x, y, z) \vee B(u, v, w)) =$$

$$= \forall x \exists y \forall z A(x, y, z) \vee \exists u \forall v \forall w B(u, v, w).$$

Формализм теории предикатов, конечно, будет неполным без рассмотрения операции отрицания многоместных предикатов. Для понимания существа дела достаточно привести одно доказательство для двухместного предиката:

$$\bar{\exists}x \forall y P(x, y) = \bar{\exists}x (P(x, a) \wedge P(x, b)) = \forall x (\bar{P}(x, a) \wedge \bar{P}(x, b)) =$$

$$= \forall x \bar{\forall}y P(x, y) = (\bar{P}(a, a) \vee \bar{P}(a, b)) \wedge (\bar{P}(b, a) \vee \bar{P}(b, b)) = \forall x \exists y \bar{P}(x, y).$$

Отсюда вытекает простое правило перемещения символа отрицания слева направо для многоместных предикатов, например:

$$\overline{\forall\forall\exists\forall\exists P} = \exists\bar{\forall}\exists\forall\exists P = \exists\exists\bar{\forall}\exists P = \exists\exists\forall\bar{\exists}P = \exists\exists\forall\exists\bar{P} = \exists\exists\forall\exists\bar{P}.$$

Таким образом, чтобы произвести полное отрицание многоместного предиката с кванторами, необходимо прибегнуть к замене:

$$\exists \Leftrightarrow \forall, \quad P \Leftrightarrow \bar{P}.$$

Процедура составления истинных клауз из предикатов с кванторами, описанная в предыдущем подразделе, позволяет построить *булеан* из кванторов (рис. 1.20).

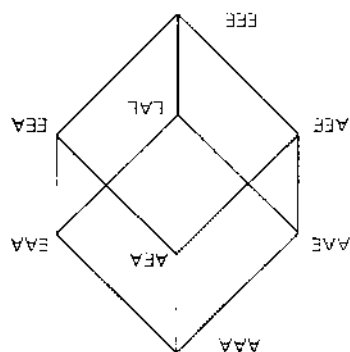


Рис. 1.20

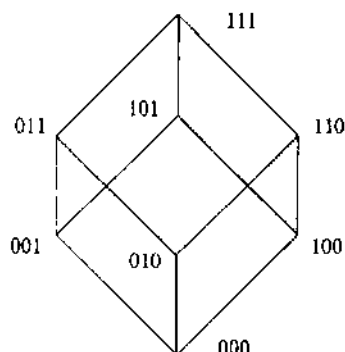


Рис. 1.21

Булеан — это очень распространенный математический объект. Так, если в кванторном булеане все символы $\forall$ заменить на 0 и $\exists$ — на 1, то получим булеан на 0,1-векторах (рис. 1.21). Если дано множество из элементов — a, b, c , то все его подмножества образуют точно такой же булеан (рис. 1.22). Наконец, приведем пример из арифметики: делители числа 30 образуют аналогичный булеан (рис. 1.23).

Булеан есть частично упорядоченное множество, на котором действуют законы логики множеств. Чтобы раскрыть его свойства, введем несколько определений.

Множество элементов любой природы называется *линейно-упорядоченным*, если любые два его элемента a и b связаны отношением порядка — либо $a \Rightarrow b$, либо $b \Rightarrow a$. Множество называется *частично упорядоченным*, если имеются по крайней мере два *несопоставимых элемента*, на которые не распространяется отношение порядка.

Верхней границей подмножества $Q \subset R$ называют такой элемент $g \in R$, что для всех $q \in Q$ справедливо отношение порядка $q \Rightarrow g$. *Нижней границей* подмножества $Q \subset R$ называют такой элемент $g' \in R$, что для всех $q \in Q$ справедливо отношение $g' \Rightarrow q$. *Наименьшая* верхняя граница называется *супремумом* ($\sup Q$), а *наибольшая* нижняя граница — *инфимумом* ($\inf Q$). Помимо супремума и инфимума, вводятся понятия *точной верхней грани* и *точной нижней грани*, которые могут

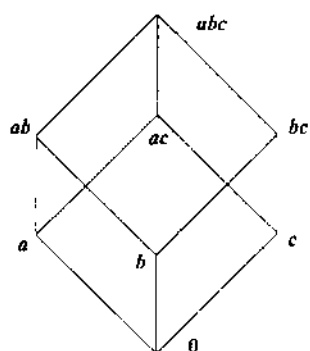


Рис. 1.22

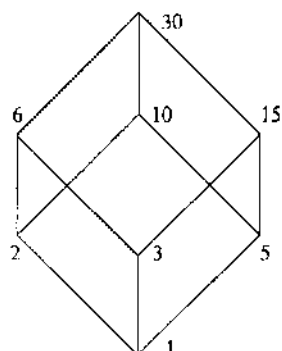


Рис. 1.23

совпадать или не совпадать, соответственно, с супремумом и инфимумом. Точную верхнюю грань двух элементов обозначим через дизъюнкцию $a \vee b$, точную нижнюю грань -- через конъюнкцию $a \wedge b$. Тогда в общем случае будем иметь:

$$a \vee b \Rightarrow \sup(a, b), \quad \inf(a, b) \Rightarrow a \wedge b.$$

Множество R называется *решеткой*, если каждая пара его элементов обязательно имеет один супремум и один инфимум. Множество $\forall\forall, \forall\exists, \exists\forall$ и $\exists\exists$ (рис. 1.24) образует решетку, так как удовлетворяет указанному требованию, например:

$$\sup(\forall\exists, \exists\exists) = \exists\exists, \quad \sup(\forall\exists, \exists\forall) = \exists\exists,$$

$$\inf(\forall\exists, \exists\exists) = \forall\exists, \quad \inf(\forall\exists, \exists\forall) = \forall\forall.$$

Множество a, b, c, d (рис. 1.25) не образует решетки, так как a и b имеют два инфимума и ни одного супремума, элементы c и d имеют два супремума и ни одного инфимума.

Решетка называется *булевой* или *булеаном*, если ее элементы удовлетворяют законам булевой логики -- *коммутативности, ассоциативности, дистрибутивности, нуля и единицы*. Для кванторных решеток все четыре закона выполняются:

$$\forall\forall\exists \vee \exists\exists\forall = \exists\exists\forall \vee \forall\forall\exists,$$

$$(\forall\exists\forall \vee \exists\forall\forall) \vee \exists\exists\forall = \forall\exists\forall \vee (\exists\forall\forall \vee \exists\exists\forall),$$

$$(\forall\forall\exists \wedge \exists\forall\forall) \vee \forall\forall\exists = (\forall\forall\exists \vee \forall\forall\forall) \wedge (\exists\forall\forall \vee \forall\forall\forall),$$

$$\forall\exists\forall \vee \exists\exists\exists = \exists\exists\exists, \quad \forall\exists\forall \wedge \exists\exists\exists = \forall\exists\forall,$$

$$\forall\exists\forall \vee \forall\forall\forall = \forall\exists\forall, \quad \forall\exists\forall \wedge \forall\forall\forall = \forall\forall\forall.$$

Поскольку в кванторном булеане предполагаются только положительные предикаты, т.е. отсутствуют обратные элементы, типа $\overline{\forall\exists\forall}$, то и в законе для нуля и единицы отсутствуют равенства, отражающие взаимное дополнение элементов. Однако вместо $\forall\forall\forall$ и $\exists\exists\exists$ можно взять полностью нулевой и единичный векторы, тогда уже все законы нуля и единицы будут выполняться, например:

$$\forall\exists\forall P \vee \exists\exists\exists \bar{P} = 1, \quad \forall\exists\forall P \wedge \exists\exists\exists \bar{P} = 0.$$

Если для кванторов справедливы аксиомы логики множеств, то на них должны распространяться и все выводимые из них тождества, например, *закон де Моргана*:

$$\overline{\forall\exists\forall \wedge \exists\forall\forall} = \overline{\forall\exists\forall} \vee \overline{\exists\forall\forall}.$$

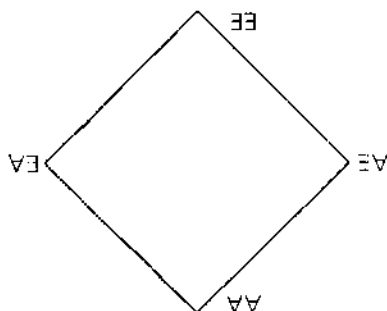


Рис. 1.24

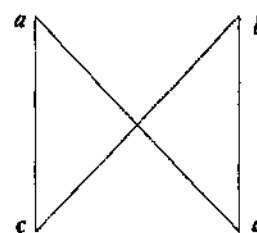


Рис. 1.25

Аксиома порядка, которая может быть выражена клаузами:

$$\forall \forall \exists, \exists \forall \forall \Rightarrow \forall \forall \exists, \quad \exists \exists \forall \Rightarrow \forall \forall \exists; \exists \exists \forall. \dots$$

также имеет место в логике предикатов.

На первый взгляд выражения типа

$$\forall \forall \exists \Rightarrow \forall \forall \exists \wedge \exists \exists \exists, \quad \forall \forall \exists \vee \exists \forall \exists \Rightarrow \exists \forall \exists$$

противоречат аксиоме порядка. Однако подобные клаузы всегда заменимы тождествами, поэтому их можно представить аксиомой порядка. Тождества возникают для линейно-упорядоченных элементов, каковыми и являются элементы $\forall \forall \exists$ и $\exists \forall \exists$:

$$\sup(\forall \forall \exists, \exists \forall \exists) = \forall \forall \exists \vee \exists \forall \exists = \exists \forall \exists,$$

$$\inf(\forall \forall \exists, \exists \forall \exists) = \forall \forall \exists \wedge \exists \forall \exists = \forall \forall \exists.$$

Несооставимые же элементы, к которым относятся, например, элементы $\forall \exists \exists$ и $\exists \forall \forall$, уже не будут описываться тождествами, а только отношением порядка:

$$\forall \exists \exists \vee \exists \forall \forall \Rightarrow \sup(\forall \exists \exists, \exists \forall \forall), \quad \inf(\forall \exists \exists, \exists \forall \forall) \Rightarrow \forall \exists \exists \wedge \exists \forall \forall.$$

Так как

$$\sup(\forall \exists \exists, \exists \forall \forall) = \exists \exists \exists, \quad \inf(\forall \exists \exists, \exists \forall \forall) = \forall \forall \forall,$$

в логике предикатов будут возникать совершенно специфические клаузы, не сводящиеся к аксиоме порядка, типа

$$\forall \exists \exists \vee \exists \forall \forall \Rightarrow \exists \exists \exists, \quad \forall \forall \forall \Rightarrow \forall \exists \exists \wedge \exists \forall \forall.$$

Рассматривая булеаны, нельзя не упомянуть о *законе четырехполюсника*. Действие его продемонстрируем сначала на числовом булеане делителей числа 30 (см. рис. 1.23). Если наибольший общий делитель (НОД) двух чисел a и b обозначить конъюнкцией ($a \wedge b$), а наименьшее общее кратное (НОК) — через дизъюнкцию ($a \vee b$), то в отношении этих двух арифметических понятий будут действовать все четыре закона булевой логики. Убедимся в справедливости закона дистрибутивности:

$$(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c);$$

при $a=6$, $b=10$ и $c=5$ получим: $(6 \wedge 10) \vee 5 = (6 \vee 5) \wedge (10 \vee 5)$, или $2 \vee 5 = 30 \wedge 10$, или $10 = 10$. Но из арифметики известен закон: произведение любых двух чисел равно произведению их НОД и НОК: $a \cdot b = (a \vee b) \cdot (a \wedge b)$. В частности, $6 \cdot 10 = (6 \vee 10) \cdot (6 \wedge 10) = 30 \cdot 2$.

Этот арифметический закон является прямым следствием булеановой структуры делителей чисел. Подобный закон имеет место в любом булеане (хотя смысл операций в нем может существенно меняться) и называется он *законом четырехполюсника*. Четыре полюса, соответствующие числам 6, 10, 2 и 30, взятые на булеане подмножеств (рис. 1.22), связаны соотношением:

$$\{a, b\} \oplus \{a, c\} = \{\{a, b\} \cup \{a, c\}\} \oplus \{\{a, b\} \cap \{a, c\}\}.$$

Под символом $\oplus$ понимается *прямое сложение множеств*, при котором повторяющиеся элементы не удаляются. В результате получим:

$$\{a, b, a, c\} = \{a, b, c\} \oplus \{a\}.$$

Закон четырехполюсника выполняется и для 0,1-векторов (рис. 1.21). Роль прямого сложения здесь заменяется на обыкновенное сложение единиц:

$$(111) + (001) = ((011) \vee (101)) + ((011) \wedge (101)); \quad 3 + 1 = 4.$$

Число единиц в 0,1-векторе a будем называть его *модулем* или *длиной* и обозначать $|a|$. Из табл. 1.25 и табл. 1.26 выпишем в символической форме модули *предикатных векторов*:

$$|P(a)| = |P(b)| = 2, \quad |\exists| = 3, \quad |\forall| = 1;$$

$$|P(k, m)| = 8, \quad |\exists\exists| = 15, \quad |\forall\exists| = 9, \quad |\exists\forall| = 7, \quad |\forall\forall| = 1.$$

Нетрудно убедиться в справедливости закона четырехполюсника для двухмерного предикатного булеана:

$$|\exists\exists| + |\forall\forall| = |\forall\exists \vee \exists\forall| + |\forall\forall \wedge \exists\exists|; \quad 15 + 1 = 11 + 5 = 16.$$

Таблица истинности для трехместных предикатов будет уже состоять из 256 строк. Чтобы определить модули 0,1-векторов кванторного булеана, таблицу истинности можно и не строить, но провести тщательный комбинаторный анализ. В итоге получим:

$$|\exists\forall\forall| = 31, \quad |\forall\exists\forall| = 49, \quad |\forall\forall\exists| = 81,$$

$$|\exists\exists\forall| = 175, \quad |\forall\forall\exists| = 207, \quad |\forall\forall\exists| = 225,$$

$$|\forall\forall\forall| = 1, \quad |\exists\exists\exists| = 255, \quad |P(k, m, n)| = 128.$$

Кванторный булеан 3-го порядка наложен на векторный булеан 256-го порядка, причем его нижняя точка совпадает не с нулевым вектором, а с вектором первого уровня (00...01), верхняя же точка лежит на предпоследнем уровне (01...11). Таким образом, кванторный булеан оказывается немного развернутым относительно векторного булеана. Тем не менее, закон четырехполюсника для него тоже выполняется, в частности:

$$|\forall\forall\forall| + |\forall\exists\forall| = |\forall\forall\exists \vee \forall\exists\forall| + |\forall\forall\exists \wedge \forall\exists\forall|;$$

$$81 + 49 = 105 + 25 = 130.$$

Вообще, величина модуля вектора a является важной *собственной* характеристикой клауз, например:

$$|\forall\forall\forall| \rightarrow |\forall\forall\forall \vee \exists\exists\forall|, \quad 31 \rightarrow 151;$$

$$\forall\forall\forall \vee \forall\exists\forall \rightarrow |\forall\exists\exists|, \quad 105 \rightarrow 225$$

и тождеств, например: 57-57 для закона дистрибутивности:

$$(\forall\forall\forall \wedge \exists\exists\forall) \vee \forall\exists\forall = ((\forall\forall\forall \vee \forall\exists\forall) \wedge (\exists\exists\forall \vee \forall\exists\forall)).$$

С помощью модулей можно осуществлять частичную проверку правильности логических действий, хотя в случае многоместных предикатов для такого контроля понадобится уже компьютер, поскольку величина модулей даже для четырехместных предикатов исчисляется сотнями тысяч:

$$|\forall\exists\exists\exists| + |\forall\forall\exists\exists| = 65\,025 + 63\,135 = 128\,160.$$

Основной задачей логики предикатов является установление истинности предикатных тождеств и клауз. Обозначим через P_i какой-либо предикат с произвольным числом аргументов, а через q_i соответствующую ему кванторную группу. Тогда, например, закон дистрибутивности примет вид:

$$q_1 P_1 \vee (q_2 P_2 \wedge q_3 P_3) = (q_1 P_1 \vee q_2 P_2) \wedge (q_1 P_1 \vee q_3 P_3).$$

В том, что он выполняется для одноместных предикатов, можно убедиться через процедуру конкретизации, к которой мы уже не раз прибегали:

$$x = a, b; \quad q_1 = \forall x, \quad P_1 = A(x);$$

$$y = c, d; \quad q_2 = \exists y, \quad P_2 = B(y);$$

$$z = e, f; \quad q_3 = \forall z, \quad P_3 = C(z).$$

$$[A(a) \wedge A(b)] \vee ([B(c) \vee B(d)] \wedge [C(e) \wedge C(f)]) =$$

$$= ([A(a) \wedge A(b)] \vee [B(c) \vee B(d)]) \wedge ([A(a) \wedge A(b)] \vee [C(e) \wedge C(f)]).$$

От того, что в квадратных скобках появится вместо дизъюнкции конъюнкция и наоборот, а также вместо одноместных предикатов будут фигурировать различные многоместные предикаты — суть тождества не изменится. Оно останется истинным в силу справедливости законов логики множеств и *принципа суперпозиции*, который гласит: замена какой-либо константы другой константой или даже группой констант не может повлиять на истинность тождества. Именно отсюда проистекает наша уверенность в справедливости законов логики множеств и по отношению к предикатам.

Те же самые рассуждения могут быть проведены и в отношении логики высказываний. Она отличается от логики Буля *аксиомой порядка* —

$$q_1 P_1 : q_2 P_2 \Rightarrow q_1 P_1.$$

Процедура конкретизации сводит предикатную аксиому порядка к простому высказыванию, так что если клауза верна для высказываний, она будет справедлива и для предикатов.

Как показывает практика, много ошибок приходится на неправильное обозначение предикатов при их, в принципе, правильной идентификации. Следует помнить, что положительный предикат должен иметь больше единиц, чем отрицательный. Будет допущена ошибка, если противоречие

$$A_1, A_2 \Rightarrow 0 \quad \text{записать как } A_2, \bar{A}_1 \Rightarrow 0.$$

Перейдем к анализу конкретных предикатных выражений.

Пример 1. Пусть дано следующее тождество:

$$(\exists x \forall y \bar{P}(x, y) \vee \exists u \forall v P(v, u)) \wedge (\forall v \exists u P(v, u) \wedge$$

$$\wedge \exists y \forall x P(x, y)) = \exists x \forall y P(y, x) \wedge \forall u \exists v P(u, v).$$

Здесь можно ввести следующие обозначения:

$$A = \forall x \exists y P(x, y) = \forall v \exists u P(v, u) = \forall u \exists v P(u, v),$$

$$B = \exists u \forall v P(v, u) = \exists y \forall x P(x, y) = \exists x \forall y P(y, x).$$

В этих обозначениях тождество выглядит следующим образом:

$$(\bar{A} \vee B) \wedge (A \wedge B) = B \wedge A.$$

Производя элементарные преобразования, мы можем убедиться в справедливости последнего равенства. Следовательно, и исходное тождество составлено верно.

Пример 2. Пусть дана предикатная клауза:

$$\begin{aligned} & \forall x \exists y P(x, y) \rightarrow \forall v P(a, v), \forall x P(a, x) \rightarrow \\ & \rightarrow \exists x \forall y P(y, x) \Rightarrow \forall u \exists v P(u, v) \rightarrow \exists v \forall u P(u, v). \end{aligned}$$

Введем обозначения:

$$\begin{aligned} A &= \forall x \exists y P(x, y) = \forall u \exists v P(u, v), \quad B = \forall v P(a, v) = \forall x P(a, x), \\ C &= \exists x \forall y P(y, x) = \exists v \forall u P(u, v). \end{aligned}$$

Получим:

$$A \rightarrow B, B \rightarrow C \Rightarrow A \rightarrow C.$$

Как известно, формула транзитивности верна, следовательно, и предикатная клауза тоже верна.

Итак, доказательство справедливости первых двух предикатных выражений свелось к простой процедуре *идентификации* их с соответствующими выражениями, существующими в логике Буля и логике высказываний. Рассмотрим более сложные примеры.

Пример 3. Доказать истинность клаузы:

$$\forall v \exists u P(u, v) \rightarrow \forall u \forall v P(u, v), \quad \exists x \forall y P(x, y) \Rightarrow \forall u P(u, u).$$

Введем обозначения:

$$A_1 = \exists x \forall y P(x, y), \quad A_2 = \forall v \exists u P(u, v), \quad B_1 = \forall u \forall v P(u, v), \quad B_2 = \forall u P(u, u).$$

В этих обозначениях клауза будет иметь вид:

$$A_2 \rightarrow B_1, A_1 \Rightarrow B_2 \quad \text{или} \quad \bar{A}_2 \vee B_1, A_1, \bar{B}_2 \Rightarrow 0.$$

По методу резолюций противоречие возможно, если возможны два других противоречия —

$$A_1, \bar{A}_2 \Rightarrow 0, \quad B_1, \bar{B}_2 \Rightarrow 0.$$

Список из восемнадцати клауз (см. п. 1.9), который мы вывели из табл. 1.26, предоставляет нам две истинных клаузы под номерами 6 и 7. Если их представить в форме противоречия, то они будут полностью отвечать последним двум выражениям:

$$\exists x \forall y P(x, y), \bar{\forall y \exists x P(x, y)} \Rightarrow 0, \quad \forall x \forall y P(x, y), \bar{\forall x P(x, x)} \Rightarrow 0.$$

Таким образом, истинность исходной клаузы можно считать установленной.

Пример 4. Доказать истинность клаузы:

$$\begin{aligned} & \forall z B(z, z) \rightarrow \exists x \bar{\exists y} B(x, y), \quad \exists z \forall y \bar{A}(z, y) \rightarrow \forall u \forall v B(v, u), \quad \exists x A(b, x) \rightarrow \\ & \rightarrow \exists z \exists x \bar{B}(x, z) \wedge \exists z \forall y \bar{A}(z, y). \end{aligned}$$

Процедура идентификации приводит к следующим выкладкам:

$$A_1 = \forall z \exists y A(z, y), \quad A_2 = \exists x A(b, x), \quad B_1 = \forall u \forall v B(v, u) = \forall z \forall x B(x, z),$$

$$\begin{aligned}
B_2 &= \forall z B(z, z), B_3 = \forall x \exists y B(x, y); \\
B_2 &\rightarrow \bar{B}_3, \bar{A}_1 \rightarrow B_1, \bar{A}_2 \Rightarrow \bar{B}_1 \wedge \bar{A}_1; \bar{B}_2 \vee \bar{B}_3, A_1 \vee B_1, \bar{A}_2 \Rightarrow 0, \\
A_1, \bar{A}_2 &\rightarrow 0, \quad \forall x \exists y A(x, y), \exists y A(k, y) \rightarrow 0, \\
B_1, \bar{B}_2 &= 0, \quad \forall x \forall y B(x, y), \forall x B(x, x) \Rightarrow 0, \\
B_1, \bar{B}_3 &\Rightarrow 0, \quad \forall x \forall y B(x, y), \forall x \exists y B(x, y) \Rightarrow 0.
\end{aligned}$$

Отсюда следует истинность исходной клаузы.

Пример 5. Докажем справедливость клаузы:

$$\begin{aligned}
&\forall x \exists y A(x, y) \vee \exists y \forall x B(x, y) \vee \forall u \forall v \forall w C(u, v, w), \forall y \exists x A(y, x) \rightarrow \\
&\rightarrow \forall x \forall y C(x, y, b), \exists x \forall y B(y, x) \rightarrow \forall u \forall v C(u, v, a) \rightarrow \\
&\Rightarrow \forall x \exists y \exists z C(x, z, y) \wedge \exists u \forall v \exists w C(u, v, w).
\end{aligned}$$

Доказательство:

$$\begin{aligned}
A &= \forall x \exists y A(x, y) = \forall y \exists x A(y, x), \quad B = \exists y \forall x B(x, y) = \exists x \forall y B(y, x), \\
C' &= \forall x \exists y \exists z C(x, z, y), \quad C'' = \exists u \forall v \exists w C(u, v, w), \\
C_1 &= \forall u \forall v C(u, v, a), \quad C_2 = \forall x \forall y C(x, y, b), \quad C_3 = \forall u \forall v \forall w C(u, v, w). \\
A \vee B \vee C_3, \bar{A} \vee C_2, \bar{B} \vee C_1 &\Rightarrow C' \wedge C''.
\end{aligned}$$

Воспользуемся свойством булсана:

$$C = \forall x \forall y \exists z C(x, y, z) = \inf(C', C'') \Rightarrow C' \wedge C''.$$

Тогда соответствующие противоречия для компенсации C_1 , C_2 и C_3 будут удовлетворены элементом C :

$$C_1, \bar{C} \Rightarrow 0, \quad C_2, \bar{C} \Rightarrow 0, \quad C_3, \bar{C} \Rightarrow 0.$$

После использования этого математического приема доказательство исходной клаузы становится очевидным.

Пример 6. Доказать истинность клаузы:

$$\begin{aligned}
&\forall x \forall y \bar{A}(x, y, c) \vee \forall y \exists z \bar{A}(a, y, z), \exists y A(a, y, c) \vee \exists z \bar{A}(b, a, z), \\
&\forall x \forall z A(x, a, z) \vee \forall y \forall z A(b, y, z) \Rightarrow \forall x \forall z A(x, b, z).
\end{aligned}$$

Доказательство:

$$\begin{aligned}
A' &= \forall x \forall y \bar{A}(x, y, c), \quad B' = \forall x \forall z A(x, a, z), \quad \bar{A}'' = \forall y \forall z \bar{A}(a, y, z), \\
B'' &= \forall y \forall z A(b, y, z), \quad A = \exists y A(a, y, c) = \inf(A', A''), \\
\bar{B} &= \exists z \bar{A}(b, a, z) = \sup(B', B''), \quad C = \forall x \forall z A(x, b, z); \\
\bar{A}' \vee \bar{A}'', \inf(A', A'') \vee \sup(B', B''), B' \vee B'' &\Rightarrow C.
\end{aligned}$$

Инфимум, супремум, верхняя и нижняя грани здесь частично конкретизированы; элемент C не влияет на истинность исходной клаузы. Продолжить доказательство клаузы далее уже не составит большого труда.

Пример 7. Любая семантика логики высказываний может быть выражена в предикатной форме. В качестве примера возьмем легенду из п. 1.6.

Для нее введем следующие предикаты:

$A(x)$ — x говорит правду,

$B(x, y)$ — x находится внутри помещения y ,

$C(x, z)$ — x способен слышать звуки z .

Область определения переменных:

$x = \{a, b\}$, где a — кассир, b — водитель;

$y = \{c, \dots\}$, где c — комната отдыха;

$z = \{d, \dots\}$, где d — звуки выстрелов.

Содержание посылок и заключений следователя раскрыто в п. 1.6; здесь же приведем только их предикатную запись и необходимые разъяснения:

$$P_1 = A(a) \rightarrow B(b, c), \quad P_2 = B(b, c) \rightarrow \forall z C(b, z),$$

$$P_3 = \forall z C(b, z) \rightarrow C(b, d), \quad P_4 = A(b) \rightarrow \bar{C}(b, d).$$

В предикатной форме посылка P_3 является тавтологией, так как квантор существования можно расписать:

$$P_3 = \exists z \bar{C}(b, z) \vee C(b, d) \rightarrow \bar{C}(b, d) \vee \dots \vee C(b, d) = 1.$$

Тавтология не влияет на процедуру установления истинности клаузы и поэтому может быть удалена из перечня посылок, что мы и сделаем. Использование кванторов позволяет также несколько иначе проинтерпретировать заключение C_1 : «не все x говорят правду» или «существует x , который говорит ложь» —

$$C_1 = A(a) \rightarrow \bar{A}(b) = \bar{A}(a) \vee \bar{A}(b) = \exists x \bar{A}(x) = \forall x A(x).$$

Ложное второе следствие C_2 тоже может быть записано через кванторы двумя эквивалентными способами: «все x говорят правду» или «нет ни одного x , который бы обманывал» —

$$C_2 = A(a) \wedge A(b) = \forall x A(x) = \bar{\exists x \bar{A}(x)}.$$

Формальная запись всей легенды без P_3 и с заключением C_1 будет:

$$A(a) \rightarrow B(b, c), B(b, c) \rightarrow \forall z C(b, z), A(b) \rightarrow \bar{C}(b, d) \rightarrow \exists x \bar{A}(x).$$

Истинность ее установим методом резолюций:

$$\bar{A}(a) \vee B(b, c), \bar{B}(b, c) \vee \forall z C(b, z), \bar{A}(b) \vee \bar{C}(b, d), \forall x A(x) \Rightarrow 0.$$

Это противоречие имеет место, так как все клаузы, отвечающие необходимым склейкам, истинны:

$$B(b, c) \Rightarrow B(b, c), \forall z C(b, z) \Rightarrow C(b, d), \forall x A(x) \Rightarrow A(a), \forall x A(x) \Rightarrow A(b).$$

Пример 8. Дана следующая простая легенда:

Если Иван повсюду ходит за Петром, а Петр находится в институте, то где же будет находиться Иван?

$$P(x, y) \text{ — «} x \text{ находится там, где } y \text{»}$$

Составим клаузу:

$$\forall z (P(\text{Петр}, z) \rightarrow P(\text{Иван}, z)), P(\text{Петр}, \text{институт}) \Rightarrow \exists z (P(\text{Иван}, z)).$$

По существу, здесь доказывается следующее предложение: существует ли такое место z , где находился бы Иван. Преобразуем исходную клаузу в противоречие:

$$\bar{P}(\text{Петр}, z) \vee P(\text{Иван}, z), P(\text{Петр}, \text{институт}), \bar{P}(\text{Иван}, z) \Rightarrow 0.$$

Здесь и ниже кванторы общности мы будем опускать, поскольку кванторы существования отсутствуют. Доказательство клаузы оформим в виде дерева (рис. 1.26).

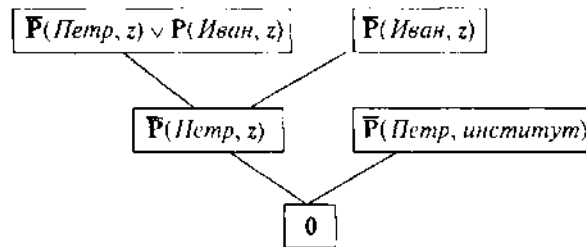


Рис. 1.26

При конкретизации $z = \text{институт}$, доказываем, что действительно существует такое место z , в котором мог бы находиться Иван.

Однако метод резолюций можно модифицировать так, чтобы итогом доказательства был бы не ноль, а непосредственно ответ в предикатной форме: *Иван находится в институте*. Этого можно достичь, если к тому, что требуется доказать, прибавить через дизъюнкцию противоположное утверждение, образовав таким образом тавтологию:

$$\bar{P}(\text{Иван}, z) \vee P(\text{Иван}, z).$$

Тогда дерево логического вывода будет выглядеть так, как это показано на рис. 1.27.

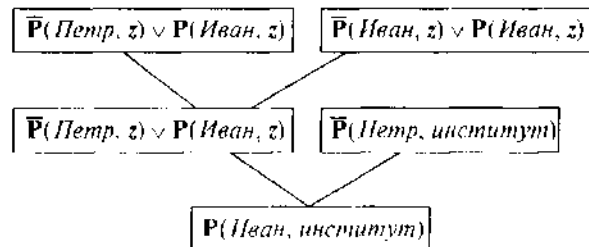


Рис. 1.27

Большинство задач с использованием предикатов носит *поисковый* характер. Поисковые задачи реализуются средствами языка логического программирования — ПРОЛОГ. Остановимся на основных структурных и функциональных элементах этого языка.

Поскольку логика высказываний имеет дело с любыми правильно построенными предложениями, существует серьезная опасность смещения объектных и субъектных предложений, а также предложений, взятых с различных иерархических уровней предметной области логики высказываний. Чтобы избежать указанной опасности, доказываемую задачу оформляют в виде отчетливой *структуры древовидной формы*. В качестве корня дерева выбирается некая *цель* S , истинность которой необходимо установить. Она всегда фигурирует в качестве заголовка *правила*, которое представляет собой *хорновскую клаузу*. Эти клаузы в данном случае удобно записать в обратном порядке:

$$S \leftarrow B_1, B_2, \dots$$

Каждая из посылок B_i представляет собой подцель основной цели C и зависит, в свою очередь, от других правил A_{ij} :

$$B_1 \leftarrow A_{11}, A_{12}, \dots, B_2 \leftarrow A_{21}, A_{22}, \dots$$

Впрочем, в роли посылок B_i могут выступать не клаузы, а элементарные высказывания — *факты*. Далее посылки A_{ij} опять могут быть либо заголовками новых правил, либо фактами. Так образуется *иерархическая структура древовидной формы*. В логических деревьях уже не возникает описанных выше парадоксов.

В ПРОЛОГе реализована *процедура унификации*, с помощью которой производится сравнение *цели* с *правилами*, а *правила* сопоставляются с *фактами*. В результате унификации переменным присваиваются конкретные значения так, что предикат цели становится истинным фактом в случае положительного исхода. Чтобы понять, как осуществляется унификация, разберем конкретный пример программы.

Пример 9. Имеется следующая легенда:

Ивана интересуют компьютеры, книги и автомобили. Петра интересует нечто, что интересует Ивана, но если это нечто является техникой и если это произведено в России. Известно, что компьютеры и автомобили — это техника. Кроме того, известно, что компьютеры производятся в Америке, а автомобили — в Америке и России. Вопрос: «Что интересует Петра?»

Для удобства пользования программой все предикаты и конкретные значения переменных не кодируются отдельными буквами, а приводятся непосредственно в словах, передающих их семантику. Мы, однако, слева от текста программы приведем символичные выражения, чтобы далее у нас была возможность продемонстрировать в аналитической форме *метод резолюций*, который лежит в основе функционирования ПРОЛОГа. Будем помнить также, что все склейки осуществляются с квантором общности, хотя сам квантор не указывается.

Программа:

1) <i>интерес (Иван, компьютеры).</i>	$A(i, a)$
2) <i>интерес (Иван, книги).</i>	$A(i, b)$
3) <i>интерес (Иван, автомобили).</i>	$A(i, c)$
4) <i>интерес (Петр, x) $\leftarrow$</i>	$A(p, x)$
5) $\leftarrow$ <i>интерес (Иван, x),</i>	$A(i, x)$
6) <i>техника (x),</i>	$T(x)$
7) <i>произведено (x, Россия).</i>	$P(x, r)$
8) <i>техника (компьютеры).</i>	$T(a)$
9) <i>техника (автомобили).</i>	$T(c)$
10) <i>произведено (компьютеры, Америка).</i>	$P(a, s)$
11) <i>произведено (автомобили, Америка).</i>	$P(c, s)$
12) <i>произведено (автомобили, Россия).</i>	$P(c, r)$
Цель: 13) <i>интерес (Петр, x).</i>	$A(p, x)$

Данная программа позволяет составить следующее противоречие, которое может быть разрешено в рамках метода резолюций:

$$A(i, a), A(i, b), A(i, c), T(a), T(c), A(p, x) \vee \bar{A}(i, x) \vee \\ \vee \bar{T}(x) \vee \bar{P}(x, r), P(a, s), P(c, s), P(c, r), \bar{A}(p, x) \Rightarrow 0.$$

Ноль можно получить только в том случае, если $x = c$. Тогда

$$A(p, c) \vee A(i, c) \vee \bar{T}(c) \vee \bar{P}(c, r)$$

нейтрализуется предикатами под номерами 3, 9, 12 и 13. Поиск нужного значения x как раз и осуществляется через процедуру унификации, которую можно отследить путем трассировки программы. *Трассировка* — это пошаговое протоколирование процесса выполнения программы. Приведем трассировку нашей программы:

1. В: цель () — 13,
2. В: интерес (Петр, _) — 1,
3. П: интерес (Петр, _) — 2,
4. П: интерес (Петр, _) — 3,
5. У: интерес (Петр, _) — 4,
6. В: интерес (Иван, _) — 5,
7. У: интерес (Иван, компьютеры) — 1 у,
8. В: техника (компьютеры) — 6,
9. У: техника (компьютеры) — 8,
10. В: произведено (компьютеры, Россия) — 7,
11. П: произведено (компьютеры, Россия) — 10,
12. П: произведено (компьютеры, Россия) — 11,
13. Н: произведено (компьютеры, Россия) — 12,
14. П: интерес (Иван, _) — 5,
15. У: интерес (Иван, книги) — 2 у,
16. В: техника (книги) — 6,
17. П: техника (книги) — 8,
18. Н: техника (книги) — 9,
19. П: интерес (Иван, _) — 5,
20. У: интерес (Иван, автомобили) — 3,
21. В: техника (автомобили) — 6,
22. П: техника (автомобили) — 8,
23. У: техника (автомобили) — 9,
24. В: произведено (автомобили, Россия) — 7,
25. П: произведено (автомобили, Россия) — 10,
26. П: произведено (автомобили, Россия) — 11,
27. У: произведено (автомобили, Россия) — 12,
28. У: цель () — 13.

Здесь использованы следующие обозначения: В — вызов нового предиката; П — повторный вызов предиката; У — успешное завершение процедуры унификации, т.е. вызванный предикат отвечает какому-либо факту; Н — неуспешное завершение унификации; у — указатель, который говорит о том, что существует по крайней мере еще один факт с подходящей унификацией. Символ подчеркивания на месте x называется *анонимной переменной* и полностью заменяет x при трассировке программы. Строка трассировки заканчивается числом, отвечающим номеру листинга программы.

Для того чтобы ответить на вопрос «Что интересует Петра?» или в предикатной форме — *интерес (Петр, x)*, ПРОЛОГ-система ищет факты и заголовки правил, сопоставимые с целью. Поиск всегда начинается с первой строки программы. Первые три факта несопоставимы с целью; далее следует правило, заголовок которого заменяется на три подцели. В строке 6 вызывается первая подцель. Затем ПРОЛОГ-система возвращается в начало программы, где ее ожидает «успех». Выставляется указатель «у», к которому система вернется в случае «неуспеха», который может появиться в другом месте программы. В строке 8 производится вызов второй подцели — *техника (компьютеры)*, для которой тут же находится подходящий факт (строка 9). Однако для третьей подцели — *произведено (компьютеры, Россия)* — нужного факта не находится (строка 13). Тогда переменная x освобождается от своей прежней конкретизации (*компьютеры*) и принимает новое значение — *книги*. Эта конкретизация не удовлетворяет вторую подцель (строка 18). Переменная вновь освобождается и принимает значение *автомобили*. При этой конкретизации удовлетворены все три подцели, следовательно, и поиск ответа на основной вопрос заканчивается «успехом»: Петра интересуют автомобили, т.е. *интерес (Петр, автомобили)* является тем конкретизированным предикатом, при котором обеспечена истинность всей клаузы.

Граф поиска ответа, сформулированного в виде цели *интерес (Петр, x)*, представлен рис. 1.28. Бинарное дерево получилось в итоге подстановок предметных констант на место переменных, правила заменялись фактами, а цель — подцелями. Трассировка показывает, что ПРОЛОГ-система не сразу вышла на это дерево склеек. В пунктах 7, 9 и 15 протокола трассировки также производились склейки, но они привели к «неуспеху». Скорейшее достижение цели зависит от правильного выбора стратегии поиска и искусства программирования.

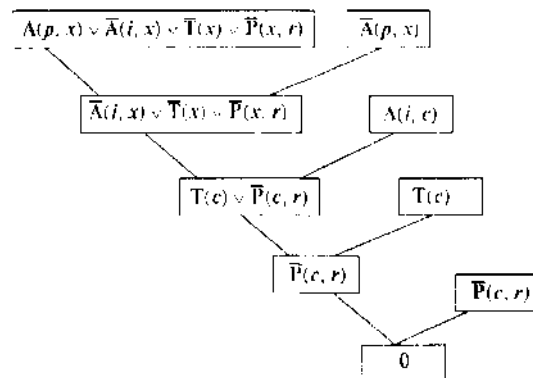


Рис. 1.28

1.11. Задания на практическую работу по логике предикатов

1) Установить истинность логического выражения своего варианта путем конкретизации.

1. $\forall x \forall y P(x, y) \Rightarrow \exists x \exists y P(x, y)$.
2. $\forall x \exists y (A(y) \vee B(x)) = \exists x A(x) \vee \forall x B(x)$.
3. $\exists x (B(x) \wedge A) \rightarrow \exists x B(x) \wedge A$.
4. $\exists x (A(x) \rightarrow B) = \forall x A(x) \rightarrow B$.
5. $\forall x \forall y P(x, y) \rightarrow \forall x P(x, x)$.
6. $\exists x (A(x) \vee B(x)) = \exists x A(x) \vee \exists x B(x)$.
7. $\exists x A(x) \rightarrow \forall x B(x) \rightarrow \forall x (A(x) \rightarrow B(x))$.
8. $\forall x (A(x) \rightarrow B) = \exists x A(x) \rightarrow B$.
9. $\forall x \forall y (A(x) \rightarrow B(y)) = \exists x A(x) \rightarrow \forall x B(x)$.
10. $\exists x (A(x) \rightarrow B(x)) = \forall x A(x) \rightarrow \exists x B(x)$.
11. $\forall x A(x) \vee \forall x B(x) \Rightarrow \forall x (A(x) \vee B(x))$.
12. $\exists x A(x) \vee \forall x B(x) = \exists x \forall y (A(x) \vee B(y))$.
13. $\exists x (A \rightarrow B(x)) = A \rightarrow \exists x B(x)$.
14. $\forall x \forall y P(x, y) \Rightarrow \forall x \exists y P(x, y)$.
15. $\exists x \forall y P(x, y) \rightarrow \exists x \exists y P(x, y)$.
16. $\forall x \exists y P(x, y) \Rightarrow \exists x \exists y P(x, y)$.
17. $\exists x \forall y (A(x) \vee B(y)) = \forall y \exists x (A(x) \vee B(y))$.
18. $\forall y P(a, y) \rightarrow \forall y \exists x P(x, y)$.
19. $\exists x \forall y P(x, y) \rightarrow \exists x P(x, b)$.
20. $\forall x (A \vee B(x)) = A \vee \forall x B(x)$.
21. $\forall x A(x) \vee \forall x B(x) = \forall x \forall y (A(x) \vee B(y))$.
22. $\exists x A(x) \rightarrow \forall x B(x) = \forall x \forall y (A(x) \rightarrow B(y))$.
23. $\forall x (A \rightarrow B(x)) = A \rightarrow \forall x B(x)$.
24. $\exists x P(x, x) \Rightarrow \exists x \exists y P(x, y)$.
25. $\forall x P(x, b) \rightarrow \exists y \forall x P(x, y)$.

2) Доказать истинность предикатных клаузов методом резолюций.

1. $\forall z B(b, z, z) \vee \exists y \bar{A}(b, y, b), \forall u B(a, u, a) \vee \forall y \forall z A(y, y, z) \Rightarrow$
 $\Rightarrow \exists w B(w, c, w) \wedge \exists u A(u, u, u); \exists w \forall u B(b, u, w) \wedge \exists z \forall x B(x, c, z).$
2. $\exists x \forall z B(x, b, z) \rightarrow \forall w A(w, b, w), \exists x \forall z A(x, z, z) \vee \forall x B(a, x, x) \vee \forall u A(a, b, u) \Rightarrow$
 $\rightarrow \exists y \forall w A(y, b, w); \exists u \forall v B(u, v, v) \wedge \exists u A(a, u, c) \wedge \forall u \exists z B(u, b, z) \wedge \exists x \forall z A(x, b, z).$
3. $\forall y \exists z B(y, c, z), \forall x \exists y A(x, y, y) \vee \forall x B(b, x, a) \vee \exists x \forall w A(x, c, w) \vee \forall u \exists w B(u, c, w) \Rightarrow$
 $\Rightarrow \exists z B(z, c, z) \wedge \forall u \exists w A(u, c, w); \forall u \exists w B(u, w, w) \wedge \exists u A(b, u, u) \wedge \exists x B(b, c, x).$

4. $\forall x \exists z B(x, z, a), \forall u \exists w A(u, w, w) \vee \exists z \forall w B(w, z, z) \vee \exists z \forall x A(x, c, z) \rightarrow$
 $\Rightarrow \forall x \exists w A(x, x, w) \wedge \forall u \exists v B(u, v, b); \exists v \exists w B(b, v, w) \wedge \exists z A(b, z, z) \wedge \exists v \forall u B(u, v, a).$
5. $\forall x \forall z A(x, x, z), \exists x \exists y B(x, x, y) \rightarrow \forall z A(z, b, z) \Rightarrow$
 $\Rightarrow \exists u \exists v A(u, v, v) \wedge \exists z \bar{B}(z, z, z); \forall u \exists v A(a, v, u) \wedge \exists y B(a, y, a) \wedge \exists x A(x, b, c).$
6. $A(b, b, c), \forall v \forall w B(c, v, w), \forall u \bar{B}(u, u, a) \Rightarrow \forall v A(b, v, b) \wedge \exists u B(c, u, u) \wedge$
 $\wedge \exists u \exists x A(u, x, c); \forall x B(x, c, a) \wedge \forall y \forall z A(y, y, z) \wedge \forall y B(c, y, y).$
7. $\forall u \exists w A(b, u, w) \vee B(c, c, c) \vee \exists w \forall u A(u, c, w) \vee \forall w B(b, w, w), \forall w \exists u B(w, u, a) \Rightarrow$
 $\Rightarrow \exists u \bar{A}(u, c, a) \wedge \exists v \exists w B(w, v, w); \exists v \exists w B(b, v, w) \wedge \exists z A(z, c, z) \wedge \exists x \forall y B(y, x, a).$
8. $\forall y \forall z A(a, y, z) \vee \forall v \exists w A(w, v, v), \forall x \forall z B(x, a, z) \vee \forall x B(x, c, a) \Rightarrow$
 $\Rightarrow \exists u \forall z A(u, z, c) \wedge \exists x B(x, x, a); \exists y B(b, y, b) \wedge \exists y \bar{B}(c, y, a).$
9. $\forall z A(z, b, z) \vee \forall x B(x, x, x), \forall z \exists x A(a, x, z) \vee \forall w \exists u A(u, b, w) \Rightarrow$
 $\Rightarrow \exists w A(a, w, w) \wedge \forall y \bar{B}(a, y, a); \exists x A(x, x, c) \wedge \exists v \exists w B(v, v, w).$
10. $\forall y \forall z A(a, y, z) \vee \forall w B(a, w, w) \vee \forall y \exists x A(x, y, c), \exists u \forall z B(u, u, z) \rightarrow \exists x \forall y A(x, y, a) \rightarrow$
 $\rightarrow \exists x \forall z B(x, z, z) \wedge \forall w \exists z A(z, w, w) \wedge \forall w \exists u B(u, b, w); \exists u \forall w A(u, w, c).$
11. $\forall x \forall y B(x, y, y) \vee \forall w \bar{A}(w, w, w), \exists x \forall y B(b, y, x) \vee \forall v A(b, v, b) \vee \forall u B(u, c, a) \rightarrow$
 $\Rightarrow \exists u \exists w B(u, u, w); \forall u \forall v A(u, u, v) \wedge \exists w B(w, c, w).$
12. $\forall y \forall z A(a, y, z) \vee \forall w B(w, b, w) \vee \forall u \exists v A(v, u, c), \exists x B(x, b, c) \rightarrow \forall y \forall z A(z, y, z) \Rightarrow$
 $\Rightarrow \exists z \forall x A(z, x, c); \exists x \forall z B(a, x, z) \wedge A(b, b, b) \wedge \forall z \exists x B(x, b, z) \wedge \exists z A(a, z, z).$
13. $\exists u A(u, b, c) \rightarrow (\exists v \exists w B(v, v, w) \rightarrow \exists v A(b, v, v)), \exists y B(a, y, a) \vee \forall x A(b, x, x) \vee$
 $\vee \forall x \forall u B(x, u, b) \Rightarrow \forall x A(x, x, c) \rightarrow \exists y \exists z A(b, y, z); B(a, a, b).$
14. $\forall w \bar{B}(b, c, w), \forall x \exists z B(x, b, z), \forall z A(a, z, z) \Rightarrow \exists u \bar{B}(u, c, a) \wedge \exists w B(c, b, w) \wedge$
 $\wedge \exists u \forall w \bar{A}(b, u, w); \exists z \forall w A(z, w, z) \wedge \forall u \exists w B(u, w, w) \wedge \exists w A(w, a, w).$
15. $\forall v \bar{A}(a, v, b) \vee \forall v A(c, v, c), \forall u A(u, u, b) \vee \forall x \exists w B(x, w, a) \rightarrow$
 $\rightarrow \exists v \exists w B(b, v, w) \wedge \exists y \forall z B(z, y, y); \exists u \exists w A(u, b, w) \wedge \exists u A(u, a, b).$
16. $\exists x A(x, b, c) \rightarrow (\exists x \forall z B(a, x, z) \rightarrow \forall z A(b, a, z)), \forall w \exists z B(w, z, w) \vee$
 $\vee \exists x \forall z A(x, z, z) \vee \forall z B(z, c, z) \Rightarrow \forall z A(a, b, z) \rightarrow \exists u \forall w A(u, a, w); \exists w B(c, w, w).$
17. $\exists z \forall x \bar{A}(x, b, z), (\forall x \exists z A(z, b, x) \rightarrow \forall x \forall z B(x, a, z)) \rightarrow (\exists u \forall y \bar{A}(y, b, u) \wedge$
 $\wedge \forall x \exists y \forall z B(x, y, z)) \Rightarrow \forall u \exists w \exists v B(u, v, w) \wedge \exists u \exists z \forall v B(z, u, v).$
18. $(\forall u A(u, a, b) \rightarrow \exists z \forall y \exists x \bar{B}(z, y, x)) \rightarrow (\forall u \exists v \forall w B(u, v, w) \vee \forall x \exists y A(x, y, a)),$
 $\exists u \forall v \bar{A}(u, v, a) \Rightarrow \forall u \exists w \exists v B(u, v, w) \wedge \exists x \exists y \forall z B(x, y, z).$
19. $\exists x \forall y \exists z B(x, y, z), \exists u \forall y \forall x A(u, x, y) \vee \forall x \exists z B(x, a, z), \forall z \exists x B(z, a, x) \rightarrow$
 $\rightarrow \forall u \exists v \forall w \bar{B}(u, v, w) \rightarrow \exists u \exists v \forall w A(u, v, w) \wedge \exists v \exists w \forall u A(w, v, u).$
20. $\forall x \exists y A(y, x) \rightarrow \forall x \forall y \exists z B(x, y, z), \exists u \forall v A(u, v) \rightarrow \forall z \forall x \exists y B(x, z, y),$
 $\forall y \exists x A(x, y) \vee \exists v \forall u A(v, u) \Rightarrow \forall y \forall z \exists x B(z, y, x) \wedge \exists y \forall z \exists x B(y, z, x).$
21. $\exists x \forall y \forall z A(x, y, z) \rightarrow A(a, b, c), \forall y \forall z A(b, y, z) \vee \exists x \forall z A(x, a, z).$
 $\exists x \exists y \forall z A(x, y, z) \rightarrow A(a, b, d) \Rightarrow \forall x \exists z A(x, b, z) \wedge \forall y \exists z A(a, y, z).$
22. $\forall x \exists y \exists z A(x, z, y) \vee \exists u \forall v \exists w A(u, v, w) \Rightarrow \exists x \forall z \bar{B}(x, b, z), (\forall u \exists v B(u, b, v) \rightarrow$
 $\rightarrow \exists y \forall x A(a, x, y)) \rightarrow (\forall z \exists x B(z, b, x) \vee \forall u \forall z \exists x A(z, u, x)).$

23. $\forall u \forall v \forall w A(u, v, w) \vee \forall x \exists y B(x, b, y) \vee \forall u \forall v C(u, v, b), \exists x \bar{A}(x, a, b) \vee$
 $\vee \forall y \exists z B(a, y, z) \vee \forall v \forall u C(v, u, a), \forall w B(a, b, w) \Rightarrow$
 $\Rightarrow \forall u \exists v \exists w C(u, v, w) \wedge \exists x \forall y \exists z C(x, y, z).$
24. $\exists u \forall w A(u, a, w) \vee \exists v \forall w A(b, v, w) \Rightarrow \exists v \exists w A(a, v, w) \wedge \forall u \exists w A(u, b, w);$
 $\forall u \exists v \exists w A(u, v, w) \wedge A(b, a, d); A(b, a, c) \wedge \forall u \forall v \exists w A(u, v, w).$
25. $\exists y \forall z B(y, a, z) \rightarrow \forall u \forall v A(b, v, u), \forall u \forall v A(v, u, a) \vee \forall y \exists u \forall z B(u, y, z),$
 $\forall z B(z, z, z) \rightarrow \exists y B(a, y, b) \wedge \exists x \forall y \exists z A(x, y, z); \exists u \forall v \exists w A(u, v, w).$

3) Для легенды вашего варианта (см. п. 1.7, задание 3) введите соответствующие предикаты, составьте предикатную клаузу и докажите ее истинность методом резолюций. Если предикаты для вашей клаузы ввести затруднительно, придумайте новую легенду, для которой введение предикатов и кванторов было бы возможно.

4) Задана ПРОЛОГ-программа «Родственные отношения». Необходимо выполнить трассировку программы отдельно для двух целей, предварительно введя недостающие предикаты и правила. Так как может существовать несколько значений для переменных x и y , удовлетворяющих одной и той же цели, при трассировке допустимо ограничиться одним истинным значением x или y . Кроме того, ввиду большого числа повторных вызовов, разрешается указывать только первую и последнюю строки повторяющихся вызовов, например:

...
 81. В: муж (Феликс) — 85,
 82. П: муж (Феликс) — 1,
 ...
 99. П: муж (Феликс) — 18,
 100. У: муж (Феликс) — 19.

ПРОЛОГ-программа «Родственные отношения»

муж (x) — x мужчина, дочь (x, y) — x дочь y ,
 жен (x) — x женщина, сын (x, y) — x сын y ,
 отец (x, y) — x отец y , род (x, y) — x родитель y ,
 мать (x, y) — x мать y , брат (x, y) — x брат y ,
 сестра (x, y) — x сестра y .

Клаузы:

- | | |
|--------------------|-------------------|
| 1) муж (Николай). | 2) муж (Иван). |
| 3) муж (Степан). | 4) муж (Сергей). |
| 5) муж (Павел). | 6) муж (Игорь). |
| 7) муж (Анатолий). | 8) муж (Иосиф). |
| 9) муж (Роман). | 10) муж (Кирилл). |
| 11) муж (Дмитрий). | 12) муж (Максим). |
| 13) муж (Евгений). | 14) муж (Петр). |
| 15) муж (Ефим). | 16) муж (Юрий). |

- | | |
|--|---|
| 17) <i>муж</i> (Вадим). | 18) <i>муж</i> (Олег). |
| 19) <i>муж</i> (Феликс). | 20) <i>жен</i> (Мария). |
| 21) <i>жен</i> (Ольга). | 22) <i>жен</i> (Татьяна). |
| 23) <i>жен</i> (Жанна). | 24) <i>жен</i> (Ирина). |
| 25) <i>жен</i> (Алиса). | 26) <i>жен</i> (Екатерина). |
| 27) <i>жен</i> (Елена). | 28) <i>жен</i> (Виктория). |
| 29) <i>жен</i> (Полина). | 30) <i>жен</i> (Луиза). |
| 31) <i>жен</i> (Наталья). | 32) <i>жен</i> (Барбара). |
| 33) <i>жен</i> (Белла). | 34) <i>жен</i> (Анна). |
| 35) <i>отец</i> (Николай, Иван). | 36) <i>отец</i> (Степан, Мария). |
| 37) <i>отец</i> (Иван, Ольга). | 38) <i>отец</i> (Иван, Сергей). |
| 39) <i>отец</i> (Иван, Татьяна). | 40) <i>отец</i> (Сергей, Виктория). |
| 41) <i>отец</i> (Павел, Роман). | 42) <i>отец</i> (Сергей, Дмитрий). |
| 43) <i>отец</i> (Иосиф, Ирина). | 44) <i>отец</i> (Ефим, Анатолий). |
| 45) <i>отец</i> (Ефим, Полина). | 46) <i>отец</i> (Юрий, Вадим). |
| 47) <i>отец</i> (Петр, Ефим). | 48) <i>отец</i> (Петр, Юрий). |
| 49) <i>отец</i> (Петр, Анна). | 50) <i>отец</i> (Максим, Петр). |
| 51) <i>отец</i> (Дмитрий, Наталья). | 52) <i>отец</i> (Феликс, Олег). |
| 53) <i>отец</i> (Олег, Евгений). | 54) <i>мать</i> (Алиса, Петр). |
| 55) <i>мать</i> (Екатерина, Елена). | 56) <i>мать</i> (Елена, Ефим). |
| 57) <i>мать</i> (Елена, Юрий). | 58) <i>мать</i> (Елена, Анна). |
| 59) <i>мать</i> (Мария, Ольга). | 60) <i>мать</i> (Анна, Виктория). |
| 61) <i>мать</i> (Луиза, Евгений). | 62) <i>мать</i> (Татьяна, Полина). |
| 63) <i>мать</i> (Мария, Сергей). | 64) <i>мать</i> (Анна, Олег). |
| 65) <i>мать</i> (Татьяна, Анатолий). | 66) <i>мать</i> (Анна, Дмитрий). |
| 67) <i>мать</i> (Виктория, Белла). | 68) <i>мать</i> (Мария, Татьяна). |
| 69) <i>мать</i> (Ольга, Жанна). | 70) <i>мать</i> (Ольга, Павел). |
| 71) <i>мать</i> (Жанна, Ирина). | 72) <i>мать</i> (Ирина, Игорь). |
| 73) <i>мать</i> (Ирина, Кирилл). | 74) <i>мать</i> (Барбара, Роман). |
| 75) $\text{род}(x, y) \leftarrow \text{отец}(x, y)$. | 76) $\text{род}(x, y) \leftarrow \text{мать}(x, y)$. |
| 77) $\text{сын}(x, y) \leftarrow \text{род}(y, x), \text{муж}(x)$. | |
| 78) $\text{дочь}(x, y) \leftarrow \text{род}(y, x), \text{жен}(x)$. | |
| 79) $\text{брат}(x, y) \leftarrow \text{род}(z, x), \text{род}(z, y), \text{муж}(x), x \neq y$. | |
| 80) $\text{сестра}(x, y) \leftarrow \text{род}(z, x), \text{род}(z, y), \text{жен}(x), x \neq y$. | |

Цели:

1. *тесть* (Феликс, у), *племянник* (Павел, у).
2. *тетя* (Анна, у), *внук* (х, Алиса).

3. двоюр. брат (Вадим, у), внучка (х, Сергей).
4. дядя (Ефим, у), свекровь (Мария, у).
5. невестка (х, Максим). внук (х, Анна).
6. племянница (Жанна, у), внук (Роман, у).
7. теща (Елена, у), внучка (Белла, у).
8. теща (Мария, у), свекор (х, Елена).
9. внук (Евгений, у), дядя (Юрий, у).
10. тетя (Гатьяна, у), двоюр. брат (Дмитрий, у).
11. зять (Петр, у), тетя (Ольга, у).
12. свекор (Петр, у), внучка (Полина, у).
13. свекровь (х, Луиза), дядя (Сергей, у).
14. тесть (х, Сергей), двоюр. брат (Вадим, у).
15. теща (х, Сергей), двоюр. сестра (х, Виктория).
16. троюр. сестра (х, Белла), зять (Сергей, у).
17. племянник (Вадим, у), внучка (Ирина, у).
18. невестка (Анна, у), двоюр. сестра (Виктория, у).
19. невестка (Елена, у), племянница (Виктория, у).
20. двоюр. сестра (Жанна, у), племянник (х, Ефим).
21. троюр. сестра (Наталья, у), свекор (Иван, у).
22. тесть (Петр, у), троюр. брат (Роман, у).
23. племянница (х, Сергей), зять (Ефим, у).
24. внучка (х, Мария), двоюр. сестра (Белла, у).
25. двоюр. сестра (х, Полина), зять (х, Петр).

1.12. Разбор решений задач по логике предикатов

1) Установим истинность следующих логических выражений путем конкретизации. Для варианта 10 имеем следующее тождество:

$$\exists x (A(x) \rightarrow B(x)) = \forall x A(x) \rightarrow \exists x B(x).$$

Доказательство:

$$\begin{aligned} \exists x (A(x) \rightarrow B(x)) &= (A(a) \rightarrow B(a)) \vee (A(b) \rightarrow B(b)) = \\ &= \bar{A}(a) \vee B(a) \vee \bar{A}(b) \vee B(b) = (\bar{A}(a) \vee \bar{A}(b)) \vee (B(a) \vee B(b)) = \\ &= \exists x \bar{A}(x) \vee \exists x B(x) = \forall x A(x) \rightarrow \exists x B(x). \end{aligned}$$

Для варианта 19 имеем следующую клаузу:

$$\exists x \forall y P(x, y) \Rightarrow \exists x P(b, x).$$

Для доказательства ее истинности избавимся от кванторов в обеих частях клаузы:

$$\begin{aligned}
& (P(a, a) \wedge P(a, b)) \vee (P(b, a) \wedge P(b, b)) \Rightarrow P(b, a) \vee P(b, b); \\
& P(a, a) \vee P(a, b), P(a, b) \vee P(b, a), P(a, a) \vee P(b, b), P(b, a) \vee P(b, b), \\
& \overline{P(b, a)} \rightarrow P(b, b); \\
& P(a, a) \vee P(a, b), P(a, b) \vee P(b, a), P(a, a) \vee P(b, b), P(b, b) \rightarrow P(b, b).
\end{aligned}$$

Последняя клауза верна в силу аксиомы порядка.

2) Решения для второго задания приведем для всех вариантов. Ответы нетрудно будет отыскать, если знать, каким образом были составлены логические выражения. Замена в соответствии с принципом двойственности предполагает одновременную перестановку местами всех заключений и всех посылок, а также замену обозначений:

$$\begin{aligned}
& \forall \Leftrightarrow \exists, \vee \Leftrightarrow \wedge, \sup \Leftrightarrow \inf, (,) \Leftrightarrow (,); \Lambda \Leftrightarrow B, \\
& a \Leftrightarrow b, b \rightarrow c, c \Rightarrow a, x < y, y \Leftrightarrow v, z \Leftrightarrow w.
\end{aligned}$$

Для варианта 1:

из принципа двойственности по варианту 9.

Для варианта 2:

$$\begin{aligned}
& \overline{B}_3 \vee C_1, A_1 \vee B_1 \Rightarrow A_2; B_2 \wedge C_2, \\
& A_1 = A'_1 \vee A''_1 = \exists x \forall z A(x, z, z) \vee \forall u A(a, b, u), \\
& A_2 = \sup(A'_1, A''_1) = \exists v \forall w A(v, b, w), A_1 \Rightarrow A_2, \\
& B_1 = \inf(B'_2, B''_2) = \forall x B(a, x, x), B_1 \Rightarrow B_2, \\
& B_2 = B'_2 \wedge B''_2 = \exists u \forall v B(u, v, v) \wedge \forall u \exists z B(u, b, z), \\
& B_1 \Rightarrow B_2 = \exists x \forall z B(x, b, z), \\
& C_2 = C'_2 \wedge C''_2 = \exists u A(a, u, c) \wedge \exists x \forall z A(x, b, z), \\
& C_1 = \inf(C'_2, C''_2) = \forall w A(w, b, w).
\end{aligned}$$

Для варианта 3:

из принципа двойственности по варианту 2.

Для варианта 4:

из принципа двойственности по варианту 10.

Для варианта 5:

$$\begin{aligned}
& A_1, B_1 \rightarrow C_1 \Rightarrow A_2 \wedge \overline{B}_1; C'_2 \wedge B_2 \wedge C''_2, \\
& A_1, \overline{B}_3 \vee C_1, \overline{A}_2 \vee B_1, B_2 \vee \overline{C}_2 \Rightarrow 0, \\
& A_1 = \forall x \forall z A(x, x, z), A_2 = \exists u \exists v A(u, v, v), A_1 \Rightarrow A_2, \\
& B_1 = \exists z \overline{B}(z, z, z), B_2 = \exists y B(a, y, a), B_1 \Rightarrow B_2, \\
& B_3 = \exists x \exists y B(x, x, y), B_1 \Rightarrow B_3, \\
& C_1 = \inf(C'_2, C''_2) = \forall z A(z, b, z), C_1 \Rightarrow C_2, \\
& C_2 = C'_2 \wedge C''_2 = \forall u \exists v A(a, v, u) \wedge \exists x A(x, b, c).
\end{aligned}$$

Для варианта 6:

из принципа двойственности по варианту 13.

Для варианта 7:

из принципа двойственности по варианту 12.

Для варианта 8:

$$\begin{aligned} A'_1 \vee A''_1, B_1 \vee C'_1 &\Rightarrow A_2 \wedge C_2; B_2 \wedge C''_1, \\ A'_1 \vee A''_1, B_1 \vee C'_1, \bar{A}_2 \vee \bar{C}_2, \bar{B}_2 \vee C''_1 &\rightarrow 0, A_1 \rightarrow A_2, \\ A_1 = A'_1 \vee A''_1 = \forall y \forall z A(a, y, z) \vee \forall v \exists w A(w, v, v), \\ A_2 = \exists u \forall z A(u, z, c), B_1 = \forall x \forall z B(x, a, z), B_1 &\Rightarrow B_2, \\ B_2 = \exists y B(b, y, b), C'_1 = \forall x B(x, c, a), C'_1 &\Rightarrow C_2, \\ C_2 = \exists x B(x, x, a), C''_1 = \forall y B(c, y, a), C''_1 &\rightarrow C_2. \end{aligned}$$

Для варианта 9:

по клаузе 8 со следующими обозначениями:

$$\begin{aligned} A_1 = A'_1 \vee A''_1 &= \forall z \exists x A(a, x, z) \vee \forall w \exists u A(u, b, w), \\ A_2 = \exists x A(x, x, c), B_1 &= \forall z A(z, b, z), \\ B_2 = \exists w A(a, w, w), C_2 &= \exists v \exists w B(v, v, w), \\ C'_1 = \forall x B(x, x, x), C''_1 &= \exists y B(a, y, a). \end{aligned}$$

Для варианта 10:

$$\begin{aligned} A'_1 \vee B_1 \vee A''_1, B_3 \rightarrow C_1 &\Rightarrow B'_2 \wedge C_2 \wedge B''_2; A_2, \\ A'_1 \vee B_1 \vee A''_1, \bar{B}_3 \vee C_1, \bar{B}'_2 \vee \bar{C}_2 \vee \bar{B}''_2, A_2 &\Rightarrow 0, \\ A_1 = A'_1 \vee A''_1 = \forall y \forall z A(a, y, z) \vee \forall y \exists x A(x, y, c), \\ A_2 = \sup(A'_1, A''_1) = \exists u \forall w A(u, w, c), B_1 = \inf(B'_2, B''_2) &= \forall w B(a, w, w), \\ B_2 = B'_2 \wedge B''_2 = \exists x \forall z B(x, z, z) \wedge \forall w \exists u B(u, b, w), \\ B_3 = \exists u \forall z B(u, u, z), A_1 \rightarrow A_2, B_1 \rightarrow B_2, B_1 \rightarrow B_3, \\ C_1 = \exists x \forall y A(x, y, a), C_2 = \forall w \exists z A(z, w, w), C_1 &\Rightarrow C_2. \end{aligned}$$

Для варианта 11:

из принципа двойственности по варианту 5.

Для варианта 12:

по клаузе 10 со следующими обозначениями:

$$\begin{aligned} A_1 = A'_1, A''_1 = \forall y \forall z A(a, y, z) \vee \forall u \exists v A(v, u, c), \\ A_2 = \exists z \forall x A(z, x, c), B_1 = \forall w B(w, b, w), B_3 = \exists x B(x, b, c), \\ C_1 = \forall y \forall z A(z, y, z), B_2 = B'_2 \wedge B''_2 = \exists x \forall z B(a, x, z) \wedge \forall z \exists x B(x, b, z), \\ C_2 = C'_2 \wedge C''_2 = A(b, b, b) \wedge \exists z A(a, z, z). \end{aligned}$$

Для варианта 13:

$$A_2 \rightarrow (B_2 \rightarrow C'_1), B_1 \vee C''_1 \vee D_1 \rightarrow A_1 \rightarrow C_2; D_2,$$

$$\bar{A}_2 \vee \bar{B}_2 \vee C'_1, B_1 \vee C''_1 \vee D_1, A_1, \bar{C}_2, \bar{D}_2 \rightarrow 0,$$

$$A_1 = \forall x A(x, x, c), \quad A_2 = \exists u A(u, b, c), \quad A_1 \Rightarrow A_2,$$

$$B_1 = \exists y B(a, y, a), \quad B_2 = \exists v \exists w B(v, v, w), \quad B_1 \Rightarrow B_2,$$

$$C'_1 = \exists v A(b, v, v), \quad C''_1 = \forall x A(b, x, x), \quad C_2 = \exists y \exists z A(b, y, z),$$

$$C'_1 \Rightarrow C_2, \quad C''_1 \Rightarrow C_2, \quad D_1 = \forall x \forall u B(x, u, b), \quad D_2 = B(a, a, b), \quad D_1 \Rightarrow D_2.$$

Для варианта 14:

из принципа двойственности по варианту 16.

Для варианта 15:

из принципа двойственности по варианту 8.

Для варианта 16:

по клаузе 13 со следующими обозначениями:

$$A_1 = \forall z A(a, b, z), \quad A_2 = \exists x A(x, b, c), \quad B_1 = \forall w \exists z B(w, z, w),$$

$$B_2 = \exists x \forall z B(a, x, z), \quad C'_1 = \forall z A(b, a, z), \quad C''_1 = \exists x \forall z A(x, z, z),$$

$$C_2 = \exists u \forall w A(u, a, w), \quad D_1 = \forall z B(z, c, z), \quad D_2 = \exists w B(c, w, w).$$

Для варианта 17:

$$\bar{A}, (A \rightarrow C) \rightarrow (\bar{A} \wedge B_1) \Rightarrow B'_2 \wedge B''_2,$$

$$\bar{A}, \bar{B}'_2 \wedge \bar{B}''_2, A \vee B_1, A \vee \bar{C}, \bar{C} \vee B_1 \Rightarrow 0,$$

$$A = \forall x \exists z A(z, b, x) = \forall z \exists x A(x, b, z) = \forall u \exists y A(y, b, u),$$

$$B_1 = \forall x \exists y \forall z B(x, y, z) = \inf(B'_2, B''_2) \rightarrow B'_2 \wedge B''_2 =$$

$$= \forall u \exists w \exists v B(u, v, w) \wedge \exists u \exists z \forall v B(z, u, v), \quad C = \forall x \forall z B(x, a, z).$$

Для варианта 18:

$$(A \rightarrow \bar{B}_1) \rightarrow (B_1 \vee C), \quad \bar{C} \Rightarrow B'_2 \wedge B''_2,$$

$$A = \forall u A(u, a, b), \quad C = \forall x \exists y A(x, y, a),$$

$$B_1 = \inf(B'_2, B''_2) = \forall u \exists v \forall w B(u, v, w) = \forall z \exists y \forall x B(z, y, x) \Rightarrow$$

$$\Rightarrow B'_2 \wedge B''_2 = \forall u \exists w \exists v B(u, v, w) \wedge \exists x \exists y \forall z B(x, y, z).$$

Для варианта 19:

$$\bar{C}, A_1 \vee B, B \rightarrow C \Rightarrow A'_2 \wedge A''_2,$$

$$A_1 = \inf(A'_2, A''_2) = \exists u \forall v \forall x A(u, x, y) \Rightarrow A'_2 \wedge A''_2 =$$

$$= \exists u \exists v \forall w A(u, v, w) \wedge \exists v \exists w \forall u A(w, v, u),$$

$$B = \forall x \exists z B(x, a, z) = \forall z \exists x B(z, a, x),$$

$$C = \forall x \exists y \forall z \bar{B}(x, y, z) = \forall u \exists v \forall w \bar{B}(u, v, w).$$

Для варианта 20:

$$A \rightarrow C_1, B \rightarrow C_1, A \vee B \Rightarrow C'_2 \wedge C''_2,$$

$$A = \forall x \exists y A(y, x) = \forall y \exists x A(x, y), \quad B = \exists u \forall v A(u, v) = \exists v \forall u A(v, u),$$

$$C_1 = \forall x \forall y \exists z B(x, y, z) = \forall z \forall x \exists y B(x, z, y) = \\ = \inf(C'_2, C''_2) \Rightarrow C'_2 \wedge C''_2 = \forall y \forall z \exists x B(z, y, x) \wedge \exists y \forall z \exists x B(y, z, x).$$

Для варианта 21:

$$B_2 \rightarrow A''_1, B_1 \vee C_1, C_2 \rightarrow A'_1 \rightarrow A'_2 \wedge A''_2, \\ A'_1 = A(a, b, c), A''_1 = A(a, b, d), A_1 = \exists z A(a, b, z) = \\ = \inf(A'_2, A''_2) \Rightarrow A'_2 \wedge A''_2 = \forall x \exists z A(x, b, z) \wedge \forall y \exists z A(a, y, z), \\ B_1 = \forall y \forall z A(b, y, z) \Rightarrow \exists x \forall y \forall z A(x, y, z) = B_2, \\ C_1 = \exists x \forall z A(x, a, z) \Rightarrow \exists x \exists y \forall z A(x, y, z) = C_2.$$

Для варианта 22:

$$C' \vee C'' \Rightarrow \bar{B}, (B \rightarrow \bar{A}) \rightarrow (B \vee C), \\ \bar{A} = \exists y \forall x A(a, x, y), C = \forall u \forall z \exists x A(z, u, x) = \sup(C', C''), \\ B = \forall x \exists z B(x, b, z) = \forall u \exists v B(u, b, v) = \forall z \exists x B(z, b, x), \\ \forall x \exists y \exists z A(x, z, y) \vee \exists u \forall v \exists w A(u, v, w) = C' \vee C'' \Rightarrow C.$$

Для варианта 23:

$$A_1 \vee B'_1 \vee C', \bar{A}_2 \vee B''_1 \vee C'', \bar{B}_2 \Rightarrow C_1 \wedge C_2, \\ A_1 \rightarrow A_2, B'_1 \rightarrow B_2, B''_1 \Rightarrow B_2, C' \Rightarrow C, \\ A_1 = \forall u \forall v \forall w A(u, v, w), A_2 = \forall x A(x, a, b), \\ B'_1 = \forall x \exists y B(x, b, y), B''_1 = \forall y \exists z B(a, y, z), \\ B_2 = \exists w B(a, b, w), C' \rightarrow C \Rightarrow C_1 \wedge C_2, C' = \forall u \forall v C(u, v, b), \\ C'' = \forall v \forall u C(v, u, a), C = \forall u \forall v \exists w C(u, v, w), \\ C_1 = \forall u \exists v \exists w C(u, v, w), C_2 = \exists x \forall y \exists z C(x, y, z).$$

Для варианта 24:

из принципа двойственности по варианту 21.

Для варианта 25:

$$B_2 \rightarrow A'_1, A''_1 \vee B_1, D \Rightarrow C \wedge A_2; A_2, \\ A'_1 = \forall u \forall v A(b, v, u), A''_1 = \forall u \forall v A(v, u, a), \\ A_2 = \exists x \forall y \exists z A(x, y, z), A'_1 \Rightarrow A_2, A''_1 \Rightarrow A_2, \\ B_1 = \forall y \exists u \forall z B(u, y, z), B_2 = \exists y \forall z B(y, a, z), B_1 \Rightarrow B_2, \\ C = \exists y B(a, y, b), D = \forall z B(z, z, z), C \wedge A_2; A_2 = A_2.$$

3) Для легенды варианта 2 практического задания п. 1.7 (3) введем следующие предикаты:

$A(x, y, z)$ — « x уважает y по причине z ».

$B(x, y, v)$ — « x дает y материальные средства v ».

$C(x, y, w)$ — « y возвращает x долг, выраженный в w ».

Области определения переменных:

$x = \{a, b, \dots\}$, где a — бизнесмен, b — банкир, ...

$y = \{c, d, \dots\}$, где c — художник, d — скульптор, ...

$z = \{e, f, \dots\}$, где e — жалость, f — мастерство, ...

$v = \{i, j, \dots\}$, где i — деньги, j — помощь в организации выставки, ...

$w = \{g, h, \dots\}$, где g — деньги, h — добрая репутация...

Посылки:

Если некоторый x уважает некоторого u по причине некоторого z , то первый всегда окажет второму конкретную материальную помощь, если имеется определенная вероятность того, что u как-то компенсирует затраты x .

$\exists x \exists y \exists z A(x, y, z) \rightarrow (\exists x \exists y \exists w C(x, y, w) \rightarrow \forall x \forall y \forall v B(x, y, v))$.

Из приведенной легенды следует, что бизнесмен уважает художника за его мастерство:

$A(a, c, f)$.

Понятно также, что бизнесмен будет иметь добрую репутацию мецената за то, что он помог художнику в организации выставки его картин:

$C(a, c, h)$.

Заключение: бизнесмен поможет художнику организовать выставку его картин:

$B(a, c, j)$.

Доказать истинность составленной из этих предикатов клаузы не составит большого труда.

Для легенды варианта 5 практического задания п. 1.7 (3) можно ввести следующие предикаты:

$A(x, y)$ — « x извергает y ».

B — «Высокая урожайность».

$C(z)$ — «Источником блага является z ».

Области:

$x = \{a, b, \dots\}$, где a — вулкан, b — гроза, ...

$y = \{c, d, \dots\}$, где c — пепел, d — вода, ...

$z = \{e, f, \dots\}$, где e — Бог, f — природа, ...

Посылки:

Все x извергают какие-то y : $\forall x \exists y A(x, y)$.

Если некоторые x извергают какие-то y , то будет высокая урожайность:

$\exists x \exists y A(x, y) \rightarrow B$.

Высокая урожайность всегда несет благо людям:

$B \rightarrow \forall z C(z)$.

Заключение: то, что источником блага является Господь Бог, не противоречит исходным посылкам:

$C(e)$.

Доказательство очевидно.

4) Произведем трассировку работы ПРОЛОГ-программы «Родственные отношения» для первой цели *варианта 12*. Для этого имеющуюся программу дополним клаузой:

81) *свекор* (x, y) $\Leftarrow$

82) *отец* (x, z),

83) *отец* (z, u),

84) *мать* (y, u).

Цель: 85) *свекор* (Петр, y).

Трассировка программы:

1. В: *цель* () — 85,

2. В: *свекор* (Петр, $_$) — 81,

3. В: *отец* (Петр, $_$) — 82,

4. П: *отец* (Петр, $_$) — 35,

...

15. П: *отец* (Петр, $_$) — 46,

16. У: *отец* (Петр, Ефим) — 47 у,

17. В: *отец* (Ефим, $_$) — 83,

18. П: *отец* (Ефим, $_$) — 35,

...

26. П: *отец* (Ефим, $_$) — 43,

27. У: *отец* (Ефим, Анатолий) — 44 у,

28. В: *мать* ($_$, Анатолий) — 84,

29. П: *мать* ($_$, Анатолий) — 54,

...

39. П: *мать* ($_$, Анатолий) — 64,

40. У: *мать* (Татьяна, Анатолий) — 65 у,

41. У: *цель* () — 85.

Из соответствующих *фактов* и *правил* составим противоречие:

$\text{свекор}(\text{Петр}, y) \vee \overline{\text{отец}(\text{Петр}, z)} \vee \overline{\text{отец}(z, u)} \vee \overline{\text{мать}(y, u)},$

$\text{отец}(\text{Петр}, \text{Ефим}), \text{отец}(\text{Ефим}, \text{Анатолий}),$

$\text{мать}(\text{Татьяна}, \text{Анатолий}) \rightarrow 0.$

Целевой дизъюнкт нейтрализуется предикатами под номерами 47, 44 и 65, когда переменные принимают конкретные значения:

$y = \text{Татьяна}, z = \text{Ефим}, u = \text{Анатолий}.$

2. Группы

Введение.

САЙТ АВТОРА: <http://sceptic-ratio.narod.ru/index.htm>

В «Лекциях о развитии математики в XIX столетии» великий немецкий математик Феликс Клейн (1849—1925) после формулировки четырех условий, определяющих алгебраическую группу, написал следующее:

Таким образом, какая-либо апелляция к воображению здесь отсутствует в принципе. Взамен этого тщательно препарируется логический скелет... Подобного рода абстрактные формулировки превосходны для полировки доказательств, но они совершенно не годятся для того, чтобы с их помощью отыскивать новые идеи и методы. Более того, как правило, они являются завершением определенного этапа предшествующего развития. Поэтому внешне они облегчают преподавание, поскольку на их основе можно просто и без каких-либо пробелов доказывать известные уже предложения. Однако они внутренне чрезвычайно затрудняют учащегося, так как он оказывается поставленным перед чем-то совершенно законченным, ничего не зная о том, как автор пришел к этим определениям; к тому же он не может себе абсолютно ничего представить. Этот метод не поощряет к тому, чтобы пользующийся им мысля; требуется лишь внимательно следить, чтобы не погрешить против данных нам четырех заповедей¹.

На сегодняшний день существует масса учебной литературы по дискретной математике, в которой теория групп, как основа для современной абстрактной алгебры, занимает видное место. В этих книгах можно отыскать любую формулировку, относящуюся к той или иной характеристике групп, причем, возможно, самую правильную и идеально отточенную дефиницию². Но там нельзя найти одного — самих групп. Этот изъян можно исправить, если отказаться от тотального *формализма*. Нужно попытаться встать на *конструктивный* путь рассмотрения групп, детально изучая их свойства и морфологию.

Раньше, два-три десятка лет назад, преподавание теории групп было облегчено тем, что группы тесно увязывались с фундаментальными областями естествознания — физикой элементарных частиц, квантовой механикой, физикой твердого тела и кристаллографией. Сегодня, лишившись предметного воплощения, прекрасная математическая концепция — база современной алгебры — оказалась невостребованной. В несколько поверхностные курсы «Дискретной математики» группы вошли отдельными главами чаще всего в слишком абстрактном, а значит, и плохо усваиваемом виде (на что в свое время сетовал Феликс Клейн). Имея немалый опыт преподавания, автор убедился в эффективности метода *самостоятельного конструирования математических объектов*. Придерживаясь из-

¹ Клейн Ф. Лекции о развитии математики в XIX столетии. В 2-х томах. Т. 1. — М.: Наука, 1989, с. 372.

² Например, «Общая алгебра» в 2-х томах под редакцией Л.А. Скорнякова. — М.: Наука, 1991.

вестной методологии конструктивизма¹, он пытается дать о группах максимально наглядное представление; при этом дотошный читатель постоянно находится в роли активного исследователя. При такой методике автор не должен стремиться к изложению как можно большего числа готовых теорем; важнее здесь позаботиться о развитии аналитических способностей обучающегося.

В отличие от первой главы «Логика», здесь отсутствуют разделы с практически заданиями. Дело в том, что последовательно разбирая все группы с 1 по 27 порядок, а также проводя частичный анализ групп высших порядков, мы тем самым закладываем безграничное поле для упражнений. Любой читатель сумеет составить для себя небольшое задание. Вот пример такого задания по теме «Подстановки»: *найти четность, декремент и число инверсий подстановки x , если известно, что*

$$x^{-1} = a^{-1} b^3 c^{-2} ba, \text{ где } a = (015)(24), b^{-1} = (14)(235), c = (0431).$$

Заданий подобного рода всякий преподаватель придумает массу. Вряд ли оправдано тратить бумагу на формулирование задач следующего содержания: *составить решетку подгрупп группы $S_2^3 C_4$; найти внутренний автоморфизм группы D_{16}^7 и т. д.* «Особо одаренным» можно выдать персональное задание: *отыскать пятимерное неприводимое представление группы вращения икосаэдра*. Наконец, можно потребовать от студентов *провести полный морфологический анализ группы 32-го порядка*. Их одних будет достаточно, чтобы полностью загрузить индивидуальными заданиями на целый семестр огромный поток студентов. Таким образом, подбор практических заданий по закреплению нового материала не должен вызывать у кого-либо затруднений.

2.1. Введение понятия группы

Линейное преобразование A вектора x в вектор y осуществляется с помощью квадратной матрицы:

$$y = Ax, \text{ где } A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}. \quad (2.1)$$

Если имеет место *прямое* преобразование (2.1), то должно существовать и *обратное* при условии, что матрица A имеет обратную:

$$y = A^{-1}x.$$

Транзитивность линейного преобразования задает операцию умножения. Пусть даны два линейных преобразования:

$$z = Ay, \quad y = Bx,$$

Тогда существует третье преобразование C , которое получается путем перемножения A и B , т.е.

$$z = Ay = A(Bx) = (AB)x = Cx. \quad (2.2)$$

¹ См. две книги Джорджа Поля «Математическое открытие» (1970) и «Математика и правдоподобные рассуждения» (1975).

Выражение (2.2) стало возможным благодаря действию закона ассоциативности в отношении операторов A и B , а также вектора x . Наряду с выполнением закона (2.2), действуют еще три закона - один ассоциативности и два дистрибутивности:

$$A(\lambda x) = (A\lambda)x = (\lambda A)x, (A + B)x = Ax + Bx, A(x + y) = Ax + Ay, \quad (2.3)$$

где λ — действительное или комплексное число.

Предположим, что матрица A в некотором базисе реализует линейное преобразование (2.1). В новом базисе это преобразование будет выглядеть иначе:

$$y' = A'x'. \quad (2.4)$$

Обозначим через T матрицу перехода векторов из нового базиса в старый:

$$x = Tx', \quad y = Ty'. \quad (2.5)$$

Подставив оба выражения (2.5) в преобразование (2.1), получим

$$Ty' = ATx'. \quad (2.6)$$

Умножим (2.6) слева на T^{-1} :

$$y' = T^{-1}ATx'. \quad (2.7)$$

Сравнивая равенства (2.4) и (2.7), окончательно находим:

$$A' = T^{-1}AT. \quad (2.8)$$

Линейное преобразование (2.8) называется *прямым преобразованием подобия*. Про матрицы A и A' говорят, что они *подобны*. Чтобы получить *обратное* преобразование подобия, нужно выражение (2.8) слева умножить на T , а справа на T^{-1} в результате получим:

$$A = TA'T^{-1}. \quad (2.9)$$

Прямое и обратное преобразования обладают следующими свойствами, которые мы выпишем здесь только для прямого:

$$\begin{aligned} T^{-1}(AB)T &= (T^{-1}AT)(T^{-1}BT), \\ T^{-1}(A+B)T &= T^{-1}AT + T^{-1}BT, \\ T^{-1}A^{-1}T &= (T^{-1}AT)^{-1}, \quad T^{-1}A^nT = (T^{-1}AT)^n. \end{aligned} \quad (2.10)$$

Среди бесчисленного множества векторов x линейного преобразования (2.1) всегда найдется такой, что под действием оператора A вектор x перейдет в коллинеарный себе, т.е. координаты преобразованного вектора отличаются от исходного только скалярным множителем λ :

$$Ax = \lambda x. \quad (2.11)$$

В этом случае ненулевой вектор x называется *собственным вектором* оператора A , а число λ — его *собственным значением*. Равенство (2.11) эквивалентно системе уравнений:

$$(A - \lambda E)x = 0, \quad (2.12)$$

которую можно использовать для нахождения собственных векторов x (здесь E — единичная матрица). Но прежде требуется найти все собственные значения оператора A . С этой целью составляют *характеристический определитель*, который затем разворачивается в *характеристический многочлен* — $p(\lambda)$:

$$p(\lambda) = \det(A - \lambda E) = 0. \quad (2.13)$$

Корни многочлена (2.13) поочередно подставляются в систему (2.12). Решая ее отдельно для каждого собственного значения λ , находят соответствующие им собственные векторы x .

Собственные значения и собственные векторы часто ищутся с помощью процедуры *диагонализации* матрицы A . В результате этой процедуры все собственные значения оказываются расположенными на главной диагонали *диагональной матрицы* Λ . Эта диагональная матрица также является линейным преобразованием типа (2.1), для которого остаются в силе свойства (2.2), (2.3) и, что особенно важно для нас сейчас, Λ связана с исходной матрицей A преобразованием подобия:

$$\Lambda = T^{-1}AT. \quad (2.14)$$

В силу *транзитивности* преобразования подобия, т.е. если

$$C = S^{-1}BS, \quad B = R^{-1}AR \quad \text{и} \quad RS = T,$$

то оператор C связан с оператором A преобразованием подобия:

$$C = S^{-1}(R^{-1}AR)S = (RS)^{-1}A(RS) = T^{-1}AT,$$

т.е. *все подобные матрицы имеют одинаковые собственные значения*.

Трансформационная матрица T , фигурирующая в преобразовании подобия (2.8), и матрица A в линейном преобразовании (2.1) на самом деле выполняют одинаковые функции, т.е. переводят одни векторы в другие. Далее мы будем рассматривать замкнутые по умножению *группы* линейных операторов, представленные в виде конечной совокупности матриц. С помощью преобразования подобия, в котором T пробегает все элементы группы, можно выявить *класс эквивалентных операторов*. В этом случае проявится *относительное* подобие. Но может получиться так, что рассматриваемая группа операторов является лишь *подгруппой* более обширного замкнутого множества. Тогда преобразование подобия по более широкой группе пополнит класс подобных операторов другими элементами. Диагональный оператор Λ , сам не являясь элементом рассматриваемой группы операторов, может символизировать *предельно* широкий класс подобных элементов, не входящих в данную группу операторов. Таким образом, *процедура диагонализации* матриц позволяет разбить группу операторов на несколько непересекающихся *абсолютных* классов подобных элементов с одинаковыми наборами собственных значений. Абсолютные классы либо совпадают, либо шире *относительных*.

В дальнейшем нам часто придется иметь дело с матрицами, поэтому напомним основные действия с ними. Правило перемножения матриц продемонстрируем на числовых примерах. Пусть даны две матрицы

$$A = \begin{pmatrix} 1 & 2 \\ -3 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 5 & -2 \\ -6 & 3 \end{pmatrix}.$$

Перемножим их слева направо как они записаны:

$$AB = \begin{pmatrix} 1 & 2 \\ -3 & 4 \end{pmatrix} \begin{pmatrix} 5 & -2 \\ -6 & 3 \end{pmatrix} = \begin{pmatrix} 1 \cdot 5 + 2 \cdot (-6) & 1 \cdot (-2) + 2 \cdot 3 \\ (-3) \cdot 5 + 4 \cdot (-6) & (-3) \cdot (-2) + 4 \cdot 3 \end{pmatrix} = \begin{pmatrix} -7 & 4 \\ -39 & 18 \end{pmatrix}.$$

Теперь справа налево —

$$BA = \begin{pmatrix} 5 & -2 \\ -6 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ -3 & 4 \end{pmatrix} = \begin{pmatrix} 5 \cdot 1 + (-2) \cdot (-3) & 5 \cdot 2 + (-2) \cdot 4 \\ (-6) \cdot 1 + 3 \cdot (-3) & (-6) \cdot 2 + 3 \cdot 4 \end{pmatrix} = \begin{pmatrix} 11 & 2 \\ -15 & 0 \end{pmatrix}.$$

Про матрицы A и B говорят, что они *не коммутируют*, поскольку $AB \neq BA$. Две другие матрицы — A_1 и B_1 — коммутируют друг с другом, в чем можно убедиться путем их непосредственного перемножения —

$$A_1 = \begin{pmatrix} 2 & 3 \\ 1 & 4 \end{pmatrix}, \quad B_1 = \begin{pmatrix} 3 & 6 \\ 2 & 7 \end{pmatrix}, \quad A_1 B_1 = B_1 A_1.$$

Рассмотрим преобразование подобия. Пусть исходный базис выражается через φ , а новый — через φ' :

$$\varphi_1 = x, \quad \varphi'_1 = \frac{1}{\sqrt{3}} \cdot (\varphi_1 + \varphi_2 + \varphi_3) = \frac{1}{\sqrt{3}} \cdot (x + y + z);$$

$$\varphi_2 = y, \quad \varphi'_2 = \frac{1}{\sqrt{2}} \cdot (\varphi_2 - \varphi_3) = \frac{1}{\sqrt{2}} \cdot (y - z);$$

$$\varphi_3 = z, \quad \varphi'_3 = \frac{1}{\sqrt{6}} \cdot (2 \cdot \varphi_1 - \varphi_2 - \varphi_3) = \frac{1}{\sqrt{6}} \cdot (2 \cdot x - y - z).$$

Тогда трансформационная матрица T и обратная ей T^{-1} выглядят следующим образом:

$$T = \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{3}} \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{2}{\sqrt{6}} & \frac{-1}{\sqrt{6}} & \frac{-1}{\sqrt{6}} \end{pmatrix}, \quad T^{-1} = \begin{pmatrix} \frac{1}{\sqrt{3}} & 0 & \frac{2}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{6}} \\ \frac{1}{\sqrt{3}} & \frac{-1}{\sqrt{2}} & \frac{-1}{\sqrt{6}} \end{pmatrix}.$$

Наша трансформационная матрица T относится к *ортонормированным*, т.е. возведение любой строки и любого столбца в квадрат дает единицу, а перемножение различных строк и столбцов — ноль, например:

$$\left(\frac{1}{\sqrt{3}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{6}}\right)^2 = 1, \quad \frac{2}{\sqrt{6}} \cdot 0 + \left(\frac{1}{\sqrt{6}}\right) \cdot \frac{1}{\sqrt{2}} + \left(\frac{-1}{\sqrt{6}}\right) \cdot \left(\frac{-1}{\sqrt{2}}\right) = 0.$$

Для ортонормированных матриц (а именно с такими мы чаще всего будем иметь дело) *обратная* матрица получается путем *транспонирования* исходной.

Пусть, далее, в старом базисе φ действует оператор A , который переводит координаты x, y, z в координаты x_A, y_A, z_A :

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad \begin{aligned} x_A &= 0 \cdot x + 1 \cdot y + 1 \cdot z = y + z, \\ y_A &= 1 \cdot x + 0 \cdot y + 1 \cdot z = x + z, \\ z_A &= 1 \cdot x + 1 \cdot y + 0 \cdot z = x + y. \end{aligned}$$

В новом базисе оператор A , согласно (2.9), превратится в A' :

$$A' = T A T^{-1} = \Lambda = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

В новом базисе действие оператора A' сводится к умножению всех координат на числа. Фактически, мы нашли *собственные значения* матрицы A , поскольку диагональная матрица A' является одновременно матрицей Λ .

Всю процедуру трансформации координат можно провести на уровне преобразования соответствующих векторов, не прибегая в явном виде к формуле преобразования подобия. В самом деле,

$$x' = \frac{1}{\sqrt{3}} \cdot (x_A + y_A + z_A) = 2 \cdot \left[\frac{1}{\sqrt{3}} \cdot (x + y + z) \right] = 2 \cdot \varphi_1 + 0 \cdot \varphi_2 + 0 \cdot \varphi_3;$$

$$y' = \frac{1}{\sqrt{2}} \cdot (y_A - z_A) = \frac{1}{\sqrt{2}} \cdot (x + z - x - y) = (-1) \cdot \left[\frac{1}{\sqrt{2}} \cdot (y - z) \right] = 0 \cdot \varphi_1 - 1 \cdot \varphi_2 + 0 \cdot \varphi_3;$$

$$z' = \frac{1}{\sqrt{6}} \cdot (2 \cdot x_A - y_A - z_A) = (-1) \cdot \left[\frac{1}{\sqrt{6}} \cdot (2x - y - z) \right] = 0 \cdot \varphi_1 + 0 \cdot \varphi_2 - 1 \cdot \varphi_3.$$

Последние выкладки призваны также показать, что любые преобразования — будь то A , A' , T — не существуют сами по себе, но всегда предполагают присутствие *базисных векторов*.

Обращаем внимание на то, что сумма диагональных элементов матрицы A (она именуется *характером* матрицы A) равна сумме диагональных элементов матрицы A' . И это неслучайно: *характеры подобных матриц всегда одинаковы*. Равенство характеров позволяет контролировать правильность нахождения собственных значений.

Перестановка строк матрицы с одновременной перестановкой соответствующих столбцов (а такая процедура также относится к преобразованию подобия) не меняет внутренней природы матрицы. Данная трансформация не влияет и на собственные значения. Если матрица A имела собственные значения λ , то эквивалентная ей матрица A' будет иметь ту же самую матрицу Λ , но в которой собственные значения окажутся на новых местах. Перестановка строк и столбцов возможна постольку, поскольку она не меняет связи диагональных элементов с недиагональными. Пусть в матрице A элемент a_{23} связывает элементы a_{22} и a_{33} , тогда после нового размещения элементов на диагонали уже в матрице A' указанная связь должна сохраниться:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}, \quad A' = \begin{pmatrix} a_{22} & a_{12} & a_{23} \\ a_{21} & a_{11} & a_{13} \\ a_{32} & a_{31} & a_{33} \end{pmatrix}, \quad \Lambda = \begin{pmatrix} \lambda_2 & 0 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}.$$

Сейчас мы достаточно подготовлены, чтобы ввести *определение группы*. *Группой* называется *операционное множество*, в котором действует процедура *умножения* и которое подчинено следующим *четырем условиям* —

1) *замкнутости*: для каждой пары элементов g_1 и g_2 из группы G однозначно определено произведение $g_1 g_2 = g_3$; причем элемент g_3 тоже должен обязательно принадлежать группе G , т.е.

$$g_1, g_2 \in G, \quad g_1 g_2 = g_3 \in G.$$

2) *наличия тождественного элемента e* : среди множества элементов группы G должен найтись такой элемент e , что для всякого g из G справедливы равенства:

$$eg = g, \quad ge = g; \quad e, g \in G.$$

3) *наличия обратных элементов*: для всякого g из G должен отыскаться единственный ему обратный элемент g^{-1} , принадлежащий G , при умножении на кото-

рый получился бы тождественный элемент e ; суть данного положения математически выражается следующим образом:

$$e = g g^{-1}, \quad e = g^{-1} g; \quad e, g, g^{-1} \in G.$$

4) *ассоциативности*: для любых трех элементов g_1, g_2 и g_3 из G справедливо равенство:

$$g_1(g_2 g_3) = (g_1 g_2)g_3.$$

Последнее условие выполняется для квадратных матриц, в чем можно убедиться путем перемножения, в частности, матриц размерности 2×2 :

$$\begin{aligned} (AB)C &= \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} = \\ &= A(BC) = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} d_1 & d_2 \\ d_3 & d_4 \end{pmatrix}, \end{aligned}$$

где

$$d_1 = a_1 b_1 c_1 + a_2 b_3 c_1 + a_1 b_2 c_3 + a_2 b_4 c_3,$$

$$d_2 = a_1 b_1 c_2 + a_2 b_3 c_2 + a_1 b_2 c_4 + a_2 b_4 c_4,$$

$$d_3 = a_3 b_1 c_1 + a_4 b_3 c_1 + a_3 b_2 c_3 + a_4 b_4 c_3,$$

$$d_4 = a_3 b_1 c_2 + a_4 b_3 c_2 + a_3 b_2 c_4 + a_4 b_4 c_4.$$

Аналогичная процедура доказательства распространяется на матрицы любой размерности.

В связи с этим для кого-то, возможно, условие ассоциативности в определении группы покажется излишним, коль скоро это свойство внутренне присуще самим исходным математическим объектам. На это следует сказать, что определение группы давалось в *алгебраической* форме, т.е. отвлеченно, посредством абстрактных символов, а для символов принадлежащие матрицам свойства должны быть оговорены отдельно. Это позволит в дальнейшем производить над символами те же действия, что и над матрицами. Однако нужно отчетливо понимать, что алгебраическое определение схватывает *сущность* группы, но не является чем-то более широким, более обобщенным или более первичным. Напротив, оно скорее основывается на свойствах конкретных математических объектов, чем обуславливает их. В конкретных объектах всегда присутствует нечто большее, чем говорится в определении. В частности, любой объект предполагает свое *субстанционное строение*: всякая *реальная* группа подразумевает два вида множеств: одно *стационарное* — базисные векторы, другое *динамическое* — операторы-матрицы, преобразующие векторы. Таким образом, группа есть не только, говоря словами Павла Флоренского, «синтез некоторого множества в единство актом духа» («О символах бесконечности»), но и синтез *движения* и *покоя*, *изменения* и *сохранения*. При чисто алгебраическом подходе, когда реальные математические объекты (матрицы) подменяются анонимными символами, эта двойственность испаряется. На первый план выходит только операционное множество, к которому и относятся четыре выше сформулированных условия.

Приверженец исключительно алгебраического взгляда на группы, приступая к анализу симметрии конкретных геометрических фигур, кристаллов или физических законов, растеряется и не будет знать, какого рода элементы остаются не-

изменными (*инвариантными*) при групповых преобразованиях: понимать ли под элементами симметрии *действительно существующую материальную вещь* или *возможную операцию*. Тот, кто научится различать два типа множеств, легко установит, что за *субстанционные элементы* необходимо принимать, например, вершины, грани, ребра геометрических фигур, а за *операционные* — различные повороты, отражения, сдвиги этих фигур. Выбор субстанционных и операционных элементов взаимно обусловлен. Так, к примеру, если в кубе в качестве субстанционного множества взять четыре его пространственных диагонали, то на них можно получить 24 элемента различных преобразований, а если в качестве субстанционного множества выбрать шесть его граней, то группа возможных преобразований возрастет до 48 элементов.

Ниже мы установим, что за абстрактным символом мнимой единицы (i) и ее алгебраическим определением ($i^2 = -1$) скрывается конкретная субстанционная конструкция на 0,1-матрицах. Групповые условия для нее не могут быть продекларированы *сверху*, без учета ее *внутренней* природы. Отсюда, чтобы создать, к примеру, абстрактную теорию комплексного числа, нужно предварительно хорошо изучить мнимую единицу *снизу*, с позиции ее субстанционного строения. Поясним сказанное примером, взятым из *булевой логики*. Известно, что логические операции типа дизъюнкции и конъюнкции подчинены закону ассоциативности, а стрелка Пирса и штрих Шеффера — нет. Проистекают указанные свойства операций непосредственно из правил их построения, которые продиктованы, в свою очередь, таблицами истинности и диаграммами Эйлера — Венна. Таким образом, *строго аксиоматическое построение логики*, когда провозглашаются единственно имеющими силу аксиомы коммутативности, ассоциативности и дистрибутивности, *не освобождает ее от возможного субстанционного конструирования*, которое часто оказывается за рамками сформировавшейся теории. Аналогичная ситуация просматривается и в геометрии. Предложение «две прямые пересекаются в одной-единственной точке» не требует доказательства только потому, что оно фактически обеспечено субстанционной данностью — геометрической плоскостью. Если же провозглашается, что «две прямые пересекаются в двух точках», то субстанционной реальностью становится шар. Выдвижение той или иной аксиомы не является исключительной прерогативой субъекта теории, как это может показаться на первый взгляд; оно всегда ставится в зависимость от наличия адекватной *математической субстанции*. Так, прежде чем постулировать аксиому в виде «две прямые пересекаются в трех точках», необходимо указать на соответствующий объект, где бы эта ситуация могла быть реализована. Если подходящего объекта не найдется, то не следует и браться за построение геометрии с такой аксиомой.

Индуктивный и конструктивный путь познания является общенаучным. Он, в частности, принят в естествознании. Математик, как и естествоиспытатель, обязан иметь перед глазами *реальный*, а не выдуманный объект исследования. Нужно следить, чтобы символы не выходили за рамки «своих полномочий», не выступали в роли *самодовлеющих сущностей*, а только как их *представители*. Чрезмерное увлечение абстрактными вещами убивает математический дух и ведет к пустой схоластике. Истинное творчество невозможно без *образного мышления*, без *механического конструирования из осязаемых деталей*. В любом случае можно согласиться: прежде чем выходить на высокие абстрактные уровни, хоро-

шо бы исследовать незнакомое явление на знакомых и понятных вещах, каковы-ми являются, в частности, векторы и матрицы.

Ниже приводятся восемь степеней одной и той же матрицы a :

$$a^1 = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{-i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}, \quad a^2 = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \quad a^3 = \begin{pmatrix} \frac{-1}{\sqrt{2}} & \frac{-i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}, \quad a^4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$a^5 = \begin{pmatrix} \frac{-1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix}, \quad a^6 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad a^7 = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}, \quad a^8 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Выписанные матрицы составляют *операционное множество*, подчиненное четы-рем групповым условиям. В роли тождественного элемента здесь выступает еди-ничная матрица $a^8 = e$. Перед нами *коммутативная группа A восьмого порядка* с таблицей умножения — табл. 2.1. *Субстанционным множеством* для нее являются восемь базисных векторов (первые столбцы матриц), которые переходят друг в друга под действием преобразований a^i :

$$1 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix}, \quad 2 = \begin{pmatrix} 0 \\ -i \end{pmatrix}, \quad 3 = \begin{pmatrix} \frac{-1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix}, \quad 4 = \begin{pmatrix} -1 \\ 0 \end{pmatrix}, \quad 5 = \begin{pmatrix} \frac{-1}{\sqrt{2}} \\ \frac{-i}{\sqrt{2}} \end{pmatrix}, \quad 6 = \begin{pmatrix} 0 \\ i \end{pmatrix}, \quad 7 = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-i}{\sqrt{2}} \end{pmatrix}, \quad 8 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Таблица 2.1

A	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8
a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^1
a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^1	a^2
a^3	a^4	a^5	a^6	a^7	a^8	a^1	a^2	a^3
a^4	a^5	a^6	a^7	a^8	a^1	a^2	a^3	a^4
a^5	a^6	a^7	a^8	a^1	a^2	a^3	a^4	a^5
a^6	a^7	a^8	a^1	a^2	a^3	a^4	a^5	a^6
a^7	a^8	a^1	a^2	a^3	a^4	a^5	a^6	a^7
a^8	a^1	a^2	a^3	a^4	a^5	a^6	a^7	a^8

Например, $8 = a^3 \times 5$, $7 = a^5 \times 2$, $a^5 = a^3 \times a^2$, или подробно:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{-1}{\sqrt{2}} & \frac{-i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix}, \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{-1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ -i \end{pmatrix}, \quad \begin{pmatrix} \frac{-1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{-1}{\sqrt{2}} & \frac{-i}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

Подмножества $\{a^2, a^4, a^6, a^8\}$ и $\{a^3, a^5, a^7, a^1\}$ образуют *подгруппы* в группе A , поскольку элементы этих подмножеств удовлетворяют всем необходимым групповым условиям — замкнутости, ассоциативности, наличию в указанных подмножест-вах тождественного и обратных элементов.

Приведем множество B , которое также состоит из восьми матриц, получен-ных путем циклического возведения в степень исходной матрицы b :

$$b^1 = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} & \frac{i}{\sqrt{2}} \end{pmatrix}, \quad b^2 = \begin{pmatrix} \frac{1}{2}(1+i) & \frac{1}{2}(1+i) \\ \frac{1}{2}(-1+i) & \frac{1}{2}(-1+i) \end{pmatrix}, \quad b^3 = \begin{pmatrix} \frac{i}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix}, \quad b^4 = \begin{pmatrix} \frac{1}{2}(1+i) & \frac{1}{2}(1+i) \\ \frac{1}{2}(-1-i) & \frac{1}{2}(-1-i) \end{pmatrix},$$

$$b^5 = \begin{pmatrix} \frac{-1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \\ \frac{-i}{\sqrt{2}} & \frac{-i}{\sqrt{2}} \end{pmatrix}, \quad b^6 = \begin{pmatrix} \frac{1}{2}(1-i) & \frac{1}{2}(1-i) \\ \frac{1}{2}(1-i) & \frac{1}{2}(1-i) \end{pmatrix}, \quad b^7 = \begin{pmatrix} \frac{i}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}, \quad b^8 = \begin{pmatrix} \frac{1}{2}(1-i) & \frac{1}{2}(1-i) \\ \frac{1}{2}(1+i) & \frac{1}{2}(1+i) \end{pmatrix}.$$

Множество B составляет группу, *изоморфную* группе A , поскольку ее элементы тоже перемножаются в соответствии с табл. 2.1 (если в последней символ a заменить на b). В группе B , как и в группе A , имеются две подгруппы из четырех и двух элементов. Примечательной особенностью циклической группы B является то, что в качестве *тождественного элемента* здесь выступает не *единичная* матрица, а ничем не примечательная матрица $b^8 = e$. Если матрицу, обозначенную в списке как b^3 (или b^5 , или b^7), взять за *образующую*, то матрица, обозначенная как b^8 , по-прежнему будет выполнять роль тождественного элемента.

Транспонируем матрицы b^i . Получим новую циклическую группу C , изоморфную как группе B , так и группе A . Табл. 2.2 демонстрирует тоже циклический закон умножения исходных (b^i) и транспонированных (c^j) матриц:

$$d^k = b^i \times c^j.$$

Таблица 2.2

$b^i \times c^j$	c^1	c^2	c^3	c^4	c^5	c^6	c^7	c^8
b^1	d^2	d^3	d^4	d^5	d^6	d^7	d^8	d^1
b^2	d^3	d^4	d^5	d^6	d^7	d^8	d^1	d^2
b^3	d^4	d^5	d^6	d^7	d^8	d^1	d^2	d^3
b^4	d^5	d^6	d^7	d^8	d^1	d^2	d^3	d^4
b^5	d^6	d^7	d^8	d^1	d^2	d^3	d^4	d^5
b^6	d^7	d^8	d^1	d^2	d^3	d^4	d^5	d^6
b^7	d^8	d^1	d^2	d^3	d^4	d^5	d^6	d^7
b^8	d^1	d^2	d^3	d^4	d^5	d^6	d^7	d^8

Однако вся совокупность из 24 матриц B , C , D и даже отдельно 8 матриц D не образуют группы, поскольку в указанных множествах, во-первых, нет тождественного элемента (во всяком случае общего на все элементы), во-вторых, произведения элементов этих множеств равны нулевой матрице, которая, согласно групповым условиям, не может входить в состав групп:

$$c^i \times b^i = d^i \times d^i = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Таким образом, произведение элементов двух групп породило *негрупповое* множество D :

$$d^1 = \begin{pmatrix} \frac{1}{\sqrt{2}}(1-i) & \frac{1}{\sqrt{2}}(1+i) \\ \frac{1}{\sqrt{2}}(1+i) & \frac{1}{\sqrt{2}}(-1+i) \end{pmatrix}, \quad d^2 = \begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix},$$

$$d^3 = \begin{pmatrix} \frac{1}{\sqrt{2}}(1+i) & \frac{1}{\sqrt{2}}(-1-i) \\ \frac{1}{\sqrt{2}}(-1+i) & \frac{1}{\sqrt{2}}(-1-i) \end{pmatrix}, \quad d^4 = \begin{pmatrix} i & -1 \\ 1 & -i \end{pmatrix},$$

$$d^5 = \begin{pmatrix} \frac{1}{\sqrt{2}}(-1+i) & \frac{1}{\sqrt{2}}(-1-i) \\ \frac{1}{\sqrt{2}}(-1-i) & \frac{1}{\sqrt{2}}(1-i) \end{pmatrix}, \quad d^6 = \begin{pmatrix} -1 & -i \\ -i & 1 \end{pmatrix},$$

$$d^7 = \begin{pmatrix} \frac{1}{\sqrt{2}}(1-i) & \frac{1}{\sqrt{2}}(1+i) \\ \frac{1}{\sqrt{2}}(1+i) & \frac{1}{\sqrt{2}}(-1-i) \end{pmatrix}, \quad d^8 = \begin{pmatrix} -i & 1 \\ 1 & i \end{pmatrix}.$$

Приведем пример *некоммутативной группы* D_3 на матрицах, элементами которых являются числа 0 и 1. Здесь при перемножении матриц следует учитывать, что сложение осуществляется по $\text{mod}(2)$, т.е. сумма $1 + 1 = 0$. То, что группа D_3 не коммутативна, видно из ее таблицы умножения (табл. 2.3), в которой не все элементы расположены симметрично относительно главной диагонали. Причем данная группа относится к весьма распространенному типу групп, имеющих общепринятое обозначение D_3 и названных Ф. Клейном группами *диэдра* («диэдр» название геометрической фигуры: *ди* – «два», *эдр* – «поверхность»):

$$0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad 1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad 2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad 3 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad 4 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad 5 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Если в качестве *образующего элемента* из выписанных матриц взять матрицу, обозначенную цифрой 1, а при перемножении матриц использовать сложение по $\text{mod}(3)$, когда $1 + 2 = 0$, $2 + 2 = 1$, то получим *циклическую*, а значит, *коммутативную* группу с общепринятым обозначением – C_6 :

$$0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad 1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad 2 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad 3 = \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix}, \quad 4 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \quad 5 = \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}.$$

Таблица умножения элементов группы C_6 (табл. 2.4) уже будет симметричной относительно своей главной диагонали.

Таблица 2.3

D_3	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	0	3	2	5	4
2	2	4	0	5	1	3
3	3	5	1	4	0	2
4	4	2	5	0	3	1
5	5	3	4	1	2	0

Таблица 2.4

C_6	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	4	3	5	0	2
2	2	3	0	1	5	4
3	3	5	1	4	2	0
4	4	0	5	2	1	3
5	5	2	4	0	3	1

Приведенных примеров, по-видимому, достаточно, чтобы усвоить понятие группы. Занимаясь *морфологическим анализом* групп, мы позже убедимся, какую исключительно важную роль играет при этом *преобразование подобия* или, как часто его называют, *трансформационное преобразование* (2.8). Оно позволяет группе G , состоящую из элементов $\{ \dots, u, v, w, x, y, z \}$, разбить на *классы эквивалентности*. Отношение эквивалентности предполагает выполнение трех законов – *рефлексивности* (каждый элемент a равен самому себе: $a = a$), *симметричности* (если $a = b$, то и $b = a$) и *транзитивности* (если $a = b$ и $b = c$, то $a = c$). Все три закона выполняются для преобразования подобия, которое для группы G с указанными элементами запишется как

$$x = z^{-1} y z. \quad (2.15)$$

В теории групп в этом случае принято говорить, что элемент x *сопряжен* элементу y посредством элемента z . Закон *рефлексивности* выполняется для преобразования подобия (2.15) в силу неперемного существования в группе G такого

элемента z , что

$$x = z^{-1} x z,$$

в частности, когда $z = e$. Для того чтобы убедиться в справедливости закона *симметричности*, достаточно преобразование (2.15) умножить справа на z^{-1} и слева на z , получим

$$y = z x z^{-1}.$$

Но, так как всякий элемент z имеет себе обратный (w), последнее равенство можно переписать в нужном нам виде, т.е. как (2.15):

$$y = w^{-1} x w.$$

Наконец, проверим выполнение закона *транзитивности*, который в данном случае формулируется следующим образом:

$$\text{если } x = z^{-1} y z \text{ и } y = v^{-1} u v, \text{ то } x = w^{-1} u w.$$

Это возможно в силу

$$x = z^{-1} y z = z^{-1} (v^{-1} u v) z = (z^{-1} v^{-1}) u (v z) = (vz)^{-1} u (v z) = w^{-1} u w.$$

В *коммутативных* группах каждый элемент образует свой собственный класс *сопряженности*, так что число классов равно *порядку* (т.е. числу элементов) группы:

$$x = z^{-1} y z = z^{-1} z y = y.$$

Отсюда разбиение группы на относительные классы эквивалентности начальных пяти порядков заранее предпрешено, так как все они коммутативны. Впервые некоммутативность между элементами встречается в группе диэдра D_3 , которая состоит, как мы уже видели, из шести элементов.

2.2. Действия с 0,1-матрицами

Двум единицам — положительной (+1) и отрицательной (−1) — поставим в соответствие две 0,1-матрицы размером 2×2 :

$$1 \rightarrow e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad -1 \rightarrow -e = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (2.16)$$

Произведем обычное перемножение этих матриц:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \text{ т.е. как } 1 \times (-1) = -1,$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \text{ т.е. как } (-1) \times (-1) = 1.$$

Убеждаемся, что при перемножении 0,1-матрицы ведут себя аналогично традиционным единицам. Следовательно, замена (2.16) позволяет воссоздать действия с отрицательными числами без использования самих отрицательных чисел.

Рассмотрим конкретный числовой пример:

$$\begin{pmatrix} -1 & 2 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 3 & -1 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 5 \\ -7 & 5 \end{pmatrix},$$

Всем этим матрицам поставим в соответствие матрицы удвоенной размерности, в которых нет отрицательных чисел —

$$\begin{pmatrix} 0 & 1 & 2 & 0 \\ 1 & 0 & 0 & 2 \\ 0 & 3 & 1 & 0 \\ 3 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 0 & 0 & 1 \\ 0 & 3 & 1 & 0 \\ 2 & 0 & 2 & 0 \\ 0 & 2 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 3 & 5 & 0 \\ 3 & 4 & 0 & 5 \\ 2 & 9 & 5 & 0 \\ 9 & 2 & 0 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 5 & 0 \\ 0 & 1 & 0 & 5 \\ 0 & 7 & 5 & 0 \\ 7 & 0 & 0 & 5 \end{pmatrix}.$$

Здесь в матричных блоках 2×2 были приняты следующие равенства:

$$\begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 2 & 9 \\ 9 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 7 \\ 7 & 0 \end{pmatrix},$$

$$4 - 3 = 1, \quad 2 - 9 = -7.$$

Однако можно принять, что

$$\begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 2 & 9 \\ 9 & 2 \end{pmatrix} \neq \begin{pmatrix} 0 & 7 \\ 7 & 0 \end{pmatrix}.$$

Если мы не захотим смешивать положительные и отрицательные числа (подобно тому, как мы не смешиваем мнимую и вещественную компоненты комплексного числа) —

$$4 \times e + 3 \times (-e) \neq 1 \times e + 0 \times (-e),$$

$$2 \times e + 9 \times (-e) \neq 0 \times e + 7 \times (-e),$$

то каждому числу будет отвечать бесчисленное множество *матричных чисел*, а одной операции умножения чисел — бесчисленное множество матричных умножений. Например, произведению $(-3) \times 4 = -12$, будет соответствовать бесконечный ряд следующих эквивалентных операций:

$$\begin{pmatrix} 2 & 5 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} 6 & 2 \\ 2 & 6 \end{pmatrix} = \begin{pmatrix} 22 & 34 \\ 34 & 22 \end{pmatrix}, \quad \begin{pmatrix} 3 & 6 \\ 6 & 3 \end{pmatrix} \begin{pmatrix} 5 & 1 \\ 1 & 5 \end{pmatrix} = \begin{pmatrix} 21 & 33 \\ 33 & 21 \end{pmatrix}, \quad \begin{pmatrix} 10 & 13 \\ 13 & 10 \end{pmatrix} \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 40 & 52 \\ 52 & 40 \end{pmatrix}, \dots$$

Теперь обратимся к *комплексным числам*. Как известно, они строятся на базе четырех единиц:

$$i_0 = 1, \quad i_1 = i, \quad i_2 = -1, \quad i_3 = -i,$$

которые перемножаются в соответствии с табл. 2.5. Индексы базисных единиц подчиняются закону сложения по mod (4). Этот закон сложения получается путем сдвига каждой последующей строки таблицы умножения на одну позицию влево относительно каждой предыдущей строки. Одновременно рассмотрим табл. 2.6, в которой индексы базисных единиц также циклически сдвинуты на одну позицию вправо. На основе табл. 2.5 построим четыре 0,1-матрицы. Непосредственным перемножением легко убеждаемся, что в отношении этих матриц действует закон умножения, выраженный табл. 2.5:

$$i_0 = i_1 \times i_3 = 1, \quad i_3 = i_1 \times i_2 = -i \quad \text{и т. д.}$$

Таблица 2.5

	i_0	i_1	i_2	i_3
i_0	i_0	i_1	i_2	i_3
i_1	i_1	i_2	i_3	i_0
i_2	i_2	i_3	i_0	i_1
i_3	i_3	i_0	i_1	i_2

Таблица 2.6

	i_0	i_1	i_2	i_3
i_0	i_0	i_1	i_2	i_3
i_1	i_3	i_0	i_1	i_2
i_2	i_2	i_3	i_0	i_1
i_3	i_1	i_2	i_3	i_0

$$i_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad i_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad i_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad i_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \quad (2.17)$$

Обобщенным комплексным числом x будем называть матрицу размером 4×4 :

$$x = x_0 i_0 + x_1 i_1 + x_2 i_2 + x_3 i_3 = \begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ x_3 & x_0 & x_1 & x_2 \\ x_2 & x_3 & x_0 & x_1 \\ x_1 & x_2 & x_3 & x_0 \end{pmatrix}. \quad (2.18)$$

Формула умножения двух обобщенных комплексных чисел x и y вытекает из перемножения двух матриц вида (2.18):

$$xy = \begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ x_3 & x_0 & x_1 & x_2 \\ x_2 & x_3 & x_0 & x_1 \\ x_1 & x_2 & x_3 & x_0 \end{pmatrix} \begin{pmatrix} y_0 & y_1 & y_2 & y_3 \\ y_3 & y_0 & y_1 & y_2 \\ y_2 & y_3 & y_0 & y_1 \\ y_1 & y_2 & y_3 & y_0 \end{pmatrix} = \quad (2.19)$$

$$= (x_0 y_0 + x_1 y_3 + x_2 y_2 + x_3 y_1) i_0 + (x_0 y_1 + x_1 y_0 + x_2 y_3 + x_3 y_2) i_1 +$$

$$+ (x_0 y_2 + x_1 y_1 + x_2 y_0 + x_3 y_3) i_2 + (x_0 y_3 + x_1 y_2 + x_2 y_1 + x_3 y_0) i_3.$$

При перемножении обобщенных комплексных чисел положительные и отрицательные компоненты результирующего числа не перемешиваются. Если принять обычные действия в отношении положительных и отрицательных единиц, которые мы обозначим как j_0 и j_1 , то из (2.19) получим:

$$(x_0 y_0 + x_1 y_3 + x_2 y_2 + x_3 y_1) j_0 + (x_0 y_1 + x_1 y_0 + x_2 y_3 + x_3 y_2) j_1 +$$

$$+ (x_0 y_2 + x_1 y_1 + x_2 y_0 + x_3 y_3) j_0 - (x_0 y_3 + x_1 y_2 + x_2 y_1 + x_3 y_0) j_1 = \quad (2.20)$$

$$= [(x_0 - x_2)(y_0 - y_2) - (x_1 - x_3)(y_1 - y_3)] j_0 +$$

$$+ [(x_0 - x_2)(y_1 - y_3) + (x_1 - x_3)(y_0 - y_2)] j_1.$$

Введя новые обозначения для координат традиционных комплексных чисел a и b , образованных на базисе j_0 и j_1 , будем иметь знакомую нам со школы формулу умножения. Итак, обозначим

$$a_0 = x_0 - x_2, \quad a_1 = x_1 - x_3, \quad b_0 = y_0 - y_2, \quad b_1 = y_1 - y_3,$$

тогда из (2.20) имеем

$$(a_0 b_0 - a_1 b_1) j_0 + (a_0 b_1 + a_1 b_0) j_1 = (a_0 j_0 + a_1 j_1)(b_0 j_0 + b_1 j_1) = ab. \quad (2.21)$$

Из равенств (2.18)–(2.21) вытекает возможность представления в матричной форме действий над комплексными числами. Возьмем для примера два конкретных комплексных числа a и b ; их произведение дает число c в соответствии с традиционной формулой:

$$ab = (-3 + i)(1 - 2i) = -1 + 7i = c.$$

В матричном представлении будем иметь:

$$ab = \begin{pmatrix} 0 & 1 & 3 & 0 \\ 0 & 0 & 1 & 3 \\ 3 & 0 & 0 & 1 \\ 1 & 3 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 2 \\ 2 & 1 & 0 & 0 \\ 0 & 2 & 1 & 0 \\ 0 & 0 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 7 & 3 & 0 \\ 0 & 2 & 7 & 3 \\ 3 & 0 & 2 & 7 \\ 7 & 3 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 7 & 1 & 0 \\ 0 & 0 & 7 & 1 \\ 1 & 0 & 0 & 7 \\ 7 & 1 & 0 & 0 \end{pmatrix} = c.$$

Здесь для числа c положительное и отрицательное матричные числа вычитались, т.е. $2 - 3 = -1$. При перемножении же обобщенных комплексных чисел x и y , как уже было сказано, отрицательные и положительные компоненты не будут перемешиваться, как того требует формула (2.19):

$$xy = (1i_0 + 3i_1 + 4i_2 + 2i_3)(2i_0 + 3i_1 - 1i_2 + 5i_3) = (27i_0 + 31i_1 + 28i_2 + 24i_3) = \\ = \begin{pmatrix} 1 & 3 & 4 & 2 \\ 2 & 1 & 3 & 4 \\ 4 & 2 & 1 & 3 \\ 3 & 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 & 1 & 5 \\ 5 & 2 & 3 & 1 \\ 1 & 5 & 2 & 3 \\ 3 & 1 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 27 & 31 & 28 & 24 \\ 24 & 27 & 31 & 28 \\ 28 & 24 & 27 & 31 \\ 31 & 28 & 24 & 27 \end{pmatrix} = z.$$

Геометрический смысл умножения двух комплексных чисел хорошо известен – это поворот в комплексной плоскости. «Вращательность» числам сообщается за счет цикличности базиса (см. табл. 2.2), которая проявляется еще и в том, что последовательное возведение в степень мнимой единицы даст все четыре типа единиц:

$$i^1 = i, \quad i^2 = -1, \quad i^3 = -i, \quad i^4 = i^0 = 1. \quad (2.22)$$

Мнимая единица называется *образующей циклического базиса* комплексного числа. Любые четыре 0,1-матрицы, обладающие свойством цикличности в смысле (2.22), будут давать изоморфные структуры. В частности, 0,1-матрицы вида:

$$i_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e, \quad i_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = i, \\ i_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -e, \quad i_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -i \quad (2.23)$$

при перемножении дадут табл. 2.5.

Базис (2.23) *подобен* базису (2.17), т.е. одни матрицы можно получить из других путем перестановки 2-го и 3-го столбцов и соответствующих строк с одновременным переобозначением базисных единиц табл. 2.6. Эту процедуру, одна-

ко, легко можно осуществить и с помощью трансформационной матрицы T , которая участвует в преобразовании подобия (2.8), для i_1 будем иметь

$$i_1 = T^{-1} \times i_1' \times T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Матрицы T и T^{-1} одинаковы, так как они ортонормированы и симметричны.

Два базиса 0,1-матриц (2.17) и (2.23) образуют изоморфные циклические группы, поскольку имеют одну и ту же таблицу умножения (табл. 2.5). Положительная (+1) и отрицательная (−1) единицы и соответствующие им 0,1-матрицы (2.16) также составляют изоморфные группы из двух элементов. Можно сконструировать такую систему «комплексных» чисел, базис которых будет обладать свойством цикличности, но с периодом равным не 4, а 3, 5, 6, 7, 8 и т.д. Все они будут группами. Соответствующие таблицы циклических сдвигов на позицию влево и на позицию вправо с периодом равным 6 представлены табл. 2.7 и табл. 2.8, в которых выписаны только индексы базисных единиц, так как именно они несут всю информацию о строении группы. Вид обобщенного комплексного числа на базе шести единиц и формула их перемножения аналогичны выражениям (2.18) и (2.19); ничего принципиально нового в них не будет.

Таблица 2.7

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

Таблица 2.8

0	1	2	3	4	5
5	0	1	2	3	4
4	5	0	1	2	3
3	4	5	0	1	2
2	3	4	5	0	1
1	2	3	4	5	0

Базисная 0,1-матрица отрицательного числа получалась путем удвоения размерности базисной 0,1-матрицы положительного числа. Комплексное число получилось за счет удвоения совокупности положительного и отрицательного чисел, что можно представить формулой:

$$x = [x_0 \ e + x_1 \ (-e)] + [x_2 \ e + x_3 \ (-e)] \ i.$$

Теперь рассмотрим гиперкомплексное число, которое называется кватернионом и которое получается путем удвоения комплексного числа:

$$\begin{aligned} x = & \{[x_0 \ e + x_1 \ (-e)] + [x_2 \ e + x_3 \ (-e)] \ i\} + \{[x_4 \ e + x_5 \ (-e)] + \\ & + [x_6 \ e + x_7 \ (-e)] \ i\} \ j = x_0 \ e + x_1 \ (-e) + x_2 \ i + x_3 \ (-i) + \\ & + x_4 \ j + x_5 \ (-j) + x_6 \ k + x_7 \ (-k). \end{aligned}$$

Приведем таблицу умножения (табл. 2.9) и таблицу базисных единиц (табл. 2.10) кватерниона. Сравнивая обе таблицы, можно заметить, что они отличаются друг от друга только порядком строк. Отсюда вывод: для построения

таблицы базисных 0,1-матриц необходимо строки таблицы умножения упорядочить так, чтобы все ее тождественные элементы оказались на главной диагонали.

На основе табл. 2.10 можно выписать полную систему базисных единиц кватерниона. В частности, для базисной единицы k 0,1-матрица выглядит следующим образом:

$$k = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Аналогично сворачиваются все остальные базисные единицы. Полная система базисных единиц на свернутых 0,1-матрицах кватерниона имеет вид:

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad -e = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad i = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \quad -i = \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix},$$

$$j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad -j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad -k = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

Таблица 2.9

e	$-e$	i	$-i$	j	$-j$	k	$-k$
$-e$	e	$-i$	i	$-j$	j	$-k$	k
i	$-i$	$-e$	e	k	$-k$	$-j$	j
$-i$	i	e	$-e$	$-k$	k	j	$-j$
j	$-j$	k	$-k$	$-e$	e	i	$-i$
$-j$	j	$-k$	k	e	$-e$	$-i$	i
k	$-k$	j	$-j$	$-i$	i	$-e$	e
$-k$	k	$-j$	j	i	$-i$	e	$-e$

Таблица 2.10

e	$-e$	i	$-i$	j	$-j$	k	$-k$
$-e$	e	$-i$	i	$-j$	j	$-k$	k
$-i$	i	$-e$	e	$-k$	k	$-j$	j
i	$-i$	e	$-e$	k	$-k$	j	$-j$
$-j$	j	k	$-k$	$-e$	e	$-i$	i
j	$-j$	$-k$	k	e	$-e$	i	$-i$
$-k$	k	$-j$	j	$-i$	i	$-e$	e
k	$-k$	j	$-j$	i	$-i$	e	$-e$

Приведенные матрицы образуют антикоммутативную группу, так как, согласно табл. 2.9, имеем:

$$ij = k, \quad ji = -k, \quad jk = i, \quad kj = -i, \quad ik = -j, \quad ki = j.$$

Приведем обобщенную формулу перемножения двух кватернионов x и y , по которой отрицательные и положительные компоненты числового агрегата уже не перемещаются:

$$(x_0y_0 + x_1y_1 + x_2y_3 + x_3y_2 + x_4y_5 + x_5y_4 + x_6y_7 + x_7y_6) \times e +$$

$$+ (x_0y_1 + x_1y_0 + x_2y_0 + x_3y_3 + x_4y_4 + x_5y_5 + x_6y_6 + x_7y_7) \times (-e) +$$

$$+ (x_0y_2 + x_1y_3 + x_2y_0 + x_3y_1 + x_4y_6 + x_5y_7 + x_6y_5 + x_7y_4) \times i +$$

$$+ (x_0y_3 + x_1y_2 + x_2y_1 + x_3y_0 + x_4y_7 + x_5y_6 + x_6y_4 + x_7y_5) \times (-i) +$$

$$+ (x_0y_4 + x_1y_5 + x_2y_7 + x_3y_6 + x_4y_0 + x_5y_1 + x_6y_2 + x_7y_3) \times j +$$

$$\begin{aligned}
& + (x_0y_5 + x_1y_4 + x_2y_6 + x_3y_7 + x_4y_1 + x_5y_0 + x_6y_3 + x_7y_2) \times (-j) + \\
& + (x_0y_6 + x_1y_7 + x_2y_4 + x_3y_5 + x_4y_3 + x_5y_2 + x_6y_0 + x_7y_1) \times k + \\
& + (x_0y_7 + x_1y_6 + x_2y_5 + x_3y_4 + x_4y_2 + x_5y_3 + x_6y_1 + x_7y_0) \times (-k) .
\end{aligned}$$

Удвоение комплексного числа можно понимать иначе, а именно, как удвоение длины цикла с 4 до 8. Тогда новое гиперкомплексное число будет иметь таблицу умножения в виде табл. 2.11.

Таблица 2.11

<i>e</i>	<i>-e</i>	<i>i</i>	<i>-i</i>	<i>j</i>	<i>-j</i>	<i>k</i>	<i>-k</i>
<i>-e</i>	<i>e</i>	<i>-i</i>	<i>i</i>	<i>-j</i>	<i>j</i>	<i>-k</i>	<i>k</i>
<i>i</i>	<i>-i</i>	<i>-e</i>	<i>e</i>	<i>k</i>	<i>-k</i>	<i>-j</i>	<i>j</i>
<i>-i</i>	<i>i</i>	<i>e</i>	<i>-e</i>	<i>-k</i>	<i>k</i>	<i>j</i>	<i>-j</i>
<i>j</i>	<i>-j</i>	<i>k</i>	<i>-k</i>	<i>i</i>	<i>-i</i>	<i>-e</i>	<i>e</i>
<i>-j</i>	<i>j</i>	<i>-k</i>	<i>k</i>	<i>-i</i>	<i>i</i>	<i>e</i>	<i>-e</i>
<i>k</i>	<i>-k</i>	<i>-j</i>	<i>j</i>	<i>-e</i>	<i>e</i>	<i>-i</i>	<i>i</i>
<i>-k</i>	<i>k</i>	<i>j</i>	<i>-j</i>	<i>e</i>	<i>-e</i>	<i>i</i>	<i>-i</i>

Последняя таблица умножения симметрична относительно главной диагонали, в отличие от предыдущего случая. Это значит, что умножение двух гиперкомплексных чисел, построенных на базисных единицах табл. 2.7, будет уже коммутативным.

Две следующие группы базисных единиц –

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & i \end{pmatrix}$$

и

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

изоморфны между собой, в чем можно убедиться, если составить для них таблицы умножения, сохранив при этом приведенный порядок элементов. Далее, если оба ряда матриц перемножить между собой, возникнут еще четыре матрицы:

$$\begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -1 \end{pmatrix}.$$

Объединив эти матрицы с двумя предыдущими рядами, получим новый коммутативный базис из 16 различных матриц.

Процедуру удвоения элементов группы можно продолжить, например, и так: удвоенные базисные единицы кватерниона –

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} j & 0 \\ 0 & j \end{pmatrix}, \begin{pmatrix} -j & 0 \\ 0 & -j \end{pmatrix}, \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}, \begin{pmatrix} -k & 0 \\ 0 & -k \end{pmatrix}$$

дополнить либо матрицами вида:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \begin{pmatrix} 0 & j \\ j & 0 \end{pmatrix}, \begin{pmatrix} 0 & -j \\ -j & 0 \end{pmatrix}, \begin{pmatrix} 0 & k \\ k & 0 \end{pmatrix}, \begin{pmatrix} 0 & -k \\ -k & 0 \end{pmatrix},$$

либо другими матрицами --

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} j & 0 \\ 0 & -j \end{pmatrix}, \begin{pmatrix} -j & 0 \\ 0 & j \end{pmatrix}, \begin{pmatrix} k & 0 \\ 0 & -k \end{pmatrix}, \begin{pmatrix} -k & 0 \\ 0 & k \end{pmatrix}.$$

В обоих случаях получается уже *некоммутативный* базис из 16 матриц.

Обратимся к вопросу о *собственных значениях*. Ранее мы показали, что всякую матрицу z вида:

$$z = \begin{pmatrix} x & -y \\ y & x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} x + \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} y = x + iy$$

можно рассматривать в качестве комплексного числа. Несложно подобрать для z такую трансформационную матрицу T , чтобы с ее помощью можно было осуществить преобразование подобия, результатом которого были бы собственные значения --

$$\Lambda = T^{-1} z T = \begin{pmatrix} 1/\sqrt{2} & i/\sqrt{2} \\ i/\sqrt{2} & 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ -i/\sqrt{2} & i/\sqrt{2} \end{pmatrix} = \begin{pmatrix} x-iy & 0 \\ 0 & x+iy \end{pmatrix}.$$

Аналогичного результата можно добиться, если для матрицы z составить характеристический определитель и затем отыскать корни характеристического уравнения. Для определителя размерности 2×2 действует простая формула, которая приводит к предыдущему результату:

$$\lambda_{1,2} = \frac{a_{11} + a_{22}}{2} \pm \sqrt{\frac{(a_{11} - a_{22})^2}{4} - a_{12}a_{21}} = x \pm iy.$$

Сейчас мы укажем еще один способ нахождения собственных значений. Для этого с помощью замены (2.16) увеличим матрицу z размерности 2×2 до размерности 8×8 , при этом все x снабдим индексами, чтобы можно было видеть, каким образом следует производить перестановку строк и столбцов для получения нужной нам структуры:

$$z = \begin{pmatrix} x_1 & 0 & 0 & 0 & 0 & 0 & y & 0 \\ 0 & x_2 & 0 & 0 & 0 & 0 & 0 & y \\ 0 & 0 & x_3 & 0 & y & 0 & 0 & 0 \\ 0 & 0 & 0 & x_4 & 0 & y & 0 & 0 \\ y & 0 & 0 & 0 & x_5 & 0 & 0 & 0 \\ 0 & y & 0 & 0 & 0 & x_6 & 0 & 0 \\ 0 & 0 & y & 0 & 0 & 0 & x_7 & 0 \\ 0 & 0 & 0 & y & 0 & 0 & 0 & x_8 \end{pmatrix} = \begin{pmatrix} x_1 & 0 & 0 & y & 0 & 0 & 0 & 0 \\ 0 & x_3 & y & 0 & 0 & 0 & 0 & 0 \\ y & 0 & x_5 & 0 & 0 & 0 & 0 & 0 \\ 0 & y & 0 & x_7 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & x_4 & 0 & y & 0 \\ 0 & 0 & 0 & 0 & 0 & x_2 & 0 & y \\ 0 & 0 & 0 & 0 & 0 & y & x_6 & 0 \\ 0 & 0 & 0 & 0 & y & 0 & 0 & x_8 \end{pmatrix} = \begin{pmatrix} x+iy & 0 \\ 0 & x-iy \end{pmatrix}.$$

Собственными значениями 0,1-матриц являются корни n -ой степени из единицы. Если какая-либо 0,1-матрица a обращается в единичную матрицу e при показателе степени, равным, скажем, четырём, то собственными значениями матрицы a будут четыре корня из единицы. Матрицы, обладающие одинаковыми наборами собственных значений, подобны между собой, причем они образуют *абсолютные* классы эквивалентности, хотя сами матрицы могут быть элементами коммутативных групп, где каждый элемент, как известно, образует свой *относительный* класс эквивалентности. Приведем несколько базисных 0,1-мат-

риц и рядом с ними выпишем наборы их собственных значений:

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} -1 \\ +1 \\ +1 \\ -1 \end{matrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ +1 \\ -1 \\ +1 \end{matrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} -1 \\ -i \\ -i \\ +1 \end{matrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ -i \\ -i \\ +1 \end{matrix},$$

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{matrix} -1 \\ +i \\ -i \\ +1 \\ -1 \\ -i \\ i \\ +1 \end{matrix}, \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} -1 \\ -\frac{1}{\sqrt{2}}(1-i) \\ -\frac{1}{\sqrt{2}}(1+i) \\ -i \\ -i \\ +1 \\ \frac{1}{\sqrt{2}}(1+i) \\ \frac{1}{\sqrt{2}}(1-i) \end{matrix}.$$

Таким образом, наборы собственных значений базисных 0,1-матриц однозначно характеризуют *периодичность* матрицы.

На основе замены (2.16) можно получить многие важные математические результаты, которые, быть может, непосредственно и не связаны с группами. Так, легко показать, что матрицы вида —

$$\begin{pmatrix} a & ic \\ -ic & b \end{pmatrix}, \begin{pmatrix} a & c \\ c & b \end{pmatrix}, \begin{pmatrix} a & -c \\ -c & b \end{pmatrix}$$

имеют одинаковые наборы собственных значений, поскольку все три матрицы после разворачивания и соответствующей перестановки диагональных элементов обнаруживают свою идентичность:

$$\begin{pmatrix} a_1 & 0 & 0 & 0 & 0 & 0 & c & 0 \\ 0 & a_2 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 0 & a_3 & 0 & 0 & c & 0 & 0 \\ 0 & 0 & 0 & a_4 & c & 0 & 0 & 0 \\ 0 & 0 & 0 & c & b_1 & 0 & 0 & 0 \\ 0 & 0 & c & 0 & 0 & b_2 & 0 & 0 \\ c & 0 & 0 & 0 & 0 & 0 & b_3 & 0 \\ 0 & c & 0 & 0 & 0 & 0 & 0 & b_4 \end{pmatrix} \begin{pmatrix} a_1 & 0 & 0 & 0 & c & 0 & 0 & 0 \\ 0 & a_2 & 0 & 0 & 0 & c & 0 & 0 \\ 0 & 0 & a_3 & 0 & 0 & 0 & c & 0 \\ 0 & 0 & 0 & a_4 & 0 & 0 & 0 & c \\ c & 0 & 0 & 0 & b_1 & 0 & 0 & 0 \\ 0 & c & 0 & 0 & 0 & b_2 & 0 & 0 \\ 0 & 0 & c & 0 & 0 & 0 & b_3 & 0 \\ 0 & 0 & 0 & c & 0 & 0 & 0 & b_4 \end{pmatrix} \begin{pmatrix} a_3 & 0 & 0 & 0 & 0 & c & 0 & 0 \\ 0 & a_4 & 0 & 0 & c & 0 & 0 & 0 \\ 0 & 0 & a_1 & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & a_2 & 0 & 0 & c & 0 \\ 0 & c & 0 & 0 & b_1 & 0 & 0 & 0 \\ c & 0 & 0 & 0 & 0 & b_2 & 0 & 0 \\ 0 & 0 & 0 & c & 0 & 0 & b_3 & 0 \\ 0 & 0 & c & 0 & 0 & 0 & 0 & b_4 \end{pmatrix}$$

Несложно убедиться в справедливости цепи эквивалентных числовых матриц:

$$\begin{pmatrix} 4 & 2i \\ -2i & 7 \end{pmatrix} \approx \begin{pmatrix} 4 & 2 \\ 2 & 7 \end{pmatrix} \approx \begin{pmatrix} 4 & 2 \\ -2 & 7 \end{pmatrix} \approx \begin{pmatrix} 55+2.5i & 0 \\ 0 & 55-2.5i \end{pmatrix}.$$

Все только что полученные результаты распространяются на матрицы больших размерностей. Кроме того, следует иметь в виду, что любую *эрмитову матрицу* (H) можно представить комплексным числом из матриц симметричной (S) и кососимметричной (K) структуры:

$$H = S + iK = \begin{pmatrix} S & -K \\ K & S \end{pmatrix}.$$

Завершим этот раздел двумя нетривиальными примерами.

Пример 1. Перемножим две матрицы A и B с вещественными, в том числе и отрицательными, матричными элементами. Далее, используя замену (2.16), развернем матрицы A и B до матриц A_1 и B_1 и вновь их перемножим. Для всех результирующих матриц C , C_1 и C_2 найдем собственные значения, которые выпишем в табл. 2.12.

$$C = A \cdot B = \begin{pmatrix} 7.3 & -4.5 & 3.1 \\ 0.5 & 8.2 & -5.9 \\ 3.4 & -2.7 & -6.3 \end{pmatrix} \begin{pmatrix} 1.8 & 4.4 & 5.9 \\ 3.7 & 1.1 & -7.6 \\ -2.5 & -6.4 & 8.7 \end{pmatrix} = \begin{pmatrix} 11.26 & -56.91 & 18.10 \\ 45.99 & 44.58 & -116.6 \\ 11.88 & 22.39 & -54.35 \end{pmatrix}$$

$$C_1 = A_1 \cdot B_1 = \begin{pmatrix} 7.3 & 0.0 & 0.0 & 4.5 & 3.1 & 0.0 \\ 0.0 & 7.3 & 4.5 & 0.0 & 0.0 & 3.1 \\ 0.5 & 0.0 & 8.2 & 0.0 & 0.0 & 5.9 \\ 0.0 & 0.5 & 0.0 & 8.2 & 5.9 & 0.0 \\ 3.4 & 0.0 & 0.0 & 2.7 & 0.0 & 6.3 \\ 0.0 & 3.4 & 2.7 & 0.0 & 6.3 & 0.0 \end{pmatrix} \begin{pmatrix} 1.8 & 0.0 & 0.0 & 4.4 & 0.0 & 5.9 \\ 0.0 & 1.8 & 4.4 & 0.0 & 5.9 & 0.0 \\ 3.7 & 0.0 & 1.1 & 0.0 & 0.0 & 7.6 \\ 0.0 & 3.7 & 0.0 & 1.1 & 7.6 & 0.0 \\ 0.0 & 2.5 & 0.0 & 6.4 & 8.7 & 0.0 \\ 2.5 & 0.0 & 6.4 & 0.0 & 0.0 & 8.7 \end{pmatrix} =$$

$$= \begin{pmatrix} 13.14 & 24.40 & 0.0 & 56.91 & 61.17 & 43.07 \\ 24.40 & 13.14 & 56.91 & 0.0 & 43.07 & 61.17 \\ 45.99 & 0.0 & 46.78 & 2.2 & 0.0 & 116.6 \\ 0.0 & 45.99 & 2.2 & 46.78 & 116.6 & 0.0 \\ 21.87 & 9.99 & 40.32 & 7.93 & 20.52 & 74.87 \\ 9.99 & 21.87 & 7.93 & 40.32 & 74.87 & 20.52 \end{pmatrix} \quad C_2 = \begin{pmatrix} 0.0 & 11.26 & 0.0 & 56.91 & 18.10 & 0.0 \\ 11.26 & 0.0 & 56.91 & 0.0 & 0.0 & 18.10 \\ 45.99 & 0.0 & 44.58 & 0.0 & 0.0 & 116.6 \\ 0.0 & 45.99 & 0.0 & 44.58 & 116.6 & 0.0 \\ 11.88 & 0.0 & 22.39 & 0.0 & 0.0 & 54.35 \\ 0.0 & 11.88 & 0.0 & 22.39 & 54.35 & 0.0 \end{pmatrix}$$

Таблица 2.12

Собст. значения C	Собст. значения C_1	Собст. значения C_2
$-0.0481 + 51.9424 i$	$-0.0481 + 51.9424 i$	$-0.0481 + 51.9424 i$
$-0.0481 - 51.9424 i$	$-0.0481 - 51.9424 i$	$-0.0481 - 51.9424 i$
-20.9338	20.9338	-20.9338
$-$	195.3817	122.02
$-$	0.4562	16.3986
$-$	-13.9279	-28.2267

Комментарий к примеру 1. Процедура умножения матриц A на B и A_1 на B_1 дала почти один и тот же результат: матрицы C , C_1 и C_2 эквивалентны, на что указывает наличие в их собственных значениях трех одинаковых чисел. Однако есть и не эквивалентная компонента. Это связано с тем, что развернутые матрицы C_1 и C_2 несут более обширную информацию, чем матрица C . Поэтому мы говорим, что матрицы C_1 и C_2 подобны (гомоморфны) C .

Пример 2. Пусть дана эрмитова матрица H ; найдем ее собственные значения Λ . Затем комплексную матрицу H развернем в вещественную матрицу H_1 с отрицательными элементами и снова найдем собственные значения Λ_1 . Наконец, найдем собственные значения Λ_2 матрицы H_2 с положительными элементами, полученными по формуле (2.17).

$$H = \begin{pmatrix} 1.3 & 4.2 - 3.7i & 0.8i \\ 4.2 + 3.7i & -7.6 & 3.6 - 7.5i \\ 0.8i & 3.6 + 7.5i & 4.9 \end{pmatrix}, \quad \Lambda = \begin{pmatrix} -13.69 & 0.0 & 0.0 \\ 0.0 & 2.75 & 0.0 \\ 0.0 & 0.0 & 9.54 \end{pmatrix},$$

$$H_1 = \begin{pmatrix} 1.3 & 4.2 & 0.0 & 0.0 & 3.7 & -0.8 \\ 4.2 & 7.6 & 3.6 & -3.7 & 0.0 & 7.5 \\ 0.0 & 3.6 & 4.9 & 0.8 & -7.5 & 0.0 \\ 0.0 & 3.7 & 0.8 & 1.3 & 4.2 & 0.0 \\ 3.7 & 0.0 & -7.5 & 4.2 & -7.6 & 3.6 \\ -0.8 & 7.5 & 0.0 & 0.0 & 3.6 & 4.9 \end{pmatrix}, \quad \Lambda_1 = \begin{pmatrix} 2.75 & 0.0 & 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 2.75 & 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0 & 9.54 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.0 & 9.54 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.0 & 0.0 & -13.69 & 0.0 \\ 0.0 & 0.0 & 0.0 & 0.0 & 0.0 & -13.69 \end{pmatrix},$$

$$H_2 = \begin{pmatrix} 1.3 & 0.0 & 0.0 & 0.0 & 4.2 & 0.0 & 0.0 & 3.7 & 0.0 & 0.8 & 0.0 & 0.0 \\ 0.0 & 1.3 & 0.0 & 0.0 & 3.7 & 4.2 & 0.0 & 0.0 & 0.0 & 0.0 & 0.8 & 0.0 \\ 0.0 & 0.0 & 1.3 & 0.0 & 0.0 & 3.7 & 4.2 & 0.0 & 0.0 & 0.0 & 0.0 & 0.8 \\ 0.0 & 0.0 & 0.0 & 1.3 & 0.0 & 0.0 & 3.7 & 4.2 & 0.8 & 0.0 & 0.0 & 0.0 \\ 4.2 & 3.7 & 0.0 & 0.0 & 0.0 & 0.0 & 7.6 & 0.0 & 3.6 & 0.0 & 0.0 & 7.5 \\ 0.0 & 4.2 & 3.7 & 0.0 & 0.0 & 0.0 & 0.0 & 7.6 & 7.5 & 3.6 & 0.0 & 0.0 \\ 0.0 & 0.0 & 4.2 & 3.7 & 7.6 & 0.0 & 0.0 & 0.0 & 0.0 & 7.5 & 3.6 & 0.0 \\ 3.7 & 0.0 & 0.0 & 4.2 & 0.0 & 7.6 & 0.0 & 0.0 & 0.0 & 0.0 & 7.5 & 3.6 \\ 0.0 & 0.0 & 0.0 & 0.8 & 3.6 & 7.5 & 0.0 & 0.0 & 4.9 & 0.0 & 0.0 & 0.0 \\ 0.8 & 0.0 & 0.0 & 0.0 & 0.0 & 3.6 & 7.5 & 0.0 & 0.0 & 4.9 & 0.0 & 0.0 \\ 0.0 & 0.8 & 0.0 & 0.0 & 0.0 & 0.0 & 3.6 & 7.5 & 0.0 & 0.0 & 4.9 & 0.0 \\ 0.0 & 0.0 & 0.8 & 0.0 & 7.5 & 0.0 & 0.0 & 3.6 & 0.0 & 0.0 & 0.0 & 4.9 \end{pmatrix}.$$

Собственные значения равны:

$$2.75, 2.75, 9.54, 9.54, -13.69, -13.69, 2.25, 1.82, 1.09, 10.46, -7.81, 19.79.$$

Комментарий к примеру 2. Если бы мы применительно к H_1 воспользовались заменой (2.16) вместо (2.17), то у вновь получившейся матрицы были бы точно такие же собственные значения, что и у матрицы H_2 . Это говорит о том, что для нахождения собственных значений важна именно связь диагональных элементов с недиагональными.

При переходе от матрицы H к матрице H_1 собственные значения просто удвоились, а при переходе от H_1 к H_2 добавились шесть различных вещественных значений. В *примере 1* дополнительные собственные значения также появились за счет структурной перестройки матриц, которая привела к положительным матричным элементам. Таким образом, требование о недопустимости смещения положительных и отрицательных чисел породило неэквивалентную процедуру. Здесь матрица H_1 *изоморфна* исходной матрице H , тогда как матрица H_2 только *гомоморфна* H .

2.3. Подстановки

Комплексное число есть двухкоординатный *вектор*, кватернион — четырехкоординатный и т.д. В предыдущем разделе мы рассматривали базисные 0, 1-матрицы, которые не дают смешиваться различным координатам числовых агрегатов и одновременно задают закон перемножения для их базисных единиц. Однако группы 0, 1-матриц образуют все же *операционные* множества. Соответствующим *субстанционным* множеством для них служат 0, 1-векторы-столбцы, о которых ниче-

го не было сказано. Между тем, для 0,1-матриц комплексного числа (2.17) в качестве базиса могут выступать, например, первые столбцы этих матриц. Мы не станем оперировать этими 0,1-векторами, а прибегнем к более эффективной методике, введя в обращение новый математический объект — *подстановки*.

Всякая 0,1-матрица переставляет числа в векторе-столбце, который нумерует строки этой матрицы. Например, для базисных единиц комплексного числа i_1 и i_2 , имеем:

$$i_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 0 \end{pmatrix}, \quad i_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 0 \\ 1 \end{pmatrix}.$$

Следовательно, любой 0,1-матрице можно поставить в соответствие двухрядную таблицу; в нашем случае это —

$$i_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix}, \quad i_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}.$$

Такие двухрядные таблицы и называются *подстановками* (алгебраический термин) или *перестановками* (комбинаторный термин, которым мы преимущественно пользоваться не будем).

Подстановки удивительным образом соединяют в себе *операционную* и *субстанционную* сущность линейных преобразований, ранее представленных матрицами и векторами. За субстанционное множество следует принять *индексы* подстановок, т.е. числа $\{0, 1, 2, 3\}$, а за операционное — сами подстановки, переставляющие эти индексы. В общем случае *число субстанционных элементов группы не совпадает с операционным*, но можно добиться того, чтобы оба множества имели одинаковое число элементов. Для этого нужно составить таблицу умножения, и затем по столбцам (так мы будем поступать в дальнейшем, хотя ничто не мешает эту процедуру проводить по строкам) выписать так называемые *регулярные подстановки*. Покажем, как это делается. Пусть дана таблица перемножения индексов (субстанционное множество), которые в этом случае являются одновременно и элементами группы (операционным множеством) — табл. 2.13. Тогда искомая группа G регулярных подстановок, отвечающая столбцам табл. 2.13, выглядит следующим образом:

$$\begin{aligned} 0 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}, & 1 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 \end{pmatrix}, \\ 2 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 \end{pmatrix}, & 3 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 \end{pmatrix}, \\ 4 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 7 & 2 & 3 & 0 & 1 \end{pmatrix}, & 5 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 7 & 6 & 3 & 2 & 1 & 0 \end{pmatrix}, \\ 6 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 4 & 5 & 0 & 1 & 2 & 3 \end{pmatrix}, & 7 &= \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 4 & 1 & 0 & 3 & 2 \end{pmatrix}. \end{aligned}$$

Таблица 2.13

0	1	2	3	4	5	6	7
1	0	3	2	5	4	7	6
2	3	0	1	6	7	4	5
3	2	1	0	7	6	5	4
4	5	6	7	2	3	0	1
5	4	7	6	3	2	1	0
6	7	4	5	0	1	2	3
7	6	5	4	1	0	3	2

Подстановки имеют ряд очевидных достоинств перед 0,1-матрицами: во-первых, они менее громоздки, во-вторых, их проще перемножать, в-третьих, существует специальная запись подстановок, при которой сразу можно определить их степень периодичности. И это при том, что имеется теорема Кэли, утверждающая, что не существует такой группы, которую нельзя было бы представить подстановками.

Покажем, как производится перемножение подстановок на примере умножения базисных единиц комплексного числа i_1 и i_2 . С этой целью проследим переход индексов от одной подстановки к другой. Индекс 0 подстановки i_1 переходит в 1, а 1 подстановки i_2 переходит в 3; следовательно, в результирующей подстановке i_3 0 будет переходить сразу в 3. Затем смотрим, во что переходит 1: $1 \rightarrow 2 \rightarrow 0$, значит, для i_3 индекс 1 перейдет в 0. Далее, $2 \rightarrow 3 \rightarrow 1$ и $3 \rightarrow 0 \rightarrow 2$, отсюда $2 \rightarrow 1$ и $3 \rightarrow 2$. В итоге получим подстановку i_3 следующего вида:

$$i_1 \times i_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 1 & 2 \end{pmatrix} = i_3.$$

Перемножая всеми возможными способами регулярные подстановки группы G , убеждаемся, что они дают табл. 2.13.

Легко перемножаются одновременно три или даже большее число подстановок, например:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 0 & 2 & 4 & 3 \end{pmatrix}.$$

Здесь $0 \rightarrow 2 \rightarrow 3 \rightarrow 1$, т.е. 0 в результирующей подстановке сразу переходит в 1.

Подстановка, не переставляющая ни одного индекса, называется *тождественной* (*нейтральной* или *единичной*). Она отвечает единичной матрице:

$$e = \begin{pmatrix} 0 & 1 & 2 & \dots \\ 1 & 2 & 3 & \dots \end{pmatrix}.$$

Тождественными подстановками являются i_0 в базисе комплексного числа и 0 в группе G (табл. 2.13). Две подстановки, дающие при перемножении тождественную подстановку e , называются *взаимно обратными*, в частности, таковыми являются подстановки i_1 и i_3 в базисе комплексного числа:

$$i_1 i_3 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{pmatrix} = i_0.$$

Подстановки 1, 2, 3 группы G являются взаимно обратными, а для подстановок 4, 5, 6, 7 обратными служат 6, 7, 4, 5, соответственно.

Чтобы из заданной подстановки a получить взаимно обратную a^{-1} , необходимо верхнюю строку подстановки поменять с нижней и упорядочить индексы верхней строки. Пусть

$$a = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix},$$

тогда, согласно определению, будем иметь:

$$a^{-1} = \begin{pmatrix} 0 & 4 & 1 & 3 & 2 & 6 & 5 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 2 & 4 & 3 & 1 & 6 & 5 \end{pmatrix}.$$

Внимательный анализ всех подстановок группы G подтверждает эту взаимосвязь между исходными и обратными подстановками.

Подстановки удобно записывать в *циклической форме*. При такой записи индексы, остающиеся на месте, обычно не пишутся. Так, подстановка a имеет следующие переходы индексов: $0 \rightarrow 0$, $1 \rightarrow 4 \rightarrow 2 \rightarrow 1$, $3 \rightarrow 3$, $5 \rightarrow 6 \rightarrow 5$. Следовательно, в циклической форме она запишется так:

$$a = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix} = (0)(142)(3)(56) = (0)(142)(3)(56)(7)(8) \dots = (142)(56).$$

Считается, что индексы 7, 8 и т.д. так же, как 0 и 3, неявно присутствуют в подстановке a , но тождественно переходят сами в себя. В связи с этим тождественную подстановку обозначают через единичный цикл: $e = (0)$. Регулярные подстановки группы G имеют следующий циклический вид:

$$\begin{aligned} 0 &= (0), & 2 &= (02)(13)(46)(57), & 4 &= (0426)(1537), & 6 &= (0624)(1735), \\ 1 &= (01)(23)(45)(67), & 3 &= (03)(12)(47)(56), & 5 &= (0527)(1436), & 7 &= (0725)(1634). \end{aligned}$$

Безразлично, с какой позиции записывать цикл:

$$(ij) = (ji), \quad (ijk) = (jki) = (kij), \quad (ijkl) = (jkli) = \dots,$$

поэтому

$$\begin{aligned} i_1 &= (0123) = (1230) = (2301) = (3012), \\ a &= (421)(56) = (421)(65) = (214)(56) = (214)(65), \\ 6 &= (6240)(1735) = (2406)(3517) = (4062)(3517). \end{aligned}$$

Циклы одной и той же подстановки можно переставлять, т.е. они коммутируют внутри этой подстановки:

$$\begin{aligned} (ijk)(l)(mn) &= (l)(ijk)(mn) = (mn)(jki)(l) = (nm)(kij)(l), \\ i_2 &= (02)(13) = (13)(02), & a &= (142)(56) = (56)(142), \\ 6 &= (1735)(0624), & 4 &= (3715)(4260). \end{aligned}$$

Разложению подстановки на систему *независимых* циклов отвечает разложение данной подстановки на систему коммутирующих множителей:

$$i_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 1 & 0 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 3 & 2 & 1 \end{pmatrix},$$

$$a = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 4 & 1 & 3 & 2 & 5 & 5 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 2 & 3 & 4 & 6 & 5 \end{pmatrix},$$

$$6 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 4 & 5 & 0 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 1 & 4 & 3 & 0 & 5 & 2 & 7 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 7 & 2 & 5 & 4 & 1 & 6 & 3 \end{pmatrix}.$$

Элементарная циклическая подстановка, переставляющая два любых индекса i и j называется *транспозицией*. Транспозиция обладает важным свойством: она обратна сама себе, т.е. $(ij) = (ij)^{-1}$, так как $(ij)(ij) = e$. Любую транспозицию (ij) можно представлять произведением смежных транспозиций по формуле:

$$(ij) = (j, j-1)(j-1, j-2) \dots \dots (i+2, i+1)(i, i+1)(i+1, i+2) \dots (j-2, j-1)(j-1, j); \quad (2.25)$$

например,

$$(48) = (87)(76)(65)(54)(56)(67)(78).$$

А любой цикл может быть разложен на транспозиции, причем несколькими способами:

$$(ijk) = (ij)(ik) = (jk)(ji) = (ki)(kj), \quad (2.26)$$

$$(ijkl) = (ij)(ik)(il) = (jk)(jl)(ji) = (jk)(jl)(il) = (ik)(lj) = (ik)(li)(lj) = \dots;$$

например,

$$a = (142)(56) = (14)(12)(56) = (42)(41)(56) = (21)(24)(56) = (56)(14)(12),$$

$$6 = (0624)(1735) = (06)(02)(04)(17)(13)(15) = (26)(46)(06)(35)(37)(13) = \dots$$

Справедливость формул (2.25) и (2.26) проверяется путем непосредственного перемножения смежных транспозиций.

Если дана подстановка, представленная в циклическом виде, то обратная ей ищется путем обратной записи последовательности всех ее индексов:

$$a = (ghijk)(lmn), \quad a^{-1} = (gkjih)(lnm);$$

например,

$$6 = (0624)(1735), \quad 6^{-1} = (0426)(1537) = 4.$$

Транспозиции, фигурирующие в формулах (2.25) и (2.26), *связанные*, так как имеют какой-либо общий индекс. Все связанные транспозиции не коммутируют и не могут быть переставлены местами. Если a , b и c — зависимые транспозиции, циклы или даже целые подстановки, то имеет место равенство:

$$abc = c^{-1}b^{-1}a^{-1}.$$

В частности, для связанных транспозиций имеем:

$$(ijkl)^{-1} = ((ij)(ik)(il))^{-1} = ((il)(ij)(ik))^{-1} = (il)(ik)(ij) = (lkji).$$

Более общий случай проиллюстрируем примером. Пусть дано следующее произведение подстановок:

$$x = c^{-1}a f^3 b^{-2}.$$

Чтобы найти x^{-1} , необходимо исходное выражение записать в обратном порядке с противоположными показателями степеней:

$$x^{-1} = b^2 f^{-3} a^{-1} c.$$

Правильность нахождения обратного выражения проверяется просто:

$$x x^{-1} = (c^{-1} a f^3 b^{-2})(b^{-1} f^{-3} a^{-1} c) = (c^{-1} (a (f^3 (b^{-2} b^2) f^{-3}) a^{-1}) c) = e.$$

Используя указанные свойства подстановок, записанных в циклическом виде, можно составить несколько полезных правил, которые сделают процедуру их перемножения почти механической. Вот некоторые из таких правил.

При умножении (слева или справа) смежной транспозиции на n -цикл длина последнего уменьшается на единицу и становится равной $n - 1$:

$$(abcdef...) \times (cd) = (abdef...)(c), (cd) \times (abcdef...) = (abcef...)(d);$$

в частности,

$$(325614) \times (56) = (32614)(5), (123) \times (12) = (23)(1).$$

Более общее правило звучит так: произвольная транспозиция делит цикл на два не-связанных подцикла:

$$(abcdefgh...) \times (cf) = (abfgh...)(cde), (cf) \times (abcdefgh...) = (abcfgh...)(fde);$$

в частности,

$$(1234) \times (13) = (12)(34), (13) \times (1234) = (14)(23).$$

Обратное правило, которое можно было бы назвать *правилом склейки двух циклов*, мы проиллюстрируем рисунком — рис. 2.1.

$$(vwxyz)(abcdefgh) \times (yz) = (vwxyzdefghabxyz).$$

Склеивание циклов произойдет в том случае, если в них имеются одинаковые индексы, которые удобно записать первыми — рис. 2.2.

$$(abc...) \times (aij...) \times (axy...) = (abc...ij...xy...).$$

При совпадении первых двух индексов склейки уже не получится:

$$(abcd...) \times (abij...) = (aij...) \times (bcd...).$$

Когда эти индексы в циклах переставлены местами, склейка снова возможна, но уже с выпадением одного из индексов:

$$(abcd...) \times (baij...) = (a)(bcd...ij...).$$

Можно продолжить составление подобных правил, только нужно помнить, что зачастую проще произвести непосредственное перемножение подстановок, чем пытаться вспомнить подходящее правило.

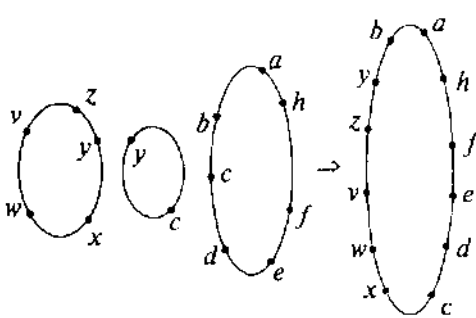


Рис. 2.1

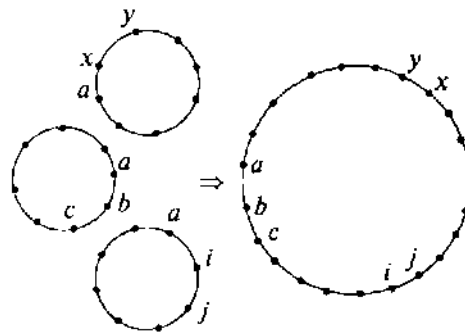


Рис. 2.2

В некоторых случаях полезными понятиями являются четность, декремент и число инверсий подстановки α . *Декрементом* (D) подстановки α называется разность между числом всех индексов (n) и количеством циклов (m), включая циклы единичной длины. *Число инверсий* (I) подсчитывается следующим образом: для каждого индекса нижней строки подстановки α определяется количество стоящих правее его меньших индексов, затем полученные результаты складываются. *Четность* подстановки α определяется четностью числа транспозиций (T), на которые можно разложить эту подстановку. Если декремент и число инверсий являются нечетными числами, то и число транспозиций также будет нечетным. Пусть задана подстановка:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 2 & 4 & 3 & 7 & 6 \end{pmatrix} = (1)(253)(4)(67) = (1)(25)(23)(4)(67).$$

В соответствии с определениями имеем:

$$T = 3, \quad D = n - m = 7 - 4 = 3, \quad I = 0 + 3 + 0 + 1 + 0 + 1 + 0 = 5.$$

К сказанному добавим: тождественная подстановка e четна, любая транспозиция — нечетна. Произведение четных подстановок и двух нечетных всегда даст четную подстановку, а умножение четной и нечетной — нечетную.

С подстановками можно встретиться и при решении задач прикладной математики, в частности, при вычислении определителей. Вспомним, как ищется определитель третьего порядка:

$$\begin{aligned} \det A &= \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \\ &= a_{11}a_{22}a_{33} + a_{13}a_{21}a_{32} + a_{12}a_{23}a_{31} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}. \end{aligned}$$

Здесь индексы представляют собой шесть подстановок третьего порядка, причем перед четными подстановками стоит плюс, а перед нечетными — минус. Аналогично будут вычисляться определители 4-го, 5-го и т.д. порядков, только число слагаемых будет равно уже 24, 120 и т.д.

Ясно, что подстановки тесно связаны с *комбинаторикой*. Первый вопрос, который здесь звучит так: сколько подстановок можно составить из n индексов? Оказывается, это число равно $n!$, т.е. равно числу *перестановок* из n индексов. Отсюда получаются числа: $3! = 6$, $4! = 24$, $5! = 120$ и т.д. Почему это именно так, понять несложно. Представим перестановку n индексов следующей подстановкой:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ i_1 & i_2 & i_3 & \dots & i_{n-1} & i_n \end{pmatrix}.$$

Первый индекс i_1 можно выбрать n различными способами. После этого выбор i_2 можно осуществить только $(n-1)$ способами; индекса $i_3 - (n-2)$ способами и т.д. Так как выбор каждого индекса i осуществляется независимо, общее число способов размещения n чисел по n позициям равно произведению:

$$n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 3 \cdot 2 \cdot 1 = n!.$$

Далее встает вопрос: сколько классов подстановок различной циклической структуры можно составить из n индексов? Ответ на этот вопрос таков: количе-

ство классов определяется числом возможных разложений n на слагаемые, причем таким образом, чтобы каждое последующее слагаемое было не больше предыдущего. В частности: при $n = 3$ имеем три способа разложения: 3, 21 и 111, так как

$$3 = 3, \quad 3 = 2 + 1, \quad 3 = 1 + 1 + 1.$$

Следовательно, может существовать три класса подстановок: (abc) , $(ab)(c)$, $(a)(b)(c)$. При $n = 5$ будет уже семь классов: 5, 41, 32, 311, 221, 2111, 11111, с подстановками вида:

$$(01234), (0123)(4), (012)(34), (034), (12)(34), (14), (0).$$

Наконец, возникает еще один вопрос комбинаторного характера: сколько подстановок содержится в классе C_r ? Для представления циклической структуры подстановок, образующих класс C_r , будем пользоваться следующей *спецификацией*:

$$C_r(k_1, k_2, \dots, k_n);$$

здесь k_1 — число 1-циклов, входящих в подстановку из класса C_r ; k_2 — число 2-циклов, ..., k_n — число n -циклов. Рассмотрим случай $n = 4$. Тогда тождественная подстановка из четырех одинарных циклов $e = (0)(1)(2)(3)$, образующая класс C_0 , будет иметь спецификацию $C_0(4, 0, 0, 0)$; подстановка $(01)(23)$ из класса C_1 имеет спецификацию $C_1(0, 2, 0, 0)$; подстановка $(0)(123)$ из класса C_2 — спецификацию $C_2(1, 0, 1, 0)$; подстановка (0123) из класса C_3 — спецификацию $C_3(0, 0, 0, 1)$; подстановка $(0)(1)(23)$ из класса C_4 — спецификацию $C_4(2, 1, 0, 0)$. Таким образом, мы перечислили все пять возможных классов для подстановок, состоящих из четырех индексов.

Так как r -цикл содержит r индексов, а всего индексов n , то для любого класса C_i справедливо равенство:

$$1 \cdot k_1 + 2 \cdot k_2 + \dots + n \cdot k_n = n.$$

Например, для классов C_2 и C_4 имеем:

$$1 \cdot k_1 + 3 \cdot k_3 = 1 \cdot 1 + 3 \cdot 1 = 4, \quad 1 \cdot k_1 + 2 \cdot k_2 = 1 \cdot 2 + 2 \cdot 1 = 4.$$

Цикл, длина которого r , можно записать $r!$ способами, причем элементы в каждом из этих циклов можно выбрать r^{k_r} способами. Так как все эти выборы можно сделать независимо, необходимо брать произведение $r^{k_r} r!$. Если помнить, что общее число подстановок равно $n!$, то формула для нахождения числа элементов в классе $C_i(k_1, k_2, \dots, k_n)$ выглядит следующим образом:

$$C_i(k_1, k_2, \dots, k_n) = n! / 1^{k_1} \cdot k_1! \cdot 2^{k_2} \cdot k_2! \cdot \dots \cdot n^{k_n} \cdot k_n!.$$

В нашем конкретном случае число элементов по классам распределится следующим образом:

$$\begin{aligned} C_0(4, 0, 0, 0) &= 1, & C_1(0, 2, 0, 0) &= 3, & C_2(1, 0, 1, 0) &= 8, \\ C_3(0, 0, 0, 1) &= 6, & C_4(2, 1, 0, 0) &= 6. \end{aligned}$$

Число элементов во всех пяти классах должно быть равно $n!$:

$$4! = 1 + 3 + 8 + 6 + 6 = 24.$$

Завершим этот раздел демонстрацией одного несложного, но весьма полезного приема. Касается он быстрого отыскания сопряженной подстановки b , если известна исходная a и трансформационная t . Демонстрацию проведем на конкретном примере.

Пусть даны следующие подстановки —

$$a = (052)(134)(67), \quad t = (0235)(1467).$$

Чтобы найти сопряженную относительно a подстановку b , необходимо осуществить преобразование подобия, сделав при этом умножение трех подстановок:

$$b = t^{-1} a t = (0532)(1764) \times (052)(134)(67) \times (0235)(1467) = (032)(17)(456).$$

Однако подстановку b можно найти без этого утомительного перемножения. Для этого нужно на место индексов подстановки a поставить индексы, указанные подстановкой t . Так, первый индекс 0 подстановки a заменяется на индекс 2, поскольку в подстановке t индекс 0 переходит в 2. Второму индексу 5 подстановки a необходимо заменить на 0, так как в подстановке t осуществляется переход $5 \rightarrow 0$ и т.д. В результате получим:

$$b = (203)(456)(71).$$

Сравнивая данную подстановку с предыдущей, убеждаемся в их полной тождественности.

2.4. Группы небольших порядков

Тождественный элемент e образует *группу первого порядка*. Обозначим ее как C_1 . Несмотря на немногочисленность элементов, она, тем не менее, удовлетворяет всем четырем условиям определения группы: в качестве элементов g, g^{-1}, g_1, g_2, g_3 будет выступать один элемент e . Положительная (+1) и отрицательная (−1) единицы образуют *группу второго порядка* C_2 . С *группой третьего порядка* (C_3) мы ранее еще не сталкивались. Следующие подстановки и 0,1-матрицы составят такую группу:

$$0 = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad 1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad 2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Базисные единицы комплексного числа $\{i_0, i_1, i_2, i_3\}$ ранее нами уже рассматривались. Они образуют *группу четвертого порядка* C_4 . Однако это не единственная группа из четырех элементов.

В самом деле, в роли *образующего элемента* a группы C_4 , в силу условия цикличности (2.22), может выступать либо i_1 , либо i_3 — в обоих случаях таблицей умножения является табл. 2.14, что также отвечает ранее приведенной таблице (табл. 2.5). Но можно в качестве образующих взять две *несвязанные* транспозиции a и b . В этом случае мы также получим группу четвертого порядка (C_2^2), но которая уже перемножается в соответствии с табл. 2.15 или, если перейти на язык только индексов, табл. 2.16. Последняя таблица нам также нужна для получения *регулярных подстановок*:

$$e = (0), \quad a = (01)(23), \quad b = (02)(13), \quad ab = (03)(12),$$

которые будут *изоморфны* исходным подстановкам группы S_2^2 :

$$e = (0), \quad a = (01), \quad b = (23), \quad ab = (01)(23).$$

Таблица 2.14

e	a	a^2	a^3
a	a^2	a^3	e
a^2	a^3	e	a
a^3	e	a	a^2

Таблица 2.15

e	a	b	ab
a	e	ab	b
b	ab	e	a
ab	b	a	e

Таблица 2.16

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

Ситуация окажется несколько иной, если в качестве образующих одной группы (C_2C_3) взять несвязанные 2-цикл и 3-цикл (табл. 2.17), а в качестве образующих другой (C_6) — единственный 6-цикл (табл. 2.18). Группы *шестого порядка*, в отличие от групп четвертого порядка, имеют только одну коммутативную структуру, в чем можно убедиться, если соответствующие клетки табл. 2.17 и табл. 2.18 закодировать одноименными индексами — табл. 2.19. Таблицы становятся неразличимыми, следовательно, группы *изоморфны*: $C_2C_3 \approx C_6$, что на элементарном уровне позволяет записать следующие соответствия:

$$\begin{aligned} a &\approx (012345) \approx ab = (01)(234), & a^4 &\approx (042)(153) \approx b = (234), \\ a^2 &= (024)(135) \approx b^2 = (243), & a^5 &= (054321) \approx ab^2 = (01)(243), \\ a^3 &= (03)(14)(25) \approx a = (01), & e &= (0). \end{aligned}$$

Здесь подстановки, получающиеся при последовательном возведении в степень исходного 6-цикла a , являются не чем иным, как регулярными подстановками по столбцам табл. 2.19.

Таблица 2.17

e	ab	b^2	a	b	ab^2
ab	b^2	a	b	ab^2	e
b^2	a	b	ab^2	e	ab
a	b	ab^2	e	ab	b^2
b	ab^2	e	ab	b^2	a
ab^2	e	ab	b^2	a	b

Таблица 2.18

e	a	a^2	a^3	a^4	a^5
a	a^2	a^3	a^4	a^5	e
a^2	a^3	a^4	a^5	e	a
a^3	a^4	a^5	e	a	a^2
a^4	a^5	e	a	a^2	a^3
a^5	e	a	a^2	a^3	a^4

Таблица 2.19

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

Две *связанные* (т.е. имеющие общий нулевой индекс) транспозиции a и b также образуют группу из шести элементов, но уже *некоммутативную*, с принципиально иной, *несимметричной* относительно главной диагонали, таблицей умножения (табл. 2.20). По названию геометрической фигуры эта группа называется *диэдральной* и обозначается как D_3 . Табл. 2.20 удобно переписать в числовых индексах — табл. 2.21, тогда можно будет составить регулярные подстановки, которые очевидно, должны быть изоморфны исходным подстановкам группы диэдра —

$$\begin{aligned} D_3: \quad a &= (01) \approx (01)(24)(35), & b &= (02) \approx (02)(13)(45), \\ ba &= (021) \approx (043)(152), & ab &= (012) \approx (034)(125), \\ aba &= (12) \approx (05)(14)(23), & e &= (0). \end{aligned}$$

Таблица 2.20

<i>e</i>	<i>a</i>	<i>b</i>	<i>ab</i>	<i>ba</i>	<i>aba</i>
<i>a</i>	<i>e</i>	<i>ab</i>	<i>b</i>	<i>aba</i>	<i>ba</i>
<i>b</i>	<i>ba</i>	<i>e</i>	<i>aba</i>	<i>a</i>	<i>ab</i>
<i>ab</i>	<i>aba</i>	<i>a</i>	<i>ba</i>	<i>e</i>	<i>b</i>
<i>ba</i>	<i>b</i>	<i>aba</i>	<i>e</i>	<i>ab</i>	<i>a</i>
<i>aba</i>	<i>ab</i>	<i>ba</i>	<i>a</i>	<i>b</i>	<i>e</i>

Таблица 2.21

0	1	2	3	4	5
1	0	3	2	5	4
2	4	0	5	1	3
3	5	1	4	0	2
4	2	5	0	3	1
5	3	4	1	2	0

Перейдя к рассмотрению групп шестого порядка, мы пропустили *группу пятого порядка*. Однако нетрудно догадаться, что группы, порядок которых равен *простому числу* (2, 3, 5, 7, ...), всегда будут иметь и простое *циклическое* строение. Но чем больше делителей у порядка группы, пусть даже и одинаковых, тем разнообразнее варианты ее строения. Далее нам предстоит рассмотреть пять различных *групп восьмого порядка*. Анализ начнем с коммутативных групп.

Поскольку восемь можно представить тремя способами — 1×8 , 2×4 , $2 \times 2 \times 2$, существуют три различных *коммутативных* группы: первая (C_8) строится с помощью одного-единственного 8-цикла, вторая ($C_2 C_4$) — на двух несвязанных 2- и 4-циклах, наконец, третья (C_2^3) — на трех несвязанных 2-циклах:

$$\begin{aligned}
 C_8: \quad & a = (01234567), \quad a^2 = (0246)(1357), \quad a^3 = (03614725), \quad a^4 = (04)(15)(26)(37), \\
 & a^5 = (05274163), \quad a^6 = (0642)(1753), \quad a^7 = (07654321), \quad e = (0); \\
 C_2 C_4: \quad & a = (0123), \quad b = (45), \quad a^2 = (02)(13), \quad a^3 = (0321), \\
 & ab = (0123)(45), \quad a^2 b = (02)(13)(45), \quad a^3 b = (0321)(45), \quad e = (0); \\
 C_2^3: \quad & a = (01), \quad b = (23), \quad c = (45), \quad ab = (01)(23), \\
 & ac = (01)(45), \quad bc = (23)(45), \quad abc = (01)(23)(45), \quad e = (0).
 \end{aligned}$$

Из *некоммутативных* групп восьмого порядка имеются две: одна обладает симметрией *диэдра* (D_4^1), другая — *кватерниона* (D_4^2). Диэдральная группа получается с помощью 4-цикла и несмежной транспозиции, индексы которой совпадают с индексами 4-цикла (табл. 2.22).

Таблица 2.22

$D_4^1 \quad e = (0),$
 $a = (0123),$
 $a^2 = (02)(13),$
 $a^3 = (0321),$
 $b = (02),$
 $ab = ba^3 = (01)(23),$
 $a^2b = ba^2 = (13),$
 $a^3b = ba = (03)(12).$

<i>e</i>	<i>a</i>	<i>a</i> ²	<i>a</i> ³	<i>b</i>	<i>ab</i>	<i>a</i> ² <i>b</i>	<i>a</i> ³ <i>b</i>
<i>a</i>	<i>a</i> ²	<i>a</i> ³	<i>e</i>	<i>ab</i>	<i>a</i> ² <i>b</i>	<i>a</i> ³ <i>b</i>	<i>b</i>
<i>a</i> ²	<i>a</i> ³	<i>e</i>	<i>a</i>	<i>a</i> ² <i>b</i>	<i>a</i> ³ <i>b</i>	<i>b</i>	<i>ab</i>
<i>a</i> ³	<i>e</i>	<i>a</i>	<i>a</i> ²	<i>a</i> ³ <i>b</i>	<i>b</i>	<i>ab</i>	<i>a</i> ² <i>b</i>
<i>b</i>	<i>a</i> ³ <i>b</i>	<i>a</i> ² <i>b</i>	<i>ab</i>	<i>e</i>	<i>a</i> ³	<i>a</i> ²	<i>a</i>
<i>ab</i>	<i>b</i>	<i>a</i> ³ <i>b</i>	<i>a</i> ² <i>b</i>	<i>a</i>	<i>e</i>	<i>a</i> ³	<i>a</i> ²
<i>a</i> ² <i>b</i>	<i>ab</i>	<i>b</i>	<i>a</i> ² <i>b</i>	<i>a</i> ²	<i>a</i>	<i>e</i>	<i>a</i> ³
<i>a</i> ³ <i>b</i>	<i>a</i> ² <i>b</i>	<i>ab</i>	<i>b</i>	<i>a</i> ³	<i>a</i> ²	<i>a</i>	<i>e</i>

Кватернион образуется на двух 4,4-циклах, несмежные индексы которых взаимосвязаны так, что при возведении в квадрат получается одна и та же подстановка — 2,2,2-цикл (табл. 2.23). Для группы диэдра D_4^1 были приведены толь-

ко три наиболее характерных соотношения. Однако общее число возможных соотношений определяется числом *перестановок* всех степеней образующих a и b .

Таблица 2.23

e	a	a^2	a^3	b	b^3	ab	ba
a	a^2	a^3	e	ab	ba	b^3	b
a^2	a^3	e	a	b^3	b	ba	ab
a^3	e	a	a^2	ba	ab	b	b^3
b	ba	b^3	ab	a^2	e	a	a^3
b^3	ab	b	ba	e	a^2	a^3	a
ab	b	ba	b^3	a^3	a	a^2	e
ba	b^3	ab	b	a	a^3	e	a^2

Для группы кватерниона D_4^2 полный перечень алгебраических соотношений выглядит следующим образом —

$$\begin{aligned}
 D_4^2: \quad & e = a^0 b^4 = b^0 a^4 = a^2 b^2 = b^2 a^2 = (0), \\
 & a = a^1 b^4 = b^0 a^1 = a^3 b^2 = b^2 a^3 = (0123)(4756), \\
 b^2 = & a^2 = a^2 b^4 = b^0 a^2 = a^4 b^2 = b^2 a^4 = (02)(13)(45)(67), \\
 & a^3 = a^3 b^4 = b^0 a^3 = a^1 b^2 = b^2 a^1 = (0321)(4657), \\
 b = & a^0 b^1 = b^1 a^4 = a^2 b^3 = b^3 a^2 = (0425)(1637), \\
 & a^1 b^1 = b^1 a^3 = a^3 b^3 = b^3 a^1 = (0627)(1534), \\
 b^3 = & a^2 b^1 = b^1 a^2 = a^4 b^3 = b^3 a^0 = (0524)(1736), \\
 & a^3 b^1 = b^1 a^1 = a^1 b^4 = b^3 a^3 = (0726)(1435).
 \end{aligned}$$

Если в качестве образующих a и b взять два несвязанных друг с другом 3-цикла, то получится коммутативная группа C_3^2 , которая не может быть сведена к циклической C_9 . Последнее означает, что существуют две различных коммутативных группы девятого порядка —

$$\begin{array}{ll}
 C_9: & a = (012345678), \\
 & a^2 = (024681357), \\
 & a^3 = (036)(147)(258), \\
 & a^4 = (048372615), \\
 & a^5 = (051627384), \\
 & a^6 = (063)(174)(285), \\
 & a^7 = (075318642), \\
 & a^8 = (087654321), \\
 & e = (0); \\
 C_3^2: & a = (012), \\
 & a^2 = (021), \\
 & b = (345), \\
 & b^2 = (354), \\
 & ab = (012)(345), \\
 & a^2 b = (021)(345), \\
 & ab^2 = (012)(354), \\
 & a^2 b^2 = (021)(354), \\
 & e = (0).
 \end{array}$$

Некоммутативных групп девятого порядка не существует. Подобная ситуация напоминает аналогичную ситуацию, сложившуюся с группами четвертого порядка. Действительно, число 9 раскладывается на два одинаковых простых множителя — 3×3 ; число 4 также раскладывается на одинаковые простые множители — 2×2 . Отсюда можно ожидать повторения данной ситуации на таких порядках, как $25 = 5 \times 5$, $49 = 7 \times 7$ и т.д.

Продолжим наши рассуждения в этом же направлении. Число 6 раскладывается на два различных простых множителя — 2×3 . Как мы видели, коммутативная группа, построенная на одном 6-цикле, и коммутативная группа, построенная на 2- и 3-циклах, получились изоморфными. Можно ожидать, что группа десятого порядка (число 10 раскладывается на два различных простых множителя

— 2×5) также имеет изоморфные коммутативные группы $C_2 C_5 \approx C_{10}$. В самом деле, следующее соответствие целиком подтверждает наше предположение.

$$\begin{array}{ll}
 C_{10} & \approx C_2 C_5 \\
 a = (0123456789) & \approx a b = (01)(23456), \\
 a^2 = (02468)(13579) & \approx b^2 = (24635), \\
 a^3 = (0369258147) & \approx ab^3 = (01)(25364), \\
 a^4 = (04826)(15937) & \approx b^4 = (26543), \\
 a^5 = (05)(16)(27)(38)(49) & \approx a = (01), \\
 a^6 = (06284)(17395) & \approx b = (23456), \\
 a^7 = (0741852963) & \approx ab^2 = (01)(24635), \\
 a^8 = (08642)(19753) & \approx b^3 = (25364), \\
 a^9 = (0987654321) & \approx ab^4 = (01)(26543), \\
 e = (0) & \approx e = (0).
 \end{array}$$

Кроме коммутативной структуры, группа десятого порядка, как и группа шестого, имеет диэдральную структуру —

$$\begin{array}{lll}
 D_5^1: & a = (01234), & ab = ba^4 = (04)(13), & b = (14)(23), \\
 & a^2 = (02413), & a^2 b = ba^3 = (03)(12), & e = (0). \\
 & a^3 = (03142), & a^3 b = ba^2 = (02)(34), & \\
 & a^4 = (04321), & a^4 b = ba = (01)(24), &
 \end{array}$$

Теперь мы вправе предположить, что в ряду групп 6-го и 10-го порядков, окажутся также группы 14-го (2×7), 22-го (2×11) и т.д. порядков, но не 15-го (3×5), поскольку число 15 нечетно, а значит, диэдральной группы для него не существует.

За простой циклической группой 11-го порядка следуют богатые на структурные вариации группы 12-го порядка. Если в качестве образующих коммутативных групп выбрать систему несвязанных циклов, отвечающую делителям числа 12, то эти четыре группы распадутся на два класса изоморфных групп: $C_3 C_4 \approx C_{12}$ и $C_2 C_6 \approx C_2^2 C_3$. Изоморфизм существует и среди некоммутирующих групп, а именно: $C_2 D_3 \approx D_6^1$, образующими которых будут:

$$\begin{array}{lll}
 C_2 D_3: & a = (012), & b = (02), & c = (34), \\
 D_6^1: & a = (012345), & b = (15)(24). &
 \end{array}$$

Чтобы лучше понять сущность изоморфизма, все группы 12-го порядка сведем в табл. 2.24. В графах d_i этой таблицы приведены результаты деления порядка группы на *наименьшее общее кратное* длин циклов, входящих в подстановки. Оказывается, изоморфные группы имеют одинаковые наборы этих чисел: для $C_3 C_4$ и C_{12} справедлив перечень чисел d_1 , для $C_2 C_6$ и $C_2^2 C_3$ — d_2 , а для $C_2 D_3$ и D_6^1 — d_3 .

Числа d_i отражают одинаковое циклическое строение подстановок. Однако одинаковые ряды d_i служат *необходимым и достаточным* условием изоморфизма только для *коммутирующих* групп. Для *некоммутирующих* групп данное условие является лишь *необходимым*, но далеко не достаточным, в чем мы убедимся, рассматривая группы 16-го порядка.

Таблица 2.24

C_{12}	C_3C_4	d_1	C_7C_5	$C_2^2C_3$	d_2	C_2D_3	D_6^1	d_3	D_6^2	d_4	T	d_5
a	ab	1	a	b	6	abc	a	2	a	4	a	2
a^2	a^2b^2	2	b	a^2c	2	ab	a^2	4	a^2	4	a^2	4
a^3	b^3	3	b^2	a	4	aba	a^3	6	b	4	a^3	6
a^4	a	4	b^3	c	6	ba	a^4	4	b^2	4	a^4	4
a^5	a^2b	1	b^4	a^2	4	bac	a^5	2	a^2b	4	a^5	2
a^6	b^2	6	b^5	ac	2	a	b	6	ba^2	4	b	3
a^7	ab^3	1	ab	a^2b^2c	2	b	ab	6	a^2b	4	ab	3
a^8	a^2	4	ab^2	ab	2	c	a^2b	6	b^2a	4	a^2b	3
a^9	b	3	ab^3	bc	6	ac	a^3b	6	ab	6	a^3b	3
a^{10}	ab^2	2	ab^4	a^2b	2	bc	a^4b	6	ba	6	a^4b	3
a^{11}	a^2b^3	1	ab^5	abc	2	$abac$	a^5b^2	6	ab^2a	6	a^5b	3
e	e	12	e	e	12	e	e	12	e	12	e	12

В табл. 2.24 приведены элементы и ряды d_i еще для двух групп 12-го порядка. Одна из них, D_6^2 с рядом d_4 , в чем-то напоминает группу кватерниона, так как для нее 2-циклы, полученные от образующих a и b равны между собой: $a^3 = b^2$. Таким образом, в подобных группах (а они встречаются для всех групп, порядок которых делится на 4) существует одна-единственная подстановка, которая состоит из совокупности транспозиций; все остальные подстановки имеют цикличность больше двух. Для сравнения D_4^2 с D_6^2 приведем полную систему равенств между элементами последней группы —

$$\begin{aligned}
 D_6^2: \quad e &= a^6b^4 = b^6a^6 = a^3b^3 = b^2a^3 = (0), \\
 a &= a^1b^4 = b^6a^1 = a^4b^2 = b^2a^4 = (012345)(6789AB), \\
 a^2 &= a^2b^4 = b^6a^2 = a^5b^3 = b^3a^5 = (024)(135)(68A)(79B), \\
 b^2 &= a^3 = a^3b^4 = b^6a^3 = a^6b^1 = b^1a^6 = (03)(14)(25)(69)(7A)(8B), \\
 a^3 &= a^4b^4 = b^6a^4 = a^1b^3 = b^3a^1 = (042)(153)(6A8)(7B9), \\
 a^5 &= a^5b^4 = b^6a^5 = a^2b^1 = b^1a^2 = (054321)(6BA987), \\
 b &= a^0b^1 = b^1a^6 = a^2b^3 = b^3a^1 = (0639)(1B48)(2A57), \\
 &= a^1b^1 = b^1a^5 = a^4b^3 = b^3a^2 = (0B38)(1A47)(2956), \\
 &= a^2b^1 = b^1a^4 = a^5b^3 = b^3a^1 = (0A37)(1946)(285B), \\
 b^3 &= a^3b^1 = b^1a^3 = a^6b^3 = b^3a^0 = (0936)(184B)(275A), \\
 &= a^4b^1 = b^1a^2 = a^1b^1 = b^1a^5 = (083B)(174A)(2659), \\
 &= a^5b^1 = b^1a^1 = a^2b^3 = b^3a^4 = (073A)(1649)(2B58).
 \end{aligned}$$

Оставшаяся некоммутативная группа 12-го порядка называется *группой тетраэдра* (T), поскольку она отвечает группе вращения этой геометрической фигуры. На примере группы T мы проиллюстрируем одно, довольно неприятное, свойство определяющих соотношений — их *неоднозначность*. Для получения конкретных элементов группы тетраэдра в качестве образующих можно взять два связанных 3-цикла с двумя общими индексами, тогда система определяющих соотношений будет выглядеть так:

$$\begin{aligned}
 T: \quad a &= (012), & a^2b^2 &= ba = (01)(23), & ab &= b^2a^2 = (02)(13), \\
 b &= (123), & a^2b &= ab^2a^2 = (031), & ab^2 &= b^2a^2b = (032),
 \end{aligned}$$

$$\begin{aligned} a^2 &= (021), & b^2 a &= ba^2 b^2 = (013), & ba^2 - a^2 b^2 a &= (023), \\ b^2 &= (132), & a^2 ba^2 &= ab^2 a = b^2 ab^2 - ba^2 b = (03)(12). \end{aligned}$$

Как видим, в этих равенствах фигурируют элементы, составленные из трех букв. Если в качестве образующих взять 2- и 3-циклы, то в определяющих соотношениях появятся элементы из четырех букв:

$$\begin{aligned} T: \quad a &= (012), & ab &= ba^2 ba^2 = (132), & ahab - ba^2 &= (123), \\ a^2 &= (021), & a^2 b^2 &= haba = (032), & a^2 ba^2 b &= ba = (023), \\ b &= (01)(23), & aba &= ba^2 b = (013), & a^2 ba^2 &= bab = (031), \\ aba^2 &= ba^2 ba = (02)(13), & a^2 ba &= haba^2 = (03)(12). \end{aligned}$$

Чтобы исчерпать все двенадцать подстановок комбинациями из двух букв, нужно выбрать в качестве образующих три 3-цикла. Однако в этом случае возрастет и число возможных равенств ...

$$\begin{aligned} T: \quad a &= bc = (012), & a^2 c &= b a^2 = cb = (023), \\ b &= ac^2 = (123), & ab^2 &= b^2 c^2 = c^2 a = (032), \\ c &= b^2 a = (013), & ab &= ca = b^2 a^2 = a^2 c^2 = (02)(13), \\ a^2 &= c^2 b^2 = (021), & a^2 b^2 &= b^2 c = ba = c^2 b = (01)(23), \\ b^2 &= ca^2 = (132), & ac &= cb^2 = c^2 a^2 = bc^2 = (03)(12), & c^2 &= a^2 b = (031). \end{aligned}$$

На примере группы тетраэдра T мы показали, как не похожи могут быть определяющие соотношения для одной и той же группы, если в качестве образующих выбрать различные системы элементов.

Число 12 раскладывается на три простых множителя — $2 \times 2 \times 3$. Зададимся вопросом, не будут ли группы 20-го ($2 \times 2 \times 5$), 28-го ($2 \times 2 \times 7$) и т.д. порядков иметь аналогичное строение? Имея перед собой упорядоченные таблицы умножения размером 12×12 , можно было бы попытаться составить аналогичные таблицы размером 20×20 , 28×28 и т.д. Приведем таблицы 12×12 для группы диэдра D_6^1 (табл. 2.25), группы типа кватерниона D_6^2 (табл. 2.26) и группы тетраэдра T (табл. 2.27).

Таблица 2.25

0	1	2	3	4	5	6	7	8	9	A	B
1	2	3	4	5	0	B	6	7	8	9	A
2	3	4	5	0	1	A	B	6	7	8	9
3	4	5	0	1	2	9	A	B	6	7	8
4	5	0	1	2	3	8	9	A	B	6	7
5	0	1	2	3	4	7	8	9	A	B	6
6	7	8	9	A	B	0	1	2	3	4	5
7	8	9	A	B	6	5	0	1	2	3	4
8	9	A	B	6	7	4	5	0	1	2	3
9	A	B	6	7	8	3	4	5	0	1	2
A	B	6	7	8	9	2	3	4	5	0	1
B	6	7	8	9	A	1	2	3	4	5	0

Таблица 2.26

0	1	2	3	4	5	6	7	8	9	A	B
1	2	3	4	5	0	B	6	7	8	9	A
2	3	4	5	0	1	A	B	6	7	8	9
3	4	5	0	1	2	9	A	B	6	7	8
4	5	0	1	2	3	8	9	A	B	6	7
5	0	1	2	3	4	7	8	9	A	B	6
6	7	8	9	A	B	3	4	5	0	1	2
7	8	9	A	B	6	2	3	4	5	0	1
8	9	A	B	6	7	1	2	3	4	5	0
9	A	B	6	7	8	0	1	2	3	4	5
A	B	6	7	8	9	5	0	1	2	3	4
B	6	7	8	9	A	4	5	0	1	2	3

Составить по аналогии таблицы умножения для коммутативных групп порядков 20-го, 28-го и т.д. не представляет большой сложности. Повторить приве-

денные таблицы для групп $D_{10}^1, D_{14}^1, D_{10}^2, D_{14}^2$ и т.д. тоже нетрудно. Однако придумать таблицы умножения размером 20×20 и 28×28 , аналогичные табл. 2.27, не удается. Группы 20-го и 28-го порядков с тетраэдральной структурой просто не существует. В табл. 2.28 приведены возможные варианты групп интересующих нас порядков. Оказывается, групп 28-го порядка только четыре, а групп 20-го — пять, однако группа, которую мы обозначили как D_5^2 , далека от тетраэдрального строения. И тут возникает законный вопрос, как вообще осуществляется поиск новых групп?

Каких-то общих методик, срабатывающих во всех возможных случаях, здесь не существует. Ниже мы продемонстрируем один из многих приемов получения определяющих соотношений для новых групп. Эту демонстрацию сначала проведем на группе, строение которой нам известно — D_{10}^2 .

Таблица 2.27

0	1	2	3	4	5	6	7	8	9	A	B
1	2	0	7	8	6	A	B	9	4	5	3
2	0	1	B	9	A	5	3	4	8	6	7
3	4	5	0	1	2	9	A	B	6	7	8
4	5	3	A	B	9	7	8	6	1	2	0
5	3	4	8	6	7	2	0	1	B	9	A
6	7	8	9	A	B	0	1	2	3	4	5
7	8	6	1	2	0	4	5	3	A	B	9
8	6	7	5	3	4	B	9	A	2	0	1
9	A	B	6	7	8	3	4	5	0	1	2
A	B	9	4	5	3	1	2	0	7	8	6
B	9	A	2	0	1	8	6	7	5	3	4

Таблица 2.28

Группы 12-го порядка	Группы 20-го порядка	Группы 28-го порядка
$C_3C_4 \approx C_{12}$	$C_4C_5 \approx C_{20}$	$C_4C_7 \approx C_{28}$
$C_2C_6 \approx C_2^2C_3$	$C_2C_{10} \approx C_2^2C_5$	$C_2C_{14} \approx C_2^2C_7$
$C_2D_3 \approx D_6^1$	$C_2D_5^1 \approx D_{10}^1$	$C_2D_7^1 \approx D_{14}^1$
D_6^2	D_{10}^2	D_{14}^2
T	D_5^2	Отсутствует

Прежде всего примем фундаментальное условие для образующих a и b , касающееся их цикличности: $a^{10} = b^4 = e$. Затем, по аналогии с группой D_6^2 , предположим справедливость равенства $ab = ba^9$. Ясно, что в группе D_{10}^2 должен существовать элемент aba^9 . Представим его двумя способами:

$$aba^9 = a \times ba^9 = a \times ab = a^2b, \quad aba^9 = ab \times a^9 = ba^9 \times a^9 = ba^8.$$

Следовательно, в искомым соотношениях есть равенство — $a^2b = ba^8$. Далее, возьмем элемент a^2ba^8 и снова распишем его двумя способами, получим новое соот-

ношение — $a^3b = ba^7$. Беря подходящие элементы, в том числе bab, b^2a^3b , и представляя их двумя указанными способами, находим все необходимые соотношения группы, которые мы сейчас выписывать не будем.

Если бы мы взяли за основу равенство $ab = ba^3$, нам не удалось бы его совместить с «кватернионным» условием $a^5 = b^2$, которое неизбежно возникает в группе D_{10}^2 . Выбранное равенство влечет за собой соотношение $ab^2 = b^2a^9$. Если принять условия: $a^{10} = b^4 = e, ab = ba^3$ и $a^5 \neq b^2$, число элементов в новой группе возросло бы до 40, что также для нас неприемлемо. Поиск неизвестной нам группы 20-го порядка тетраэдрального строения уместно начать с предположения $a^5 = b^4 = e$. Далее, наудачу, берем снова равенство $ab = ba^3$ и смотрим, что получится из элемента aba^3 :

$$aba^3 = a \times ba^3 = a \times ab = a^2b, \quad aba^3 = ab \times a^3 = ba^3 \times a^3 = ba.$$

Так, мы получаем новое равенство $a^2b = ba$. Затем ищем равенство, отвечающее элементу a^2ba . Продолжая аналогичным образом, находим все элементы новой группы, которая, однако, совершенно не похожа на группу T . Обозначив ее как D_5^2 (общепринятой системы обозначений для всех групп пока не выработано), выпишем все ее элементы вместе с определяющими соотношениями:

$$D_5^2: \quad \begin{array}{ccccc} a, & b, & ab = ba^3, & ab^2 = b^3a^4, & ab^3 = b^3a^2, \\ a^2, & b^2, & a^2b = ba, & a^2b^2 = b^2a^3, & a^2b^3 = b^3a^4, \\ a^3, & b^3, & a^3b = ba^4, & a^3b^2 = b^2a^2, & a^3b^3 = b^3a, \\ a^4, & e, & a^4b = ba^2, & a^4b^2 = b^2a, & a^4b^3 = b^3a^3. \end{array}$$

В данном случае нам повезло: выбор какого-то нового исходного равенства, например, $ab = ba^4$, приведет к изоморфной группе. Других же групп 20-го порядка, кроме перечисленных в табл. 2.28, не существует.

Итак, какой-либо универсальной формулы, по которой можно было бы заранее рассчитать число групп и их структурную организацию для любого наперед заданного порядка, не существует, хотя имеются вполне закономерные ряды групп, порядки которых удовлетворяют определенной системе делителей, в частности:

$$\{4 = 2 \times 2, 9 = 3 \times 3, 25 = 5 \times 5, \dots\}, \quad \{6 = 2 \times 3, 10 = 2 \times 5, 14 = 2 \times 7, \dots\}.$$

Только что рассмотренная группа попадает в ряд групп, порядок которых определяется формулой: $n = (p-1) \cdot p$, где p — простое число. Так получается последовательность —

$$\{2 = 1 \times 2, 6 = 2 \times 3, 20 = 4 \times 5, 42 = 6 \times 7, \dots\}.$$

Одни последовательности возрастают медленно, как например, ряды групп диэдра и кватерниона:

$$\{2, 4, 6, 8, 10, 12, \dots, n = 2 \cdot k\}, \{4, 8, 12, 16, 20, \dots, n = 4 \cdot k\},$$

другие стремительно, как например, ряд из симметрических групп:

$$\{2, 6, 24, 120, 720, \dots, n = k!\}.$$

Последовательности пересекаются друг с другом. В точках пересечения могут получаться изоморфные группы или совершенно отличные — предсказывать здесь что-либо трудно. Существуют такие порядки, где пересекаются множество рядов с самыми разнообразными организационными принципами. Такими точками

пересечения являются группы порядков 16, 24, 32, 48, 64 и т.д. Так, для 64-го порядка имеется 267 структурных разновидностей. Дать определяющие соотношения всем группам даже для такого достаточно скромного порядка, как 64-й, представляется весьма непростой задачей.

Изоморфизм является, пожалуй, одной из основных форм существования эквивалентности. Две группы A и B считаются изоморфными, если можно найти такую трансформационную подстановку t , не принадлежащую ни A , ни B , что все элемента a трансформируются в элементы b :

$$b = t^{-1} a t. \quad (2.27)$$

В этом случае группы A и B имеют одинаковые таблицы умножения. Однако идентичность таблиц является не всегда очевидным фактом.

Пусть дана конкретная таблица умножения — табл. 2.29. Поскольку она не симметрична относительно главной диагонали и имеет на ней два тождественных элемента, можно предположить, что группа, которую представляет табл. 2.29, по-видимому, является группой D_8^2 . Следовательно, нам нужно установить идентичность табл. 2.29 и табл. 2.26. С этой целью из табл. 2.29 выберем, причем достаточно произвольно, регулярную подстановку 4. Этой подстановке поставим в соответствие упорядоченную подстановку 1 эквивалентной циклической структуры, взятой из табл. 2.26 --

$$4 = (042A78)(1B9356), \quad 1 = (012345)(6789AB).$$

Таблица 2.29

0	1	2	3	4	5	6	7	8	9	A	B
1	A	9	0	B	4	2	5	6	8	3	7
2	5	7	B	A	9	3	0	4	1	8	6
3	0	6	A	5	7	8	B	9	2	1	4
4	6	A	9	2	3	5	8	0	B	7	1
5	8	1	2	6	A	7	9	3	4	B	0
6	7	B	4	1	2	A	3	5	0	9	8
7	9	0	6	8	1	B	2	A	5	4	3
8	B	4	5	0	6	1	A	7	3	2	9
9	4	5	7	3	8	0	1	B	A	6	2
A	3	8	1	7	B	9	4	2	6	0	5
B	2	3	8	9	0	4	6	1	7	5	A

Теперь воспользуемся приемом, обратным тому, о котором шла речь в конце п. 2.3. Считаем подстановку 1 верхней строкой трансформационной подстановки t , а подстановку 4 ее нижней строкой (подстановку t перепишем в циклической форме):

$$t = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & A & B \\ 0 & 4 & 2 & A & 7 & 8 & 1 & B & 9 & 3 & 5 & 6 \end{pmatrix} = (0)(147B6)(2)(3A589).$$

Далее запишем обратное к (2.27) преобразование подобия —

$$a = t b t^{-1}.$$

Подставив вместо b регулярные подстановки из табл. 2.29, получим:

$$\begin{aligned} 6 &= t(01A3)(258B)(4679) t^{-1} &= (0639)(1B48)(2A57), \\ 2 &= t(027)(195)(36B)(4A8) t^{-1} &= (024)(135)(68A)(79B), \\ 9 &= t(03A1)(2B85)(4976) t^{-1} &= (0936)(184B)(275A), \\ 1 &= t(042A78)(1B9356) t^{-1} &= (012345)(6789AB), \\ A &= t(05AB)(1437)(2986) t^{-1} &= (0A37)(1946)(285B), \\ B &= t(06A9)(1238)(457B) t^{-1} &= (0B38)(1A47)(2956), \\ 4 &= t(072)(159)(3B6)(48A) t^{-1} &= (042)(153)(6A8)(7B9), \\ 5 &= t(087A24)(16539B) t^{-1} &= (054321)(6BA987), \\ 8 &= t(09A6)(1832)(4B75) t^{-1} &= (083B)(174A)(2659), \\ 3 &= t(0A)(13)(28)(47)(5B)(69) t^{-1} &= (03)(14)(25)(69)(7A)(8B), \\ 7 &= t(0BA5)(1734)(2689) t^{-1} &= (073A)(1649)(2B58). \end{aligned}$$

Строя по вновь полученным подстановкам a таблицу умножения, убеждаемся, что она в точности совпадает с табл. 2.26. Следовательно, табл. 2.29 есть не что иное, как таблица умножения группы D_6^2 .

Изоморфизм является важной, но не единственной формой эквивалентности. Целью даже весьма поверхностного *морфологического анализа группы* служит установление отношения эквивалентности между отдельными ее элементами. Всякое отношение эквивалентности, как мы уже знаем, разбивает группу на классы эквивалентных элементов. По причине коммутативности тождественного элемента e со всеми другими элементами группы он всегда образует свой собственный класс. В группе может находиться несколько таких элементов, которые, как и тождественный элемент, коммутируют со всеми элементами группы. Тогда каждый из них будет образовывать свой класс эквивалентности. Совокупность таких элементов называется *центром* группы. Центр группы G , который мы будем обозначать через Z , всегда образует *подгруппу* в G . В коммутативных группах получается, что все элементы центральны.

Подгруппы G_i группы G делятся на *собственные* и *несобственные*. К *несобственным* относятся подгруппа тождественного элемента G_0 и сама группа G , все остальные подгруппы — *собственные*. *Индексом* подгруппы G_i в группе G , что обозначается как $|G : G_i|$, называется частное от деления порядка группы G (обозначается как $|G|$) на порядок подгруппы $|G_i|$. В этом случае выполняются элементарные числовые соотношения:

$$|G : G_i| = |G| / |G_i|, \quad |G_i| = |G| / |G : G_i|, \quad |G| = |G : G_i| \times |G_i|$$

(путаницы между терминами «индекс подгруппы» и «индекс подстановки» обычно не возникает). Индекс всегда является *целым* числом. Это значит, что порядок подгруппы должен быть одним из *делителей* порядка группы. Поэтому, в частности, в группе шестого порядка не может быть подгрупп четвертого или пятого порядков. Однако из факта существования того или иного делителя еще не следует, что обязательно должна существовать соответствующая ему подгруппа. Например, в группе тетраэдра T нет подгрупп шестого порядка.

Вообще говоря, *подгруппы* являются объектами морфологического анализа с точки зрения *отношения порядка*, которым мы сейчас подробно заниматься не

будем. Вместе с тем отметим, что эквивалентность элементов тесно связана с их иерархией, поэтому, нередко, оба вида отношений трудно рассматривать раздельно. Наш морфологический анализ с точки зрения эквивалентности начнем с первой некоммукативной группы диэдра, которую мы запишем как D_3 :

$$\begin{aligned} 0 = (0) &= e, & 1 = (01) &= a, & 2 = (02) &= b, \\ 3 = (12) &= aba = bab, & 4 = (012) &= ab, & 5 = (021) &= ba. \end{aligned}$$

Элемент 1 трансформируется по элементам D_3 следующим образом:

$$\begin{aligned} 0 \cdot 1 \cdot 0^{-1} &= e \cdot a \cdot e = a = 1, & 3 \cdot 1 \cdot 3^{-1} &= aba \cdot a \cdot bab = b = 2, \\ 1 \cdot 1 \cdot 1^{-1} &= a \cdot a \cdot a = a = 1, & 4 \cdot 1 \cdot 4^{-1} &= ab \cdot a \cdot ba = b = 2, \\ 2 \cdot 1 \cdot 2^{-1} &= b \cdot a \cdot b = bab = 3, & 5 \cdot 1 \cdot 5^{-1} &= ba \cdot a \cdot ab = bab = 3. \end{aligned}$$

Отсюда видно, что элемент 1 сопряжен с элементами 2 и 3, т.е. в группе D_3 имеется класс эквивалентности

$$C_1 = \{1, 2, 3\} = \{a, b, bab\} = \{(01), (02), (12)\}$$

(обозначения классов эквивалентности и коммутативных групп совпадают, но путаницы не возникает, так как классы рассматриваются только в некоммукативных группах). Если любой из этих элементов подвергнуть трансформации, он не даст в результате элементы 4 и 5, поскольку последние объединены в свой класс эквивалентности —

$$\begin{aligned} 0 \cdot 4 \cdot 0^{-1} &= e \cdot ab \cdot e = ab = 4, & 3 \cdot 4 \cdot 3^{-1} &= aba \cdot ab \cdot bab = ba = 5, \\ 1 \cdot 4 \cdot 1^{-1} &= a \cdot ab \cdot a = ba = 5, & 4 \cdot 4 \cdot 4^{-1} &= ab \cdot ab \cdot ba = ab = 4, \\ 2 \cdot 4 \cdot 2^{-1} &= b \cdot ab \cdot b = ba = 5, & 5 \cdot 4 \cdot 5^{-1} &= ba \cdot ab \cdot ab = ab = 4. \end{aligned}$$

Таким образом, появился класс

$$C_2 = \{4, 5\} = \{ab, ba\} = \{(012), (021)\}.$$

Кроме того, имеется класс

$$C_0 = \{0\} = \{e\} = \{(0)\}.$$

Итак, группа диэдра D_3 разбивается на три класса эквивалентности — C_0, C_1, C_2 , что согласуется с нашими комбинаторными рассуждениями.

Классы эквивалентности можно перемножать. Произведение $C_i \times C_j$ есть множество всевозможных произведений элементов, взятых из C_i и C_j , причем совпадающие элементы не опускаются. В результате перемножения *целых* классов всегда получаются тоже *целые* классы:

$$\begin{aligned} C_2 \times C_2 &= \{4, 5\} \times \{4, 5\} = \{5, 0, 0, 4\} = 2 \cdot C_0 + C_2, \\ C_1 \times C_2 &= \{1, 2, 3\} \times \{4, 5\} = \{2, 3, 3, 1, 1, 2\} = 2 \cdot C_1, \\ C_1 \times C_1 &= \{1, 2, 3\} \times \{1, 2, 3\} = \{0, 4, 5, 5, 0, 4, 4, 5, 0\} = 3 \cdot C_0 + 3 \cdot C_2. \end{aligned}$$

В группе D_3 содержатся следующие *несобственные* подгруппы:

$$G_0 = \{0\}, \quad G = \{0, 1, 2, 3, 4, 5\}.$$

Три транспозиции образуют три *собственных* подгруппы второго порядка:

$$G_1 = \{0, 1\}, \quad G_2 = \{0, 2\}, \quad G_3 = \{0, 3\}.$$

Еще одна *собственная* подгруппа образована 3-циклом — $G_4 = \{0, 4, 5\}$.

Индексы подгрупп G_1, G_2, G_3 равны 3, а для $G_4 = 2$. Центр группы D_3 состоит из одного тождественного элемента — $Z = G_0 = \{0\}$.

Подгруппы G_1, G_2, G_3 отличаются от G_4 не только порядком, но и еще одним важным обстоятельством: G_4 состоит из полных классов C_0 и C_2 , в то время как *эквивалентные* элементы класса C_1 оказываются поделенными между *различными* подгруппами второго порядка. Это отличие между подгруппами выявляется при составлении так называемых *классов смежности*. Существуют *левые* и *правые* смежные классы, поскольку каждый элемент g из группы G , но не входящий в подгруппу G_i может образовывать всевозможные произведения справа $G_i g$ и слева gG_i . Найдем правые и левые смежные классы, например, для подгруппы G_1 , получим:

$$\begin{aligned} \{0, 1\} \cdot 2 &= \{2, 4\} = C'_1, & 2 \cdot \{0, 1\} &= \{2, 5\} = C''_1, \\ \{0, 1\} \cdot 3 &= \{3, 5\} = C'_2, & 3 \cdot \{0, 1\} &= \{3, 4\} = C''_2, \\ \{0, 1\} \cdot 4 &= \{4, 2\} = C'_3, & 4 \cdot \{0, 1\} &= \{4, 3\} = C''_3, \\ \{0, 1\} \cdot 5 &= \{5, 3\} = C'_4, & 5 \cdot \{0, 1\} &= \{5, 2\} = C''_4. \end{aligned}$$

Мы видим, что левые и правые смежные классы для этой подгруппы не совпадают. Такая же картина будет наблюдаться и для двух других подгрупп второго порядка. В отношении G_4 ситуация изменится:

$$\begin{aligned} \{0, 4, 5\} \cdot 1 &= \{1, 3, 2\} = C', & 1 \cdot \{0, 4, 5\} &= \{1, 2, 3\} = C'', \\ \{0, 4, 5\} \cdot 2 &= \{2, 1, 3\} = C', & 2 \cdot \{0, 4, 5\} &= \{2, 3, 1\} = C'', \\ \{0, 4, 5\} \cdot 3 &= \{3, 2, 1\} = C', & 3 \cdot \{0, 4, 5\} &= \{3, 1, 2\} = C''. \end{aligned}$$

Итак, для подгруппы G_4 *левые и правые классы совпали: $C' = C''$* .

Такое положение вещей распространяется на любые подгруппы G_i , в состав которых входят *полные классы сопряженности*. Для них выполняются равенства:

$$G_i g = g G_i, \quad G_i = g G_i g^{-1}.$$

Последнее выражение демонстрирует тесную связь между классами смежности и классами сопряженности. Поскольку для подгруппы G_i отдельно левые и отдельно правые классы смежности *не пересекаются*, они также являются *классами эквивалентности*, и так как подгруппа G_i не изменяется под трансформационным действием элемента g , ее называют *инвариантной* или *нормальным делителем* группы G (обозначают $N = G_i$).

Введем понятие *факторгруппы*. С этой целью рассмотрим два класса смежности Nx и Ny (для нормального делителя N не имеет значения, какие классы — левые или правые). Выберем из этих классов по конкретному представителю: $a \in Nx, b \in Ny$ и составим из них произведение $a \cdot b$. Полученный таким образом новый элемент будет принадлежать классу смежности Nxy , что нетрудно доказать. Для этого запишем:

$$\begin{aligned} a \cdot b &= mx \cdot ny = mx \cdot n \cdot e \cdot y = mx \cdot n \cdot (x^{-1}x) \cdot y = m \cdot (xnx^{-1}) \cdot xy = mly \in Nxy; \\ a &= mx, \quad b = ny; & N &= xNx^{-1}; & m, n, l, lm &\in N. \end{aligned}$$

Представленное доказательство одновременно демонстрирует условие *замкнутости*, при котором один смежный класс Nx умножится на другой Ny и получится третий Nxy , причем все элементы классы принадлежат группе G . Так при помощи нормального делителя N получилась факторгруппа, которую обозначают G/N . Роль тождественного элемента для факторгруппы G/N играет сам

нормальный делитель N . В качестве обратных элементов для Nx и Ny выступают Nx^{-1} и Ny^{-1} . Закон ассоциативности здесь также не нарушается. Порядок факторгруппы $|G/N|$ равен индексу инвариантной подгруппы $|G:N|$.

В нашем примере с D_3 имеется только один нормальный делитель — подгруппа G_4 , поэтому здесь можно построить только одну факторгруппу D_3/G_4 с таблицей умножения — табл. 2.30. Из таблицы видно, как элементы группы D_3 проецируются на группу второго порядка. Такое отношение между группами называется *гомоморфизмом*. В случае построения именно факторгруппы получается так называемый *естественный* или *канонический* гомоморфизм. Но элементы группы D_3 можно проецировать ($\rightarrow$) на *любую* подгруппу второго порядка, в том числе и на подгруппу, например $G_1 = \{0, 1\}$, т.е. имеет место *изоморфизм*:

Таблица 2.30

$$D_3/G_4 \approx G_1: \text{ если } D_3 \rightarrow G_1, \text{ то } \begin{array}{|c|c|} \hline \{0, 4, 5\} & \{1, 2, 3\} \\ \hline \{1, 2, 3\} & \{0, 4, 5\} \\ \hline \end{array}$$

$$\{0, 4, 5\} \rightarrow 0 \text{ и } \{1, 2, 3\} \rightarrow 1.$$

В этом специальном случае, когда элементы группы G проецируются на элементы своей подгруппы, гомоморфизм уже называется *эндоморфизмом*.

Добавим также, что нормальный делитель, по которому строится факторгруппа, называется *ядром* гомоморфизма. При эндоморфизме ядро проецируется на тождественный элемент неинвариантной подгруппы. В проекции $D_3 \rightarrow G_1$ группа G_1 называется *образом*, а группа D_3 — *прообразом*.

Введем понятие *внутреннего автоморфизма* группы G , которое определяется следующим преобразованием —

$$x = g y g^{-1}.$$

Автоморфное преобразование отличается от похожего на него *трансформационного* тем, что элемент g фиксирован, а x и y пробегает все элементы группы G .

Найдем внутренний автоморфизм для нашей группы D_3 :

$$\begin{aligned} 0 \cdot 0 \cdot 0^{-1} &= 0, & 1 \cdot 0 \cdot 1^{-1} &= 0, & 2 \cdot 0 \cdot 2^{-1} &= 0, & 3 \cdot 0 \cdot 3^{-1} &= 0, & 4 \cdot 0 \cdot 4^{-1} &= 0, & 5 \cdot 0 \cdot 5^{-1} &= 0, \\ 0 \cdot 1 \cdot 0^{-1} &= 1, & 1 \cdot 1 \cdot 1^{-1} &= 1, & 2 \cdot 1 \cdot 2^{-1} &= 3, & 3 \cdot 1 \cdot 3^{-1} &= 2, & 4 \cdot 1 \cdot 4^{-1} &= 2, & 5 \cdot 1 \cdot 5^{-1} &= 3, \\ 0 \cdot 2 \cdot 0^{-1} &= 2, & 1 \cdot 2 \cdot 1^{-1} &= 3, & 2 \cdot 2 \cdot 2^{-1} &= 2, & 3 \cdot 2 \cdot 3^{-1} &= 1, & 4 \cdot 2 \cdot 4^{-1} &= 3, & 5 \cdot 2 \cdot 5^{-1} &= 1, \\ 0 \cdot 3 \cdot 0^{-1} &= 3, & 1 \cdot 3 \cdot 1^{-1} &= 2, & 2 \cdot 3 \cdot 2^{-1} &= 1, & 3 \cdot 3 \cdot 3^{-1} &= 3, & 4 \cdot 3 \cdot 4^{-1} &= 1, & 5 \cdot 3 \cdot 5^{-1} &= 2, \\ 0 \cdot 4 \cdot 0^{-1} &= 4, & 1 \cdot 4 \cdot 1^{-1} &= 5, & 2 \cdot 4 \cdot 2^{-1} &= 5, & 3 \cdot 4 \cdot 3^{-1} &= 5, & 4 \cdot 4 \cdot 4^{-1} &= 4, & 5 \cdot 4 \cdot 5^{-1} &= 4, \\ 0 \cdot 5 \cdot 0^{-1} &= 5, & 1 \cdot 5 \cdot 1^{-1} &= 4, & 2 \cdot 5 \cdot 2^{-1} &= 4, & 3 \cdot 5 \cdot 3^{-1} &= 4, & 4 \cdot 5 \cdot 4^{-1} &= 5, & 5 \cdot 5 \cdot 5^{-1} &= 5. \end{aligned}$$

Числа, отвечающее y , образуют верхнюю строку подстановок автоморфизма, а числа, отвечающие x , — нижнюю строку этих подстановок. Тогда в циклической форме подстановки внутреннего автоморфизма примут вид:

$$0' = (0), \quad 1' = (23)(45), \quad 2' = (13)(45), \quad 3' = (12)(45), \quad 4' = (123), \quad 5' = (123).$$

Вновь полученные подстановки образуют группу, изоморфную исходной группе D_3 . Такое совпадение неслучайно и объясняется оно тем, что *внутренний автоморфизм группы G всегда изоморфен факторгруппе G/Z* . Так как *центр Z группы D_3 состоит из единственного тождественного элемента*, то и получилось:

$$D_3/Z \approx D_3 \approx \{0', 1', 2', 3', 4', 5'\}.$$

Здесь надо помнить, что центр любой группы является ее нормальным делителем и построение по нему соответствующей факторгруппы всегда возможно.

Проведем *морфологический анализ* кватерниона D_4^2 с подстановками:

$$0 = (0), \quad 1 = (0123)(4756), \quad 2 = (02)(13)(45)(67), \quad 3 = (0321)(4657), \\ 4 = (0425)(1637), \quad 5 = (0524)(1736), \quad 6 = (0627)(1534), \quad 7 = (0726)(1435).$$

Группа D_4^2 разбивается на пять классов сопряженности:

$$C_0 = \{0\}, \quad C_1 = \{2\}, \quad C_2 = \{1, 3\}, \quad C_3 = \{4, 5\}, \quad C_4 = \{6, 7\}.$$

Таблица умножения классов представлена табл. 2.31. Все подгруппы кватерниона G_i *инвариантны*.

Таблица 2.31

C_0	C_1	C_2	C_3	C_4
C_1	$2 \cdot C_0 + 2 \cdot C_1$	C_2	C_3	C_4
C_2	C_2	$2 \cdot C_0 + 2 \cdot C_1$	$2 \cdot C_4$	$2 \cdot C_3$
C_3	C_3	$2 \cdot C_4$	$2 \cdot C_0 + 2 \cdot C_1$	$2 \cdot C_2$
C_4	C_4	$2 \cdot C_3$	$2 \cdot C_2$	$2 \cdot C_0 + 2 \cdot C_1$

В группе D_4^2 имеются четыре нетривиальные подгруппы:

$$G_1 = \{0, 2\}, \quad G_2 = \{0, 1, 2, 3\}, \quad G_3 = \{0, 2, 4, 5\}, \quad G_4 = \{0, 2, 6, 7\}.$$

Таблица умножения смежных классов для факторгрупп D_4^2/G_3 и D_4^2/G_1 представлены соответственно табл. 2.32 и табл. 2.33. Таблицы умножения для D_4^2/G_2 и D_4^2/G_4 аналогичны табл. 2.32.

Таблица 2.32

$\{0, 2, 4, 5\}$	$\{1, 3, 6, 7\}$
$\{1, 3, 6, 7\}$	$\{0, 2, 4, 5\}$

Таблица 2.33

$\{0, 2\}$	$\{1, 3\}$	$\{4, 5\}$	$\{6, 7\}$
$\{1, 3\}$	$\{0, 2\}$	$\{6, 7\}$	$\{4, 5\}$
$\{4, 5\}$	$\{6, 7\}$	$\{0, 2\}$	$\{1, 3\}$
$\{6, 7\}$	$\{4, 5\}$	$\{1, 3\}$	$\{0, 2\}$

Центр кватерниона состоит из двух элементов $Z = G_1 = \{0, 2\}$. Следовательно, его *внутренний автоморфизм* будет состоять только из четырех подстановок:

$$D_4^2/Z = \{(0), (45)(67), (13)(67), (13)(45)\} \approx C_2^2.$$

— *внутренний автоморфизм кватерниона изоморфен группе C_2^2* (табл. 2.33).

Введем понятие *голоморфа* и проанализируем его свойства. Это сделаем сначала на основе группы диэдра D_3 , затем кватерниона D_4^2 . С этой целью составим обычную таблицу умножения для D_3 (табл. 2.34) и выпишем для нее *регулярные подстановки*, причем отдельно отвечающие *столбцам* (их называют *правыми*) и отдельно — *строкам* (*левые*, выделены штрихом):

D_3 : D'_3 :

Таблица 2.34

$0 = (0),$
 $1 = (01)(25)(34),$
 $2 = (02)(14)(35),$
 $3 = (03)(15)(24),$
 $4 = (045)(123),$
 $5 = (054)(132),$

$0 = (0),$
 $1' = (01)(24)(35),$
 $2' = (02)(15)(34),$
 $3' = (03)(14)(25),$
 $4' = (045)(132),$
 $5' = (054)(123).$

0	1	2	3	4	5
1	0	4	5	2	3
2	5	0	4	3	1
3	4	5	0	1	2
4	3	1	2	5	0
5	2	3	1	0	4

Перемножим эти подстановки:

$11' = (23)(45),$ $21' = (04)(12),$ $31' = (05)(13),$ $41' = (025143),$ $51' = (034152),$
 $12' = (05)(12),$ $22' = (13)(45),$ $32' = (04)(23),$ $42' = (035241),$ $52' = (014253),$
 $13' = (04)(13),$ $23' = (05)(23),$ $33' = (12)(45),$ $43' = (015342),$ $53' = (024351),$
 $14' = (035142),$ $24' = (015243),$ $34' = (025341),$ $44' = (054),$ $54' = (123),$
 $15' = (024153),$ $25' = (034251),$ $35' = (014352),$ $45' = (132),$ $55' = (045).$

Поскольку все левые регулярные подстановки коммутируют со всеми правыми, других подстановок здесь нет: перед нами группа 36-го порядка, которая и является голоморфом группы диэдра D_3 .

Голоморф какой-либо группы G , который мы обозначим как $\mathbf{H}(G)$, является группой и обладает тем замечательным свойством, что среди его нормальных делителей всегда имеются две подгруппы, отвечающие его правым и левым регулярным подстановкам. Удостоверимся, что голоморф $\mathbf{H}(D_3)$ имеет в своем составе две инвариантные подгруппы — D_3 и D'_3 . Для этого проведем морфологический анализ группы $\mathbf{H}(D_3)$. Прежде всего найдем все классы сопряженности $\mathbf{H}(D_3)$:

$C_0 = \{0\},$ $C_1 = \{1, 2, 3\},$ $C_2 = \{4, 5\},$ $C_3 = \{1', 2', 3'\},$
 $C_4 = \{4', 5'\},$ $C_5 = \{11', 12', 13', 21', 22', 23', 31', 32', 33'\},$
 $C_6 = \{44', 45', 54', 55'\},$ $C_7 = \{14', 15', 24', 25', 34', 35'\},$
 $C_8 = \{41', 42', 43', 51', 52', 53'\}.$

В голоморфе $\mathbf{H}(D_3)$ имеется 15 подгрупп второго порядка, отвечающих подстановкам на транспозициях, и 4 третьего порядка, причем две из них являются нормальными делителями —

$N_1 = \{0, 4, 5\},$ $N_2 = \{0, 4', 5'\}.$

Далее, имеется 9 подгрупп четвертого порядка типа $\{0, 1, 1', 11'\}$ (все они не инвариантны). Подгруппы шестого порядка распределены следующим образом: 6 подгрупп отвечают 6-циклам и 12 диэдральных, причем 6 из них типа $\{0, 33', 44', 55', 12', 21'\}$ и 6 типа $\{0, 11', 12', 13', 4', 5'\}$. Сравнивая элементы этих подгрупп с элементами выписанных классов сопряженности, можно заключить, что ни одна из упомянутых 18 подгрупп шестого порядка не будет инвариантной, и только две исходные группы на регулярных подстановках D_3 и D'_3 дадут нормальные делители индекса 6, которые обозначим как

$N_3 = \{0, 1, 2, 3, 4, 5\},$ $N_4 = \{0, 1', 2', 3', 4', 5'\}.$

В нашем голоморфе содержатся 6 неинвариантных диэдральных подгрупп двенадцатого порядка $\{0, 1', 2', 3', 4', 5', 11', 12', 13', 14', 15'\}$, один нормальный делитель 9-го порядка коммутативной структуры:

$$N_5 = \{0, 4, 5, 4', 5', 44', 54', 45', 55'\},$$

и 3 нормальных делителя двенадцатого порядка с двумя различными некоммутативными структурами:

$$N_6 = \{0, 4, 5, 4', 5', 44', 54', 45', 55', 11', 12', 13', 21', 22', 23', 31', 32', 33'\},$$

$$N_7 = \{0, 1', 2', 3', 4', 5', 4, 5, 41', 42', 43', 44', 45', 51', 52', 53', 54', 55'\},$$

$$N_8 = \{0, 1', 2', 3', 4', 5', 4, 5, 14', 15', 24', 25', 34', 35', 44', 45', 54', 55'\}.$$

(Можно доказать, что все подгруппы индекса 2 являются нормальными делителями своих групп.) В голоморфе неинвариантные подгруппы *взаимно сопряжены*, т.е. переходят друг в друга ($G_i \rightarrow G_j$) посредством элемента g , не входящего ни в G_i , ни в G_j , например:

$$\begin{array}{lll} 52' \cdot 0 \cdot 42' = 0, & 24' \cdot 0 \cdot 25' = 0, & 14' \cdot 0 \cdot 15' = 0, \\ 52' \cdot 1 \cdot 42' = 3, & 24' \cdot 3 \cdot 25' = 1, & 14' \cdot 2' \cdot 15' = 1', \\ 52' \cdot 4' \cdot 42' = 5', & 24' \cdot 5' \cdot 25' = 5', & 14' \cdot 4 \cdot 15' = 5, \\ 52' \cdot 5' \cdot 42' = 4', & 24' \cdot 4' \cdot 25' = 4', & 14' \cdot 5 \cdot 15' = 4, \\ 52' \cdot 14' \cdot 42' = 35', & 24' \cdot 35' \cdot 25' = 15', & 14' \cdot 42' \cdot 15' = 51', \\ 52' \cdot 15' \cdot 42' = 34', & 24' \cdot 34' \cdot 25' = 14', & 14' \cdot 52' \cdot 15' = 41'. \end{array}$$

Найдем гомоморфизм голоморфа $H(D_3)$ с ядром N_4 , т.е. $H(D_3)/N_4$:

$$\begin{array}{ll} \{0, 1', 2', 3', 4', 5'\} \rightarrow 0, & \{3, 31', 32', 33', 34', 35'\} \rightarrow 3, \\ \{1, 11', 12', 13', 14', 15'\} \rightarrow 1, & \{4, 41', 42', 43', 44', 45'\} \rightarrow 4, \\ \{2, 21', 22', 23', 24', 25'\} \rightarrow 2, & \{5, 51', 52', 53', 54', 55'\} \rightarrow 5. \end{array}$$

Элементы образа этого гомоморфизма удовлетворяют группе D_3 :

$$H(D_3)/D_3 \approx D_3, \quad (2.28)$$

— гомоморфизм голоморфа $(H(D_3)/D_3)$, ядром которого является исходная группа (D_3) , изоморфен ($\approx$) внутреннему автоморфизму (D_3) .

Изящность формулы (2.28) объясняется тем, что центр Z группы D_3 состоит из одного тождественного элемента. Ситуация будет несколько иной в случае кватерниона, но прежде чем мы приступим к анализу D_4^2 , покажем на примере диэдрального голоморфа $H(D_3)$ действие одной важной формулы, которая, однако, применима к любым группам, где имеется соответствующий расклад нормальных делителей.

Найдем три системы гомоморфных прожекций —

$$H(D_3)/N_1:$$

$$\begin{array}{ll} \{0, 4, 5\} \rightarrow 0, & \{1, 2, 3\} \rightarrow 1, \\ \{1', 41', 51'\} \rightarrow 1', & \{11', 21', 31'\} \rightarrow 11', \\ \{2', 42', 52'\} \rightarrow 2', & \{12', 22', 32'\} \rightarrow 12', \\ \{3', 43', 53'\} \rightarrow 3', & \{13', 23', 33'\} \rightarrow 13', \\ \{4', 44', 54'\} \rightarrow 4', & \{14', 24', 34'\} \rightarrow 14', \\ \{5', 45', 55'\} \rightarrow 5', & \{15', 25', 35'\} \rightarrow 15'; \end{array}$$

$H(D_3)/N_5$:

$\{0, 4, 5, 4', 5', 44', 54', 45', 55'\} \rightarrow 0$,
 $\{1, 2, 3, 14', 15', 24', 25', 34', 35'\} \rightarrow 1$,
 $\{1', 2', 3', 41', 51', 42', 52', 43', 53'\} \rightarrow 1'$,
 $\{11', 12', 13', 21', 22', 23', 31', 32', 33'\} \rightarrow 11'$;

N_5/N_1 :

$\{0, 4, 5\} \rightarrow 0$, $\{4', 44', 54'\} \rightarrow 4'$, $\{5', 45', 55'\} \rightarrow 5'$.

Из первой и третьей составим четвертую проекцию $(H(D_3)/N_1)/(N_5/N_1)$:

$\{0, 4', 5'\} \rightarrow 0$, $\{1', 2', 3'\} \rightarrow 1'$, $\{1, 14', 15'\} \rightarrow 1$, $\{11', 12', 13'\} \rightarrow 11'$.

Итак, мы получили, что $(H(D_3)/N_1)/(N_5/N_1) \approx H(D_3)/N_5 \approx \{0, 1, 1', 11'\}$.

В общем случае справедлива формула сокращения наименьшего нормального делителя:

$$(A / C) / (B / C) \approx A / B, \quad (2.29)$$

т.е. нормальные делители групп ведут себя подобно числовым делителям, в частности:

$$(36/3)/(9/3) = 36/9, (36/6)/(18/6) = 36/18.$$

Теперь по изложенной методике построим голоморф на базе кватерниона $H(D_4^2)$ (табл. 2.35). Его порядок равен уже не 64 м, как это могло показаться на первый взгляд (8×8), а только 32-м. Объясняется это тем, что порядок центра кватерниона равен двум. Формула, по которой рассчитывается порядок голоморфа $H(G)$, следующая –

$$|H(G)| = \frac{|G|^2}{Z_G}.$$

Таблица 2.35

0	1	2	3	4	5	6	7
1	2	3	0	6	7	5	4
2	3	0	1	5	4	7	6
3	0	1	2	7	6	4	5
4	7	5	6	2	0	1	3
5	6	4	7	0	2	3	1
6	4	7	5	3	1	2	0
7	5	6	4	1	3	0	2

Выпишем все 32 подстановки $H(D_4^2)$:

$0 = (0)$, $0' = 0$, $2 = (02)(13)(45)(67)$, $2' = 2$,
 $1 = (0123)(4756)$, $1' = (0123)(4657)$, $11' = 33' = (02)(13)$, $41' = 53' = (06)(15)(27)(34)$,
 $3 = (0321)(4657)$, $3' = (0321)(4756)$, $13' = 31' = (45)(67)$, $43' = 51' = (0627)(1435)$,
 $4 = (0425)(1637)$, $4' = (0425)(1736)$, $14' = 35' = (07)(15)(26)(34)$, $44' = 55' = (02)(45)$,
 $5 = (0524)(1736)$, $5' = (0524)(1637)$, $15' = 34' = (06)(14)(27)(35)$, $45' = 54' = (13)(67)$,
 $6 = (0627)(1534)$, $6' = (0627)(1435)$, $16' = 37' = (04)(17)(25)(36)$, $46' = 57' = (03)(12)(47)(56)$,

$$\begin{aligned}
7 &= (0726)(1435), & 7' &= (0726)(1534), & 17' &= 36' = (05)(16)(24)(37), & 47' &= 56' = (01)(23)(46)(57), \\
67' &= 73' = (05)(17)(24)(36), & & & 65' &= 74' = (03)(12)(46)(57), \\
63' &= 71' = (04)(16)(25)(37), & & & 66' &= 77' = (02)(67), \\
64' &= 75' = (01)(23)(47)(56), & & & 67' &= 76' = (13)(45).
\end{aligned}$$

Разобьем голоморф $H(D_4^2)$ на классы:

$$\begin{aligned}
C_1 &= \{1, 3\}, & C_5 &= \{4', 5'\}, & C_9 &= \{14', 15'\}, & C_{13} &= \{46', 47'\}, \\
C_2 &= \{2\}, & C_6 &= \{6, 7\}, & C_{10} &= \{16', 17'\}, & C_{14} &= \{61', 63'\}, \\
C_3 &= \{1', 3'\}, & C_7 &= \{6', 7'\}, & C_{11} &= \{41', 43'\}, & C_{15} &= \{64', 65'\}, \\
C_4 &= \{4, 5\}, & C_8 &= \{11', 13'\}, & C_{12} &= \{44', 45'\}, & C_{16} &= \{66', 67'\}.
\end{aligned}$$

Один из кватернионов группы $H(D_4^2)$, а именно —

$$N_1 = \{0, 1', 2', 3', 4', 5', 6', 7'\}$$

используем для построения проекции $H(D_4^2)/N_1$:

$$\begin{aligned}
\{0, 1', 2, 3', 4', 5', 6', 7'\} &\rightarrow 0, & \{1, 11', 3, 13', 14', 15', 16', 17'\} &\rightarrow 1, \\
\{4, 41', 5, 43', 44', 45', 46', 47'\} &\rightarrow 4, & \{6, 61', 7, 63', 64', 65', 66', 67'\} &\rightarrow 6.
\end{aligned}$$

Элементы $\{0, 1, 4, 6\}$ факторгруппы $H(D_4^2)/N_1$ перемножаются в соответствии с таблицей умножения группы C_2^2 . Таким образом, для кватерниона имеем

$$H(D_4^2)/D_4^2 \approx C_2^2,$$

что существенно отличается от результата для диэдра (2.28).

В состав $H(D_4^2)$ входит делитель

$$N_2 = \{0, 1, 2, 3, 1', 3', 4', 5', 6', 7', 11', 13', 14', 15', 16', 17'\},$$

используем его для нахождения еще двух гомоморфизмов —

$$H(D_4^2)/N_2:$$

$$\begin{aligned}
\{0, 1, 2, 3, 1', 3', 4', 5', 6', 7', 11', 13', 14', 15', 16', 17'\} &\rightarrow 0, \\
\{4, 5, 6, 7, 41', 43', 44', 45', 46', 47', 61', 63', 64', 65', 66', 67'\} &\rightarrow 1,
\end{aligned}$$

$$N_2/N_1:$$

$$\{0, 1', 3', 4', 5', 6', 7'\} \rightarrow 0, \quad \{1, 3, 11', 13', 14', 15', 16', 17'\} \rightarrow 1.$$

Формула сокращения наименьшего нормального делителя (2.29) для делителей кватерниона тоже подтвердилась —

$$(H(D_4^2)/N_1)/(N_2/N_1) \approx H(D_4^2)/N_2.$$

2.6. Геометрическая интерпретация групповых преобразований

На рис. 2.3 изображены ромб (а) и прямоугольник (б). Вершины этих простых геометрических фигур образуют *субстанционные* или *базисные* множества, которые насчитывают по четыре элемента. Пачав вращать эти симметричные фигуры относительно обозначенных на рисунке горизонтальных и вертикальных осей, а также вокруг необозначенных осей, направленных перпендикулярно к плоскости рисунка, мы получим множество *отображений* или *операционных* элементов в виде подстановок. Так появляются две изоморфных группы подстановок типа C_2^2

— для ромба:

$$e = (0), \quad a = (02), \quad b = (13), \\ ab = (02)(13);$$

и для прямоугольника:

$$e = (0), \quad a = (01)(23), \quad b = (03)(12), \\ ab = (02)(13).$$

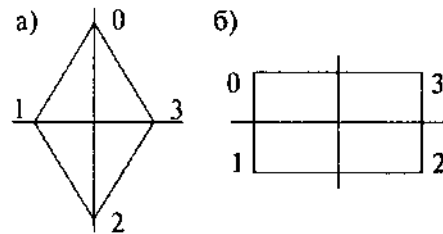


Рис. 2.3

Здесь в обоих случаях число субстанционных элементов, представленных вершинами фигур, совпадает с числом операционных.

Теперь изменим субстанционные множества: пусть для ромба в качестве базисных выступают два элемента — верхняя и нижняя его поверхности, а для прямоугольника две его диагонали — 0–2 и 1–3. Тогда группы операционных элементов тоже уменьшатся в два раза и станут типа C_2 .

Повороты геометрических фигур в пространстве представляют собой *линейные преобразования* (2.1), в которых в качестве операторов A могут выступать 0,1-матрицы. Степень периодичности наших матриц равна двум, значит, их собственными значениями (2.11) являются числа $(+1)$ и (-1) . Положительная и отрицательная единицы образуют группу C_2 , гомоморфную группе C_2^2 . В коммутативных группах каждый элемент образует класс эквивалентности. Поставим в соответствие каждому элементу группы C_2^2 столбец из собственных значений (табл. 2.36). Классы эквивалентности не пересекаются. Этот факт отражается в том, что скалярные произведения столбцов должны быть равны нулю. Следовательно, в табл. 2.36 все положительные и отрицательные единицы надо расставить так, чтобы произведение векторов-столбцов отвечало этим требованиям. Такая расстановка собственных значений автоматически приводит к выполнению условия *ортонормированности* и в отношении строк E_i , которые называются *представлениями* группы C_2^2 . Все представления у нас получились гомоморфными, причем представление E_0 является *единичным*, так как элементы группы C_2^2 проецируются на тривиальную группу *тождественного элемента* G_0 (или C_1). Проецирование $C_2^2 \rightarrow C_2$ можно осуществить тремя способами — E_1 , E_2 и E_3 .

В группе C_4 так же, как и C_2^2 , четыре элемента. С точки зрения геометрии, она отвечает вращению квадрата в плоскости рисунка (рис. 2.4б). Собственными значениями 0,1-матриц, которые соответствуют группе подстановок C_4 :

$$e = (0), \quad a = (0123), \quad a^2 = (02)(13), \quad a^3 = (0321),$$

служат корни четвертой степени из единицы (см. табл. 2.37). Проецирование элементов группы C_4 на эти корни дает четыре возможных представления, два из которых (E_0 и E_1) являются *гомоморфизмами*, а два (E_2 и E_3) — *изоморфизмами*.

Представление E_0 соответствует проецированию всей группы C_4 на единицу $\{e\}$; представление E_1 есть проекция C_4 на подгруппу $\{e, a^2\}$; представления E_2 и E_3 осуществляют проецирование элементов C_4 на собственные значения 0,1-матриц, отвечающие элементам a и a^3 . Произведение столбцов a на a^3 и строк E_2 на E_3 уже не равно нулю, т.е. *изоморфные представления не будут ортогональными*. Это связано с тем, что элементы a и a^3 попадают в один *абсолютный*

класс эквивалентности, в результате чего выполняются следующие соотношения:

$$E_0 \cdot E_1 = E_0 \cdot E_2 = E_0 \cdot E_3 = E_1 \cdot E_2 = E_1 \cdot E_3 = 0, \text{ но } E_2 \cdot E_3 = 4.$$

Введенные понятия об *относительном* и *абсолютном подобии* позволяют объяснить наличие или отсутствие ортогональности между отдельными представлениями коммутативных групп.

Таблица представлений для группы C_2 тривиальна (табл. 2.38). Мы бы ее не приводили, если бы не одно обстоятельство: она поможет нам понять принцип построения таблиц представлений больших размерностей.

Таблица 2.36

C_2^2	e	a	b	ab
E_0	1	1	1	1
E_1	1	-1	1	-1
E_2	1	1	-1	-1
E_3	1	-1	-1	1

Таблица 2.37

C_4	e	a	a^2	a^3
E_0	1	1	1	1
E_1	1	-1	1	-1
E_2	1	i	-1	$-i$
E_3	1	$-i$	-1	i

Таблица 2.38

C_2	e	a
E_0	1	1
E_1	1	-1

Остановимся на вращениях в плоскости рисунка правильного треугольника (рис. 2.4а), пятиугольника (рис. 2.5) и семиугольника, которые образуют *простые циклические группы* C_3 , C_5 и C_7 . Для них все представления являются *изоморфизмами*, за исключением единичного E_0 : C_3 (табл. 2.39), C_5 (табл. 2.40), C_7 (табл. 2.41), причем прямая и обратная подстановки попадают в один абсолютный класс эквивалентности. Следовательно, в один класс неортогональных друг к другу представлений в группе C_5 , например, попадут представления E_1 и E_4 или E_2 и E_3 .

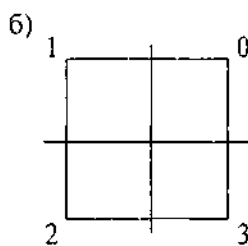
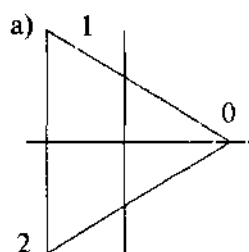


Рис. 2.4

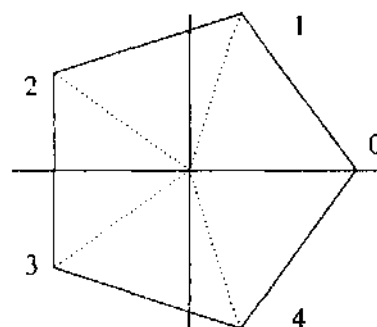


Рис. 2.5

Корни 3-й, 5-й и 7-й степени из единицы (ω_i) расставляются по строкам и столбцам таблиц представлений соответственно своим подстановкам. Это значит, что индексы при ω_i , например, для группы правильного пятиугольника C_5 чередуются в соответствии с индексами следующих четырех подстановок:

$$a = (01234), \quad a^2 = (02413), \quad a^3 = (03142), \quad a^4 = (04321).$$

Таблица 2.39

C_3	e	a	a^2
E_0	1	1	1
E_1	1	ω_1	ω_2
E_2	1	ω_2	ω_1

Таблица 2.40

C_5	e	a	a^2	a^3	a^4
E_0	1	1	1	1	1
E_1	1	ω_1	ω_2	ω_3	ω_4
E_2	1	ω_2	ω_4	ω_3	ω_1
E_3	1	ω_3	ω_1	ω_4	ω_2
E_4	1	ω_4	ω_3	ω_2	ω_1

Таблица 2.41

C_7	e	a	a^2	a^3	a^4	a^5	a^6
E_0	1	1	1	1	1	1	1
E_1	1	ω_1	ω_2	ω_3	ω_4	ω_5	ω_6
E_2	1	ω_2	ω_4	ω_6	ω_1	ω_3	ω_5
E_3	1	ω_3	ω_6	ω_2	ω_5	ω_1	ω_4
E_4	1	ω_4	ω_1	ω_5	ω_2	ω_6	ω_3
E_5	1	ω_5	ω_3	ω_1	ω_6	ω_4	ω_2
E_6	1	ω_6	ω_5	ω_4	ω_3	ω_2	ω_1

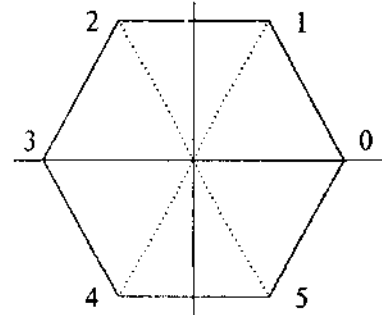


Рис. 2.6

Согласно симметрии правильного шестиугольника (рис. 2.6), группа C_6 имеет, помимо *единичного* класса $\{E_0\}$, еще два *абсолютных* класса *гомоморфных* представлений — $\{E_1\}$, $\{E_2, E_3\}$, а также один класс *изоморфных* представлений — $\{E_4, E_5\}$, которые расписаны в табл. 2.42. В ней приняты следующие обозначения корней:

$$\omega = \omega^4, \quad -\omega^2 = \omega^5, \quad -1 = \omega^3.$$

Таблица 2.42

C_6	e	a	a^2	a^3	a^4	a^5
E_0	1	1	1	1	1	1
E_1	1	-1	1	-1	1	-1
E_2	1	ω^2	$-\omega$	1	ω^2	$-\omega$
E_3	1	$-\omega$	ω^3	1	$-\omega$	ω^2
E_4	1	ω	ω^2	-1	$-\omega$	$-\omega^2$
E_5	1	$-\omega^2$	ω	-1	ω^2	ω

Обозначения для элементов представлений группы C_8 можно выбрать такие же, как и для группы C_6 (табл. 2.42), если помнить, что

$$1 = \omega_0, \quad -1 = \omega_4, \quad i = \omega_2, \quad -i = \omega_6, \quad -\omega^3 = \omega_7, \quad -\omega = \omega_5.$$

Однако при составлении нашей табл. 2.43 использовалась методика чередования индексов корней при ω_i , согласно подстановкам группы C_8 . Здесь изоморфный класс состоит уже не из двух, а из четырех представлений — $\{E_1, E_3, E_5, E_7\}$. Остальные классы абсолютной эквивалентности гомотоморфны — $\{E_0\}$, $\{E_4\}$, $\{E_2, E_6\}$.

Таблица 2.43

C_8	e	a	a^2	a^3	a^4	a^5	a^6	a^7
E_0	ω_0	ω_0	ω_0	ω_0	ω_0	ω_0	ω_0	ω_0
E_1	ω_0	ω_1	ω_3	ω_7	ω_4	ω_5	ω_6	ω_2
E_2	ω_0	ω_2	ω_4	ω_6	ω_0	ω_2	ω_4	ω_6
E_3	ω_0	ω_3	ω_6	ω_1	ω_4	ω_7	ω_2	ω_5
E_4	ω_0	ω_4	ω_0	ω_4	ω_0	ω_4	ω_0	ω_4
E_5	ω_0	ω_5	ω_2	ω_7	ω_4	ω_7	ω_6	ω_3
E_6	ω_0	ω_6	ω_4	ω_2	ω_0	ω_6	ω_4	ω_2
E_7	ω_0	ω_7	ω_1	ω_3	ω_4	ω_3	ω_2	ω_1

Две последующие таблицы представлений для коммутативных групп восьмого порядка — $C_2^3 \cong C_2 C_2^2$ (табл. 2.44) и $C_2 C_4$ (табл. 2.45) — получены из элементов C_2^2 (табл. 2.36) и C_4 (табл. 2.37), путем умножения их на 1 или (-1) , отвечающих группе C_2 (табл. 2.38).

Таблицы представлений для коммутативных групп больших порядков составляются по аналогии с рассмотренными. Далее переходим к анализу *некоммутативных* групп.

Таблица 2.44

C_2^3	e	a	b	ab	c	ac	bc	abc
E_0	1	1	1	1	1	1	1	1
E_1	1	-1	1	-1	1	-1	1	-1
E_2	1	1	-1	-1	1	1	-1	-1
E_3	1	-1	-1	1	1	-1	-1	1
E_4	1	1	1	1	-1	-1	-1	-1
E_5	1	-1	1	-1	-1	1	1	1
E_6	1	1	-1	-1	-1	-1	1	1
E_7	1	1	1	1	1	1	1	-1

Таблица 2.45

$C_2 C_4$	e	a	a^2	a^3	b	ab	$a^2 b$	$a^3 b$
E_0	1	1	1	1	1	1	1	1
E_1	1	-1	1	-1	1	-1	1	-1
E_2	1	i	-1	- i	1	i	-1	- i
E_3	1	- i	-1	i	1	- i	-1	i
E_4	1	1	1	1	-1	-1	-1	-1
E_5	1	-1	1	-1	-1	1	-1	1
E_6	1	i	-1	- i	-1	- i	1	i
E_7	1	- i	-1	i	-1	i	1	- i

Начнем с группы диэдра D_3 . Она отвечает вращению равностороннего треугольника (рис. 2.4а) не только в плоскости рисунка, но и в пространстве оси z , перпендикулярной к осям x и y . В группу D_3 входят шесть подстановок:

$$e = (0), \quad a = (012), \quad a^2 = (021), \quad b = (02), \quad ab = (01), \quad ba = (12),$$

которые разбиваются, как мы уже знаем, на три класса эквивалентности (для некоммутативных групп есть смысл говорить только об относительных классах эквивалентности):

$$C_0 = \{e\}, \quad C_1 = \{a, a^2\}, \quad C_2 = \{b, ab, ba\}.$$

Этим классам отвечают два гомоморфных (E_0 и E_1) и одно изоморфное *ортогональное* представление — E_2 (табл. 2.46). Поскольку свойство некоммутативности уже не может быть воспроизведено с помощью одномерных представлений из собственных значений, E_2 является *двухмерным*. Кроме того, в табл. 2.46 включено еще одно *неортогональное, эквивалентное* (относительно E_2) *двухмерное* представление E_3 и одно *трехмерное* E_4 . Матрицы последнего представления отвечают приведенным подстановкам группы D_3 .

Таблица 2.46

D_3	$e = (0)$	$a = (012)$	$a^2 = (021)$	$b = (02)$	$ab = (01)$	$ba = (12)$
E_0	1	1	1	1	1	1
E_1	1	1	1	-1	-1	-1
E_2	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$	$\begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$	$\begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$
E_3	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$	$\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$	$\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
E_4	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$

Можно подобрать такую трансформационную матрицу t , которая позволит разбить все 0,1-матрицы представления E_4 на сумму E_0 и E_3 :

$$E_0 + E_3 = t E_4 t^{-1}.$$

В частности, для элемента a группы D_3 будем иметь следующее разложение:

$$E_4(a) = E_0(a) + E_3(a) = \begin{pmatrix} 0 & 1 & 0 \\ -1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -2 & 1 \\ 1 & 1 & -2 \\ 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1/3 & 1/3 & 1/3 \\ -1/3 & 1/3 & 1/3 \\ 0 & 1/3 & 1/3 \end{pmatrix}.$$

Когда все матрицы одного представления E_a под действием трансформационной матрицы t разлагаются на сумму двух или большего числа других представлений ($E_\beta + E_\gamma + \dots$), в этом случае говорят, что представление E_a — *приводимо*. Если матрицы представлений E_β , E_γ и т.д. больше нельзя разложить на меньшие матрицы, значит, они являются *неприводимыми*. Так, все матрицы представлений E_0 , E_1 , E_2 и E_3 — *неприводимы*, поскольку невозможно найти такую трансформационную матрицу, чтобы в результате преобразования из них получились матрицы меньших размерностей. Заметим, что под «суммой» матричных пред-

ставлений следует понимать *прямую сумму* матриц, т.е. когда приводимая матрица трансформируется в *блочную диагональную*.

Про представления E_2 и E_3 было сказано, что они *эквивалентны*, т.е. существует такая матрица t_1 , которая способна трансформировать все матрицы E_2 в матрицы E_3 , и наоборот:

$$E_3 = t_1 E_2 t_1^{-1}, \quad E_2 = t_1^{-1} E_3 t_1.$$

Такая матрица t_1 существует. Продемонстрируем действие этой матрицы на элементе a :

$$\begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix}.$$

Таким образом, все матрицы представлений E_3 и E_4 в табл. 2.46 взаимосвязаны с *ортгональным неприводимым представлением* E_2 .

Единичное представление E_0 образовано базисом —

$$r = \sqrt{x^2 + y^2 + z^2}.$$

Базисом другого одномерного представления — E_1 — служит ось z . Оси x и y являются базисом для матриц E_2 , если учесть, что координаты на плоскости преобразуются по известным формулам:

$$x' = x \cos \varphi - y \sin \varphi, \quad y' = x \sin \varphi + y \cos \varphi,$$

то при значениях угла поворота в $2\pi/3$, имеем

$$\cos(2\pi/3) = -1/2, \quad \sin(2\pi/3) = \sqrt{3}/2,$$

и тогда преобразование координат примет следующую матричную форму —

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Вершины треугольника (рис. 2.4а) имеют координаты:

$$0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad 1 = \begin{pmatrix} 1/2 \\ \sqrt{3}/2 \end{pmatrix}, \quad 2 = \begin{pmatrix} -1/2 \\ \sqrt{3}/2 \end{pmatrix},$$

причем $2 = -0 - 1$. Этим вершинам соответствуют три *не ортогональных* друг к другу вектора — 0 , 1 , и 2 , которые образуют базис для представлений E_3 и E_4 . *Ортгональное* представление $E_2(a)$ и *неортгональное* $E_3(a)$ преобразуют свои системы базисных векторов:

$$\begin{pmatrix} 1/2 \\ \sqrt{3}/2 \end{pmatrix} = \begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Следует также напомнить, что существует так называемая *активная* система координат, когда объект (например, наш треугольник) находится в покое, а координатные оси вращаются вокруг него; и *пассивная*, когда система координат покоится, а объект вращается внутри нее. Кроме того, для согласования действия подстановок и матричных преобразований может быть использована противоположная расстановка сомножителей либо для матриц, либо для подстановок, т.е. для выполнения одного и того же группового преобразования для подстановок берется произведение ab , а для матриц — ba (или наоборот).

Если неприводимое матричное представление ортонормировано, то оно подчиняется следующему фундаментальному тождеству:

$$\sum_{g \in G} E_{\alpha}^{ij}(g) E_{\beta}^{kl}(g^{-1}) = \frac{n}{n_{\alpha}} \delta_{\alpha\beta} \delta_{ik} \delta_{jl}, \quad (2.30)$$

где g — элементы группы G , n — порядок группы G ,
 n_{α} — размерность матриц представления E_{α} ,
 $E_{\alpha}^{ij}(g) E_{\beta}^{kl}(g^{-1})$ — матричные элементы представлений.

Проиллюстрируем справедливость (2.30) на наших конкретных ортонормированных неприводимых представлениях E_1 и E_2 :

$$\sum_{g \in G} E_1^{11}(g) E_2^{21}(g^{-1}) = 0 \quad \text{и} \quad \sum_{g \in G} E_2^{22}(g) E_2^{22}(g^{-1}) = 3,$$

поскольку

$$1 \cdot 0 + 1 \cdot \frac{-\sqrt{3}}{2} + 1 \cdot \frac{\sqrt{3}}{2} + (-1) \cdot 0 + (-1) \cdot \frac{\sqrt{3}}{2} + (-1) \cdot \frac{-\sqrt{3}}{2} = 0$$

и

$$1^2 + \left(\frac{-1}{2}\right)^2 + \left(\frac{-1}{2}\right)^2 + (-1)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{6}{2} = 3.$$

Теперь, в соответствии с таблицей умножения элементов группы D_3 , построим одну 0,1-матрицу *регулярного* представления $E_5(a)$ (аналогичным образом находятся все остальные матрицы *приводимого* представления E_5):

$$\begin{pmatrix} a \\ a^2 \\ e \\ ab \\ ba \\ b \end{pmatrix} = a \cdot \begin{pmatrix} e \\ a \\ a^2 \\ b \\ ab \\ ba \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} e \\ a \\ a^2 \\ b \\ ab \\ ba \end{pmatrix}.$$

Существует такая трансформационная матрица T , которая позволит все матрицы E_5 разложить на матрицы *неприводимых* представлений E_0, E_1, E_2 . Для нахождения элементов матрицы T пользуемся элементами матриц E_0, E_1, E_2 (табл. 2.46) и формулой —

$$T_{\alpha}^{ij}(g) = E_{\alpha}^{ij}(g) \sqrt{\frac{n_{\alpha}}{n}}. \quad (2.31)$$

Произведем разложение матрицы $E_5(a)$ на неприводимые представления, используя конкретную трансформационную матрицу (2.31), получим:

$$E'_5(a) = T^{-1} \cdot E_5(a) \cdot T = E_0(a) + E_1(a) + 2 \cdot E_2(a), \quad (2.32)$$

где $E'_5(a)$ — блочно-диагональная матрица, имеющая вид:

$$E'_5(a) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1/2 & -\sqrt{3}/2 & 0 & 0 \\ 0 & 0 & \sqrt{3}/2 & -1/2 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1/2 & -\sqrt{3}/2 \\ 0 & 0 & 0 & 0 & \sqrt{3}/2 & -1/2 \end{pmatrix}.$$

Трансформационная матрица T выглядит так —

$$T = \begin{pmatrix} 1/\sqrt{6} & 1/\sqrt{6} & 1/\sqrt{6} & 1/\sqrt{6} & 1/\sqrt{6} & 1/\sqrt{6} \\ 1/\sqrt{6} & 1/\sqrt{6} & 1/\sqrt{6} & -1/\sqrt{6} & -1/\sqrt{6} & -1/\sqrt{6} \\ 1/\sqrt{3} & -1/2\sqrt{3} & -1/2\sqrt{3} & 1/\sqrt{3} & -1/2\sqrt{3} & -1/2\sqrt{3} \\ 0 & 1/2 & -1/2 & 0 & 1/2 & -1/2 \\ 1/\sqrt{3} & 1/2\sqrt{3} & -1/2\sqrt{3} & 1/\sqrt{3} & 1/2\sqrt{3} & 1/2\sqrt{3} \\ 0 & 1/2 & 1/2 & 0 & 1/2 & -1/2 \end{pmatrix}.$$

Таким образом, все регулярные матрицы $E_5(g)$ распадутся на прямую сумму блоков, причем каждый из блоков неприводимого представления $E_a(g)$ входит в блочно-диагональную матрицу $E'_5(g)$ ровно n_a раз. В нашем случае размерности представлений n_a равны: $n_0 = n_1 = 1$, $n_2 = 2$.

Наряду с прямой суммой можно ввести понятие о *прямом произведении* матриц. Пусть даны две матрицы A и B :

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}.$$

Определим их прямое произведение следующим образом:

$$A \times B = \begin{pmatrix} a_{11}B & a_{12}B & a_{13}B \\ a_{21}B & a_{22}B & a_{23}B \\ a_{31}B & a_{32}B & a_{33}B \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} & a_{13}b_{11} & a_{13}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} & a_{13}b_{21} & a_{13}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} & a_{23}b_{11} & a_{23}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} & a_{23}b_{21} & a_{23}b_{22} \\ a_{31}b_{11} & a_{31}b_{12} & a_{32}b_{11} & a_{32}b_{12} & a_{33}b_{11} & a_{33}b_{12} \\ a_{31}b_{21} & a_{31}b_{22} & a_{32}b_{21} & a_{32}b_{22} & a_{33}b_{21} & a_{33}b_{22} \end{pmatrix}.$$

В частности,

$$E_2(a) \times E_2(a) = \begin{pmatrix} 1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix} \times \begin{pmatrix} 1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix} = \begin{pmatrix} 1/4 & \sqrt{3}/4 & \sqrt{3}/4 & 3/4 \\ -\sqrt{3}/4 & 1/4 & -3/4 & \sqrt{3}/4 \\ -\sqrt{3}/4 & -3/4 & 1/4 & \sqrt{3}/4 \\ 3/4 & -\sqrt{3}/4 & -\sqrt{3}/4 & 1/4 \end{pmatrix}.$$

Ортонормированный базис двухмерного неприводимого представления $E_2(a)$ имеет вид:

$$x' = -\frac{1}{2}x - \frac{\sqrt{3}}{2}y, \quad y' = \frac{\sqrt{3}}{2}x - \frac{1}{2}y.$$

Если составить всевозможные произведения x' и y' ,

$$\begin{aligned}x'x' &= \frac{1}{4}xx + \frac{\sqrt{3}}{4}xy + \frac{\sqrt{3}}{4}yx - \frac{3}{4}yy, & x'y' &= -\frac{\sqrt{3}}{4}xx + \frac{1}{4}xy - \frac{3}{4}yx + \frac{\sqrt{3}}{4}yy, \\y'x' &= -\frac{\sqrt{3}}{4}xx - \frac{3}{4}xy + \frac{1}{4}yx + \frac{\sqrt{3}}{4}yy, & y'y' &= \frac{3}{4}xx - \frac{\sqrt{3}}{4}xy - \frac{\sqrt{3}}{4}yx + \frac{1}{4}yy,\end{aligned}$$

то станет понятен и смысл матрицы прямого произведения. Добавим, что при прямом перемножении свойство ортонормированности сохраняется.

Совокупность матриц прямых произведений образует новое представление группы D_3 , причем *приводимое*, которое мы обозначим как

$$E_6(a) = E_2(a) \times E_2(a).$$

Приводимость означает, что матрицы $E_6(a)$ каким-то образом раскладываются в прямую сумму неприводимых представлений. Чтобы уметь решать подобного рода задачи, необязательно искать соответствующие трансформационные матрицы типа (2.31). Достаточно знать характеры матричных представлений по трем классам эквивалентности C_0 , C_1 и C_2 группы D_3 . Затем, для определения числа неприводимых представлений E_α , содержащихся в приводимом E_β , необходимо воспользоваться простым соотношением:

$$E_\beta = \sum_{\alpha} m_{\alpha} E_{\alpha}, \quad \text{где } m_{\alpha} = \frac{1}{n} \sum_{g \in G} h_{\alpha} h_{\beta}, \quad (2.33)$$

здесь n — порядок группы G , h_{α} и h_{β} — характеры представлений E_{α} и E_{β} , которые приведены в табл. 2.47.

По формуле (2.33) найдем коэффициенты m_{α} сначала для приводимого представления E_4 :

Таблица 2.47

$$m_0 = 1/6 \cdot [3 \cdot 1 + 0 \cdot 1 + 0 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1] = 1,$$

$$m_1 = 1/6 \cdot [3 \cdot 1 + 0 \cdot 1 + 0 \cdot 1 + 1 \cdot (-1) + 1 \cdot (-1) + 1 \cdot (-1)] = 0,$$

$$m_2 = 1/6 \cdot [3 \cdot 2 + 0 \cdot (-1) + 0 \cdot (-1) + 1 \cdot 0 + 1 \cdot 0 + 1 \cdot 0] = 1.$$

$$\text{Отсюда получаем: } E_4 = E_0 + E_2.$$

D_3	C_0	C_1	C_2
E_0	1	1	1
E_1	1	1	-1
E_2	2	-1	0
E_3	2	-1	0
E_4	3	0	1
E_5	6	0	0
E_6	4	1	0

Аналогичным расчетом убеждаемся в справедливости еще одного известного нам разложения (2.32):

$$E_5 = E_0 + E_1 + 2 \cdot E_2.$$

В случае прямого произведения формула (2.33) не меняется и результат будет следующим:

$$E_6 = E_2 \times E_2 = E_0 + E_1 + E_2.$$

Для нахождения характеров представления E_6 необязательно искать матрицы прямых произведений $E_2 \times E_2$. Достаточно строку характеров E_2 (табл. 2.47) возвести в квадрат. Все другие разложения приводимых представлений (E_4 и E_5) на неприводимые (E_0 , E_1 , E_2) также можно проверить по таблице характеров.

Для характеров неприводимых представлений, как и для матриц, выполняется закон об ортонормированности (2.30), который удобно расписать на два соотношения — отдельно для *столбцов* (классов C_i) табл. 2.47 и отдельно для *строк* (представлений E_α):

$$\sum_{i=1}^K n_i h_\alpha(C_i) \cdot h_\beta(C_i) = n \delta_{\alpha\beta}, \quad \sum_{\alpha=1}^L n_i h_\alpha(C_i) \cdot h_\alpha(C_j) = n \delta_{ij},$$

где n_i — число элементов в классе C_i , n — порядок группы G ,

K — число классов C_i , L — число представлений E_α .

Приведем примеры, подтверждающие ортонормированность характеров:

$$\sum_{i=1}^3 n_i \cdot h_3(C_i) \cdot h_3(C_i) = 1 \cdot 2 \cdot 2 + 2 \cdot (-1) \cdot (-1) + 3 \cdot 0 \cdot 0 = 6,$$

$$\sum_{\alpha=1}^3 n_1 \cdot h_\alpha(C_1) \cdot h_\alpha(C_2) = 2 \cdot 1 \cdot 1 + 2 \cdot 1 \cdot (-1) + 2 \cdot (-1) \cdot 0 = 0.$$

У нас получилось, что $K = L$. На самом деле число неприводимых представлений E_α всегда равно числу классов сопряженности C_i . Критерием неприводимости представления E_α служит формула

$$\sum_{g \in G} h_\alpha^2(g) = n. \quad (2.34)$$

Так, представление E_2 является неприводимым, т.к.

$$\sum_{g \in G} h_2^2(g) = 2^2 + (-1)^2 + (-1)^2 + 0^2 + 0^2 + 0^2 = 6,$$

а представление E_4 будет уже приводимым —

$$\sum_{g \in G} h_4^2(g) = 3^2 + 0^2 + 0^2 + 1^2 + 1^2 + 1^2 = 12.$$

Еще одним важным критерием является критерий полноты набора неприводимых представлений, который гласит: сумма квадратов размерностей матриц всех неприводимых представлений должна быть равна порядку группы —

$$\sum_{\alpha} n_{\alpha}^2 = n, \quad D_3: 6 = 1^2 + 1^2 + 2^2. \quad (2.35)$$

Разложение (2.35), вообще говоря, неоднозначно. Например, числа 27 и 92 можно разложить на сумму квадратов многими способами:

$$27 = 1^2 + 1^2 + 5^2 = 1^2 + 1^2 + 3^2 + 4^2 = 3^2 + 3^2 + 3^2 = 1^2 + 1^2 + \dots + 1^2 = \dots;$$

$$92 = 1^2 + 1^2 + 3^2 + 9^2 = 3^2 + 3^2 + 3^2 + 4^2 + 7^2 = 1^2 + 1^2 + \dots + 1^2 + 2^2 = \dots.$$

Критерий неприводимости представлений свидетельствует о существовании определенной связи между классами эквивалентности C_i и неприводимыми представлениями E_α . По-видимому, каждому классу можно поставить в соответствие определенное представление. Для группы D_3 это соответствие могло бы выглядеть следующим образом: $E_0 \leftrightarrow C_0$, $E_1 \leftrightarrow C_2$, $E_2 \leftrightarrow C_1$.

Однако не все так просто, как может показаться на первый взгляд. Каждое неприводимое представление E_α определяется своим векторным базисом (иначе го-

вора, своим субстанционным множеством), а каждый класс эквивалентности C_i определяется специфической *периодичностью подстановок*, входящих в класс (т.е. своим *операционным* множеством). Прямой связи между субстанционным и операционным множествами не существует. Тем не менее, используя так называемые *диаграммы Юнга* (их иногда называют *диаграммами Ферре*), можно однозначно установить *размерность базиса линейного преобразования E_a* на основе *периодичности подстановок C_i* . На примере нашей группы диэдра D_3 покажем, как это делается.

Заметим, что изложенная ниже методика применима только для *симметрических групп S_n* , порядок которых определяется формулой $n!$ и которые состоят из всевозможных перестановок из n индексов (рассматриваемая нами группа как раз такова: $D_3 \equiv S_3$). Далее, подобную методику можно использовать для *полной группы симметрии тетраэдра T_d* , которая состоит не только из поворотов этой геометрической фигуры (T), но и отражений ее в плоскостях симметрии ($T_d \equiv S_4$), а также *группы вращений икосаэдра ($I \equiv S_5$)*. Однако для несимметрических групп, например D_4 , поиск всех неприводимых представлений E_o является уже нестандартной задачей, требующей иногда значительных творческих усилий.

Введем понятие *диаграммы Юнга*. Для группы первого порядка $C_1 = S_1$ диаграмма Юнга представляется единственной пустой клеткой, которая обозначается символом [1]. Для $C_2 \equiv S_2$ имеем две диаграммы Юнга: *симметричную* [2] и *антисимметричную* [11], которые соответствуют двум способам разбиения числа 2. Для S_3 к полностью симметричной [3] и антисимметричной [111] добавляется диаграмма со смешанной симметрией [21]. Все перечисленные диаграммы Юнга изображены на рис. 2.7.

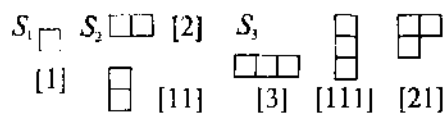


Рис. 2.7

Размерность представления, т.е. то, что нас сейчас больше всего интересует, зависит от числа возможных способов образования конкретной диаграммы Юнга. На рис. 2.8 показано, как получить двумерное представление, отвечающее диаграмме [21] для S_3 , из двух диаграмм ([11] и [2]) для S_2 . С этой целью производят различную нумерацию клеток, при которой индексы могут только возрастать слева направо в каждой строке и сверху вниз в каждом столбце. Так, учитывая способы образования диаграмм Юнга для S_4 из диаграмм для S_3 , определяем, что для S_4 будет существовать два *одномерных* ([4]),

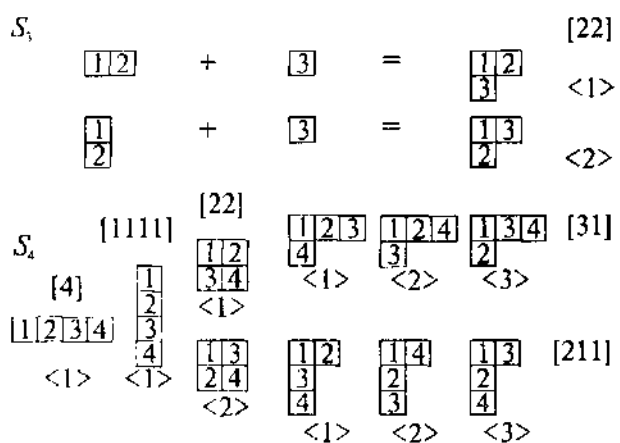


Рис. 2.8

[1111]), два *трехмерных* ([31], [211]) и одно *двухмерное* представления ([22]). Различные способы заполнения диаграмм обозначены в угловых скобках.

Изложенный способ нахождения размерности, характеров и самих матриц неприводимых представлений симметрических групп подробно описан в книге М. Хамермеша «Теория групп». Однако в другом месте, в частности, в книге М. Айгнера «Комбинаторная теория» представлена совершенно иная методика определения размерности. Там вводится понятие *угловой длины* для каждой клетки диаграммы Юнга. Угловая длина (l_i) равна числу клеток, расположенных справа и ниже i -ой клетки, плюс единица (т.е. учитывается сама i -ая клетка, для которой ищется угловая длина). Размерность диаграммы ($D[\Lambda]$) определяется как частное от деления порядка симметрической группы ($n!$) на произведение угловых длин от всех клеток данной диаграммы:

$$D[\Lambda] = \frac{n!}{\prod_i l_i}.$$

Рассчитаем размерность представлений симметрической группы S_5 :

$$D[11111] = D[5] = 5!/1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 1, \quad D[41] = D[2111] = 5!/1 \cdot 1 \cdot 2 \cdot 3 \cdot 5 = 4,$$

$$D[32] = D[221] = 5!/1 \cdot 1 \cdot 2 \cdot 3 \cdot 4 = 5, \quad D[311] = 5!/1 \cdot 1 \cdot 2 \cdot 2 \cdot 5 = 6.$$

С помощью диаграмм Юнга можно непосредственно вычислить характеры и сами ортонормированные неприводимые матричные представления без предварительного нахождения их базиса. Подробное изложение этой методики можно найти у М. Хамермеша в указанной нами книге, где помимо прочего описан способ нахождения так называемых *символов Яманучи*, придающих представлениям однозначность. Мы же предпримем сейчас сокращенное изложение, позволяющее, тем не менее, найти все матрицы двухмерного представления E_2 , отвечающего диаграмме [21] группы $D_3 \cong S_3$.

Диагональные матричные элементы для диаграммы $\langle i \rangle$ и смежной транспозиции $(k-1, k)$ определяются по формуле:

$$\langle i | k-1, k | i \rangle = [P_{(k-1, k)}^{\langle i \rangle}]^{-1}, \quad (2.36)$$

где $P_{(k-1, k)}^{\langle i \rangle} = [C(k) - C(k-1)] - [R(k) - R(k-1)]$.

Здесь $P_{(k-1, k)}^{\langle i \rangle}$ — аксиальное расстояние между числами $k-1$ и k в диаграмме $\langle i \rangle$; $C(k)$ и $C(k-1)$ — номер столбца k или $k-1$ элемента в диаграмме $\langle i \rangle$; $R(k)$ и $R(k-1)$ — номер строки k или $k-1$ элемента в диаграмме $\langle i \rangle$. Если числа k и $k-1$ находятся в одной строке, то аксиальное расстояние равно 1, а если k и $k-1$ находятся в одном столбце, то аксиальное расстояние равно (-1) . Недиagonальные матричные элементы между диаграммой $\langle i \rangle$ и диаграммой $\langle j \rangle$ транспозиции $(k-1, k)$ не равны нулю, если $\langle i \rangle$ получается из $\langle j \rangle$ путем перемены мест индексов k и $k-1$, в противном случае недиагональный элемент равен нулю. Ненулевой матричный элемент определяется по формуле:

$$\langle i | k-1, k | j \rangle = \{1 - [P_{(k-1, k)}^{\langle i \rangle}]^{-2}\}^{1/2}. \quad (2.37)$$

Если помнить, что любую транспозицию можно представить произведением смежных транспозиций (2.25), а всякую подстановку можно разложить на про-

извлечение транспозиций (2.26), то приведенных формул будет достаточно для вычисления матричных представлений. При пользовании формулами (2.36) и (2.37) счет индексов у транспозиций $(k-1, k)$ будет начинаться не с $k=0$, а с $k=1$, так что наша транспозиция $(012) \equiv (123)$. Методику вычисления матричных элементов продемонстрируем на примере двухмерного неприводимого представления E_2 группы D_3 , отвечающего диаграмме [21] с двумя способами расстановки индексов $<1>$ и $<2>$ (рис. 2.8).

Для смежной транспозиции (23) диаграммы $<1>$ имеем диагональный элемент, равный

$$\langle 1|2\ 3|1\rangle = [P_{(23)}^{<1>}]^{-1} = [1-2-(2-1)]^{-1} = -1/2.$$

Для этой же транспозиции, но диаграммы $<2>$ имеем другой диагональный элемент —

$$\langle 2|2\ 3|2\rangle = [P_{(23)}^{<2>}]^{-1} = [2-1-(1-2)]^{-1} = 1/2.$$

Недиагональные элементы равны между собой:

$$\langle 1|2\ 3|2\rangle = \langle 2|2\ 3|1\rangle = \{1 - [P_{(23)}^{<1>}]^{-2}\}^{1/2} = \sqrt{3}/2.$$

Следовательно, матрица неприводимого представления E_2 для транспозиции (23) — она же выступает в роли одной из подстановок группы D_3 — выглядит следующим образом:

$$(23) = \begin{pmatrix} 1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}.$$

Для транспозиции (12) имеем:

$$\langle 1|1\ 2|1\rangle = 1, \quad \langle 2|1\ 2|2\rangle = -1, \quad \langle 1|1\ 2|2\rangle = \langle 2|1\ 2|1\rangle = 0.$$

Соответствующая матрица равна:

$$(12) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Так как

$$(13) = (32)(12)(23), \quad (123) = (12)(13), \quad (132) = (13)(12),$$

после перемножения вычисленных матриц находим окончательно:

$$(13) = \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & 1/2 \end{pmatrix}, \quad (123) = \begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}, \quad (132) = \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}.$$

Перейдем к рассмотрению некоммукативной группы — D_4^1 . Она отвечает пространственному вращению квадрата (рис. 2.46). Вращения описываются следующей системой преобразования координат:

$$\begin{array}{llll} e = (0), & x' = x, & y' = y, & z' = z, \\ a = (0123), & x' = y, & y' = -x, & z' = z, \\ a^2 = (02)(13), & x' = -x, & y' = -y, & z' = z, \\ a^3 = (0321), & x' = -y, & y' = x, & z' = z, \\ b = (01)(23), & x' = -x, & y' = y, & z' = -z, \end{array}$$

$$\begin{array}{llll} ab = (13), & x' = y, & y' = x, & z' = -z, \\ a^2b = (03)(12), & x' = x, & y' = -y, & z' = -z, \\ a^3b = (02), & x' = -y, & y' = -x, & z' = -x. \end{array}$$

Все элементы D_4^1 распадаются на пять классов эквивалентности:

$$C_0 = \{e\}, \quad C_1 = \{a^2\}, \quad C_2 = \{a, a^3\}, \quad C_3 = \{b, a^2b\}, \quad C_4 = \{ab, a^3b\}.$$

Число неприводимых представлений равно числу классов. Пользуясь критерием полноты набора неприводимых представлений (2.35), определим размерности пяти представлений:

$$\sum_{\alpha} n_{\alpha}^2 = 1^2 + 1^2 + 1^2 + 1^2 + 2^2 = 8.$$

Неприводимые представления $\{E_0, E_1, E_2, E_3, E_4\}$ приведены в табл. 2.48. Двухмерное представление E_4 получается из преобразований координат для осей x и y ; одномерное E_1 отвечает преобразованиям оси z ; минус единица представления E_3 ставится для нечетных подстановок; строка для E_2 записывается из соображений об ортогональности (2.30), когда известны три других одномерных представления. Помимо указанных пяти неприводимых представлений, в табл. 2.48 дано еще одно, эквивалентное E_4 , ортогональное, двухмерное представление E_5 , полученное на базисе векторов, проведенных из центра координат к вершинам 0 и 3. Координаты вершин квадрата (рис. 2.26) определяют базис для E_4 :

$$0 = (1, 1), \quad 1 = (1, -1), \quad 2 = (-1, -1), \quad 3 = (-1, 1).$$

Таблица 2.48

D_4^1	e	a	a^2	a^3	b	ab	a^2b	a^3b
E_0	1	1	1	1	1	1	1	1
E_1	1	1	1	1	-1	-1	-1	-1
E_2	1	-1	1	1	1	-1	1	-1
E_3	1	-1	1	-1	-1	1	-1	1
E_4	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$
E_5	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

В таблицу характеров (табл. 2.49), помимо неприводимых представлений, входят четыре приводимых: E_6 — полученное на базисе x, y, z ; E_7 — полученное на базисе 0, 1, 2, 3; $E_8 = E_4 \times E_4$; E_9 — регулярное представление. Используя формулу (2.33), можно провести следующие разложения:

$$\begin{aligned} E_6 &= E_1 + E_4, & E_8 &= E_0 + E_1 + E_2 + E_3, \\ E_7 &= E_0 + E_3 + E_4, & E_9 &= E_0 + E_1 + E_2 + E_3 + 2 \cdot E_4. \end{aligned}$$

Таблица 2.49

$D_4^{1,2}$	C_0	C_1	C_2	C_3	C_4
E_0	1	1	1	1	1
E_1	1	1	1	-1	-1
E_2	1	1	-1	1	-1
E_3	1	1	-1	-1	1
E_4	2	2	0	0	0
E_5	2	-2	0	0	0
E_6	3	-1	1	-1	-1
E_7	4	0	0	0	2
E_8	4	4	0	0	0
E_9	8	0	0	0	0

Из групп восьмого порядка осталась не рассмотренной группа кватерниона D_4^2 . Если в качестве базиса взять векторы:

$$\begin{aligned} 0 &= (1, i), & 2 &= (i, 1), & 4 &= (1, -i), & 6 &= (-i, 1), \\ 1 &= (-1, -i), & 3 &= (-i, -1), & 5 &= (-1, i), & 7 &= (i, -1), \end{aligned}$$

то они породят операционное множество, образующее двухмерное неприводимое представление:

$$\begin{aligned} e &= (0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & -e &= (01)(23)(45)(67) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \\ i &= (0213)(4756) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, & -i &= (0312)(4657) = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \\ j &= (0415)(2637) = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, & -j &= (0514)(2736) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \\ k &= (0617)(2534) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, & -k &= (0716)(2435) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \end{aligned}$$

Группа кватерниона D_4^2 , как и группа диэдра D_4^1 , состоит из пяти классов —

$$C_0 = \{e\}, \quad C_1 = \{-e\}, \quad C_2 = \{i, -i\}, \quad C_3 = \{j, -j\}, \quad C_4 = \{k, -k\},$$

следовательно, одномерные представления — E_0, E_1, E_2, E_3 — у нее совпадают с предыдущим случаем (табл. 2.48).

В разделе, который называется «Геометрическая интерпретация групповых преобразований», нельзя не сказать о важнейшей интерпретации произведения двух кватернионов. Подобно тому, как произведению двух комплексных чисел

$$\begin{aligned} z &= \cos \varphi + i \sin \varphi = a + i b = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \\ z' &= \cos \varphi' + i \sin \varphi' = c + i d = \begin{pmatrix} c & -d \\ d & c \end{pmatrix}, \end{aligned}$$

отвечают два последовательных поворота в плоскостях, ix и iy :

$$\begin{aligned} Z = z z' &= (\cos \varphi + i \sin \varphi)(\cos \varphi' + i \sin \varphi') = \\ &= (a + i b)(c + i d) = (ac - bd) + i(ad + cb) = \\ &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac - bd & -(ad + cb) \\ ad + cb & ac - bd \end{pmatrix} = (ac - bd) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + (ad + cb) \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \end{aligned}$$

произведению кватернионов соответствуют последовательные вращения в пространстве трех измерений.

Кватернион, как мы уже знаем, получается за счет удвоения комплексного числа или на базисных матрицах, которые могут иметь следующий вид:

$$\begin{aligned} q = z + j z' &= (a + i b) + j(c + i d) = a + i b + j c + k d = \\ &= a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} + c \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + d \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} a + ic & -(b - id) \\ b + id & a - ic \end{pmatrix}. \end{aligned}$$

Составим произведение двух кватернионов:

$$\begin{aligned} Q = q q' &= (a + i b + j c + k d)(a' + i b' + j c' + k d') = \\ &= (aa' - bb' - cc' - dd') + a(i b' + j c' + k d') + a'(i b + j c + k d) + \begin{pmatrix} i & j & k \\ b & c & d \\ b' & c' & d' \end{pmatrix}. \end{aligned}$$

Здесь скалярная часть произведения есть произведение скалярных частей множителей минус скалярное произведение их векторных частей. Векторная часть произведения состоит из суммы произведений скалярной части каждого множителя на векторную часть другого плюс произведение векторной части первого множителя на векторную часть второго. Таким образом, все существующие виды умножения в векторной алгебре являются осколками одной операции перемножения двух кватернионов.

Перемножение двух сопряженных кватернионов дает скаляр:

$$(a + i b + j c + k d)(a - i b - j c - k d) = a^2 + b^2 + c^2 + d^2.$$

Кватернион с нормированными коэффициентами:

$$a^2 + b^2 + c^2 + d^2 = 1$$

можно представить через тригонометрические функции:

$$q = \cos \varphi/2 + \sin \varphi/2 (i \cos \alpha + j \cos \beta + k \cos \gamma),$$

где α, β и γ — углы между некоторым вектором p и осями координат, φ — угол вращения вокруг p .

Пространственное вращение, описываемое кватернионом q , за которым следует вращение q' , даст результирующее изменение ориентации, описываемое третьим кватернионом Q . Предположим, кватернион q отвечает повороту вокруг оси x на угол $\varphi = \pi/2$, а q' — точно на такой же угол, но вокруг оси y , что соответствует формулам:

$$q = \cos \pi/4 + i \sin \pi/4 = \frac{1}{\sqrt{2}}(1 + i), \quad q' = \frac{1}{\sqrt{2}}(1 + j).$$

Тогда результирующее вращение будет равно:

$$Q = \cos \pi/3 + \sin \pi/3 \cdot \frac{1}{\sqrt{3}}(i + j - k) = \frac{1}{2}(1 + i + j - k).$$

Таким образом, результирующее вращение происходит на угол $2\pi/3$ вокруг вектора p с направляющими косинусами, равными $1/\sqrt{3}$.

Известны другие формулы задания вращения в трехмерном пространстве. Так, матрица A в линейном преобразовании (2.1) может выглядеть либо так:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \cos\varphi \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + (1 - \cos\varphi) \begin{pmatrix} \cos^2\alpha & \cos\alpha\cos\beta & \cos\alpha\cos\gamma \\ \cos\beta\cos\alpha & \cos^2\beta & \cos\beta\cos\gamma \\ \cos\gamma\cos\alpha & \cos\gamma\cos\beta & \cos^2\gamma \end{pmatrix} + \sin\varphi \begin{pmatrix} 0 & -\cos\gamma & \cos\beta \\ \cos\gamma & 0 & -\cos\alpha \\ -\cos\beta & \cos\alpha & 0 \end{pmatrix},$$

и тогда взаимосвязь между параметрами вращения и матричными элементами будет такой:

$$\begin{aligned} \cos\varphi &= (1/2)(a_{11} + a_{22} + a_{33} - 1), \quad \cos\alpha = (1/2\sin\varphi)(a_{32} - a_{23}), \\ \cos\beta &= (1/2\sin\varphi)(a_{13} - a_{31}), \quad \cos\gamma = (1/2\sin\varphi)(a_{21} - a_{12}); \\ a_{11} - \cos\varphi &= (1 - \cos\varphi)\cos^2\alpha \text{ и т.д.}, \end{aligned}$$

либо через углы Эйлера ϕ_1, ϕ_2 и ϕ_3 :

$$A = \begin{pmatrix} \cos\phi_1 & -\sin\phi_1 & 0 \\ \sin\phi_1 & \cos\phi_1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \cos\phi_2 & 0 & \sin\phi_2 \\ 0 & 1 & 0 \\ \sin\phi_2 & 0 & \cos\phi_2 \end{pmatrix} \begin{pmatrix} \cos\phi_3 & \sin\phi_3 & 0 \\ \sin\phi_3 & \cos\phi_3 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

и тогда

$$\cos\frac{\varphi}{2} = \cos\frac{\phi_1 + \phi_3}{2} \cos\frac{\phi_2}{2}, \quad a_{11} = \cos\phi_1 \cos\phi_2 \cos\phi_3 - \sin\phi_1 \sin\phi_3 \text{ и т.д.}$$

Если производить перемножение двух матриц A и B , то результирующая матрица C будет иметь вид исходных матриц сомножителей, т.е. закон замкнутости здесь тоже действует. В силу ассоциативности и существования обратных матриц можно говорить о бесконечных группах поворотов векторов в трехмерном пространстве.

Введем удвоение кватерниона, в результате чего получим *октаву*:

$$\begin{aligned} o = q_1 + E q_2 &= (a + ib + jc + kd) + E(A + iB + jC + kD) = \\ &= a + ib + jc + kd + EA + IB + JC + KD. \end{aligned}$$

Закон умножения базисных единиц октавы будет задаваться табл. 2.50 (из соображений экономии места таблица 16×16 приведена частично: она задает умножения только для положительных базисных единиц). Для октав перестает выполняться закон ассоциативности:

$$(ij)E \neq i(jE), \text{ так как } (ij)E = K, \text{ а } i(jE) = -K,$$

поэтому базисные единицы октавы уже не образуют группы.

В квантовой физике часто приходится иметь дело с так называемыми *матрицами Паули*:

$$s_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad s_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad s_2 = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad s_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

1	i	j	k	E	I	J	K
i	-1	k	$-j$	I	$-E$	$-K$	J
j	$-k$	-1	i	J	K	$-E$	$-I$
k	j	$-i$	-1	K	$-J$	I	$-E$
E	$-I$	$-J$	$-K$	-1	i	j	k
I	E	$-K$	J	$-i$	-1	$-k$	j
J	K	E	$-I$	$-j$	k	-1	$-i$
K	$-J$	I	E	$-k$	$-j$	i	-1

Существует простая связь между ними и матрицами базисных единиц кватерниона, которые мы приводили только что:

$$i = is_2 = s_1s_3, \quad j = is_3 = s_2s_1, \quad k = is_1 = s_3s_2.$$

Закон ассоциативности для матриц Паули выполняется:

$$s_1(s_2s_3) = (s_1s_2)s_3 = -i.$$

Однако группы эти базисные единицы тоже не образуют по причине нарушения закона о замкнутости. Тем не менее, на них можно построить любопытный математический объект — *алгебру Клиффорда*.

Алгебра Клиффорда на матрицах Паули представляет собой числовой агрегат следующего вида:

$$A = a_0s_0 + a_1s_1 + a_2s_2 + a_3s_3 + a_{12}s_1s_2 + a_{23}s_2s_3 + a_{31}s_3s_1 + a_{123}s_1s_2s_3.$$

В состав агрегата A входит *скаляр*, *3-вектор*, *3-бивектор* и *тривектор* (или *псевдоскаляр*). При перемножении таких агрегатов, в силу условий $s_is_j + s_js_i = 0$ и $s_i^2 = 1$, будут возникать два типа умножения базисных единиц — *внутреннее* и *внешнее*. Внутреннее произведение (его еще называют *скалярным*) возникает тогда, когда s_i входит в базисную единицу n -вектора $s_1s_2 \dots s_n$, например:

$$s_2 \cdot s_1s_2s_3 = s_2s_1s_2s_3 = -s_1s_2s_3s_2 = -s_1s_3,$$

в результате чего, если говорить об общем случае, n -вектор переходит в $(n-1)$ -вектор; а внешнее (или *векторное*), когда s_i не входит в $s_1s_2 \dots s_n$, например: $s_2 \times s_1s_3 = s_2s_1s_3 = -s_1s_2s_3$, и тогда n -вектор переходит в $(n+1)$ -вектор. (При нашем формализме эти произведения различать специальными символами « $\cdot$ » и « $\times$ » не нужно.) Так, при перемножении двух векторов —

$$s = u s_1 + v s_2 + w s_3 = \begin{pmatrix} w & u+iv \\ u-iv & -w \end{pmatrix}, \quad s' = u' s_1 + v' s_2 + w' s_3 = \begin{pmatrix} w' & u'+iv' \\ u'-iv' & -w' \end{pmatrix},$$

возникают скаляр и бивектор —

$$S = ss' = (uu' + vv' + ww') + \begin{pmatrix} s_2s_3 & s_3s_1 & s_1s_2 \\ u & v & w \\ u' & v' & w' \end{pmatrix}.$$

Перейдем от геометрической интерпретации умножения z , q и s к представлениям некоммутативной группы десятого порядка D_5^1 . Она имеет четыре класса —

$$C_0 = \{e\}, \quad C_1 = \{a, a^4\}, \quad C_2 = \{a^2, a^3\}, \quad C_3 = \{b, ab, a^2b, a^3b\}.$$

поэтому имеется два одномерных и два двумерных представления. Характеры этих представлений помещены в табл. 2.51. Если принять, что

$$p = \cos(2\pi/5) = \frac{-1 + \sqrt{5}}{4}, \quad q = \cos(4\pi/5) = \frac{-1 - \sqrt{5}}{4}, \quad r = \sin(2\pi/5), \quad s = \sin(4\pi/5),$$

то базисными векторами для неприводимого представления E_2 могут служить вершины правильного пятиугольника (рис. 2.5):

$$0 = (1, 0), \quad 1 = (p, r), \quad 2 = (q, s), \quad 3 = (q, -s), \quad 4 = (p, -r).$$

Таблица 2.51

D_5^1	C_0	C_1	C_2	C_3
E_0	1	1	1	1
E_1	1	1	1	-1
E_2	2	$2 \cdot p$	$2 \cdot q$	0
E_3	2	$2 \cdot q$	$2 \cdot p$	0

Эти векторы вращаются под действием матриц представления E_2 в соответствии с подстановками:

$$\begin{aligned} e = (0) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad a = (01234) = \begin{pmatrix} p & -r \\ r & p \end{pmatrix}, \quad a^2 = (02413) = \begin{pmatrix} q & -s \\ s & q \end{pmatrix}, \quad a^3 = (3142) = \begin{pmatrix} q & s \\ -s & q \end{pmatrix}, \\ a^4 &= (04321) = \begin{pmatrix} p & r \\ -r & p \end{pmatrix}, \quad b = (14)(23) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad ab = (04)(13) = \begin{pmatrix} p & -r \\ -r & -p \end{pmatrix}, \\ a^2b &= (03)(12) = \begin{pmatrix} q & -s \\ -s & q \end{pmatrix}, \quad a^3b = (02)(34) = \begin{pmatrix} q & s \\ s & -q \end{pmatrix}, \quad a^4b = (01)(24) = \begin{pmatrix} p & r \\ r & -p \end{pmatrix}. \end{aligned}$$

Проведем через середины сторон правильного пятиугольника перпендикуляры с координатами, получим новую систему векторов:

$$0 = (-q, s), \quad 1 = (-1, 0), \quad 2 = (-q, -s), \quad 3 = (-p, r), \quad 4 = (-p, -r).$$

Они могут служить базой для ортогонального представления E_3 :

$$\begin{aligned} e &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad a = \begin{pmatrix} q & -s \\ s & q \end{pmatrix}, \quad a^2 = \begin{pmatrix} p & r \\ -r & p \end{pmatrix}, \quad a^3 = \begin{pmatrix} p & -r \\ r & p \end{pmatrix}, \quad a^4 = \begin{pmatrix} q & s \\ -s & q \end{pmatrix}, \\ b &= \begin{pmatrix} p & r \\ r & -p \end{pmatrix}, \quad ab = \begin{pmatrix} p & -r \\ -r & -p \end{pmatrix}, \quad a^2b = \begin{pmatrix} q & s \\ s & q \end{pmatrix}, \quad a^3b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad a^4b = \begin{pmatrix} q & -s \\ -s & -q \end{pmatrix}. \end{aligned}$$

Из пяти групп двенадцатого порядка три некоммутативных. Начнем с анализа группы диэдра D_6^1 . Она содержит шесть классов эквивалентности, следовательно, для нее существует четыре одномерных и два двумерных представления (табл. 2.52), причем одно из них (E_4) гомоморфное, другое (E_5) изоморфное.

$$\begin{aligned} C_0 &= \{e\}, \quad C_1 = \{a^3\}, \quad C_2 = \{a, a^5\}, \quad C_3 = \{a^2, a^4\}, \\ C_4 &= \{b, a^2b, a^4b\}, \quad C_5 = \{ab, a^3b, a^5b\}. \end{aligned}$$

Таблица 2.52

$D_6^{1,2}$	C_0	C_1	C_2	C_3	C_4	C_5
E_0	1	1	1	1	1	1
E_1	1	1	1	1	-1	-1
E_2	1	-1	-1	1	1	-1
E_3	1	-1	-1	1	-1	1
E_4	2	2	-1	-1	0	0
E_5	2	2	1	1	0	0

Базисом для изоморфного представления E_3 служат векторы, проведенные из начала координат к вершинам правильного шестиугольника (рис. 2.6):

$$\begin{aligned}
 0 &= (1, 0), & 1 &= (1/2, \sqrt{3}/2), & 2 &= (-1/2, \sqrt{3}/2), \\
 3 &= (-1, 0), & 4 &= (-1/2, -\sqrt{3}/2), & 5 &= (1/2, -\sqrt{3}/2); \\
 e=(0) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & a=(012345) &= \begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}, \\
 a^2 &= (024)(135) = \begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}, & a^3 &= (03)(14)(25) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \\
 a^4 &= (042)(153) = \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & 1/2 \end{pmatrix}, & a^5 &= (054321) = \begin{pmatrix} 1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & 1/2 \end{pmatrix}, \\
 b &= (15)(24) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, & ab &= (05)(14)(23) = \begin{pmatrix} 1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}, \\
 a^2b &= (04)(13) = \begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}, & a^3b &= (03)(12)(45) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \\
 a^4b &= (02)(35) = \begin{pmatrix} 1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}, & a^5b &= (01)(25)(34) = \begin{pmatrix} 1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}.
 \end{aligned}$$

Базисом для гомоморфного представления E_4 служат перпендикуляры, проведенные из начала координат к серединам сторон шестиугольника. Имеется только три таких прямых, каждую из которых мы обозначим двумя индексами:

$$\{0, 3\} = (\sqrt{3}/2, 1/2), \quad \{2, 5\} = (-\sqrt{3}/2, 1/2), \quad \{1, 4\} = (0, -1).$$

Операционное множество тоже сократится вдвое:

$$\begin{aligned}
 \{e, a^3\} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \{a, a^4\} = \begin{pmatrix} 1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}, \quad \{a^2, a^5\} = \begin{pmatrix} 1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix}, \\
 \{b, a^3b\} &= \begin{pmatrix} 1/2 & \sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}, \quad \{ab, a^4b\} = \begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ -\sqrt{3}/2 & 1/2 \end{pmatrix}, \quad \{a^2b, a^5b\} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.
 \end{aligned}$$

Группа D_6^2 отличается от D_6^1 тем, что вместо шести элементов с периодом 2 появляются шесть элементов с периодом 4. Отличная от D_6^1 часть операционного

множества D_6^2 изоморфного представления E_5 выглядит следующим образом:

$$b = (0639)(174A)(285B) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad ab = (073A)(184B)(2956) = \begin{pmatrix} i/2 & -i\sqrt{3}/2 \\ -i\sqrt{3}/2 & i/2 \end{pmatrix},$$

$$a^2b = (083B)(1946)(2A57) = \begin{pmatrix} -i/2 & i\sqrt{3}/2 \\ i\sqrt{3}/2 & i/2 \end{pmatrix}, \quad a^3b = (0936)(1A47)(2B58) = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix},$$

$$a^4b = (0A37)(1B48)(2659) = \begin{pmatrix} i/2 & -i\sqrt{3}/2 \\ -i\sqrt{3}/2 & i/2 \end{pmatrix}, \quad a^5b = (0B38)(1649)(275A) = \begin{pmatrix} i/2 & i\sqrt{3}/2 \\ i\sqrt{3}/2 & -i/2 \end{pmatrix}.$$

Гомоморфное представление E_4 :

$$\{b, a^3b\} = \begin{pmatrix} i/2 & i\sqrt{3}/2 \\ i\sqrt{3}/2 & i/2 \end{pmatrix}, \quad \{a^2b, a^5b\} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \quad \{ab, a^4b\} = \begin{pmatrix} i/2 & -i\sqrt{3}/2 \\ -i\sqrt{3}/2 & i/2 \end{pmatrix}.$$

Дополнительными базисными векторами для представлений E_4 и E_5 группы D_6^2 являются первые столбцы приведенных матриц.

Группа *тетраэдра* T отличается от двух рассмотренных групп двенадцатого порядка. Характеры четырех представлений выписаны в табл. 2.53. Рассмотрим трехмерное представление E_3 , базисом которого являются четыре вектора:

$$0 = (-1/3, -\sqrt{2}/3, -\sqrt{6}/3), \quad 1 = (-1/3, -\sqrt{2}/3, \sqrt{6}/3),$$

$$2 = (-1/3, -2\sqrt{2}/3, 0), \quad 3 = (1, 0, 0).$$

Таблица 2.53

$D_6^{1,2}$	C_0	C_1	C_2	C_3
E_0	1	1	1	1
E_1	1	1	ω	ω^2
E_2	1	1	ω^2	ω
E_3	3	-1	0	0

Классы сопряженности группы тетраэдра T :

$$C_0 = \{e\}, \quad C_1 = \{ab, ba, ab^2a\}, \quad C_2 = \{a, b^2, a^2b, ba^2\}, \quad C_3 = \{a^2, b, ab^2, b^2a\}.$$

В представлениях E_1 и E_2 участвуют кубические корни из единицы – $\{1, \omega, \omega^2\}$, представление E_3 состоит из двенадцати матриц:

$$e = (0) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad a = (012) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/2 & \sqrt{3}/2 \\ 0 & \sqrt{3}/2 & 1/2 \end{pmatrix},$$

$$a^2 = (021) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/2 & \sqrt{3}/2 \\ 0 & \sqrt{3}/2 & -1/2 \end{pmatrix}, \quad b = (123) = \begin{pmatrix} -1/3 & \sqrt{8}/3 & 0 \\ \sqrt{8}/3 & -1/6 & \sqrt{3}/2 \\ \sqrt{6}/3 & \sqrt{3}/6 & 1/2 \end{pmatrix},$$

$$\begin{aligned}
b^2 = (132) &= \begin{pmatrix} \frac{1}{3} & -\frac{\sqrt{3}}{3} & \frac{\sqrt{6}}{3} \\ \frac{\sqrt{8}}{3} & \frac{1}{6} & \frac{\sqrt{3}}{6} \\ 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}, & ab = (02)(13) &= \begin{pmatrix} \frac{1}{3} & -\frac{\sqrt{2}}{3} & \frac{\sqrt{6}}{3} \\ -\frac{\sqrt{2}}{3} & \frac{2}{3} & -\frac{\sqrt{3}}{3} \\ \frac{\sqrt{6}}{3} & -\frac{\sqrt{3}}{3} & 0 \end{pmatrix}, \\
ba = (01)(23) &= \begin{pmatrix} -\frac{1}{3} & \frac{\sqrt{8}}{3} & 0 \\ \frac{\sqrt{8}}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 1 \end{pmatrix}, & ab^2a = (03)(12) &= \begin{pmatrix} -\frac{1}{3} & -\frac{\sqrt{2}}{3} & -\frac{\sqrt{6}}{3} \\ -\frac{\sqrt{5}}{3} & \frac{2}{3} & \frac{\sqrt{3}}{3} \\ -\frac{\sqrt{6}}{3} & \frac{\sqrt{3}}{3} & 0 \end{pmatrix}, \\
a^2b = (031) &= \begin{pmatrix} -\frac{1}{3} & \frac{\sqrt{3}}{3} & \frac{\sqrt{6}}{3} \\ -\frac{\sqrt{2}}{3} & \frac{5}{6} & -\frac{\sqrt{3}}{6} \\ \frac{\sqrt{6}}{3} & \frac{\sqrt{3}}{6} & \frac{1}{2} \end{pmatrix}, & ba^2 = (023) &= \begin{pmatrix} -\frac{1}{3} & \frac{\sqrt{8}}{3} & 0 \\ -\frac{\sqrt{8}}{3} & \frac{1}{6} & -\frac{\sqrt{3}}{2} \\ -\frac{\sqrt{6}}{3} & -\frac{\sqrt{3}}{6} & \frac{1}{2} \end{pmatrix}, \\
ab^2 = (032) &= \begin{pmatrix} \frac{1}{3} & -\frac{\sqrt{3}}{3} & -\frac{\sqrt{6}}{3} \\ \frac{\sqrt{8}}{3} & -\frac{1}{6} & \frac{\sqrt{3}}{6} \\ 0 & -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}, & b^2a = (013) &= \begin{pmatrix} \frac{1}{3} & \frac{\sqrt{3}}{3} & \frac{\sqrt{6}}{3} \\ \frac{\sqrt{3}}{3} & \frac{5}{6} & \frac{\sqrt{3}}{6} \\ -\frac{\sqrt{6}}{3} & -\frac{\sqrt{3}}{6} & -\frac{1}{2} \end{pmatrix}.
\end{aligned}$$

Представление E_0 — единичное; E_1 и E_2 — гомоморфные, возникшие благодаря наличию в группе тетраэдра T нормального делителя $N = \{e, ab, ba, ab^2a\}$. Соответствие между классами и представлениями здесь такое: $E_0 \leftrightarrow C_0$, $E_1 \leftrightarrow C_2$, $E_2 \leftrightarrow C_3$, $E_3 \leftrightarrow C_1$. Таким образом, на первый взгляд возникла необычная ситуация: класс коммутативных элементов C_1 породил изоморфное некоммутирующее представление E_3 , а два смежных класса некоммутирующих элементов C_2 и C_3 отвечают двум коммутативным представлениям E_1 и E_2 . Странным кажется и то, что восемь внешне одинаковых 3-цикла распались на два различных класса эквивалентности.

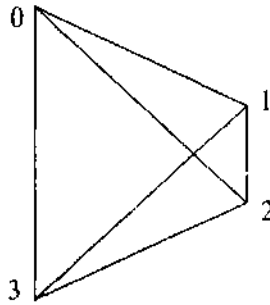


Рис. 2.9

Тетраэдр, который изображен на рис. 2.9, складывается из четырех равносторонних треугольников. Следовательно, он имеет четыре граневые оси третьего порядка, совпадающих с его вершинными осями, и три реберных оси второго порядка. Граневые оси дадут 8 элементов симметрии, вершинные — 3; добавив сюда один тождественный элемент, мы как раз и получим 12 элементов симметрии для этой геометрической фигуры.

Некоммутирующую группу вращений тетраэдра (T) можно получить путем перемножения элементов двух коммутативных — C_3 и C_2^2 — с образующими:

$$a = (012), \quad x = (01)(23), \quad y = (02)(13);$$

при перемножении $C_3 \cdot C_2^2$ будем иметь —

$$T = \{e, a, a^2\} \cdot \{e, x, y, xy\} = \{e, a, a^2, x, y, xy, ax, a^2x, ay, a^2y, axy, a^2xy\}.$$

С дидактической точки зрения, а мы постоянно вынуждены заботиться о доступности изложения, поскольку рассчитываем на широкий круг читателей, здесь уместно рекомендовать замечательную книгу Феликса Клейна «Икосаэдр», в которой знаменитый математик, придерживаясь «милый нашему сердцу» методологии конструктивизма, рекомендует:

Я советую читателю — здесь и в изложении последующих разделов — делать соответствующие рисунки или мысленно представлять себе на модели, которую легко построить, все рассматриваемые конструкции. Факты, о которых пойдет речь, очень просты, и в них легко разобраться при помощи простейших средств, но это обязательно надо сделать, поскольку в противном случае неизбежно возникнут осложнения. Я слишком перегрузил бы свое сочинение подробностями, если бы не рассчитывал на активное сотрудничество читателя¹.

В шестом параграфе своей книги Клейн очень наглядно разъясняет, почему «квадратичная» группа S_2^2 должна быть *инвариантной* в группе вращений тетраэдра T , а также почему *некоммутативная* группа T *гомоморфна* (или, как выразился Клейн, «кратно изоморфна») *коммутативной* группе из трех элементов — C_3 , и почему восемь, казалось бы, одинаковых 3-цикла распались на два класса сопряженности:

Мы уже отмечали выше, что при любом вращении, переводящем правильный тетраэдр в себя, двойственный к нему тетраэдр также переходит в себя. Восемь вершин этих двух тетраэдров образуют куб. Если же отметить на сфере 6 точек, соответствующих серединам ребер тетраэдра, то получим 6 вершин правильного *октаэдра*. Мы видим, таким образом, тесную связь между группами вращений тетраэдра и октаэдра, которую и намереваемся изучить. < ... >

Четыре вершины тетраэдра сопряжены друг другу и каждая из них сохраняется тремя вращениями — тождественным и двумя поворотами периода 3 вокруг диагоналей куба, проходящих через вершины тетраэдра. Мы видим также, что 8 из 12 вращений имеют период 3. Из них две четверки сопряжены между собой, а именно те, которые представляют собой поворот в *одном направлении* на угол $2\pi/3$ около вершины тетраэдра, которую они оставляют неподвижной. К этим 8 вращениям и единице нужно добавить еще 3 сопряженных друг другу вращения периода 2. Эти три вращения вокруг взаимно перпендикулярных диагоналей октаэдра сопряжены, так как переводятся друг в друга любым вращением периода 3. Вместе с единицей эти три вращения образуют квадратичную группу.

Мы заключаем отсюда, что квадратичная группа, полученная таким образом, *нормальна* в группе тетраэдра. Это следует из того, что 3 сопряженных друг другу октаэдра переходят в себя при всех вращениях из квадратичной группы и только при них. < ... >

Группа тетраэдральных вращений просто изоморфна группе соответствующих перестановок диагоналей куба. < ... > Сравним это с поведением трех диагоналей октаэдра. Поскольку они переходят в себя под действием квадратичной группы, 12 вращений тетраэдральной группы порождают лишь 3 различные перестановки трех диагоналей, а именно *циклические*. Таким образом, *группа тетраэдра кратно изоморфна (гомоморфна) циклической группе из трех элементов*².

С геометрической точки зрения, рассмотренная группа симметрии тетраэдра T не является полной. Ее можно увеличить в два раза, если произвести умножение группы тетраэдра $T = C_3 \cdot C_2^2$ на группу $C_2 = \{e, z\}$, где в качестве образующего z выбрать транспозицию (01). Группа C_2 будет отвечать плоскости зеркальной симметрии, проходящей через две вершины (2, 3) и середину ребра (0, 1) (см. рис. 2.9). Эта зеркальная плоскость за счет осей симметрии размножится на шесть (по числу ребер), что приведет к появлению шести различных транспозиций. Комбинируя эти транспозиции между собой, получим еще шесть циклических подстановок четвертого порядка. *Полная группа симметрии тетраэдра T_d*

¹ Клейн Ф. *Икосаэдр*, с. 17.

² Там же, с. 21–22.

будет состоять уже из 24 х элементов симметрии, которые приведены в табл. 2.54.

Тетраэдр можно вписать в куб (рис. 2.10), который имеет 6 квадратных граней с тремя осями четвертого порядка, 8 вершин с четырьмя осями третьего порядка и 6 реберных осей второго порядка. Таким образом, группа вращений куба (октаэдра) O складывается из следующих операций: вокруг каждой вершинной оси имеются два нетождественных поворота до полного совмещения всех геометрических элементов куба; вокруг каждой граневой оси также имеется по три нетождественных поворота; наконец, существует по одному повороту вокруг реберных осей. После того, как мы добавим один тождественный поворот, получится полная группа вращений куба, в состав которой тоже входит 24 элемента, т.е. полная (с отражениями) группа симметрии тетраэдра T изоморфна группе вращений куба O . Добавим к сказанному, что в кубе, как и в тетраэдре, можно провести зеркальные плоскости, а также ввести центр симметрии. Тогда число элементов в группе куба возрастет с 24 до 48.

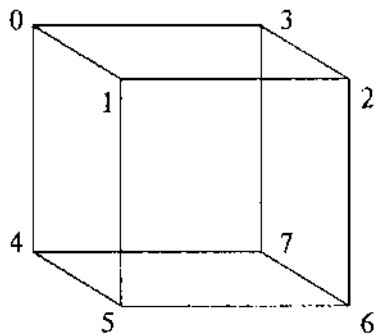


Рис. 2.10

Если пространственные диагонали куба пронумеровать числами от 0 до 3, вершины куба — от 0 до 7, как показано на рис. 2.10, а грани куба — числами от 0 до 5 (причем грань 0123 как 0, 4567 как 1, 1256 как 2, 2367 как 3, 3478 как 4 и 0145 как 5), то будем иметь три системы изоморфных подстановок — $O(4)$, $O(6)$, $O(8)$. Подстановки можно получить многими способами, в частности, как умножение группы тетраэдра (T) на одну из 6 циклических подстановок четвертого порядка (u), или как различные произведения двух образующих a и b . Упомянутые элементы симметрии приведены в табл. 2.54, в которой принято: $\bar{a} = a^{-1}$ и $\bar{b} = b^{-1}$.

Характеры всех пяти представлений полной группы симметрии тетраэдра T_d (группы вращений куба или октаэдра O) приведены в табл. 2.55. Образующими гомоморфного представления E_2 являются:

$$a = \begin{pmatrix} 1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{pmatrix}, \quad b = \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & 1/2 \end{pmatrix};$$

образующие изоморфного представления E_3 —

$$a = \begin{pmatrix} -1/3 & -\sqrt{2}/3 & -\sqrt{6}/2 \\ \sqrt{8}/3 & 1/6 & -\sqrt{3}/6 \\ 0 & \sqrt{3}/2 & -1/2 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1/2 & \sqrt{3}/2 \\ 0 & -\sqrt{3}/2 & 1/2 \end{pmatrix};$$

и образующие изоморфного представления E_4 —

$$a = \begin{pmatrix} 1/2 & \sqrt{3}/2 & 0 \\ \sqrt{3}/6 & 1/6 & \sqrt{8}/3 \\ \sqrt{6}/3 & \sqrt{2}/3 & 1/3 \end{pmatrix}, \quad b = \begin{pmatrix} -1/2 & \sqrt{3}/2 & 0 \\ \sqrt{3}/2 & -1/2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Таблица 2.54

№	$T_d, O(4)$	$O(6)$	$O(8)$	a, b	a, x, y, u	C_i
0	(0)	(0)	(0)	e	e	C_0
1	(01)(23)	(01)(35)	(07)(16)(25)(34)	$\overline{baba}$	x	C_1
2	(02)(13)	(24)(35)	(02)(13)(46)(57)	a^2	y	
3	(03)(12)	(01)(24)	(05)(14)(27)(36)	$\overline{baba}$	xy	
4	(012)	(043)(125)	(072)(146)	b	a	C_2
5	(021)	(034)(152)	(027)(164)	b	a^2	
6	(123)	(054)(132)	(143)(257)	$\overline{babab}$	a^2y	
7	(132)	(045)(123)	(134)(275)	$\overline{babab}$	ax	
8	(023)	(025)(143)	(025)(364)	$\overline{babab}$	axy	
9	(032)	(052)(134)	(052)(346)	$\overline{babab}$	a^2y	
A	(013)	(032)(154)	(075)(136)	a^2b	a^2xy	
B	(031)	(023)(145)	(057)(163)	$\overline{ba^2}$	ay	
C	(0123)	(2345)	(0123)(4567)	a	u	C_3
D	(0321)	(2543)	(0321)(4765)	$\overline{a}$	uy	
E	(0213)	(0513)	(0473)(1562)	$\overline{ba}$	ua^2y	
F	(0312)	(0315)	(0374)(1265)	$\overline{ab}$	ua^2xy	C_4
G	(0132)	(0214)	(0154)(2673)	$\overline{ba}$	$uaxy$	
H	(0231)	(0412)	(0451)(2376)	$\overline{ab}$	ua	
I	(23)	(01)(25)(34)	(06)(17)(23)(45)	ab	ua^2	
J	(13)	(03)(12)(45)	(06)(15)(24)(37)	$\overline{ababa}$	ux	
K	(12)	(02)(14)(35)	(06)(12)(35)(47)	$\overline{aba^2}$	uay	
L	(03)	(04)(12)(35)	(03)(17)(24)(56)	ba	uax	
M	(02)	(01)(23)(45)	(04)(17)(26)(35)	$\overline{baba^2}$	uxy	
N	(01)	(05)(13)(24)	(01)(24)(35)(67)	a^2ba	ua^2y	

Напомним, что группа T_d относится к симметрической S_4 , поэтому к ней применима методика диаграмм Юнга, которая использовалась нами для нахождения матриц неприводимых представлений группы $S_3 = D_3$, а также для определения размерности неприводимых представлений S_4 (рис. 2.8).

Таблицу характеров для представлений полной (с отражениями) группы симметрии куба O_d из 48-ми элементов можно получить путем «учетверения» табл. 2.55, т.е. можно использовать методику, которая применялась нами для составления таблиц характеров коммутативных групп C_2^3 (табл. 2.44) и C_2C_4 (табл. 2.45).

Таблица 2.55

I_d	C_2	C_1	C_2	C_3	C_4
E_0	1	1	1	1	1
E_1	1	1	1	1	1
E_2	2	2	-1	0	0
E_3	3	-1	0	-1	1
E_4	3	-1	0	1	-1

Перейдя от группы вращений тетраэдра T 12-го порядка к полной группе тетраэдра T_d 24-го порядка, мы, конечно, пропустили множество интересных групп, о которых необходимо сказать хотя бы несколько слов. На примере циклической группы 13-го порядка мы сделаем одно существенное замечание к матричным представлениям. Дело в том, что представления необязательно должны быть ортонормированными. В вводимом п. 2.1 для представления группы D_3 использовались матрицы с элементами, рассчитанными по $\text{mod } (2)$, а для коммутативной группы C_6 — по $\text{mod } (3)$. Следующие 12 матриц (без единичной) с элементами из целых чисел, взятых по $\text{mod } (3)$, вполне *представляют* коммутативную группу C_{13} :

$$\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 2 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 2 \\ 1 & 1 & 1 \\ 1 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 & 0 \\ 1 & 1 & 2 \\ 2 & 1 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 2 & 1 \\ 2 & 1 & 2 \\ 2 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 2 \\ 2 & 2 & 0 \\ 0 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 & 1 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 2 \\ 2 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 2 & 1 & 1 \\ 1 & 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 2 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Эти матрицы интересны тем, что все они симметричны относительно неглавной (второй) диагонали. Однако никакого геометрического содержания в приведенных матрицах не заключено.

Ортонормированные представления любой диэдральной группы имеют вполне определенный геометрический смысл, поскольку группе диэдра можно поставить в соответствие действия над *дипирамидами*. Группа диэдра 14-го порядка здесь не является исключением. Неприводимые представления группы D_7^1 отличаются от аналогичных для группы D_7^2 (табл. 2.51) наличием третьего двухмерного представления E_4 . Характеры всех представлений приведены в табл. 2.56, в которой тремя константами обозначены косинусы трех углов:

$$c_1 = \cos(2\pi/7) \cong 0.6234, \quad c_2 = \cos(4\pi/7) \cong -0.2224, \quad c_3 = \cos(6\pi/7) \cong -0.9017.$$

Таблица 2.56

D_7^1	C_0	C_1	C_2	C_3	C_4
E_0	1	1	1	1	1
E_1	1	1	1	1	1
E_2	2	$2 \cdot c_1$	$2 \cdot c_2$	$2 \cdot c_3$	0
E_3	2	$2 \cdot c_3$	$2 \cdot c_1$	$2 \cdot c_2$	0
E_4	2	$2 \cdot c_2$	$2 \cdot c_3$	$2 \cdot c_1$	0

Представления двух групп 16-го порядка D_8^1 и D_8^2 с одинаковыми таблицами характеров (табл. 2.57) строятся во многом по аналогии с представлениями групп D_6^1 и D_6^2 .

$D_8^{1,2}$	C_0	C_1	C_2	C_3	C_4	C_5	C_6
E_0	1	1	1	1	1	1	1
E_1	1	1	1	1	1	-1	-1
E_2	1	1	-1	1	-1	-1	1
E_3	1	1	-1	1	-1	1	-1
E_4	2	2	0	2	0	0	0
E_5	2	2	$\sqrt{2}$	0	$-\sqrt{2}$	0	0
E_6	2	-2	$-\sqrt{2}$	0	$\sqrt{2}$	0	0

Таблицы характеров двух других групп 16-го порядка типа $C_2D_4^1$ и $C_2D_4^2$ получаются путем «четверения» таблицы характеров для групп D_4^1 и D_4^2 (табл. 2.48). Для группы 16-го порядка D_8^3 двухмерное изоморфное представление уже заметно отличается от всех ранее рассмотренных; его образующими являются две матрицы:

$$a = \begin{pmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}, \quad b = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Геометрический смысл для группы D_8^3 все еще сохраняется, поскольку базисные векторы (первые столбцы матриц) могут быть вычерчены в геометрическом пространстве с мнимой осью. Однако общее число групп 16-го порядка равно 14. Чтобы рассмотреть представления всех этих групп, потребуется много места. Мы же завершим рассмотрение симметрии геометрических фигур *икосаэдром*.

Икосаэдр (рис. 2.11) имеет 20 треугольных граней, 30 ребер и 12 вершин, в каждой из которых сходятся по 5 ребер. Отсюда, очевидно, вытекает наличие у него 6 вершинных осей пятого порядка, 10 граневых осей третьего порядка и 15 реберных осей второго порядка. Несложный подсчет дает нам 60 элементов вращения. Группу симметрии икосаэдра (Y) можно получить, умножая элементы группы вращений тетраэдра (T) на одну из циклических подстановок пятого порядка. Точно так же, как в группах тетраэдра и куба, число элементов симметрии икосаэдра удваивается за счет введения зеркальных отражений и центра симметрии. Напомним, что если центры граней правильных многогранников при-

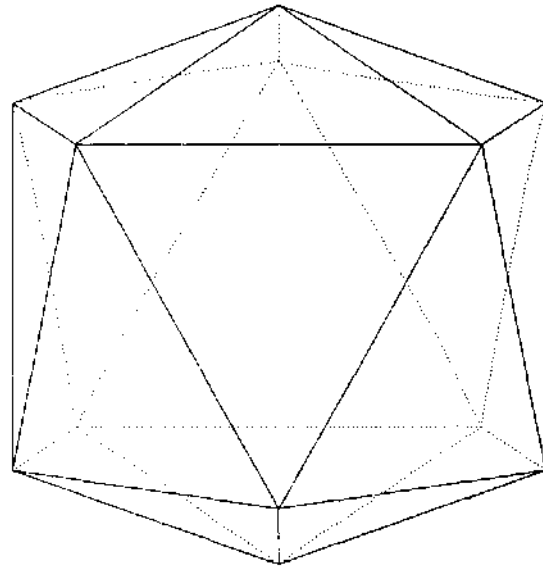


Рис. 2.11

нять за вершины новых многогранников, то в тетраэдр, куб и икосаэдр можно вписать соответственно *сопряженные* тетраэдр, октаэдр и додекаэдр. Построенные таким образом геометрические фигуры относительно своих исходных называются *двойственными*. «Двойники» имеют ту же самую группу симметрии и систему подгрупп, что и исходные фигуры. *Тетраэдр, гексаэдр (куб), октаэдр, икосаэдр и додекаэдр* образуют пять *Платоновых тел*. (Платон в своем сочинении «Тимей» атомам пяти элементов — *огню, воздуху, воде, земле и эфиру* — приписал форму этих пяти геометрических фигур.) Теперь, как и в случае с тетраэдром, мы воспользуемся книгой Фелiksa Клейна «Икосаэдр».

Группа икосаэдра наиболее интересна для нас тем, что она *проста* в отличие от групп диэдра, тетраэдра и октаэдра. Она разделяет это свойство с циклическими группами простого порядка. Для исследования группы икосаэдра вообразим, что на сфере отмечены 12 вершин икосаэдра, 20 вершин двойственного ему додекаэдра и тридцать точек, соответствующих серединам ребер икосаэдра. 12 вершин соединяются попарно 6 диаметрами, которые мы будем кратко называть диагоналями икосаэдра. Аналогично 20 вершин додекаэдра соединяются 10 диаметрами — диагоналями додекаэдра. Наконец, введем 15 перекрестных линий, соединяющих середины противоположных ребер.

Убедимся, что общее число вращений икосаэдра равно 60. В самом деле, каждая из 12 (очевидно, попарно сопряженных) вершин остается неподвижной относительно 5 вращений. Таким образом, каждой из 6 диагоналей икосаэдра соответствует 4 (помимо единичного) вращения периода 5, а всего 24 таких элемента. Точно так же 10 диагоналей додекаэдра дают $10 \cdot 2 = 20$ вращений периода 3, а 15 перекрестных линий дают 15 вращений периода 2; если добавить сюда единичное преобразование, получается 60, т.е. совокупность всех вращений икосаэдра. Из перечисленных вращений 15 элементов периода 2 и аналогично 20 элементов периода 3 образуют один класс сопряженных элементов, поскольку 15 перекрестных линий, как и десять диагоналей додекаэдра, переводятся друг в друга нашей группой, а вращения на угол $2\pi/3$ и $4\pi/3$ переходят друг в друга при перестановке полюсов вращения. Аналогичное рассмотрение показывает, что вращения периода 5 распадаются на 2 класса сопряженных элементов по 12 вращений в каждом. Первый класс содержит повороты на угол $\pm 2\pi/5$, а второй — на угол $\pm 4\pi/5$ вокруг диагоналей икосаэдра.

На основе полученных данных мы можем перечислить все *циклические подгруппы*, содержащиеся в группе икосаэдра. А именно, имеется 15 подгрупп порядка 2, 10 подгрупп порядка 3 и 6 подгрупп порядка 5; циклические подгруппы одинакового порядка попарно сопряжены. < ... >

Что касается остальных, *нециклических подгрупп*, то рассмотренные модели дают прежде всего 6 диэдральных групп с $n = 5$ и 10 диэдральных групп с $n = 3$. Первые имеют в качестве главных осей диагонали икосаэдра, вторые — диагонали додекаэдра, осями второго порядка для них служат 15 перекрестных линий. Можно было бы по аналогии с этим предположить наличие 15 диэдральных групп с $n = 2$, т.е. квадратичных групп. Однако для квадратичных групп нет разницы между главной осью и осями второго порядка. Поэтому мы получаем всего 5 попарно сопряженных квадратичных подгрупп. Это соответствует разбиению 15 перекрестных линий на 5 прямоугольных триад. Наличием этих триад и обусловлено то свойство группы икосаэдра, которое будет для нас важнее всего в дальнейшем. Поскольку существует лишь 5 прямоугольных триад, построенных из 15 перекрестных линий, эти триады должны сохраняться не только соответствующей квадратичной группой, но и целой совокупностью из 12 вращений. Можно показать, что они образуют тетраэдрическую группу. В самом деле, 8 вершин куба, соответствующих прямоуг-

льной триаде, содержатся среди 20 вершин додекаэдра. Таким образом, в икосаэдральной группе содержится 8 вращений периода 3, которые вместе с квадратичной группой образуют группу тетраэдра. Ясно также, что эти 5 тетраэдральных групп сопряжены друг с другом.

Оставляя опять без доказательства то, что перечисленными подгруппами исчерпываются все подгруппы группы икосаэдра, укажем только изоморфизм, возникающий из наличия 5 упомянутых выше прямоугольных триад. Можно показать, что каждое вращение периода 5 циклически переставляет эти триады в определенном порядке. Под действием вращений периода 3, с другой стороны, 2 триады остаются на месте, а остальные 3 циклически переставляются. Наконец, вращение периода 2 сохраняет одну триаду неподвижной, а остальные 4 попарно переставляются. Таким образом, группа из 60 вращений икосаэдра просто изоморфна группе из 60 четных перестановок 5 элементов¹.

Далее, мы возьмем небольшую выдержку из книги этого же автора под названием «Лекции о развитии математики в XIX столетии»:

Существует замечательная связь между группой икосаэдра G_{60} и шестидесятью четными перестановками из пяти элементов. Если середины тринадцати сторон икосаэдра взять в качестве вершин пяти октаэдров, то при любом из шестидесяти вращений икосаэдра октаэдры эти будут переставляться друг с другом. Таким образом, группа вращений икосаэдра G_{60} изоморфна группе четных перестановок из пяти элементов.

Что касается расширения группы икосаэдра G_{60} , то она, наоборот, не изоморфна группе G_{120} всех перестановок из пяти элементов. «Диаметральное» отражение (с помощью которого группа G_{120} получается из группы G_{60}) оставляет каждый из этих октаэдров на месте и, значит, не имеет ничего общего с перестановками этих октаэдров. У расширенной группы G_{120} имеются следующие инвариантные подгруппы: а) группа вращений G_{60} ; б) группа C_2 , состоящая из тождественного преобразования и диаметрального отражения. Группа же G_{120} перестановок из пяти элементов хотя и обладает инвариантной подгруппой G_{60} (является не чем иным, как знакопеременной группой), но никакой инвариантной подгруппы G_2 не имеет. Таким образом, ее структура совершенно иная².

Итак, на основе одних лишь манипуляций с геометрическими образами Клейн установил, что группа вращений икосаэдра U не имеет *нормальных делителей*, т.е. в группе U нет подгрупп, куда бы входили полные классы сопряженности. Если утверждается, что группа *проста*, значит, все ее представления будут *изоморфными*, одномерных представлений не будет, за исключением единичного E_0 (табл. 2.58). (Константы p и q в табл. 2.58 те же, что и в табл. 2.51.) Критерий полноты набора неприводимых представлений дает единственно возможное разложение числа 60:

$$60 = 1^2 + 3^2 + 3^2 + 4^2 + 5^2 = 1 + 12 + 12 + 20 + 15.$$

Таблица 2.58

γ	C_0	C_1	C_2	C_3	C_4
E_0	1	1	1	1	1
E_1	3	1	0	$2 \cdot p$	$-2 \cdot q$
E_2	3	-1	0	$-2 \cdot q$	$-2 \cdot p$
E_3	4	0	1	-1	-1
E_4	5	1	-1	0	0

¹ Там же, с. 23–26.

² Клейн Ф. Лекции ... В 2-х томах. Т. 1. М.: Наука, 1989, с. 379.

Клейн утверждает, что вращения икосаэдра периода 5 распадутся на два класса, в одном из которых окажутся повороты на угол $\pm 2\pi/5$, в другом — на угол $\pm 4\pi/5$. Теперь спросим себя: каким образом 24 подстановки «догадались» тоже разделиться на два класса по 12 подстановок в каждом; ведь подстановки ничего не «знали» о существовании икосаэдра? Тем не менее, обыкновенная процедура преобразования подобия приводит к тому, что одна часть 5-циклов попадает в класс C_3 , другая — в класс C_4 (табл. 2.59). Следовательно, индексы подстановок удивительным образом обладают одинаковыми свойствами с вершинами, диагоналями и другими деталями икосаэдра. Оказывается, что в столь разнородные объекты, каковыми являются подстановки и геометрические фигуры, поселился один и тот же дух симметрии.

Таблица 2.59

Подстановки группы икосаэдра $Y(A_5)$				C_i
(02)(34)	(04)(12)	(14)(23)	(0)	C_0
(23)(04)	(01)(24)	(24)(03)	(02)(14)	
(14)(03)	(02)(13)	(01)(34)	(03)(12)	C_1
(12)(34)	(13)(04)	(01)(23)	(13)(24)	
(024)	(042)	(013)	(031)	C_2
(143)	(043)	(124)	(142)	
(134)	(034)	(014)	(041)	
(243)	(132)	(032)	(021)	
(234)	(123)	(023)	(012)	
(01324)	(04231)	(03142)	(02413)	
(04312)	(02134)	(03214)	(04123)	C_3
(01243)	(03421)	(02341)	(01432)	
(01234)	(04321)	(02143)	(03412)	C_4
(03124)	(04213)	(01342)	(02431)	
(01423)	(03241)	(02314)	(04132)	

И все-таки не настолько уж они единосущностны, как это может показаться вначале. Стоит ввести для икосаэдра плоскости симметрии, как тут же обнаруживается расхождение его симметрии с симметрией 120 подстановок, переставляющих всеми возможными способами 5 индексов, т.е. с симметрией группы S_5 . Полная (с отражениями) группа симметрии икосаэдра не содержит в своем составе инвариантной подгруппы C_2 , хотя подгруппа такого порядка там имеется. Геометрическая интерпретация есть проведение аналогий. Но всякое сравнение имеет свои границы: то, что справедливо для тетраэдра и икосаэдра как фигур вращения, уже неверно для них как фигур с элементами отражения.

Подгруппу четных подстановок в симметрической группе S_n часто называют *знакопеременной* и обозначают как A_n . У нас получилось следующее: знакопеременная подгруппа A_4 четных подстановок изоморфна группе вращения тетраэдра T ; полная группа симметрических подстановок S_4 изоморфна полной группе симметрии тетраэдра T_d , т.е. переходы $A_4 \rightarrow S_4$ и $T \rightarrow T_d$ эквивалентны. Что же касается икосаэдра, то здесь наблюдается иная картина: знакопеременная подгруппа A_5 четных подстановок также изоморфна группе вращений икосаэдра Y , но полная группа симметрических подстановок S_5 уже не изоморфна полной

группе симметрии икосаэдра Y_d , т.е. переходы $A_5 \rightarrow S_5$ и $Y \rightarrow Y_d$ не эквивалентны. Судя по описанию симметрии икосаэдра, сделанному Клейном, такое различие довольно трудно уловить человеческим воображением.

В этом подразделе мы продолжим *морфологический анализ групп*, но теперь уже с заметным упором на *отношение порядка*, которое прежде всего реализуется в словах «быть подгруппой» или, более развернуто, «совокупность элементов G_1 образует подгруппу в группе G_2 ». Естественно, подгруппа G_1 *включена* в группу G_2 , однако *отношение включения* является слишком широким, а значит и более бедным понятием, чем *быть подгруппой*. Оно больше подходит к *аморфным множествам*, о которых речь впереди, хотя любое отношение порядка определяется через три закона: *рефлексивности*, *антисимметричности* и *транзитивности*. Для отношения «быть подгруппой» все три закона выполняются. Закон *рефлексивности* выполняется постольку, поскольку всякая группа G является *несобственной подгруппой* группы G . Закон *антисимметричности* также выполняется, так как если G_1 является подгруппой G_2 и G_2 является подгруппой G_1 , то группы G_1 и G_2 *изоморфны*. Наконец, для подгрупп справедлив и закон *транзитивности*: если G_1 является подгруппой G_2 и G_2 является подгруппой G_3 , то G_1 непременно будет подгруппой G_3 .

Подгруппы G_1 , G_2 , G_3 и т.д. образуют узлы, а отношения типа « G_1 является подгруппой G_2 » — *связи между узлами* G_1 и G_2 . Узлы и связи вместе составляют *решетку* или *структуру* подгрупп группы G , которая обозначается $S(G)$. Две *несобственных подгруппы* группы G ограничивают решетку $S(G)$ снизу и сверху, являясь ее *полюсами*. Решетку $S(G)$ удобно изображать графически и, как некий графический объект, она обладает определенными *групповыми* свойствами, отличными от групповых свойств исходной группы G . Группу симметрии решетки обозначим символами $S[S(G)]$. Нередко группа $S[G]$ *изоморфна* или *инвариантна* (т.е. G является подгруппой группы $S[G]$) относительно всех преобразований исходной группы G ; в этих случаях она называется *прозрачной*.

Решетки всех коммутативных групп *инверсные*. Это значит, что существует такая подстановка i , которая без нарушения связей переворачивает решетку «с ног на голову» и заменяет полюса на противоположные. Встречаются такие некоммутативные группы, решетка которых совпадает с решеткой от какой-нибудь коммутативной группы. В таких случаях решетка от некоммутативной группы тоже будет инверсной. Инверсная подстановка i не входит в группу симметрии решетки $S[G]$. Это особая подстановка, осуществляющая преобразование узлов решетки вдоль ее вертикальной оси, соединяющей полюса, тогда как группа преобразований $S[G]$ переставляет узлы, не изменяя их порядка. *Порядок узла* совпадает с порядком подгруппы, которую он представляет. Совокупность узлов одного порядка образует *уровень* соответствующего порядка. Порядок узла или порядок всего уровня, естественно, является *делителем* порядка группы G . Число уровней для группы с небольшим числом элементов в большинстве случаев равно числу делителей порядка группы. Если это условие выполняется, решетка называется *правильной*. В правильных решетках все пути от нижнего полюса до верхнего содержат одинаковое число связей. Группа тетраэдра T двенадцатого

порядка, у которой отсутствуют подгруппы шестого порядка, начинает бесконечный ряд *неправильных* решеток. В неправильных решетках число связей между полюсами различно.

Чрезвычайно важно понять с самого начала одну простую истину: подгруппы не появляются в результате какой-либо нашей с вами деятельности, например, через процедуры объединения, пересечения или умножения элементов. Объективно существуют группы, и они независимо от нас поделены на подгруппы. Наша задача состоит лишь в том, чтобы найти эти подгруппы и установить имеющиеся между ними связи. Для групп с большим числом элементов такая задача становится трудоемкой и требует особых приемов поиска. Часто сама решетка подсказывает нам, все ли подгруппы найдены и верно ли установлены связи. При последовательном изучении решеток обнаруживаются определенные закономерности. Для групп 16-го и 24-го порядка эти закономерности становятся особенно заметными. Так, для 14 решеток, построенных на подгруппах от групп 16-го порядка, можно сформулировать, например, такие правила: *число узлов на каждом из уровней нечетно и может быть одним из восьми следующих — 1, 3, 5, 7, 9, 11, 15 и 35; число подходящих или отходящих связей тоже нечетно и равно 1, 3, 5, 7, 9, 11 и 15 (два последних числа относятся к полюсам)*. Аналогичным образом выглядят правила для 12 правильных решеток, построенных от групп 24-го порядка: *количество узлов на всех уровнях нечетно — 1, 3, 5, 7, 9, 13, 15 и 19; число связей при полюсах всегда четно — 2, 4, 6, 8, 10, 14 и 16; число связей, отходящих от уровней 2-го и 4-го порядков, а также число связей, подходящих к уровням 6-го и 12-го порядков четно — 2, 4, 6, 8; число связей, подходящих к уровням 4-го и 8-го порядков и отходящих от уровней 3-го и 6-го порядков нечетно — 1, 3, 5, 7, 9, 13, 15 и 19*.

Нашей конечной целью будет построение так называемых *метарешеток* M_{16} и M_{24} от правильных решеток групп 16-го и 24-го порядков. Дело в том, что все правильные решетки от групп одного какого-то порядка являются подрешетками одной *верхнеполюсной* решетки. И, так как все правильные решетки, кроме того, включают в себя в качестве своей подрешетки одну общую для всех них *нижнеполюсную* решетку, они образуют «сверхрешетку», которую мы и называем *метарешеткой*. В роли верхнеполюсной могут выступать решетки от различных групп, например, решетки типа $S(C_2^m)$ и $S(D_n)$, но в роли нижнеполюсной выступит всегда одна — решетка от простой циклической группы $S(C_n)$. Неправильные решетки тоже могут образовать свои метарешетки, в частности, две из трех неправильных решеток, построенных от групп 24-го порядка, находятся в отношении порядка.

Таким образом, наряду с отношением порядка типа «быть подгруппой» существует совершенно другое отношение порядка, а именно: «быть подрешеткой». Если утверждается, что « $S(G_1)$ является подрешеткой $S(G_2)$ », то это еще не значит, что группа симметрии решетки $S[G_1]$ является подгруппой группы симметрии решетки $S[G_2]$. Чаще всего *группы симметрии* решеток $S[G_1]$ и $S[G_2]$ из-за принципиально различного строения вообще не сопоставимы. Отношение порядка типа « $S(G_1)$ является подрешеткой $S(G_2)$ » означает, что множества узлов и связей решетки $S(G_1)$ являются подмножествами множеств узлов и связей решетки $S(G_2)$. Здесь узлы и связи решеток выступают в роли *аморфных*, т.е. не групповых, множеств. Поэтому отношение «быть подрешеткой», по существу, является *отношением включения* одного множества (меньшего по мощности)

в другое (большее по мощности). С графической же точки зрения *метарешетки* по сравнению с *решетками* значительно менее *регулярны*. В них нельзя, в частности, найти закономерности по четности узлов и связей. Они заметно отличаются даже от *неправильных* решеток, поэтому их можно охарактеризовать как *очень неправильные*. Такой термин хорошо подходит к метарешеткам M_{16} и M_{24} , хотя метарешетки от групп с небольшим числом структурных вариантов (т.е. M_6 , M_8 , M_{12} , M_{16} , M_{20} , M_{27}) вполне правильны.

Простые циклические группы C_2 , C_3 , C_5 , ..., C_p , где p — простое число, имеют решетку, которая, если ее изобразить графически, выглядит как вертикальный отрезок прямой, ограниченный двумя узлами, соответствующими собственным подгруппам $\{e\} = (0)$ и C_p . Из двух отрезков состоит решетка для групп типа C_4 , C_9 , C_{25} , ..., C_{p^2} (рис. 2.12). Группы 4-го, 9-го, 25-го порядков имеют еще по одному коммутативному варианту, обозначаемому как C_2^2 , C_3^2 , C_5^2 , ..., C_p^2 .

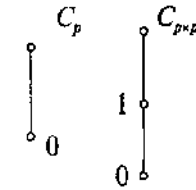


Рис. 2.12

Собственными подгруппами для C_3^2 , к примеру, являются:

$$1 - \{e, a, a^2\}, \quad 2 - \{e, b, b^2\}, \quad 3 - \{e, ab, a^2b^2\}, \quad 4 - \{e, a^2b, ab^2\}.$$

Все четыре узла имеют порядок равный 3. Поскольку собственные подгруппы образуют единственный уровень между полюсами, то и инверсная подстановка i представляет собой транспозицию, у которой в качестве индексов выступают нижний и верхний полюса (транспозицию полюсов здесь и ниже писать не будем). Три решетки для $p = 2, 3$ и 5 изображены на рис. 2.13.

Группа симметрии таких решеток определяется простой формулой:

$$S[C_p^2] \approx D_{p-1}.$$

Так, группа $S[C_3^2]$ определяется подстановками D_3 :

$$S[C_3^2] = \{ (0), (12), (23), (13), (123), (132) \} \approx D_3.$$

Групп шестого порядка две — $C_6 \approx C_2C_3$ и D_3 . Их *правильные* решетки изображены на рис. 2.14. Для $S(C_6)$ инверсная подстановка равна $i = (12)$. Несмотря на то, что узлы решеток $S(C_6)$ и $S(D_3)$ образованы непохожими собственными подгруппами —

$$C_6: 1 = \{e, a^2, a^4\}, \quad 2 = \{e, a^3\};$$

$$D_3: 1 = \{e, a, a^2\}, \quad 2 = \{e, b\}, \quad 3 = \{e, ab\}, \quad 4 = \{e, a^2b\},$$

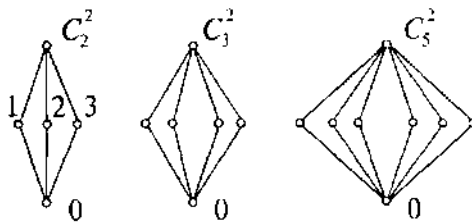


Рис. 2.13

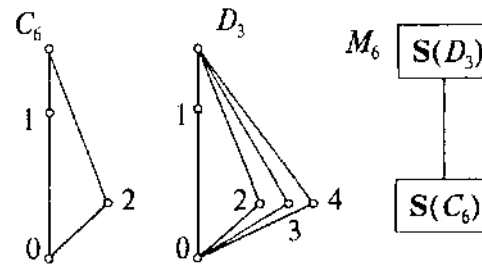


Рис. 2.14

графически решетку $S(C_6)$ можно вписать в решетку $S(D_3)$, т.е. узлы и связи решетки $S(C_6)$ образуют подмножества соответствующих множеств решетки $S(D_3)$, следовательно, решетка $S(C_6)$ образует *нижний*, а $S(D_3)$ *верхний* полюс *метарешетки* M_6 . Симметрия решеток $S(C_6)$, $S(C_{10})$ и т.д. минимальна — C_1 ; решетки $S(D_3)$, $S(D_5)$ и т.д. *прозрачны*:

$$S[C_2 C_p] \approx S[C_{2,p}] \approx C_1, \quad S[D_p] \approx D_p.$$

Групп 8-го порядка пять; самой элементарной из них с точки зрения структуры подгрупп является циклическая группа C_8 . Решетка $S(C_8)$ представляет из себя трехзвенную цепь; она является нижним полюсом метарешетки M_8 . Теперь выпишем все собственные подгруппы группы C_8^3 :

$$1 = \{e, a\}, 2 = \{e, b\}, 3 = \{e, c\}, 4 = \{e, ab\}, 5 = \{e, ac\}, 6 = \{e, bc\},$$

$$7 = \{e, abc\}, 8 = \{e, a, b, ab\}, 9 = \{e, a, c, ac\}, A = \{e, b, c, bc\},$$

$$B = \{e, a, bc, abc\}, C = \{e, b, ac, abc\}, D = \{e, c, ab, abc\},$$

$$E = \{e, ab, ac, bc\}.$$

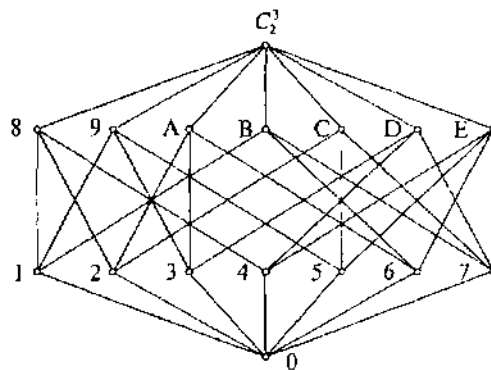


Рис. 2.15

Решетка из этих подгрупп $S(C_8^3)$ изображена на рис. 2.15. Она является верхним полюсом метарешетки M_8 . Решетка $S(C_8^3)$ является *инверсной*, причем инверсию можно осуществить несколькими способами, в частности, подстановкой —

$$i = (18)(29)(3A)(4B)(5C)(6D)(7E).$$

Группа симметрии $S[C_8^3]$ обладает удивительными свойствами. Подобно группе вращения икосаэдра I , она не имеет нормальных делителей, т.е. является *простой*. Все ее подстановки *четны*, поскольку образующими группы являются *антикоммутирующие четные транспозиции*. Действительно, если переобозначить узлы решетки в соответствии с подстановками —

$$a = (23)(45)(89)(CD), \quad b = (12)(56)(9A)(BC),$$

$$c = (24)(67)(AD)(CE), \quad d = (13)(27)(8D)(AB),$$

то графическая структура $S(C_8^3)$ останется без изменения. Составим несколько произведений из этих подстановок, получим:

$$ab = (123)(465)(8A9)(BCD), \quad ba = (132)(456)(89A)(BDC),$$

$$cb = (124)(567)(9AD)(BCE), \quad bc = (142)(576)(9DA)(BEC),$$

$$cd = (13)(2476)(8DBA)(CE), \quad dc = (13)(2674)(8ABD)(CE).$$

Если учесть, что узлы уровней 2-го и 4-го порядков при всех групповых преобразованиях не переставляются, то для представления группы $S[C_8^3]$ достаточно взять подстановки, составленные для одного какого-то уровня, например, ниж-

него. Все 168 четных подстановок простой группы $S[C_2^3]$ разбиты на пять классов и выписаны в табл. 2.60.

Таблица 2.60

Подстановки простой группы симметрии $S[C_2^3]$							C_i
(1476523)	(1523764)	(1375426)	(1742563)	(1345762)	(1235746)	(0)	C_0
(1753462)	(1635472)	(1624573)	(1234675)	(1736425)	(1367452)	(1462537)	C_1
(1637245)	(1274536)	(1432765)	(1627354)	(1647532)	(1642375)	(1657423)	
(1542736)	(1467325)	(1746352)	(1524637)	(1452673)	(1726534)	(1276345)	
(1264357)	(1342657)	(1453726)	(1267543)	(1724365)	(1435627)	(1543672)	
(1325674)	(1253647)	(1576432)	(1472356)	(1563427)	(1573246)	(1324756)	
(1756243)	(1567234)	(1365247)	(1653274)	(1376254)	(1254763)	(1735264)	
(256)(374)	(135)(467)	(176)(254)	(175)(236)	(167)(234)	(135)(247)	(154)(236)	C_2
(236)(457)	(176)(345)	(127)(456)	(136)(275)	(162)(347)	(153)(274)	(145)(263)	
(237)(456)	(165)(374)	(142)(576)	(157)(263)	(126)(374)	(124)(357)	(123)(465)	
(265)(347)	(167)(354)	(172)(465)	(163)(257)	(174)(263)	(142)(375)	(132)(456)	
(275)(346)	(156)(347)	(124)(567)	(167)(257)	(124)(376)	(134)(257)	(135)(264)	
(273)(465)	(153)(476)	(164)(275)	(176)(235)	(147)(236)	(143)(275)	(153)(246)	
(263)(475)	(173)(456)	(167)(245)	(135)(276)	(142)(367)	(152)(374)	(124)(365)	
(257)(364)	(137)(465)	(146)(257)	(153)(267)	(176)(243)	(125)(347)	(142)(356)	
(67)(2345)	(36)(1745)	(47)(1256)	(56)(1327)	(13)(2476)	(17)(2435)	(16)(2354)	C_3
(67)(2543)	(36)(1547)	(47)(1652)	(56)(1723)	(13)(2674)	(17)(2534)	(16)(2453)	
(24)(3756)	(14)(3567)	(26)(1754)	(12)(3675)	(27)(1436)	(45)(1372)	(25)(1463)	
(24)(3657)	(14)(3765)	(26)(1457)	(12)(3576)	(27)(1634)	(45)(1273)	(25)(1364)	
(35)(2746)	(57)(1643)	(15)(2467)	(37)(1625)	(46)(1732)	(23)(1475)	(34)(1562)	
(35)(2647)	(57)(1346)	(15)(2764)	(37)(1526)	(46)(1237)	(23)(1574)	(34)(1265)	C_4
(24)(35)	(16)(25)	(15)(47)	(17)(45)	(14)(57)	(12)(56)	(13)(46)	
(24)(67)	(16)(34)	(15)(26)	(17)(23)	(14)(36)	(12)(37)	(13)(27)	
(35)(67)	(25)(34)	(26)(47)	(23)(45)	(36)(57)	(37)(56)	(27)(46)	

Как видно из этой таблицы, подстановки класса C_4 , принадлежащие одному столбцу, коммутируют между собой: если подстановки берутся из различных столбцов, они будут антикоммутировать. Для аналогичных простых верхнеплюсовых групп прослеживается та же самая закономерность: число коммутирующих подгрупп равно числу узлов (в данном случае равно 7), а число элементов, входящих в каждую подгруппу, но отличных от тождественного, равно числу отходящих связей. У нас на каждый узел приходится по три таких связи, следовательно, максимальной коммутационной подгруппой является C_2^3 , в силу чего наша группа *непрозрачна*.

Группу $S[C_2^3]$ можно задать, например, такими определяющими ее соотношениями:

$$\begin{aligned}
 a^6cb &= b^2c^2a = b^2a^6c = c^2ab^2, & ac^3b^2 &= bca = ca^6b^2, ca^2 = a^4bc^2, \\
 ab^3c^2 &= ba^6c^2 = cab^3 = cba^6, & a^4b^3c &= a^2cb = b^3a^4c^2 = c^2a^4, \\
 ac^2b &= b^2a^6c^2 = cb^3a = ca^6b, & a^4b^2 &= c^2b^2a^2, acb^2 = b^3a^3, \\
 a^2b^2c &= b^3a^2c^2 = ca^5b = c^2b^3a^5, & a^3b^2c &= bac^2 = bca^6 \text{ и т.д.}
 \end{aligned}$$

В справедливости этих соотношений можно убедиться, если вместо букв a, b и c подставить, например, следующие подстановки:

$$a = (1476523)(8DBECA9), \quad b = (67)(2345)(89)(ADEC), \quad c = (123)(465)(8A9)(CDB).$$

Все остальные решетки от групп 8-го порядка являются подрешетками решетки $S(C_2^3)$. Так, восемь собственных подгрупп диэдра —

$$D_4^1: \quad 1 = \{e, b\}, \quad 2 = \{e, a^2\}, \quad 4 = \{e, a^2b\}, \quad 5 = \{e, ab\}, \quad 7 = \{e, a^3b\},$$

$$8 = \{e, a^2, b, a^2b\}, \quad A = \{e, a, a^2, a^3\}, \quad C = \{e, a^2, ab, a^3b\}$$

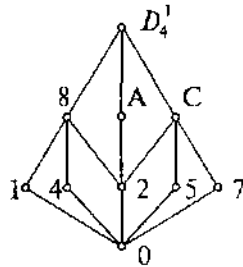


Рис. 2.16

являются соответствующими узлами $S(C_2^3)$. Решетка диэдра $S(D_4^1)$ изображена на рис. 2.16. Она прозрачна, поскольку восемь диэдральных подстановок оставляют графическую структуру рис. 2.16 неизменной

$$S[D_4^1] \approx D_4^1 = \{(0), (14), (57), (14)(57), (15)(47)(8C), (17)(45)(8C), (1547)(8C), (1745)(8C)\}.$$

Если из решетки диэдра $S(D_4^1)$ исключить два узла — 5 и 7, — то в результате получим решетку от коммутативной группы — C_2C_4 . Другими словами, непрозрачная, но инверсная ($i = (28)(1A)(4C)$ и $\bar{i} = (28)(4A)(1C)$) решетка $S(C_2C_4)$

вкладывается в прозрачную, но не инверсную решетку $S(D_4^1)$. Группа симметрии $S[C_2C_4]$ определяется следующими четырьмя подстановками:

$$S[C_2C_4] \approx C_2^2 = \{(0), (14), (AC), (14)(AC)\}.$$

Наконец, решетка кватерниона $S(D_4^2)$ получается из инверсной решетки $S(C_2C_4)$ путем отбрасывания еще одной пары узлов — 1 и 4. Группа симметрии решетки кватерниона изоморфна группе D_3 :

$$S[D_4^2] \approx D_3 = \{(0), (8A), (8C), (AC), (8AC), (8CA)\}.$$

Итак, пять решеток от групп 8-го порядка образуют одну метарешетку M_8 , изображенную на рис. 2.17. Все решетки от групп 8-го порядка являются правильными и имеют четное число узлов (4, 6, 8, 10, 16) и нечетное число связей (3, 7, 11, 15, 35).

Пропуская очевидные решетки от групп 9-го, 10-го и 11-го порядков, перейдем к рассмотрению пяти решеток от групп 12-го порядка. Нам удобнее всего начать с верхнеполюсной решетки $S(D_6^1)$. Группа диэдра содержит следующие подгруппы:

$$D_6^1: \quad 1 = \{e, a^3\}, \quad 2 = \{e, a, a^2, a^3, a^4, a^5\}, \quad 3 = \{e, a^2, a^4\}, \quad 4 = \{e, a^3, b, a^3b\},$$

$$5 = \{e, a^3, ab, a^4b\}, \quad 6 = \{e, a^3, a^2b, a^5b\}, \quad 7 = \{e, a^2, a^4, b, a^2b, a^4b\},$$

$$8 = \{e, a^2, a^4, ab, a^3b, a^5b\}, \quad 9 = \{e, b\}, \quad A = \{e, a^3b\}, \quad B = \{e, ab\},$$

$$C = \{e, a^4b\}, \quad D = \{e, a^2b\}, \quad E = \{e, a^5b\}.$$

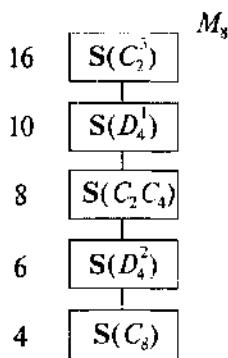


Рис. 2.17

Решетка $S(D_6^1)$, изображенная на рис. 2.18, является *прозрачной*, так как образующие —

$$a = (456)(78)(9BDACE), \\ b = (45)(78)(9B)(AC)(DE),$$

инвариантно переставляющие узлы решетки $S(D_6^1)$, порождают группу D_6^1 , так что $S[D_6^1] \approx D_6^1$.

Восемь узлов верхнеполюсной решетки $S(D_6^1)$, а именно: 1, 2, 3, 4, 7, 8, 9, А, дают все узлы инверсной решетки $S(C_2C_6)$, шесть узлов — 1, 2, 3, 4, 5, 6 — дают решетку $S(D_6^2)$ и четыре узла — 1, 2, 3, 4 — дают нижнеполюсную решетку $S(C_{12})$. Четыре правильных решетки образуют одну метарешетку M_{12} , которая изображена на рис. 2.19. Число узлов у всех названных решеток — четно (6, 8, 10 и 16); число связей — нечетно (7, 11, 17 и 33).

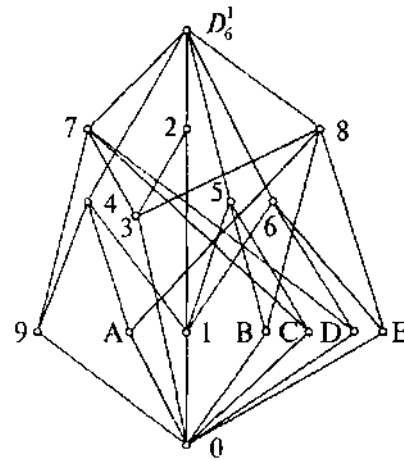


Рис. 2.18

Решетка тетраэдра $S(T)$ (рис. 2.20) особая и образована следующими узлами:

$$1 = \{e, ab\}, \quad 2 = \{e, a^2b^2\}, \quad 3 = \{e, ab^2a\}, \quad 4 = \{e, ab, a^2b^2, ab^2a\}, \\ 5 = \{e, a, a^2\}, \quad 6 = \{e, b, b^2\}, \quad 7 = \{e, a^2b, b^2a\}, \quad 8 = \{e, ab^2, ba^2\}.$$

На рисунке, где изображена решетка $S(T)$, можно увидеть, что 3 пути между полюсами образованы тремя связями, а 4 других пути составлены только из двух связей, поэтому $S(T)$ и называется *неправильной*. Три узла нижнего уровня подчинены симметрической группе $S_3 \approx D_3$, а четыре узла верхнего — симметрической группе S_4 . В итоге, группа симметрии решетки тетраэдра содержит 144 элемента:

$$S[T] \approx S_3 \times S_4, \quad \text{кроме того, } S[C_2C_6] \approx S[D_6^2] \approx D_3.$$

Структуры от групп 13-го, 14-го и 15-го порядков нам знакомы, поэтому не будем здесь на них останавливаться и сразу перейдем к морфологическому анализу групп 16-го порядка.

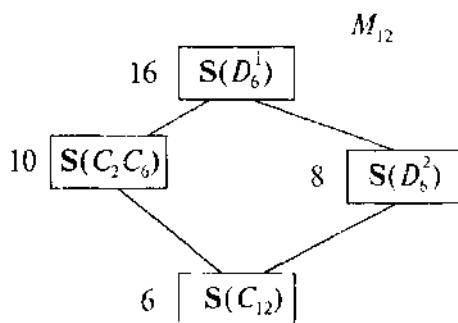


Рис. 2.19

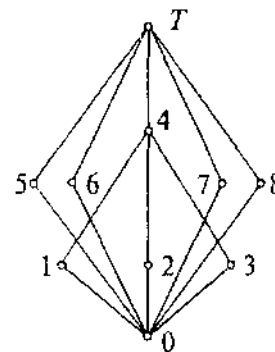


Рис. 2.20

Самой простой из них является цепь из четырех звеньев структуры $S(C_{16})$, а наиболее разветвленной — решетка $S(C_2^4)$. Ее условно-схематическое изображение показано на рис. 2.21. Между полюсами имеется три уровня. Уровень 2-го порядка состоит из 15 узлов:

$$\begin{aligned} 1 &= \{e, a\}, & 2 &= \{e, b\}, & 3 &= \{e, c\}, & 4 &= \{e, d\}, & 5 &= \{e, ab\}, \\ 6 &= \{e, ac\}, & 7 &= \{e, ad\}, & 8 &= \{e, bc\}, & 9 &= \{e, bd\}, & A &= \{e, cd\}, \\ B &= \{e, abc\}, & C &= \{e, abd\}, & D &= \{e, bcd\}, & E &= \{e, acd\}, & F &= \{e, abcd\}. \end{aligned}$$

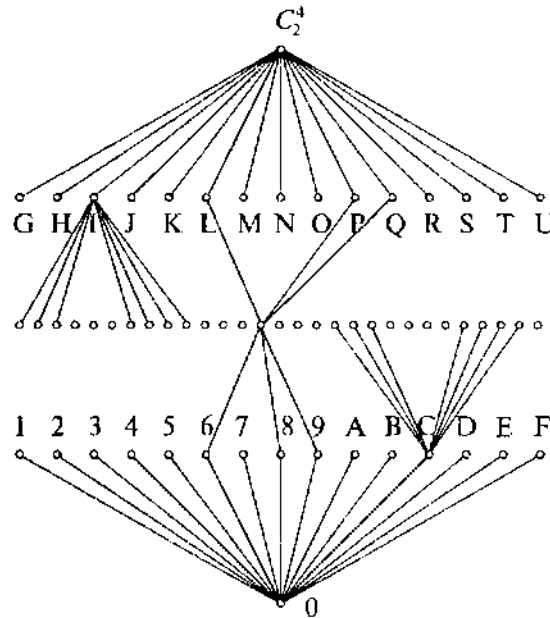


Рис. 2.21

Уровень 8-го порядка также состоит из 15 узлов:

$$\begin{aligned} G &= \{e, a, b, c, ab, ac, bc, abc\}, \\ H &= \{e, a, b, d, ab, ad, bd, abd\}, \\ I &= \{e, a, c, d, ac, ad, cd, acd\}, \\ J &= \{e, b, c, d, bc, bd, cd, bcd\}, \\ K &= \{e, ab, ad, bd, ac, bc, cd, abcd\}, \\ L &= \{e, c, d, cd, ab, abc, abd, abcd\}, \\ M &= \{e, a, d, ad, bc, abc, bcd, abcd\}, \\ N &= \{e, b, d, bd, ac, abc, acd, abcd\}, \\ O &= \{e, a, c, bd, ac, abd, bcd, abcd\}, \\ P &= \{e, b, c, bc, ad, abd, acd, abcd\}, \\ Q &= \{e, a, b, cd, ab, bcd, acd, abcd\}, \\ R &= \{e, a, bc, bd, cd, abc, abd, acd\}, \\ S &= \{e, b, ac, ad, cd, abc, abd, bcd\}, \\ T &= \{e, c, ab, ad, bd, abc, acd, bcd\}, \\ U &= \{e, d, bc, ab, ac, abd, acd, bcd\}. \end{aligned}$$

Уровень 4-го порядка образован 35 узлами. Подгруппы мы перечислим, но присваивать им специальных обозначений не будем:

$$\begin{aligned} &\{e, a, b, ab\}, \{e, a, c, ac\}, \{e, a, d, ad\}, \{e, b, c, bc\}, \{e, b, d, bd\}, \\ &\{e, c, d, cd\}, \{e, a, bc, abc\}, \{e, b, ac, abc\}, \{e, c, ab, abc\}, \\ &\{e, a, bd, abd\}, \{e, b, ad, abd\}, \{e, d, ab, abd\}, \{e, b, ad, bcd\}, \\ &\{e, c, bd, bcd\}, \{e, d, bc, bcd\}, \{e, a, cd, acd\}, \{e, abc, bcd, ad\}, \\ &\{e, abc, acd, bd\}, \{e, abd, bcd, ac\}, \{e, ab, acd, bcd\}, \{e, d, abc, abcd\}, \\ &\{e, ab, cd, abcd\}, \{e, ac, bd, abcd\}, \{e, ad, bc, abcd\}, \{e, c, ad, acd\}, \\ &\{e, d, ac, acd\}, \{e, a, bcd, abcd\}, \{e, b, acd, abcd\}, \{e, ab, ad, bd\}, \\ &\{e, ab, ac, bc\}, \{e, ac, ad, cd\}, \{e, bc, cd, bd\}, \{e, abd, acd, bc\}, \\ &\{e, c, abd, abcd\}, \{e, abc, abd, cd\}. \end{aligned}$$

Сравнивая выписанные подгруппы между собой, мы можем заключить: каждая подгруппа 2-го порядка входит в 7 различных подгрупп 4-го порядка; каждая подгруппа 4-го порядка состоит из элементов 3 подгрупп 2-го порядка (напри-

мер, подгруппа $\{e, a, b, ab\}$ состоит из элементов подгруппы 1, 2 и 5); каждая подгруппа 4-го порядка целиком входит в три подгруппы 8-го порядка (например, подгруппа $\{e, a, b, ab\}$ входит в подгруппы G, H и Q); каждая подгруппа 8-го порядка состоит из элементов 7 подгрупп 4-го порядка. Таким образом, число подходящих связей к каждому узлу 8-го порядка и число отходящих связей от каждого узла 2-го порядка равно 7. Это, в свою очередь, означает, что число связей для узлов названных уровней у других структур, построенных на основе групп 16-го порядка, также не может превосходить число 7. Далее, число подходящих и отходящих связей для уровня 4-го порядка у других структур не может превосходить число 3.

Группа $S[C_2^4]$ *простая*. Все ее подстановки *четны*. Группа содержит 32 256 элементов, которые разбиты на 12 классов. В табл. 2.61 приведены примеры конкретных подстановок, взятые из каждого класса; здесь же указано количество подстановок в классе.

Таблица 2.61

C_i	Подстановки группы $S[C_2^4]$	Количество
C_0	(0)	1
C_1	(25)(36)(9C)(AE)	105
C_2	(2E)(36)(48)(5A)(7B)(9C)	546
C_3	(1FD)(2B6)(3E7)(89A)	1 456
C_4	(2BE7)(3C69)(5BA4)	2 184
C_5	(2C4)(3BE)(597)(68A)	2 912
C_6	(DF)(24C)(579)(3AB6E8)	2 912
C_7	(16EBD)(258CA)(3497F)	2 912
C_8	(2E)(5A)(37C8)(49B6)	3 276
C_9	(1DF)(23BE67)(4AC859)	4 368
C_{10}	(2697E8D)(53C4ABF)	5 760
C_{11}	(124659E87DCFDA3)	5 824

В классе C_1 выполняются известные нам *антикоммутационные* соотношения. Все подстановки этого класса приведены в табл. 2.62. Таблица разбита на 15 частей (по числу узлов на одном нижнем уровне); в каждую часть входит по 7 *коммутирующих* между собой подстановок (по числу связей, приходящихся на один узел). Последнее обстоятельство делает решетку $S(C_2^4)$ *непрозрачной*.

Следующей группой 16-го порядка, решетка которой вписывается в верхне-полюсную решетку $S(C_2^4)$, является группа $C_2D_4^1$. Прежде чем приступить к морфологическому анализу группы $C_2D_4^1$, нам необходимо выписать все ее подстановки:

0 = (0), 1 = (0123)(4657), 2 = (02)(13)(45)(67), 3 = (0321)(4756),
 4 = (04)(17)(25)(36), 5 = (05)(16)(24)(37), 6 = (06)(14)(27)(35),
 7 = (07)(15)(26)(34), 8 = (89), 9 = (0123)(4657)(89),
 A = (02)(13)(45)(67)(89), B = (0321)(4756)(89), C = (04)(17)(25)(36)(89),
 D = (05)(16)(24)(37)(89), E = (06)(14)(27)(35)(89), F = (07)(15)(26)(34)(89).

Таблица 2.62

Наименьший класс (C_1) подстановок группы симметрии $S[C_2^3]$					
(25)(36)(9C)(AE)	(15)(38)(7C)(AD)	(16)(28)(7E)(9D)	(29)(5C)(8D)(BF)	(68)(DE)(3B)(AF)	
(25)(36)(47)(DE)	(15)(38)(49)(EF)	(16)(28)(4A)(CF)	(29)(17)(8D)(6E)	(68)(12)(79)(DE)	
(25)(47)(8B)(AE)	(15)(49)(6B)(AD)	(16)(4A)(5B)(9D)	(29)(17)(3A)(BF)	(68)(12)(4C)(AF)	
(25)(8B)(9C)(DF)	(15)(6B)(7C)(FF)	(16)(5B)(7F)(CF)	(29)(3A)(5C)(6E)	(68)(79)(3B)(4C)	
(36)(8B)(AE)(DF)	(38)(6B)(AD)(EF)	(28)(5B)(9D)(CF)	(8D)(3A)(6E)(BF)	(4C)(79)(AF)(DE)	
(36)(47)(8B)(9C)	(38)(49)(6B)(7C)	(28)(4A)(5B)(7E)	(8D)(17)(3A)(5C)	(12)(3B)(4C)(DE)	
(47)(9C)(AE)(DF)	(49)(7C)(AD)(EF)	(4A)(7E)(9D)(CF)	(17)(5C)(6E)(BF)	(12)(3B)(79)(AF)	
(CD)(4E)(9F)(7A)	(14)(6A)(59)(8D)	(1B)(4D)(23)(CE)	(24)(1C)(6F)(8A)	(34)(1E)(2D)(BC)	
(CD)(4E)(13)(2B)	(14)(6A)(2C)(8F)	(1B)(4D)(9A)(56)	(24)(57)(8A)(BE)	(34)(1E)(5F)(89)	
(CD)(13)(58)(7A)	(14)(2C)(3E)(BD)	(1B)(23)(9A)(7F)	(24)(1C)(3D)(BE)	(34)(67)(89)(BC)	
(CD)(58)(2B)(9F)	(14)(3E)(59)(8F)	(1B)(56)(7F)(CE)	(24)(3D)(57)(6F)	(34)(2D)(5F)(67)	
(4E)(58)(7A)(2B)	(6A)(3E)(BD)(8F)	(4D)(23)(56)(7F)	(8A)(3D)(1C)(57)	(1E)(5F)(67)(BC)	
(4E)(13)(58)(9F)	(6A)(2C)(3E)(59)	(4D)(7F)(9A)(CE)	(8A)(3D)(6F)(BE)	(1E)(2D)(67)(89)	
(13)(2B)(7A)(9F)	(2C)(59)(BD)(8F)	(23)(56)(9A)(CE)	(1C)(57)(6F)(BE)	(2D)(5F)(89)(BC)	
(18)(26)(4F)(AC)	(6D)(3F)(8E)(AB)	(7B)(39)(48)(6C)	(2F)(1A)(46)(8C)	(78)(1D)(2E)(69)	
(18)(35)(4F)(9E)	(6D)(AB)(19)(45)	(7B)(1F)(5E)(6C)	(2F)(5D)(8C)(9B)	(78)(1D)(3C)(5A)	
(18)(35)(7D)(AC)	(6D)(27)(3F)(45)	(7B)(1F)(2A)(39)	(2F)(37)(46)(5D)	(78)(2E)(4B)(5A)	
(18)(26)(7D)(9E)	(6D)(19)(27)(8E)	(7B)(2A)(48)(5E)	(2F)(1A)(37)(9B)	(78)(3C)(4B)(69)	
(4F)(7D)(9E)(AC)	(AB)(19)(27)(3F)	(6C)(2A)(39)(5E)	(8C)(37)(46)(9B)	(1D)(2E)(3C)(4B)	
(4F)(35)(26)(7D)	(AB)(27)(45)(8E)	(6C)(1F)(2A)(48)	(8C)(1A)(37)(5D)	(1D)(4B)(5A)(69)	
(26)(35)(9E)(AC)	(19)(3F)(45)(8E)	(1F)(39)(48)(5E)	(1A)(46)(5D)(9B)	(2E)(3C)(5A)(69)	

Путаницы не произойдет, если для обозначения подгруппы (узлов) группы $C_2D_4^1$ мы используем те же самые символы, что и для индексов подстановок:

1 = {0, 2, 6, 7, 8, A, E, F}, 2 = {0, 2, 6, 7, 9, B, C, D}, 3 = {0, 2, 4, 5, 9, B, E, F},
 4 = {0, 1, 2, 3, 8, 9, A, B}, 5 = {0, 1, 2, 3, C, D, E, F}, 6 = {0, 1, 2, 3, 4, 5, 6, 7},
 7 = {0, 2, 4, 5, 8, A, C, D}, 8 = {0, 2, 8, A}, 9 = {0, 2}, A = {0, 8, 7, F}, B = {0, 8, 6, E},
 C = {0, A, 6, F}, D = {0, A, 7, E}, E = {0, 2, E, F}, F = {0, 2, 9, B}, G = {0, 2, 6, 7},
 H = {0, 2, 4, 5}, I = {0, 1, 2, 3}, J = {0, 2, C, D}, K = {0, 8, 5, D}, L = {0, 8, 4, C},
 M = {0, A, 4, D}, N = {0, A, 5, C}, O = {0, 8}, P = {0, F}, Q = {0, E}, R = {0, 6},
 S = {0, 7}, T = {0, 5}, U = {0, 4}, X = {0, D}, Y = {0, C}, Z = {0, A}.

Решетка $S(C_2D_4^1)$ изображена на рис. 2.22. Она состоит как бы из трех решеток $S(C_2^3)$ — одна сверху и две внизу. Характеристика ее такова: число узлов на всех уровнях *нечетно* — 7, 15 и 11; число связей тоже *нечетно* — 1, 3, 5 и 7. Решетка *прозрачна*, так как подстановки a и b порождают группу диэдра D_4^1 , а коммутирующая с a и b подстановка c расширяет группу D_4^1 до $C_2D_4^1$:

$$a = (25)(36)(EG)(FI)(ACBD)(KM)(LN)(OZ)(PRQS)(TU),$$

$$b = (AD)(BC)(OZ)(PQ)(KM)(LN)(TU), c = (KL)(MN)(TU)(XY).$$

Однако такие длинные подстановки, инвариантно переставляющие узлы на всех уровнях, можно не писать. Как и в предыдущем случае, группа симметрии $S[C_2D_4^1]$ вполне представима 64-мя подстановками, составленными по 11 узлам только одного нижнего уровня (табл. 2.63).

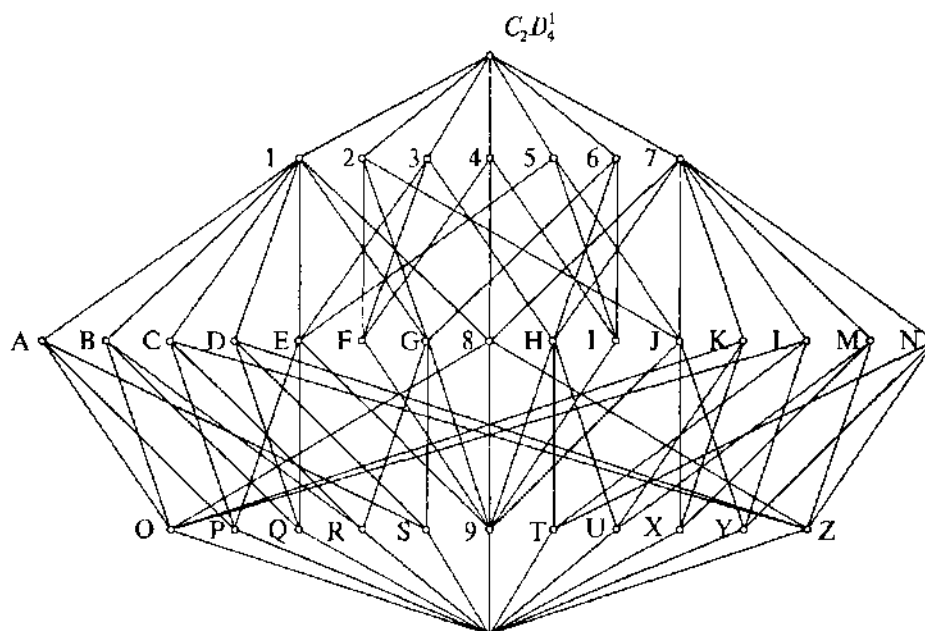


Рис. 2.22

Таблица 2.63

Подстановки группы симметрии $S[C_2D_4^1]$			
(0)	(PTSX)(QURY)	(OZ)(PQ)(TU)	(OZ)(PTRX)(QUSY)
(TU)(XY)	(PUSY)(QTRX)	(OZ)(PQ)(XY)	(OZ)(PXRT)(QYSU)
(TX)(UY)	(PXST)(QYRU)	(OZ)(RS)(TU)	(OZ)(PURY)(QTSX)
(TY)(UX)	(PYSU)(QXRT)	(OZ)(RS)(TU)	(OZ)(PYRU)(QXST)
(PQ)(RS)	(PTRY)(QUSX)	(OZ)(PROS)(TU)	(OZ)(PROS)(TXUY)
(PQ)(RS)(TU)(XY)	(PUHX)(QTSY)	(OZ)(PSQR)(TU)	(OZ)(PSQR)(TYUX)
(PQ)(RS)(TX)(UY)	(PXRU)(QYST)	(OZ)(TYUX)(RS)	(OZ)(PRQS)(TYUX)
(PQ)(RS)(TY)(UX)	(PYRT)(QXSU)	(OZ)(TXUY)(RS)	(OZ)(PSQR)(TXUY)
(PR)(QS)	(PTQU)(RYSX)	(OZ)(PROS)(XY)	(OZ)(PXQY)(RTSU)
(PR)(QS)(TU)(XY)	(PUQT)(RXSY)	(OZ)(PSQR)(XY)	(OZ)(PYQX)(RUST)
(PR)(QS)(TX)(UY)	(PXQY)(RUST)	(OZ)(TYUX)(PQ)	(OZ)(PTQU)(RXSY)
(PR)(QS)(TY)(UX)	(PYQX)(RTSU)	(OZ)(TXUY)(PQ)	(OZ)(PUQT)(RYSX)
(PS)(QR)	(PX)(QY)(RU)(ST)	(OZ)(PTSY)(QURX)	(OZ)(PT)(QU)(RX)(SY)
(PS)(QR)(TU)(XY)	(PU)(QT)(RX)(SY)	(OZ)(PYST)(QXRU)	(OZ)(PU)(QT)(RY)(SX)
(PS)(QR)(TX)(UY)	(PY)(QX)(RT)(SU)	(OZ)(PUSX)(QTRY)	(OZ)(PX)(QY)(RT)(SU)
(PS)(QR)(TY)(UX)	(PT)(QU)(RY)(SX)	(OZ)(PXSU)(QYRT)	(OZ)(PY)(QX)(RU)(ST)

- Решетка $S(C_2^2 C_4)$ от коммутативной группы *инверсная* и состоит из двух симметрично расположенных решеток $S(C_2^2)$. Она получается из решетки $S(C_2 D_4^1)$ путем удаления восьми узлов — A, B, C, D, P, Q, R, S. Инверсной подстановкой для $S(C_2^2 C_4)$ является:

$$i = (1Z)(2X)(3T)(4O)(5Y)(6U)(79)(KF)(LI)(MG)(NE).$$

Решетка $S(C_2^2 C_4)$ прозрачна, так как имеются три коммутирующие подстановки, образующие группу

$$C_2^2 C_4: a = (25)(36)(EG)(FI), \quad b = (14)(36)(EI)(FG), \quad c = (KI NM)(TU)(XOYZ).$$

Группу $S[C_2^2 C_4]$ определяют подстановки, составленные по 11 узлам среднего уровня. При их нахождении очень удобно ориентироваться на хорошо известную нам группу $S[C_2^3]$, для которой ищется подгруппа, оставляющая один узел на месте (у нас это узел 7 для верхнего этажа и узел 9 для нижнего). Далее, необходимо помнить, что верхняя и нижняя подрешетки $S(C_2^3)$ рассматриваемой решетки $S(C_2^2 C_4)$ существуют практически независимо. Выпишем порождающие элементы двух подгрупп преобразований, действующих на этих подрешетках:

$$\begin{aligned} a &= (EG)(FI), & a' &= (KM)(LN), & b &= (EFG)(8HJ), & b' &= (LNM), \\ c &= (EFGI)(HJ), & c' &= (KMLN), & d &= (EF)(8J), & d' &= (KI). \end{aligned}$$

Обратим несколько большее внимание на группу диэдра 16-го порядка D_8^1 . Это позволит нам понять структуру еще двух групп примерно этого же строения. С этой целью выпишем для нее все основные соотношения и подстановки:

$$\begin{aligned} D_8^1: \quad a &= (01234567), & ab &= ba^7 = (07)(16)(25)(34), \\ a^2 &= (0246)(1357), & a^2 b &= ba^6 = (06)(15)(24), \\ a^3 &= (03614725), & a^3 b &= ba^5 = (05)(14)(23)(67), \\ a^4 &= (04)(15)(26)(37), & a^4 b &= ba^4 = (04)(13)(57), \\ a^5 &= (05274163), & a^5 b &= ba^3 = (03)(12)(47)(56), \\ a^6 &= (0642)(1753), & a^6 b &= ba^2 = (02)(37)(46), \\ a^7 &= (07654321), & a^7 b &= ba = (01)(27)(36)(45), \\ e &= (0), & b &= (17)(26)(35). \end{aligned}$$

Заметим, что помимо a и a^7 , представляющих собой 8-циклы и фигурирующих в главном соотношении, имеются еще два элемента — a^3 и a^5 — точно таким же периодом. Если возможна группа с равенством $ab = ba^7$, то нельзя ли попытаться построить еще две группы на равенствах — $ab = ba^3$ и $ab = ba^5$? Такая попытка увенчается успехом, если в качестве образующих b взять, соответственно:

$$D_8^3: \quad b = (02)(15)(46), \quad D_8^4: \quad b = (04)(26).$$

Тогда получим следующую картину определяющих соотношений:

$$\begin{aligned} D_8^3: \quad ab &= ba^3 = (0541)(2367), & D_8^4: \quad ab &= ba^5 = (01674523), \\ a^2 b &= ba^6 = (13)(26)(57), & a^2 b &= ba^2 = (0642)(1357), \\ a^3 b &= ba = (0347)(1652), & a^3 b &= ba^7 = (03254761), \\ a^4 b &= ba^4 = (06)(24)(37), & a^4 b &= ba^4 = (15)(37), \\ a^5 b &= ba^7 = (0145)(2763), & a^5 b &= ba = (05634127), \\ a^6 b &= ba^2 = (04)(17)(35), & a^6 b &= ba^6 = (0246)(1753), \\ a^7 b &= ba^5 = (0743)(1256), & a^7 b &= ba^3 = (07214365). \end{aligned}$$

Здесь нужно не забыть о существовании еще одной группы *кватернионного типа* с образующими —

$$D_8^2: \quad a = (01234567)(89ABCDEF), \\ b = (084C)(1F5B)(2E6A)(3D79).$$

Теперь выпишем все подгруппы группы диэдра. Так как решетка $S(D_8^1)$ вписывается в решетку $S(C_2D_4^1)$, нам удобно узлы *подрешетки* $S(D_8^1)$ обозначить через соответствующие узлы *надрешетки* $S(C_2D_4^1)$:

$$D_8^1: \quad 3 = \{e, a^2, a^4, a^6\}, \quad 4 = \{e, a, a^2, a^3, a^4, a^5, a^6, a^7\}, \\ 7 = \{e, a^2, a^4, a^6, b, a^2b, a^4b, a^6b\}, \quad 8 = \{e, a^2, a^4, a^6, ab, a^3b, a^5b, a^7b\}, \\ 9 = \{e, a^4\}, \quad E = \{e, a^4, b, a^4b\}, \quad G = \{e, a^4, a^2b, a^6b\}, \\ H = \{e, a^4, ab, a^5b\}, \quad J = \{e, a^4, a^3b, a^7b\}, \quad P = \{e, b\}, \\ Q = \{e, a^4b\}, \quad R = \{e, a^2b\}, \quad S = \{e, a^6b\}, \quad T = \{e, ab\}, \\ U = \{e, a^5b\}, \quad X = \{e, a^3b\}, \quad Y = \{e, a^7b\}.$$

Решетка $S(D_8^1)$ изображена на рис. 2.23. Если из этой решетки удалить четыре узла — T, U, X, Y , — получим решетку $S(D_8^3)$. Затем, если удалить еще четыре узла — P, Q, R, S , получим решетку $S(D_8^2)$. Наконец, если из решетки $S(D_8^1)$ удалить восемь других узлов — H, J, R, S, T, U, X, Y , — получим решетку $S(D_8^4)$.

Группа симметрии диэдральной решетки $S\{D_8^1\}$ состоит из 96 подстановок, которые выписаны в табл. 2.64.

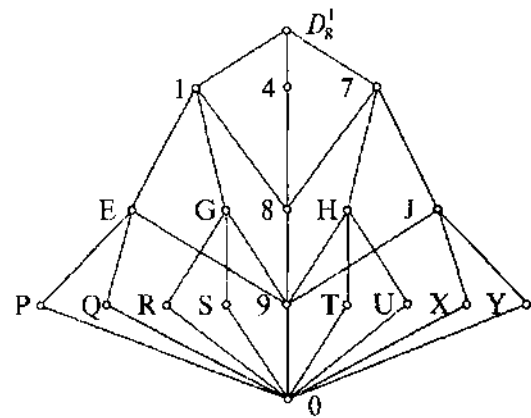


Рис. 2.23

Для группы $S\{D_8^1\}$ все определяется уровнем 2-го порядка. Из табл. 2.64 видно, что решетка диэдра *прозрачна*, что нельзя сказать про другие решетки этой серии, в частности:

$$S[D_8^2] \approx D_4^1 = \{(0), (HJ), (EG), (HJ)(EG), (EJGH), \\ (EHGJ), (EH)(GJ), (EJ)(HG)\};$$

$$S[D_8^3] \approx C_2D_4^1 = \{(0), (PQ), (RS), (PQ)(RS), (PRQS), (PSQR), \\ (PS)(QR), (PR)(QS), (HJ), (PQ)(HJ), (RS)(HJ), (PQ)(RS)(HJ), \\ (PRQS)(HJ), (PSQR)(HJ), (PS)(QR)(HJ), (PR)(QS)(HJ)\};$$

$$S[D_8^4] \approx S[C_2C_8] \approx C_2^2 = \{(0), (47), (QP), (47)(QP)\}.$$

Подстановки группы симметрии $S[D_8^1]$			
(O)	(PSQR)(XY)	(PTRXQUSY)	(PQ)(RS)(TU)(XY)
(PQ)	(TYUX)(PQ)	(PXSTQYRL)	(PS)(QR)(TX)(UY)
(RS)	(TYJX)(RS)	(PURYQTSX)	(PS)(QR)(TY)(XU)
(TU)	(PQ)(RS)(TU)	(PYSUQXRT)	(PR)(SQ)(TX)(UY)
(XY)	(PQ)(RS)(XY)	(PXRUQYST)	(PR)(SQ)(TY)(UX)
(PQ)(RS)	(PQ)(TU)(XY)	(PUSXQTRY)	(PT)(QU)(RX)(SY)
(PQ)(TU)	(RS)(TU)(XY)	(PYRTQXSU)	(PU)(QT)(RX)(SY)
(PQ)(XY)	(PQ)(TY)(UX)	(PTSYQURX)	(PX)(QY)(RT)(SU)
(RS)(TU)	(RS)(TX)(UY)	(PUSYQTRX)	(PX)(QY)(RU)(ST)
(RS)(XY)	(RS)(TY)(UX)	(PYRUQXST)	(PT)(QU)(RY)(SX)
(TU)(XY)	(PQ)(TX)(UY)	(PTSXQURY)	(PU)(QT)(RY)(SX)
(PS)(QR)	(TU)(PS)(RQ)	(PXRQYSU)	(PY)(QX)(RT)(SU)
(PR)(SQ)	(TU)(PR)(SQ)	(PURXQTSY)	(PY)(QX)(RU)(ST)
(TX)(UY)	(XY)(PS)(RQ)	(PXSUQYRT)	(PS)(RQ)(TU)(XY)
(TY)(XU)	(XY)(PR)(SQ)	(PTRYQJSX)	(PR)(SQ)(TU)(XY)
(PRQS)	(PS)(QR)(TU)	(PYSTQXRU)	(PQ)(RS)(TX)(UY)
(PSQR)	(PS)(QR)(XY)	(TYUX)(PH)(SQ)	(PQ)(RS)(TY)(XU)
(TXUY)	(TX)(UY)(PQ)	(TYUX)(PS)(QR)	(PSQR)(TX)(UY)
(TYUX)	(TX)(UY)(RS)	(TXUY)(PR)(SQ)	(PSQR)(TY)(UX)
(PRQS)(TU)	(PR)(SQ)(TU)	(TXUY)(PS)(QR)	(PRQS)(TX)(UY)
(PRQS)(XY)	(PR)(SQ)(XY)	(PSQR)(TYUX)	(PRQS)(TY)(UX)
(TXUY)(PQ)	(TY)(UX)(PQ)	(PSQR)(TXUY)	(PRQS)(TU)(XY)
(TXUY)(RS)	(TY)(UX)(RS)	(PRQS)(TYUX)	(PSQR)(TU)(XY)
(PSQR)(TU)	(PRQS)(TXUY)	(TYUX)(PQ)(RS)	(TXUY)(PQ)(RS)

Самым поразительным математическим фактом здесь является то, что решетка $S(D_8^4)$ от *некоммутативной* группы является *инверсионной* и в точности совпадает с решеткой $S(C_2 C_8)$ от *коммутативной* группы. Их общей инверсионной подстановкой является —

$$i = (19)(8E)(4Q)(7P).$$

Решетку $S(D_8^1)$ (рис. 2.23) полезно сравнить с решеткой $S(D_4^1)$ (рис. 2.16), поскольку они очевидным образом находятся в *отношении порядка*. Четыре узла — E, G, H, J, — среднего уровня дают группу $S[D_4^1] \approx D_4^1$, которая является *гомоморфным* представлением группы $S[D_8^1]$ из восьми узлов нижнего уровня — P, Q, R, S, T, U, X, Y. Причем из рис. 2.23 можно сразу записать систему проецирования элементов группы $S[D_8^1]$ на группу $S[D_4^1]$. Так, например, перестановка двух узлов (PQ) оставляет узел E на месте; перестановка же четырех узлов типа (PR)(QS), (PS)(QR) или (PSQR) проецируется на транспозицию (EG) и т.д. Если построить следующую решетку $S(D_{16}^1)$, то ее узлы будут связаны с узлами $S(D_8^1)$ аналогичным образом и группа $S[D_8^1]$ уже станет гомоморфным представлением группы $S[D_{16}^1]$. Так возникает иерархия решеток от диэдральных групп, которая выражается в *метарешетке MD* в виде бесконечной цепи. Главное отличие диэдр-

альной метарешетки MD от ранее рассмотренных метарешеток M_n состоит в том, что для MD цепь решетчатых вложений сопровождается цепью групповых вложений —

$$S(D_4^1) \subset S(D_8^1) \subset S(D_{16}^1) \subset \dots$$

$$S[D_4^1] \subset S[D_8^1] \subset S[D_{16}^1] \subset \dots$$

Рассмотрим следующие две группы 16-го порядка, которые мы обозначили как D_4^3 и D_4^4 (напомним, что D_4^1 и D_4^2 относятся к группам 8-го порядка). Для наглядности приведем основные групповые соотношения и подстановки —

$$\begin{aligned} D_4^3: \quad & a = (0123)(4567), \quad a^2 = (02)(13)(46)(57), \quad a^3 = (0321)(4765), \\ & b = (03)(12)(4567), \quad b^2 = (46)(57), \quad b^3 = (03)(12)(4765), \\ & ab = b^3a^3 = (02)(46)(57), \quad ab^2 = b^2a = (0123)(4765), \\ & a^2b = ba^2 = (01)(23)(4765), \quad a^2b^2 = b^2a^2 = (02)(13), \\ & a^3b = b^3a = (13), \quad a^3b^2 = b^2a^3 = (0321)(4567), \\ & ab^3 = ba^3 = (02), \quad a^2b^3 = b^3a^2 = (01)(23)(4567), \\ & a^3b^3 = ba = (13)(46)(57), \quad e = (0); \\ D_4^4: \quad & a = (0123)(46)(57), \quad a^2 = (02)(13), \quad a^3 = (0321)(46)(57), \\ & b = (03)(12)(4567), \quad b^2 = (46)(57), \quad b^3 = (03)(12)(4765), \\ & ab = ba^3 = (02)(4765), \quad ab^2 = b^2a = (0123), \\ & a^2b = ba^2 = (01)(23)(4567), \quad a^2b^2 = b^2a^2 = (02)(13)(46)(57), \\ & a^3b = ba = (13)(4765), \quad a^3b^2 = b^2a^3 = (0321), \\ & ab^3 = b^3a^3 = (02)(4567), \quad a^2b^3 = b^3a^2 = (01)(23)(4765), \\ & a^3b^3 = b^3a = (13)(4567), \quad e = (0). \end{aligned}$$

Для группы D_4^4 приведем еще один изоморфный вариант на базе кватерниона —

$$\begin{aligned} D_4^4: \quad & e = (0), \quad a = (0123)(4657)(89AB), \quad a^2 = (02)(13)(45)(67)(8A)(9B), \\ & a^3 = (0321)(4756)(8BA9), \quad b = (0425)(1736)(8A9B), \\ & b^2 = (02)(13)(45)(67), \quad b^3 = (0524)(1637)(8A)(9B), \\ & a^2b^3 = b^3a^2 = (01)(23)(4765), \quad a^2b^2 = b^2a^2 = (8A)(9B), \\ & a^3b = b^3a^3 = (0627)(1435)(89AB), \quad a^3b^2 = b^2a^3 = (0123)(4657)(8BA9), \\ & ab^3 = ba = (0627)(1435)(8BA9), \quad a^3b^3 = ba^3 = (0726)(1534)(89AB), \\ & ab^2 = b^2a = (0321)(4756)(89AB), \quad a^2b = ba^2 = (0524)(1637). \end{aligned}$$

Выпишем подгруппы группы D_4^3 . Как и в предыдущих случаях, воспользуемся обозначениями узлов решетки $S(C_2D_4^3)$, поскольку узлы рассматриваемой решетки $S(D_4^3)$ являются подмножеством узлов решетки $S(C_2D_4^3)$.

$$\begin{aligned} D_4^3: \quad & 1 = \{e, a, a^2, a^3, b^2, ab^2, a^2b^2, a^3b^2\}, \quad 4 = \{e, b, b^2, b^3, a^2, a^2b, a^2b^2, a^2b^3\}, \\ & 7 = \{e, a^2, b^2, a^2b^2, ab, a^3b, ab^3, a^3b^3\}, \quad 8 = \{e, a^2, b^2, a^2b^2\}, \quad 9 = \{e, b^2\}, \end{aligned}$$

$B = \{e, a^2, ab^2, a^3b^2\}$, $A = \{e, a, a^2, a^3\}$, $H = \{e, b^2, a^3b^3, a^3b\}$, $O = \{e, a^2\}$,
 $F = \{e, b, b^2, b^3\}$, $I = \{e, b^2, a^2b, a^2b^3\}$, $Y = \{e, ab\}$, $Z = \{e, a^2b^2\}$,
 $J = \{e, b^2, ab, ab^3\}$, $K = \{e, a^2, ab^3, a^3b^3\}$, $L = \{e, a^2, a^3b, ab\}$,
 $T = \{e, a^3b^3\}$, $U = \{e, a^3b\}$, $M = \{e, ab^3, a^2b^2, a^3b\}$,
 $N = \{e, ab, a^2b^2, a^3b^3\}$, $X = \{e, ab^3\}$.

Решетка $S(D_4^3)$ изображена на рис. 2.24. Между уровнями 2-го и 4-го порядка расположена подрешетка $S(C_2^3)$, что облегчает поиск группы $S[D_4^3]$. В группе $S[D_4^3]$ 48-го порядка имеется подгруппа, изоморфная D_4^3 , с образующими —

$a = (14)(9O)(HL)(KJ)(TY)(AIBF)$, $b = (14)(9O)(MN)(HKJL)(TXYU)(AFBI)$.

Таким образом, решетка $S(D_4^3)$ прозрачна. Узлы решетки $S(D_4^3)$ и узлы *инверсной* ($i = (1O)(49)(7Z)$) решетки $S(C_2^3)$ образуют два подмножества от множества узлов решетки $S(D_4^3)$:

$S(D_4^4) = \{1, 4, 7, 8, 9, A, B, H, J, F, I, O, Z\}$,

$S(C_4^2) = \{1, 4, 7, 8, 9, A, B, M, N, F, I, O, Z\}$.

$S[D_4^4] \approx C_2D_4^1 = \{(0), (HJ), (FI), (IJ)(FI), (FHIJ), (FH)(IJ), (FJIH), (AB),$
 $(AB)(HJ), (AB)(FI), (AB)(HJ)(FI), (AB)(FHIJ), (AB)(FH)(IJ), (AB)(FJIH)\}$;

$S[C_4^2] \approx C_2D_4^1 = \{(0), (AB), (FI), (AB)(FI), (AFBI), (AF)(BI), (AIBF), (MN),$
 $(MN)(AB), (MN)(FI), (MN)(AB)(FI), (MN)(AFBI), (MN)(AF)(BI),$
 $(MN)(AIBF)\}$.

Отсюда можно видеть, что решетки $S(D_4^4)$ и $S(C_4^2)$ непрозрачны.

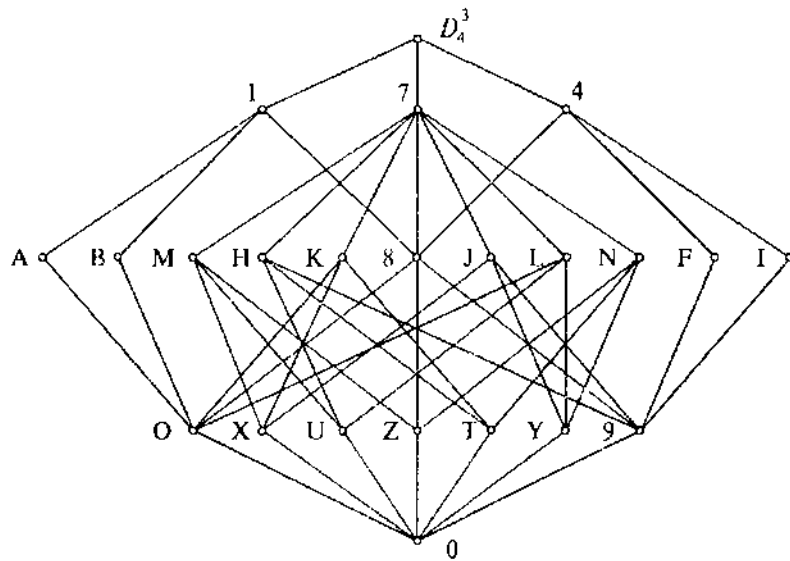


Рис. 2.24

Перейдем к группе D_4^3 . Ее целиком определяют следующие простые соотношения:

$$a^2 = b^2 = c^2 = e, \quad abc = bca = cab.$$

Из этих равенств несложно вывести вспомогательные соотношения —

$$acb = cba = bac, \quad aba = cbc, \quad aca = bcb, \quad bab = cac,$$

которые позволяют составить таблицу умножения из 16 элементов группы —

$$D_4^3: \{e, a, b, c, ab, ac, ba, ca, bc, cb, abc, acb, aba, aca, bab, abab\}.$$

Очень удобно образующие приводить в виде *регулярных подстановок*, тогда при их умножении сразу будем получать столбцы таблицы умножения, а не ее отдельные элементы —

$$a = (01)(23)(45)(67)(89)(AB)(CD)(EF), \quad b = (02)(16)(3E)(4C)(5B)(7F)(8D)(9A), \\ c = (04)(18)(2A)(3D)(5E)(6B)(7C)(9F).$$

Решетка $S(D_4^3)$ изображена на рис. 2.25. Если из этой решетки удалить узлы R, S, T и U, то получим решетку $S(C_2D_4^2)$. Несмотря на внешнее различие решеток, их группы симметрии одинаковые и изоморфны полной группе куба:

$$S[D_4^3] \approx S[C_2D_4^2] \approx O_h.$$

Таким образом, у нас появился прекрасный повод для изучения O_h — этой важнейшей группы симметрии (хотя кое-что о ней было сказано в предыдущем разделе). В табл. 2.65 приведены подстановки $S[D_4^3]$, составленные по нижнему уровню решетки.

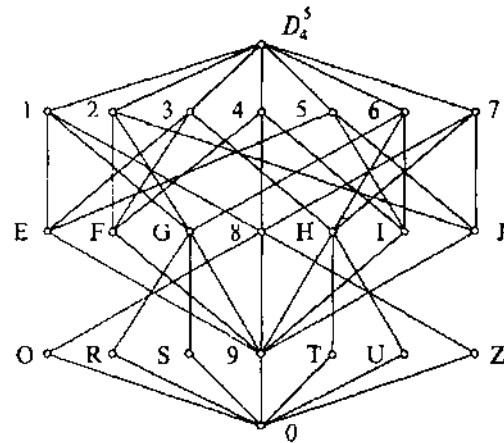


Рис. 2.25

Таблица 2.65

Подстановки группы симметрии $S[D_4^3] \approx O_h$							
0	(0)	C	(ZUOT)	0'	(RS)(ZO)(UT)	C'	(RZSO)(UT)
1	(RS)(UT)	D	(ZTOU)	1'	(RS)	D'	(ROSZ)(UT)
2	(ZO)(UT)	E	(RTSU)	2'	(ZO)	E'	(ZUOT)(RS)
3	(RS)(ZO)	F	(RUST)	3'	(UT)	F'	(ZTOU)(RS)
4	(ROU)(SZT)	G	(RZSO)	4'	(RT)(SU)	G'	(RUOSTZ)
5	(RUO)(STZ)	H	(ROSZ)	5'	(RU)(ST)	H'	(RZTSOU)
6	(RTO)(SUZ)	I	(RS)(ZT)(OU)	6'	(RZ)(SO)	I'	(RUZSTO)
7	(ROT)(SZU)	J	(RU)(ST)(ZO)	7'	(RO)(SZ)	J'	(ROTSZU)
8	(RZT)(SOU)	K	(RZ)(SO)(UT)	8'	(ZU)(OT)	K'	(RTOSUZ)
9	(RTZ)(SUO)	L	(RO)(SZ)(UT)	9'	(ZT)(OU)	L'	(RZUSOT)
A	(RUZ)(STO)	M	(RS)(ZU)(OT)	A'	(RUST)(ZO)	M'	(RTZSUO)
B	(RZU)(SOT)	N	(RT)(SU)(ZO)	B'	(RTSU)(ZO)	N'	(ROUSZT)

Табл. 2.65 для группы $S[D_4^5]$ связана с табл. 2.54 для группы вращения куба (или октаэдра) следующим образом: если пронумерованные грани куба (рис. 2.10) обозначить буквами по следующей схеме:

$$0 \rightarrow R, 1 \rightarrow S, 2 \rightarrow Z, 3 \rightarrow U, 4 \rightarrow O, 5 \rightarrow T,$$

то первые 24 подстановки (с 0 по N) табл. 2.65 полностью совпадут с 24 подстановками столбца $O(6)$ табл. 2.54.

Группа O_d является одновременно группой симметрии декартовых координат. В табл. 2.66 показано соответствие между нашими подстановками и матрицами, преобразующими всеми возможными способами оси координат x, y, z . Табл. 2.66 составить несложно, если помнить, что матрицы одного класса должны иметь один и тот же характер; подстановки на транспозициях соответствуют симметричным матрицам; обратные подстановки отвечают транспонированным матрицам. Ввиду важности группы O_d перечислим все ее подгруппы. При этом мы ставим перед собой цель напомнить два простых приема, позволяющих по нескольким известным подгруппам найти большое число неизвестных. Дело в том, что когда группа небольшого порядка, все ее подгруппы отыскать несложно, но наша группа 48-го порядка содержит уже 84 подгруппы и отыскать их только на основе знания определения группы довольно тяжело.

Самый эффективный способ поиска неизменяемых подгрупп состоит в сопряжении одной какой-то известной подгруппы. Предположим, нам удалось отыскать одну из подгрупп 4-го порядка, не являющуюся нормальным делителем, — $\{0, 2', 4', N\}$. Тогда с помощью элемента K и D по методике, изложенной в конце подраздела 2.3, с использованием приема поиска сопряженных подгрупп 6-го порядка для голоморфа $H(D_3)$, найдем группы $\{0, 1', 8', M\}$ и $\{0, 3', 7', L\}$. Подробно: из табл. 2.65 находим подстановки $K = (RZ)(SO)(UT)$ и $D = (Z\Gamma OU)$, тогда $0 \rightarrow 0, 0 \rightarrow 0$ и далее автоматически:

$$2' = (ZO) \rightarrow (RS) = 1', \quad 4' = (RT)(SU) \rightarrow (ZU)(OT) = 8',$$

$$2' = (ZO) \rightarrow (TU) = 3', \quad 4' = (RT)(SU) \rightarrow (RO)(SZ) = 7',$$

$$N = (RT)(SU)(ZO) \rightarrow (ZU)(OT)(RS) = M,$$

$$N = (RT)(SU)(ZO) \rightarrow (RO)(SZ)(TU) = L.$$

Второй способ, наоборот, связан с нормальными делителями, и он нам тоже, в основном, известен: аналогичным образом мы искали систему гомоморфных проекций для голоморфа $H(D_3)/N_1$ и т.д. Очень несложно определить *нормальный делитель* группы $S[D_4^5] \approx O_d$ второго порядка — $\{0, 0'\}$. Далее, ищем все *классы смежности* по этому делителю, т.е. *систему гомоморфных проекций*:

$$\begin{aligned} \{0, 0'\} &\rightarrow 0, & \{1, 2'\} &\rightarrow 1, & \{2, 1'\} &\rightarrow 2, & \{3, 3'\} &\rightarrow 3, & \{4, 1'\} &\rightarrow 4, \\ \{5, K'\} &\rightarrow 5, & \{6, G'\} &\rightarrow 6, & \{7, H'\} &\rightarrow 7, & \{8, J'\} &\rightarrow 8, & \{9, I'\} &\rightarrow 9, \\ \{A, M'\} &\rightarrow A, & \{B, N'\} &\rightarrow B, & \{C, F'\} &\rightarrow C, & \{D, E'\} &\rightarrow D, & \{E, A'\} &\rightarrow E, \\ \{F, B'\} &\rightarrow F, & \{G, D'\} &\rightarrow G, & \{H, C'\} &\rightarrow H, & \{I, 8'\} &\rightarrow I, & \{J, 4'\} &\rightarrow J, \\ \{K, 7'\} &\rightarrow K, & \{L, 6'\} &\rightarrow L, & \{M, 9'\} &\rightarrow M, & \{N, 5'\} &\rightarrow N. \end{aligned}$$

Таблица 2.66

Матрицы преобразования декартовых координат группы O_d							
0	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	C	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$	0'	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$	C'	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$
1	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$	D	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$	1'	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	D'	$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
2	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$	E	$\begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$	2'	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	E'	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}$
3	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	F	$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$	3'	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	F'	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$
4	$\begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}$	G	$\begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	4'	$\begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$	G'	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$
5	$\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$	H	$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	5'	$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$	H'	$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}$
6	$\begin{pmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$	I	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$	6'	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	I'	$\begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$
7	$\begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}$	J	$\begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$	7'	$\begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	J'	$\begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$
8	$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix}$	K	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$	8'	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$	K'	$\begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$
9	$\begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$	L	$\begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$	9'	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$	L'	$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix}$
A	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$	M	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$	A'	$\begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$	M'	$\begin{pmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$
B	$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$	N	$\begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$	B'	$\begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$	N'	$\begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix}$

Затем, по известным группам 2-го порядка (их количество определяется числом подстановок на транспозициях, которые берутся непосредственно из табл. 2.65) ищем группы 4-го порядка по схеме:

$$\{0, 1\} \rightarrow \{0, 0', 1, 2'\}, \{0, 2\} \rightarrow \{0, 0', 2, 1'\}, \dots, \{0, N\} \rightarrow \{0, 0', 5', N\}.$$

По известным подгруппам 3-го порядка находим неизвестные подгруппы 6-го порядка или по подгруппам 4-го порядка ищем подгруппы 8-го порядка и т.д.:

$$\{0, 8, 9\} \rightarrow \{0, 8, 9, 0', 1', 2'\}, \{0, 3, L, K\} \rightarrow \{0, 3, K, L, 0', 3', 6', 7'\}, \dots$$

Точно таким же образом находим смежные классы по другим инвариантным подгруппам, в частности, по нормальному делителю $\{0, 1, 2, 3\}$ найдем все 12 проекций:

$$\begin{aligned} \{0, 1, 2, 3\} &\rightarrow 0, \{0', 1', 2', 3'\} \rightarrow 0', \{E, F, J, N\} \rightarrow E, \{C, D, I, M\} \rightarrow C, \\ \{4, 7, 8, A\} &\rightarrow 4, \{4', 5', A', B'\} \rightarrow 4', \{G, H, K, L\} \rightarrow G, \{G', I', K', M'\} \rightarrow G', \\ \{5, 6, 9, B\} &\rightarrow 5, \{6', 7', C', D'\} \rightarrow 6', \{8', 9', E', F'\} \rightarrow 8', \{H', J', L', N'\} \rightarrow H'. \end{aligned}$$

По известным подгруппам 2-го порядка сразу найдем подгруппы 8-го порядка:

$$\{0, 0'\} \rightarrow \{0, 1, 2, 3, 0', 1', 2', 3'\}, \{0, 1\} \rightarrow \{0, 1, 2, 3, C, D, I, M\}, \dots$$

Таким образом, комбинируя оба изложенных способа, нам удалось отыскать 84 подгруппы полной группы симметрии куба O_d

$$\begin{aligned} &\{0, 0'\}, \{0, 1'\}, \{0, 2'\}, \{0, 3'\}, \{0, 4'\}, \{0, 5'\}, \{0, 6'\}, \{0, 7'\}, \{0, 8'\}, \{0, 9'\}, \{0, 1\}, \{0, 2\}, \\ &\{0, 3\}, \{0, 4\}, \{0, 5\}, \{0, 6\}, \{0, 7\}, \{0, 8\}, \{0, 9\}, \{0, A\}, \{0, B\}, \\ &\{0, 1, 1, N\}, \{0, 2, M, J\}, \{0, 3, L, K\}, \{0, 1, E, F\}, \{0, 2, C, D\}, \{0, 3, G, H\}, \\ &\{0, 1, 2, 3\}, \{0, 1, 1', 3'\}, \{0, 2, 2', 3'\}, \{0, 3, 1', 2'\}, \{0, 0', 1, 2'\}, \{0, 0', 2, 1'\}, \\ &\{0, 0', 3, 3'\}, \{0, 3', 6', K\}, \{0, 3', 7', L\}, \{0, 2', 5', J\}, \{0, 2', 4', N\}, \{0, 1', 8', M\}, \\ &\{0, 1', 9', I\}, \{0, 0', 8', I\}, \{0, 0', 4', J\}, \{0, 0', 5', N\}, \{0, 0', 6', L\}, \{0, 0', 7', K\}, \\ &\{0, 0', 9', M\}, \{0, 4, 5, 0', L', K'\}, \{0, 6, 7, 0', G', H'\}, \{0, 8, 9, 0', I', J'\}, \\ &\{0, A, B, 0', M', N'\}, \{0, 4, 5, K, M, N\}, \{0, 6, 7, I, J, K\}, \{0, 8, 9, J, L, M\}, \\ &\{0, A, B, 1, L, N\}, \{0, 4, 5, 5', 7', 9'\}, \{0, 6, 7, 4', 7', 8'\}, \{0, 8, 9, 4', 6', 9'\}, \\ &\{0, A, B, 5', 6', 8'\}, \{0, 1, 2, 3, 0', 1', 2', 3'\}, \{0, 1, 2, 3, 4', 5', A', B'\}, \\ &\{0, 1, 2, 3, 6', 7', C', D'\}, \{0, 1, 2, 3, 8', 9', E', F'\}, \{0, 1, 2, 3, C, D, I, M\}, \\ &\{0, 1, 2, 3, E, F, J, N\}, \{0, 1, 2, 3, G, H, K, L\}, \{0, 3, K, L, 0', 3', 6', 7'\}, \\ &\{0, 1, J, N, 0', 2', 4', 5'\}, \{0, 2, I, M, 0', 1', 8', 9'\}, \{0, 1, E, F, 0', 2', A', B'\}, \\ &\{0, 2, C, D, 0', 1', E', F'\}, \{0, 3, G, H, 0', 3', C', D'\}, \\ &\{0, 4, 5, K, M, N, 0', 5', 7', 9', K', L'\}, \{0, 6, 7, I, J, K, 0', 4', 7', 8', G', H'\}, \\ &\{0, 8, 9, J, L, M, 0', 4', 6', 9', I', J'\}, \{0, A, B, 1, L, N, 0', 5', 6', 8', M', N'\}, \\ &\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B\}, \{0, 1, 2, 3, G, H, K, L, 0', 1', 2', 3', 6', 7', C', D'\}, \\ &\{0, 1, 2, 3, E, F, J, N, 0', 1', 2', 3', 4', 5', A', B'\}, \\ &\{0, 1, 2, 3, C, D, I, M, 0', 1', 2', 3', 8', 9', E', F'\}, \\ &\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, G, H, I, J, K, L, M, N\}, \\ &\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, 0', 1', 2', 3', G', H', I', J', K', L', M', N'\}, \\ &\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, 4', 5', 6', 7', 8', 9', A', B', C', D', E', F'\}. \end{aligned}$$

Итак, нами были рассмотрены все 14 групп 16-го порядка. Осталось сделать последний небольшой шаг — составить метарешетку M_{16} . Несложный анализ графических изображений всех 14 решеток дает результат, который представлен на рис. 2.26 (числа рядом с обозначениями решеток указывают количество узлов на уровнях).

Однако мы не станем останавливаться на достигнутом, а пойдем дальше. За простой циклической группой C_{17} идут пять групп 18-го порядка. Как выглядят их метарешетка M_{18} ? Анализ будем проводить по сокращенной программе: без поиска групп симметрии решеток. Верхнеполюсной является решетка, постро-

енная от группы, которую мы обозначим как D_{18}^2 . Ее образующими являются —

$$a = (012)(345),$$

$$b = (02)(35), \quad c = (12)(34).$$

Тогда главными определяющими соотношениями будут —

$$ab = ba^2 = (01)(34),$$

$$ac = ca^2 = (02)(45),$$

$$bcb = cbc = (01)(45),$$

$$a^2b = ba = (12)(45),$$

$$a^2c = ca = (12)(45),$$

$$abcb = bcha^2 = (12)(35).$$

Решетка $S(D_{18}^2)$ изображена на рис. 2.27. Ее подгруппы —

$$\begin{aligned} D_{18}^2: & 1 = \{e, c\}, 2 = \{e, ac\}, 3 = \{e, a^2c\}, 4 = \{e, bc\}, 5 = \{e, b^2c\}, 6 = \{e, abc\}, \\ & 7 = \{e, a^2bc\}, 8 = \{e, ab^2c\}, 9 = \{e, a^2b^2c\}, A = \{e, a, a^2, c, ac, a^2c\}, \\ & B = \{e, a, a^2, a^2bc, abc, bc\}, C = \{e, a, a^2, ab^2c, a^2b^2c, b^2c\}, \\ & D = \{e, b, b^2, c, bc, b^2c\}, E = \{e, b, b^2, abc, ab^2c, ac\}, \\ & F = \{e, b, b^2, a^2c, a^2b^2c, a^2bc\}, G = \{e, a^2b, ab^2, c, a^2bc, ab^2c\}, \\ & H = \{e, a^2b, ab^2, ac, bc, a^2b^2c\}, I = \{e, a^2b, ab^2, a^2c, b^2c, abc\}, \\ & J = \{e, ab, a^2b^2, c, a^2b^2c, abc\}, K = \{e, ab, a^2b^2, ac, b^2c, a^2bc\}, \\ & L = \{e, ab, a^2b^2, a^2c, ab^2c, bc\}, M = \{e, a, a^2\}, N = \{e, b, b^2\}, \\ & O = \{e, a^2b, ab^2\}, P = \{e, ab, a^2b^2\}, Q = \{e, a, a^2, b, b^2, ab, a^2b^2, a^2b, ab^2\}. \end{aligned}$$

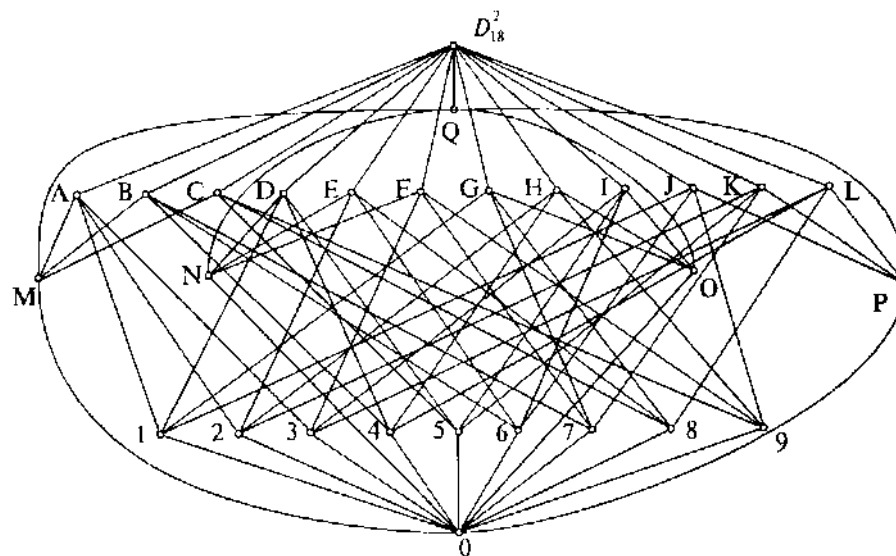


Рис. 2.27

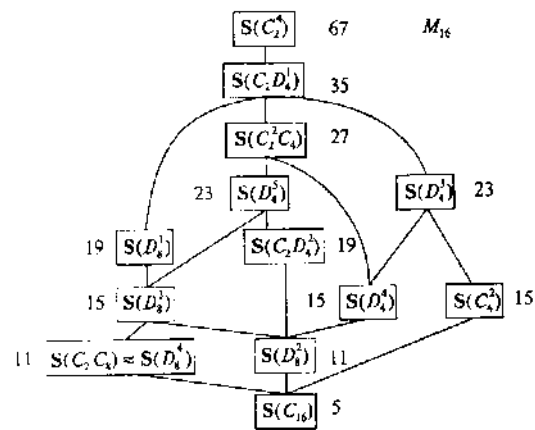


Рис. 2.26

Группу C_3D_3 можно получить либо на трех образующих $a = (012)$, $b = (02)$, $c = (345)$, либо на двух: $a = (012345)$, $b = (024)$. Решетка $S(C_3D_3)$ сохраняет от решетки $S(D_{18}^2)$ следующие узлы: $\{1, 2, 3, A, D, E, F, M, N, P, O, Q\}$. Решетка от группы диэдра $S(D_9^1)$ образована узлами $\{1, 2, 3, 4, 5, 6, 7, 8, 9, D, E, F, N, Q\}$, а две инверсных решетки $S(C_3C_6)$ и $S(C_2C_9)$ — соответственно узлами $\{5, C, D, I, K, M, N, O, P, Q\}$ и $\{5, D, N, Q\}$. Последняя решетка является нижнеполюсной ($C_2C_9 \approx C_{18}$). Метарешетка M_{18} изображена на рис. 2.28. Аналогичная метарешетка получается на решетках от групп 20-го порядка (рис. 2.29). Число рядом с обозначениями решеток указывает на количество узлов на уровнях. Верхним полюсом M_{20} является решетка $S(D_{10}^1)$ (рис. 2.30).

$$D_{10}^1: \begin{aligned} 1 &= \{e, b\}, 2 = \{e, a^5b\}, 3 = \{e, a^6b\}, 4 = \{e, ab\}, 5 = \{e, a^2b\}, \\ 6 &= \{e, a^5\}, 7 = \{e, a^7b\}, 8 = \{e, a^8b\}, 9 = \{e, a^3b\}, A = \{e, a^4b\}, \\ B &= \{e, a^9b\}, C = \{e, a^5, b, a^5b\}, D = \{e, a^5, ab, a^6b\}, E = \{e, a^5, a^2b, a^7b\}, \\ I &= \{e, a^2, a^4, a^6, a^8, b, a^2b, a^4b, a^6b, a^8b\}, F = \{e, a^5, a^3b, a^8b\}, \\ J &= \{e, a^2, a^4, a^6, a^8, ab, a^3b, a^5b, a^7b, a^9b\}, G = \{e, a^5, a^4b, a^9b\}, \\ K &= \{e, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9\}, H = \{e, a^2, a^4, a^6, a^8\}. \end{aligned}$$

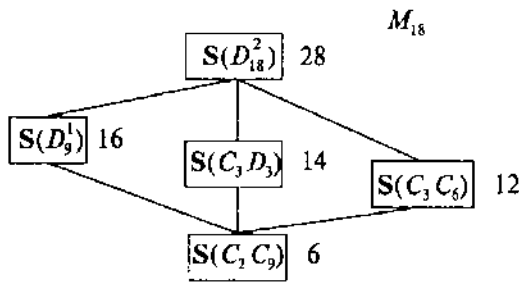


Рис. 2.28

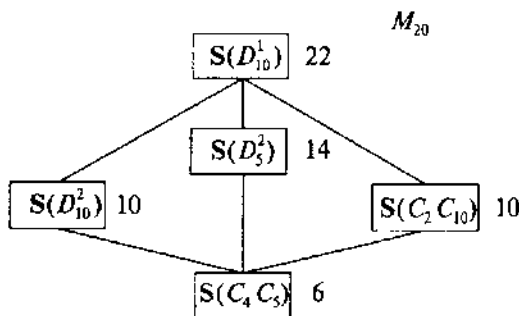


Рис. 2.29

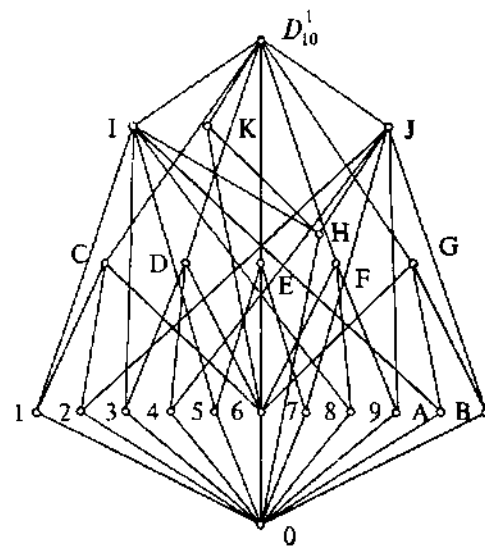


Рис. 2.30

Решетка $S(D_{10}^2)$ сохраняет узлы $\{6, C, D, E, F, G, H, K\}$, решетка $S(D_5^2) = \{1, 3, 5, 8, A, C, D, E, F, G, H, I\}$, инверсные решетки $S(C_2C_{10}) = \{1, 2, 6, C, H, I, J, K\}$ и $S(C_4C_5) = \{6, C, H, K\}$. Опре-

деляющие соотношения группы D_5^2 можно найти в конце четвертого раздела. Следует также напомнить, что для групп 20-го порядка имеют место изоморфизмы (табл. 2.28):

$$C_2 C_{10} \approx C_2^2 C_5, \quad C_4 C_5 \approx C_{20}, \quad C_2 D_5^1 \approx D_{10}^1.$$

По понятным причинам пропускаем группы 21-го, 22-го, 23-го порядков и переходим к анализу групп 24-го порядка. Верхним полюсом метарешетки M_{24} из 12 правильных решеток является $C_2 D_6^2 \approx C_2^2 D_3$ с образующими —

$$a = (012), \quad b = (02), \quad c = (34), \quad d = (56).$$

Если элементы группы $C_2^2 D_3$ обозначить через —

$$\begin{aligned} 0 = e, \quad 1 = a, \quad 2 = a^2, \quad 3 = b, \quad 4 = ab, \quad 5 = a^2 b, \\ 6 = c, \quad 7 = ac, \quad 8 = a^2 c, \quad 9 = bc, \quad A = abc, \quad B = a^2 bc, \\ C = d, \quad D = ad, \quad E = a^2 d, \quad F = bd, \quad G = abd, \quad H = a^2 bd, \\ I = cd, \quad J = acd, \quad K = a^2 cd, \quad L = bcd, \quad M = abcd, \quad N = a^2 bcd, \end{aligned}$$

то подгруппы для построения решетки $S(C_2^2 D_3)$ будут такими:

$$\begin{aligned} \{0, 3\}, \{0, 4\}, \{0, 5\}, \{0, 6\}, \{0, 9\}, \{0, A\}, \{0, B\}, \{0, C\}, \{0, F\}, \\ \{0, G\}, \{0, H\}, \{0, I\}, \{0, L\}, \{0, M\}, \{0, N\}, \{0, 1, 2\}, \{0, 3, 6, 9\}, \\ \{0, 4, 6, A\}, \{0, 5, 6, B\}, \{0, C, 6, I\}, \{0, 3, C, F\}, \{0, 4, C, G\}, \\ \{0, 5, C, H\}, \{0, 3, I, L\}, \{0, 4, I, M\}, \{0, 5, I, N\}, \{0, 9, I, F\}, \\ \{0, A, I, G\}, \{0, B, I, H\}, \{0, 9, C, L\}, \{0, A, C, M\}, \{0, B, C, N\}, \\ \{0, F, 6, L\}, \{0, G, 6, M\}, \{0, H, 6, N\}, \{0, 1, 2, 3, 4, 5\}, \\ \{0, 1, 2, 6, 7, 8\}, \{0, 1, 2, 9, A, B\}, \{0, 1, 2, C, D, E\}, \{0, 1, 2, I, J, K\}, \\ \{0, 1, 2, L, M, N\}, \{0, 6, C, I, 3, 9, F, L\}, \{0, 6, C, I, 4, A, G, M\}, \\ \{0, 6, C, I, 5, B, H, N\}, \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B\}, \\ \{0, 1, 2, 3, 4, 5, C, D, E, F, G, H\}, \{0, 1, 2, 3, 4, 5, I, J, K, L, M, N\}, \\ \{0, 1, 2, 6, 7, 8, C, D, E, I, J, K\}, \{0, 1, 2, 6, 7, 8, F, G, H, L, M, N\}, \\ \{0, 1, 2, 9, A, B, F, G, H, I, J, K\}, \{0, 1, 2, 9, A, B, C, D, E, L, M, N\}. \end{aligned}$$

Нет смысла анализировать многие решетки от группы 24-го порядка, так как их геометрия вполне понятна. Например, решетка $S(D_{12}^1)$ является простым расширением решетки $S(D_6^1)$. В самом деле, следующие 15 подгрупп D_{12}^1 образуют решетку $S(D_6^1)$ (рис. 2.18):

$$\begin{aligned} 0 = \{e, a^6\}, \quad 2 = \{e, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}\}, \\ 1 = \{e, a^3, a^6, a^9\}, \quad 3 = \{e, a^2, a^4, a^6, a^8, a^{10}\}, \quad 9 = \{e, a^6, a^4 b, a^{10} b\}, \\ 4 = \{e, a^3, a^6, a^9, ab, a^4 b, a^7 b, a^{10} b\}, \quad A = \{e, a^6, ab, a^7 b\}, \\ 5 = \{e, a^3, a^6, a^9, a^2 b, a^5 b, a^8 b, a^{11} b\}, \quad B = \{e, a^6, a^5 b, a^{11} b\}, \\ 6 = \{e, a^3, a^6, a^9, b, a^3 b, a^6 b, a^9 b\}, \quad C = \{e, a^6, a^2 b, a^8 b\}, \\ 7 = \{e, a^2, a^4, a^6, a^8, a^{10}, b, a^2 b, a^4 b, a^6 b, a^8 b, a^{10} b\}, \quad D = \{e, a^6, b, a^6 b\}, \\ 8 = \{e, a^2, a^4, a^6, a^8, a^{10}, ab, a^3 b, a^5 b, a^7 b, a^9 b, a^{11} b\}, \quad E = \{e, a^6, a^3 b, a^9 b\}. \end{aligned}$$

Таким образом, $S(D_6^1)$ является верхней частью решетки $S(D_{12}^1)$, и вообще

$$S(D_3^1) \subset S(D_6^1) \subset S(D_{12}^1) \subset \dots$$

Далее опишем новую для нас (с точки зрения определяющих соотношений) группу D_6^3 с образующими —

$$a = (012345)(6AEKLC)(7BFJMN)(8DGH19), \\ b = (0678)(19BC)(21FI)(3HJK)(4EMG)(5DNA),$$

и соотношениями —

$$ab = b^3a^5, \quad a^5b = b^3a, \quad a^3b^3 = ba^3, \quad a^2b = ba^4, \quad a^5b^2 = b^2a^5, \\ a^5b^3 = ba, \quad ab^3 = ba^5, \quad a^3b = b^3a^3, \quad a^4b = ba^2, \quad a^3b^2 = b^2a^3.$$

Если элементы группы D_6^3 обозначить через —

$$0 = e, \quad 1 = a, \quad 2 = a^2, \quad 3 = a^3, \quad 4 = a^4, \quad 5 = a^5, \\ 6 = b, \quad 7 = b^2, \quad 8 = b^3, \quad 9 = ab, \quad A = ba, \quad B = ab^2, \\ C = ab^3, \quad D = a^5b, \quad E = a^4b, \quad F = a^2b^2, \quad G = a^4b^3, \quad H = a^3b, \\ I = a^2b^3, \quad J = a^3b^2, \quad K = a^3b^3, \quad L = a^2b, \quad M = a^4b^2, \quad N = a^5b^2,$$

то подгруппы для построения решетки $S(D_6^3)$ будут такими:

$$\{0, 3\}, \{0, 7\}, \{0, 9\}, \{0, A\}, \{0, C\}, \{0, D\}, \{0, H\}, \{0, J\}, \{0, K\}, \{0, 1, 2\}; \\ \{0, 6, 7, 8\}, \{0, E, 7, G\}, \{0, I, 7, L\}, \{0, 7, C, 9\}, \{0, 7, H, K\}, \{0, 7, A, D\}, \\ \{0, 7, 3, J\}, \{0, 1, 2, 3, 4, 5\}, \{0, 2, 4, B, J, N\}, \{0, 2, 4, 7, F, M\}, \\ \{0, 2, 4, A, C, K\}, \{0, 2, 4, 9, H, D\}, \{0, 3, 6, 7, 8, H, J, K\}, \{0, 3, 7, 9, C, E, G, J\}, \\ \{0, 3, 7, A, D, I, J, L\}, \{0, 1, 2, 3, 4, 5, 7, B, F, J, M, N\}, \\ \{0, 2, 4, 7, 9, A, C, D, F, H, K, M\}, \{0, 2, 4, 6, 7, 8, F, G, E, I, L, M\}.$$

Весьма свособразной является группа с образующими —

$$a = (0AK68I4EG2CM)(1JD7HB5N93LF), \\ b = (01234567)(89ABCDEFG)(GHIJKLMN)$$

и определяющими соотношениями —

$$ab = a^7b^5 = ba^5 = b^3a^8 = b^5a^{11}, \quad ab^5 = a^{11}b^5 = ba = b^3a^4 = b^5a^7, \\ ab^3 = a^7b^7 = ba^2 = b^3a^5 = b^5a^8, \quad ab^7 = a^4b = b^3a^{11} = b^5a^2 \text{ и т.д.}$$

Группу D_{12}^3 можно представить матрицами 2×2 с элементами по mod (3):

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix}, \\ \begin{pmatrix} 2 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}, \\ \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}.$$

Если считать матрицы —

$$\begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ и т.д.}$$

недопустимыми, то общее число *допустимых* матриц рассматриваемого типа равно 48 и они образуют группу. Эта группа не изоморфна полной группе куба O_8 , хотя бы потому, что D_{12}^3 является у нее нормальным делителем (как известно,

у группы O_d нет подгрупп D_{12}^3). Решетка $S(D_{12}^4)$ содержит всего 8 узлов, так как D_{12}^3 имеет по одной подгруппе 2-го, 3-го, 4-го, 6-го и 12-го порядка и три подгруппы 8-го порядка. Остальные решетки, входящие в метарешетку M_{24} ничего примечательного не представляют. В табл. 2.67 содержится информация об узлах и связях как правильных, так и неправильных решеток от групп 24-го порядка.

Таблица 2.67

Узлы и связи решеток	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Верхнеполюсные связи	10	6	8	6	6	4	6	6	4	4	4	2	8	6	5
Отходящие связи	1	1	1	1	1	1	1	1	1	1	1	1	1	1	—
Узлы 12-го порядка	7	3	7	3	3	3	3	3	3	3	1	1	1	1	—
Приходящие связи	4	2, 6	4	4, 6	2, 4, 6	2, 4	4	2, 4	2, 4	2	2	2	5	5	—
Отходящие связи	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Узлы 8-го порядка	3	3	1	3	3	1	3	3	1	1	3	1	3	1	1
Приходящие связи	7	3	7	3	3	3	3	3	3	3	1	1	3	7	3
Отходящие связи	3	1, 3	3	1, 3	1, 3	1, 3	1, 3	3	1, 3	3	1	1	1	1	1
Узлы 6-го порядка	7	5	7	5	3	5	3	1	3	1	1	1	4	4	4
Приходящие связи	2, 4	2, 4	2	2, 4	2, 4	2	2	2	2	2	2	2	4	2	2
Отходящие связи	2, 4	2, 4	2	2, 4	2, 4	2	2, 4	2, 4	2, 4	2	4	2	1, 4	1, 2	1
Узлы 4-го порядка	19	7	7	7	7	3	7	7	3	3	1	1	7	7	3
Приходящие связи	3	1, 3	3	1, 3	1, 3	3	1, 3	1	1, 3	1	1	1	1, 3	3	1
Отходящие связи	7	5	7	5	3	5	3	1	3	1	1	1	2	2	1
Узлы 3-го порядка	1	1	1	1	1	1	1	1	1	1	1	1	4	4	4
Приходящие связи	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Отходящие связи	4, 8	2, 8	4	2, 8	2, 8	2, 4	2, 8	8	2, 4	4	2	2	3	3, 7	7
Узлы 2-го порядка	15	13	7	9	7	5	3	1	3	1	1	1	9	7	1
Нижнеполюсные связи	16	14	8	10	8	6	4	2	4	2	2	2	13	11	5
Общее количество узлов	52	32	30	28	24	18	18	16	14	10	8	6	28	24	13

В заголовке табл. 2.67 решеткам присвоены следующие позиции:

$$\begin{aligned}
 1 - S(C_2^2 D_3), \quad 2 - S(D_{12}^1), \quad 3 - S(C_2^2 C_6), \quad 4 - S(D_6^3), \quad 5 - S(C_4 D_3), \\
 6 - S(C_3 D_4^1), \quad 7 - S(C_2 D_6^2), \quad 8 - S(D_{12}^2), \quad 9 - S(C_2 C_{12}), \quad 10 - S(C_3 D_4^2), \\
 11 - S(D_{12}^3), \quad 12 - S(C_{24}), \quad 13 - S(T_d), \quad 14 - S(C_2 T_3), \quad 15 - S(T_6).
 \end{aligned}$$

Все связи условно подделены на «отходящие» (идущие от узла вверх) и «приходящие» (подходящие к узлу снизу). Если в ячейке стоят два числа, например 2, 4; это значит, что от одной части узлов отходят 2 связи, а от другой — 4 связи. Общее количество узлов дается без учета полюсов. На рис. 2.31 приведено графическое изображение метарешетки M_{24} , которое показывает иерархию всех 12 правильных решеток, построенных на базе группы 24-го порядка.

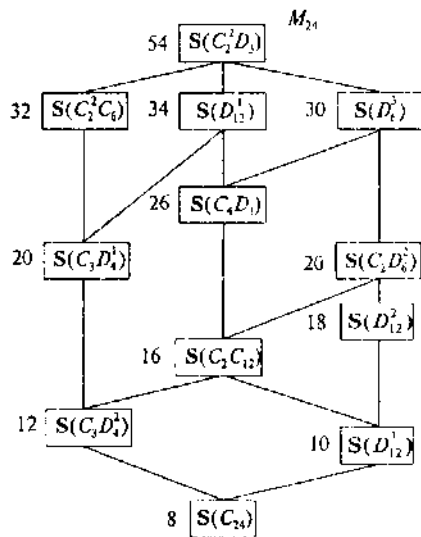


Рис. 2.31

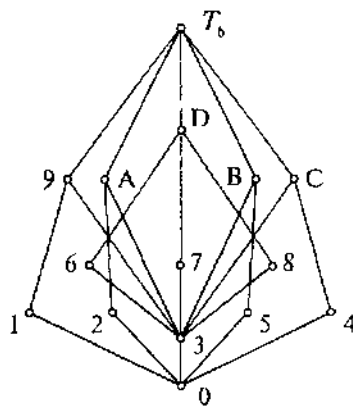


Рис. 2.32

Анализ неправильных решеток начнем структурой подгрупп группы T_6 , которая самым очевидным образом связана со структурой группы тетраэдра $T_3 = T$. Образующими элементами для T_6 являются —

$$a = (012345)(6789AB)(CDEFGH)(IJKLMN),$$

$$b = (08J3BM)(1G74DA)(2NF5KC)(GEL9HI);$$

определяющими соотношениями —

$$a^2 b = a^3 b^4 = b^2 a^4 = b^5 a, \quad b^4 a = b a^4,$$

$$ab^2 = a^4 b^5 = b a^5 = b^4 a^2,$$

$$a^5 b = a^2 b^4 = b^2 a = b^5 a^4,$$

$$a^4 b^2 = ab^5 = b a^2 = b^4 a^5, \quad a^4 b = ab^4,$$

$$aba = bab = a^2 b^2 a^2 = a^5 b^2 a^5 = b^2 a^2 b^2 = b^5 a^2 b^5 =$$

$$= a^4 b a^4 = b^4 a b^4,$$

$$a^5 b^5 a^5 = b^5 a^5 b^5 = a^4 b^4 a^4 = ab^4 a = b^4 a^4 b^4 =$$

$$= ba^4 b = a^2 b^5 a^2 = b^2 a^5 b^2.$$

Решетка $S(T_6)$ изображена на рис. 2.32. Ее структура является *надрешеткой* $S(T_3)$ (рис. 2.20) и одновременно *подрешеткой* $S(C_2 T_3)$, которая изображена на рис. 2.33. Выпишем подгруппы T_6 и $C_2 T_3$, используя общие символы для соответствующих узлов —

$$T_6: \quad 1 = \{e, a^2, a^4\}, \quad 2 = \{e, a^2 b^5, b a^4\}, \quad 3 = \{e, a^3\},$$

$$4 = \{e, ab^4, b^2 a^5\}, \quad 5 = \{e, b^2, b^4\},$$

$$6 = \{e, aba, a^3, ab^4 a\}, \quad 7 = \{e, a^5 b, a^3, a^2 b\},$$

$$8 = \{e, ab^2, a^3, ab^5\}, \quad 9 = \{e, a, a^2, a^3, a^4, a^5\},$$

$$B = \{e, b, b^2, b^3, b^4, b^5\},$$

$$A = \{e, ba, a^3, ba^4, a^2 b^2, a^2 b^5\},$$

$$C = \{e, ab, b^3, ab^4, b^2 a^2, b^2 a^5\},$$

$$D = \{e, aba, a^3, a^5 b^5 a^5, a^5 b, a^2 b, ab^2, ab^5\}.$$

$$C_2 T_3: \quad 1 = \{e, a, a^2\}, \quad 2 = \{e, b, b^2\}, \quad 3 = \{e, c\}, \quad 4 = \{e, a^2 b, b^2 a\},$$

$$5 = \{e, ab^2, ba^2\}, \quad 6 = \{e, ab, c, abc\}, \quad 7 = \{e, ba, c, bac\},$$

$$8 = \{e, a^2 ba^2, c, a^2 ba^2 c\}, \quad E = \{e, ab\}, \quad J = \{e, bac\}, \quad I = \{e, abc\},$$

$$9 = \{e, a, a^2, c, ac, a^2 c\}, \quad F = \{e, ba\}, \quad C = \{e, ab^2, ba^2, c, ab^2 c, ba^2 c\},$$

$$A = \{e, b, b^2, c, bc, b^2 c\}, \quad G = \{e, a^2 ba^2\}, \quad H = \{e, a^2 ba^2 c\},$$

$$B = \{e, a^2 b, b^2 a, c, a^2 bc, b^2 ac\}, \quad K = \{e, ba, abc, a^2 ba^2 c\},$$

$$D = \{e, ab, ba, a^2 ba^2, c, abc, bac, a^2 ba^2 c\}, \quad L = \{e, a^2 ba^2, bac, abc\},$$

$$M = \{e, ab, bac, a^2 ba^2 c\}, \quad N = \{e, ab, ba, a^2 ba^2\},$$

$$P = \{e, a, a^2, b, b^2, ab, ba, a^2 b, b^2 a, ab^2, ba^2, a^2 ba^2\}.$$

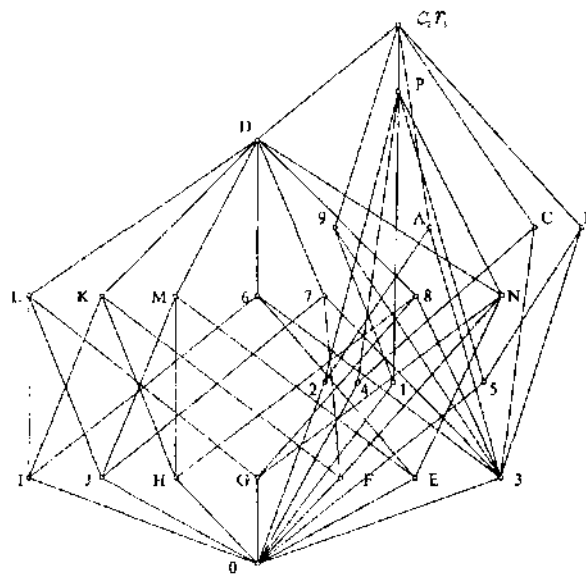


Рис. 2.33

Если решетки $S(C_2 T_3)$ и $S(T_6)$ являются верхним и нижним полюсами одной метарешетки, то третья неправильная решетка $S(T_d)$ никак не связана с другими решетками от групп 24-го порядка. Ее 28 подгрупп приведены в списке 84 подгрупп для группы O_d (там необходимо выбрать те подмножества, куда не входят штрихованные символы).

Интересен и сравнительный анализ структур. Например, три решетки от коммутативных групп 40-го порядка —

$$C_{40} \approx C_5 C_8, \quad C_2 C_{20} \approx C_4 C_{10} \approx C_2 C_4 C_5, \quad C_2^2 C_{10} \approx C_2^3 C_5$$

с графической точки зрения полностью совпадают с решетками от групп C_{24} , $C_2 C_{12}$ и $C_2^2 C_6$. Очень схожи решетки $S(C_2^2 D_3)$ и $S(C_2^2 D_5)$ (несмотря на то, что первая насчитывает 52 узла, а вторая 74), $S(C_2 D_6^3)$ и $S(C_2 D_{10}^2)$ (число узлов соответственно 18 и 26), $S(C_4 D_3)$ и $S(C_4 D_5^1)$ (24 и 34) и т.д. Хотя для правильной решетки $S(C_2 D_5^2)$ от группы 40-го порядка уже нельзя найти аналога среди решеток от групп 24-го порядка.

Мы знаем, сколь важную роль играют делители чисел. Схожесть разложений двух чисел:

$$24 = 2 \times 2 \times 2 \times 3, \quad 40 = 2 \times 2 \times 2 \times 5$$

обеспечивает и определенную схожесть в структурах для групп соответствующих порядков. Однако здесь нужно иметь в виду следующее обстоятельство. При последовательном возведении в степень подстановки a , представляющей из себя 12-цикл, возникают еще три подстановки аналогичной периодичности — a^{11} , a^7 и a^5 . Отсюда можно пытаться найти три группы 24-го порядка с определяющими соотношениями:

$$ab = ba^{11}, \quad ab = ba^7, \quad ab = ba^5.$$

Но для подстановки a , представляющей из себя 20-цикл, существует уже семь таких композиций:

$$ab = ba^{19}, ab = ba^{17}, ab = ba^{13}, ab = ba^{11}, ab = ba^9, ab = ba^7, ab = ba^5.$$

Таким образом, число групп 40-го порядка будет заметно больше, чем групп 24-го порядка. Тем не менее, сравнительный анализ дает многое в понимании строения групп.

Свой морфологический анализ мы закончим группами 27-го порядка ($27 = 3 \times 3 \times 3$) с тем, чтобы можно было решетки от этих групп сравнить с решетками от групп 8-го порядка ($8 = 2 \times 2 \times 2$). Подгруппы верхнеполюсной группы —

$$\begin{aligned} C_3^3: \quad 1 &= \{e, b, b^2\}, 2 = \{e, ab, a^2b^2\}, 3 = \{e, a^2b, ab^2\}, 4 = \{e, c, c^2\}, 5 = \{e, ac, a^2c^2\}, \\ 6 &= \{e, a^2c, ac^2\}, 7 = \{e, a, a^2\}, 8 = \{e, b^2c, bc^2\}, 9 = \{e, abc^2, a^2b^2c\}, \\ A &= \{e, a^2bc^2, ab^2c\}, B = \{e, bc, b^2c^2\}, C = \{e, a^2bc, ab^2c^2\}, \\ D &= \{e, abc, a^2b^2c^2\}, E = \{e, b, b^2, bc, b^2c^2, c, c^2, b^2c, bc^2\}, \\ F &= \{e, ab, a^2b^2, ab^2c^2, a^2c^2, ac, bc^2, b^2c, a^2bc\}, \\ G &= \{e, a, a^2, ab, a^2b^2, b, b^2, a^2b, ab^2\}, \\ H &= \{e, a^2b, ab^2, a^2bc, ab^2c^2, c, c^2, a^2bc^2, ab^2c\}, \\ I &= \{e, a^2c, ac^2, a^2b, ab^2, b^2c, bc^2, abc, a^2b^2c^2\}, \\ J &= \{e, a, a^2, ac, a^2c^2, c, c^2, a^2c, ac^2\}, \\ K &= \{e, a^2c, ac^2, a^2bc, ab^2c^2, b, b^2, abc^2, a^2b^2c\}, \\ L &= \{e, b^2c, bc^2, ab^2c, a^2bc^2, a, a^2, a^2b^2c, abc^2\}, \\ M &= \{e, ac, a^2c^2, abc, a^2b^2c^2, b, b^2, a^2bc^2, ab^2c\}, \\ N &= \{e, bc, b^2c^2, a^2bc^2, ab, a^2b^2, ac^2, a^2c, ab^2c\}, \\ O &= \{e, bc, b^2c^2, abc, a^2b^2c^2, a, a^2, ab^2c^2, a^2bc\}, \\ P &= \{e, ab, a^2b^2, abc, a^2b^2c^2, c, c^2, abc^2, a^2b^2c\}, \\ Q &= \{e, ac, a^2c^2, abc^2, a^2b^2c, a^2b, ab^2, bc, b^2c^2\}. \end{aligned}$$

Решетка $S(C_3^3)$, изображенная на рис. 2.34, обладает *простой* группой симметрии $S[C_3^3]$, которая разбивается на восемь классов сопряженности. Общее число элементов в группе равно 5 928. По одному представителю от каждого класса и количество элементов в классе отражено в табл. 2.68.

Таблица 2.68

C_i	Подстановки из группы $S[C_3^3]$	Количество
C_0	{0}	1
C_1	(46)(8C)(9B)(AD)	117
C_2	(1)(5)(A)(D)(2C8)(39B)(476)	416
C_3	(5)(1AD)(263)(49C)(7B8)	624
C_4	(5)(13)(27)(486C)(9ABD)	702
C_5	(3)(5)(9B)(6D8)(1C7A24)	936
C_6	(5)(1237)(4A8B6DC9)	1 404
C_7	(14D5682A73CB9)	1 728

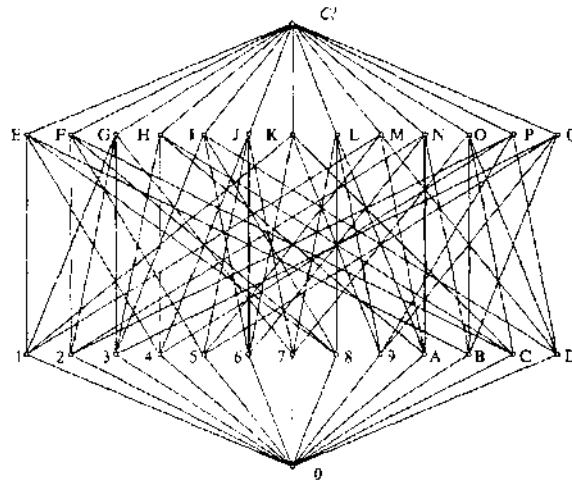


Рис. 2.34

Представители могут выполнять роль образующих элементов группы. Для группы $S[C_3^3]$ имеется 13 подгрупп 3-го порядка и такое же число подгрупп 9-го порядка, причем подгруппы четырежды связаны между собой отношением порядка, т.е. каждый узел решетки имеет четыре связи. Несложно подсчитать, что решетка $S(C_3^3)$ будет содержать 31 узел на одном уровне и на каждый узел будет приходиться уже 6 связей; далее, решетка $S(C_7^3)$ имеет 57 узлов на уровне и 8 связей на узел и т.д. Отсюда можно вывести две простых формулы для подсчета числа связей (M) и числа узлов (N) верхнеполюсных решеток типа $S(C_p^3)$ (p — простое число):

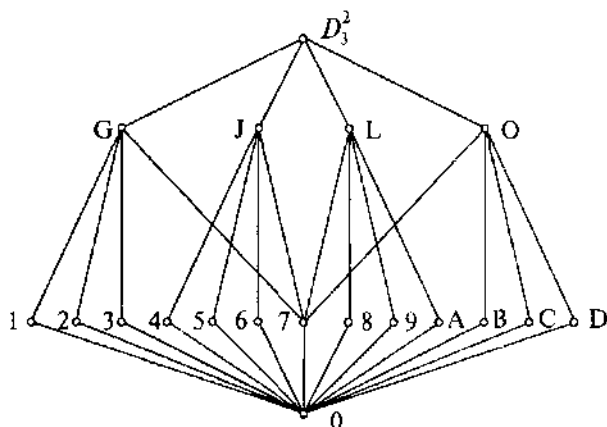
$$M = p + 1, \quad N = 3 \cdot p + (p - 1)^2.$$

Если взять две четные подстановки —

$$a = (012)(345)(678), \quad b = (034)(578)(126),$$

и перемножить всеми возможными способами, мы уже не получим *простой* группы, но возникшие при этом 27 подстановок заслуживают самого пристального внимания. Дело в том, что получившаяся группа D_3^2 , отдаленно напоминающая группу диэдра $D_3^1 \cong D_3$, обладает замечательным свойством — все ее подстановки представляют собой 3-циклы. Группа распадается на одиннадцать классов сопряженности и имеет следующие подгруппы, обозначенные в соответствии с узлами $S(C_3^3)$, —

$$\begin{aligned} D_3^2: \quad 1 &= \{e, a, a^2\}, \quad 2 = \{e, bab^2, ba^2b^2\}, \quad 3 = \{e, b^2ab, b^2a^2b\}, \quad 4 = \{e, b, b^2\}, \\ 5 &= \{e, ab^2a^2, aba^2\}, \quad 6 = \{e, a^2ba, a^2b^2a\}, \quad 7 = \{e, aba^2b^2, bab^2a^2\}, \quad 8 = \{e, ab, b^2a^2\}, \\ 9 &= \{e, ba, a^2b^2\}, \quad A = \{e, ab^2a, b^2ab^2\}, \quad B = \{e, a^2b, b^2a\}, \quad C = \{e, ba^2, ab^2\}, \\ D &= \{e, uba, hab\}, \quad G = \{e, aba^2b^2, bab^2a^2, a, a^2, hab^2, ba^2b^2, b^2ab, b^2a^2b\}, \\ J &= \{e, aba^2b^2, bab^2a^2, b, b^2, ab^2a^2, aba^2, a^2ba, a^2b^2a\}, \\ L &= \{e, aba^2b^2, bab^2a^2, ab, b^2a^2, ba, a^2b^2, ab^2a, b^2ab^2\}, \\ O &= \{e, aba^2b^2, bab^2a^2, a^2b, b^2a, ba^2, ab^2, aba, bab\}. \end{aligned}$$

[illegible]

Эти матрицы образуют нормальный делитель в группе 216-го порядка, состоящей из подобных треугольных матриц, у которых на главной диагонали 8 способами расположены элементы 1 и 2. Решетка $S(D_3^2)$ показана на рис. 2.35.

Две регулярные подстановки —

$$b = (091)(1AJ)(2BK)(3CL)(4DM)(5EN)(6FO)(7GP)(8HQ)$$

$$D_3^3: \quad ab = ba^7, \quad a^2b = ba^5, \quad a^3b = ba^3, \quad a^4b = ba, \quad a^5b = ba^8, \\ a^6b = ba^6, \quad a^7b = ba^4, \quad a^8b = ba^2, \quad ab^2 = b^2a^4, \quad a^2b^2 = b^2a^8, \\ a^3b^2 = b^2a^3, \quad a^4b^2 = b^2a^7, \quad a^5b^2 = b^2a^2, \quad a^6b^2 = b^2a^6, \quad a^7b^2 = b^2a.$$
$$\begin{aligned} I &= \{e, b, b^2\}, \quad 2 = \{e, a^3b, a^6b^2\}, \quad 3 = \{e, a^6b, a^3b^2\}, \\ 7 &= \{e, a^3, a^6\}, \quad G = \{e, a^3, a^6, b, b^2, a^3b, a^3b^2, a^6b, a^6b^2\}, \\ J &= \{e, a^3, a^6, ab, a^4b, a^7b, a^2b^2, a^5b^2, a^7b^2\}, \\ L &= \{e, a^3, a^6, a^2b, a^5b, a^8b, ab^2, a^4b^2, a^8b^2\}, \\ O &= \{e, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8\}, \end{aligned}$$

Страница 203

Группы являются краеугольным камнем *общей* или *абстрактной алгебры*. «Общей» или «абстрактной» алгебра называется потому, что ее объектами являются уже не конкретные «представления» (матрицы или подстановки), а *абстрактные символы*, для которых заранее вводятся определенные аксиомами операции. Не надо думать, что абстрактные символы к нам «падают с неба», их существование должно быть обеспечено наличием соответствующего представления. Если такового не находится, то убежденный конструктивист, ориентированный на содержательную математику, ко всяким манипуляциям с «пустыми» знаками должен отнестись с настороженностью. Если нам говорят, что $(a + b)^2 = a^2 + 2ab + b^2$, мы доверимся этому равенству в силу существования бесконечного множества конкретных равенств:

$$(2 + 3)^2 = 2^2 + 2 \cdot 2 \cdot 3 + 3^2 = 25, \quad (1 + 4)^2 = 1^2 + 2 \cdot 1 \cdot 4 + 4^2 = 25, \dots$$

Примеры с числами обуславливают действия с буквами, но никак не наоборот.

Абстрактная запись предоставляет нам определенные преимущества. Так, например, вместо индуктивного поиска выражения для разложения кубического бинома, мы могли бы воспользоваться общей формой записи чисел посредством букв, тем более, что, с точки зрения письма, нет никакой разницы между символами, скажем, a и 2, b и 3. Если взять значения $a = 2$, $b = 3$, затем $a = 1$, $b = 4$ и т.д., то вероятность, что при $a = 73$, $b = 152$ произойдет сбой и общая формула разложения квадратичного бинома окажется неверной, очень незначительна. С одной стороны, чтобы верить в сбой формулы при каком-то числовом значении буквы, нужно верить в чудеса, в сверхъестественную силу, которая бы нарушила монотонность числового ряда. С другой стороны, человек, отрицающий преимущества, которые предоставляет нам абстрактная (равно общая, алгебраическая) запись, поступает неразумно. Античный математик Диофант, живший в III столетии в Александрии, сначала тоже использовал только цифры, но потом его числовые выкладки разрослись настолько, что он просто вынужден был прибегнуть к буквам. Эта его невинная уловка позволила нынешним историкам математики присвоить ему почетное звание *первого алгебраиста мира*. Однако трудно поверить, что где-нибудь в Древнем Египте или Вавилоне кто-нибудь из математиков уже не сделал то же самое: этот естественный прием придет каждому в голову, когда дело имешь с большими числами.

В отношении получения принципиально новых знаний буквенная запись дает крайне мало. Она практически не способна выполнять функцию лопаты для откапывания истин. Единственное ее неоспоримое достоинство: убеждать

путем алгебраических выкладок справедливость уже обнаруженных математических соотношений. Продемонстрируем это на следующем примере. Известно, что группа S_2^3 коммутативна и для любого ее элемента выполняется равенство: $a^2 = e$. Этот тривиальный факт вытекает мгновенно, стоит нам мельком бросить взгляд на подстановки:

$$e = (0), \quad a = (01), \quad b = (23), \quad c = (45), \quad ab = (01)(23), \\ ac = (01)(45), \quad bc = (23)(45), \quad abc = (01)(23)(45).$$

И мы прекрасно знаем, что обратное утверждение ошибочно, т.е. из коммутативности группы $ab = ba$ вовсе не вытекает равенство $a^2 = e$ для любого элемента a . В этом мы убедились при рассмотрении самых элементарных групп, в частности, C_2C_4 :

$$e = (0), \quad a = (0123), \quad a^2 = (02)(13), \quad a^3 = (0321), \quad b = (45), \\ ab = (0123)(45), \quad a^2b = (02)(13)(45), \quad a^3b = (0321)(45).$$

Что же делает убежденный «формалист»? Он берется доказать, что для каждой группы, для которой имеет место равенство $a^2 = e$, будет выполняться коммутативный закон: $ab = ba$. Исходя из условий, абстрактно определяющих группу, он может провести свое доказательство по крайней мере двумя способами — а и б:

- | | |
|---------------------------------------|-----------------------------|
| а) 1. $(ab)c = a(bc),$ | б) 1. $(ab)c = a(bc),$ |
| 2. $ae = ea = a,$ | 2. $ae = ea = a,$ |
| 3. $aa^{-1} = a^{-1}a = e,$ | 3. $aa^{-1} = a^{-1}a = e,$ |
| 4. $aa = e.$ | 4. $aa = e.$ |
| 5. $ab = ba?$ | 5. $ab = ba?$ |
| 6. $abab = e,$ | 6. $abab = e,$ |
| 7. $ab = b^{-1}a^{-1},$ | 7. $aabb = e,$ |
| 8. $ab = bb^{-1}b^{-1}a^{-1}a^{-1}a,$ | 8. $abab = aabb,$ |
| 9. $ab = b(b^{-1})^2(a^{-1})^2a,$ | 9. $bab = abb,$ |
| 10. $ab = beea,$ | 10. $ba = ab,$ |
| 11. $ab = ba.$ | 11. $ab = ba.$ |

После представления этих выкладок, кто-то может попросить нашего формалиста столь же ловко доказать обратное, а именно, что из условия коммутативности $ab = ba$ вытекает равенство $a^2 = e$. У конструктивистов есть пример коммутативной группы C_2C_4 , показывающий, что $a^2 \neq e$. Но как обязан поступить последовательный формалист, у которого этого примера нет перед глазами? Он ведь должен, исходя из аксиом группы и общих алгебраических выкладок, показать возможность или невозможность этого утверждения. Мы уверены, что он никогда не подтвердит и не опровергнет это положение, поскольку для одних групп оно верно, а для других уже нет.

Между тем, коммутативные группы не представляют собой ничего такого, что может вызвать у нас затруднения. Сложнее обстоит дело с так называемыми *нильпотентными группами*, для которых справедливо тождество $a^m = e$, где $m > 2$. Одну из таких групп мы хорошо знаем, это D_3^2 с образующими:

$$a = (012)(345)(678), \quad b = (034)(578)(126).$$

которая состоит из 27 подстановок, представляющих собой 3-циклы; возведение в куб любого элемента этой группы даст e .

Для нильпотентных групп вводят понятие *коммутатора*, определяемого следующим образом:

$$[a, b] = a^{-1}b^{-1}ab = aba^{-1}b^{-1}.$$

Коммутатор равен e , если группа коммутативна, в общем же случае он равен некоему другому элементу группы. Так, для группы D_3^2 коммутатор, составленный из a и b , равен: $[a, b] = (065)(173)(284)$. Следовательно, коммутатор можно рассматривать как определенную на группе *метаоперацию*. Для любых коммутаторов справедливы следующие законы, которые проверяются прямой подстановкой:

$$\begin{aligned} [a, b][b, a] &= e, \quad [a, b]^{-1} = [b, a], \quad [a, b^{-1}] = b[b, a]b^{-1}, \\ [a^{-1}, b] &= a[b, a]a^{-1}, \quad [ab, c] = b^{-1}[a, c]b[b, c], \\ [a, bc] &= [a, c]c^{-1}[a, a]c. \end{aligned}$$

Но если группа нильпотентная, то для метаоперации выполняются законы ассоциативности, дистрибутивности и другие замечательные тождества:

$$\begin{aligned} [[a, b], c] &= [a, [b, c]], \quad [ab, c] = [a, c][b, c], \\ [a, bc] &= [a, b][a, c], \quad [a, b]^{-1} = [a^{-1}, b] = [a, b^{-1}], \quad [[a, b], b] = e, \dots \end{aligned}$$

Чтобы доказать любое из этих тождеств, конструктивисту не требуется больших интеллектуальных усилий, особенно если у него под рукой компьютер. Нильпотентная группа D_3^2 легко разбивается на одиннадцать классов эквивалентности и прямой подстановкой их представителей устанавливается справедливость любого тождества. Для алгебраиста-формалиста поиск доказательства подобных тождеств выливается в тяжелый и неблагодарный труд; никогда не знаешь, увенчаются ли твои поиски успехом или ты обречен на бесконечное манипулирование символами. Докажем в общем виде, для примера, что из равенства $a^3 = e$ вытекает равенство $[[a, b], b] = e$:

- | | |
|--------------------------------|---|
| 1. $(ab)c = a(bc)$, | 10. $aba = b^{-1}a^{-1}b^{-1}$, |
| 2. $ae = ea = a$ | 11. $abaabaaba = e$, |
| 3. $aa^{-1} = a^{-1}a = e$, | 12. $abaaabab^{-1}a^{-1}b^{-1} = e$, |
| 4. $aaa = e$, | 13. $aba^{-1}bab^{-1}a^{-1}b^{-1} = e$, |
| 5. $[a, b] = aba^{-1}b^{-1}$, | 14. $aba^{-1}(b^{-1}b)bab^{-1}a^{-1}b^{-1} = e$, |
| 6. $[[a, b], b] = e?$ | 15. $(aba^{-1}b^{-1})b(bab^{-1}a^{-1})b^{-1} = e$, |
| 7. $bababa = e$, | 16. $(aba^{-1}b^{-1})b(aba^{-1}b^{-1})b^{-1} = e$, |
| 8. $ababa = b^{-1}$, | 17. $[a, b]b[a, b]^{-1}b^{-1} = e$, |
| 9. $baba = a^{-1}b^{-1}$, | 18. $[[a, b], b] = e$. |

Теперь алгебраистам-формалистам предлагается установить: будет ли из равенства $[[a, b], b] = e$ вытекать равенство $a^3 = e$ или не будет.

Конечно же, любое из выписанных тождеств для нильпотентной группы с определяющим ее равенством $a^3 = e$ прежде устанавливалось индуктивно, на подстановках или выписанных выше матрицах, в частности, для конкретной группы D_3^2 , и лишь затем разрабатывались какие-то общие схемы их доказатель-

ства. Искать же «вѣстную» правильное решение очень сложно, да и вряд ли необходимо. Число разнообразных групп огромно, а количество «красивых» соотношений между их элементами еще больше. Сейчас мы хотим познакомить нашего читателя с математическими объектами, тесно связанными с группами. Этими объектами являются *поля многочленов*, свойство которых сегодня широко используется в процедуре *кодирования информации*. Чтобы подступиться к конкретным многочленам, нам понадобится ряд новых понятий, в частности, мы вновь вернемся к *линейным пространствам*, с которых начали главу, чтобы рассмотреть их уже с точки зрения *поля*. Оговоримся, в этом подразделе любое множество с определенными на нем законами будет называться *алгебраической системой*, а также просто *алгеброй* или *системой*. Группы и поля являются примерами таких алгебраических систем, но они не единственные алгебры, причем мы не станем рассматривать их абстрактно, поскольку это мало поможет в практическом деле, каковым является кодирование информации.

Если введена какая-либо операция на множестве, не выводящая элементы за пределы этого множества, то данная алгебраическая система называется *группоидом*. Если в группоиде существует нейтральный элемент, то система называется *квазигруппой* (*луной*). Если в квазигруппе выполняется закон ассоциативности, то система называется *полугруппой* (*моноидом*). Если в полугруппе каждому элементу можно найти обратный, то система называется *группой*. Если в системе введены одновременно две операции — сложение и умножение, — причем для сложения выполняются все законы коммутативной группы, а по умножению законы группоида и дистрибутивный закон, то система называется *кольцом*. Если умножение в кольце еще и ассоциативно, то кольцо называется *ассоциативным*. Если в ассоциативном кольце умножение коммутативно, то система называется *ассоциативно-коммутативным кольцом*. Если все отличные от нуля элементы кольца составляют группу по умножению, то система называется *телом*. Если мультипликативная группа, входящая в тело, коммутативна, то система называется *полем*.

Приведем примеры этих алгебраических систем. Множество всех квадратных матриц образует ассоциативное кольцо. Множество многочленов с действительными коэффициентами от одной переменной с операциями сложения и умножения тоже образуют ассоциативное кольцо. Множество векторов евклидова пространства с операциями сложения векторов и векторного умножения образуют просто кольцо. Множество действительных чисел без нуля по умножению образуют мультипликативную группу. Множество натуральных чисел по сложению образуют аддитивную полугруппу. Множество целых чисел с операциями сложения и умножения образуют поле. Поля образуют и комплексные числа, кватернионы же являются телами. Комплексные числа, кватернионы и числа Клиффорда подчиняются закону ассоциативности, октава ему не подчиняется.

Если в ассоциативной алгебре сохранить аддитивную группу, а операцию умножения заменить метаоперацией *симметрирования*, т.е. $a * b = ab + ba$, то будет получено неассоциативное кольцо, в котором для элементов a и b выполняются равенства:

$$a * b = b * a, \quad ((a * a) * b) * a = (a * a) * (b * a).$$

Проверим второе равенство прямой подстановкой, для чего распишем правую часть:

$$\begin{aligned} & [(aa + aa)b + b(aa + aa)]a + a[(aa + aa)b + b(aa + aa)] = \\ & = aaba + aaba + baaa + baaa + aaab + aaab + abaa + abaa = \\ & = (aa + aa)(ba + ab) + (ba + ab)(aa + aa) = (a \circ a) \circ (b \circ a). \end{aligned}$$

В результате получили левую часть нашего равенства. Такая алгебраическая система получила название *кольца Ёрдана*. Если в ассоциативной алгебре вместо симметрирования ввести метаоперацию *антисимметрирования*, т.е. $a \circ b = ab - ba$, то будут выполняться два других равенства:

$$a \circ b = 0, \quad (a \circ b) \circ c + (b \circ c) \circ a + (c \circ a) \circ b = 0$$

(проверяется аналогично). Такая система получила название *кольца Ли*. Метаоперации симметрирования и антисимметрирования по своей сущности схожи с выведенной метаоперацией *коммутирования*. Кольца Ли и Ёрдана здесь введены абстрактно, как выше были введены нильпотентные группы. Сейчас мы перейдем к рассмотрению двух конкретных полей, а именно: *линейные пространства векторов* и *пространства двухкомпонентных чисел на базе иррациональности*.

Граница между понятиями числа и вектора, как мы убедились выше, достаточно условна. Тем не менее зададим два разнородных множества элементов, одно из которых назовем *векторами*: $a, b, c, \dots \in V$, другое — *числами (скалярами)*: $a, b, c, \dots \in U$. Алгебраическая система называется *линейным пространством над полем чисел*, если векторы представлены через числа в виде некоторой комбинации базисных векторов e_i :

$$a = a_1 e_1 + a_2 e_2 + \dots + a_n e_n.$$

При этом предполагается, что векторы по сложению образуют коммутативную группу, а числа удовлетворяют законам поля; кроме того, выполняются четыре следующих условия —

$$a(a + b) = aa + ab, \quad (a + b)a = aa + ba, \quad (ab)a = a(ba), \quad ea = a.$$

Говорят, что векторы e_i образуют *базис* векторного пространства V размерности n . Базис будет считаться линейно независимым, если из равенства $a_1 e_1 + a_2 e_2 + \dots + a_n e_n = 0$ следует $a_1 + a_2 + \dots + a_n = 0$. Векторное пространство V может иметь несколько наборов базисных векторов, поскольку сам базисный вектор e_i может быть выражен через систему векторов, в которой эта базисная составляющая заменена любым другим вектором: $e_i = b_1 e_1 + b_2 e_2 + \dots + b_i a + \dots + b_n e_n$. Однако любой набор базисных векторов всегда имеет одинаковое количество базисных компонентов, определяющих размерность пространства V . При нахождении набора базисных векторов или при определении размерности пространства V важно установить, является ли данная совокупность векторов a_i линейно независимой. Это можно сделать несколькими способами, в частности, если система векторов a_i зависима, то составленный на их основе *определитель Грама* равен нулю; для трехмерного случая имеем —

$$\gamma = \begin{vmatrix} (a_1 a_1) & (a_1 a_2) & (a_1 a_3) \\ (a_2 a_1) & (a_2 a_2) & (a_2 a_3) \\ (a_3 a_1) & (a_3 a_2) & (a_3 a_3) \end{vmatrix} = 0.$$

Если V_i есть подмножество базисных векторов пространства V , то говорят о *подпространстве* V_i относительно пространства V . *Прямой суммой* двух подпространств V_1 и V_2 называется множество векторов вида $a_i + b_i$, где $a_i \in V_1$, $b_i \in V_2$. Размерность нового пространства $N(V_1 + V_2)$ определяется формулой включения и исключения подмножеств. В нашем случае она выглядит следующим образом:

$$N(V_1 + V_2) = N(V_1) + N(V_2) - N(V_1 \cap V_2).$$

Доопределим линейное пространство V скалярным произведением векторов a и b : $(ab) = a_1b_1 + a_2b_2 + \dots + a_nb_n$. В теории кодирования информации дело имеет, как правило, с двоичной системой, так что $(ab) \in \{0, 1\}$. Если скалярное произведение равно нулю $(ab) = 0$, то векторы a и b *ортогональны*. Подпространства V_1 и V_2 будем называть *ортогональными дополнениями* до пространства V , если каждый вектор из V_1 ортогонален любому вектору из V_2 , а прямая сумма подпространств V_1 и V_2 дает целиком пространство V .

Пусть задано линейное пространство V из 16 векторов $a_0 = 0000$, $a_1 = 0001$, $a_2 = 0010, \dots, a_{15} = 1111$. Поставим перед собой задачу выбора системы базисных векторов таким образом, чтобы в нее входили векторы $a_7 = 0111$ и $a_{14} = 1110$. С помощью определителя Грама установим линейную независимость своего базиса, а затем разобьем двумя различными способами пространство V на два ортогональных дополнения.

Размерность нашего пространства равна $N(V) = 4$. Испытаем четыре вектора a_1, a_4, a_7 и a_{14} на независимость. С этой целью вычислим соответствующие скалярные произведения:

$$\begin{aligned} (a_1a_1) &= 0 \cdot 0 + 0 \cdot 0 + 0 \cdot 0 + 1 \cdot 1 = 1, & (a_4a_4) &= 1, & (a_7a_{14}) &= 0, \\ (a_1a_4) &= 0 \cdot 0 + 0 \cdot 1 + 0 \cdot 0 + 1 \cdot 0 = 0, & (a_4a_{14}) &= 1, & (a_{14}a_{14}) &= 1, \\ (a_1a_7) &= 1, & (a_4a_{14}) &= 0, & (a_7a_7) &= 1. \end{aligned}$$

Определитель Грама отличен от нуля:

$$\gamma = \begin{vmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{vmatrix} = 1.$$

Следовательно, четыре вектора a_1, a_4, a_7 и a_{14} могут составить базис, а раз так, то все остальные векторы должны выражаться через них:

$$\begin{aligned} a_0 &= 0 \cdot a_1 + 0 \cdot a_4 + 0 \cdot a_7 + 0 \cdot a_{14}, & a_8 &= 1 \cdot a_1 + 0 \cdot a_4 + 1 \cdot a_7 + 1 \cdot a_{14}, \\ a_1 &= 1 \cdot a_1 + 0 \cdot a_4 + 0 \cdot a_7 + 0 \cdot a_{14}, & a_9 &= 0 \cdot a_1 + 0 \cdot a_4 + 1 \cdot a_7 + 1 \cdot a_{14}, \\ a_2 &= 1 \cdot a_1 + 1 \cdot a_4 + 1 \cdot a_7 + 0 \cdot a_{14}, & a_{10} &= 0 \cdot a_1 + 1 \cdot a_4 + 0 \cdot a_7 + 1 \cdot a_{14}, \\ a_3 &= 0 \cdot a_1 + 1 \cdot a_4 + 1 \cdot a_7 + 0 \cdot a_{14}, & a_{11} &= 1 \cdot a_1 + 1 \cdot a_4 + 0 \cdot a_7 + 1 \cdot a_{14}, \\ a_4 &= 0 \cdot a_1 + 1 \cdot a_4 + 0 \cdot a_7 + 0 \cdot a_{14}, & a_{12} &= 1 \cdot a_1 + 1 \cdot a_4 + 1 \cdot a_7 + 1 \cdot a_{14}, \\ a_5 &= 1 \cdot a_1 + 1 \cdot a_4 + 0 \cdot a_7 + 0 \cdot a_{14}, & a_{13} &= 0 \cdot a_1 + 1 \cdot a_4 + 1 \cdot a_7 + 1 \cdot a_{14}, \\ a_6 &= 1 \cdot a_1 + 0 \cdot a_4 + 1 \cdot a_7 + 0 \cdot a_{14}, & a_{14} &= 0 \cdot a_1 + 0 \cdot a_4 + 0 \cdot a_7 + 1 \cdot a_{14}, \\ a_7 &= 0 \cdot a_1 + 0 \cdot a_4 + 1 \cdot a_7 + 0 \cdot a_{14}, & a_{15} &= 1 \cdot a_1 + 0 \cdot a_4 + 0 \cdot a_7 + 1 \cdot a_{14}. \end{aligned}$$

Смена базиса привела к *перекодированию* всех наших векторов, координаты которых можно представлять некими *кодowymi словами*. Так, вместо $a_{12} = 1100$ появился код 1111, что соответствовало кодовому слову a_{16} , вместо a_{13} появился код 0111.

Ортогональными дополнениями могут быть два векторных подпространства — $V_1 = \{a_0, a_1, a_4, a_5\}$ и $V_2 = \{a_0, a_2, a_8, a_{10}\}$, поскольку соответствующие скалярные произведения $(a_1 a_{10}) = 0, (a_5 a_2) = 0$ и т.д. — равны нулю. Ортогональными дополнениями будут и пространства $V_1 = \{a_0, a_2\}$ и $V_2 = \{a_0, a_1, a_4, a_5, a_8, a_9, a_{12}, a_{13}\}$; комбинаций здесь существует множество.

Мы уже говорили, что векторы и матрицы есть некие специфические числа, над которыми можно осуществлять определенные математические действия. Так, традиционные *комплексные числа* — это двухкомпонентные числа на базе *действительной* (1) и *мнимой* ($i = \sqrt{-1}$) единиц. В роли мнимой единицы может выступать какая-нибудь *иррациональная «единица»*, например, $\sqrt{2}$ или $\sqrt[3]{4}$. Вообще, иррациональные числа подразделяются на *трансцендентные* ($\pi, e, \lg 2, \sin 5$) и *алгебраические*. Действительное число называют алгебраическим, если оно является корнем некоторого многочлена с целыми коэффициентами. С этой точки зрения традиционные комплексные числа тоже будут алгебраическими, так как они являются корнями уравнения n -ой степени. В практических задачах электротехники рациональное число, например 2,1, часто складывают с иррациональным $\sqrt{3} \approx 1,7$ и в результате получают приближительное значение 3,8. С точки зрения теории чисел этого делать нельзя: иррациональные числа, как и комплексные, являются типичными представителями двухкомпонентных векторов. В частности, корнями квадратного уравнения с целыми коэффициентами $x^2 - 6x + 1 = 0$ является пара двухкомпонентных чисел

$$x_1 = 3 + 2\sqrt{2} \quad \text{и} \quad x_2 = 3 - 2\sqrt{2}.$$

Общий вид таких чисел — $c = a + bi, i = \sqrt{2}$ — схож с видом комплексных чисел, только в роли мнимой единицы здесь выступает иррациональное число. Действия над двухкомпонентными числами на базе иррациональности во многом аналогичны действиям над комплексными числами. В частности, формула умножения в обоих случаях выглядит одинаково:

$$(a_1 + b_1 i)(a_2 + b_2 i) = (a_1 a_2 + b_1 b_2 i^2) + (a_1 b_2 + a_2 b_1)i.$$

Кроме того, нормированным комплексным числам удовлетворяет уравнение окружности:

$$1 = x^2 + y^2 = (x + yi)(x - yi), \quad \text{где } x = \cos \varphi, y = \sin \varphi.$$

Двухкомпонентным числам на базе $\sqrt{2}$ также можно поставить в соответствие аналогичное уравнение — $1 = x^2 - 2y^2 = (x + y\sqrt{2})(x - y\sqrt{2})$. Решениями этого уравнения служат два числа $x_0 = 3, y_0 = 2$, но не только. Чтобы найти другие решения этого уравнения, нужно последовательно возводить в степень числа $3 \pm 2\sqrt{2}$, в частности, $(3 \pm 2\sqrt{2})^2 = 17 \pm 12\sqrt{2}$, следовательно, пара чисел $x_1 = 17, y_1 = 12$ также удовлетворяет уравнению. Следующее решение получается при возведении исходного числа в куб $(3 \pm 2\sqrt{2})^3 = 99 \pm 70\sqrt{2}$, значит, $x_2 = 99, y_2 = 70$ и т.д. Уравнения вида $1 = x^2 - Dy^2$ называются *уравнениями Пелля*, которым удовлетворяет бесконечная последовательность пар чисел, например, если $D = 7$, т.е. $i = \sqrt{7}$, то уравне-

ние Пелля $1 = x^2 - 7y^2$ выполняется при $x_0 = 8, y_0 = 3; x_1 = 127, y_1 = 48$ и т.д.; если $D = 13$, то $x_0 = 18, y_0 = 5; x_1 = 649, y_1 = 180$ и т.д.

Пусть дано уравнение $2x^2 + 5x + 4 = 0$. В поле действительных чисел оно не имеет решений, но в поле комплексных чисел решение уже есть. Существует оно и в поле вычетов по $\text{mod}(11)$. В самом деле,

$$x_{1,2} = \frac{-5 \pm \sqrt{-7}}{4} = \frac{6 \pm \sqrt{4}}{4} \text{mod}(11) = \{2, 1\}.$$

Данная ситуация схожа с решением кубического уравнения $x^3 - 1 = 0$ в полях действительных и комплексных чисел. В поле действительных чисел $x^3 - 1$ разлагается на два неприводимых множителя — $(x - 1)(x^2 + x + 1)$, а в поле комплексных чисел этот многочлен можно представить тремя сомножителями $(x - c_1) \times (x - c_2)(x - c_3)$, где c_1, c_2 и c_3 — кубические корни из единицы, образующие группу с умножением по табл. 2.69. В поле двух чисел $\{0, 1\}$, т.е. в поле вычетов по $\text{mod}(2)$ это кубическое уравнение может быть разложено на три скобки с корнями $c_1 = 1, c_2 = x, c_3 = x + 1$, в чем мы убедимся позднее.

Теперь рассмотрим только такие квадратные уравнения $ax^2 + bx + c = 0$, у которых коэффициенты являются всевозможными вычетами по $\text{mod}(5)$. Тогда корнями этих уравнений станут числа 0, 1, 2, 3 или 4. Квадраты этих чисел могут дать только три из пяти чисел: $0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 4, 4^2 = 1$. Другими словами, среди вычетов по $\text{mod}(5)$ нет чисел, квадраты которых равнялись бы 2 или 3, а это значит, что уравнения $x^2 = 2$ или $x^2 = 3$ не имеют решений. Чтобы эти уравнения все же решались, введем иррациональность $\sqrt{2}$. Тогда вместо пяти чисел получим поле из 25 чисел:

$0 + 0\sqrt{2},$	$1 + 0\sqrt{2},$	$2 + 0\sqrt{2},$	$3 + 0\sqrt{2},$	$4 + 0\sqrt{2},$
$0 + 1\sqrt{2},$	$1 + 1\sqrt{2},$	$2 + 1\sqrt{2},$	$3 + 1\sqrt{2},$	$4 + 1\sqrt{2},$
$0 + 2\sqrt{2},$	$1 + 2\sqrt{2},$	$2 + 2\sqrt{2},$	$3 + 2\sqrt{2},$	$4 + 2\sqrt{2},$
$0 + 3\sqrt{2},$	$1 + 3\sqrt{2},$	$2 + 3\sqrt{2},$	$3 + 3\sqrt{2},$	$4 + 3\sqrt{2},$
$0 + 4\sqrt{2},$	$1 + 4\sqrt{2},$	$2 + 4\sqrt{2},$	$3 + 4\sqrt{2},$	$4 + 4\sqrt{2},$

Таблица 2.69

Корни:	c_1	c_2	c_3
$c_1 = 1,$	c_1	c_2	c_3
$c_2 = -1/2 + \sqrt{3}/2i,$	c_2	c_3	c_1
$c_3 = -1/2 - \sqrt{3}/2i,$	c_3	c_1	c_2

Не выходя за рамки этого множества, можно производить сложение и умножение чисел. Каждый элемент этой *фигитной арифметики* является той или иной степенью образующего элемента $2 + \sqrt{2}$:

$$(2 + \sqrt{2})^2 = 1 + 4\sqrt{2}, \dots, (2 + \sqrt{2})^{24} = 1 + 0\sqrt{2}.$$

Можно ввести числа $a + b\sqrt{3}$ и путем последовательного возведения в степень получить новое поле на базе иррациональности $\sqrt{3}$, в частности:

$$(3 + 2\sqrt{3})^2 = 1 + 2\sqrt{3}, (3 + 2\sqrt{3})^3 = 0 + 3\sqrt{3}, \dots$$

Возможно построение поля на базе двух иррациональностей — $\sqrt{2}$ и $\sqrt{3}$; в этом случае будем иметь трехкомпонентные числа $a + b\sqrt{2} + c\sqrt{3}$, взятые по $\text{mod}(5)$, и т.д.

Чтобы двигаться дальше, напомним некоторые общие сведения из *теории чисел*. Всякое натуральное число p , не имеющее других натуральных делителей, кроме единицы и самого себя, называется *простым*, в противном случае — *составным* (единица считается ни простым, ни составным). Всякое натуральное число a , кроме единицы, может быть представлено произведением простых множителей: $a = p_1 p_2 \dots p_n$. Среди простых сомножителей этого представления могут встретиться равные. Если через $p_1, p_2, \dots, p_k$ обозначить именно различные простые числа и допустить, что они встречаются соответственно $n_1, n_2, \dots, n_k$ раз, то получаем *представление* $a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$, которое называется *каноническим*. Так, каноническое разложение числа 360 выглядит следующим образом: $2^3 3^2 5$. Каноническое разложение показывает, что все делители числа a исчерпываются числами вида $d = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$, где $0 \leq m_1 \leq n_1, 0 \leq m_2 \leq n_2, \dots, 0 \leq m_k \leq n_k$. Отношение делимости не

является *отношением эквивалентности*: $a/b \neq b/a$, но операция сравнения по $\text{mod}(m)$ будет таковой, поскольку для нее выполняются все три закона эквивалентности: $a = a \text{ mod}(m)$ — *рефлексивности*, из $a = b \text{ mod}(m)$ следует $b = a \text{ mod}(m)$ — *симметричности*, если $a = b \text{ mod}(m)$ и $b = c \text{ mod}(m)$, то $a = c \text{ mod}(m)$ — *транзитивности*.

Вычеты по $\text{mod}(m)$ определяют разбиение множества целых чисел на m *классов эквивалентности*: $\{C_0, C_1, C_2, \dots, C_{m-1}\}$, где $C_i = \{i, i+m, i+2m, \dots\}$. Например, для неотрицательных целых чисел по $\text{mod}(4)$ имеется четыре класса —

$$C_0 = \{0, 4, 8, 12, \dots\}, \quad C_2 = \{2, 6, 10, 14, \dots\}, \\ C_1 = \{1, 5, 9, 13, \dots\}, \quad C_3 = \{3, 7, 11, 15, \dots\}.$$

Объединение непересекающихся классов дает бесконечный монотонно возрастающий числовой ряд. Классы образуют *фактор-множество*, которое может быть представлено в нашем случае четырьмя представителями — $\{0, 1, 2, 3\}$; представители образуют *ядро* этого фактор-множества. Для представителей можно ввести операции сложения и умножения по $\text{mod}(4)$, которые удобно оформить таблицами — табл. 2.70 и табл. 2.71.

Таблица 2.70

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

Таблица 2.71

0	0	0	0
0	1	2	3
0	2	0	2
0	3	2	1

По сложению (табл. 2.70) имеем коммутативную группу, а по умножению (табл. 2.71) — нет, так как у нас получилось $2 \cdot 2 = 0$, что недопустимо для группы, но допустимо для кольца, которое имеет *делители нуля*. Примером кольца с делителем нуля является кольцо квадратных матриц:

$$\begin{pmatrix} 2 & 6 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} 3 & -9 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Кольца без делителей нуля называются *кольцами целостности*.

Если вычеты образованы по модулю простого числа, то фактор-множество или ядро его представителей является полем $GR(p)$, которое имеет специальное название — *поле Гауа*. В этих полях делители нуля уже отсутствуют, поэтому они занимают особое место в алгебре. Отбросив окаймляющие нули в таблице умножения для полей Гауа, которые есть и в табл. 2.71, мы получим элементы, образующие *циклическую группу*. Табл. 2.72 и табл. 2.73 являются примерами группового сложения и умножения в поле Гауа $GF(5)$.

Таблица 2.72

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

Таблица 2.73

0	0	0	0	0
0	1	2	3	4
0	2	4	1	3
0	3	1	4	2
0	4	3	2	1

При работе с полями многочленов нам понадобятся понятия *наибольшего общего делителя* двух чисел a и b — НОД(a, b) и *наименьшего общего кратного* — НОК(a, b), а также *алгоритм Евклида*. Напомним их содержание с помощью конкретного примера. Пусть даны два числа $a = 24$ и $b = 30$. Выпишем все делители этих чисел:

$$d(24) = \{1, 2, 3, 4, 6, 8, 12, 24\}, \quad d(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}.$$

Совокупность общих делителей образует множество $\{1, 2, 3, 6\}$. Следовательно, наибольший общий делитель равен 6. При больших числах для разыскания НОД используют алгоритм Евклида. Его содержание сводится к последовательному вычислению следующих равенств:

[illegible]

Действие алгоритма прекращается тогда, когда полученный остаток равен нулю; последний ненулевой остаток (r_n) равен *наибольшему общему делителю*. Как следствие из алгоритма Евклида, вытекает, что для любых целых чисел a и b всегда существуют числа m и n такие, что НОД(a, b) представляется в виде линейной комбинации этих чисел:

$$ma + nb = r_n = \text{НОД}(a, b).$$

Кроме того, отношение a/b можно представить в виде целной дроби. Чтобы к ней перейти, разделим все равенства, полученные в алгоритме Евклида, на $b, r_1, r_2, \dots, r_{n-1}, r_n$, получим:

$$a/b = q_1 + r_1/b = q_1 + \frac{1}{b/r_1};$$

$$b/r_1 = q_2 + r_2/r_1 = q_2 + \frac{1}{r_1/r_2};$$

$$r_1/r_2 = q_3 + r_3/r_2 = q_3 + \frac{1}{r_2/r_3};$$

.....

$$r_{n-1}/r_n = q_n + \frac{1}{r_n/r_{n-1}}.$$

При последовательной подстановке этих равенств друг в друга получаем цепную дробь:

$$a/b = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{\ddots}}}$$

Заданы два числа $a = 1656$ и $b = 1150$. Найдем НОД(a, b) и НОК(a, b), составим цепную дробь и линейную комбинацию:

$$1656 = 1150 \cdot 1 + 506, \quad 46 = 138 - 92 = 138 - 506 + 138 \cdot 3 =$$

$$1150 = 506 \cdot 2 + 138, \quad = 4 \cdot 138 - 506 = 4 \cdot 1150 - 9 \cdot 506 =$$

$$506 = 138 \cdot 3 + 92, \quad = 4 \cdot 1150 - 9 \cdot 1656 + 9 \cdot 1150 =$$

$$138 = 92 \cdot 1 + 46, \quad = 13 \cdot 1150 - 9 \cdot 1656;$$

$$92 = 46 \cdot 2; \quad m = -9, \quad n = 13;$$

$$\text{НОД}(a, b) = 46; \quad \text{НОК}(a, b) = a \cdot b / \text{НОД}(a, b) = 41400;$$

$$1656 / 1150 = 1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2}}}}$$

2.9. Поля многочленов

Теперь мы приобрели необходимые сведения для действия с многочленами n -ой степени вида:

$$a_n(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n.$$

Если $a_n(c) = 0$, то c — *корень* многочлена $a_n(x)$. Число c будет корнем $a_n(x)$ тогда и только тогда, когда $a_n(x)$ делится на скобку $(x - c)$ без остатка. Действительно, пусть $a(x) = (x - c)b(x) + r(x)$ при $x = c$, имеем $a(c) = (c - c)b(c) + r(c)$. Таким образом, остаток $r(c) = a(c)$, который равен нулю по определению.

Поиск корней многочлена $a_n(x)$ равносильен поиску его линейных делителей; при $a_0 = 1$ получим

$$a_n(x) = (x - c_1)b_1(x) = (x - c_1)(x - c_2)b_2(x) = \dots = (x - c_1)(x - c_2) \dots (x - c_n).$$

Общее число корней многочлена $a_n(x)$ всегда равно n . Однако могут встречаться кратные корни, тогда

$$a_n(x) = (x - c_1)^{n_1} (x - c_2)^{n_2} \dots (x - c_k)^{n_k}.$$

Это называется *каноническим разложением* многочлена $a(x)$ на *простые (неприводимые)* множители. Многочлен $a(x)$ называется *приводимым*, если он может быть разложен в произведение двух множителей без остатка — $a(x) = b(x)q(x)$. Но известна ситуация, когда многочлен $a(x)$ часть корней имеет в поле действительных чисел, а часть — в поле комплексных чисел. Таким образом, о приводимости или неприводимости многочленов можно говорить лишь по отношению к данному полю, поскольку многочлен, неприводимый в одном поле, может оказаться приводимым в другом. Ранее приведенный пример с многочленом $x^3 - 1$ в этом отношении показателен.

Далее нас будут интересовать многочлены $a(x)$, у которых коэффициенты a_i взяты из числового поля $GF(p)$. Эти многочлены образуют кольцо относительно сложения и умножения. Пусть этими многочленами будут $a(x) = x^3 + x + 1$ и $b(x) = x^2 + x + 1$, а числовое поле $GF(2) = \{0, 1\}$, тогда сумма и произведение $a(x)$ и $b(x)$ дадут два новых многочлена —

$$a(x) + b(x) = x^3 + x^2 \quad \text{и} \quad a(x) \cdot b(x) = x^5 + x^4 + 1.$$

В своей совокупности многочлены образуют именно *ассоциативно-коммутативное кольцо*, но не поле, поскольку не существует таких многочленов степени больше единицы, которые бы при перемножении давали единицу: $a(x) \cdot b(x) = 1$, т.е. в алгебре многочленов для каждого элемента отсутствует обратный.

Многочлены можно делить друг на друга:

$$\begin{array}{r} a(x) = x^3 + x + 1 \quad \left| \begin{array}{l} x^2 + x + 1 = b(x) \\ x^3 + x^2 + x \\ \hline x^2 + x + 1 \end{array} \right. \\ x^3 + x^2 + x \\ \hline x^2 + x + 1 \\ \hline x = r(x) \end{array} \quad a(x) = b(x) \cdot q(x) + r(x).$$

Многочлен $b(x)$ называется делителем $a(x)$, если остаток $r(x)$ равен нулю. Наибольший общий делитель двух многочленов $a(x)$ и $b(x)$ находится по алгоритму Евклида, только роль чисел уже выполняют многочлены. Покажем, как его найти на многочленах $a(x)$ и $b(x)$ с коэффициентами, взятыми из числового поля $GF(3)$:

$$a(x) = x^6 + 2x^3 + x^2 + 2x + 2, \quad b(x) = x^5 + x^4 + x^3 + x^2 + x + 1.$$

Следуем алгоритму Евклида:

$$\begin{array}{r} a(x) = x^6 + 2x^3 + x^2 + 2x + 2 \quad \left| \begin{array}{l} x^5 + x^4 + x^3 + x^2 + x + 1 = b(x) \\ x^6 + x^5 + x^4 + x^3 + x^2 + x \\ \hline 2x^5 + 2x^3 + x^3 + x + 2 \\ 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 2 \\ \hline 2x^3 + x^2 + 2x = r_1(x) \end{array} \right. \\ x^5 + x^4 + x^3 + x^2 + x + 1 \\ \hline 2x^4 + x^2 + x + 1 \\ 2x^4 + x^3 + 2x^2 \\ \hline 2x^3 + 2x^2 + x + 1 \\ 2x^3 + x^2 + 2x \\ \hline x^2 + 2x + 1 = r_2(x) \end{array} \quad \begin{array}{l} x + 2 = q_1(x) \\ 2x^3 + x^2 + 2x = r_1(x) \\ 2x^2 + x + 1 = q_2(x) \\ a(x) = b(x)q_1(x) + r_1(x), \\ b(x) = r_1(x)q_2(x) + r_2(x), \\ r_1(x) = r_2(x)q_3(x); \end{array}$$

$$\begin{array}{r|l} r_1(x) = 2x^3 + x^2 + 2x & | x^2 + 2x + 1 = r_2(x) \\ \underline{2x^3 + x^2 + 2x} & 2x = q_3(x) \\ 0 & \end{array}$$

Таким образом, $\text{НОД}(a(x), b(x)) = x^2 + 2x + 1 = r_2(x)$. Чтобы найти НОК, необходимо знать результат от перемножения исходных многочленов; он равен:

$$a(x)b(x) = x^{11} + x^{10} + x^9 + x^7 + x^5 + x^4 + x^3 + 2x^2 + x + 2;$$

$$\begin{aligned} \text{НОК}(a(x), b(x)) &= a(x)b(x) / \text{НОД}(a(x), b(x)) = \\ &= x^9 + 2x^8 + 2x^7 + 2x^5 + 2x^2 + x^3 + 2. \end{aligned}$$

Наконец, коэффициенты $m(x)$ и $n(x)$ линейного разложения $\text{НОД}(a(x), b(x))$ по $a(x)$ и $b(x)$ равны:

$$m(x) = x^3 + 2x^2 + x, \quad n(x) = 2x^4 + 2x^3 + x^2 + x + 1.$$

Для многочлена, как и для чисел, можно ввести сравнение многочлена $a(x)$ по модулю многочлена $q(x)$: $a(x) = r(x) \bmod q(x)$. А раз так, то можно говорить и о *поле многочленов* $GF(q)$ над числовым полем $GF(p)$. Если $GF(2)$ и $q(x) = x^3 + 1$, то имеем поле многочленов $GF(x^3 + 1)$, состоящее из восьми многочленов: $\{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$. Здесь $p = 2$ называется *характеристикой* поля $GF(p)$; характеристика определяет *размерность* или *порядок* полей многочлена: $q = p^n = 2^3 = 8$, где n — *степень* многочлена $q(x)$. Перемножим два произвольных элемента поля $GF(q)$ по $\bmod q(x)$:

$$(x^2 + 1)x^2 = x^4 + x^2 = x(x^3 + 1) + (x^2 + x) = x^2 + x.$$

Продолжая далее перемножать элементы $GF(q)$, мы могли бы составить таблицу умножения. Но мы составим таблицы сложения (табл. 2.74) и умножения (табл. 2.75) для другого поля многочленов — $GF(x^2 + x + 1)$, размерность которого в два раза меньше: $\{0, 1, x, x + 1\}$. Каждому элементу последнего множества можно поставить в соответствие либо двоичное число: $\{00, 01, 10, 11\}$, либо десятичное: $\{0, 1, 2, 3\}$, тогда таблицы сложения (табл. 2.74) и умножения (табл. 2.75) поля $GF(x^2 + x + 1)$ предстанут в виде числовых таблиц (табл. 2.76) и (табл. 2.77), схожих с табл. 2.70 и табл. 2.71.

Таблица 2.74

0	1	x	$x + 1$
1	0	$x + 1$	x
x	$x + 1$	0	1
$x + 1$	x	1	0

Таблица 2.75

0	0	0	0
0	1	x	$x + 1$
0	x	$x + 1$	1
0	$x + 1$	1	x

Таблица 2.76

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

Таблица 2.77

0	0	0	0
0	1	2	3
0	2	3	1
0	3	1	2

Обращаем внимание читателя на тот примечательный факт, что табл. 2.77 по сравнению с табл. 2.71 не имеет делителя нуля, а три элемента, отличных от 0, образуют циклическую группу; другими словами, множество $GF(x^2 + x + 1)$, состоящее из четырех элементов, образует *поле Галуа*. Напомним, что выше числовое поле Галуа $GF(p)$ могло получиться только для простых чисел: $p = 2, 3, 5, 7, \dots$. У нас же $q = p^n = 2^2 = 4$, а поле получилось как от простого числа. В литературе¹ показано, что поля Галуа возникают тогда, когда число элементов q равно степени простого числа; или, иначе, $GF(q)$ будет полем Галуа, когда $q(x)$ является *простым (неприводимым)* многочленом. Приведем по одному простому многочлену степени 2–27:

$x^2 + x + 1,$	$x^{15} + x + 1,$
$x^3 + x + 1,$	$x^{16} + x^{12} + x^3 + x + 1,$
$x^4 + x + 1,$	$x^{17} + x^3 + 1,$
$x^5 + x^2 + 1,$	$x^{18} + x^7 + 1,$
$x^6 + x + 1,$	$x^{19} + x^5 + x^2 + x + 1,$
$x^7 + x^3 + 1,$	$x^{20} + x^3 + 1,$
$x^8 + x^4 + x^3 + x^2 + 1,$	$x^{21} + x^2 + 1,$
$x^9 + x^4 + 1,$	$x^{22} + x + 1,$
$x^{10} + x^3 + 1,$	$x^{23} + x^5 + 1,$
$x^{11} + x^2 + 1,$	$x^{24} + x^7 + x^2 + x + 1,$
$x^{12} + x^6 + x^4 + x + 1,$	$x^{25} + x^3 + 1,$
$x^{13} + x^4 + x^3 + x + 1,$	$x^{26} + x^6 + x^2 + x + 1,$
$x^{14} + x^{10} + x^6 + x + 1,$	$x^{27} + x^5 + x^2 + x + 1.$

Циклическая группа по умножению (табл. 2.75) изоморфна циклической группе корней кубических из единицы (табл. 2.69), только в качестве элементов в данном случае выступают многочлены: $c_1 = 1$, $c_2 = x$, $c_3 = x + 1$, получающиеся за счет расширения числового поля, подобного расширению числового поля действительных чисел за счет комплексных. Если в качестве образующего взять элемент $c_2 = x$, то последовательным возведением его в первую, вторую и третью степень получим все три элемента: $x^1 = x$, $x^2 = x + 1$, $x^3 = 1$. Эти элементы являются корнями уравнения $x^3 + 1 = (x + 1)(x^2 + x + 1) = 0$, решенного в поле $GF(2)$.

Приведем примеры таблиц сложения и умножения для следующих полей многочленов:

$$GF(3^2) = \{0, 1, 2, 3, 4, 5, 6, 7, 8\} = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\},$$

$$g(x) = x^2 + x + 2,$$

таблица сложения — табл. 2.78, таблица умножения — табл. 2.79.

$$GF(2^5) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\} =$$

$$= \{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1, x^3, x^3 + 1, x^3 + x, x^3 + x + 1,$$

$$x^4 + x^2, x^4 + x^2 + 1, x^4 + x^2 + x, x^4 + x^2 + x + 1\}, \quad g(x) = x^4 + x^3 + 1,$$

таблица сложения — табл. 2.80, таблица умножения — табл. 2.81.

¹ Галлер Р. Теория информации и надежная связь. — М., 1974, с. 252–256, а также Блэйхут Р. Теория и практика кодов, контролирующая ошибки (гл. 4.2). — М., 1986.

Таблица 2.78

0	1	2	3	4	5	6	7	8
1	2	0	4	5	3	7	8	6
2	0	1	5	3	4	8	6	7
3	4	5	6	7	8	0	1	2
4	5	3	7	8	6	1	2	0
5	3	4	8	6	7	2	0	1
6	7	8	0	1	2	3	4	5
7	8	6	1	2	0	4	5	3
8	6	7	2	0	1	5	3	4

Таблица 2.79

0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8
0	2	1	6	8	7	3	5	4
0	3	6	7	1	4	5	8	2
0	4	8	1	5	6	2	3	7
0	5	7	4	6	2	8	1	3
0	6	3	5	2	8	7	4	1
0	7	5	8	3	1	4	2	6
0	8	4	2	7	3	1	6	5

Таблица 2.80

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

Таблица 2.81

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2	4	6	8	A	C	E	9	B	D	F	1	3	5	7
0	3	6	5	C	F	A	9	1	2	7	4	D	E	B	8
0	4	8	C	9	D	1	5	B	F	3	7	2	6	A	E
0	5	A	F	D	8	7	2	3	6	9	C	E	B	4	1
0	6	C	A	1	7	D	B	2	4	E	8	3	5	F	9
0	7	E	9	5	2	B	C	A	D	4	3	F	8	1	6
0	8	9	1	B	3	2	A	F	7	6	E	4	C	D	5
0	9	B	2	F	6	4	D	7	E	C	5	8	1	3	A
0	A	D	7	3	9	E	4	6	C	B	1	5	F	8	2
0	B	F	4	7	C	8	3	E	5	1	A	9	2	6	D
0	C	1	D	2	E	3	F	4	8	5	9	6	A	7	B
0	D	3	E	6	B	5	8	C	1	F	2	A	7	9	4
0	E	5	B	A	4	F	1	D	3	8	6	7	9	2	C
0	F	7	8	E	1	9	6	5	A	2	D	B	4	C	3

Все выписанные таблицы определяют хорошо знакомые нам коммутативные группы. Если по таблицам составить регулярные подстановки, то их структура сразу же будет узнаваема. Естественно, для этих групп можно найти все их подгруппы, включая нормальные делители. Та роль, которую в группах играют нормальные делители, в кольцах принадлежит *идеалам*. Подмножество I кольца K называется идеалом, если оно является подгруппой аддитивной группы кольца. Для того чтобы подмножество I было идеалом в K , необходимо выполнение единственного условия, а именно: если $i \in I$ и $k \in K$, то их произведения ik и ki должны принадлежать подмножеству I . Если в определении идеала отказаться от требования, что оба произведения ik и ki принадлежат I , то придем к понятию *одностороннего идеала*: если $ik \in I$ — *правый идеал*, если $ki \in I$ — *левый идеал*. Всякий идеал кольца будет *подкольцом*. Пересечение любой системы идеалов кольца будет идеалом. В кольцах Ли и Ёрдана левые и правые идеалы совпадают; такие идеалы называются *двухсторонними*. Из определения идеала следует, что во всяком кольце K идеалами являются само кольцо K и так называемый *нуль-идеал*, состоящий из одного нулевого элемента. Кольцо, не содержащее других идеалов, кроме этих двух, называется *простым*. Все тела и поля являются *простыми кольцами*. Можно было бы продолжать вводить для колец и полей понятия гомоморфизма, фактор-множества и т.д., только все это нас слишком уведет в сторону. Между тем, овладев техникой анализа групп, провести подобный анализ для полей не составит большого труда. Поэтому вернемся непосредственно к многочленам.

Рассмотрим самый общий случай. Пусть дано некоторое поле многочленов $GF(q)$, где $q = p^n$, n — степень модуля q , а p — характеристика. Обозначим через $g_1(x), g_2(x), \dots, g_{q-1}(x)$ различные неприводимые многочлены над полем чисел $GF(p)$, отвечающие *примитивным* корням: $c_1, c_2, \dots, c_{q-1}$. Утверждается, что существует единственно возможное разложение многочлена $x^{q-1} - 1$ на множители $g_i(x)$; или, что одно и то же, каждый элемент c_i является корнем многочлена $x^{q-1} - 1$; или, наконец, исходный приводимый многочлен можно представить в виде произведения *порождающего* $g(x)$ и *проверочного* $h(x)$ многочленов:

$$x^{q-1} - 1 = \prod_{i=1}^{q-1} g_i(x) = \prod_{i=1}^{q-1} (x - c_i) = g(x)h(x),$$

где $g(x) = (x - c)(x - c^p)(x - c^{p^2}) \dots (x - c^{p^{k-1}})$, $h(x) = \prod_j (x - c^j)$.

Здесь c — примитивный корень порождающего многочлена $g(x)$, а для проверочного многочлена $h(x)$ берутся те степени c^j , которые не вошли в многочлен $g(x)$. Как видим, действия с многочленами во многом схожи с действиями над числами. Приводимый многочлен вида $x^{q-1} - 1$ играет роль составного числа a , его примитивные корни $c_1, c_2, \dots, c_{q-1}$ ассоциируются с простыми сомножителями $p_1, p_2, \dots, p_k$, а последняя формула разложения на множители аналогична каноническому разложению составного числа $a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$. Многочлены $g(x)$ и $h(x)$ играют роль двух делителей числа $a = g \times h$. Корни исходного многочлена играют роль базиса, по которому многочлены $g(x)$ и $h(x)$ могут быть разложены. Таким образом, *теория полей многочленов* смыкается с *теорией линейных пространств*. Покажем, как это осуществляется практически.

Если c — примитивный корень многочлена $g(x)$, то $g(c) = g_0 + g_1c + g_2c^2 + \dots + g_nc^n = 0$. Выразим степени корней c^n и c^{n+1} через линейную комбинацию младших степеней корней $c, c^2, \dots, c^{n-1}$ ($g_n = 1$):

$$\begin{aligned} c^n &= g_0 + g_1c + g_2c^2 + \dots + g_{n-1}c^{n-1}, \\ c^{n+1} &= g_0c + g_1c^2 + g_2c^3 + \dots + g_{n-1}(g_0 + g_1c + g_2c^2 + \dots + g_{n-1}c^{n-1}). \end{aligned}$$

Следовательно, все степени c^i при $i \geq n$ линейно выражаются через первые n степеней; число таких комбинаций не превышает величину $q - 1$. Следует также иметь в виду, что не только $g(c) = 0$, но и $g(c^p) = g(c^{p^2}) = \dots = g(c^{q-1}) = 0$.

Рассмотрим поле многочленов $GF(q)$ по модулю неприводимого многочлена $g(x) = x^3 + x + 1$. Пусть примитивным корнем многочлена $g(x)$ является корень c , тогда $g(c) = c^3 + c + 1 = 0$. Так как $q = 2^3 = 8$, то циклический порядок корня c равен $q - 1 = 7$. Все корни степени $i \geq 3$ выражаются через c и c^2 , при этом многочлен $g(c)$ берется за модуль:

$$\begin{aligned} c^3 &= (c^3 + c + 1) \cdot 1 + (c + 1) = c + 1, \\ c^4 &= (c^3 + c + 1) \cdot c + (c^2 + c) = c^2 + c, \\ c^5 &= (c^3 + c + 1) \cdot c^2 + (c^3 + c^2) = c^2 + c + 1, \\ c^7 &= (c^3 + c + 1) \cdot c^3 + (c^4 + c^3) = c^2 + 1. \end{aligned}$$

Проверим, что числа c, c^2 и c^4 действительно являются корнями многочлена $g(x) = x^3 + x + 1$:

$$\begin{aligned} g(c) &= c^3 + c + 1 = c + 1 + c + 1 = 0, \\ g(c^2) &= c^6 + c^2 + 1 = c^2 + 1 + c^2 + 1 = 0, \\ g(c^4) &= c^{12} + c^4 + 1 = c^5 + c^4 + 1 = 0. \end{aligned}$$

Отсюда порождающий многочлен $g(x)$ раскладывается на следующие примитивные множители:

$$g(x) = x^3 + x + 1 = (x + c)(x + c^2)(x + c^4),$$

на долю же проверочного многочлена $h(x)$ приходятся все остальные степени корня c :

$$h(x) = (x + c^3)(x + c^5)(x + c^6)(x + c^7).$$

Таким образом, исходный приводимый многочлен $x^7 + 1$ может быть разложен «каноническим» образом в расширенном поле примитивных корней (аналог поля комплексных чисел):

$$x^7 + 1 = (x + c)(x + c^2)(x + c^3)(x + c^4)(x + c^5)(x + c^6)(x + c^7),$$

и «неканоническим», где в скобках стоят простые сомножители (аналог поля действительных чисел):

$$x^7 + 1 = (x^3 + x + 1)(x^3 + x^2 + 1)(x + 1),$$

а также в виде двух сомножителей:

$$x^7 + 1 = g(x)h(x) = (x^3 + x + 1)(x^4 + x^2 + x + 1).$$

Если в роли модуля будет выступать порождающий многочлен $g(x) = x^3 + x^2 + 1$, то его примитивный корень d даст несколько отличный цикл высших степеней корней, а именно:

$$d^3 = d^2 + 1, d^4 = d^2 + d + 1, d^5 = d + 1, d^6 = d^2 + d,$$

во всем же остальном процедура не изменится.

Рассмотрим еще несколько конкретных примеров.

Пример 1. Составим полную таблицу неприводимых многочленов $g_i(x)$ поля вычетов $GF(2^4)$ по модулю $g(x) = x^4 + x + 1$ над числовым полем $GF(2)$.

Заполнение таблицы неприводимых многочленов (табл. 2.82) начнем с исходного многочлена. Так как

$$g(x) = (x - c)(x - c^2)(x - c^4)(x - c^8),$$

против степеней c, c^2, c^4 и c^8 можно писать многочлен $g(x)$. Далее, выразим все степени c^i через c, c^2 и c^3 , как это было сделано в предыдущем случае. Чтобы найти все остальные неприводимые множители, необходимо поступить следующим образом. Возьмем произвольный корень $a = c^{14} = c^3 + 1$. Тогда

$$g_a(x) = (x - a)(x - a^2)(x - a^4)(x - a^8).$$

Так как

$$a^2 = c^{28 + 15} = c^{13} = c^3 + c^2 + 1,$$

$$a^4 = c^{56 + 45} = c^{11} = c^3 + c^2 + c,$$

$$a^8 = c^{112 + 105} = c^7 = c^3 + c + 1,$$

можно написать

$$\begin{aligned} g_a(x) &= (x - c^{14})(x - c^{13})(x - c^{11})(x - c^7) = \\ &= [x^2 - (c^{14} + c^{13})x + c^{12}][x - c^{11}][x - c^7] = \\ &= (x^2 - c^2x + c^{12})(x - c^{11})(x - c^7) = \\ &= [x^3 - (c^{11} + c^2)x^2 + (c^{12} + c^{13})x - c^8] \cdot (x - c^7) = \\ &= (x^3 - c^9x^2 + cx - c^8)(x - c^7) = \\ &= x^4 - (c^9 + c^7)x^3 + (c + c)x^2 - (c^8 + c^8)x + c^{15}. \end{aligned}$$

Следовательно, против корней c^7, c^{11}, c^{13} и c^{14} ставим неприводимый многочлен $g_a(x) = x^4 + x^3 + 1$. Затем берется следующий неизвестный корень и предыдущая процедура повторяется. Так происходит последовательное заполнение всей табл. 2.82. Проверка правильности нахождения состоит в выполнении основного тождества:

$$x^{15} + 1 = (x^4 + x^3 + 1)(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x + 1).$$

Таблица 2.82

c^i	$k \cdot c^3 + l \cdot c^2 + m \cdot c + n$	$g_i(x)$
c^1	c	$x^4 + x + 1$
c^2	c^2	$x^4 + x + 1$
c^3	c^3	$x^4 + x^3 + x^2 + x + 1$
c^4	$c + 1$	$x^4 + x + 1$
c^5	$c^2 + c$	$x^4 + x + 1$
c^6	$c^3 + c^2$	$x^4 + x^3 + x^2 + x + 1$
c^7	$c^3 + c + 1$	$x^4 + x^3 + 1$
c^8	$c^2 + 1$	$x^4 + x + 1$
c^9	$c^3 - c$	$x^4 + x^3 + x^2 + x + 1$
c^{10}	$c^2 + c + 1$	$x^4 + x + 1$
c^{11}	$c^3 + c^2 + c$	$x^4 + x^3 + 1$
c^{12}	$c^3 + c^2 + c + 1$	$x^4 + x^3 + x^2 + x + 1$
c^{13}	$c^3 - c^2 + 1$	$x^4 + x^3 + 1$
c^{14}	$c^3 + 1$	$x^4 + x^3 + 1$
c^{15}	1	$x + 1$

Пример 2. Рассмотрим поле $GF(3^2)$ по модулю $g(x) = x^2 + 1$ над полем $GF(3)$. Здесь многочлен $g(x)$ является неприводимым, но он не является и порождающим или образующим многочленом поля, поскольку степени его корни дают единицу уже при c^4 , а не 8: $c^2 = (c^2 + 1) \cdot 1 + 2 = 2$, $c^3 = (c^2 + 1) \cdot c + 2c - 2c$, $c^4 = (c^2 + 1) \cdot c^2 + 1 = 1$, $c^5 = c$, $c^6 = 2$, $c^7 = 2c$, $c^8 = 1$. Аналогичная ситуация возникает и в числовых полях, например, в поле $GF(7)$ элемент 3 является образующим, так как его степени порождают все элементы поля: $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$, тогда как элемент 2 уже не будет образующим; в самом деле, его степени не дают элементы 3, 5 и 6: $2^1 = 2$, $2^2 = 4$, $2^3 = 1$, $2^4 = 2$, $2^5 = 4$, $2^6 = 1$. Поэтому исходным порождающим элементом нужно выбрать другой неприводимый многочлен, например, $g(x) = x^2 + x + 2$. При составлении полной таблицы неприводимых многочленов (табл. 2.83) для случая поля $GF(3)$ действуем аналогично примеру 1. При этом необходимо помнить, что представителями классов вычетов по модулю 3 могут быть как числа 0, 1, 2, так и числа $-1, 0, 1$. Отсюда возникают две формы записи неприводимых многочленов с двумя проверочными соотношениями:

$$x^8 + 2 = (x^2 + x + 2)(x^2 + 2x + 2)(x^2 + 1)(x + 1)(x + 2),$$

$$x^8 - 1 = (x^2 + x^3 - 1)(x^4 - x - 1)(x^2 + 1)(x + 1)(x - 1).$$

Таблица 2.83

c^i	$k \cdot c + l$	$g_i(x) \{0, 1, 2\}$	$g_i(x) \{-1, 0, 1\}$
c^1	c	$x^2 + x + 2$	$x^2 - x - 1$
c^2	$2c + 1$	$x^2 + 1$	$x^2 - 1$
c^3	$2c + 2$	$x^2 + x + 2$	$x^2 + x - 1$
c^4	2	$x + 1$	$x + 1$
c^5	$2c$	$x^2 + 2x + 2$	$x^2 - x - 1$
c^6	$c + 2$	$x^2 + 1$	$x^2 - 1$
c^7	$c + 1$	$x^2 + 2x + 2$	$x^2 - x - 1$
c^8	1	$x + 2$	$x - 1$

Полные таблицы неприводимых многочленов и линейные комбинации корней для полей $GF(5^2)$, $GF(3^3)$ и $GF(2^5)$ приведены соответственно в табл. 2.84, табл. 2.85 и табл. 2.86. Порождающие многочлены $g(x)$ во всех трех таблицах стоят в первых строчках напротив корня c^1 .

Таблица 2.84

c^i	$k \cdot c + l$	$g_i(x)$
c^1	c	$3x^2 + 2x + 1$
c^2	$c + 3$	$x^2 + 2x + 4$
c^3	$4c + 3$	$x^2 + 3$
c^4	$2c + 2$	$x^2 + x + 1$
c^5	$4c + 1$	$3x^2 + 2x + 1$
c^6	2	$x^2 + 4x + 4$
c^7	$2c$	$x^2 + 2x + 3$
c^8	$2c + 1$	$x^2 + 4x + 1$
c^9	$3c + 1$	$x^2 - 2$
c^{10}	$4c + 4$	$x^2 + 2x + 4$
c^{11}	$3c + 2$	$x^2 + 2x + 3$
c^{12}	4	$x^2 + 3x + 1$
c^{13}	$4c$	$x^2 + 4x + 2$
c^{14}	$4c + 2$	$x^2 + 3x + 4$
c^{15}	$c + 2$	$x^2 + 3$
c^{16}	$3c + 3$	$x^2 + 4x + 1$
c^{17}	$c - 4$	$x^2 + 4x + 2$
c^{18}	3	$x^2 + x + 4$
c^{19}	$3c$	$x^2 + 3x + 3$
c^{20}	$3c + 4$	$x^2 + x + 1$
c^{21}	$2c + 4$	$x^2 + 2$
c^{22}	$c + 1$	$x^2 - 4$
c^{23}	$2c + 3$	$x^2 + 3x + 3$
c^{24}	1	$x + 1$

Таблица 2.85

c^i	$l \cdot c^2 + m \cdot c + n$	$g_i(x)$
c^1	c	$x^3 + 2x + 1$
c^2	c^2	$x^3 + x^2 - x + 2$
c^3	$c + 2$	$x^3 + 2x + 1$
c^4	$c^2 + 2c$	$x^3 + x^2 + 2$
c^5	$2c^2 + c + 2$	$x^3 + 2x^2 + x + 1$
c^6	$c^2 + c + 1$	$x^3 + x^2 + x + 2$
c^7	$c^2 + 2c + 2$	$x^3 + x^2 + 2x + 1$
c^8	$2c^2 + 2$	$x^3 + 2x^2 + 2x + 2$
c^9	$c + 1$	$x^3 + 2x + 1$
c^{10}	$c^2 + c$	$x^3 + x^2 + 2$
c^{11}	$c^2 + c + 2$	$x^3 + x^2 + 2x + 1$
c^{12}	$c^2 + 2$	$x^3 + x^2 + 2$
c^{13}	2	$x + 1$
c^{14}	$2c$	$x^3 + 2x + 2$
c^{15}	$2c^2$	$x^3 + 2x^2 + x + 1$
c^{16}	$2c + 1$	$x^3 + 2x + 2$
c^{17}	$2c^2 + c$	$x^3 + 2x^2 + 1$
c^{18}	$c^2 + 2c + 1$	$x^3 + x^2 + x + 2$
c^{19}	$2c^2 + 2c + 2$	$x^3 + 2x^2 + x + 1$
c^{20}	$2c^2 + c + 1$	$x^3 + 2x^2 + 2x + 2$
c^{21}	$c^2 + 1$	$x^3 + x^2 + 2x + 1$
c^{22}	$2c + 2$	$x^3 + 2x + 2$
c^{23}	$2c^2 + 2c$	$x^3 + 2x^2 + 1$
c^{24}	$2c^2 + 2c + 1$	$x^3 + 2x^2 + 2x + 2$
c^{25}	$2c^2 + 1$	$x^3 + 2x + 1$
c^{26}	1	$x + 2$

c'	$j \cdot c^4 + k \cdot c^3 + l \cdot c^2 + m \cdot c + n$	$g_i(x)$
c^1	c	$x^5 - x^4 + x^2 + x + 1$
c^2	c^2	$x^5 - x^4 + x^2 + x + 1$
c^3	c^3	$x^5 + x^4 + x^3 + 1$
c^4	c^4	$x^5 + x^4 + x^2 + x + 1$
c^5	$c^4 + c^2 + c + 1$	$x^5 + x^3 + x^2 + x + 1$
c^6	$c^4 + c^3 + 1$	$x^5 + x^4 + x^3 + 1$
c^7	$c^2 + 1$	$x^5 + x^2 + 1$
c^8	$c^3 + c$	$x^5 + x^4 + x^2 + x + 1$
c^9	$c^4 + c^2$	$x^5 + x^3 + x^2 + x + 1$
c^{10}	$c^4 + c^3 + c^2 + c + 1$	$x^5 + x^3 + x^2 + x + 1$
c^{11}	$c^4 + c^3 + 1$	$x^5 + x^4 + x^3 + x^2 + 1$
c^{12}	$c^4 + c$	$x^5 + x^4 + x^3 + 1$
c^{13}	$c^4 + c + 1$	$x^5 + x^4 + x^3 + x^2 + 1$
c^{14}	$c^4 + 1$	$x^5 + x^2 - 1$
c^{15}	$c^4 + c^2 + 1$	$x^5 + x^4 + x^3 + x^2 + x + 1$
c^{16}	$c^4 + c^3 + c^2 + 1$	$x^5 + x^4 + x^2 + x + 1$
c^{17}	$c^3 + c^2 + 1$	$x^5 + x^4 + x^3 + 1$
c^{18}	$c^4 + c^3 + c$	$x^5 + x^3 + x^2 + x + 1$
c^{19}	$c + 1$	$x^5 + x^2 + 1$
c^{20}	$c^2 + c$	$x^5 + x^3 + x^2 + x + 1$
c^{21}	$c^3 + c^2$	$x^5 + x^4 + x^3 + x^2 + 1$
c^{22}	$c^4 + c^3$	$x^5 + x^4 + x^3 + x^2 + 1$
c^{23}	$c^2 + c + 1$	$x^5 + x^4 + x^3 + x^2 + x + 1$
c^{24}	$c^3 + c^2 + c$	$x^5 + x^4 + x^3 + 1$
c^{25}	$c^4 + c^3 + c^2$	$x^5 + x^2 - 1$
c^{26}	$c^3 - c^2 + c - 1$	$x^5 + x^4 + x^3 + x^2 + 1$
c^{27}	$c^4 + c^3 + c^2 + c$	$x^5 + x^4 + x^3 + x^2 + x - 1$
c^{28}	$c^3 + c + 1$	$x^5 + x^2 + 1$
c^{29}	$c^4 + c^2 + c$	$x^5 + x^4 + x^3 + x^2 + x + 1$
c^{30}	$c^4 + c^2 + c + 1$	$x^5 + x^4 + x^3 + x^2 + x + 1$
c^{31}	1	$x - 1$

2.10. Корректирующие коды

Рассмотрим вопрос использования теории полей многочленов для защиты информации от помех в канале связи. Считается, что помехи в канале связи действуют независимо от нас, и мы не в состоянии повлиять на случайное изменение нуля на единицу, и наоборот; мы можем лишь на выходе канала связи исправить кодовое слово, восстановив его первоначальную форму. С этой целью и используются специальные *корректирующие коды*, которые основываются на введении информационной *избыточности*. При корректирующем кодировании в каждое кодовое слово, помимо информационных символов, вводят *проверочные* или *кор-*

ректирующие. Например, можно ввести лишь один корректирующий символ в конце информационного слова, для которого определить: 0 — число единиц в кодовом слове четно и 1 — число единиц в кодовом слове нечетно. Если принятое кодовое число имеет четное число единиц, а корректирующий символ равен 1, то в канале связи произошел сбой. При регистрации сбоя осуществляется повторная передача сообщения. Такой корректирующий код с проверкой на четность единиц в информационном слове используется для контроля передачи информации между отдельными регистрами компьютера. Это самый простой способ проверки. Для контроля считываемой информации из оперативной памяти компьютера используются так называемые *коды Хэмминга*. *Циклические коды* применяются в основном при передаче данных между компьютером и периферийными устройствами, в частности, дисковыми. В свою очередь, циклические коды являются подклассом в большом классе *линейных кодов*, удовлетворяющих дополнительным структурным требованиям. Важность циклических же кодов обусловлена еще и тем, что они приводят к очень эффективным процедурам шифровки и дешифровки, легко реализуемым с помощью логических схем. Рассмотрим кратко принцип этого кодирования.

Информационное сообщение $a = a_0a_1 \dots a_{k-1}$ будем записывать с помощью многочлена:

$$a(x) = a_0 + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1}.$$

Если многочлен $a(x)$ умножить на x^m , то символы, составляющие сообщение, будут коэффициентами при более высоких степенях. Далее $a(x)x^m$ разделим на примитивный многочлен $g(x)$, тем самым найдя частное от деления $p(x)$ и остаток $r(x)$. Зашифрованное информационное слово определится многочленом:

$$f(x) = a(x)x^m - r(x) - g(x)p(x),$$

степень которого равна $n = k + m$. Кодовое слово f будет состоять из k информационных и m проверочных символов. В случае, когда полученное слово f' совпадает с переданным словом f , то при делении многочлена $f'(x)$ на $g(x)$ получается нулевой остаток $r(x)$. Но если остаток отличен от нуля, то в канале связи произошел сбой:

$$f'(x) = g(x)p(x) + r(x), \quad \text{где } r(x) \neq 0.$$

Пусть $a = 1001$, $k = 4$, $m = 3$, $n = 7$, $g(x) = 1 + x + x^3$ — примитивный многочлен. Найдем многочлен, отвечающий коду a : $a(x) = 1 + x^4$;

$$x^3a(x) = g(x)p(x) + r(x) = (1 + x + x^3)(x + x^3) + (x + x^2);$$

$$f(x) = x + x^2 + x^3 + x^6; \quad f = 0111001.$$

В кодовом слове f первые три символа 011 являются проверочными, последние четыре 1001 — информационными. Пусть при передаче f произошел сбой и мы приняли слово $f' = 0111011$. При делении многочлена $f'(x)$ на $g(x)$ получаем остаток $r(x) = 1 + x + x^2$, что соответствует коду ошибки $r = 111$. Если сбой произойдет не в шестом символе, как у нас, а в любом другом месте, то код ошибки изменится.

Существует несколько иной способ кодирования и декодирования информации, а именно, при шифровке многочлен информационного слова $a(x)$ умножается на порождающий многочлен $g(x)$; так получается многочлен $f(x)$. При де-

шифровке кодовый многочлен $f(x)$ умножается на проверочный $h(x)$, в результате получим:

$$A(x) = f(x)h(x) = a(x)g(x)h(x) = a(x)(x^n + 1) = a(x)s(x)a(x),$$

где $s(x)$ — синдром ошибки, выполняющий роль кода ошибки: $s = r$. При такой форме кодирования при том же информационном слове и порождающем многочлене, что и в предыдущем случае, сформируется другой кодовый многочлен:

$$f(x) = (1 + x^3)(1 + x + x^3) = 1 + x + x^4 + x^6, \quad f = 1100101.$$

В процессе декодирования получим нулевой синдром:

$$A(x) = f(x)h(x) = (1 + x + x^4 + x^6)(1 + x + x^2 + x^4) = 1 + x^3 + x^7 + x^{10};$$

$$A = asa = 1001\ 000\ 1001; \quad s = 000.$$

Пусть произошел сбой и было получено слово $f' = 1100001$; тогда в результате декодирования возникнет набор: $A' = 1001\ 111\ 1101$ с синдромом ошибки $s = 111$.

Вместо многочленов можно использовать матрицы. Чтобы получить кодовое слово f , нужно информационное слово a умножить на порождающую матрицу G , т.е. $f = aG$. Так, если $a = 011$ — информационное слово из $k = 3$ символов и задана порождающая матрица G размерности 3×5 , то кодовое слово f будет состоять из $n = 5$ символов, из которых два последних ($m = 2$) являются проверочными:

$$f = aG = (011) \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} = 01110.$$

Откуда же берутся порождающие матрицы G ? Отвечаем: порождающая матрица получается путем последовательного сдвига соответствующего порождающего многочлена $g(x)$ по разрядам вправо. Последовательному сдвигу вправо отвечает умножение $g(x)$ на x^i :

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ x^2g(x) \\ \dots \\ x^{k-1}g(x) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_m & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{m-1} & g_m & \dots & 0 \\ 0 & 0 & g_0 & \dots & g_{m-2} & g_{m-1} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & g_0 & g_1 & \dots & g_m \end{pmatrix}.$$

Порождающая матрица G имеет размерность $(k-1) \times m$, поскольку для сдвига берутся степени x^i в пределах $0 < i < k-1$, а степень порождающего многочлена $g(x)$ равна m . Мы знаем, что каждому порождающему многочлену соответствует проверочный многочлен $h(x)$, который нам удобно записать в порядке убывания степеней:

$$g(x) = g_0 + g_1x + g_2x^2 + \dots + g_mx^m, \quad h(x) = h_kx^k + h_{k-1}x^{k-1} + \dots + h_0,$$

причем $x^n + 1 = g(x)h(x)$, где, напомним, n — общее число символов, k — число информационных, а m — число проверочных символов в кодовом слове. Если существует порождающая матрица G , то должна существовать и соответствующая ей проверочная матрица H . Действительно, такую матрицу можно получить путем последовательного сдвига проверочного многочлена $h(x)$ влево:

$$H = \begin{pmatrix} h(x) \\ xh(x) \\ x^2h(x) \\ \dots \\ x^{m-1}h(x) \end{pmatrix} = \begin{pmatrix} 0 & \dots & 0 & h_k & \dots & h_2 & h_1 & h_0 \\ 0 & \dots & h_k & h_{k-1} & \dots & h_1 & h_0 & 0 \\ 0 & \dots & h_{k-1} & h_{k-2} & \dots & h_0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ h_k & \dots & h_0 & 0 & \dots & 0 & 0 & 0 \end{pmatrix}.$$

Предположим, у нас есть конкретный порождающий многочлен $g(x) = 1 + x^2 + x^3$. Проверочный многочлен $h(x)$ находится простым делением многочлена $x^7 + 1$ на заданный многочлен $g(x)$; в результате имеем: $h(x) = x^4 + x^3 + x^2 + 1$. В соответствии с вышеприведенными определениями, находим конкретный вид порождающей G и проверочной H матриц:

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad GH^* = (HG^*)^* = 0.$$

Последнее равенство говорит о том, что матрицы G и H ортогональны относительно друг друга (звездочка означает операцию транспонирования матрицы).

Рассмотренные G и H матрицы называются *ленточными*, потому что нули и единицы вдоль обеих диагоналей этих матриц образуют своеобразные ленты. Но любая ленточная матрица может быть сведена к *систематическому* виду:

$$G' = (E_{k \times k} \mid G_{m \times k}), \quad H' = (H_{k \times m} \mid E_{m \times m}),$$

где $E_{k \times k}$ и $E_{m \times m}$ — единичные матрицы.

Существуют по крайней мере два способа сведения ленточных матриц к систематическому виду. Первый наиболее надежный способ состоит в нахождении ряда остаточных многочленов. Если $r_i(x)$ — остаточный многочлен от деления x^i на порождающий многочлен $g(x)$, то сумма элементов $r_i(x) + x^i$ дают строки систематической матрицы G . Аналогичным способом находятся строки проверочной матрицы H . Второй способ заключается в том, чтобы найти соответствующие линейные комбинации строк или столбцов исходных матриц ленточного типа. Найдем G и H для нашего предыдущего случая:

$$\begin{aligned} G: \quad & x^3 = (x^3 + x^2 + 1) \cdot 1 + x^2 + 1, & 1 + x^2 + x^3; \\ & x^4 = (x^3 + x^2 + 1) \cdot (x + 1) + x^2 + x + 1, & 1 + x + x^2 + x^4; \\ & x^5 = (x^3 + x^2 + 1) \cdot (x^2 + x + 1) + x + 1, & 1 + x + x^5; \\ & x^6 = (x^3 + x^2 + 1) \cdot (x^3 + x^2 + 1) + x^2 + x, & x + x^2 + x^6. \\ H: \quad & x^6 = (x^4 + x^3 + x^2 + 1) \cdot (x^2 + x) + x^3 + x^2 + x, & x^6 + x^3 + x^2 + x; \\ & x^5 = (x^4 + x^3 + x^2 + 1) \cdot (x + 1) + x^2 + x + 1, & x^5 + x^2 + x + 1; \\ & x^4 = (x^4 + x^3 + x^2 + 1) \cdot 1 + x^3 + x^2 + 1, & x^4 + x^3 + x^2 + 1. \end{aligned}$$

$$G' = \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array} \right), \quad H' = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array} \right).$$

Эти две систематические матрицы можно было бы получить путем сложения векторов-столбцов исходных ленточных матриц (напоминаем, счет столбцов для матрицы G начинается с нуля, а для матрицы H — с шести).

$$G': \quad 0' = 1 + 2, 1' = 1 + 5, 2' = 3, 3' = 0, 4' = 1, 5' = 4 + 1, 6' = 6;$$

$$H': \quad 0' = 5, 1' = 3, 2' = 4, 3' = 2, 4' = 6, 5' = 1, 6' = 0.$$

Теперь поясним, как составить проверочные соотношения и определить коды ошибок s_i по известной проверочной матрице. С этой целью выпишем три равенства, отвечающих строкам матрицы H' :

$$s_1 = h_6 + h_3 + h_2 + h_1 = 0, \quad s_2 = h_5 + h_2 + h_1 + h_0 = 0, \quad s_3 = h_4 + h_3 + h_2 + h_0 = 0.$$

При ошибке в символе h_0 суммы s_2 и s_3 изменятся на 1, а при ошибке в h_1 не будут равны нулю суммы s_1 и s_2 . Таким образом, можно составить все коды ошибок для всех символов (табл. 2.87). При одновременном появлении ошибок в двух символах, например в h_5 и h_6 , коды ошибок будут складываться; в данном конкретном случае код становится таким же, как и при одиночной ошибке в символе h_1 . Поэтому, характеризуя код с точки зрения помехозащищенности, мы должны сказать, что он обнаруживает и исправляет любые одиночные ошибки, а также обнаруживает, но не исправляет двойные ошибки.

Таблица 2.87

h_i	s_1, s_2, s_3
h_0	011
h_1	110
h_2	111
h_3	101
h_4	001
h_5	010
h_6	100

Помехозащищенность кода можно выяснить на основе известного кодового расстояния. Кодовое расстояние между словами a и b определяется как число несовпадающих символов в этих словах, например: $a = 10110$, $b = 11011$, здесь расстояние равно $d(a, b) = 3$. Корректирующий код способен исправлять любые комбинации из m и меньшего числа ошибок, если его минимальное кодовое расстояние удовлетворяет условию: $d_{\min} \geq 2m + 1$. Для иллюстрации этого неравенства приведем следующий пример. Возьмем три рядом стоящих слова (термин «рядом стоящие» означает, что между этими словами других слов быть не может): $a = 0100$, $b = 0110$, $c = 0010$. Для получения соответствующих кодовых слов, их нужно умножить на порождающую матрицу, которую мы возьмем из предыдущего примера G' : $f_a = 1110100$, $f_b = 0010110$, $f_c = 1100010$. Кодовые расстояния между этими словами равны: $d(f_a, f_b) = 3$, $d(f_b, f_c) = 4$, $d(f_a, f_c) = 3$. Предположим, что при передаче информации в канале связи произошел сбой и второе кодовое слово изменилось на $f'_b = 0110110$. Тогда по минимальному кодовому расстоянию мы все же сможем определить, что из трех возможных слов передавалось скорее всего слово f_b , так как: $d(f_a, f'_b) = 2$, $d(f_b, f'_b) = 1$, $d(f_c, f'_b) = 3$. Если же были допущены

ны две ошибки, например, в пятом и четвертом разрядах, то становится непонятным, какое из кодовых слов f_b или f_c – на самом деле передавалось, так как $f_b'' = 0111110$, $d(f_a, f_b'') = 3$, $d(f_b, f_b'') = 2$, $d(f_c, f_b'') = 2$. Отсюда, чем больше минимальное кодовое расстояние между словами, тем лучше защищен код от помех. По вышеприведенному неравенству можно установить, что при $d_{\min} = 3$ число обнаруженных и исправленных ошибок не может быть больше одной ($m \leq 1$), поскольку $m \leq (d_{\min} - 1)/2$.

К сказанному добавим, что все коды ошибок, представленные в табл. 2.87, можно было бы установить и по проверочной матрице H' . С этой целью каждое кодовое слово необходимо было бы умножить на транспонированную матрицу H' : $s = f(H')^*$. Все рассуждения мы проводим на матрицах, записанных именно в систематической форме; если брать ленточные матрицы, то информационные и проверочные символы в кодовых словах окажутся перемешанными, что вызывает определенные неудобства при декодировании. Для закрепления последнего материала, исследуем помехозащищенность нетривиального кода с $n = 15$ и $g(x) = 1 + x^4 + x^6 + x^7$. Делением $x^{15} + 1$ на $g(x)$ находим проверочный многочлен $h(x) = x^8 + x^7 + x^6 + x^4 + 1$. Порождающая и проверочные матрицы в ленточной форме имеют вид:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Методом остаточного многочлена находим эти же матрицы, но записанные уже в систематической форме:

$$G' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad H' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Комбинируя столбцы исходных ленточных матриц, мы можем лишний раз убедиться в правильности нахождения этих матриц.

$$\begin{aligned} G': \quad 0' &= 0 + 8, \quad 1' = 1 + 9, \quad 2' = 2 + 10, \quad 3' = 3 + 11, \quad 4' = 5 + 6, \quad 5' = 6 + 7, \\ 6' &= 7, \quad 7' = 0, \quad 8' = 1, \quad 9' = 2, \quad 10' = 3, \quad 11' = 0 + 4, \quad 12' = 1 + 5, \\ 13' &= 13 + 14, \quad 14' = 14. \\ H': \quad 0' &= 3 + 13, \quad 1' = 0 + 6 + 12, \quad 2' = 11 + 5, \quad 3' = 3 + 6 + 14, \quad 4' = 9 + 14, \\ 5' &= 8 + 13 + 14, \quad 6' = 0 + 1 + 12, \quad 7' = 4 + 14, \quad 8' = 14, \quad 9' = 1 + 5, \\ 10' &= 0 + 4, \quad 11' = 3, \quad 12' = 2, \quad 13' = 1, \quad 14' = 0. \end{aligned}$$

Проверочные соотношения равны:

$$\begin{aligned}s_1 &= h_{14} + h_7 + h_6 + h_5 + h_3 = 1, \\s_2 &= h_{13} + h_6 + h_5 + h_4 + h_2 = 1, \\s_3 &= h_{12} + h_5 + h_4 + h_3 + h_1 = 1, \\s_4 &= h_{11} + h_4 + h_3 + h_2 + h_0 = 1, \\s_5 &= h_{10} + h_7 + h_6 + h_5 + h_2 + h_1 = 0, \\s_6 &= h_9 + h_6 + h_5 + h_4 + h_1 + h_0 = 0, \\s_7 &= h_8 + h_7 + h_6 + h_4 + h_0 = 1.\end{aligned}$$

Все коды ошибок представлены в табл. 2.88.

Таблица 2.88

h_i	$s_1s_2s_3s_4s_5s_6s_7$	h_i	$s_1s_2s_3s_4s_5s_6s_7$
h_0	1110010	h_8	1111000
h_1	1101111	h_9	1111011
h_2	1010101	h_{10}	1111101
h_3	0100001	h_{11}	1110001
h_4	1000010	h_{12}	1101001
h_5	0001111	h_{13}	1011001
h_6	0011110	h_{14}	0111001
h_7	0111100	—	—

Помехозащищенность исследуем на трех кодовых словах:

$$a = 00110011, b = 10110011, c = 10010011,$$

которые дают следующие защищенные последовательности:

$$f_a = 101000000110011, f_b = 001010110110011, f_c = 110001110010011.$$

Расстояния между словами: $d(f_a, f_b) = 4$, $d(f_b, f_c) = 6$, $d(f_a, f_c) = 6$. Так как $m \leq (d_{\min} - 1)/2 = 3/2$, данный код может обнаружить и исправить не более одной ошибки. Действительно, если в 10 и 14 разрядах одновременно произойдет сбой, т.е. $f_b'' = 101000110110011$, появятся два одинаковых расстояния: $d(f_a, f_b'') = 2$, $d(f_b, f_b'') = 2$, $d(f_c, f_b'') = 4$, и мы не сможем определить истинное слово.

Для задания *произвольного* кода нужно указать полный список кодовых слов. Например, следующий список слов имеет довольно приличную (для своего значения $n = 11$) степень защищенности:

11000011000	10100100001	00110011000	00000011110	00100101000
10001001100	10010001001	01010000110	00010110001	00100110010
10000010101	10010100100	00001100101	00001111000	01000100011
11001100000	00110000011	11110000000	01100001010	01000110100
01011000001	10101010000	10001000011	10010010010	10000101010
01000001101	00111100000	00011010100	00011001010	01010101000

Для задания *циклического* кода достаточно указать всего лишь один порождающий многочлен $g(x)$, а для задания *линейного* кода C нужно задать список базисных кодовых векторов, в роли которых, как мы убедились, могут выступать ко-

довые многочлены $f(x)$. Линейный код C является циклическим только тогда, когда C является идеалом в кольце многочленов $P_n(x)$ (понятие идеала мы ввели в предыдущем подразделе). Во всяком идеале C существует порождающий многочлен $g(x)$, которому кратен всякий многочлен идеала C . Если C — идеал, то для всякого кодового многочлена $f(x)$ можно получить циклические сдвиги $xf(x)$, $x^2f(x)$, $x^3f(x)$, ... $\in C$, т.е. сдвиги снова являются кодовыми многочленами; и наоборот, если C — циклический код, то для всякого кодового многочлена $f(x)$ его сдвиги будут кодовыми многочленами. Рассмотренные кодовые слова суть векторы линейного пространства G над полем Галуа $GF(q)$. Если выразиться точнее, то G является лишь подпространством пространства E , поскольку у него имеется ортогональное дополнение H :

$$E = \left(\begin{array}{cc} E_{k \times k} & G_{m \times k} = H_{k \times m}^* \\ H_{k \times m} = G_{m \times k}^* & E_{m \times m} \end{array} \right),$$

здесь символ «звездочка» означает транспонирование.

Если f есть n -мерный кодовый вектор, полученный из информационного слова a с помощью порождающей матрицы G , то произведение $fH^* = aGH^* = 0$, т.е. H^* переводит любой вектор f из линейного пространства G в нулевой вектор; если же попадет такой вектор f' , который не будет принадлежать линейному пространству G , то матрица H^* уже не сможет перевести его в нулевой вектор, сигнализируя нам об этом соответствующим синдромом s . Примером классического линейного кода является код Хэмминга (n, k) , для которого выполняется условие: $n = 2^m - 1$. Согласно этому условию в поле Галуа $GF(2)$ будем иметь следующие коды Хэмминга: $(7, 4)$, $(15, 11)$, $(31, 26)$, $(63, 57)$, $(127, 120)$, ...; в поле $GF(2^2)$: $(5, 3)$, $(21, 18)$, $(85, 81)$, $(341, 336)$, ...; в поле $GF(2^3)$: $(9, 7)$, $(73, 70)$, $(585, 581)$, ...; в поле $GF(2^4)$: $(17, 15)$, $(273, 270)$, Существует код Хэмминга $(13, 10)$ над полем $GF(3)$ с проверочной матрицей

$$H = \left(\begin{array}{cccccccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 1 & 2 & 0 \end{array} \right) \begin{array}{l} 1 \\ 0 \\ 0 \end{array}$$

по которой нетрудно найти порождающую матрицу G . Существуют различные модификации кодов Хэмминга, в частности, из кода (n, k) можно получить код $(n+1, k)$, который способен исправлять одинарную ошибку и обнаруживать двойную. Так, для модифицированного кода Хэмминга $(8, 4)$ проверочной матрицей служит

$$H = \left(\begin{array}{cccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array} \right).$$

Тогда к трем вышеприведенным проверочным соотношениям добавится еще одно: $s_4 = h_7 + h_6 + h_5 + h_4 + h_3 + h_2 + h_1 + h_0 = 0$. Если оно не выполняется, это означает, что произошла одиночная ошибка, которую можно исправить с помощью первых трех соотношений. Если последнее соотношение выполняется, но не вы-

полняется по крайней мере одно из первых трех, то имеет место двойная ошибка, хотя исправить ее будет нельзя.

Код Хэмминга (7, 4) нами уже рассмотрен, причем мы показали, что он может быть преобразован в циклический код с ленточной матрицей G , образованной от порождающего многочлена $g(x) = 1 + x^2 + x^3$. Для кодирования информации и исправления сразу нескольких ошибок Боуз, Чоудхури и Хиквингем (сокращенно: код БЧХ) предложили использовать сразу несколько порождающих или, как мы говорили в предыдущем подразделе, неприводимых многочленов $g_i(x)$. Порождающий многочлен БЧХ-кода можно представить в виде

$$g(x) = \text{НОК}[g_1(x), g_2(x), g_3(x), \dots, g_t(x)],$$

где $g_i(x)$ — неприводимые многочлены, t — число исправленных ошибок. Так, для исправления двух ошибок ($t = 2$) с длиной кодового слова $n = 2^4 - 1 = 15$ получаем следующий порождающий многочлен:

$$\begin{aligned} g(x) &= \text{НОК}[g_1(x), g_2(x), g_3(x), g_4(x)] = \\ &= \text{НОК}[x^4 + x + 1, x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1, x^4 + x + 1] = \\ &= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^7 + x^6 + x^4 + 1, \end{aligned}$$

здесь $m = 8$, $k = 7$, т.е. мы получили корректирующий БЧХ-код (15, 7), одновременно исправляющий два любых сбоя в канале связи при передаче $N = 2^k = 128$ сообщений. Неприводимые многочлены $g_1(x)$, $g_2(x)$, $g_3(x)$ и $g_4(x)$ предварительно были нами найдены и теперь только взяты из табл. 2.82.

Для исправления трех ошибок ($t = 3$) имеем следующий порождающий элемент:

$$\begin{aligned} g(x) &= \text{НОК}[g_1(x), g_2(x), g_3(x), g_4(x), g_5(x), g_6(x)] = (x^4 + x + 1) \times \\ &\times (x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1, \end{aligned}$$

который дает (15, 5) БЧХ-код. При $t = 4, 5, 6, 7$ будем иметь одинаковые порождающие многочлены, отличающиеся от $x^{15} + 1$ на множитель $x + 1$, а от предыдущего случая на множитель $x^4 + x^3 + 1$, т.е.

$$g(x) = x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

Этот БЧХ-код способен нести лишь один бит информации (15, 1).

Аналогичным образом мы можем найти порождающие многочлены для других БЧХ-кодов. Воспользовавшись полными таблицами неприводимых многочленов (табл. 2.83 – табл. 2.86) мы способны исправить до 32 одновременно произошедших ошибок (табл. 2.86). Любопытно сравнить помехозащищенность БЧХ-кода над полем многочленов $GF(2^4)$ (табл. 2.82) и $GF(4^2)$ (табл. 2.89).

Порождающий многочлен для исправления одиночной ошибки в поле $GF(4^2)$, кажется, принципиально ничем не отличается от порождающего многочлена в поле $GF(2^4)$ ($g(x) = x^4 + x + 1$):

$$g(x) = \text{НОК}[g_1(x), g_2(x)] = (x^2 + x + 2)(x^2 + x + 3) = x^4 + 2x^3 + 2x^2 + x + 3,$$

который тоже дает код (15, 1).

c^i	$m \cdot c + n$	$g_i(x)$
c^1	c	$x^2 + x + 2$
c^2	$c + 2$	$x^2 + x + 3$
c^3	$3c + 2$	$x^2 + 3x + 1$
c^4	$c + 1$	$x^2 + x + 2$
c^5	2	$x + 2$
c^6	$2c$	$x^2 + 2x + 1$
c^7	$2c + 3$	$x^2 + 2x + 2$
c^8	$c + 3$	$x^2 + x + 3$
c^9	$2c + 2$	$x^2 + 2x + 1$
c^{10}	3	$x + 3$
c^{11}	$3c$	$x^2 + 3x + 3$
c^{12}	$3c + 1$	$x^2 + 3x + 1$
c^{13}	$2c + 1$	$x^2 + 2x + 2$
c^{14}	$3c + 3$	$x^2 + 3x + 3$
c^{15}	1	$x + 1$

Порождающий многочлен для исправления двух ошибок для $GF(2^4)$ был $g(x) = x^8 + x^7 + x^6 + x^4 + 1$, что давал код $(15, 7)$; для $GF(4^2)$ будем иметь уже код $(15, 9)$:

$$\begin{aligned}
 g(x) &= \text{НОК}[g_1(x), g_2(x), g_3(x), g_4(x)] = \\
 &= (x^2 + x + 2)(x^2 + x + 3)(x^2 + 3x + 1) = \\
 &= x^6 + 3x^5 + x^4 + x^3 + 2x^2 + 2x + 1.
 \end{aligned}$$

Степень многочлена $g(x)$ получилась на два порядка ниже, а это значит, что данный код при той же помехозащищенности имеет преимущество: из 15 символов, отведенных на каждое кодовое слово, у него вместо 7 будет уже 9 информационных символов, причем каждый символ принимает значения не 0 и 1, а 0, 1, 2 и 3.

3. Графы

Доказательства истинности логических тождеств и клауз мало чем отличаются от вычислений, типа

$$(a + b)^2 = a^2 + 2ab + b^2 \quad \text{или} \quad 3 \times (4 + 5) < 30.$$

Изучение групп также свелось к исчислению неких математических структур, основанных на разложениях, типа

$$2 \times 2 \times 2 = 8, \quad 3 \times 3 \times 3 = 27, \quad 2 \times 3 \times 5 = 30, \dots,$$

к сравнению этих равенств между собой, к исследованию влияния состава простых сомножителей на природу групп 8, 27, 30 и т.д. порядков. При этом большая часть объема изложенного нами материала была посвящена конкретным группам, анализу их строения и состава, но мы не касались абстрактных теорем, которые, собственно, образуют алгебраическую теорию групп. Аналогичный подход мы попытаемся использовать при изучении и графов. Нас не будут интересовать многочисленные отвлеченные теоремы, которыми полны учебники, начиная с К. Берж «Теория графов и ее применения» (М.: ИЛ, 1962), О. Оре «Теория графов» (М.: Наука, 1968), Ф. Харари «Теория графов» (М.: Мир, 1973) и др. Критика Ф. Клейна в отношении изложения групп нам представляется во многом справедливой и в отношении графов.

Изложение теории графов в современных учебниках начинается с рассмотрения довольно очевидного синтаксиса и длинного списка дефиниций, где говорится о двух множествах V и X :

Элементы множества V будем называть *вершинами*, а элементы набора X — *ребрами*. В общем случае в наборе X могут встречаться пары с одинаковыми элементами вида (v, v) , а также одинаковые пары. Ребра вида (v, v) называются *петлями*. Одинаковые пары в X называются *кратными* (или *параллельными*) ребрами. Количество одинаковых пар (v, w) в X называется *кратностью* ребра (v, w) . Про множество V и набор X будем говорить, что они определяют *граф с кратными ребрами и петлями* (или *псевдограф*) $G = (V, X)$. Псевдограф без петель называется графом с кратными ребрами (или *мультиграфом*). Если в наборе X ни одна пара не встречается более одного раза, то мультиграф $G = (V, X)$ называется *графом*. Если пары в наборе X являются упорядоченными, то граф называется *ориентированным* (кратко — *орграфом*). Ребра орграфа называются *дугами*. Если пары в наборе X являются неупорядоченными, то граф называется *неориентированным* графом (или просто графом). Ребра в неориентированном графе (в отличие от дуг в орграфе) будем обозначать $\{v, w\}$. Неориентированные графы будем обозначать буквой G или G с индексами (например, $G_a, G_i, \dots$), а орграфы — буквой D или D с индексами (например, $D_a, D_i, \dots$). Кроме того, договоримся обозначать вершины буквами v, u, w (без индексов или с индексами), а ребра и дуги — буквами x, y, z (без индексов или с индексами).

Всюду далее будем соответствующую некоторому графу геометрическую конфигурацию, в которой вершины изображены кружочками, а ребра — линиями, соединяющими соответствующие вершины, называть *изображением* этого графа. При изображении орграфа направления дуг будем отмечать стрелками, примыкающими к их концам... <Далее идут примеры.>

Если $x = \{v, w\}$ — ребро графа, то вершины v, w называются *концами* ребра x ; в этом случае также говорят, что ребро x *соединяет* вершины v, w .

Если $x = (v, w)$ — дуга орграфа, то вершина v называется *началом*, а вершина w — *концом* дуги x ; в этом случае также говорят, что дуга x *исходит* из вершины v и *заходит* в вершину w .

Если вершина v является концом (началом или концом) ребра (дуги) x , то говорят, что v и x *инцидентны*.

Вершины v, w графа $G = (V, X)$ называются *смежными*, если $\{v, w\} \in X$. Два ребра называются смежными, если они имеют общую вершину.

Степенью вершины v графа G называется число $\delta(v)$ ребер графа G , инцидентных вершине v . Вершина графа, имеющая степень 0, называется *изолированной*, а степень 1 — *висячей*¹.

Наверное, необходимость этих и других подобных им определений не вызовет ни у кого сомнений. Тем не менее нам кажется не слишком важным, как назвать точки, соединенные линиями: «графом», «орграфом», «мультиграфом», «псевдографом». Графы, построенные на основе реальных структур, слишком разнообразны, чтобы их классифицировать по тем признакам, о которых говорили родоначальники этой науки. Нас гложет сомнение: нужно ли вообще различать такие понятия, как «ребро» — «дуга», «контур» — «цикл», «путь» — «маршрут», «центр» — «центроид» и т.д. Ведь на практике (а графы в основном имеют прикладное значение) все эти ряды терминов забываются и заменяются каким-либо одним словом: «граф», «ребро», «цикл», «путь», «центр». Информатику трудно понять, почему граф с петлей уже не является полноценным графом, а только «псевдографом». Эти еретические настроения толкнули нас на введение более вольной терминологии. В частности, следующим не слишком принципиальным различием, взятым из цитируемого учебника, мы безжалостно пожертвовали:

Введем понятие *маршрута* для графа $G = (V, X)$ (и соответственно понятие *пути* для орграфа $D = (V, X)$). Последовательность

$$v_1 x_1 v_2 x_2 v_3 \dots x_k v_{k+1} \quad (4.4)$$

(где $k \geq 1$, $v_i \in V$, $i = 1, \dots, k+1$, $x_j \in X$, $j = 1, \dots, k$), в которой чередуются вершины и ребра (дуги) и для каждого $j = 1, \dots, k$ ребро (дуга) x_j имеет вид $\{v_j, v_{j+1}\}$ ((v_j, v_{j+1})), называется *маршрутом*, соединяющим вершины v_1, v_{k+1} (путем из v_1 в v_{k+1}), при этом v_1 называется *начальной*, v_{k+1} — *конечной* вершинами маршрута (пути) (4.4), а остальные вершины *внутренними*. Одна и та же вершина может одновременно оказаться начальной, конечной и внутренней. Последовательность вершин в маршруте определяет на ребрах, входящих в маршрут, ориентацию. Заметим в этой связи, что ориентацию некоторого ребра $x = (v, w)$ всегда можно указать при записи его как пары вершин. Например, запись $\{v, w\}$ указывает на то, что ребро x ориентировано от вершины v к вершине w .

Пример 4.7.

1. Последовательность $v_1 x_1 v_2 x_2 v_3 x_3 v_4$ — маршрут, соединяющий вершины v_1, v_4 в графе G (см. пример 4.2).

2. Последовательность $v_1 x_1 v_2 x_2 v_3 x_3 v_4$ — путь из v_1 в v_4 в ориентированном псевдографе D (см. пример 4.1).

¹ Нефедов В.Н., Осипова В.А. Курс дискретной математики: Учеб. пособие. — М.: Изд-во МАИ, 1992, с. 161–163.

Замечание 4.5. Последовательность (4.4) можно однозначно восстановить по последовательности

$$x_1, x_2, \dots, x_l \quad (4.5)$$

(если (4.4) — маршрут, предполагается, что в последовательности (4.5) дополнительно указывается ориентация ребер, определяемая маршрутом (4.4)), а следовательно, вместо (4.4) можно использовать более короткую запись (4.5). Отметим далее, что в случае, когда в последовательности (4.4) $x_1, \dots, x_l$ имеют кратности, равные 1, ее можно однозначно восстановить по последовательности вершин

$$v_1, v_2, \dots, v_{l+1} \quad (4.6)$$

а следовательно, вместо (4.4) также можно использовать более краткую запись (4.6). В общем случае вместо последовательности (4.4) можно использовать сокращенную последовательность, в которой опущены все x_i кратности 1.¹

Разве информатик или кто-либо другой из специалистов не в состоянии сам решить, каким словом ему пользоваться — «путь» или «маршрут», — и через какие буквы его маршрут-путь лучше обозначить? Граф — это наглядный образ, достоинство которого как раз и состоит в том, что он требует минимума слов и символов. В приведенном же отрывке это преимущество перечеркивается.

Традиционная теория графов, как нам кажется, перегружена малопродуктивными доказательствами. Вот один из примеров:

Путь в орграфе D из вершины v в вершину w , где $v \neq w$, называется *минимальным*, если он имеет минимальную длину среди всех путей орграфа D из v в w . Аналогично определяется и минимальный маршрут в графе G .

Рассмотрим некоторые свойства минимальных путей (маршрутов).

Утверждение 4.21. *Любой минимальный путь (маршрут) является простой цепью.*

Доказательство проведем для пути (для маршрута оно аналогично). Предположим, что в некотором орграфе D найден минимальный путь $\pi = v_1 v_2 \dots v_l$, где $v_i \neq v_k$, не являющийся простой цепью. Тогда найдутся номера i, j такие, что $1 \leq i < j \leq l$ и $v_i = v_j$. Пусть $i > 1$, $j < l$. Рассмотрим путь $v_1 v_2 \dots v_{i-1} v_{j+1} \dots v_l$. Его длина равна $(i-1) + (l-j) = l - (j-i) < l$, что противоречит минимальности π . Случаи $i=1$ или $j=l$ доказываются аналогично (случая $i=1, j=l$ быть не может в силу $v_i \neq v_k$).²

Определение прямой в геометрии дается через понятие *кратчайшего расстояния* между двумя точками, т.е. предполагается, что представление о *минимальном пути* первично по отношению к свойству линии «быть прямой». Есть что-то очень схоластическое в доказательстве приведенного утверждения; непредвзятый ум этому противится. Мало того, что дается тавтологичная дефиниция (минимальный путь определяется через минимальную длину), здесь еще делается попытка *доказать аксиому*, которая в геометрических терминах гласит: *кратчайшее расстояние между двумя точками является прямой*. Следующее доказательство в этом учебнике посвящено уже «утверждению о минимальности подпути минимального пути».

Подобных утверждений в цитируемом учебнике множество. Однако их *эвристическая* ценность нам представляется далеко не бесспорной. *Исчисление* дискретных объектов — вот по-настоящему эвристическая процедура в математике, которая, наряду с получением нового знания, имеет и доказательную силу. Поэтому, избегая отвлеченных рассуждений, не претендуя на полноту и строгость, сведя к минимуму

¹ Там же, с. 165.

² Там же, с. 182–183.

нормативно-декларативную базу и оперируя исключительно с конкретикой, мы попытались максимально прозрачным образом представить те нехитрые математические объекты, которые чаще всего именуются просто *графами*.

Множество точек (вершин, узлов) и множество линий (ребер, дуг), которые соединяют эти точки, называются *графом* G . Граф G_3 (рис. 3.1а) и ему подобные называются *полным*, поскольку три его вершины связаны между собой линиями. Граф, изображенный на рис. 3.1б, полным уже не назовем, однако линии такого частичного графа образуют *полную цепь*. Цепь называется *полной*, если она связывает все точки графа линиями без образования петель и контуров. Цепи, связывающие только часть точек (рис. 3.1в), мы рассматривать пока не будем и, следовательно, термин «полная» применительно к цепи можно будет опускать без риска быть непонятыми.

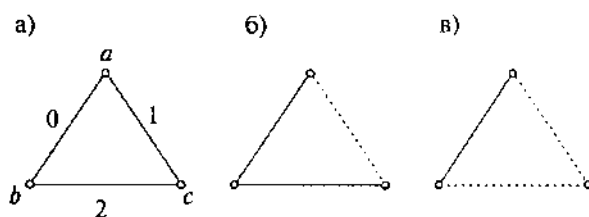


Рис. 3.1

Цепь имеет *голову* и *хвост*. Голова цепи привязывается к какой-либо точке, которую мы будем в этом случае называть *привязкой*. Для графа G_3 , если в качестве привязки выступает точка a , имеем две цепи $abc = 02$, $acb = 12$; если привязкой является точка b , получим еще две цепи — $bac = 01$, $bca = 21$; на-

копец, если c — привязка, то $cab = 10$, $cba = 20$ — цепи. Вместо шести мы на самом деле имеем только три цепи A , B и C , поскольку не столь уж важно, как записать цепь — с головы или с хвоста; отсюда $A = 01 = 10$, $B = 02 = 20$, $C = 12 = 21$.

Одной из тем этого подраздела является поиск *групп преобразования цепей*. Дело в том, что, скажем, цепь 01 переходит в цепь 02 путем замены линии 1 на линию 2 при этом линия 0 остается на месте. Этот переход можно записать как $\bar{1}2$ или $2\bar{1}$. Обратный переход цепей друг в друга осуществляется при противоположной замене линий, т.е. $\bar{2}1 = 1\bar{2}$. Последовательная замена линий: сначала $\bar{1}2$, затем $\bar{2}1$, оставляет исходную цепь 01 тождественной самой себе. Но осуществление двух различных замен, например, $\bar{1}2$ и $\bar{0}1$ по отношению к исходной цепи 01, приводит к преобразованию: из 01 в 02 и из 02 в 12, что равносильно действию замены 02.

Цепи образуют *субстанционное* множество, а преобразования — *операционное*. При замене отдельных звеньев цепи удобно воспользоваться *аддитивной* записью. В частности, действие преобразования $\bar{m}n$ на цепь lm выразится через суммы:

$$01 + \bar{1}2 = 02, \quad 01 + \bar{0}2 = 12, \quad 02 + \bar{0}1 = 12, \dots,$$

а переходы от одной цепи к другой запишутся через разности, например, преобразование A в B как $A - B = 01 - 02 = 12$, обратное преобразование как $B - A = 02 - 01 = 12$. Все остальные преобразования в G_3 запишутся с помощью следующих простых выражений:

$$\begin{array}{ll}
A - C = 01 - 12 = \bar{02}, & B - C = 02 - 12 = \bar{01}, \\
C - A = 12 - 01 = \bar{02}, & C - B = 12 - 02 = \bar{01}, \\
A - B - A = A - A = \bar{12} + \bar{12} = e, & B - A - B = B - B = \bar{12} + \bar{12} = e, \\
A - C - A = A - A = \bar{02} + \bar{02} = e, & C - A - C = C - C = \bar{02} + \bar{02} = e, \\
B - C - B = B - B = \bar{01} + \bar{01} = e, & C - B - C = C - C = \bar{01} + \bar{01} = e, \\
C - A - B = C - B = \bar{02} + \bar{12} = \bar{01}, & B - A - C = B - C = \bar{12} + \bar{02} = \bar{01}, \\
A - C - B = A - B = \bar{02} + \bar{01} = \bar{12}, & B - C - A = B - A = \bar{01} + \bar{02} = \bar{12}, \\
A - B - C = A - C = \bar{12} + \bar{01} = \bar{02}, & C - B - A = C - A = \bar{01} + \bar{12} = \bar{02}.
\end{array}$$

Перед нами множество элементов, удовлетворяющих всем условиям *группы*: каждое преобразование имеет обратное; последовательное действие прямого и обратного преобразований дает тождественное; для любых трех различных преобразований справедливо условие ассоциативности; наконец, все множество преобразований замкнуто.

Однако в графовых группах имеются и важные отличия по сравнению с ранее рассмотренными группами, а именно: не всякое преобразование g_i может следовать за преобразованием g_j . В частности, преобразование 12 не может следовать за преобразованием 02 , поскольку первое отвечает переходу цепи A в цепь B , а второе — переходу цепи A в цепь C ; между тем разрешен переход от A к B и от B к C . Таким образом, в графах на операционное множество накладывается жесткое ограничение, продиктованное субстабионным множеством. Своенравная природа графа проявляется и в совершенно новом делении элементов группы на классы эквивалентности. Здесь уже нет классов сопряженных элементов и классов смежности, иначе находятся подгруппы, отсутствуют делители и т.д. Покажем на примере группы G_3 от графа Γ_3 , как производится групповой анализ графа.

Пусть вершина a треугольника, изображенного на рис. 3.1а, является привязкой. Следовательно, она находится в особом положении относительно двух других вершин треугольника — b и c . Так возникают два класса вершин — $\{a\}$ и $\{b, c\}$. Стороны треугольника также разбиваются на два класса в зависимости от степени удаленности от привязки — $\{0, 1\}$ и $\{2\}$. Это деление на классы пока никак не проявляется на строении группы G_3 . Привязка a определяет две цепи — B и C , для которых возможны переходы 01 и $0\bar{1}$, принадлежащие одному классу. Вместе с тождественным преобразованием они дают элементарную подгруппу $G_{3a} = \{e, \bar{01}, 0\bar{1}\}$. Каждая привязка определяет свою подгруппу: $G_{3b} = \{e, \bar{02}, 0\bar{2}\}$, $G_{3c} = \{e, 12, \bar{12}\}$. Все вместе элементы G_{3a} , G_{3b} и G_{3c} образуют графовую группу преобразований цепей в треугольнике G_3 , состоящую из семи элементов:

$$G_3 = \{e, \bar{01}, 0\bar{1}, \bar{12}, 1\bar{2}, \bar{02}, 0\bar{2}\}.$$

В процессе формирования группы G_3 была установлена и соответствующая иерархия элементарных подмножеств, которую, как мы знаем, удобно представлять в виде *решетки* $S(G_3)$. Если наши подгруппы обозначить через числа 1, 2, 3, тождественный элемент через 0, то *отношение порядка* между подгруппами $S(G_3)$ будет выглядеть так, как это показано на рис. 3.2.

Прежде чем переходить к анализу следующей группы, обратим внимание на то, что, очевидно, наименьшей группой преобразова-

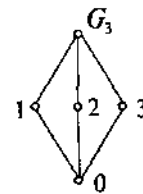


Рис. 3.2

ния цепей является $G_2 = \{e\}$, которая оставляет свою единственную цепь, соединяющую две вершины, в покое. Группа G_3 является первой нетривиальной графовой группой преобразования цепей с двумя образующими, неоднозначно определенными, например, такими: $a = \bar{0}1$, $b = \bar{1}2$. Тогда все остальные элементы группы G_3 выразятся следующим образом:

$$G_3 = \{e, a, \bar{a}, b, \bar{b}, ab, \bar{ab}\}.$$

где $e = a + \bar{a} = b + \bar{b}$, $ab = a + b = \bar{0}1 + \bar{1}2 = \bar{0}2$, $\bar{ab} = \bar{a} + \bar{b} = \bar{0}\bar{1} + \bar{1}\bar{2} = \bar{0}\bar{2}$.

Не забудем сказать и о том, что все графовые группы коммутативны и нечетны. Проявлением аддитивной сущности графовых групп является факт отсутствия степеней образующих. Для мультипликативных подстановок было справедливо условие:

$$\text{если } a \cdot b = c, \text{ то } a = c \cdot b^{-1} \text{ и } b = a^{-1} \cdot c;$$

для аддитивных реберных подстановок истинным является аналогичный закон с учетом коммутативности:

$$\text{если } a + b = c, \text{ то } a = b + c \text{ и } b = a + c.$$

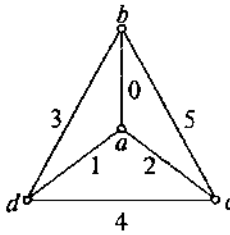


Рис. 3.3

На рис. 3.3 изображен граф T_4 , представляющий соответствующую графовую группу G_4 , переводящую полные цепи тетраэдра друг в друга.

Пусть для начала вершина a послужит нам привязкой. Тогда вершины и ребра тетраэдра разобьются на классы эквивалентности: вершины на $\{a\}$ и $\{b, c, d\}$; ребра на $\{0, 1, 2\}$ и $\{3, 4, 5\}$. Относительно привязки a существует шесть цепей:

$$A = abcd = 054, C = acdb = 243, E = adbc = 135,$$

$$B = abdc = 034, D = acbd = 253, F = adcb = 145.$$

Преобразования цепей разбиваются на несколько классов. Прежде всего выделяются два класса, в первом из которых участвуют ребра из класса $\{0, 1, 2\}$, во втором — ребра из класса $\{3, 4, 5\}$:

$$\begin{aligned} C_{a1}: \quad A - F = \bar{0}1, \quad B - C = \bar{0}2, \quad C_{a2}: \quad A - B = \bar{3}5, \quad E - F = \bar{3}4, \\ F - A = \bar{0}\bar{1}, \quad C - B = \bar{0}\bar{2}, \quad B - A = \bar{3}5, \quad F - E = \bar{3}\bar{4}, \\ D - E = \bar{2}1, \quad E - D = \bar{2}\bar{1}, \quad C - D = \bar{4}5, \quad D - C = \bar{4}\bar{5}. \end{aligned}$$

Третий класс C_{a3} определяется последовательным преобразованием, взятым из класса C_{a1} и C_{a2} , или сначала из C_{a2} , потом из C_{a1} , т.е. по формуле:

$$C_{a3} = \{C_{a1} - C_{a2}, C_{a2} - C_{a1}\}.$$

Конкретно — класс C_{a3} :

$$\begin{aligned} A - F - E = A - E = \bar{1}0 \bar{3}4, \quad E - F - A = E - A = \bar{1}0 \bar{3}\bar{4}, \\ F - A - B = F - B = \bar{1}0 \bar{5}3, \quad B - A - F = B - F = \bar{1}0 \bar{5}\bar{3}, \\ A - B - C = A - C = \bar{2}0 \bar{3}5, \quad C - B - A = C - A = \bar{2}0 \bar{3}\bar{5}, \\ B - C - D = B - D = \bar{2}0 \bar{5}4, \quad D - C - B = D - B = \bar{2}0 \bar{5}\bar{4}, \\ D - E - F = D - F = \bar{2}1 \bar{3}4, \quad F - E - D = F - D = \bar{2}1 \bar{3}\bar{4}, \\ E - D - C = E - C = \bar{2}1 \bar{4}5, \quad C - D - E = C - E = \bar{2}1 \bar{4}\bar{5}. \end{aligned}$$

Четвертый класс C_{a4} определяется формулой:

$$C_{a4} = \{C_{a1} \cap C_{a2} \cap C_{a1}, C_{a2} \cap C_{a1} \cap C_{a2}\}.$$

$$C_{a4}: \begin{aligned} A - F - E - D = A - D = \overline{20} \overline{34}, & \quad D - E - F - A = D - A = \overline{20} \overline{34}, \\ B - C - D - E - B = E - \overline{10} \overline{54}, & \quad E - D - C - B - E = \overline{10} \overline{54}, \\ C - B - A - F = C - F = \overline{12} \overline{53}, & \quad F - A - B - C - F = \overline{12} \overline{53}. \end{aligned}$$

По рисунку графа Γ_4 (рис. 3.3) можно установить, что в подстановках класса C_{a3} ребра $\{0, 1, 2\}$ расположены относительно ребер $\{3, 4, 5\}$ несколько иначе, чем они расположены в классе C_{a2} . Полезно обратить внимание и на другое. В цепи A ребра чередуются как $0, 5, 4$; в цепи C как $2, 4, 3$. При переходе от цепи A к цепи C происходит исчезновение ребер $0, 5$ и появление ребер $1, 3$. Вместе с тем ребро 4 , расположенное в хвосте цепи A , оказывается в середине цепи C . При переходе от цепи A к цепи D сохраняющееся ребро 5 уже не меняет своего серединного положения. В индивидуальных реберных заменах $A - C$ и $A - D$ эти факты не получили никакого отражения; замены $\overline{20} \overline{35}$ и $\overline{20} \overline{34}$ ничем принципиальным не отличаются. Но они различимы коллективно при делении реберных подстановок на классы эквивалентности: $A - C$ отнесена к классу C_{a3} , $A - D$ — к классу C_{a4} .

Помимо упомянутых классов, имеется еще один нулевой класс C_{a0} или класс тождественного элемента $\{e\}$, образованный всеми переходами, типа

$$A - A = B - B = \dots = F - F = e.$$

Таким образом, в группе G_{2a} имеется 31 элемент преобразования цепей, которые разнесены по пяти классам эквивалентных преобразований.

Обратимся к поиску подгрупп группы G_{4a} . С этой целью будем последовательно удалять ребра из графа Γ_4 и смотреть, какие из цепей остались, а вместе с ними и ценные преобразования. Сначала удалим ребро 5 . Получим неполный граф Γ_{41} , показанный на рис. 3.4а. В графе Γ_{41} можно провести две цепи $B = 034$ и $C = 243$, в которых ребро 1 не участвует в образовании цепей, поэтому его также можно было бы удалить вместе с ребром 5 . Цепи B и C определяют минимальную группу $\{e, 02, 0\overline{2}\}$. К аналогичному результату приводит удаление по отдельности ребер 3 и 4 : в первом случае от всей группы G_{4a} остается группа $\{e, 01, 0\overline{1}\}$, во втором — $\{e, \overline{12}, 1\overline{2}\}$. Это означает, что класс ребер $\{3, 4, 5\}$ играет важную роль в формировании цепей. Меньшее влияние оказывают ребра из класса $\{0, 1, 2\}$. Удалим ребро 0 , получим граф Γ_{42} (рис. 3.4б).

Прежде всего отметим, что в графе Γ_{42} вершины и ребра распадаются на три класса эквивалентности относительно привязки a : вершины — $\{a\}$, $\{d, c\}$, $\{b\}$; ребра — $\{1, 2\}$, $\{4\}$, $\{3, 5\}$. На пяти ребрах можно составить четыре из шести ранее приведенных цепей: C, D, E и F . Классы переходов от одной цепи к другой здесь будут такими:

$$C_{a1}: \begin{aligned} E - D = \overline{21}, & \quad C_{a4}: C - F = \overline{21} \overline{35}, \\ D - E = \overline{21}, & \quad F - C = \overline{21} \overline{35}; \end{aligned}$$

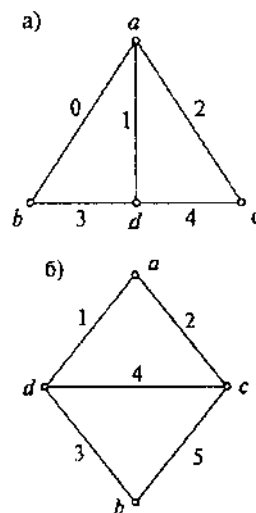


Рис. 3.4

$$\begin{array}{ll}
C_{a2}: & E - F = \overline{43}, & C_{a3}: & C - E = \overline{21} \overline{45}, \\
& F - E = \overline{43}, & & E - C = \overline{21} \overline{45}, \\
& C - D = \overline{45}, & & D - F = \overline{21} \overline{34}, \\
& D - C = \overline{45}, & & F - D = \overline{21} \overline{34}.
\end{array}$$

Таким образом, группа G_{42a} состоит из 13 элементов, включая тождественный. Удалив из графа G_{42} ребро 4, мы удаляем цепи C и F , а вместе с ними все переходы классов C_{a2} , C_{a3} и C_{a4} . Останется группа $\{e, 12, \overline{12}\}$.

Отсутствие ребра 1 в графе Γ_4 дает четыре цепи A, B, C, D , для которых возможны следующие 13 переходов: $\{B - C, C - B, A - B, B - A, D - C, C - D, C - A, A - C, D - B, B - D, A - D, D - A\}$. Отсутствие ребра 2 оставляет цепи A, B, E, F с переходами: $\{A - F, F - A, A - B, B - A, E - F, F - E, E - A, A - E, F - B, B - F, E - B, B - E\}$.

Группа G_{4a} , в которую входят 3 группы 13-го порядка и три группы третьего порядка, сама является подгруппой группы G_4 , в которую входят также подгруппы G_{4b} , G_{4c} , G_{4d} . Структура последних трех подгрупп аналогична только что рассмотренной. Важным вопросом здесь является пересечение элементов этих подгрупп. Дело в том, что цепи A, B, C, D, E, F оканчиваются в трех точках — b, c, d . Следовательно, если в качестве привязки выбрать, скажем, вершину b , то цепи C и F , а вместе с ними и преобразования $C - F, F - C$ войдут в группу G_{4b} . Кроме того, может случиться так, что замена $\underline{tn}$ или $\overline{tn}$ преобразует в группе G_{4a} одну пару цепей, а в группе G_{4b} совершенно другую. Эти обстоятельства нельзя не учитывать при определении порядка групп и построении решетки.

Итак, выберем в качестве привязки вершину b . В этом случае имеем шесть цепей, две из которых нам уже известны:

$$\begin{aligned}
G &= bade = 014, & C &= bdca = 342, & J &= bcad = 521, \\
H &= bacd = 024, & I &= bdac = 312, & F &= bcda = 541.
\end{aligned}$$

Ребра, входящие в эти цепи разделены по двум классам $\{0, 3, 5\}$ и $\{1, 2, 4\}$. Поэтому элементы преобразования группы G_{4b} разбиваются на четыре класса:

$$\begin{array}{lll}
C_{b1}: & H - C = \overline{03}, & C_{b2}: & H - G = \overline{12}, & C_{b4}: & G - I = \overline{30} \overline{24}, \\
& C - H = \overline{03}, & & G - H = \overline{12}, & & I - G = \overline{30} \overline{24}, \\
& G - F = \overline{05}, & & F - J = \overline{42}, & & H - J = \overline{50} \overline{14}, \\
& F - G = \overline{05}, & & J - F = \overline{42}, & & J - H = \overline{50} \overline{14}, \\
& J - I = \overline{53}, & & I - C = \overline{14}, & & C - F = \overline{53} \overline{12}, \\
& I - J = \overline{53}, & & C - I = \overline{14}, & & F - C = \overline{53} \overline{12}; \\
C_{b3}: & G - C = \overline{30} \overline{21}, & C - G = \overline{30} \overline{21}, & J - C = \overline{50} \overline{14}, \\
& G - J = \overline{50} \overline{24}, & J - G = \overline{50} \overline{24}, & C - J = \overline{53} \overline{14}, \\
& I - F = \overline{53} \overline{42}, & F - I = \overline{53} \overline{42}, & F - H = \overline{50} \overline{12}, \\
& H - I = \overline{30} \overline{14}, & I - H = \overline{30} \overline{14}, & H - F = \overline{50} \overline{12}.
\end{array}$$

Сравним классы C_b с классами C_a . Преобразования цепей C и F , ранее входившие в класс C_{a4} , теперь входят в класс C_{b4} ; преобразование цепей J и H происходит так же, как E и B , с заменами ребер 0, 1, 4, 5, а цепей I и G , как D и A , с заменами ребер 0, 2, 3, 4. Получилось, что $C_{b4} = C_{a4}$. Цепи I и J из класса C_{b1} преобразу-

зуются так же, как цепи A и B из класса C_{a2} , а цепи H и G из класса C_{b2} , как цепи D и E из класса C_{a1} . Получилось также, что замены ребер 1, 2 и 3, 5 преобразуют разные цепи, а значит, они входят и в разные классы. В третьих классах оказались одинаковыми четыре преобразования: $A - E = H - I$, $E - A = I - H$, $J - G = D - B$, $G - J = B - D$. Таким образом, с появлением группы G_{4b} прибавилось не 30, а только 16 новых элементов реберных преобразований.

Если в качестве привязки выбрать вершину c , то она определит цепи $I = 213$, $K = 203$, $B = 430$, $G = 410$, $L = 501$, $E = 531$, преобразующиеся по формулам:

$$\begin{aligned} C_{c1}: \quad & K - B = \bar{2}4, \quad G - I = 45, \quad E - I = \bar{5}2, \\ & B - K = \bar{2}4, \quad L - G = 4\bar{5}, \quad I - E = \bar{5}2; \\ C_{c2}: \quad & K - I = \bar{1}0, \quad G - B = \bar{1}3, \quad E - L = \bar{3}0, \\ & I - K = \bar{1}0, \quad B - G = \bar{1}3, \quad L - E = \bar{3}0; \\ C_{c3}: \quad & B - I = \bar{2}4 \bar{1}0, \quad I - L = \bar{5}2 \bar{0}3, \quad G - E = \bar{5}4 \bar{3}0, \\ & I - B = \bar{2}4 \bar{1}0, \quad L - I = \bar{5}2 \bar{0}3, \quad E - G = \bar{5}4 \bar{3}0, \\ & G - K = \bar{2}4 \bar{3}1, \quad K - E = \bar{5}2 \bar{1}0, \quad B - L = \bar{5}4 \bar{1}3, \\ & K - G = \bar{2}4 \bar{3}1, \quad E - K = \bar{5}2 \bar{1}0, \quad L - B = \bar{5}4 \bar{1}3; \\ C_{c4}: \quad & G - I = \bar{3}0 \bar{2}4, \quad B - E = \bar{5}4 \bar{1}0, \quad K - L = \bar{5}2 \bar{1}3, \\ & I - G = \bar{3}0 \bar{2}4, \quad E - B = \bar{5}4 \bar{1}0, \quad L - K = \bar{5}2 \bar{1}3. \end{aligned}$$

Наконец, если вершина d — привязка, то цепи $J = 125$, $L = 105$, $A = 450$, $H = 420$, $K = 302$, $D = 352$ преобразуются по формулам:

$$\begin{aligned} C_{d1}: \quad & J - D = \bar{1}3, \quad K - H = \bar{3}4, \quad A - L = \bar{4}1, \\ & D - J = \bar{1}3, \quad H - K = \bar{3}4, \quad L - A = \bar{4}1; \\ C_{d2}: \quad & J - L = \bar{0}2, \quad A - H = \bar{5}2, \quad D - K = \bar{5}0, \\ & L - J = \bar{0}2, \quad H - A = \bar{5}2, \quad K - D = \bar{5}0; \\ C_{d3}: \quad & A - J = \bar{2}0 \bar{4}1, \quad K - J = \bar{5}0 \bar{3}1, \quad H - D = \bar{3}4 \bar{5}0, \\ & J - A = \bar{2}0 \bar{4}1, \quad J - K = \bar{5}0 \bar{3}1, \quad D - H = \bar{3}4 \bar{5}0, \\ & H - L = \bar{5}2 \bar{1}4, \quad D - L = \bar{1}3 \bar{0}2, \quad K - A = \bar{4}3 \bar{5}2, \\ & L - H = \bar{5}2 \bar{1}4, \quad L - D = \bar{1}3 \bar{0}2, \quad A - K = \bar{4}3 \bar{5}2; \\ C_{d4}: \quad & D - A = \bar{4}3 \bar{0}2, \quad H - J = \bar{5}0 \bar{1}4, \quad K - L = \bar{1}3 \bar{5}2, \\ & A - D = \bar{4}3 \bar{0}2, \quad J - H = \bar{5}0 \bar{1}4, \quad L - K = \bar{1}3 \bar{5}2. \end{aligned}$$

Мы целиком рассмотрели графовую группу преобразования цепей тетраэдра G_4 . Сейчас можно было бы назначить систему образующих и выразить через них все элементы G_4 . Если принять, что

$$a = \bar{0}1, \quad b = \bar{1}2, \quad c = \bar{0}3, \quad d = \bar{3}5, \quad f = \bar{1}4,$$

то все элементы группы G_4 предстанут как все возможные суммы этих образующих, например:

$$\begin{aligned} \bar{a}c &= \bar{1}3, \quad \bar{b}f = \bar{2}4, \quad ad = \bar{0}1\bar{3}5, \quad \bar{b}d = \bar{1}2\bar{3}5, \quad \bar{a}bd = \bar{0}2\bar{3}5, \\ \bar{a}cf &= \bar{3}4, \quad \bar{a}bcd = \bar{2}5, \quad acdf = 45, \quad \bar{a}bcdf = \bar{1}245, \dots \end{aligned}$$

Однако число образующих на единицу меньше числа ребер. Поэтому есть смысл оставить элементы группы выраженными через ребра, которые несут прямой графический смысл, и не пытаться вводить отвлеченные элементы.

В табл. 3.1 приведены элементы группы G_4 без тождественного и обратных, которые преобразуют 12 цепей тетраэдра друг в друга. Цепи образуют субстанционное множество: $A = 054$, $B = 034$, $C = 243$, $D = 253$, $E = 135$, $F = 145$, $G = 014$, $H = 024$, $I = 213$, $J = 125$, $K = 203$, $L = 105$. Элементы же табл. 3.1 образуют операционное множество, причем каждый оператор связывает определенные пары субстанционных элементов, например: $1234 = F \cdot D = 145 \cdot 253 = G \cdot K = 410 \cdot 203$.

Таким образом, группа преобразования цепей тетраэдра G_4 состоит из 73 элементов, куда входят: тождественный элемент; 24 элемента типа xy , образующих классы C_1 и C_2 ; 24 элемента типа $pqrs$, образующих класс C_3 , и 6 элементов такого же типа класса C_4 . Кроме того, в табл. 3.1 не вошли еще 6 элементов класса C_5 , которые связывают цепи, проведенные от четырех различных вершин:

$$1\bar{5} = A \cdot G = D \cdot I, \quad 2\bar{3} = B \cdot H = E \cdot J, \quad 0\bar{4} = C \cdot K = F \cdot L;$$

и 12 элементов класса C_6 , описывающие переходы между взаимно дополняющими цепями тетраэдра:

$$\begin{aligned} 0\bar{1}234\bar{5} &= A - I, & 0\bar{1}2\bar{3}45 &= C - L, & 0\bar{1}2\bar{3}4\bar{5} &= E - H, \\ 0\bar{1}2345 &= B - J, & 0\bar{1}2\bar{3}4\bar{5} &= D - G, & 0\bar{1}234\bar{5} &= F - K. \end{aligned}$$

Таблица 3.1

№	C_1	№	C_1	C_2	C_3	C_4	№
1	01	D	12	34 45	1245 1234	1235	P
2	02	E	02	35 45	0235 0245	0234	
3	12	F	01	35 34	0134 0135	0145	
4	03	G	35	14 24	1345 2345	1235	Q
5	05	H	05	12 24	0125 0245	0145	
6	35	I	03	12 14	0123 0134	0234	
7	24	J	45	13 03	0345 1345	0145	R
8	25	K	25	01 03	0125 0235	1235	
9	45	L	24	01 13	0124 1234	0234	
A	13	M	34	05 25	0345 2345	0234	S
B	14	N	14	02 25	0124 1245	0145	
C	34	O	13	02 05	0123 0135	1235	

Вообще, число возможных переходов между $m = 12$ цепями равно $m \cdot (m - 1) + 1 = 133$, но в группу G_4 вошли только 73 элемента. Сокращение на 60 элементов произошло за счет симметрии тетраэдра.

Эти 73 элемента образуют: одну подгруппу первого порядка, состоящую из одного тождественного элемента и обозначаемую через 0; 12 подгрупп третьего порядка типа $\{e, xy, xy\}$, обозначенных в табл. 3.1 символами от 1 до С; 12 подгрупп 13-го порядка, обозначенных буквами от D до O, и 4 подгруппы 31-го порядка, обозначенных буквами P (G_{4a}), Q (G_{4b}), R (G_{4c}), S (G_{4d}). Восемнадцать элементов из двух последних классов C_5 и C_6 не входят ни в одну из собственных

подгрупп, число которых равно 28. Все названные подгруппы тетраэдра упорядочены в решетку $S(G_4)$, изображенную на рис. 3.5. Решетка $S(G_4)$ правильная, имеет 36 четырехзвенных цепей, привязанных к полюсам $S(G_4)$.

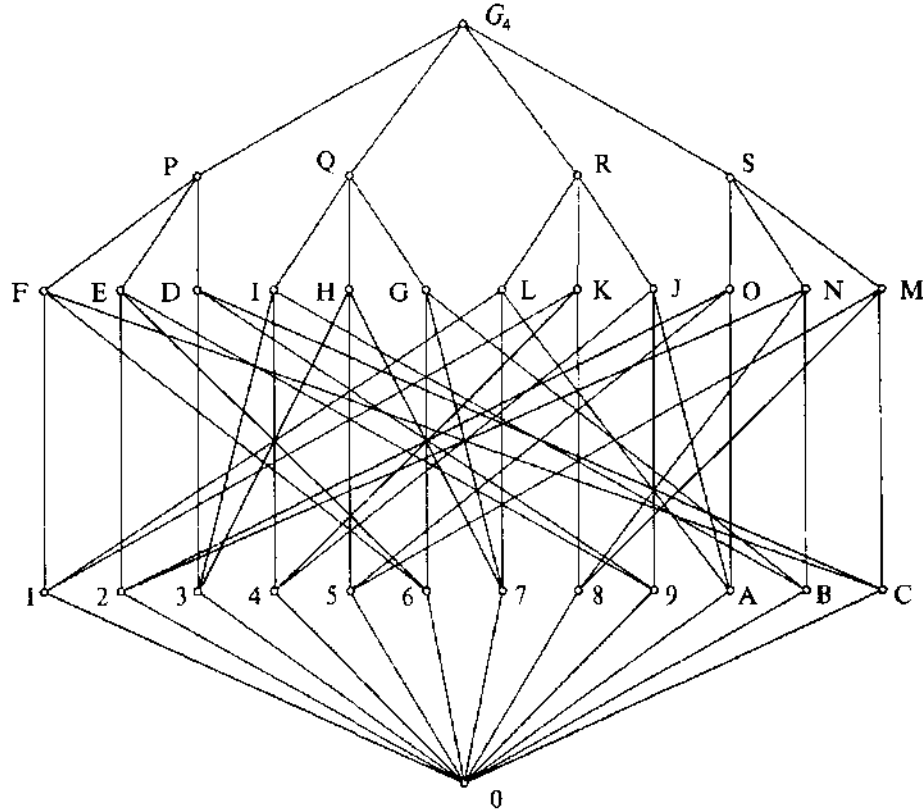


Рис. 3.5

Перейдем к рассмотрению группы преобразования цепей куба G_8 (рис. 3.6). Если в качестве привязки принять вершину a , то в зависимости от ее удаленности получим *четыре класса вершин*: класс 0 — $\{a\}$, класс 1 — $\{b, c, d\}$, класс 2 — $\{e, f, g\}$ и класс 3 — $\{h\}$; и *три класса ребер*: класс 1 — $\{1, 2, 3\}$, класс 2 — $\{4, 5, 6, 7, 8, 9\}$, класс 3 — $\{A, B, C\}$. Привязка a определяет 18 цепей. Частота появления ребер в цепях распределяется по трем классам следующим образом: для класса 1 она равна 6, для класса 2 — 13 и для класса 3 — 10.

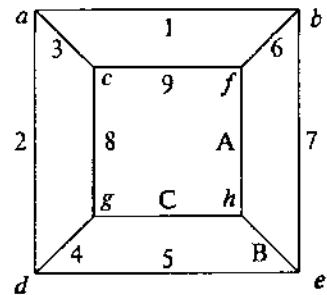


Рис. 3.6

Приведем список цепей, которые привязываются к вершине a :

- 1: $1 = abfcgdeh = 169845B$, $4 = adebfchg = 257698C$, $7 = acgdebhf = 384576A$,
 $2 = abfcghed = 1698CB5$, $5 = adebfhgc = 2576AC8$, $8 = acgdehfb = 3845BA6$,
 $3 = adehgcfb = 25BC896$, $6 = acghfbed = 38CA675$, $9 = abfhedgc = 16AB548$,

II: 10 = $abedghfc$ = 1754CA9, 13 = $adgcfheb$ = 2489AB7, 16 = $acfbhegd$ = 3967BC4,
 11 = $abedgcfh$ = 175489A, 14 = $adgcfbeh$ = 248967B, 17 = $acfbhedgh$ = 396754C,
 12 = $abehfcgd$ = 17BA984, 15 = $adghehfc$ = 24CB769, 18 = $acfhgdeb$ = 39AC457.

Список разбит на два цикла: первый (I) – с 1 по 9, второй (II) – с 10 по 18. Внутри каждого цикла переход от одной цепи к другой осуществляется заменой одного ребра. Новое ребро появляется путем присоединения восьмой (хвостовой) вершины каждой цепи к первой (головной), третьей или пятой. Таким образом, происходит *инверсия* хвостовой части каждой из цепей, т.е. два, четыре или шесть хвостовых ребер присоединяются к вновь установленному ребру в обратном порядке. Так, переход от цепи 1 к цепи 2 осуществляется путем удаления ребра $gd = 4$ и введением ребра $gh = C$, при этом чередование вершин хвостовой части цепи (deh) меняется на противоположное (hed). Переход от цепи 2 к цепи 3 осуществляется путем инверсии семи хвостовых вершин ($bfcghed$) и т.д.; цепь 9 переходит в цепь 1 путем инверсии пяти вершин ($hedgc$). Аналогичная картина наблюдается во втором цикле, куда включены цепи с 10 по 18.

Чтобы получить цепи от семи других вершин куба (рис. 3.6), достаточно в имеющихся 18 цепях произвести замену ребер в соответствии с семью подстановками, которые вместе с тождественной образуют коммутативную группу, типа C_2C_4 :

$b = (1752)(36B4)(89AC)$, $c = (19)(28)(5C)(7A)$, $d = (1257)(34B6)(8CA9)$,
 $e = (15)(27)(3B)(46)(8A)(9C)$, $g = (185A)(2C79)(34B6)$,
 $f = (1A58)(297C)(36B4)$, $h = (1C)(2A)(3B)(46)(59)(78)$.

В результате действия группы подстановок получим $18 \times 8 = 144$ цепи. Однако в кубе можно провести только 72 различных цепи. Удвоение числа можно понять из анализа хвостовых вершин приведенных цепей. На восемнадцать головных вершин класса 0, т.е. вершин a , приходится по четыре хвостовых вершины класса 1, т.е. вершин b, c, d , и шесть вершин h класса 3 (вершины e, f, g класса 2 в хвостах отсутствуют). Следовательно, все восемнадцать цепей, привязанных к вершине a , повторяются в списке из 144 цепей, только головная вершина a окажется уже в хвосте. Аналогичное удвоение произойдет с цепями, привязанными к вершине b и т.д.

Из 72 цепей куба можно составить один большой цикл, основанный на том же самом принципе, что заложен в малых циклах, образованных девятью цепями. В 72-цикле в отличие от 9-циклов инверсии подлежат не только хвостовые, но и головные части цепей.

1 = 169845B,	19 = 248967B,	37 = 396754C,	55 = 384576A,
2 = 1698CB5,	20 = 2489AB7,	38 = 931754C,	56 = 832576A,
3 = 25BC896,	21 = BA98421,	39 = 457139A,	57 = CA67523,
4 = CB52396,	22 = BA61248,	40 = 45BA931,	58 = 76AC423,
5 = CB52169,	23 = AB71248,	41 = 54CA931,	59 = 76AC832,
6 = 896125B,	24 = 4217BA9,	42 = 39AC457,	60 = 5238CA6,
7 = 89AB521,	25 = 4239AB7,	43 = CA93257,	61 = 8325BA6,
8 = 98CB521,	26 = 423967B,	44 = CA93175,	62 = 3845BA6,
9 = 6125BC8,	27 = CB76932,	45 = 7139AC4,	63 = AB54831,

$10 = 5216AC8$, $28 = 67BC832$, $46 = 7124CA9$, $64 = AB71384$,
 $11 = 521698C$, $29 = 67BC423$, $47 = 1754CA9$, $65 = BA61384$,
 $12 = BC89612$, $30 = 9324CB7$, $48 = AC45713$, $66 = 8316AB5$,
 $13 = 98CB712$, $31 = 9317BC4$, $49 = AC83175$, $67 = 6138CB5$,
 $14 = 89AB712$, $32 = 3967BC4$, $50 = AC83257$, $68 = 613845B$,
 $15 = 17BA984$, $33 = 24CB769$, $51 = 675238C$, $69 = 548316A$,
 $16 = 175489A$, $34 = BC42169$, $52 = 257698C$, $70 = 54CA613$,
 $17 = 712489A$, $35 = BC42396$, $53 = 2576AC8$, $71 = 45BA613$,
 $18 = 984217B$, $36 = 769324C$, $54 = 38CA675$, $72 = 16AB548$.

Большой 72-цикл симметрично укладывается на грани и ребра гиперкуба Γ_{72} , развертка которого приведена на рис. 3.7, при этом каждая цепь связана с четырьмя другими отношением инверсии хвоста или головы. Два 9-цикла отвечают узлам, расположенным вблизи диаметрально противоположных вершин гиперкуба Γ_{72} , обозначенных через a :

$$\{1 - 2 - 3 - 52 - 53 - 54 - 55 - 62 - 72\},$$

$$\{47 - 16 - 15 - 20 - 19 - 33 - 32 - 37 - 42\}.$$

Привязке h куба Γ_8 соответствуют те же самые вершины Γ_{72} , а узлы двух 9-циклов частично перекрываются с двумя предыдущими циклами:

$$\{16 - 17 - 18 - 19 - 26 - 36 - 37 - 38 - 39\},$$

$$\{1 - 6 - 11 - 52 - 51 - 56 - 55 - 69 - 68\}.$$

На рис. 3.7, помимо вершин $a-h$, помечены также вершины $b-g$, $c-e$ и $d-f$, вблизи которых располагаются еще двенадцать 9-циклов, дважды покрывающие все узлы гиперкуба Γ_{72} .

На гранях Γ_{72} можно выделить шесть 8-циклов:

$$\{2 - 3 - 8 - 9 - 5 - 6 - 11 - 12\},$$

$$\{14 - 15 - 20 - 21 - 17 - 18 - 23 - 24\},$$

$$\{26 - 27 - 32 - 33 - 29 - 30 - 35 - 36\},$$

$$\{44 - 45 - 41 - 42 - 47 - 48 - 38 - 39\},$$

$$\{53 - 54 - 59 - 60 - 50 - 51 - 56 - 57\},$$

$$\{65 - 66 - 71 - 72 - 62 - 63 - 68 - 69\}.$$

Распишем первый из них конкретно через цепи:

$$2 = 1698CB5, \quad 3 = 25BC896, \quad 4 = CB52396, \quad 5 = CB52169,$$

$$8 = 98CB521, \quad 9 = 6125BC8, \quad 11 = 521698C, \quad 12 = BC89612.$$

Как видим, 8-цикл связан отношением инверсии только шести головных или хвостовых ребер. Переходы $2-5=82$ и $8-11=\overline{B6}$ сопровождаются заменой одного-единственного ребра. Однорреберные замены характерны и для всех остальных переходов между узлами грани A гиперкуба.

$$\Gamma_{72}: \quad 3 - 5 = \overline{81}, \quad 12 - 5 = \overline{85}, \quad 3 - 11 = \overline{B1}, \quad 9 - 11 = \overline{B9}, \quad 9 - 2 = \overline{29},$$

$$6 - 2 = \overline{2C}, \quad 12 - 8 = \overline{65}, \quad 6 - 8 = \overline{6C}, \quad 3 - 6 = \overline{C1}, \quad 9 - 12 = \overline{59},$$

$$3 - 9 = \overline{91}, \quad 3 - 12 = \overline{51}, \quad 6 - 9 = \overline{9C}, \quad 6 - 12 = \overline{5C}, \quad 2 - 8 = \overline{62},$$

$$2 - 11 = \overline{B2}, \quad 5 - 8 = \overline{68}, \quad 5 - 11 = \overline{B8}.$$

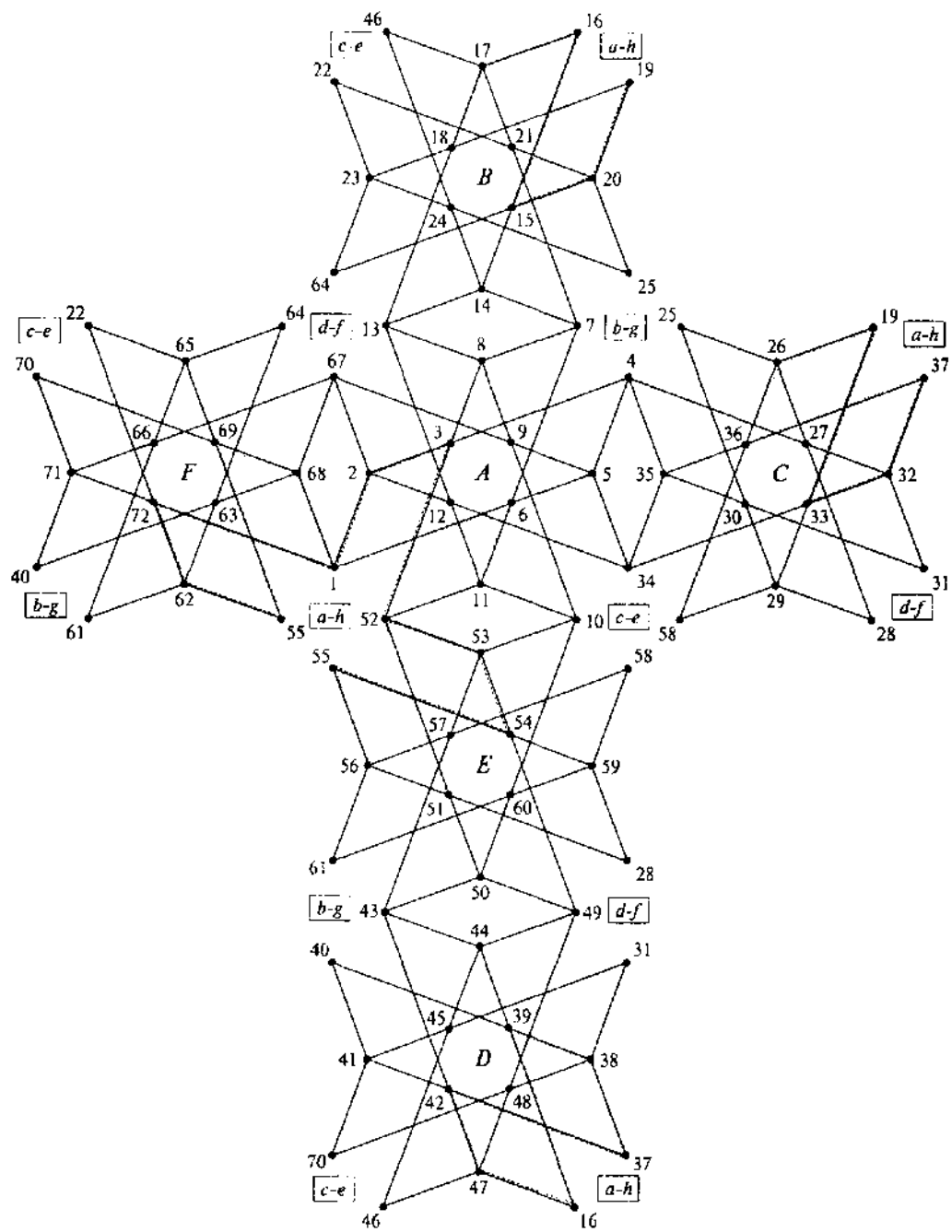


Рис. 3.7

С учетом этого связи грани A могли бы выглядеть иначе (рис. 3.8). Та же самая картина наблюдается на других гранях гиперкуба Γ_{72} . Благодаря этому возможны пяти- и семизвенные циклы, например: $\{2 - 3 - 9 - 6 - 12\}$ или $\{2 - 3 - 8 - 9 - 6 - 11 - 12\}$, что кажется странным, поскольку числа 5 и 7 не являются делителями числа 72. Однако последние выписанные нами переходы отходят от принципа инверсии двух, четырех и шести головных или хвостовых ребер.

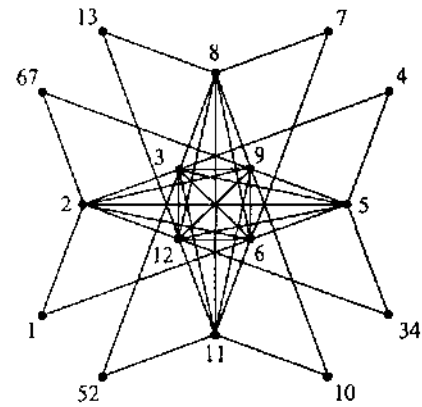


Рис. 3.8

Если оставаться в рамках провозглашенного принципа перехода от одной цепи к другой, то связи на гранях Γ_{72} следует оставить такими, как они показаны на рис. 3.7. Впрочем, 4-, 6-, 8-, 9-, 12-, 18-, 24-, 36-циклы, которые можно выделить в G_{72} , также не являются делителями 72-цикла, поскольку, например, 4-циклов всего 12 (вместо 18); они расположены на ребрах гиперкуба Γ_{72} :

$\{1 - 2 - 67 - 68\}$, $\{4 - 5 - 34 - 35\}$, $\{7 - 8 - 13 - 14\}$,
 $\{10 - 11 - 52 - 53\}$, $\{16 - 17 - 46 - 47\}$, $\{19 - 20 - 25 - 26\}$,
 $\{22 - 23 - 64 - 65\}$, $\{28 - 29 - 58 - 59\}$, $\{31 - 32 - 37 - 38\}$,
 $\{40 - 41 - 70 - 71\}$, $\{43 - 44 - 49 - 50\}$, $\{55 - 56 - 61 - 62\}$.

В первом 4-цикле имеем следующие переходы:

$- 169845B - 1698CB5 - 6138CB5 - 613845B -$.

Аналогичные одnoreберные переходы характерны и для остальных 4-циклов.

Возьмем другой пример: 18-циклов можно провести только два (вместо 4), например:

$\{1 - 2 - 3 - 4 - 5 - 6 - 7 - 14 - 24 - 46 - 17 - 21 - 22 - 65 - 69 - 55 - 62 - 72\}$

и

$\{43 - 44 - 39 - 16 - 47 - 42 - 37 - 32 - 33 - 34 - 35 - 36 - 58 - 59 - 60 - 61 - 56 - 57\}$.

Всякий третий 18-цикл будет иметь пересечение с узлами уже выписанных циклов, в частности:

$\{8 - 9 - 10 - 11 - 12 - 34 - 35 - 36 - 37 - 32 - 33 - 19 - 20 - 15 - 64 - 23 - 18 - 13\}$.

Прежде чем рассматривать группу преобразований цепей куба, установим реберный состав цепей. Цепи, привязанные к вершине a , можно разбить на три класса. Так, цепь $1 = 169845B$, согласно реберной классификации, состоит из ребер следующих классов: 1222223; цепь $72 = 16AB548$ имеет состав 1233222 и цепь $62 = 3845BA6 \rightarrow 1222332$. Эти три цепи принадлежат грани F гиперкуба Γ_{72} . Они могут служить представителями соответствующих классов цепей других пяти граней

класс A : $\{1, 55, 52, 37, 19, 16\} \rightarrow 1222223$;

класс B : $\{72, 54, 3, 42, 33, 15\} \rightarrow 1233222$;

класс C : $\{62, 53, 2, 47, 32, 20\} \rightarrow 1222332$.

Цепи первых двух классов *симметричны*, третьего класса — *асимметричны*. Симметричность цепи является ее *абсолютной* характеристикой; она не зависит от привязки. Ее можно установить следующим образом: для каждой цепи, начиная от вершины a , согнем вдоль соответствующих ребер реального куба жесткую проволоку, сохраняющую свою форму. Для симметричных цепей «хвост» и «голова» соответствующей изогнутой проволоки могут меняться местами, т.е. независимо от того, каким концом прикреплять проволоку к вершине a ; всегда можно добиться того, чтобы она прошла по нужным нам ребрам. Если изогнутую проволоку от асимметричной цепи прикрепить «хвостом» к вершине a , то в любом случае, как бы ее не поворачивать, она укажет новые ребра. Таким образом, за счет вращения куба G_8 или проволоки вокруг оси, проходящей через вершину a , каждая симметричная цепь порождает только две новых цепи; асимметричная же цепь дает уже пять новых цепей.

Осуществив переход от цепей класса C к цепям класса B , мы получим *первый класс реберных подстановок*:

$$\bar{1}2 = 2 - 3 = 15 - 20, \quad \bar{3}1 = 62 - 72 = 42 - 47, \quad \bar{2}3 = 53 - 54 = 33 - 32.$$

Второй класс получается благодаря следующим преобразованиям:

$$\bar{9}A = 1 - 72 = 52 - 53, \quad \bar{6}A = 37 - 42 = 19 - 20, \quad \bar{7}B = 52 - 3 = 55 - 62, \\ \bar{5}B = 16 - 15 = 37 - 32, \quad \bar{4}C = 55 - 54 = 1 - 2, \quad \bar{8}C = 19 - 33 = 16 - 47.$$

В этом классе можно было бы отдельно выделить два подкласса: первый описывал бы переходы между цепями классов A и B , другой — между цепями классов A и C . Тогда всевозможные переходы между этими двумя подклассами породили бы *третий класс*:

$$\bar{9}A \bar{4}C = 2 - 72, \quad \bar{6}A \bar{8}C = 33 - 20, \quad \bar{7}B \bar{9}A = 53 - 3, \\ \bar{5}B \bar{6}A = 42 - 32, \quad \bar{4}C \bar{7}B = 62 - 54, \quad \bar{8}C \bar{5}B = 15 - 47.$$

Однако мы не будем различать подобные подклассы. Вместо этого введем классификацию подстановок в зависимости от реберной классификации. В частности, во втором классе подстановок при переходах от одной цепи к другой удаляется ребро, принадлежащее реберному классу 1 , и вводится ребро, принадлежащее классу 2 . Поэтому к *третьему классу* отнесем подстановки, где имеют место замены, аналогичные для этого класса:

$$\bar{9}A \bar{8}C = 37 - 55, \quad \bar{7}B \bar{6}A = 16 - 1, \quad \bar{4}C \bar{5}B = 19 - 52.$$

Из этих же соображений мы не станем делить на самостоятельные подклассы подстановки *четвертого класса*:

$$\bar{1}2 \bar{4}C = 1 - 3, \quad \bar{1}2 \bar{7}B = 2 - 52, \quad \bar{2}3 \bar{9}A = 52 - 54, \\ \bar{2}3 \bar{4}C = 53 - 55, \quad \bar{3}1 \bar{7}B = 55 - 72, \quad \bar{3}1 \bar{9}A = 62 - 1, \\ \bar{1}2 \bar{6}A = 15 - 19, \quad \bar{1}2 \bar{5}B = 16 - 20, \quad \bar{2}3 \bar{5}B = 33 - 37, \\ \bar{2}3 \bar{8}C = 19 - 32, \quad \bar{3}1 \bar{8}C = 42 - 16, \quad \bar{3}1 \bar{6}A = 37 - 47.$$

Ниже дается классификация всех остальных переходов между цепями, привязанными к вершине a :

Класс 5

$$\begin{array}{lll} \bar{9}A \bar{8}4 = 37 - 54, & \bar{6}A \bar{5}7 = 1 - 15, & \bar{4}C \bar{5}7 = 19 - 3, \\ \bar{8}C \bar{6}9 = 55 - 42, & \bar{7}B \bar{6}9 = 16 - 72, & \bar{5}B \bar{8}4 = 52 - 33; \end{array}$$

Класс 6

$$\bar{1}2 \bar{5}7 = 1 - 19, \quad \bar{2}3 \bar{8}4 = 52 - 37, \quad \bar{3}1 \bar{6}9 = 55 - 16;$$

Класс 7

$$\bar{6}9 \bar{5}7 = 15 - 72, \quad \bar{5}7 \bar{8}4 = 33 - 3, \quad \bar{8}4 \bar{6}9 = 42 - 54;$$

Класс 8

$$\begin{array}{lll} \bar{2}1 \bar{5}7 \bar{8}4 = 33 - 2, & \bar{3}2 \bar{5}7 \bar{8}4 = 32 - 3, & \bar{3}2 \bar{8}4 \bar{6}9 = 42 - 53, \\ \bar{1}3 \bar{8}4 \bar{6}9 = 47 - 54, & \bar{1}3 \bar{6}9 \bar{5}7 = 15 - 62, & \bar{2}1 \bar{6}9 \bar{5}7 = 20 - 72, \\ \bar{3}1 \bar{5}7 \bar{8}4 = 32 - 2, & \bar{1}2 \bar{8}4 \bar{6}9 = 47 - 53, & \bar{2}3 \bar{6}9 \bar{5}7 = 20 - 62; \end{array}$$

Класс 9

$$\begin{array}{lll} \bar{1}2 \bar{6}A \bar{8}4 = 47 - 52, & \bar{1}2 \bar{8}C \bar{5}7 = 1 - 33, & \bar{2}3 \bar{5}B \bar{6}9 = 20 - 55, \\ \bar{2}3 \bar{6}A \bar{8}4 = 52 - 42, & \bar{3}1 \bar{8}C \bar{5}7 = 32 - 1, & \bar{3}1 \bar{5}B \bar{6}9 = 55 - 15, \\ \bar{1}2 \bar{9}A \bar{5}7 = 72 - 19, & \bar{1}2 \bar{6}A \bar{5}7 = 1 - 20, & \bar{2}3 \bar{7}B \bar{8}4 = 3 - 37, \\ \bar{2}3 \bar{5}B \bar{8}4 = 52 - 32, & \bar{3}1 \bar{4}C \bar{6}9 = 54 - 16, & \bar{3}1 \bar{8}C \bar{6}9 = 55 - 47, \\ \bar{1}2 \bar{4}C \bar{6}9 = 16 - 53, & \bar{1}2 \bar{4}C \bar{5}7 = 2 - 19, & \bar{2}3 \bar{9}A \bar{5}7 = 19 - 62, \\ \bar{2}3 \bar{9}A \bar{8}4 = 53 - 37, & \bar{3}1 \bar{7}B \bar{8}4 = 37 - 2, & \bar{3}1 \bar{7}B \bar{6}9 = 62 - 16; \end{array}$$

Класс 10

$$\begin{array}{lll} \bar{1}2 \bar{6}A \bar{5}B \bar{4}C = 15 - 52, & \bar{2}1 \bar{6}A \bar{7}B \bar{4}C = 3 - 16, & \bar{2}3 \bar{9}A \bar{5}B \bar{8}C = 33 - 55, \\ \bar{3}2 \bar{9}A \bar{5}B \bar{4}C = 54 - 19, & \bar{3}1 \bar{6}A \bar{7}B \bar{8}C = 42 - 1, & \bar{1}3 \bar{9}A \bar{7}B \bar{8}C = 72 - 37, \\ \bar{2}1 \bar{6}A \bar{5}B \bar{8}C = 33 - 16, & \bar{1}2 \bar{9}A \bar{7}B \bar{4}C = 72 - 52, & \bar{3}2 \bar{6}A \bar{5}B \bar{8}C = 42 - 19, \\ \bar{2}3 \bar{9}A \bar{7}B \bar{4}C = 3 - 55, & \bar{1}3 \bar{6}A \bar{5}B \bar{8}C = 15 - 37, & \bar{3}1 \bar{9}A \bar{7}B \bar{4}C = 54 - 1, \\ \bar{2}1 \bar{9}A \bar{7}B \bar{4}C = 53 - 1, & \bar{1}2 \bar{6}A \bar{5}B \bar{8}C = 47 - 19, & \bar{3}2 \bar{9}A \bar{7}B \bar{4}C = 62 - 52, \\ \bar{2}3 \bar{6}A \bar{5}B \bar{8}C = 20 - 37, & \bar{1}3 \bar{9}A \bar{7}B \bar{4}C = 2 - 55, & \bar{3}1 \bar{6}A \bar{5}B \bar{8}C = 32 - 16; \end{array}$$

Класс 11

$$\begin{array}{ll} \bar{6}9 \bar{7}B \bar{8}C = 42 - 62 = 47 - 72, & \bar{8}4 \bar{6}A \bar{7}B = 47 - 2, \\ \bar{5}7 \bar{6}A \bar{4}C = 15 - 2 = 20 - 3, & \bar{6}9 \bar{5}B \bar{4}C = 20 - 53, \\ \bar{8}4 \bar{9}A \bar{5}B = 33 - 53 = 32 - 54, & \bar{5}7 \bar{9}A \bar{8}C = 32 - 62; \end{array}$$

Класс 12

$$\begin{array}{lll} \bar{6}A \bar{7}B \bar{8}C = 1 - 47, & \bar{6}A \bar{7}B \bar{4}C = 16 - 2, & \bar{6}A \bar{5}B \bar{4}C = 52 - 20, \\ \bar{9}A \bar{7}B \bar{8}C = 37 - 62, & \bar{9}A \bar{5}B \bar{8}C = 55 - 32, & \bar{9}A \bar{5}B \bar{4}C = 19 - 53; \end{array}$$

Класс 13

$$\begin{array}{lll} \bar{1}2 \bar{6}A \bar{4}C \bar{5}7 = 15 - 3, & \bar{2}1 \bar{6}A \bar{4}C \bar{5}7 = 20 - 2, & \bar{2}3 \bar{9}A \bar{5}B \bar{8}4 = 33 - 54, \\ \bar{3}2 \bar{9}A \bar{5}B \bar{8}4 = 32 - 53, & \bar{3}1 \bar{7}B \bar{8}C \bar{6}9 = 42 - 72, & \bar{1}3 \bar{7}B \bar{8}C \bar{6}9 = 47 - 62, \\ \bar{2}1 \bar{9}A \bar{8}C \bar{5}7 = 33 - 72, & \bar{1}2 \bar{6}A \bar{7}B \bar{8}4 = 47 - 3, & \bar{3}2 \bar{6}A \bar{7}B \bar{8}4 = 42 - 3, \\ \bar{2}3 \bar{5}B \bar{4}C \bar{6}9 = 20 - 54, & \bar{1}3 \bar{5}B \bar{4}C \bar{6}9 = 15 - 54, & \bar{3}1 \bar{9}A \bar{8}C \bar{5}7 = 32 - 72, \\ \bar{1}2 \bar{5}B \bar{4}C \bar{6}9 = 15 - 53, & \bar{2}3 \bar{9}A \bar{8}C \bar{5}7 = 33 - 62, & \bar{3}1 \bar{6}A \bar{7}B \bar{8}4 = 42 - 2; \end{array}$$

Класс 14

$$\begin{aligned}
 \overline{12} \overline{7B} \overline{4C} &= 1 & 52 &= 72 - 53, & \overline{12} \overline{5B} \overline{8C} &= 47 - 20, \\
 \overline{23} \overline{9A} \overline{4C} &= 52 - 55 = 3 - 62, & \overline{23} \overline{6A} \overline{8C} &= 20 - 32, \\
 \overline{31} \overline{9A} \overline{7B} &= 55 - 1 = 54 - 2, & \overline{31} \overline{6A} \overline{5B} &= 32 - 47, \\
 \overline{12} \overline{6A} \overline{5B} &= 16 - 19 = 47 - 33, & \overline{12} \overline{9A} \overline{7B} &= 2 - 53, \\
 \overline{23} \overline{5B} \overline{8C} &= 19 - 37 = 20 - 42, & \overline{23} \overline{7B} \overline{4C} &= 53 - 62, \\
 \overline{31} \overline{6A} \overline{8C} &= 37 - 16 = 32 - 15, & \overline{31} \overline{9A} \overline{4C} &= 62 - 2, \\
 \overline{12} \overline{9A} \overline{4C} &= 72 - 3, & \overline{12} \overline{6A} \overline{8C} &= 15 - 33, & \overline{23} \overline{9A} \overline{7B} &= 3 - 54, \\
 \overline{23} \overline{6A} \overline{5B} &= 33 - 42, & \overline{31} \overline{7B} \overline{4C} &= 54 - 72, & \overline{31} \overline{5B} \overline{8C} &= 42 - 15, \\
 \overline{12} \overline{6A} \overline{4C} &= 16 - 52, & \overline{23} \overline{9A} \overline{5B} &= 19 - 55, & \overline{31} \overline{7B} \overline{8C} &= 37 - 1.
 \end{aligned}$$

Как видим, через однореберные замены, которые фигурировали в двух первоначальных 9-циклах, выражаются все многореберные подстановки данной подгруппы. Табл. 3.2 представляет собой таблицу сложения наших укрупненных классов.

Таблица 3.2

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	—	4	14	2	9	—	8	7, 8	5, 9	10, 12	13	10	11, 13	3, 14
2	4	3	2, 5, 12	1, 4	3, 7, 11	9	5	9	6, 8, 13, 14	13, 14	5, 12	3, 11	9, 10	4, 9, 10
3	14	2, 5, 12	—	9, 10	2, 12	14	11	13	4, 9, 10	4, 9	7, 11	2, 5	8, 13	1, 6, 14
4	2	1, 14	9, 10	14	6, 8, 13	5, 9	9	5, 9, 13	3, 6, 7, 8, 11, 13, 14	3, 11	9, 10	13, 14	5, 8, 9, 10, 12	2, 4, 9, 10, 12
5	9	3, 7, 11	2, 12	6, 8, 13	—	4	2	4	1, 14	13, 14	2	3	4, 10	9, 10
6	—	9	14	5, 9	4	—	—	—	2, 4	10, 12	—	10	—	3, 14
7	8	5	11	9	2	—	—	1	4	10	3	—	14	13
8	7, 8	9	13	5, 9, 13	4	—	1	1	2, 4	10, 12	14	10	3, 4, 14	11, 13
9	5, 9	6, 8, 13, 14	4, 9, 10	3, 6, 7, 8, 11, 13, 14	1, 14	2, 4	4	2, 4	1, 3, 14	3, 11, 13, 14	4, 10	14	2, 4, 10	2, 4, 5, 9, 10, 12
10	10, 12	13, 14	4, 9	3, 11, 12, 14	13, 14	10, 12	13	10, 12	3, 11, 13, 14	1, 6, 7, 8	4, 9	1, 6, 8	2, 4, 5, 9	2, 4, 5, 9
11	13	5, 12	7, 11	9, 10	2	—	3	14	4, 10	4, 9	3	2	1, 14	8, 13
12	10	3, 11	2, 5	12, 14	3	10	—	10	14	1, 6, 8	2	—	4	4, 9
13	11, 13	9, 10	8, 13	5, 8, 9, 10, 12	4, 10	—	14	3, 4, 14	2, 4, 10	2, 4, 5, 9	1, 14	4	1, 3, 14	7, 8, 11, 13
14	3, 14	4, 9, 10	1, 6, 14	2, 4, 9, 10, 12	9, 10	3, 14	13	11, 13	2, 4, 5, 9, 10, 12	2, 4, 5, 9	8, 13	4, 9	7, 8, 11, 13	1, 3, 6, 14

Ранее мы уже говорили, что для аддитивных групп выполняются очевидные равенства: если $a + b = c$, то $a + c = b$ и $b + c = a$. Если это условие справедливо для отдельных подстановок, то оно будет справедливым и для целых классов. В частности, если при сложении подстановок второго и пятого классов получаются подстановки третьего, седьмого и одиннадцатого классов, т.е. если в отношении классов имеет место равенство: $2 + 5 = 3, 7, 11$, то класс 5 обязательно окажется во второй строке на пересечениях 3-го, 7-го и 11-го столбцов; а поскольку табл. 3.2 симметричная, то класс 2 нужно искать в пятой строке на пересечениях этих же трех столбцов. Таким образом, каждая клеточка таблицы несет двойную информацию: во-первых, она указывает, в какие классы попадают результирую-

щие подстановки; во-вторых, она указывает, где нужно искать подстановки исходных слагаемых. Поэтому, когда заполнена первая строка, мы имеем информацию не только о первом столбце, но можем проставить первый класс по всей таблице сложения. При заполнении второй строки мы узнаем, в каких клетках нужно проставить 2 и т.д.

Мультипликативная группа симметрии октаэдра (рис. 3.9) та же, что и куба. Поэтому узлы Γ_{72} можно попытаться уложить на ребра и грани октаэдра, и наоборот, большой цикл из цепей октаэдра можно уложить на кубе.

Ребрами октаэдра определяются 120 пятизвенных цепей, что значительно больше числа семизвенных цепей куба. Это объясняется тем, что в вершинах куба соединяются три ребра, а в вершинах октаэдра — четыре: чем выше степень связи каждой вершины со всеми остальными вершинами, тем больше количество цепей.

Приведем полную мультипликативную группу вращения октаэдра (см. табл. 2.54, столбец $O(6)$):

$(bcde)$,	$(af)(be)(cd)$,	$(aeb)(cdf)$,	$(aed)(bfc)$,
$(bedc)$,	$(af)(bc)(de)$,	$(abe)(cdf)$,	$(ade)(bcf)$,
$(abfd)$,	$(ae)(bd)(cf)$,	$(acd)(bfe)$,	$(af)(ce)$,
$(adfb)$,	$(ad)(bf)(ce)$,	$(adc)(bef)$,	$(af)(bd)$,
$(acfe)$,	$(ac)(bd)(ef)$,	$(acb)(dfe)$,	$(bd)(ce)$,
$(aefc)$,	$(ab)(ce)(df)$,	$(abc)(def)$,	e .

Действуя этой группой на 6-, 12- и два 8-цикла из цепей октаэдра —

6-цикл: $\{defbca, edfbca, bfdeca, bfdeac, bfcaed, fbcaed\}$;

8-цикл: $\{abcfed, abcfde, aedfcb, aedfbc, acbfde, acbfed, adefcb, adefcb\}$;

8-цикл: $\{abhfed, abhfde, aedcfb, aedcbf, aefbcd, aefdc b, abcdfe, abcdef\}$;

12-цикл: $\{adcbfe, adcbef, adfebc, acbefd, acbedf, acfdeb, abedfc, abedcf, abfcde, aedcfb, aedcbf, aefbcd\}$,

мы получим достаточную информацию для составления большого 120-цикла, который затем можно попытаться уложить на ребра и грани куба или октаэдра.

До сих пор мы рассматривали симметричные графы. Но любой несимметричный граф так или иначе является подграфом полного высокосимметричного графа. Единственным неудобством группового анализа графов является быстро возрастающий с ростом числа вершин порядок группы. Так, субстанционным множеством для аддитивной группы G_5 полного графа Γ_5 , изображенного на рис. 3.10, служат 60 четырехзвенных цепей:

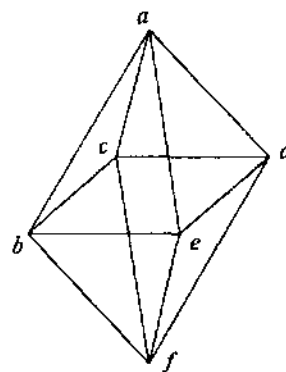


Рис. 3.9

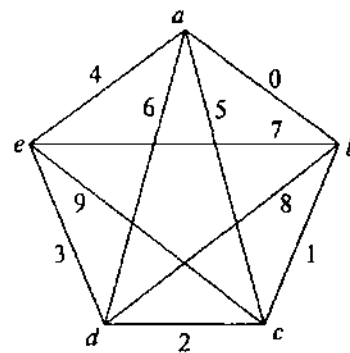


Рис. 3.10

1 = 0123	11 = 4782	21 = 6819	31 = 0629	41 = 7956	51 = 5083
2 = 0193	12 = 4712	22 = 6879	32 = 0639	42 = 7365	52 = 5073
3 = 0839	13 = 5173	23 = 6297	33 = 0593	43 = 1043	53 = 5687
4 = 0829	14 = 5183	24 = 6217	34 = 0523	44 = 1063	54 = 5478
5 = 0792	15 = 5237	25 = 1264	35 = 8254	45 = 1746	55 = 2104
6 = 0732	16 = 5287	26 = 1946	36 = 8345	46 = 1864	56 = 2507
7 = 4321	17 = 5978	27 = 1563	37 = 8659	47 = 2607	57 = 6019
8 = 4381	18 = 5938	28 = 1543	38 = 8649	48 = 2804	58 = 6517
9 = 4918	19 = 6371	29 = 0432	39 = 7452	49 = 9408	59 = 8154
10 = 4928	20 = 6391	30 = 0492	40 = 7462	50 = 9706	60 = 8059

Первые 24 цепи приходятся на привязку a . Относительно этой привязки существует два класса ребер $\{0, 4, 5, 6\}$ и $\{1, 2, 3, 7, 8, 9\}$. Следовательно, можно выделить 11 укрупненных классов, по которым раскладываются элементы подгруппы G_{5a} —

Класс 1:		Класс 2:	
$\overline{40} = 7 - 1 - 10$	4,	$\overline{21} = 10 - 9 - 15$	13,
$\overline{50} = 18 - 3 = 15 - 6$,		$\overline{71} = 6 - 1 - 22$	21,
$\overline{60} = 20 - 2 - 23 - 5$,		$\overline{81} = 3 - 2 = 11 - 12$,	
$\overline{54} = 14 - 8 = 16 - 11$,		$\overline{91} = 18 - 14 = 23 - 24$,	
$\overline{64} = 21 - 9 = 24 - 12$,		$\overline{82} = 8 - 7 = 22 - 23$,	
$\overline{65} = 19 - 13 = 22 - 17$;		$\overline{92} = 2 - 1 = 17 - 16$,	
		$\overline{23} = 4 - 5 = 24 - 19$,	
		$\overline{73} = 12 - 7 = 17 - 18$,	
		$\overline{83} = 16 - 15 = 21 - 20$,	
		$\overline{93} = 9 - 8 = 5 - 6$,	
		$\overline{78} = 5 - 4 = 13 - 14$,	
		$\overline{79} = 11 - 10 = 19 - 20$;	
Класс 3:			
$\overline{4017} = 7 - 6$,	$\overline{5439} = 14 - 9$,	$\overline{4029} = 7 - 2$,	$\overline{5482} = 14 - 7$,
$\overline{4073} = 12 - 1$,	$\overline{5491} = 18 - 8$,	$\overline{4082} = 8 - 1$,	$\overline{5478} = 13 - 8$,
$\overline{4087} = 10 - 5$,	$\overline{5479} = 16 - 10$,	$\overline{4023} = 10 - 3$,	$\overline{5481} = 16 - 12$,
$\overline{4079} = 11 - 4$,	$\overline{5492} = 17 - 11$,	$\overline{4012} = 9 - 4$,	$\overline{5438} = 15 - 11$,
$\overline{5081} = 18 - 2$,	$\overline{6493} = 21 - 8$,	$\overline{5032} = 18 - 4$,	$\overline{6471} = 22 - 9$,
$\overline{5071} = 15 - 1$,	$\overline{6438} = 20 - 9$,	$\overline{5039} = 15 - 5$,	$\overline{6418} = 24 - 11$,
$\overline{5019} = 14 - 3$,	$\overline{6473} = 24 - 7$,	$\overline{5073} = 17 - 3$,	$\overline{6491} = 23 - 12$,
$\overline{5012} = 13 - 6$,	$\overline{6432} = 19 - 12$,	$\overline{5083} = 16 - 6$,	$\overline{6412} = 21 - 10$,
$\overline{6018} = 20 - 3$,	$\overline{6512} = 19 - 15$,	$\overline{6092} = 20 - 1$,	$\overline{6578} = 19 - 14$,
$\overline{6083} = 21 - 2$,	$\overline{6523} = 24 - 13$,	$\overline{6079} = 19 - 2$,	$\overline{6597} = 20 - 13$,
$\overline{6078} = 23 - 4$,	$\overline{6592} = 22 - 16$,	$\overline{6093} = 23 - 6$,	$\overline{6518} = 22 - 18$,
$\overline{6082} = 22 - 5$,	$\overline{6528} = 23 - 17$,	$\overline{6019} = 24 - 5$,	$\overline{6517} = 21 - 17$;
Класс 4:			
$\overline{408173} = 11 - 1$,	$\overline{549237} = 18 - 11$,	$\overline{402819} = 7 - 3$,	$\overline{547183} = 16 - 7$,
$\overline{407918} = 12 - 4$,	$\overline{541932} = 14 - 10$,	$\overline{408321} = 10 - 2$,	$\overline{547821} = 15 - 8$,
$\overline{409387} = 10 - 6$,	$\overline{547391} = 17 - 8$,	$\overline{403912} = 8 - 4$,	$\overline{543287} = 14 - 12$,
$\overline{403917} = 7 - 5$,	$\overline{547129} = 16 - 9$,	$\overline{408293} = 9 - 1$,	$\overline{541832} = 13 - 11$,
$\overline{501287} = 14 - 6$,	$\overline{643297} = 20 - 12$,	$\overline{503879} = 15 - 4$,	$\overline{647819} = 24 - 10$,
$\overline{508192} = 18 - 1$,	$\overline{643879} = 19 - 9$,	$\overline{502973} = 16 - 3$,	$\overline{641297} = 21 - 11$,
$\overline{501879} = 13 - 3$,	$\overline{648392} = 21 - 7$,	$\overline{508237} = 18 - 5$,	$\overline{647128} = 23 - 9$,
$\overline{507921} = 15 - 2$,	$\overline{642873} = 24 - 8$,	$\overline{508392} = 17 - 6$,	$\overline{648291} = 22 - 12$,
$\overline{601289} = 21 - 5$,	$\overline{659123} = 23 - 13$,	$\overline{609371} = 23 - 1$,	$\overline{651978} = 19 - 18$,
$\overline{608371} = 22 - 2$,	$\overline{659283} = 22 - 15$,	$\overline{601297} = 20 - 6$,	$\overline{653817} = 20 - 17$,
$\overline{603218} = 20 - 4$,	$\overline{652819} = 24 - 17$,	$\overline{602379} = 24 - 2$,	$\overline{659371} = 22 - 14$,
$\overline{607328} = 23 - 3$,	$\overline{651238} = 19 - 16$,	$\overline{603912} = 19 - 5$,	$\overline{659783} = 21 - 13$;

Класс 5:

$$\begin{aligned} \overline{5471} &= 15 - 7 = 17 - 9, & \overline{5432} &= 18 - 10 = 13 - 12, & \overline{6492} &= 20 - 7 = 22 - 11, & \overline{6478} &= 23 - 10 = 19 - 8, \\ \overline{5082} &= 14 - 1 = 17 - 5, & \overline{5079} &= 16 - 4 = 13 - 2, & \overline{6073} &= 24 - 1 = 22 - 3, & \overline{6012} &= 21 - 4 = 19 - 6, \\ \overline{4019} &= 8 - 3 = 12 - 5, & \overline{4083} &= 11 - 6 = 9 - 2, & \overline{6518} &= 20 - 18 = 24 - 16, & \overline{6593} &= 23 - 15 = 21 - 14; \end{aligned}$$

Класс 6:

$$\begin{aligned} \overline{4013} &= 9 - 3 = 12 - 6, & \overline{5472} &= 13 - 7 = 17 - 10, & \overline{4089} &= 8 - 2 = 11 - 5, & \overline{5431} &= 18 - 9 = 15 - 12, \\ \overline{5072} &= 13 - 1 = 17 - 4, & \overline{6498} &= 23 - 11 = 20 - 8, & \overline{5089} &= 14 - 2 = 16 - 5, & \overline{6472} &= 22 - 10 = 19 - 7, \\ \overline{6013} &= 21 - 3 = 24 - 6, & \overline{6513} &= 24 - 15 = 21 - 18, & \overline{6072} &= 22 - 4 = 19 - 1, & \overline{6598} &= 23 - 16 = 20 - 14; \end{aligned}$$

Класс 7:

$$\begin{aligned} \overline{401782} &= 9 - 5 = 8 - 6, & \overline{501932} &= 13 - 5 = 14 - 4, & \overline{548192} &= 17 - 12 = 18 - 7, \\ \overline{402973} &= 12 - 2 = 11 - 3, & \overline{507183} &= 16 - 1 = 17 - 2, & \overline{547938} &= 13 - 9 = 15 - 10, \\ \overline{607819} &= 19 - 3 = 24 - 4, & \overline{649371} &= 22 - 8 = 23 - 7, & \overline{659712} &= 20 - 15 = 21 - 16, \\ \overline{608392} &= 22 - 6 = 21 - 1, & \overline{643812} &= 19 - 11 = 20 - 10, & \overline{657328} &= 23 - 18 = 24 - 14; \end{aligned}$$

Класс 8:

$$\begin{aligned} \overline{408193} &= 10 - 1, & \overline{401839} &= 7 - 4, & \overline{502978} &= 15 - 3, & \overline{509287} &= 18 - 6, \\ \overline{601237} &= 20 - 5, & \overline{601237} &= 23 - 2, & \overline{541237} &= 14 - 11, & \overline{541237} &= 16 - 8, \\ \overline{642978} &= 24 - 9, & \overline{642978} &= 21 - 12, & \overline{658193} &= 22 - 13, & \overline{658193} &= 19 - 17; \end{aligned}$$

Класс 9:

$$\begin{aligned} \overline{40217983} &= 11 - 2, & \overline{54217983} &= 15 - 9, & \overline{40217983} &= 8 - 5, & \overline{54217983} &= 13 - 10, \\ \overline{40217983} &= 9 - 6, & \overline{54217983} &= 18 - 12, & \overline{40217983} &= 12 - 3, & \overline{54217983} &= 17 - 7, \\ \overline{50217983} &= 16 - 2, & \overline{64217983} &= 23 - 8, & \overline{50217983} &= 14 - 5, & \overline{64217983} &= 19 - 10, \\ \overline{50217983} &= 13 - 4, & \overline{64217983} &= 20 - 11, & \overline{50217983} &= 17 - 1, & \overline{64217983} &= 22 - 7, \\ \overline{60217983} &= 22 - 1, & \overline{65217983} &= 23 - 14, & \overline{60217983} &= 24 - 3, & \overline{65217983} &= 21 - 15, \\ \overline{60217983} &= 19 - 4, & \overline{65217983} &= 20 - 16, & \overline{60217983} &= 21 - 6, & \overline{65217983} &= 24 - 18; \end{aligned}$$

Класс 10:

$$\begin{aligned} \overline{7129} &= 6 - 2 = 11 - 9, & \overline{7328} &= 12 - 8 = 5 - 3, & \overline{8123} &= 4 - 2 = 16 - 13, \\ \overline{9371} &= 5 - 1 = 17 - 14, & \overline{9281} &= 3 - 1 = 24 - 22, & \overline{9783} &= 21 - 19 = 4 - 6, \\ \overline{8293} &= 9 - 7 = 17 - 15, & \overline{9187} &= 18 - 13 = 10 - 12, & \overline{9321} &= 10 - 8 = 23 - 19, \\ \overline{8371} &= 22 - 20 = 11 - 7, & \overline{2178} &= 15 - 14 = 23 - 21, & \overline{9237} &= 18 - 16 = 20 - 24; \end{aligned}$$

Класс 11:

$$\begin{aligned} \overline{9381} &= 4 - 1 = 17 - 13 = 22 - 19 = 10 - 7, & \overline{7123} &= 5 - 2 = 11 - 8 = 16 - 14 = 23 - 20, \\ \overline{7928} &= 12 - 9 = 15 - 18 = 24 - 21 = 6 - 3. \end{aligned}$$

Табл. 3.3 является таблицей сложения выписанных здесь укрупненных классов подгруппы G_{5a} .

Удалим из нашего графа (рис 3.10) ребро 9; вслед за этим исчезнут цепи 2, 3, 4, 5, 9, 10, 17, 18, 20, 21, 22, 23 и от подгруппы G_{5a} останется подгруппа, определяемая цепями {1, 6, 7, 8, 11, 12, 13, 14, 15, 16, 19, 24}. Выпишем все подгруппы группы G_{5a} :

$$\begin{aligned} \{1, 2\}, & \{13, 14\}, \{1, 7\}, \{8, 14\}, \{22, 23\}, \{13, 15\}, \{20, 21\}, \{10, 11\}, \\ \{3, 4\}, & \{15, 16\}, \{2, 20\}, \{9, 21\}, \{16, 17\}, \{19, 24\}, \{7, 12\}, \{8, 9\}, \\ \{5, 6\}, & \{17, 18\}, \{3, 18\}, \{11, 16\}, \{15, 23\}, \{7, 20\}, \{6, 11\}, \{1, 14\}, \\ \{7, 8\}, & \{19, 20\}, \{4, 10\}, \{12, 24\}, \{16, 24\}, \{10, 18\}, \{9, 17\}, \{2, 13\}, \\ \{9, 10\}, & \{21, 22\}, \{5, 23\}, \{13, 19\}, \{14, 18\}, \{2, 3\}, \{4, 5\}, \{1, 6\}, \\ \{11, 12\}, & \{23, 24\}, \{6, 15\}, \{17, 22\}, \{5, 12\}, \{3, 22\}, \{8, 19\}, \{4, 21\}; \end{aligned}$$

Таблица 3.3

+	1	2	3	4	5	6	7	8	9	10	11
1	—	3	2, 5	7, 10	3	6	4	11	9	4	8
2	3	10	1, 4, 6, 7	3, 5, 8, 9	4, 6	3, 5	3, 9	4	4, 7	2, 11	10
3	2, 5	1, 4, 6, 7	4, 6, 7, 10	2, 3, 5, 9, 11	1, 4, 6, 10	2, 3, 5	2, 3, 8, 9	7, 10	4, 7, 10	3, 5, 8, 9	4
4	7, 10	3, 5, 8, 9	2, 3, 5, 9, 11	4, 6, 7, 10	2, 3, 8, 9	4, 7, 10	1, 4, 6, 10	2, 5	2, 3, 5	1, 4, 6, 7	3
5	3	4, 6	1, 4, 6, 10	2, 3, 8, 9	7	2, 3	5, 11	4	4, 10	3, 9	7
6	6	3, 5	2, 3, 5	4, 7, 10	2, 3	1	4, 10	9	8, 11	4, 7	9
7	4	3, 9	2, 3, 8, 9	1, 4, 6, 10	5, 11	4, 10	7	3	2, 3	4, 6	5
8	11	4	7, 10	2, 5	4	9	3	—	6	3	1
9	9	4, 7	4, 7, 10	2, 3, 5	4, 10	8, 11	2, 3	6	1	3, 5	6
10	4	2, 11	3, 5, 8, 9	1, 4, 6, 7	3, 9	4, 7	4, 6	3	3, 5	10	2
11	8	10	4	3	7	9	5	1	6	2	—

{2, 19, 20}, {5, 23, 24}, {1, 2, 20}, {5, 6, 23}, {3, 17, 18}, {3, 4, 18},
 {5, 6, 15}, {6, 15, 16}, {3, 4, 10}, {4, 9, 10}, {1, 2, 7}, {1, 7, 8},
 {17, 18, 22}, {17, 21, 22}, {13, 19, 20}, {13, 14, 19}, {9, 21, 22}, {9, 10, 21},
 {12, 23, 24}, {11, 12, 24}, {11, 15, 16}, {8, 13, 14}, {11, 12, 16}, {7, 8, 14};

{1, 6, 13, 15}, {3, 17, 18, 22}, {7, 12, 13, 15}, {13, 15, 19, 24},
 {1, 6, 19, 24}, {3, 4, 10, 18}, {7, 8, 9, 10}, {13, 14, 15, 16},
 {1, 6, 7, 12}, {3, 4, 5, 6}, {7, 8, 11, 12}, {13, 14, 17, 18},
 {1, 7, 8, 14}, {4, 5, 16, 17}, {8, 9, 20, 21}, {14, 18, 20, 21},
 {1, 2, 7, 20}, {4, 5, 22, 23}, {8, 9, 14, 18}, {15, 16, 17, 18},
 {1, 2, 3, 4}, {4, 5, 10, 11}, {8, 13, 14, 19}, {16, 17, 22, 23},
 {1, 2, 5, 6}, {4, 9, 10, 21}, {9, 17, 21, 22}, {19, 20, 23, 24},
 {2, 3, 14, 18}, {5, 6, 15, 23}, {9, 10, 11, 12}, {19, 20, 21, 22},
 {2, 3, 20, 21}, {5, 12, 23, 24}, {10, 11, 22, 23}, {21, 22, 23, 24},
 {2, 3, 8, 9}, {6, 11, 15, 16}, {10, 11, 16, 17},
 {2, 13, 19, 20}, {7, 12, 19, 24}, {11, 12, 16, 24},

{1, 2, 3, 4, 20, 21}, {2, 3, 13, 14, 17, 18}, {8, 9, 13, 14, 17, 18},
 {1, 2, 5, 6, 7, 12}, {3, 4, 5, 6, 10, 11}, {8, 9, 14, 18, 20, 21},
 {1, 2, 3, 4, 14, 18}, {3, 4, 5, 6, 22, 23}, {8, 9, 19, 20, 21, 22},
 {1, 2, 3, 4, 5, 6}, {4, 5, 9, 10, 11, 12}, {9, 10, 11, 12, 16, 17},
 {1, 2, 5, 6, 13, 15}, {4, 5, 10, 11, 22, 23}, {10, 11, 13, 14, 15, 16},
 {1, 6, 7, 12, 19, 24}, {4, 5, 16, 17, 22, 23}, {10, 11, 16, 17, 22, 23},
 {1, 6, 7, 12, 13, 15}, {4, 5, 21, 22, 23, 24}, {13, 14, 15, 16, 17, 18},
 {1, 6, 7, 8, 11, 12}, {4, 5, 10, 11, 16, 17}, {13, 15, 19, 20, 23, 24},
 {1, 6, 13, 14, 15, 16}, {7, 8, 9, 10, 20, 21}, {13, 14, 15, 16, 19, 24},
 {1, 6, 13, 15, 19, 24}, {7, 8, 11, 12, 19, 24}, {15, 16, 17, 18, 22, 23},
 {2, 3, 8, 9, 14, 18}, {7, 8, 9, 10, 14, 18}, {16, 17, 21, 22, 23, 24},
 {2, 3, 8, 9, 20, 21}, {7, 8, 9, 10, 11, 12}, {19, 20, 21, 22, 23, 24},
 {2, 3, 14, 18, 20, 21}, {7, 12, 13, 15, 19, 24},
 {2, 3, 19, 20, 21, 22}, {7, 12, 19, 20, 23, 24},

{1, 2, 3, 4, 7, 8, 9, 10}, {2, 3, 8, 9, 13, 14, 17, 18}, {4, 5, 16, 17, 21, 22, 23, 24},
 {1, 2, 3, 4, 14, 18, 20, 21}, {2, 3, 8, 9, 14, 18, 20, 21}, {7, 8, 9, 10, 14, 18, 20, 21},
 {1, 2, 5, 6, 7, 12, 13, 15}, {2, 3, 8, 9, 19, 20, 21, 22}, {7, 8, 11, 12, 13, 14, 15, 16},

$\{1, 2, 5, 6, 19, 20, 23, 24\}, \{3, 4, 5, 6, 15, 16, 17, 18\}, \{7, 12, 13, 15, 19, 20, 23, 24\},$
 $\{1, 6, 7, 12, 13, 15, 19, 24\}, \{3, 4, 5, 6, 10, 11, 22, 23\}, \{9, 10, 11, 12, 21, 22, 23, 24\},$
 $\{1, 6, 7, 8, 11, 12, 19, 24\}, \{4, 5, 9, 10, 11, 12, 16, 17\}, \{10, 11, 15, 16, 17, 18, 22, 23\},$
 $\{1, 6, 13, 14, 15, 16, 19, 24\}, \{4, 5, 10, 11, 16, 17, 22, 23\}, \{13, 14, 17, 18, 19, 20, 21, 22\};$
 $\{1, 2, 3, 4, 7, 8, 9, 10, 14, 18\}, \{3, 4, 5, 6, 10, 11, 15, 16, 17, 18\},$
 $\{1, 2, 3, 4, 7, 8, 9, 10, 20, 21\}, \{3, 4, 5, 6, 15, 16, 17, 18, 22, 23\},$
 $\{1, 2, 5, 6, 7, 12, 19, 20, 23, 24\}, \{4, 5, 9, 10, 11, 12, 21, 22, 23, 24\},$
 $\{1, 2, 5, 6, 13, 15, 19, 20, 23, 24\}, \{7, 8, 11, 12, 13, 14, 15, 16, 19, 24\},$
 $\{1, 6, 7, 8, 11, 12, 13, 14, 15, 16\}, \{8, 9, 13, 14, 17, 18, 19, 20, 21, 22\},$
 $\{2, 3, 13, 14, 17, 18, 19, 20, 21, 22\}, \{9, 10, 11, 12, 16, 17, 21, 22, 23, 24\};$
 $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}, \{2, 3, 8, 9, 13, 14, 17, 18, 19, 20, 21, 22\},$
 $\{1, 2, 3, 4, 5, 6, 13, 14, 15, 16, 17, 18\}, \{3, 4, 5, 6, 10, 11, 15, 16, 17, 18, 22, 23\},$
 $\{1, 2, 3, 4, 5, 6, 19, 20, 21, 22, 23, 24\}, \{4, 5, 9, 10, 11, 12, 16, 17, 21, 22, 23, 24\},$
 $\{1, 2, 3, 4, 7, 8, 9, 10, 14, 18, 20, 21\}, \{7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18\},$
 $\{1, 2, 5, 6, 7, 12, 13, 15, 19, 20, 23, 24\}, \{7, 8, 9, 10, 11, 12, 19, 20, 21, 22, 23, 24\},$
 $\{1, 6, 7, 8, 11, 12, 13, 14, 15, 16, 19, 24\}, \{13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24\};$
 $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18\},$
 $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 19, 20, 21, 22, 23, 24\},$
 $\{1, 2, 3, 4, 5, 6, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24\},$
 $\{7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24\}.$

В 1859 г. сэр Вильям Гамильтон, знаменитый ирландский математик, давший миру теорию комплексного числа и кватерниона, предложил детскую головоломку, в которой предлагалось совершить «кругосветное путешествие» по 20 городам, расположенным в различных частях земного шара. Каждый город соединялся дорогами с тремя соседними так, что дорожная сеть образовывала 30 ребер додекаэдра, в вершинах которого находились города $a, b, \dots, t$ (рис. 3.11). Обязательным условием являлось требование: каждый город, за исключением первого, можно посетить лишь один раз.

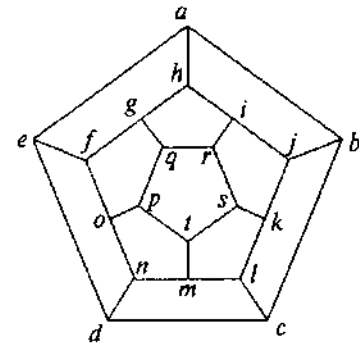


Рис. 3.11

Если путешествие начать из города a , то последними должны быть города b, e или h , иначе мы не сможем вернуться в первоначальный пункт a . Непосредственное исчисление показывает, что число таких замкнутых маршрутов равно 60.

Можно потребовать посещения всех городов строго по одному разу, включая и первый, т.е. допускается окончание путешествия в любом городе (например, предполагается, что в начальный пункт можно будет вернуться самолетом). Тогда общее число цепных маршрутов увеличится до 162. В табл. 3.4 перечислены все эти цепи, причем в специально организованной последовательности.

Принцип организации цепей для додекаэдра выбран тот же, что и ранее для куба, т.е. принцип инверсии хвостовой последовательности вершин. Однореберная замена касается 1, 4, 7, 10, 13 или 16 ребра. Таким образом, получается 11 циклов по 15 цепей в каждом, за исключением трех последних, где насчитывается по 14 цепей.

Рассматривая табл. 3.4, можно заметить, что ни один из предложенных дорожных маршрутов не заканчивается в пунктах c, d, f, g, i и j . В пункте t заканчиваются только 6 маршрутов, в пунктах m, p и s — по 8 для каждого пункта, в l, k, n, o, q, r — по 12 и в b, e, h — по 20. Это происходит потому, что для додекаэдра существует пять классов вершин и семь классов ребер, которые в табл. 3.5 количественно разнесены по 11 циклам.

В столбце S табл. 3.4 указана симметрия цепи, которая для додекаэдра определяется так же, как и для куба. Общее число цепей додекаэдра равно произведению $162 \times 10 = 1620$. Подгруппа G_{20a} состоит из $162 \times 161 + 1 = 26\,083$ переходов между цепями, привязанными к вершине a . В группе же G_{20} насчитывается почти в сто раз больше переходов.

Гамильтонова задача о путешественнике нередко преобразуется в задачу о коммивояжере. Коммивояжер — не праздное путешествующий турист, а деловой человек, ограниченный временными, денежными или какими-либо другими ресурсами. Пусть каждое из ребер снабжено числовой характеристикой: это может быть километраж, время на дорогу или стоимость билета. Таким образом, условные характеристики ребер дадут числовой ряд от 1 до 30, элементы которого могут быть распределены между ребрами додекаэдра как угодно, в частности, в табл. 3.5 дается три варианта распределения реберных характеристик — A, B и C .

Таблица 3.4

№	Гамильтоновы цепи	S	Δ_i	ΣA	ΣB	ΣC
Цикл 1						
1	<i>abclkjihgfednmtsrqpo</i>	s	$-\Delta_{16}$	342	247	302
2	<i>abclkjihgfednopqrstm</i>	a	$-\Delta_{17}$	349	240	299
3	<i>abclmtsrqpondefghijk</i>	s	$-\Delta_7$	339	250	302
4	<i>abclmtskjihgfednopqr</i>	s	$-\Delta_{11}$	341	248	307
5	<i>abclmtskjirqpondefgh</i>	a	Δ_1	321	268	318
6	<i>ahgfednopqrijkstmclb</i>	a	$-\Delta_{12}$	320	269	313
7	<i>ahgfednopqrijbclmtsk</i>	a	Δ_{17}	338	251	312
8	<i>ahgfednopqrijbclktm</i>	s	Δ_{16}	348	241	309
9	<i>ahgfednmtsklcbjirqpo</i>	a	$-\Delta_{10}$	341	248	312
10	<i>ahgfopqrijbclktmnde</i>	a	Δ_3	319	270	301
11	<i>aednmtsklcbjirqpofgh</i>	a	Δ_{11}	318	271	302
12	<i>aednmtsklcbjihgfopqr</i>	a	Δ_7	338	251	291
13	<i>aednmtsrqpfghijbclkt</i>	a	Δ_{12}	336	253	286
14	<i>aednmtsrqpfghijklcb</i>	a	Δ_2	318	271	287
15	<i>abclkjihgfopqrstmnde</i>	a	Δ_{10}	320	269	291
Цикл 2						
16	<i>aednofghijbclmtpqrsk</i>	s	Δ_{17}	331	258	300
17	<i>aednofghijbclksrqptm</i>	a	Δ_{16}	341	248	297
18	<i>aednmtprsklcbjihgfo</i>	s	Δ_8	334	241	300
19	<i>aednmtpfghijbclksrq</i>	s	Δ_{13}	333	242	312
20	<i>aednmtpfqgrsklcbjih</i>	a	$-\Delta_3$	309	266	323
21	<i>ahijbclksrqgfopmtnde</i>	a	Δ_{10}	310	265	322
22	<i>ahijbclksrqgfednmtpo</i>	a	$-\Delta_{16}$	332	243	333

№	Гамильтоновы цепи	S	Δ_i	ΣA	ΣB	ΣC
23	<i>ahijbclksrqgfednoptm</i>	s	$-\Delta_{17}$	339	250	330
24	<i>ahijbclmtpondelfgqrsk</i>	a	Δ_{12}	329	260	333
25	<i>ahijksrqgfednoptmlcb</i>	a	$-\Delta_1$	311	278	334
26	<i>abclmtpondelfgqrskjih</i>	a	$-\Delta_{13}$	312	277	339
27	<i>abclmtpondelfghijksrq</i>	a	$-\Delta_8$	336	253	328
28	<i>abclmtpqrsjkjihgfedno</i>	a	Δ_{10}	337	252	316
29	<i>abclmtpqrsjkjihgfonde</i>	a	$-\Delta_2$	315	274	305
30	<i>aednofghijksrqptmlcb</i>	a	$-\Delta_{12}$	313	276	301
Цикл 3						
31	<i>ahgqrijbcedefoptsklmn</i>	s	Δ_{15}	325	264	299
32	<i>ahgqrijbcedefonmlkstp</i>	a	Δ_{19}	330	259	294
33	<i>ahgqptsklmnofedcbjir</i>	s	Δ_7	324	265	281
34	<i>ahgqptsrijbcedefonmlk</i>	s	Δ_{12}	322	267	276
35	<i>ahgqptsrijklmnofedcb</i>	a	$-\Delta_1$	304	285	277
36	<i>abcedefonmlkjirstpqgh</i>	a	Δ_{11}	305	284	282
37	<i>abcedefonmlkjihqptsr</i>	a	$-\Delta_{19}$	325	264	271
38	<i>abcedefonmlkjihgqrstp</i>	s	$-\Delta_{18}$	331	258	284
39	<i>abcedefoptsrqghijklmn</i>	a	Δ_{14}	326	263	289
40	<i>abcdnmlkjihgqrstpofe</i>	a	$-\Delta_2$	305	284	295
41	<i>aefoptsrqghijklmndcb</i>	a	$-\Delta_{12}$	303	286	291
42	<i>aefoptsrqghijbcdnmlk</i>	a	$-\Delta_7$	321	268	290
43	<i>aefoptsklmndcbjihgqr</i>	a	$-\Delta_{11}$	323	266	295
44	<i>aefoptsklmndcbjirqgh</i>	a	$-\Delta_3$	303	286	306
45	<i>ahgqrijbcdnmlkstpofe</i>	a	$-\Delta_{14}$	304	285	305
Цикл 4						
46	<i>ahirqgfedcbjksponml</i>	s	$-\Delta_{20}$	323	266	326
47	<i>ahirqgfedcbjklmnopts</i>	a	$-\Delta_{21}$	330	259	320
48	<i>ahirstponmlkjbcdefgq</i>	s	$-\Delta_8$	320	269	316
49	<i>ahirstpqgfedcbjklmno</i>	s	$-\Delta_{10}$	321	268	304
50	<i>ahirstpqgfonmlkjbcde</i>	a	Δ_3	299	290	293
51	<i>aedcbjklmnofgqptsrih</i>	a	$-\Delta_{13}$	298	291	294
52	<i>aedcbjklmnofghirstpq</i>	a	Δ_{21}	322	267	283
53	<i>aedcbjklmnofghirqpts</i>	s	Δ_{20}	332	257	287
54	<i>aedcbjksptqrihgfonml</i>	a	$-\Delta_{15}$	325	264	293
55	<i>aedclmnofghirqptsjkb</i>	a	Δ_2	304	285	281
56	<i>abjksptqrihgfonmlcde</i>	a	Δ_{10}	306	283	285
57	<i>abjksptqrihgfedclmno</i>	a	Δ_8	328	261	296
58	<i>abjksptponmlcdefghirq</i>	a	Δ_{13}	327	262	308
59	<i>abjksptponmlcdefgqrih</i>	a	Δ_1	303	286	319
60	<i>ahirqgfedclmnoptsjkb</i>	a	Δ_{15}	302	287	314
Цикл 5						
61	<i>aefondcbjihgqptmlksr</i>	s	$-\Delta_{19}$	322	267	299
62	<i>aefondcbjihgqrsklmtp</i>	a	$-\Delta_{18}$	328	261	312
63	<i>aefoptmlksrqghijbcdn</i>	s	$-\Delta_9$	323	266	317

№	Гамильтоновы цепи	S	Δ_i	ΣA	ΣB	ΣC
64	<i>aefoptmndcbjihgqrskl</i>	s	$-\Delta_{15}$	325	264	316
65	<i>aefoptmndclksrqghijb</i>	a	Δ_2	304	285	304
66	<i>abjihgqrsklcdnmtpofe</i>	a	$-\Delta_{14}$	306	283	308
67	<i>abjihgqrsklcdefoptmn</i>	a	Δ_{18}	327	264	302
68	<i>abjihgqrsklcdefonmtp</i>	s	Δ_{19}	332	257	297
69	<i>abjihgqptmnofedclksr</i>	a	$-\Delta_{11}$	326	263	284
70	<i>abjirsklcdefonmtpqgh</i>	a	Δ_1	306	283	295
71	<i>ahgqptmnofedclksrijb</i>	a	Δ_{15}	305	284	290
72	<i>ahgqptmnofedcbjirskl</i>	a	Δ_9	326	263	302
73	<i>ahgqptmlksrijbcdefon</i>	a	Δ_{14}	324	265	303
74	<i>ahgqptmlksrijbcdnife</i>	a	Δ_3	303	286	309
75	<i>aefondcbjirsklmtpqgh</i>	a	Δ_{11}	302	287	310
Цикл 6						
76	<i>abjklcdefghirstmnopq</i>	s	Δ_{21}	331	258	298
77	<i>abjklcdefghirqponmts</i>	a	Δ_{20}	341	248	302
78	<i>abjkstmnopqrihgfedcl</i>	s	Δ_9	334	255	308
79	<i>abjkstmlcdefghirqpon</i>	s	Δ_{14}	332	257	309
80	<i>abjkstmlcdnopqrihgfe</i>	a	$-\Delta_2$	311	278	315
81	<i>aefghirqpondclmtskjb</i>	a	Δ_{15}	309	280	311
82	<i>aefghirqpondcbjkstml</i>	a	$-\Delta_{20}$	330	259	323
83	<i>aefghirqpondcbjklmts</i>	s	$-\Delta_{21}$	337	252	317
84	<i>aefghirstmlkjbcnopq</i>	a	Δ_{13}	327	262	313
85	<i>aefgqpondcbjklmtsrih</i>	a	$-\Delta_3$	303	286	324
86	<i>ahirstmlkjbcnopqgfe</i>	a	$-\Delta_{14}$	304	285	323
87	<i>ahirstmlkjbcdefgqpon</i>	a	Δ_9	325	264	317
88	<i>ahirstmnopqgfedclbjkl</i>	a	$-\Delta_{15}$	327	262	316
89	<i>ahirstmnopqgfedclkjib</i>	a	$-\Delta_1$	306	283	304
90	<i>abjklcdefgqponmtsrih</i>	a	$-\Delta_{13}$	307	282	309
Цикл 7						
91	<i>ahgfedclkstmnopqrijb</i>	a	Δ_{15}	335	254	304
92	<i>ahgfedcbjirqponmtskl</i>	a	Δ_{22}	356	233	316
93	<i>ahgfedcbjirqponmlkst</i>	s	$-\Delta_{23}$	348	241	312
94	<i>ahgfedcbjirqptsklmno</i>	a	$-\Delta_{10}$	350	239	304
95	<i>ahgfomlksptqrijbcde</i>	s	Δ_3	328	261	293
96	<i>aedcbjirqptsklmnofgh</i>	a	Δ_{11}	327	262	294
97	<i>aedcbjihgfonmlkstpqr</i>	a	Δ_{26}	347	242	283
98	<i>aedcbjihgfonmlksrapt</i>	s	$-\Delta_{22}$	341	248	300
99	<i>aedcbjihgfonmtpqrskl</i>	a	$-\Delta_{12}$	349	240	304
100	<i>aedclksraptmnofghijb</i>	s	Δ_2	328	261	292
101	<i>abjihgfonmtpqrsklcde</i>	a	Δ_{10}	330	259	296
102	<i>abjihgfedclksraptmno</i>	a	Δ_{23}	352	237	307
103	<i>abjihgfedclksraponmt</i>	s	$-\Delta_{26}$	350	239	315
104	<i>abjihgfedclkstmnopqr</i>	a	$-\Delta_{11}$	356	233	298
105	<i>abjirqponmtskldefgh</i>	s	Δ_1	336	253	309

№	Гамильтоновы цепи	S	Δ_i	ΣA	ΣB	ΣC
Цикл 8						
106	<i>ahijbcdnoptmiksrggfe</i>	a	$-\Delta_{14}$	324	265	344
107	<i>ahijbcdefgqrsklmtpon</i>	a	$-\Delta_{25}$	345	244	338
108	<i>ahijbcdefgqrsklmnopt</i>	s	Δ_{27}	339	250	333
109	<i>ahijbcdefgqrstponmlk</i>	a	Δ_{12}	343	241	311
110	<i>ahijklmnoptsrggfedcb</i>	s	$-\Delta_1$	325	264	312
111	<i>abcdefgqrstponmlkjih</i>	a	$-\Delta_{13}$	326	263	317
112	<i>abcdefghijklmnoptsrq</i>	a	$-\Delta_{24}$	350	239	306
113	<i>abcdefghijklmnopqrst</i>	s	Δ_{25}	349	240	302
114	<i>abcdefghijklmtrsrapon</i>	a	Δ_{14}	355	234	307
115	<i>abcdnopqrstmlkjihgfe</i>	s	$-\Delta_2$	334	255	313
116	<i>aefghijklmtrsrapondcb</i>	a	$-\Delta_{12}$	332	257	309
117	<i>aefghijbcdnopqrstmlk</i>	a	$-\Delta_{27}$	350	239	308
118	<i>aefghijbcdnopqrsklmt</i>	s	Δ_{24}	346	243	330
119	<i>aefghijbcdnoptmiksrg</i>	a	Δ_{13}	347	242	334
120	<i>aefgqrsklmtpondcbjih</i>	s	$-\Delta_3$	323	266	345
Цикл 9						
121	<i>ahgqpofednmtsrijklcb</i>	a	$-\Delta_{12}$	295	294	285
122	<i>ahgqpofednmtsrijbclik</i>	a	$-\Delta_7$	313	276	284
123	<i>ahgqpofednmtsklcbjir</i>	s	$-\Delta_{19}$	315	274	289
124	<i>ahgqrijbclktmndefop</i>	s	Δ_4	321	268	302
125	<i>ahgqrijbclktspofednm</i>	a	$-\Delta_{17}$	319	270	291
126	<i>ahgqrijbclmndefoptsk</i>	a	Δ_{12}	309	280	294
127	<i>ahgqrijkstspofednmlcb</i>	s	$-\Delta_1$	291	298	295
128	<i>abclmndefoptskijrqgh</i>	a	Δ_{11}	292	297	300
129	<i>abclmndefoptskjihgqr</i>	a	Δ_7	312	277	289
130	<i>abclmndefoptsrqghijk</i>	s	Δ_{17}	310	279	284
131	<i>abclkihgqrstspofednm</i>	s	$-\Delta_4$	320	269	281
132	<i>abclkihgqrstmnndefop</i>	a	Δ_{19}	322	267	292
133	<i>abclkihgqpofednmtsr</i>	a	$-\Delta_{11}$	316	273	279
134	<i>abclkjirstmnndefopqgh</i>	s	Δ_1	296	293	290
Цикл 10						
135	<i>ahirskjbcclmtppqgfonde</i>	a	Δ_{10}	285	304	315
136	<i>ahirskjbcclmtppqgfedno</i>	a	Δ_8	307	282	326
137	<i>ahirskjbcclmtpondefgq</i>	s	Δ_{21}	306	283	338
138	<i>ahirqgfednoptmlcbjks</i>	s	$-\Delta_5$	316	273	342
139	<i>ahirqgfednoptskjbcclm</i>	a	Δ_{16}	315	274	319
140	<i>ahirqgfednmlcbjkstpo</i>	a	$-\Delta_{10}$	308	281	322
141	<i>ahirqgfoptskjbcclmnde</i>	s	Δ_3	286	303	311
142	<i>aednmlcbjkstppqgrih</i>	a	$-\Delta_{13}$	285	304	312
143	<i>aednmlcbjkstppqghirq</i>	a	$-\Delta_8$	309	280	301
144	<i>aednmlcbjkstppqrihgfo</i>	s	$-\Delta_{16}$	310	279	289
145	<i>aednqfghirqstskjbcclm</i>	s	Δ_5	317	272	286

№	Гамильтоновы цепи	S	Δ_i	ΣA	ΣB	ΣC
146	<i>aednofghirqptmlcbjks</i>	a	Δ_{21}	318	271	309
147	<i>aednofghirskjbcmltpq</i>	a	Δ_{13}	308	281	305
148	<i>aednofgqptmlcbjksrih</i>	s	Δ_3	284	305	316
Цикл 11						
149	<i>aefopqghirstmndclkbj</i>	a	Δ_{15}	284	305	283
150	<i>aefopqghirstmndcbjkl</i>	a	Δ_9	305	284	295
151	<i>aefopqghirstmikjbcdn</i>	s	Δ_{18}	303	286	296
152	<i>aefondcbjklmtsrihgqp</i>	s	$-\Delta_6$	308	281	291
153	<i>aefondcbjklmtpqghirs</i>	a	Δ_{20}	307	282	303
154	<i>aefondcbjksrihgqptmi</i>	a	$-\Delta_{15}$	300	289	309
155	<i>aefondclmtpqghirskjb</i>	s	Δ_2	279	310	297
156	<i>abjksrihgqptmlcdnfe</i>	a	$-\Delta_{11}$	281	308	301
157	<i>abjksrihgqptmlcdefon</i>	a	$-\Delta_9$	302	287	295
158	<i>abjksrihgqptmnofedcl</i>	s	$-\Delta_{20}$	304	285	294
159	<i>abjklcdefonmtpqghirs</i>	s	Δ_8	311	278	288
160	<i>abjklcdefonmtsrihgqp</i>	a	$-\Delta_{16}$	312	277	276
161	<i>abjklcdefopqghirstmn</i>	a	Δ_{14}	307	282	281
162	<i>abjklcdnmtsrihgqpofe</i>	s	$-\Delta_2$	286	303	287

В литературе, например, Ж.-Л. Лорье «Системы искусственного интеллекта» (М.: Мир, 1991, с. 278–289), можно найти описания алгоритмов поиска маршрута с минимальной суммой реберных характеристик. Эти алгоритмы, как правило, не учитывают классификацию ребер, а значит и маршрутов, с *топологической* точки зрения; оптимизация ведется только по *метрическим* характеристикам ребер. Между тем, табл. 3.5 (столбец N) показывает, что чисто топологический вклад ребер в гамильтоновы маршруты весьма различен. Например, частота появления в гамильтоновой цепи ребра *bc* на 30 процентов превышает частоту появления, казалось бы, точно такого же ребра *cl*. Все ребра в додекаэдре равноправны, если не существует привязки. Но как только появляется привязка (начало путешествия или некий центр управления симметричной системой типа додекаэдра), тотчас появляется неравноправие между связями. Величина этого неравноправия, едва заметная для ребер классов C_3 , C_6 и C_7 , становится весьма ощутимой для ребер классов C_1 , C_2 , C_4 и C_5 .

Предположим, мы являемся не коммивояжерами и не путешественниками, а проектировщиками некой структуры типа додекаэдра, в которой используется ранжированная по 30 градациям система связей. В зависимости от исходного распределения реберных характеристик (табл. 3.5, столбцы A, B и C), мы будем иметь и совершенно различные системы распределения суммарных характеристик ΣA , ΣB и ΣC (табл. 3.4), которые называются *длинами*. Распределения A и B дают соответственно *максимальные* и *минимальные* длины относительно *всей* совокупности гамильтоновых цепей; распределение C — промежуточное.

Таблица 3.5

C_i	xy	1	2	3	4	5	6	7	8	9	10	11	N	A	B	C
C_1	ab	6	4	5	4	5	6	5	5	7	0	7	54	3	28	8
	ae	4	6	4	5	6	5	5	5	0	7	7	54	1	30	4
	ah	5	5	6	6	4	4	5	5	7	7	0	54	2	29	3
C_2	bc	15	15	15	9	8	7	8	15	14	14	5	125	30	1	18
	bj	7	9	8	15	15	15	15	8	5	14	14	125	25	6	13
	cd	15	15	9	15	7	8	15	8	14	14	5	125	29	2	11
	ef	9	7	15	8	15	15	8	15	14	5	14	125	27	4	12
	hg	15	8	15	7	15	9	15	8	14	5	14	125	28	3	9
	hi	8	15	7	15	9	15	8	15	5	14	14	125	27	5	10
C_3	cd	0	0	15	15	15	15	15	15	0	0	14	104	10	21	5
	fg	15	15	0	15	0	15	15	15	0	14	0	104	11	20	16
	ij	15	15	15	0	15	0	15	15	14	0	0	104	12	19	2
C_4	cl	15	15	0	6	7	8	7	0	14	14	9	95	9	22	6
	dn	15	15	6	0	8	7	0	7	14	14	9	95	8	23	17
	gq	0	7	15	8	15	6	0	7	14	9	14	95	4	27	20
	fo	6	8	15	7	15	0	7	0	14	9	14	95	5	26	1
	jk	8	6	7	15	0	15	0	7	9	14	14	95	7	24	14
	ir	7	0	8	15	6	15	7	0	9	14	14	95	6	25	21
C_5	rq	15	15	10	10	7	7	15	15	9	9	0	112	24	7	28
	on	7	10	7	15	10	15	15	15	0	9	9	112	22	9	22
	lk	10	7	15	7	15	10	15	15	9	0	9	112	23	8	23
C_6	pq	15	6	5	9	8	15	15	6	5	7	14	105	18	13	15
	po	15	9	8	6	5	15	6	15	14	7	5	105	17	14	27
	sk	9	15	6	8	15	5	15	6	7	14	5	105	16	15	29
	sr	6	15	9	5	15	8	6	15	7	5	14	105	14	17	24
	ml	5	8	15	15	6	9	6	15	5	14	7	105	13	18	26
	mn	8	5	15	15	9	6	15	6	14	5	7	105	15	16	25
C_7	tm	15	15	0	0	15	15	9	9	7	7	14	106	21	10	30
	tp	0	15	15	15	15	0	9	9	7	14	7	106	19	12	19
	ts	15	0	15	15	0	15	9	9	14	7	7	106	20	11	7
Сумма:		285	285	285	285	285	285	285	285	266	266	266	3078	465	465	465

Для привязки a существует 27 одnoreберных замен Δ_i , распадающихся на 6 классов (табл. 3.6). Для Δ_i выполняются следующие равенства:

$$\sum_{C_1} \Delta_i - \Delta_1 + \Delta_2 + \Delta_3 = 0, \quad \sum_{C_2} \Delta_i - \Delta_2 + \Delta_3 + \Delta_6 = 0,$$

$$\sum_{C_3} \Delta_i + \sum_{C_5} \Delta_i = 0, \quad \sum_{C_4} \Delta_i - \sum_{C_5} \Delta_i = 0, \quad \sum_{C_6} \Delta_i - \sum_{C_7} \Delta_i = 0.$$

Таблица 3.6

C_i	Δ_i	$xy - xz$	A	B	C	C_i	Δ_i	$xy - xz$	A	B	C
C_1	Δ_1	$ah - ab$	-1	1	-5	C_5	Δ_{16}	$nm - no$	-7	7	3
	Δ_2	$ab - ac$	2	-2	4		Δ_{17}	$lk - lm$	10	10	-3
	Δ_3	$ae - ah$	-1	1	1		Δ_{18}	$on - op$	5	-5	-5
C_2	Δ_4	$tp - tm$	-2	2	-11	C_5	Δ_{19}	$qp - qr$	-6	6	-13
	Δ_5	$tm - ts$	1	1	23		Δ_{20}	$ks - kl$	-7	7	6
	Δ_6	$ts - tp$	1	-1	-12		Δ_{21}	$rq - rs$	10	-10	4
C_3	Δ_7	$sr - sk$	-2	2	5	C_6	Δ_{22}	$ml - mt$	-8	8	4
	Δ_8	$pc - pq$	-1	1	12		Δ_{23}	$po - pt$	-2	2	8
	Δ_9	$ml - mn$	-2	2	1		Δ_{24}	$pt - pq$	1	-1	4
C_4	Δ_{10}	$fe - fo$	22	-22	11		Δ_{25}	$mt - mn$	6	-6	5
	Δ_{11}	$ih - ir$	20	-20	-11		Δ_{26}	$sr - st$	-6	6	17
	Δ_{12}	$jk - jb$	18	18	1		Δ_{27}	$st - sk$	4	-4	-22
	Δ_{13}	$qq - gh$	-24	24	11						
	Δ_{14}	$dn - de$	-21	21	6						
	Δ_{15}	$cb - cl$	21	-21	12						

Реберные разности Δ_i позволяют существенно сократить число операций при нахождении длин, поскольку каждая последующая цепь в цикле отличается от предыдущей на какую-то одну из 27 величин Δ_i . Следовательно, необходимо рассчитать 11 цепей для варианта ΣC , представляющих циклы, и столько же для ΣA ; для варианта ΣB длина может быть уже вычислена из формулы:

$$\Sigma B + \Sigma A = 589 = 31 \times 19 = \sum_{i=1}^{19} i + \sum_{i=12}^{30} i = 190 + 399,$$

где числа 190 и 399 отвечают самой короткой и самой длинной цепи, которые только и возможны.

Суммы всех длин гамильтоновых цепей по максимальному ($\Sigma \Sigma A$), минимальному ($\Sigma \Sigma B$) и промежуточному ($\Sigma \Sigma C$) вариантам распределения равны следующим величинам:

$$\Sigma \Sigma A = 51\,939, \quad \Sigma \Sigma B = 35\,747, \quad \Sigma \Sigma C = 46\,229,$$

что составляет весьма заметную разницу между вариантами распределения одних и тех же величин. Отметим также, что максимальная (минимальная) длина в 356 (233) условных единицы приходится на гамильтоновы цепи под номерами 92 и 104. Минимальное значение для промежуточного варианта распределения равно 271 (цепь 37), а максимальное — 345 (цепь 120).

Таким образом, мы продемонстрировали один из возможных подходов к графам. Эту тему мы начали с рассмотрения цепей; далее можно было бы переходить к анализу деревьев. Однако наша задача состоит в том, чтобы дать более широкую картину существующих методов, для чего в следующем подразделе мы введем новые понятия.

3.2. Виды графов. Пути и контуры в графе

На рис. 3.12 изображено множество точек V и множество линий E , соединяющих эти точки, которые все вместе образуют *граф* G . Если линии имеют стрелки, то граф называется *ориентированным* или *орграфом* G_0 (рис. 3.13). Внутренних различий между G и G_0 гораздо меньше, чем между графом, изображающим *правильную решетку* из подгрупп для какой-нибудь группы, например, $S(D_6^1)$ (рис. 2.18), и графом, изображающим *сильно неправильную* метарешетку M_{16} (рис. 2.26). Внешняя морфология графа (со стрелками или без них) играет подчиненную роль, математическая же сущность представленного графом объекта всегда остается где-то за рамками рисунка. Изображение графа в большинстве случаев является проекцией или тенью этой сущности и самостоятельного значения не имеет. Однако морфология расположения точек и линий тем не менее поддается определенной математической классификации и описанию. Этим мы намерены заняться в этом и последующем подразделах.

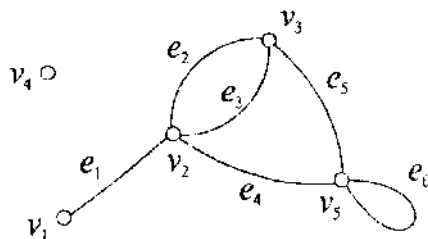


Рис. 3.12

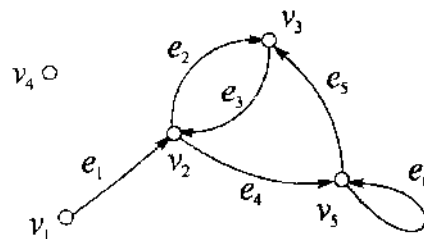


Рис. 3.13

Линии в графе G здесь и далее будем называть *ребрами*, а ориентированные линии в орграфу G_0 — *дугами*. О вершинах и ребрах (дугах) говорят, что они *инцидентны*, если вершина принадлежит ребру (дуге); если вершина не инцидентна никакому ребру (дуге), то она называется *изолированной* (v_4). Путь называется *простым*, если никакая дуга или ребро не встречается в нем дважды. Путь называется *элементарным*, если никакая вершина в нем не встречается дважды.

Цикл — это замкнутый путь в неориентированном графе. *Контур* — это ориентированный цикл в орграфу. Понятия простоты и элементарности распространяются на циклы и контуры. Контур или цикл, который содержит все ребра или дуги графа, называется *эйлеровым*. Можно показать, что *связанный* орграф (т.е. без изолированных фрагментов) содержит эйлеров контур тогда и только тогда, когда для каждой вершины число входящих дуг равно числу выходящих; связанный неориентированный граф содержит эйлеров цикл тогда и только тогда, когда степень каждой вершины четна. *Степенью вершины* называется число инцидентных ей ребер. *Простой путь, который проходит через все вершины графа, называется гамильтоновым*. Если в простом графе с n вершинами степень каждой вершины не меньше $n/2$, то такой граф обязательно будет гамильтоновым. Однако легко построить гамильтонов граф, у которого степень вершины меньше $n/2$.

Графы G и G_0 можно представить в аналитической форме либо *матрицей смежности* A , либо *матрицей инцидентности* B . Для нашего конкретного неориентированного графа G матрица A и B выглядят следующим образом:

$$A(G) = \begin{matrix} & v_1 & v_2 & v_3 & v_4 & v_5 \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{matrix} & \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 1 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} \end{matrix} \quad B(G) = \begin{matrix} & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{matrix} & \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{matrix}$$

Матрица смежности для неориентированного графа всегда симметрична. Фигурирующая в ней 2 может быть в некоторых случаях заменена на 1. В матрице инцидентности сумма единиц по столбцам указывает на степень вершины v_i . Нередко расположение вершин и ребер в этой матрице меняют местами (транспонируют). Так, для нашего конкретного орграфа G_0 матрицы A и B выглядят существенно иначе:

$$A(G_0) = \begin{matrix} & v_1 & v_2 & v_3 & v_4 & v_5 \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{matrix} & \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \end{matrix} \quad B(G_0) = \begin{matrix} & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \\ \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{matrix} & \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 \end{pmatrix} \end{matrix}$$

В общем случае матрица смежности для ориентированного графа уже не будет симметричной. В матрице инцидентности ставится 1, если дуга исходит из вершины, и -1 , если дуга заходит в нее.

Число дуг в пути минимальной длины от вершины v_i до v_j называется *расстоянием* $r(v_i, v_j)$. Если между этими вершинами не существует никакого пути, то расстояние принимается за бесконечное:

$$r(v_i, v_j) = \infty.$$

Для любой вершины v_i можно определить среднее отклонение от центра графа:

$$D(v_i) = \frac{1}{m} \sum_{v \in V} r(v_i, v),$$

где m — число дуг в графе G , v — пробегает вершины V графа G .

Вершина v_0 , для которой эта сумма окажется минимальной, называется *центром графа* G . В роли центра могут выступать несколько вершин.

Чтобы пересчитать возможные пути длины k , рассмотрим различные степени конкретной матрицы смежности. Пусть дан орграф G_0 (рис. 3.14).

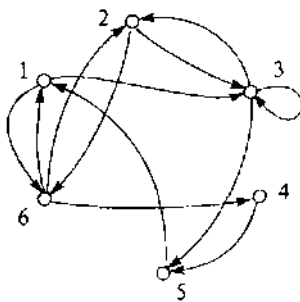


Рис. 3.14

$$A(\Gamma_0) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad R = r(i, j) = \begin{pmatrix} 0 & 2 & 1 & 2 & 2 & 1 \\ 2 & 0 & 1 & 2 & 2 & 1 \\ 2 & 1 & 0 & 3 & 1 & 2 \\ 2 & 4 & 3 & 0 & 1 & 3 \\ 1 & 3 & 2 & 3 & 0 & 2 \\ 1 & 1 & 2 & 1 & 3 & 0 \end{pmatrix}.$$

Общее число дуг $m = 12$; матрица $R = r(i, j)$ отражает расстояние между вершинами; на ее основе рассчитываем все возможные отклонения: $D(1) = D(2) = D(6) = 2/3$ — центр графа Γ_0 , который состоит из трех вершин 1, 2 и 6; остальные отклонения равны:

$$D(3) = 3/4, \quad D(4) = 13/12, \quad D(5) = 11/12.$$

Сама матрица смежности $A(\Gamma_0)$ дает число путей, длина которых равна единице. Квадрат матрицы смежности $A^2(\Gamma_0)$ дает число путей, длина которых равна двум дугам. Куб матрицы $A^3(\Gamma_0)$ дает число путей в три дуги и т.д. В частности, на пересечении 2-го столбца и 3-ей строки матрицы $A^3(\Gamma_0)$ стоит 3. Это означает, что из вершины 3 в вершину 2 имеется три пути, а из вершины 2 в вершину 3 существует уже четыре пути в три дуги:

$$A^2(\Gamma_0) = \begin{pmatrix} 1 & 2 & 1 & 1 & 1 & 0 \\ 1 & 2 & 1 & 1 & 1 & 0 \\ 1 & 1 & 2 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 1 & 2 \end{pmatrix}, \quad A^3(\Gamma_0) = \begin{pmatrix} 1 & 1 & 4 & 0 & 2 & 3 \\ 1 & 1 & 4 & 0 & 2 & 3 \\ 2 & 3 & 4 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 2 & 1 & 1 & 1 & 0 \\ 3 & 4 & 2 & 2 & 2 & 0 \end{pmatrix},$$

$$A^4(\Gamma_0) = \begin{pmatrix} 5 & 7 & 6 & 3 & 4 & 2 \\ 5 & 7 & 6 & 3 & 4 & 2 \\ 4 & 6 & 9 & 2 & 5 & 5 \\ 1 & 2 & 1 & 1 & 1 & 0 \\ 1 & 1 & 4 & 0 & 2 & 3 \\ 2 & 2 & 9 & 0 & 4 & 7 \end{pmatrix}, \quad A^5(\Gamma_0) = \begin{pmatrix} 6 & 8 & 18 & 2 & 9 & 12 \\ 6 & 8 & 18 & 2 & 9 & 12 \\ 10 & 14 & 19 & 5 & 11 & 10 \\ 1 & 1 & 4 & 0 & 2 & 3 \\ 5 & 7 & 6 & 3 & 4 & 2 \\ 11 & 16 & 13 & 7 & 9 & 4 \end{pmatrix}, \dots$$

Введем понятие об *означенной* матрице смежности $A(\Gamma_0)$, в которой вместо единиц выставляются соответствующие вершины. *Вспомогательная* матрица $A^*(\Gamma_0)$ получается из $A(\Gamma_0)$ путем отбрасывания первого символа в означенных дугах. Матрица $A^*(\Gamma_0)$ нужна для получения соответствующей степени матрицы $A(\Gamma_0)$. Так,

$$A(\Gamma_0) \times A^*(\Gamma_0) = A^2(\Gamma_0), \quad A^2(\Gamma_0) \times A^*(\Gamma_0) = A^3(\Gamma_0), \dots$$

Означенная матрица A^* , по сравнению с матрицей A , помимо числа путей, указывает еще и вершины, через которые эти пути пролегают. На диагонали матрицы A^* будут указаны всевозможные контуры, длина которых равна 1, 2, 3 и т.д. дугам. Неповторяющиеся вершины для отдельных путей укажут на *элементарные* пути. Так как в нашем графе Γ_0 имеется шесть вершин, то элементарных путей, длина которых равнялась бы шести дугам, вообще быть не может. Отсюда максимальная степень означенной матрицы для определения всех *гамильтоновых путей* должна быть равна пяти. В нашем графе Γ_0 , как на то указывает матрица

$A^5(\Gamma_0)$, только три гамильтоновых пути: 326451, 451623 и 235164. На диагонали матрицы $A^6(\Gamma_0)$ стоит один и тот же *гамильтонов контур* 1326451, который всякий раз начинается с новой вершины.

$$A(\Gamma_0) = \begin{pmatrix} 0 & 0 & 13 & 0 & 0 & 16 \\ 0 & 0 & 23 & 0 & 0 & 26 \\ 0 & 32 & 33 & 0 & 35 & 0 \\ 0 & 0 & 0 & 0 & 45 & 0 \\ 51 & 0 & 0 & 0 & 0 & 0 \\ 61 & 62 & 0 & 64 & 0 & 0 \end{pmatrix}, \quad A^2(\Gamma_0) = \begin{pmatrix} 0 & 0 & 3 & 0 & 0 & 6 \\ 0 & 0 & 3 & 0 & 0 & 6 \\ 0 & 2 & 3 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & 5 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 4 & 0 & 0 \end{pmatrix},$$

$$A^2(\Gamma_0) = A(\Gamma_0) \times A(\Gamma_0) = \begin{pmatrix} 161 & 132 & 133 & 164 & 135 & 0 \\ & 261 & 232 & 262 & 233 & 264 & 235 & 0 \\ 351 & 332 & 323 & 333 & 0 & 335 & 326 \\ 451 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 513 & 0 & 0 & 516 \\ 0 & 0 & 613 & 0 & 645 & 616 & 626 \end{pmatrix},$$

$$A^3(\Gamma_0) = \begin{pmatrix} 1351 & 1332 & 1613 & 1323 & 1623 & 1333 & 1645 & 1616 & 1326 & 1626 \\ & 2351 & 2332 & 2613 & 2323 & 2623 & 2333 & 2335 & 2616 & 2326 & 2626 \\ 3351 & 3332 & 3513 & 3323 & 3233 & 3333 & 3264 & 3235 & 3516 & 3326 \\ 3261 & 3262 & 3262 & 3262 & 3262 & 3262 & 3262 & 3262 & 3262 & 3262 \\ 0 & 0 & 4513 & 0 & 0 & 4516 \\ 5161 & 5132 & 5133 & 5164 & 5135 & 0 \\ 6451 & 6132 & 6133 & 6164 & 6135 & 0 \\ 6161 & 6232 & 6233 & 6124 & 6235 \\ 6261 & 6262 \end{pmatrix}.$$

При получении следующих степеней означенных матриц будем оставлять только те пути и контуры, которые являются гамильтоновыми:

$$A^4(\Gamma_0) = \begin{pmatrix} 16451 & 0 & 0 & 13254 & 16235 & 0 \\ 13261 & 0 & 0 & 0 & 26135 & 23516 \\ 26451 & 26132 & 0 & 0 & 26135 & 23516 \\ 0 & 35162 & 32613 & 35164 & 32645 & 0 \\ 0 & 45132 & 0 & 45164 & 0 & 0 \\ 0 & 45162 & 0 & 0 & 0 & 0 \\ 0 & 0 & 51623 & 0 & 51645 & 51326 \\ 62351 & 0 & 64513 & 0 & 0 & 64516 & 61235 \end{pmatrix},$$

$$A^5(\Gamma_0) = \begin{pmatrix} 162351 & 0 & 0 & 0 & 132645 & 0 \\ 0 & 235162 & 264513 & 235164 & 0 & 0 \\ 326451 & 0 & 351623 & 0 & 0 & 0 \\ 0 & 451623 & 0 & 0 & 0 & 451326 \\ 0 & 0 & 0 & 513264 & 516235 & 0 \\ 0 & 645132 & 0 & 0 & 0 & 623516 \end{pmatrix},$$

$$A^6(\Gamma_0) = \begin{pmatrix} 1326451 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2645132 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3264513 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4513264 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5132645 & 0 \\ 0 & 0 & 0 & 0 & 0 & 6451326 \end{pmatrix}.$$

Зададимся вопросом: какое число графов (N) возможно на n вершинах и m ребрах? Так, для $n = 4$ можно вычертить $N = 11$ принципиально различающихся графов (рис. 3.15).

Вычерченная система графов находится в отношении дополнения. Дополнением графа G является граф G' , который дополняет исходный граф до полного. Матрица смежности дополнительного графа находится по формуле:

$$A(G') = J - A(G),$$

где J — матрица смежности полного графа, состоящая полностью из единиц, за исключением элементов диагонали.

Два графа с $m = 2$ находятся в отношении дополнения с двумя графами, имеющими $m = 4$ и т.д. В табл. 3.7, где приведены количества графов с n вершинами и m ребрами, нетрудно заметить, что в пределах одного столбца возрастающая последовательность его чисел, достигая максимума, в точности повторяет его убывающую последовательность.

Аналогичная симметрия взаимного дополнения имеет место и для орграфов (табл. 3.8). На рис. 3.16 изображены всевозможные вариации орграфов на трех вершинах.

Любой граф обладает некоторыми свойствами симметрии. Граф и его дополнение всегда имеют одну и ту же группу симметрии. В частности, полный граф и его дополнение — пустой граф на n вершинах обладают симметрической группой S_n . Известно, что, например, в группе S_4 содержится подгруппа S_3 , т.е. группа симметрии треугольника. На рис.

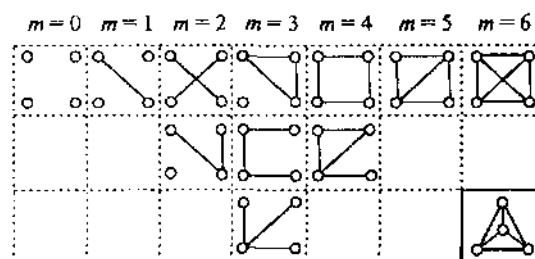


Рис. 3.15

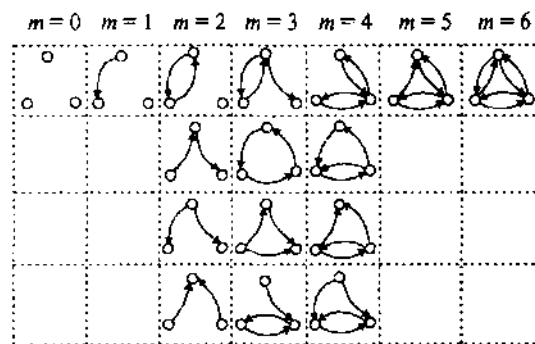


Рис. 3.16

3.15 для $m = 6$ изображено два графа (треугольной формы взят в рамку) как раз для того, чтобы продемонстрировать это свойство полного графа на четырех вершинах.

Таблица 3.7

$m \backslash n$	1	2	3	4	5	6	7	8
0	1	1	1	1	1	1	1	1
1	-	1	1	1	1	1	1	1
2	-	-	1	2	2	2	2	2
3	-	-	-	3	4	5	5	5
4	-	-	-	-	2	6	9	10
5	-	-	-	-	-	1	6	15
6	-	-	-	-	-	-	1	6
7	-	-	-	-	-	-	-	4
8	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-
14	-	-	-	-	-	-	-	-
15	-	-	-	-	-	-	-	-
N	1	2	4	11	34	156	1 044	12 344

Таблица 3.8

$m \backslash n$	1	2	3	4
0	1	1	1	1
1	-	1	1	1
2	-	-	1	4
3	-	-	-	4
4	-	-	-	-
5	-	-	-	-
6	-	-	-	-
7	-	-	-	-
8	-	-	-	-
9	-	-	-	-
10	-	-	-	-
11	-	-	-	-
12	-	-	-	-
N	1	3	16	218

Граф с меньшим числом ребер, чем у полного графа, имеет в качестве своей группы симметрии какую-нибудь подгруппу группы S_n . Например, группа приведенного на рис. 3.15 графа с числом ребер, равным $m = 5$, состоит из четырех элементов; если вершины графа пронумеровать соответствующим образом, то его группа выразится подстановками: $a = (02)$, $b = (13)$, $c = (02)(13)$ и $e = (0)$. Между тем, как нам известно, группа симметрии полного графа ($m = 6$) S_4 состоит из 24-х элементов (подстановки см. в табл. 2.54).

Любой граф имеет для себя тождественную подстановку. Поэтому его группа симметрии имеет по крайней мере один элемент симметрии. Для нахождения группы G , которая порождается симметричным графом Γ , используются подстановочные 0,1-матрицы. Если граф Γ определяется матрицей смежности $A(\Gamma)$, то его группа симметрии G определяется теми подстановочными 0,1-матрицами $M(G)$, которые коммутируют с матрицей смежности $A(\Gamma)$:

$$A(\Gamma) \times M(G) = M(G) \times A(\Gamma).$$

Так, для только что приведенного в качестве примера графа с $n=4$, $m=5$ (рис. 3.15) и подстановкой $c = (02)(13)$ имеем:

$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

Если уже найдено какое-то количество подстановок, то их принимают за образующие группы и пытаются найти остальные элементы симметрии. При этом учитывают тот факт, что симметрия исходного и дополнительного к нему графа

одна и та же. Коммутационное отношение обыкновенно выступает в роли проверочного.

Пусть дан довольно сложный исходный граф Γ , по нему находим более простой дополнительный граф Γ' (рис. 3.17). Затем отыскиваем несколько очевидных транспозиций, перемножая их между собой, определяем полную группу симметрии исходного графа Γ . В конце по коммутационному соотношению проверяем справедливость одной из найденных подстановок.

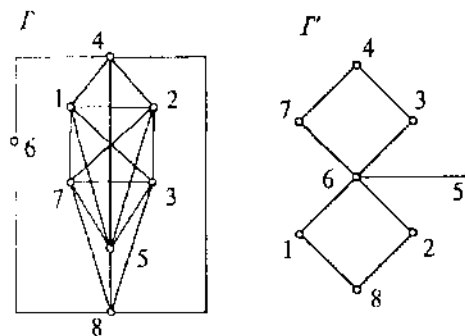


Рис. 3.17

$$e = (1), \quad b = (37), \quad d = (17)(23)(48), \quad g = (1723)(48),$$

$$a = (12), \quad c = (12)(37), \quad f = (13)(27)(48), \quad h = (1327)(48).$$

$$\begin{aligned} & A(\Gamma) \quad M(d) \quad M(d) \quad A(\Gamma) \\ & \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} = \\ & \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \end{aligned}$$

Если все вершины графа имеют одинаковую степень, то такой граф называется *регулярным*. Регулярный граф, как правило, имеет более высокую степень симметрии, чем нерегулярный, но всегда меньшую, чем у полного, построенного на тех же самых вершинах. Для регулярного графа Γ матрицы смежности и инцидентности связаны соотношением:

$$A(\Gamma) = B^*(\Gamma) \times B(\Gamma) - d(v)E,$$

где E — единичная матрица, $d(v)$ — степень вершины v регулярного графа Γ ,

$B^*(\Gamma)$ — транспонированная матрица инцидентности $B(\Gamma)$.

Схожую с этой формулой имеет реберный граф. Граф Γ_p называется *реберным*, если в качестве вершин его выбраны ребра исходного графа Γ с m ребрами и n вершинами, имеющего матрицу инцидентности $B(\Gamma)$. В этом случае матрица смежности реберного графа находится по формуле:

$$A(\Gamma_p) = B(\Gamma) \times B^*(\Gamma) - 2E.$$

Важно подчеркнуть, что исходный граф Γ для построения реберного Γ_p обязательно должен быть регулярным. Но если Γ все же регулярный, то и реберный Γ_p тоже будет регулярным. В общем случае, если ребро e_i в графе Γ ограничено вершинами v_j и v_k , степень которых равна $d(v_j)$ и $d(v_k)$, то степень вершины e_i в реберном графе Γ_p определится формулой:

$$d(e_i) = d(v_j) + d(v_k) - 2.$$

Число ребер в реберном графе Γ_p в общем, а не только регулярном случае, определяется следующим выражением:

$$m' = \frac{1}{2} \sum_{i=1}^n d^2(v_i) - m = \frac{1}{2} \sum_{i=1}^m d(e_i).$$

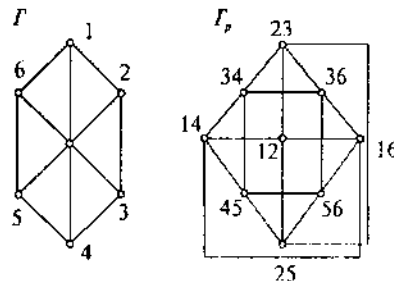


Рис. 3.18

Пусть дан регулярный граф Γ (рис. 3.18). Его матрицей инцидентности является $B(\Gamma)$, которую мы примем в своем расчете за исходную. По выписанным выше формулам находим $A(\Gamma)$ и $A(\Gamma_p)$, а также $d(e_i) = 4$ и $m' = 18$.

$$B(\Gamma) = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \begin{matrix} 12 \\ 14 \\ 16 \\ 23 \\ 25 \\ 34 \\ 36 \\ 45 \\ 56 \end{matrix}, \quad A(\Gamma) = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \quad A(\Gamma_p) = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

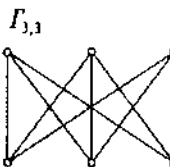
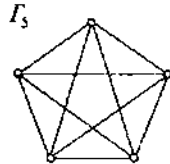


Рис. 3.19

Граф называется *плоским* (планарным), если его можно уложить на плоскости так, чтобы его ребра нигде не пересекались, кроме как в вершинах. Имеется два основных непланарных графа — Γ_5 и $\Gamma_{3,3}$, изображение которых дано на рис. 3.19.

Оба графа Γ_5 и $\Gamma_{3,3}$ являются регулярными, но последний относится еще и к так называемому *двудольному*, который определяется здесь как многозначное отображение трех верхних вершин на три нижние вершины, или наоборот. В общем случае в двудольном графе Γ_n число вершин в обоих рядах может быть любым.

Гиперграф — это такое обобщение простого графа, когда ребрами могут быть не только двухэлементные, но и любые подмножества вершин. Пусть конкретно заданы два множества: $V = \{v_1, v_2, \dots, v_9\}$ — множество вершин, $E = \{e_1, e_2, \dots, e_6\}$ — множество ре-

бер. Тогда за гиперграф $H(V, E)$ можно принять, например, следующее семейство подмножеств:

$$H(V, E) = \{e_1, e_2, e_3, e_4, e_5, e_6\} \\ = \{\{v_1, v_2, v_3\}, \{v_2, v_4, v_5, v_6\}, \{v_6, v_7, v_8\}, \{v_3, v_8\}, \{v_9\}, \{v_6\}\}.$$

Любому гиперграфу $H(V, E)$ можно поставить в соответствие *двудольный* граф $\Gamma_d(H)$ (рис. 3.20).

В особый тип графов выделяются деревья. *Дерево* – это связанный граф, не имеющий циклов, так как любые две его вершины соединены *простым* путем. Число ребер в нем всегда на единицу меньше числа его вершин ($m = n - 1$). На рис. 3.21 изображены все 6 деревьев, которые могут быть построены на шести вершинах.

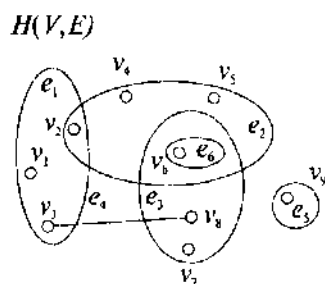


Рис. 3.20

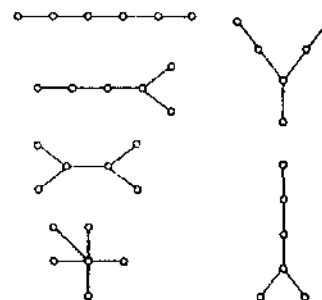
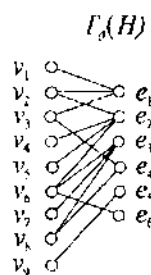


Рис. 3.21

Количество деревьев резко увеличится, если вершины как-нибудь пометить. Число *помеченных деревьев* и число других видов графов приведено в табл. 3.9.

Таблица 3.9

Виды графов	n	1	2	3	4	5	6
Дерева	1	1	1	2	3	6	120
Помеченные деревья	1	1	3	16	125	1296	1296
Простые графы	1	2	4	11	34	156	156
Связанные простые графы	1	1	2	6	21	112	112
Эйлеровы простые графы	1	0	1	1	4	8	8
Гамильтоновы простые графы	1	0	1	3	8	48	48
Простые планарные графы	1	1	2	6	20	105	105
Простые орграфы	1	3	16	213	9608	1540944	1540944
Связанные простые орграфы	1	2	13	199	9364	1439822	1439822

Чтобы произвести идентификацию деревьев различной конфигурации, производят упорядочение вершин по корневому признаку. Суть этой процедуры состоит в следующем. Из дерева T удаляются все концевые вершины вместе с инцидентными им ребрами, т.е. вершины степени, равной единице. Так получается новое дерево T_1 . Затем из T_1 вновь удаляются все концевые вершины; получается дерево T_2 . Эта процедура повторяется до тех пор, пока исходное дерево T не сократится до единственной вершины, которая и называется *корнем* дерева T . Если в результате удаления концевых вершин осталось две вершины, соединен-

ные ребром, то за корень дерева принимается любая из этих вершин. Каждой вершине приписывается вес, т.е. число, соответствующее общему количеству вершин поддеревьев. Вершины, смежные с корнем дерева T , рассматриваются как корни поддеревьев. При таком представлении корневое дерево однозначно определяется упорядоченной последовательностью весов его вершин, в которой

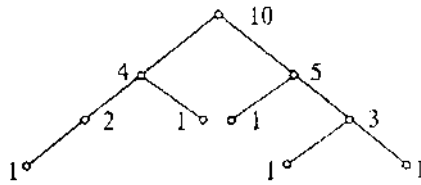


Рис. 3.22

на первом месте стоит вес корня всего дерева, а затем следуют соответствующие последовательности для поддеревьев в порядке возрастания весовых характеристик их корней. На рис. 3.22 в качестве примера приведено дерево вместе с весами его вершин, которые удобно записать в следующем порядке:

$T(10, 4, 1, 2, 1, 5, 1, 3, 1, 1)$.

3.3. Морфология графа

Разложение графа на его базисные составляющие проведем на конкретном примере. Пусть будет задан простой связанный планарный граф G , в котором пронумерованы все его ребра (рис. 3.23). Сплошными линиями выделен остов графа.

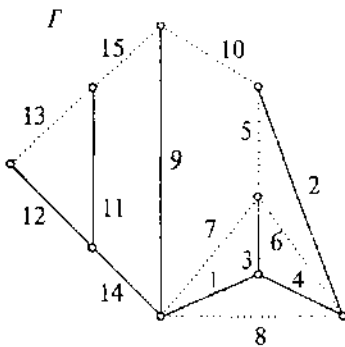


Рис. 3.23

Остовом (или *покрывающим деревом*) называется любое дерево графа G , покрывающее все его вершины. Ребра, не вошедшие в остов, называются *хордами*. Символическим представлением остова является следующая последовательность весовых характеристик: $T(9, 1, 2, 1, 5, 1, 3, 1, 1)$.

Прежде всего найдем ранг (k) и цикломатическое число (l) нашего графа G . Ранг определяется числом ребер покрывающего дерева, а *цикломатическое число* — не вошедшими в дерево ребрами; следовательно: $m = k + l = 8 + 7 = 15$ — общее число ребер в графе G .

Выделим в графе G базисные циклы и разрезы. Во всякий *базисный цикл* должна входить только одна хорда. Так, цикл $c = (1, 3, 7)$ является базисным, а другой цикл $c' = (1, 3, 5, 10)$ уже не будет таковым. *Разрезом* (или *сечением*) графа G в общем случае называется минимальное множество ребер, удаление которых делает граф несвязанным. Множество разрезов, отвечающих остову графа $T(G)$, называется *базисным множеством разрезов*. Каждый *базисный разрез* содержит точно одно ребро остова $T(G)$; все остальные ребра такого разреза будут хордами. Для нашего случая базисным является, например, разрез $s = (2, 5, 10)$, но не $s' = (2, 4, 6, 8)$. Базисные разрезы и циклы удобно представлять матрицами. Число строк в *матрице разрезов* (S) равно числу базисных разрезов (k), а число столбцов — общему числу ребер (m); причем если ребро участвует в данном разрезе, то в соответствующей позиции выставляется единица, в противном случае — ноль. Размерность *матрицы циклов* (C) равна $l \times m$; нули и единицы в ней выставляются точно так же, как и в матрице S , но уже относительно базисных циклов:

$$S = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Путем перегруппировки столбцов матрицы S и C можно привести к систематическому виду:

$$S' = (E_{k^2} | G_{lk}), \quad C' = (H_{kl} | E_{l^2});$$

$$S' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad C' = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

При перемножении матриц убеждаемся, что

$$S' \times C'^* = 0, \quad G_{lk} = H_{kl}^*, \quad H_{kl} = G_{lk}^*,$$

здесь звездочка означает транспонирование, а умножение производится по mod (2). Матрицы разрезов (S) и циклов (C) взаимно ортогональны.

Матрица инцидентности $B(\Gamma)$ путем линейной комбинации только строк может быть сведена к матрице разрезов S , при этом высвобождается одна нулевая строка:

$$B(\Gamma) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \end{matrix},$$

$$S = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 2 \\ 4 \\ 5 \\ 3 \\ 9 \\ 1+3+5+8+9 \\ 1+3+4+5+6+8+9 \\ 3+8+9 \\ 1+2+3+4+5+6+7+8+9 \end{matrix}.$$

Строки матрицы $B(\Gamma)$ пронумерованы как если бы были пронумерованы соответствующие вершины графа Γ (рис. 3.23). Справа от матрицы S показана линейная комбинация строк (суммирование производится по mod (2)).

Графу Γ отвечает 15-компонентный вектор:

$$\gamma = (1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1).$$

Всякий вектор может быть представлен линейной комбинацией базисных векторов. Следовательно, и наш вектор γ может быть представлен базисными разрезами и циклами. Чтобы определить, через какие именно разрезы и циклы выража-

ется наш вектор γ , необходимо вычислить некоторую совокупность *определителей Грама*. Сначала запишем *исходные* определители Грама для разрезов (g) и циклов (h) в общем виде:

$$g = \begin{vmatrix} s_{11} & s_{12} & \dots & s_{1k} \\ s_{21} & s_{22} & \dots & s_{2k} \\ \dots & \dots & \dots & \dots \\ s_{k1} & s_{k2} & \dots & s_{kk} \end{vmatrix}, \quad h = \begin{vmatrix} c_{11} & c_{12} & \dots & c_{1l} \\ c_{21} & c_{22} & \dots & c_{2l} \\ \dots & \dots & \dots & \dots \\ c_{l1} & c_{l2} & \dots & c_{ll} \end{vmatrix}.$$

Элементы определителей Грама g и h симметричны, т.е. $s_{ij} = s_{ji}$, $c_{ij} = c_{ji}$, и представляют собой скалярные произведения по $\text{mod } (2)$ базисных векторов соответствующих индексов. Базисные векторы разрезов берутся как строки матрицы S , а базисными векторами циклов являются строки матрицы C . Для нашего примера скалярные произведения принимают следующие значения:

$$\begin{aligned} s_{11} &= s_1 s_1 = (0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0) (0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0) = \\ &= 0 + 1 + 0 + 0 + 1 + 0 + 0 + 0 + 0 + 1 + 0 + 0 + 0 + 0 = 1, \\ s_{12} &= s_1 s_2 = (0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0) (0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0) = \\ &= 0 + 0 + 0 + 0 + 0 + 0 + 1 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 1, \dots \\ c_{45} &= c_4 c_5 = (1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0) (1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0) = \\ &= 1 + 0 + 0 + 1 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0, \dots \end{aligned}$$

После этих вычислений *исходные* определители Грама примут следующий вид:

$$g = \begin{vmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{vmatrix}, \quad h = \begin{vmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{vmatrix}.$$

Далее алгоритм вычислений строится следующим образом. Диагональ определителя g поочередно ставят на место первой его строки, получая таким образом *производный* определитель g_1 , затем на место второй, получая g_2 , и т.д. до тех пор, пока не получат g_8 . Аналогично находят все семь производных определителей для циклов:

$$g_1 = \begin{vmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{vmatrix} = 1, \quad g_2 = \begin{vmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{vmatrix} = 1,$$

$$h_1 = \begin{vmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{vmatrix} = 0, \dots, h_7 = \begin{vmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{vmatrix} = 1.$$

Определители вычисляются обычным образом, но по mod (2). В итоге получим:

$$g_1 = 1, g_2 = 1, g_3 = 0, g_4 = 0, g_5 = 1, g_6 = 1, g_7 = 1, g_8 = 0;$$

$$h_1 = 0, h_2 = 1, h_3 = 1, h_4 = 1, h_5 = 0, h_6 = 0, h_7 = 1.$$

Значения производных определителей играют роль коэффициентов линейного разложения вектора γ по базисным векторам разрезов и циклов:

$$\gamma_s = g_1 s_1 + g_2 s_2 + \dots + g_8 s_8, \quad \gamma_c = h_1 c_1 + h_2 c_2 + \dots + h_7 c_7, \quad \gamma = \gamma_s + \gamma_c.$$

Базисные компоненты с отличным от нуля коэффициентом участвуют в образовании вектора γ :

$$\gamma_s = 111110000101100$$

$$\gamma_c = 000001111010011$$

$$\gamma = 111111111111111.$$

Подробно:

$$s_1 = 010010000100000$$

$$s_2 = 001011100000000$$

$$s_5 = 000000000001100$$

$$s_6 = 100000110100000$$

$$s_7 = 000111010100000$$

$$c_2 = 001101000000000$$

$$c_3 = 101000100000000$$

$$c_4 = 100100010000000$$

$$c_7 = 000000001010011$$

$$\gamma = 111111111111111.$$

Ниже (рис. 3.24) приведены пара графов (Γ_1 и Γ_2) вместе с вычисленными результатами разложения их по базисным разрезам и циклам (γ_1 и γ_2).

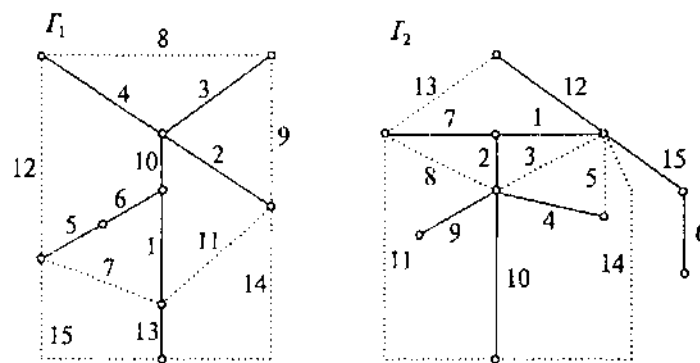


Рис. 3.24

$s_1 = 1000000100010011$
 $s_2 = 0100000001010010$
 $s_3 = 0010000011000000$
 $s_4 = 0001000010001000$
 $s_5 = 0000101000001001$
 $s_6 = 0000011000001001$
 $s_7 = 0000000000111010$
 $s_8 = 0000000000000111$
 $c_1 = 0011000010000000$
 $c_2 = 0110000001000000$
 $c_3 = 0001110000101000$
 $c_4 = 1100000000100110$
 $c_5 = 1000110000000101$
 $\gamma_1 = 1111111111111111$

$s_1 = 1010100000000110$
 $s_2 = 011010010010010$
 $s_3 = 0001100000000000$
 $s_4 = 0000010000000000$
 $s_5 = 000000110010100$
 $s_6 = 000000001000000$
 $s_7 = 000000000110010$
 $s_8 = 0000000000000001$
 $c_1 = 1110000000000000$
 $c_2 = 0100001100000000$
 $c_3 = 10000001000001100$
 $\gamma_2 = 1111111111111111$

На рис. 3.25 изображены еще два простых связанных планарных графа G_3 и G_4 на 15 ребрах, внешне ничем не отличающихся от своих предшественников, но

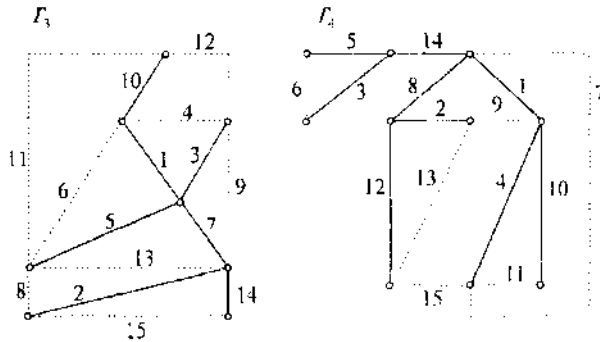


Рис. 3.25

которые, однако, уже не могут быть разложены в поле чисел по mod (2) по своим базисным разрезам и циклам. Все их определители Грама, вычисленные по изложенной выше методике, оказываются равными нулю. С точки зрения традиционной линейной алгебры, это свидетельствует о наличии линейной зависимости между векторами.

Тем не менее разложение графов G_3 и G_4 по их выделенным базисным компонентам теоретически возможно, если использовать, скажем, операции по mod (3), mod (4) или вообще без модуля, при которых появятся отличные от нуля определители.

Здесь обнаруживается основной изъян в геометрической интерпретации «бинарного» разложения графа на базисные разрезы и циклы. Дело в том, что трактовку 1 и 0 как «вхождение» или «невхождение» ребра в линейное разложение, нужно дополнить еще одним содержанием: *всякое нечетное вхождение ребра означает 1, а четное — 0*. Графы G_3 и G_4 отличаются от G_1 и G_2 тем, что первая пара графов поддается именно *бинарному* разложению, а вторая пара — нет, но разложение для них как таковое, вообще говоря, не исключено.

Еще один вопрос, который здесь возникает: каково общее число возможных остовов?

Оно рассчитывается с помощью определителя размерности $(n-1) \times (n-1)$, на диагонали которого выставляются степени $n-1$ вершин (отсутствовать может любая из n вершин), а недиагональные элементы ij могут быть вида: 0 (если вершины i и j между собой не связаны), -1 (если i и j связаны одной связью), -2 (если i и j связаны двумя связями) и т.д.

Часто ребра снабжены какой-либо весовой характеристикой, и покрывающее дерево требуется выбрать из *оптимальных* соображений: минимального или максимального веса покрывающего дерева. Для нахождения, например, *остова минимального веса* поступают следующим образом. Из всех предложенных ребер выбирают ребро с наименьшим весом. Затем на каждом следующем шаге из оставшегося числа рассматривается наименьшее по весу ребро. Если оно не образует цикла с ранее выбранными ветвями графа, то вводится в остов. Построение прекращается после $n - 1$ шага. Все остовы графов G, G_1, G_2, G_3, G_4 выбраны как раз по этому алгоритму, при этом номер ребра принимался за его вес.

Покрывающее дерево графа G нужно отличать от его реберного покрытия. *Реберным покрытием* графа $G(V, E)$ называется такое подмножество E' из E , которое инцидентно всему множеству вершин V . Наряду с реберным покрытием, вводят понятие независимого подмножества ребер: подмножество E'' из E попарно не смежных ребер называется *независимым* (или *паросочетанием*). Аналогичная пара понятий существует для вершин. Подмножество вершин V' графа $G(V, E)$ называется *независимым*, если никакие две вершины из этого множества не смежны. Если подмножество вершин V'' из V — независимо, то порожденный этими вершинами подграф $G(V'', 0)$ является *пустым*. Упомянем попутно, антиподом независимого множества является понятие *клики*. Подмножество вершин называется *кликкой*, если любые две входящие в него вершины смежны, т.е. когда порождаемый этим подмножеством подграф будет *полным*. И последнее понятие в этом ряду: подмножество вершин V''' называется *вершинным покрытием*, если множество V''' покрывает все ребра E графа G .

Оптимальные значения введенных характеристик обозначим следующим образом:

α_0 — максимальное число независимых вершин,

β_0 — минимальное вершинное покрытие,

α_1 — максимальное число независимых ребер,

β_1 — минимальное реберное покрытие.

Для любого графа G выполняется условие:

$$\alpha_0 + \beta_0 = \alpha_1 + \beta_1 = n.$$

Двудольные графы выделяются среди прочих тем, что для них выполняется дополнительное условие:

$$\alpha_0 = \beta_1, \quad \alpha_1 = \beta_0.$$

Поэтому для G_0 имеет место расширенное условие:

$$\alpha_0 + \beta_0 = \alpha_1 + \beta_1 = \alpha_0 + \alpha_1 = \beta_0 + \beta_1 = n.$$

Кроме того, независимое множество ребер графа G находится во взаимно однозначном соответствии с независимым множеством вершин реберного графа G_p , поэтому $\alpha_1(G) = \alpha_0(G_p)$.

Теперь рассмотрим конкретный двудольный граф G_0 , изображенный на рис. 3.26. Рядом с ним построим соответствующий ему реберный граф G_p . Для построения $G_p(V, E)$ сначала были найдено общее число ребер в G_p , а затем матрица смежности:

$$G_p(V, E) = \{e_1, e_2, e_3, e_4\} = \{\{v_1, v_4, v_3\}, \{v_1\}, \{v_2, v_3, v_2\}, \{v_2, v_4\}\},$$

$$m' = (1/2)(3^2 + 1^2 + 3^2 + 2^2 + 2^2 + 2^2 + 1^2 + 3^2 + 1^2) - 9 = 12,$$

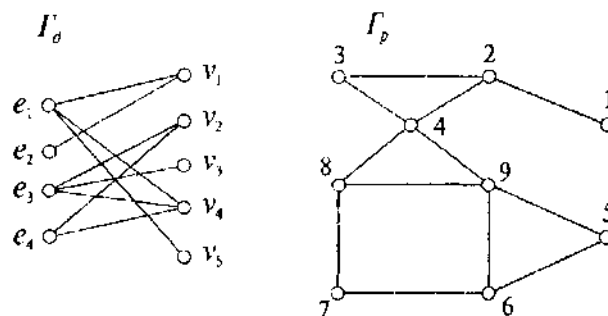


Рис. 3.26

$$A(\Gamma_p) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \end{matrix}$$

В соответствии с определением составим пять максимальных паросочетаний с числом $\alpha_1(\Gamma_d) = 4$:

- 1) $e_1 - v_4, e_2 - v_1, e_3 - v_3, e_4 - v_2,$
- 2) $e_1 - v_5, e_2 - v_1, e_3 - v_3, e_4 - v_2,$
- 3) $e_1 - v_5, e_2 - v_1, e_3 - v_3, e_4 - v_4,$
- 4) $e_1 - v_5, e_2 - v_1, e_3 - v_2, e_4 - v_4,$
- 5) $e_1 - v_5, e_2 - v_1, e_3 - v_3, e_4 - v_2.$

Имеется четыре минимальных реберных покрытия с числом $\beta_1(\Gamma_d) = 5$:

- 1) $e_1 - v_3, e_2 - v_1, e_3 - v_3, e_3 - v_2, e_4 - v_4,$
- 2) $e_1 - v_5, e_2 - v_1, e_3 - v_3, e_4 - v_2, e_4 - v_4,$
- 3) $e_1 - v_5, e_2 - v_1, e_3 - v_3, e_3 - v_4, e_4 - v_2,$
- 4) $e_1 - v_5, e_2 - v_1, e_3 - v_3, e_4 - v_4, e_4 - v_2.$

Каждое из этих четырех покрытий определяется минимальным числом единиц, которые покрывают все строки и столбцы матрицы инцидентности (эти покрывающие единицы заменены на звездочки):

$$\begin{pmatrix} 1 & * & 0 & 0 \\ 0 & 0 & * & 1 \\ 0 & 0 & * & 0 \\ 1 & 0 & 1 & * \\ * & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & * & 0 & 0 \\ 0 & 0 & 1 & * \\ 0 & 0 & * & 0 \\ 1 & 0 & 1 & * \\ * & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & * & 0 & 0 \\ 0 & 0 & 1 & * \\ 0 & 0 & * & 0 \\ 1 & 0 & * & 1 \\ * & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & * & 0 & 0 \\ 0 & 0 & 1 & * \\ 0 & 0 & * & 0 \\ * & 0 & 1 & 1 \\ * & 0 & 0 & 0 \end{pmatrix}.$$

Множество независимых вершин в графе Γ_p отвечает множеству независимых ребер в графе Γ_d , откуда $\alpha_1(\Gamma_d) = \alpha_0(\Gamma_p) = 4$:

$$\{1, 3, 7, 9\}, \{1, 4, 5, 7\}, \{1, 3, 6, 8\}, \{1, 3, 5, 7\}, \{1, 3, 5, 8\}.$$

Для реберного графа Γ_p можно указать и три максимальных клики: $\{2, 3, 4\}$, $\{4, 8, 9\}$ и $\{5, 6, 9\}$. Наконец, выпишем минимальные множества вершинных покрытий для графа Γ_p , которые получаются как дополнения к максимальным множествам независимых вершин:

$$\{2, 4, 5, 6, 8\}, \{2, 3, 6, 8, 9\}, \{2, 4, 5, 7, 9\}, \{2, 4, 6, 8, 9\}, \{2, 4, 6, 7, 9\}.$$

Для поиска подмножества независимых вершин и вершинных покрытий пользуются *методом булевых функций*. С этой целью запишем граф G_p в булевой конъюнктивной нормальной форме (КНФ), при этом сам символ конъюнкции опустим:

$$f(G_p) = (2 \vee 1)(2 \vee 3)(2 \vee 4)(9 \vee 4)(9 \vee 5)(9 \vee 6)(9 \vee 8)(7 \vee 8) \times \\ \times (7 \vee 6)(5 \vee 6)(4 \vee 8)(4 \vee 3).$$

Пользуясь только законами поглощения —

$$a \vee (ab) = a, \quad a(a \vee b) = a,$$

переведем нашу булеву функцию $f(G_p)$ в минимальную дизъюнктивную нормальную форму (ДНФ). На практике удобно использовать законы поглощения не после полного раскрытия скобок, а в процессе их последовательного перемножения:

$$f(G_p) = (2 \vee 134)(9 \vee 4568)(7 \vee 68)(5 \vee 6)(4 \vee 38) = \\ = (29 \vee 24568 \vee 1349 \vee 134568)(457 \vee 467 \vee 468 \vee 368 \vee 3578) = \\ = \underline{24579} \vee \underline{24679} \vee \underline{24689} \vee \underline{23689} \vee \underline{24568} \vee 235789 \vee 134579 \vee 134679 \vee 134689 \vee 134568.$$

Подчеркнутые конъюнкты образуют известные нам пять минимальных вершинных покрытий. Их дополнениями являются максимальные множества независимых вершин.

Чтобы проверить правильность нахождения всех вершинных покрытий, необходимо воспользоваться *принципом двойственности*, который действует в рамках логики Буля. Для этого результирующее выражение запишем в КНФ и с помощью того же закона поглощения приведем его к ДНФ:

$$f'(G_p) = (2 \vee 4 \vee 5 \vee 7 \vee 9)(2 \vee 4 \vee 7 \vee 9) \dots (1 \vee 3 \vee 4 \vee 5 \vee 6 \vee 8) = \\ = 21 \vee 23 \vee 24 \vee 94 \vee 95 \vee 96 \vee 98 \vee 78 \vee 76 \vee 56 \vee 48 \vee 43.$$

В конъюнктах этой дизъюнктивной формы легко узнаются ребра исходного графа G_p . Следовательно, минимальные покрытия были найдены верно.

Снова вернемся к нашему исходному двудольному графу $G_b(V, E)$ и введем в оборот новое важное понятие — *трансверсаль*. *Трансверсалью* (или *системой различных представителей*) называется подмножество T из V , состоящее из элементов v_i по одному из каждого подмножества e_j . В нашем конкретном случае —

$$G_b(V, E) = \{e_1, e_2, e_3, e_4\} = \{\{v_1, v_4, v_3\}, \{v_1\}, \{v_2, v_3, v_4\}, \{v_2, v_4\}\}$$

можно выделить четыре трансверсали:

$$T_1 = \{v_1, v_2, v_3, v_4\}, T_2 = \{v_1, v_2, v_3, v_3\}, T_3 = \{v_1, v_3, v_4, v_3\}, T_4 = \{v_1, v_2, v_4, v_3\}.$$

В определенном смысле нам повезло с двудольным графом G_b . Ясно, что трансверсаль существует только в том случае, если для любых k элементов подмножеств e_j их объединение содержит по меньшей мере k элементов. Например, в семействе

$$\{e_1, e_2, e_3, e_4, e_5\} = \{\{v_1, v_2\}, \{v_1, v_3\}, \{v_2, v_3\}, \{v_1, v_2, v_3\}, \{v_1, v_3, v_4, v_5\}\}$$

невозможно найти пять различных элементов v_i по одному из каждого e_j , поэтому данное семейство не имеет ни одной трансверсали. Здесь объединение четырех множеств содержит только три элемента:

$$e_1 \cup e_2 \cup e_3 \cup e_4 = \{v_1, v_2, v_3\}.$$

Такие семейства, с точки зрения образования системы различных представителей, выпадают из анализа.

Трансверсали обладают одним замечательным свойством: если T и T' — любые две трансверсали семейства E и v — элемент из T , то существует элемент v' из T' такой, что $(T - v) \cup v' = T'$ — тоже трансверсаль. Например, для нашего графа $G_0(V, E)$, возьмем в качестве $T = T_2$, $T' = T_4$ и $v = v_2$. Тогда в T_4 найдется элемент $v' = v_4$ такой, что $(T_2 - v_2) \cup v_4 = T_4$.

Точно таким же свойством обладают *остовы* графов. Покрывающие деревья выполняют роль трансверсалей, потому что если T и T' — любые два остова и e — некоторое ребро из остова T , то в остова T' можно найти такое ребро e' , которое даст новый остов: $T' - (T - e) \cup e'$. Значит, можно говорить не только о *вершинных* трансверсалиях, но и о *реберных*, что уже предполагает наличие некоторой *двойственности*.

Нужно заметить, что понятие трансверсали достаточно основополагающее для всей дискретной математики. С ним мы встречались в логике, существует оно в комбинаторике и линейной алгебре. Что касается последней области знания, указанное свойство демонстрируется следующей формулировкой: если V и V' — два базиса одного и того же векторного пространства и v — вектор из V , то найдется базисный вектор v' из V' , что $(V - v) \cup v' = V'$, где V' — новая система базисных векторов.

Трансверсаль позволяет ввести новое понятие в теорию графов — матроид. *Матроидом* $M(T, C)$ графа называется система, состоящая из двух компонентов: в первую компоненту входит вся совокупность *остовов* T , т.е. совокупность подмножеств, в каждое из которых входит максимальное число, равное рангу k , *независимых элементов*; вторая совокупность C составлена из l *ячеечных циклов*, представляющих собой минимальные подмножества *зависимых элементов*. Цикломатическое число l определяется либо количеством хорд, т.е. числом ребер, не вошедших в остов, либо числом внутренних областей (ячеек) планарного графа, которые так же, как и хорды, образуют базисную систему циклов.

Матроид M может иметь двойственный к себе матроид M^* , для которого ранг $k^* = l$, а цикломатическое число $l^* = k$. Двойственному матроиду M^* отвечает двойственный граф G^* , причем i^* -ребро графа G^* соответствует i -ребру графа G , поэтому количество ребер в обоих графах одинаковое, $m = m^*$. Сказанное поясним на конкретном примере.

Пусть дан граф G на шести ребрах (рис. 3.27): граф G^* называется *двойственным* к графу G , если векторы базисных разрезов графа G^* служат векторами базисных циклов графа G и наоборот. Методика построения двойственного графа показана на этом же рисунке черными кружками и пунктирными линиями. Таким образом, граф G^* имеет столько же ребер, сколько и граф G ; число вершин графа G^* равно числу областей, на которые делит плоскость своими ребрами граф G , причем имеется соответствие: цикл $\{1, 2, 3\}$ графа G отвечает разрезу $\{1^*, 2^*, 3^*\}$ графа G^* , цикл $\{3, 4, 5\}$ отвечает разрезу $\{3^*, 4^*, 5^*\}$, разрез $\{6\}$ отвечает циклу $\{6^*\}$, разрез $\{1, 2\}$ отвечает циклу $\{1^*, 2^*\}$, разрез $\{4, 5\}$ отвечает циклу $\{4^*, 5^*\}$, наконец, разрез $\{2, 3, 5\}$ отвечает циклу $\{2^*, 3^*, 5^*\}$.

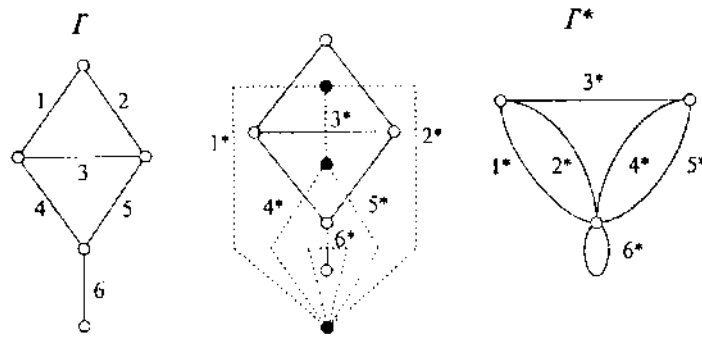


Рис. 3.27

Число покрывающих деревьев исходного графа Γ и двойственного Γ^* , как рассказывалось выше, находится путем вычисления определителей:

$$D = \begin{vmatrix} 3 & -1 & -1 & 0 \\ -1 & 2 & -1 & 0 \\ -1 & -1 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix} = 8, \quad D^* = \begin{vmatrix} 4 & -2 \\ -2 & 3 \end{vmatrix} = 8.$$

Следовательно, в матроиде M графа Γ имеется 8 трансверселей; перечислим их:

$$T_1 = \{1, 2, 4, 6\}, T_2 = \{1, 2, 5, 6\}, T_3 = \{1, 3, 4, 6\}, T_4 = \{1, 3, 5, 6\}, \\ T_5 = \{1, 4, 5, 6\}, T_6 = \{2, 3, 4, 6\}, T_7 = \{2, 3, 5, 6\}, T_8 = \{2, 4, 5, 6\}.$$

В матроид M входят также два ячеечных цикла минимальной длины:

$$C_1 = \{1, 2, 3\} \text{ и } C_2 = \{3, 4, 5\}.$$

Зависимость ребер в ячеечных циклах и независимость их в остовах связаны с линейной зависимостью или независимостью соответствующих столбцов матрицы инцидентности $B(\Gamma)$. В частности, столбцы $\{1, 2, 4, 6\}$, $\{1, 2, 5, 6\}$ и т.д. независимы, а столбцы $\{1, 2, 3\}$ и $\{3, 4, 5\}$ зависимы. Зависимость столбцов означает, что каждый из них может быть выражен через два других:

$$B(\Gamma) = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

Матроид M^* от двойственного графа Γ^* образован следующими трансверселями:

$$T_1^* = \{1, 3\}, T_2^* = \{1, 4\}, T_3^* = \{1, 5\}, T_4^* = \{2, 3\}, \\ T_5^* = \{2, 4\}, T_6^* = \{2, 5\}, T_7^* = \{3, 4\}, T_8^* = \{3, 5\}.$$

Имеется четыре ячеечных цикла, которые охватывают соответствующие элементарные области:

$$C_1^* = \{6\}, C_2^* = \{1, 2\}, C_3^* = \{4, 5\}, C_4^* = \{1, 3, 4\}.$$

Кроме того,

$$k = l^* = 4, l = k^* = 2, k + l = k^* + l^* = 6.$$

Остановимся несколько подробнее на двойственности графов. При изучении групп мы узнали о пяти правильных многогранниках (первое число в круглых скобках означает количество граней, второе — число сторон каждой грани): тетраэдр (4, 3), куб (6, 4), октаэдр (8, 4), додекаэдр (12, 5), икосаэдр (20, 3). Между этими многогранниками существует *двойственность*: если у одного из этих многогранников соединить отрезками

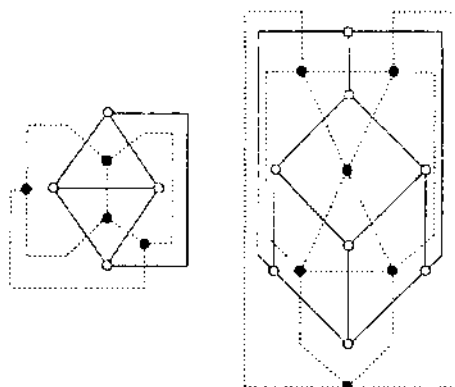


Рис. 3.28

прямых центры граней, имеющих общее ребро, то получится другой многогранник. Двойственными друг к другу будут: куб — октаэдр, додекаэдр — икосаэдр, левый тетраэдр — правый тетраэдр (с точки зрения симметрии, вернее было бы говорить не о пяти, а о шести правильных геометрических телах). Если ребра этих многогранников спроецировать на плоскость, то геометрическая двойственность переходит в двойственность графов. На рис. 3.28 показана двойственность для тетраэдров и куб — октаэдра.

Для произвольных многогранников (не обязательно правильных) с n вершинами, лежащими на сфере, m ребрами и f гранями выполняется равенство Эйлера: $n - m + f = 2$, например, для куба имеем: $8 - 12 + 6 = 2$. Между точками бесконечной плоскости и точками сферы конечного радиуса существует взаимно однозначное соответствие. Поэтому планарный граф проецируется на сферу в виде выпуклого многогранника. Число граней многогранника всегда на единицу больше цикломатического числа соответствующего графа, т.е. $f = l + 1$, так как помимо ячеечных циклов, очерчивающих все «видимые» грани, всегда присутствует окаймляющий цикл (сумма по mod (2) всех ячеечных циклов), который очерчивает «невидимую» нам грань многогранника, представленного графом. Ранг графа на единицу меньше числа вершин, т.е. $k = n - 1$. Наконец, напомним известное равенство: $m = k + l$. Из этих трех равенств вытекает доказательство истинности тождества Эйлера:

$$n - m + f = n - (n - 1 + l) + (l + 1) = 2.$$

Теперь главный вывод. Если в многограннике провести пространственную диагональ, то в графе на плоскости появится «непланарное» ребро, равенство Эйлера нарушится, а вместе с ним и все остальные равенства, в том числе базисное: $m = k + l$, выполняемое для любого матроида. Поэтому на непланарном графе нельзя построить матроид.

В отношении построения двойственных графов существует некоторая неоднозначность. На рис. 3.29 изображен один и тот же граф G , но с двумя различными укладками вершин и ребер G_1 и G_2 . В зависимости от укладки будут получаться и различные двойственные графы — G_1^* и G_2^* . В частности, в графе G_1^* имеется вершины шестой и четвертой степени, а в графе G_2^* вместо них две вершины пятой степени. Данный факт нарушает главное свойство графов — их независи-

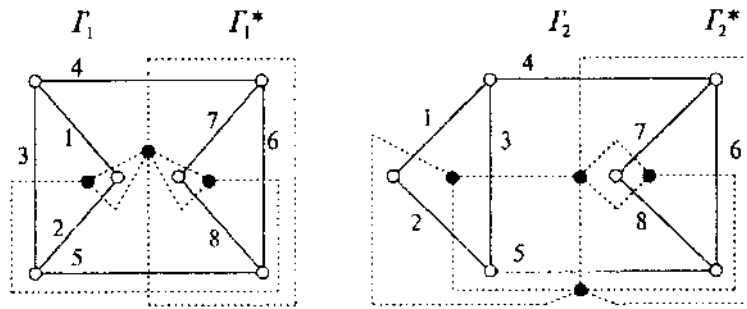


Рис. 3.29

мость от укладки вершин и ребер. Ранее говорилось, что граф однозначно характеризуется матрицами инцидентности, куда не заложена информация об укладке элементов графа на плоскости. Двойственный же граф, оказывается, зависит от этой несущественной детали: матрицы инцидентности для графов G_1^* и G_2^* различаются:

$$B(G_1^*) = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}, \quad B(G_2^*) = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Однако, если мы подсчитаем число покрывающих деревьев для обоих графов G_1^* и G_2^* , то оно окажется одинаковым:

$$D(G_1) = D(G_2) = \begin{vmatrix} 3 & -1 & -1 & -1 & 0 \\ -1 & 3 & 0 & 1 & 0 \\ -1 & 0 & 3 & 0 & -1 \\ -1 & -1 & 0 & 2 & 0 \\ 0 & 0 & -1 & 0 & 2 \end{vmatrix} = 30,$$

$$D(G_1^*) = \begin{vmatrix} 3 & -1 & 0 \\ -1 & 4 & -1 \\ 0 & -1 & 3 \end{vmatrix} = 30, \quad D(G_2^*) = \begin{vmatrix} 3 & -1 & 0 \\ -1 & 5 & -2 \\ 0 & -2 & 3 \end{vmatrix} = 30.$$

Одинаковыми будут, по сути, и матроиды, так как остовы у них полностью совпадают:

$$\begin{aligned} M(G_1) &= M(G_2) & M(G_1^*) &= M(G_2^*) \\ T_1 &= \{1, 2, 5, 6, 7\}, & T_1^* &= \{1^*, 3^*, 6^*\}, \\ T_2 &= \{1, 2, 5, 6, 8\} \text{ и т.д.} & T_2^* &= \{1^*, 4^*, 6^*\} \text{ и т.д.} \end{aligned}$$

Внешнее различие наблюдается лишь в циклической части. Так, для $M(G_1)$ средняя ячеечная область выражается циклом $C = \{1, 2, 4, 5, 7, 8\}$, а для $M(G_2)$ средняя область выражается уже циклом $C' = \{3, 4, 5, 7, 8\}$. Аналогичные различия могут возникнуть и в двойственных матроидах $M(G_1^*)$ и $M(G_2^*)$. Однако, если C_1 и C_2 являются двумя смежными ячеечными циклами и цепь ребер e_i является для них общей, то результирующий цикл C_3 , получившийся как объединение $(C_1 \cup C_2) - e_i = C_3$, может участвовать в множестве S матроида $M(T, S)$ вместо одного из ячеечных циклов. Путем подобных объединений мы можем заменить все ячеечные циклы на хордовые, получающиеся от хордального из покрывающих деревьев. Таким

образом, для матроида циклическая часть C определена неоднозначно; что же касается множества остовов T , то оно строго неизменно, какова бы ни была укладка исходного графа G , и называется *базой* матроида $M(T, C)$.

Тем не менее удобная укладка графа может сыграть принципиально важную роль в разрешении прикладных задач. Предположим, нам задан сложный орграф G_0 (рис. 3.30) с различными весовыми характеристиками дуг, например, их длиной, и требуется найти минимальный путь между двумя заранее заданными

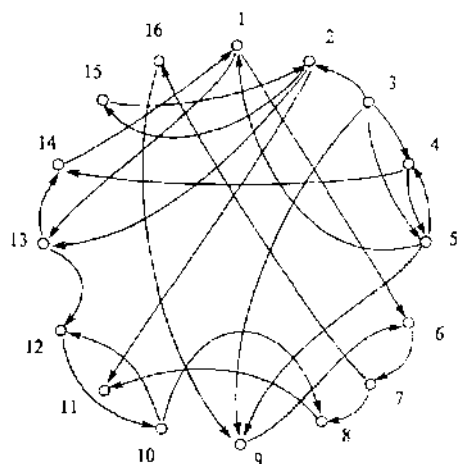


Рис. 3.30

вершинами. Ясно, что без серьезного «анатомирования» здесь не обойтись. Однако отвлечемся пока от весовых характеристик дуг и займемся чисто морфологическим анализом орграфа G_0 . Прежде чем приступить к нему, введем в оборот новые понятия.

Одна из основных задач, которые решаются по морфологическому анализу ориентированных графов, это разбиение вершин на непересекающиеся *классы эквивалентности и порядка*. С отношениями эквивалентности и порядка мы сталкивались в теории групп. Оказывается, эти отношения встречаются и в теории графов. Сначала рассмотрим вопрос разбиения вершин G_0 на классы эквивалентности или *сильно связанные подграфы*.

Введем оператор G , который указывает на связь вершины i с другими вершинами графа G_0 . Будем различать две группы G -операторов: *прямого действия* $G^n(i)$ и *обратного* $G^{-n}(i)$. Оператор $G^1(i)$ указывает на те вершины, в которые можно попасть непосредственно из вершины i ; обратный оператор $G^{-1}(i)$ указывает на совокупность вершин, из которых можно попасть в вершину i . Степени G -операторов определяются обычным образом:

$$G^0(i) = i, \quad G^2(i) = G^1(G^1(i)), \quad G^{-2}(i) = G^{-1}(G^{-1}(i)), \dots$$

Непосредственно по рис. 3.30 находим результат действия G -оператора на вершины 1 и 2:

$$\begin{aligned} G^0(1) &= 1; & G^1(1) &= 6, 13; & G^2(1) &= 7, 12, 14; & G^3(1) &= 8, 16, 10, 1; \\ G^{-1}(1) &= 6, 13, 11, 8, 12, 9; & G^{-1}(1) &= 5, 14; & G^{-2}(1) &= 3, 4, 13; \\ G^0(2) &= 2; & G^1(2) &= 11, 13, 15; & G^{-1}(2) &= 3, 15; & \text{и т.д.} \end{aligned}$$

Для всякой вершины i орграфа G_0 можно определить *прямое* $G^+(i)$ и *обратное* $G^-(i)$ *транзитивные замыкания*. Они определяются через объединение всех степеней G -оператора, соответственно, положительных и отрицательных:

$$\begin{aligned} G^+(i) &= G^0(i) \cup G^1(i) \cup G^2(i) \cup G^3(i) \cup \dots, \\ G^-(i) &= G^0(i) \cup G^{-1}(i) \cup G^{-2}(i) \cup G^{-3}(i) \cup \dots. \end{aligned}$$

Смысл прямого транзитивного замыкания $G^+(i)$ состоит в том, что оно указывает множество вершин орграфа Γ_0 , в которые можно попасть из вершины i . Обратное транзитивное замыкание $G^-(i)$ указывает на те вершины Γ_0 , из которых можно попасть в вершину i . В обоих случаях длина пути по числу дуг не ограничивается. Пересечение прямого и обратного транзитивных замыканий определяет подграф сильно связанных вершин или класс эквивалентности вершины i :

$$C(i) = G^+(i) \cap G^-(i).$$

Смысл сильной связи заключен в *достижимости* любой вершины из любой вершины данного класса. Сама вершина i называется *представителем класса* $C(i)$. В качестве представителя класса эквивалентных вершин, естественно, может выступать любая вершина этого класса.

Для нашего конкретного орграфа Γ_0 имеем:

$$G^+(1) = 1, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16;$$

$$G^-(1) = 1, 2, 3, 4, 5, 13, 14, 15.$$

Следовательно, первый класс сильно связанных вершин образован тремя вершинами:

$$C_1(1) = G^+(1) \cap G^-(1) = 1, 13, 14.$$

Вершина 2 попадает во второй класс эквивалентности, где помимо представителя присутствует еще одна вершина — 15-ая:

$$G^+(2) = 2, 11, 15; \quad G^-(2) = 2, 3, 15; \quad C_2(2) = 2, 15.$$

Всего подобная процедура позволяет найти восемь непересекающихся классов эквивалентности. Перечислим их без указания вершин-представителей:

$$C_1 = 1, 13, 14; \quad C_2 = 2, 15;$$

$$C_3 = 3; \quad C_4 = 4, 5;$$

$$C_5 = 6, 7, 9, 16; \quad C_6 = 10, 12;$$

$$C_7 = 8; \quad C_8 = 11.$$

Теперь орграф Γ_0 распался на сильно связанные подграфы, которые подчинены *отношению порядка* (рис. 3.31). Но прежде чем приступить к изучению *классов порядка*, опишем метод нахождения классов эквивалентности при помощи матрицы смежности. Она позволит описанный процесс алгоритмизировать так, чтобы поиск эквивалентных классов можно было осуществить на компьютере. Справа от матрицы $A(\Gamma_0)$ размещен столбец прямого транзитивного замыкания, построенного для вершины 1, т.е. $G^+(1)$, а под ней строка $G^-(1)$.

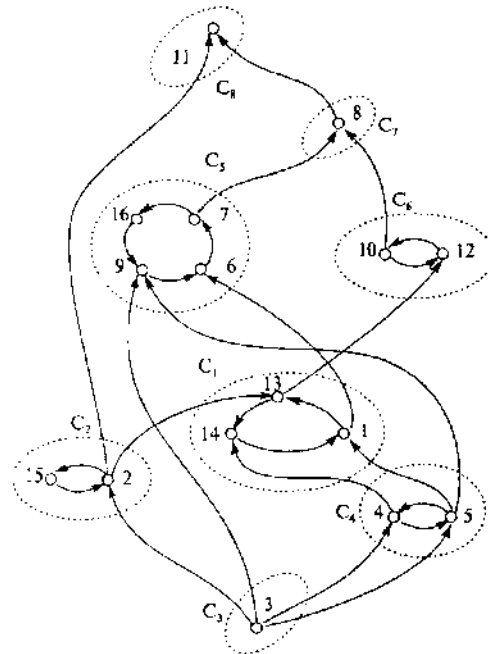


Рис. 3.31

$$\begin{array}{c}
\begin{array}{cccccccccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16
\end{array} \\
A(F_0) = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}
\begin{array}{l}
0 \\
* \\
* \\
* \\
* \\
1 \\
2 \\
3 \\
4 \\
3 \\
4 \\
2 \\
1 \\
2 \\
* \\
3
\end{array}
\end{pmatrix}
\end{array}$$

Если $i = 1$, то в клетку столбца против этой вершины ставим нулевую степень. В клетку столбца напротив вершины 6 ставим первую степень, так как для первой вершины соответствующая ей строка содержит 1 на позиции 6. Из этих же соображений 1 ставим на 13 месте столбца $G^+(1)$. Поскольку строка 6 матрицы $A(F_0)$ содержит 1 в позиции 7, то напротив вершины 7 ставим степень 2. Вместе со строкой 6 рассматривается строка 13; здесь уже две единицы: на позициях 12 и 14; следовательно, в столбце $G^+(1)$ на этих местах тоже появляются 2. Это означает, что кратчайшее расстояние от вершины 1 в вершины 7, 12 и 14 равно двум дугам. Строки 7, 12 и 14 содержат 1 на местах 8, 16, 10 и 1. Из этих четырех чисел последнее отбрасывается, поскольку из вершины 1 мы начали свое движение; соответствующая ей клеточка занята 0. Остальные три числа укажут места, куда выставляется степень 3. Далее, в строках 8, 10 и 16 единицы расположены на 8, 9, 11 и 12 месте; числа 8 и 12 игнорируем, а на 9 и 11 местах столбца $G^+(1)$ выставляем 4. Наконец, в строках 9 и 11 мы не находим новых позиций, значит остальные вершины орграфа F_0 из вершины 1 недостижимы. Прямое транзитивное замыкание $G^+(1)$ образовано вершинами $\{1, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16\}$, как и должно было получиться. В пустых клетках столбца $G^+(1)$ выставляем символы «*».

Аналогичным образом действуем в отношении обратного транзитивного замыкания $G^-(1)$, только вместо строк будем рассматривать уже столбцы матрицы смежности $A(F_0)$. Получающиеся числа в строке под матрицей $G^-(1)$ являются степенями G -оператора, которые указывают соответствующие длины путей до вершины 1. После проделанной процедуры у нас получается известный набор вершин: $\{1, 2, 3, 4, 5, 13, 14, 15\}$ с различными степенями достижимости вершины 1. Удаляя из матрицы $A(F_0)$ общие для $G^+(1)$ и $G^-(1)$ вершины, т.е. 1, 13, 14, переходим к матрице $A'(F_0)$. В ней выбираем произвольную вершину; пусть ею будет вершина 2. Затем целиком повторяем ту же процедуру, что и над матрицей $A(F_0)$. Так мы находим прямое и обратное транзитивные замыкания для вершины 2, которые были нами уже выписаны. В новой матрице смежности $A''(F_0)$ по сравнению с $A'(F_0)$ отсутствуют позиции 2 и 15. Общее число матриц смежности

с последовательно удаленными строками и столбцами равно числу классов эквивалентности; в нашем случае оно равно 8; выпишем еще три матрицы:

$$A(\Gamma_0) = \begin{pmatrix} 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 15 & 16 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 0 \\ * \\ * \\ * \\ * \\ * \\ * \\ * \\ * \\ * \\ 1 \\ * \\ 1 \\ * \end{matrix},$$

$$A''(\Gamma_0) = \begin{pmatrix} 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 16 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} * \\ * \\ * \\ 0 \\ 1 \\ 2 \\ 3 \\ * \\ * \\ 3 \\ * \\ * \\ 2 \end{matrix},$$

$$A'''(\Gamma_0) = \begin{pmatrix} 3 & 4 & 5 & 8 & 10 & 11 & 12 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} * \\ 0 \\ 1 \\ * \\ * \\ * \\ * \end{matrix},$$

$$\begin{matrix} 0 & 1 & * & * & * & * & * & * & * & * & * & 1 & * \\ 2 & 3 & 2 & 0 & 3 & * & 1 & * & * & * & 2 \end{matrix}$$

Разбиению на классы порядка поддаются только те орграфы, которые не содержат контуров и петель. Если таковые имеются, то прежде необходимо произвести разбивку на классы эквивалентности, а затем каждый из классов принять за вершину нового орграфа. В нашем случае этот новый орграф будет содержать восемь вершин, причем их упорядочение из рис. 3.26 вполне очевидно. Чтобы не играть с читателем в поддавки, возьмем в качестве исходного орграфа Γ_0 , подлежащего упорядочению, более сложную структуру на 18 вершинах, изображенную на рис. 3.32; здесь уже иерархию вершин предугадать сложно.

Упорядочение по матрице смежности $A(\Gamma_0)$ производится строго по столбцам. Если упорядочение производить по строкам, то полученная иерархия будет соответствовать противоположному направлению дуг. Мы приводим оба вида

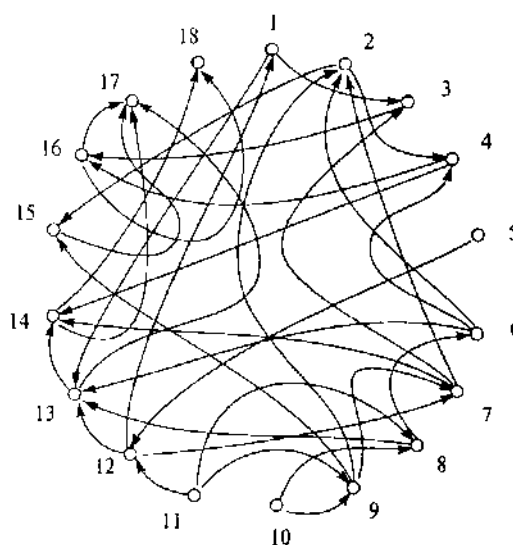


Рис. 3.32

упорядочения, чтобы продемонстрировать их различие. Когда спрашивается, изменится ли разбиение вершин на классы порядка при одновременной смене направления всех дуг орграфа G_0 (рис. 3.32), обычно отвечают: «нет, классы останутся прежними». Но это не так: упорядочение по противоположному направлению дуг, т.е. по строкам матрицы смежности $A(G_0)$, создает другие классы порядка.

Итак, опишем прямое разложение орграфа на классы порядка по столбцам матрицы $A(G_0)$. Для нахождения первого класса порядка C_1 подсчитаем число единиц в каждом столбце и выпишем результаты в первую строку под матрицей $A(G_0)$. В трех позициях, а именно: 5, 10 и 11, оказались нули, так как в соответствующих столбцах отсутствуют единицы. Это означает, что вершины 5, 10 и 11 образовали самый нижний уровень: им не предшествует ни одна дуга; они являются «истоками»; эти три вершины образовали класс порядка C_1 .

$$A(G_0) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} 2 & 2 & 2 & 0 & * & * & * \\ 2 & 2 & 2 & 0 & * & * & * \\ 1 & 1 & 0 & * & * & * & * \\ 2 & 2 & 0 & * & * & * & * \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 3 & 3 & 3 & 1 & 0 & * & * \\ 3 & 3 & 2 & 1 & 0 & * & * \\ 2 & 2 & 2 & 1 & 1 & 0 & * \\ 3 & 3 & 3 & 2 & 1 & 0 & * \\ 2 & 2 & 2 & 2 & 2 & 2 & 0 \\ 3 & 3 & 3 & 3 & 3 & 3 & 0 \\ 3 & 3 & 3 & 2 & 1 & 0 & * \\ 2 & 1 & 0 & * & * & * & * \\ 2 & 1 & 0 & * & * & * & * \\ 2 & 1 & 0 & * & * & * & * \\ 2 & 0 & * & * & * & * & * \\ 0 & * & * & * & * & * & * \\ 0 & * & * & * & * & * & * \end{matrix}$$

$$\begin{matrix} 1 & 3 & 2 & 2 & 0 & 1 & 2 & 2 & 2 & 0 & 0 & 2 & 4 & 3 & 2 & 3 & 4 & 2 \\ 1 & 3 & 2 & 2 & * & 1 & 2 & 0 & 0 & * & * & 0 & 4 & 3 & 2 & 3 & 4 & 2 \\ 0 & 2 & 2 & 2 & * & 0 & 0 & * & * & * & * & 2 & 3 & 1 & 3 & 4 & 2 \\ * & 0 & 0 & 1 & * & * & * & * & * & * & * & 0 & 2 & 1 & 3 & 4 & 2 \\ * & * & * & 0 & * & * & * & * & * & * & * & * & 1 & 0 & 2 & 3 & 2 \\ * & * & * & * & * & * & * & * & * & * & * & * & 0 & * & 0 & 2 & 2 \\ * & * & * & * & * & * & * & * & * & * & * & * & * & * & 0 & 0 & 0 \end{matrix}$$

Далее, «мысленно» (чтобы не выписывать новую матрицу смежности) вычеркнем из матрицы $A(G_0)$ названные строки и вновь подсчитаем число единиц по столбцам, а результат запишем во вторую строку под матрицей; на местах же 5, 10 и 11 выставим символы «*». Во второй строке нули окажутся в 8, 9 и 12 позициях, значит, вершины под этими номерами образуют класс C_2 . Снова вычеркиваем три строки, соответствующие уже этим вершинам. Начинаем искать вершины третьего класса порядка C_3 и т.д. В результате получим семь классов порядка.

Обратное разложение орграфа на классы порядка по строкам матрицы $A(G_0)$, которое будет соответствовать противоположному направлению дуг, по количеству тоже дает семь классов, но по составу вершин три из них отличаются от прямого разложения. Выпишем для сравнения все классы порядка, причем классы разложения по противоположному направлению дуг пометим штрихом:

$$C_1 = \{5, 10, 11\}, \quad C'_1 = \{5, 10, 11\},$$

$$C_2 = \{8, 9, 12\}, \quad C'_2 = \{8, 9, 12\},$$

$$\begin{aligned}
C_2 &= \{1, 6, 7\}, & C'_2 &= \{6, 7\}, \\
C_3 &= \{2, 3, 13\}, & C'_3 &= \{1, 2\}, \\
C_4 &= \{4, 15\}, & C'_4 &= \{3, 4, 13, 15\}, \\
C_5 &= \{14, 16\}, & C'_5 &= \{14, 16\}, \\
C_6 &= \{17, 18\}, & C'_6 &= \{17, 18\}.
\end{aligned}$$

Если бы на каком-либо этапе появилась строка (для прямого разложения) или столбец (для обратного разложения) без нулей, то это означало бы, что исходный орграф G_0 содержит контуры и требуется предварительная процедура разложения G_0 на подграфы сильно связанных вершин. У нас такой ситуации не возникло. На рис. 3.33 изображен упорядоченный орграф G_0 по прямому разложению на классы порядка C_r .

Теперь поставим перед собой новую задачу. Пусть каждая дуга нашего упорядоченного орграфа снабжена весом, который складывается из сумм весов инцидентных ей вершин. За вес вершины примем ее порядковый номер. Так, у нас имеется дуга, идущая из вершины 2 в вершину 15, следовательно, вес этой дуги равен 17. Для наглядности будем считать, что она имеет длину 17 километров. Задача формулируется так: найти два пути, соответствующие минимальной и максимальной длине.

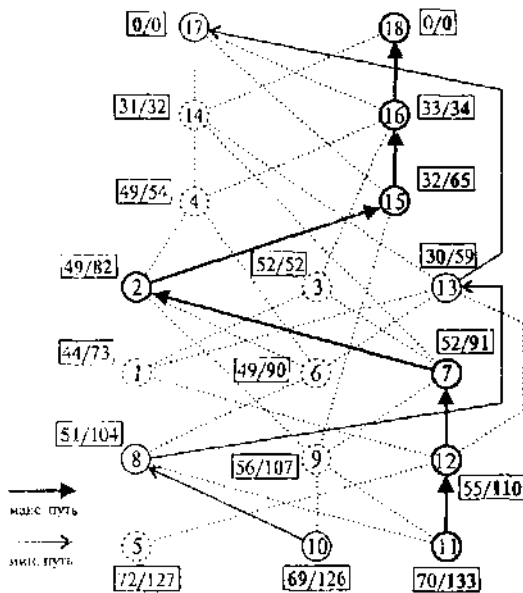


Рис. 3.33

Поиск оптимального пути предполагает расстановку *потенциалов* для каждой вершины, т.е. образно говоря, некоего счета, на котором указывается километраж (мин./макс.). Расстановка потенциалов начинается сверху. Потенциал седьмого уровня принимается за 0; потенциалы других вершин получают из общей длины пути, отсчитанной от вершин самого верхнего уровня до данной вершины, при этом подсчитывается длина всех путей, ведущих к этой вершине. Так, от вершины 2, принадлежащей 4 уровню, к вершинам 17 и 18, принадлежащих седьмому уровню, ведут семь путей; перечислим их по степени возрастания:

- 1) $17 + 32 = 49$, 2) $6 + 18 + 31 = 55$, 3) $6 + 18 + 32 = 56$,
- 4) $6 + 20 + 33 = 59$, 5) $6 + 20 + 34 = 60$, 6) $17 + 31 + 33 = 81$,
- 7) $17 + 31 + 34 = 82$.

Следовательно, минимальный потенциал равен 49, максимальный — 82 километрам. Если потенциалы вершин 4 и 15, принадлежащих пятому уровню, известны, вычислений понадобится гораздо меньше; ясно, что максимальный и минимальный путь для вершины 2 определится дугой в 17 километров, которая

ведет к вершине 15 с потенциалами 32/65. Поэтому расстановку потенциалов и рекомендуется начинать с самых верхних вершин, двигаясь последовательно по уровням вниз.

Таким образом, получаем минимальный, равный 69 километрам, и максимальный, равный 133 километрам, потенциалы. Далее остается только провести отличительными линиями дуги, инцидентные вершинам с максимальным и минимальным потенциалами, взятыми уже по каждому уровню. Если расстановку потенциалов мы начинали сверху, то проводка оптимальных путей начинается снизу. Для обратного движения сверху вниз расстановка потенциалов начинается снизу, а проводка путей — сверху. Хотя разложение вершин на классы порядка для обратного движения отличается от прямого, длина минимального и максимального путей не меняется, т.е. если мы ехали от пункта A в пункт B по дороге с минимальной длиной пути в 69 километров, то обратная поездка из пункта B в пункт A должна составить тот же самый минимальный километраж и проходить по тем же самым промежуточным пунктам.

Вообще, следует заметить, задача поиска оптимального пути *в принципе* может быть решена без предварительного разбиения на классы порядка. Разбиение на классы в особо запутанных графах лишь существенно облегчает этот поиск.

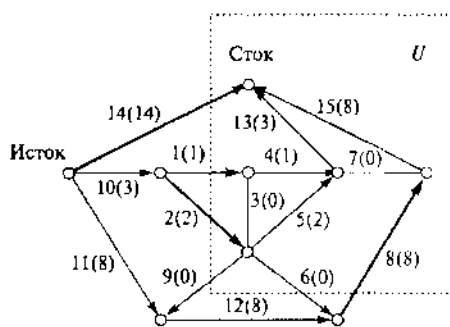


Рис. 3.34

Пусть орграф G_0 (рис. 3.34) представляет собой *транспортную сеть*, каждая дуга которой обладает заранее определенной *пропускной способностью* μ (в качестве таковой примем числа, нумерующие дуги). Поставим задачу нахождения максимальной пропускной способности сети между ее истоком и стоком. При нахождении *общего фактического потока* λ необходимо помнить об очевидных правилах: сумма потоков дуг, выходящих из истока транспортной сети, должна быть равна сумме потоков дуг, входящих в сток; алгебраическая сумма потоков при любой вершине, не принадлежащей стоку или истоку, должна быть равна нулю; максимальный поток на пути от вершины i к вершине j определяется дугой k , которая имеет минимальную пропускную способность из всех дуг, принадлежащих этому пути.

Если пропускная способность k -дуги μ_k равна идущему через нее потоку λ_k , то такую дугу будем называть *насыщенной*, а любой путь, куда она включена, — *насыщенным путем*. У нас k -й номер дуги (число вне скобок) определяет величину пропускной способности μ_k , а число в скобках говорит о фактическом потоке λ_k , т.е. в наших обозначениях имеем $\mu_k(\lambda_k)$. Общий поток транспортной сети будет максимальным $\lambda_{\max}$, если любой путь, соединяющий исток со стоком, окажется насыщенным. В этом случае поток $\lambda_{\max}$ станет равным минимальной пропускной способности $\mu_{\min}$ разреза, отделяющего сток от истока.

Если пропускная способность k -дуги μ_k равна идущему через нее потоку λ_k , то такую дугу будем называть *насыщенной*, а любой путь, куда она включена, — *насыщенным путем*. У нас k -й номер дуги (число вне скобок) определяет величину пропускной способности μ_k , а число в скобках говорит о фактическом потоке λ_k , т.е. в наших обозначениях имеем $\mu_k(\lambda_k)$. Общий поток транспортной сети будет максимальным $\lambda_{\max}$, если любой путь, соединяющий исток со стоком, окажется насыщенным. В этом случае поток $\lambda_{\max}$ станет равным минимальной пропускной способности $\mu_{\min}$ разреза, отделяющего сток от истока.

В связи с последним замечанием дадим определение разреза применительно к транспортной сети. Пусть сток принадлежит некоторому множеству вершин U (они лежат внутри прямоугольника). Тогда разрезом $S(U)$ называются все *входя-*

щие в вершины U насыщенные дуги (в нашем случае это дуги 1, 2, 8 и 14); пропускная способность *выходящих* из вершин U дуг при этом не учитывается (выходящими дугами у нас являются 6 и 9). Поиск максимального потока осуществляется путем перебора всех возможных насыщенных путей от истока к стоку, причем при расстановке потока в дугах ориентируются только на три выше сформулированных правила. В результате перебора получим величину максимального потока:

$$\lambda_{\max} = \mu_{\min} = 1 + 2 + 8 + 14 = 25.$$

Поскольку изображенный на рис. 3.34 орграф достаточно простой, предварительной работы по разбиению его на сильно связанные классы вершин с последующим упорядочением их между уровнями истока и стока проводить необязательно.

Разбиение на классы порядка не требуется проводить еще в двух важных случаях. Во-первых, когда иерархия вершин возникла сама собой, по причине внутренней природы математического объекта, представленного графом. Лучшей иллюстрацией здесь являются *решетки, образованные подгруппами*. Какой бы сложной ни была решетка, ее вершины всегда заранее разбиты на классы порядка, при этом в самом низу оказывается вершина, представляющая тождественный элемент, а на самом веру вершина, представляющая всю группу целиком. Число элементов в подгруппе является естественным критерием упорядочения. Во-вторых, упорядочение излишне в *корневых деревьях*: чем дальше вершина расположена от корня, который можно принять за первый класс порядка, тем выше класс порядка рассматриваемой вершины. Количество ребер, соединяющих данную вершину с корневой, здесь также является естественным критерием упорядочения. С корневыми деревьями мы, например, встречались в разделе «Логика» при рассмотрении *метода резолюций* (см. рис. 1.19). Далее мы продолжим изучение структур древовидной формы, но уже в рамках теории кодирования и автоматов.

3.4. Решение задач по теории кодирования, автоматов и языков с использованием графов

Кодирование производится с целью:

- 1) сокращения символьного текста при ограниченном количестве кодовых символов -- *оптимальное кодирование*;
- 2) обнаружения и исправления ошибок при передаче и хранении информации -- *корректирующее кодирование*;
- 3) защиты информации от несанкционированного доступа -- *секретное кодирование*.

Редко, когда все перечисленные задачи выступают отдельно; на практике чаще бывает совмещение двух или даже трех целей. Однако для лучшего понимания предмета разберем каждый пункт в отдельности, начиная с оптимального кодирования.

Предположим, нужно передать четыре сообщения -- a_1, a_2, a_3, a_4 . Эти сообщения можно закодировать так, как показано в табл. 3.10.

При таком кодировании вероятность появления сообщений не учитывалась или предполагалась одинаковой для всех четырех сообщений ($p = 0,25$). Между тем их появление в информационном тексте может происходить с различной частотой; предположим, вероятности появления сообщений равны:

$$p_1 = 0,5, \quad p_2 = 0,25, \quad p_3 = 0,125, \quad p_4 = 0,125.$$

Фано, учитывая вероятность сообщений, предложил следующее оптимальное кодирование (табл. 3.10).

Таблица 3.10

Сообщения	a_1	a_2	a_3	a_4
Коды	00	01	10	11

Таблица 3.11

Сообщения	a_1	a_2	a_3	a_4
Коды	1	01	001	000

Показателем экономичности кода служит *средняя длина кодового слова*, которая определяется как

$$l = \sum_{i=1}^n l_i p_i,$$

где l_i — длина кодового слова a_i , p_i — вероятность появления a_i , n — число сообщений.

Для кодировки сообщений по табл. 3.10 средняя длина равна 2, а по табл. 3.11 — 1,75. Следовательно, закодированный по методике Фано информационный текст окажется короче.

На первый взгляд кодирование по методу Фано кажется избыточным, поскольку коды, представленные табл. 3.11, можно сократить, например, так, как это показано в табл. 3.12.

Таблица 3.12

Сообщения	a_1	a_2	a_3	a_4
Коды	1	0	01	00

Теперь возьмем следующий закодированный текст: 00101000. Согласно табл. 3.12, данный текст не может быть однозначно дешифрован, так как непонятно, что, собственно, подразумевается: сообщения вида — a_2, a_3, a_3, a_4, a_2 ; или — $a_4, a_1, a_1, a_2, a_2, a_2$; или — $a_2, a_2, a_1, a_2, a_1, a_2, a_4$ и т.д. Расшифровка же текста по табл. 3.11 производится однозначно — a_1, a_2, a_4 . В связи с этим замечательным свойством код Фано называется *префиксным*. Никакое кодовое слово префиксного кода не является началом другого кодового слова. Наряду с методом Фано, существует префиксное кодирование по *методу Хаффмана*, экономичность которого выше первого.

Для защиты передаваемых текстов от помех используются *корректирующие коды*, которые основываются на *информационной избыточности*. Самый простой способ создания избыточности достигается многократным дублированием передаваемых символов, т.е. образованием символьных блоков: $0 \rightarrow 000, 1 \rightarrow 111$. В случае сбоя, решение при дешифровке принимается по большинству оставшихся однотипных символов в блоке. Сами блоки могут включать большее (чем 3) число символов, тогда степень защищенности текста окажется выше. Если длину блока выбрать заранее достаточно огромной, то практически любые ошибки

можно исключить, правда, при этом скорость передачи информации упадет пропорционально количеству символов в блоке.

Существует очень простая, но эффективная защита информационного текста от *одиночного* сбоя, которая требует минимальную избыточность в один дополнительный символ. Это — *проверка на четность*. При шифровке к тексту добавляется 0 или 1 в зависимости от четности или нечетности суммы единиц в тексте. Если при дешифровке обнаружится нечетное число единиц, значит, текст был передан неверно; если четное — ошибки при передаче не было.

Корректирующий код можно построить с помощью квадратной матрицы, которая не только обнаруживает одиночную ошибку, но и определяет ее местонахождение. Пусть требуется передать девятиразрядное информационное слово $a = a_{11} \dots a_{13}$. Тогда к нему прибавляют семиразрядное корректирующее слово $a' = a_{41} \dots a_{14}$, символы которого удовлетворяет совокупности проверочных соотношений:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}, \quad \begin{aligned} a_{11} &= a_{11} + a_{12} + a_{13}, & a_{41} &= a_{11} + a_{21} + a_{31}, \\ a_{24} &= a_{21} + a_{22} + a_{23}, & a_{42} &= a_{12} + a_{22} + a_{32}, \\ a_{34} &= a_{31} + a_{32} + a_{33}, & a_{43} &= a_{13} + a_{23} + a_{33}, \\ a_{44} &= a_{21} + a_{42} + a_{43}, & a_{44} &= a_{14} + a_{24} + a_{34}. \end{aligned}$$

(суммирование осуществляется по mod (2)).

Предположим, получено следующее закодированное сообщение:

$$A = a \ a' = 011001011 \ 1010000.$$

Размещаем его в матрице размерности 4×4 и составляем проверочные равенства:

$$A = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \quad \begin{aligned} 0 &= 0+1+1, & 1 &= 0+0+0, \\ 0 &= 0+0+1, & 0 &= 1+0+1, \\ 0 &= 0+1+1, & 1 &= 1+1+1, \\ 0 &= 1+0+1, & 0 &= 0+0+0. \end{aligned}$$

Проверочные соотношения для a_{24} и a_{41} ошибочны; следовательно, вместо $a_{21} = 0$, на самом деле нужно брать $a_{21} = 1$; исходная последовательность должна была выглядеть как 011101011 1010000.

Для засекречивания информации исходные сообщения могут кодироваться с помощью *адресной матрицы*. Дело в том, что любое сообщение хранится на информационном носителе по определенному адресу и считывается по определенному коммуникационному каналу. Пусть сообщение a хранится по адресу A , который выражается трехзначным числом — $A_0A_1A_2$. Коммуникационные каналы обозначим как c_1, c_2, c_3 и c_4 . Адресная матрица программируется так, чтобы на ней происходило смешивание адресов и коммуникационных каналов, например, в следующем конкретном виде:

$$\begin{aligned} c'_1 &= c_1A_0\bar{A}_1\bar{A}_2 + c_2A_0\bar{A}_1A_2 + c_3\bar{A}_0A_1A_2 + c_4A_0A_1\bar{A}_2, \\ c'_2 &= c_4A_0A_1\bar{A}_2 + c_2A_0A_1A_2 + c_1\bar{A}_0A_1A_2 + c_3A_0A_1\bar{A}_2, \\ c'_3 &= c_3A_0A_1\bar{A}_2 + c_1A_0\bar{A}_1A_2 + c_2\bar{A}_0A_1A_2 + c_4A_0A_1A_2, \\ c'_4 &= c_2A_0A_1A_2 + c_3A_0\bar{A}_1A_2 + c_4A_0A_1A_2 + c_1A_0A_1\bar{A}_2. \end{aligned}$$

Если информационное сообщение имеет адрес 100 ($A_0\bar{A}_1\bar{A}_2$), то коммуникационный канал c'_1 подключается к каналу c_1 , канал c'_2 — к инверсному каналу c_4 , c'_3 — к инверсному c_3 и, наконец, c'_4 — к c_2 ; если идет сообщение с адресом 101 ($A_0A_1\bar{A}_2$), то осуществляется подключение канала c'_1 к инверсному c_4 и т.д. В результате перемешивания каналов информационные сообщения попадают на чужие адресные места, так что несанкционированное считывание становится невозможным. Таков один из принципов засекречивания информации.

Мы рассмотрели «азы» теории кодирования. К секретному кодированию мы больше не вернемся; корректирующее кодирование было детально рассмотрено в последнем подразделе главы «Группы»; остается рассмотреть методы оптимального кодирования, в частности, Фано и Хаффмана.

Фано предложил следующий принцип кодирования сообщений, имеющих вероятностную характеристику. Все сообщения выписываются в таблицу по степени убывания вероятности и разбиваются на две группы равной (насколько это возможно) вероятности. Первой группе присваивается символ 0, второй — 1. Затем каждая из групп вновь делится на две подгруппы равной вероятности, которым также присваиваются символы 0 и 1. В результате многократного повторения этой процедуры получается таблица кодовых слов. Продемонстрируем данную методику на конкретном примере.

Предположим, необходимо закодировать 13 сообщений, причем вероятность одного из них равна 0,653, вероятность трех других сообщений равна 0,023, еще четырех — 0,027, и, наконец, пяти оставшихся — 0,034. Сумма вероятностей всех сообщений равна 1. Эти вероятности внесены во второй столбец табл. 3.13 в порядке убывания; первый столбец нумерует сообщения, а в третьем записаны окончательные коды Фано.

Таблица 3.13

n	P_n	Коды
1	0,653	0
2	0,034	1 0 0 0
3	0,034	1 0 0 1
4	0,034	1 0 1 0 0
5	0,034	1 0 1 0 1
6	0,034	1 0 1 1
7	0,027	1 1 0 0 0
8	0,027	1 1 0 0 1
9	0,027	1 1 0 1 0
10	0,027	1 1 0 1 1
11	0,023	1 1 1 0 0
12	0,023	1 1 1 0 1
13	0,023	1 1 1 1

Средняя длина кодового слова равна:

$$l = 2,263.$$

Процедура кодирования с помощью двух символов может быть представлена *бинарным деревом* (рис. 3.35). Длина ветвей, равная длине каждого кодового слова, определяет естественные порядковые уровни. В нашем дереве символу 0 от-

вечает ребро, отклоняющееся влево, а символу 1 — ребро, отклоняющееся вправо. Например, пятое сообщение имеет код 10101; соответствующая ему ветвь выделена жирной линией.

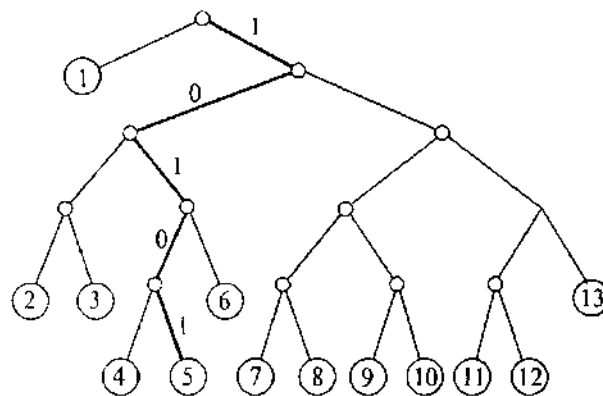


Рис. 3.35

Коды Фано по оптимальности несколько уступают кодам Хаффмана, который показал, что его методика дает предельное сжатие информационного текста. Пусть требуется закодировать все ту же последовательность сообщений. Кодовая таблица Хаффмана (табл. 3.14) начинает заполняться со столбца P_1 ; столбец P берем за исходный, а столбцы K, K_1, K_2 и т.д. пока оставляем без внимания. В столбце P_1 затемненная вероятность 0,046 получается путем сложения двух наименьших вероятностей, остальные вероятности записываются без изменений. Аналогично заполняются все последующие столбцы P_2, P_3 , и т.д. Далее Хаффман рассуждал примерно следующим образом. Два сообщения с наименьшими вероятностями должны иметь одинаковые длины кодовых слов и различаться последними символами. Поэтому в последнем столбце K_{11} против двух вероятностей выставляются символы 0 и 1. Затем идут по табл. 3.14 в обратном направлении, заполняя столбцы $K_{10}, K_9, \dots, K_1, K$. При этом символы 0 и 1 ставятся против тех вероятностей, которые в сумме давали затемненную вероятность. В частности, сначала в столбце K_{10} против вероятности 0,653 записываем 0, а против чисел 0,211 и 0,136 — 1. Затем к этим единицам приписываем новую пару символов 0 и 1, получая коды 10 и 11.

Таблица 3.14

n	P	K	P_1	K_1	P_2	K_2	P_3	K_3	P_4	K_4	P_5	K_5	P_6	K_6	P_7	K_7	P_8	K_8	P_9	K_9	P_{10}	K_{10}	P_{11}	K_{11}
1	0,653	0	0,653	0	0,653	0	0,653	0	0,653	0	0,653	0	0,653	0	0,653	0	0,653	0	0,653	0	0,653	0	0,653	0
2	0,034	1	0,046	1011	0,050	1010	0,054	1001	0,060	1000	0,068	111	0,068	110	0,096	101	0,115	100	0,136	11	0,211	10	0,347	1
3	0,034	1101	0,034	1100	0,046	1011	0,050	1010	0,054	1001	0,060	1000	0,068	111	0,068	110	0,096	101	0,115	100	0,136	11		
4	0,034	1110	0,034	1101	0,034	1100	0,046	1011	0,050	1010	0,054	1001	0,060	1000	0,068	111	0,068	110	0,096	101	0,115	100	0,136	11
5	0,034	1111	0,034	1110	0,034	1101	0,034	1100	0,046	1011	0,050	1010	0,054	1001	0,060	1000	0,068	111	0,068	110	0,096	101		
6	0,034	1000	0,034	1111	0,034	1110	0,034	1101	0,034	1100	0,046	1011	0,050	1010	0,054	1001	0,060	1000	0,068	111				
7	0,027	1001	0,034	1000	0,034	1111	0,034	1110	0,034	1101	0,034	1100	0,046	1011	0,050	1010	0,054	1001	0,060	1000	0,068	111		
8	0,027	1001	0,027	1000	0,034	1000	0,034	1111	0,034	1110	0,034	1101	0,034	1100	0,046	1011	0,050	1010	0,054	1001	0,060	1000	0,068	111
9	0,027	1001	0,027	1001	0,027	1000	0,034	1000	0,034	1111	0,034	1110	0,034	1101										
10	0,027	1010	0,027	1000	0,027	1000	0,027	1000	0,027	1000														
11	0,023	1010	0,027	1010	0,027	1001																		
12	0,023	1011	0,023	1010																				
13	0,023	0111																						

Далее обращаем внимание на затемненное число 0,211 столбца P_{10} ; оно получилось при суммировании чисел 0,15 и 0,096 столбца P_9 , следовательно, этим вероятностям сообщаем одинаковый код 10 и приписываем по третьему символу, так что в столбце K_9 возникают коды 100 и 101. Два других кода — 0 и 11 — переписываются в K_9 из K_{10} без изменений. Продолжая эту процедуру, мы заполняем последний кодовый столбец K , который образует окончательную систему кодовых слов. По ней вычерчиваем бинарное дерево (рис. 3.36) на тех же принципах, что и предыдущее дерево, т.е. отклонение ребра влево означает ноль, вправо — единицу.

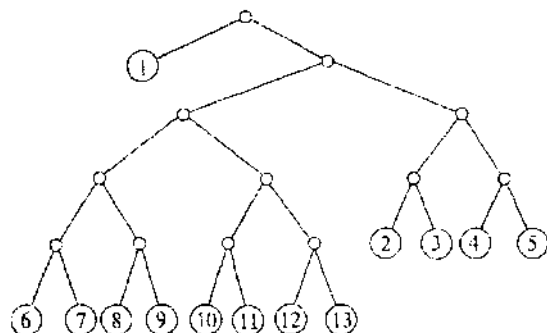


Рис. 3.36

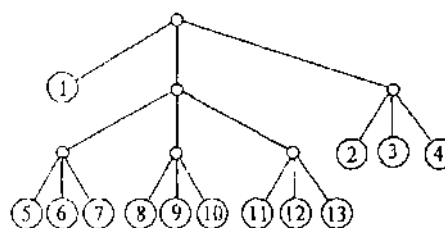


Рис. 3.37

Средняя длина слова, закодированного по Хаффману, равна 2,252, что несколько меньше, чем по Фано. Большей оптимизации достичь невозможно, за исключением того случая, если вместо двух символов (0 и 1) использовать три символа — 0, 1 и 2. *Тринарное дерево* Хаффмана изображено на рис. 3.37. По нему легко установить коды сообщений, если помнить, что для каждого ребра левое ребро означает 0, правое — 2, а серединное — 1. Методика, по которой рассчитываются коды, та же, что и в предыдущем случае, только суммируются не две наименьшие вероятности, а три. Длина кодового слова при тринарной кодировке равна 1,592, что почти в полтора раза меньше, чем при бинарном кодировании.

Кодовые деревья Фано и Хаффмана можно рассматривать как графическое задание алгоритмов поиска. При таком понимании средняя длина кодового слова пропорциональна стоимости поиска: чем выше частота обращения к конечной (внешней) вершине, тем меньше должна быть длина пути к ней. С этой точки зрения рассмотренные деревья являются оптимальными только в отношении обращения к конечным вершинам. А как нужно было бы изменить алгоритм построения оптимального дерева, если бы наряду с вероятностями обращения к внешним вершинам были бы заданы вероятности обращения и к внутренним вершинам?

Пусть задан тот же самый ряд вероятностей, который, однако, мы разделим на две части; первая часть будет связана с вероятностью (частотой) обращения к *внешним* вершинам a_i (табл. 3.15), вторая — с вероятностью обращения к *внутренним* вершинам b_i (табл. 3.16).

Таблица 3.15

Вершина	a_0	a_1	a_2	a_3	a_4	a_5	a_6
Вероятность	0,653	0,034	0,034	0,027	0,027	0,023	0,023

Таблица 3.16

Вершина	b_1	b_2	b_3	b_4	b_5	b_6
Вероятность	0,034	0,034	0,034	0,027	0,027	0,023

Нахождение бинарного дерева по оптимальному достижению внешних и внутренних вершин начнем с допущения. Предположим, что дерево $t_{i,j}$ уже является оптимальным, а внутренняя вершина b_k является его корнем. Тогда это дерево можно разбить на два поддерева: $t_{i,k-1}$, являющееся оптимальным на множестве вершин $\{a_i, b_{i+1}, a_{i+1}, \dots, b_{k-1}, a_{k-1}\}$, и $t_{k,j}$, являющееся оптимальным на множестве $\{a_k, b_{k+1}, a_{k+1}, \dots, b_j, a_j\}$. В отношении индексов должно выполняться условие: $i \leq k \leq j$. Суммарная частота обращения к вершинам оптимального дерева $t_{i,j}$ рассчитывается по формуле:

$$r_{i,j} = q_{i,j} + \min(r_{i,k-1} + r_{k,j}), \quad q_{i,j} = q_{i,j-1} + p(a_j) + p(b_j),$$

где $p(a_j)$ и $p(b_j)$ — вероятности обращения к вершинам a_j и b_j , а индекс k под знаком $\min$ пробегает значения от i до j .

Результаты расчета по этой формуле лучше всего оформить таблицей, в которой по горизонтали меняется значение индекса i , а по вертикали — номер строки h ; при этом $j = i + h$. В каждую клетку таблицы будем заносить значения $r_{i,j}$ и $q_{i,j}$.

Понятно, что $t_{i,i}$ являются «пустыми» деревьями с корнем во внешней вершине a_i ($r_{i,i} = 0$, $q_{i,i} = p_i$). Таким образом, первая строка табл. 3.17 заполняется без всякого предварительного расчета. Вторая строка этой таблицы также не требует больших вычислений, поскольку для деревьев типа $t_{i,i+1}$, состоящих из двух вершин и одного инцидентного им ребра, выполняется условие: $r_{i,i+1} = q_{i,i+1}$; конкретно:

$$\begin{aligned} q_{0,1} &= q_{0,0} + p(a_1) + p(b_1) = 0,653 + 0,034 + 0,034 = 0,721, \\ q_{1,2} &= q_{1,1} + p(a_2) + p(b_2) = 0,034 + 0,034 + 0,034 = 0,102, \\ q_{2,3} &= 0,095, \quad q_{3,4} = 0,081, \quad q_{4,5} = 0,077, \quad q_{5,6} = 0,065. \end{aligned}$$

Третью строку табл. 3.17 вычисляем с учетом минимальной вероятности поддерева:

$$\begin{aligned} q_{0,2} &= q_{0,1} + p(a_2) + p(b_2) = 0,721 + 0,034 + 0,034 = 0,789, \\ r_{0,2} &= q_{0,2} + \min_{0 \leq k \leq 2} (r_{0,k} + r_{k,2}) = 0,789 + 0,102 = 0,891; \\ q_{1,3} &= q_{1,2} + p(a_3) + p(b_3) = 0,102 + 0,034 + 0,027 = 0,163, \\ r_{1,3} &= q_{1,3} + \min_{1 \leq k \leq 3} (r_{1,k} + r_{k,3}) = 0,163 + 0,095 = 0,258; \quad \text{и т.д.} \end{aligned}$$

Покажем, как выглядят конкретные формулы для вычисления вероятности $r_{1,6}$:

$$q_{1,6} = q_{1,5} + p(a_6) + p(b_6) = 0,267 + 0,023 + 0,023 = 0,313,$$

$$r_{1,6} = q_{1,6} + \min_{1 \leq k \leq 6} \begin{pmatrix} r_{1,1} + r_{2,6} \\ r_{1,2} + r_{3,6} \\ r_{1,3} + r_{4,6} \\ r_{1,4} + r_{5,6} \\ r_{1,5} + r_{6,6} \end{pmatrix} = 0,313 + (0,102 + 0,327) = 0,742.$$

Таблица 3.17

$q_{0,0} = 0,653$ $r_{0,0} = 0,000$	$q_{1,1} = 0,034$ $r_{1,1} = 0,000$	$q_{2,2} = 0,034$ $r_{2,2} = 0,000$	$q_{3,3} = 0,027$ $r_{3,3} = 0,000$	$q_{4,4} = 0,027$ $r_{4,4} = 0,000$	$q_{5,5} = 0,023$ $r_{5,5} = 0,000$	$q_{6,6} = 0,023$ $r_{6,6} = 0,000$
$q_{0,1} = 0,721$ $r_{0,1} = 0,721$	$q_{1,2} = 0,102$ $r_{1,2} = 0,102$	$q_{2,3} = 0,095$ $r_{2,3} = 0,095$	$q_{3,4} = 0,081$ $r_{3,4} = 0,081$	$q_{4,5} = 0,077$ $r_{4,5} = 0,077$	$q_{5,6} = 0,069$ $r_{5,6} = 0,069$	
$q_{0,2} = 0,781$ $r_{0,2} = 0,891$	$q_{1,3} = 0,163$ $r_{1,3} = 0,258$	$q_{2,4} = 0,149$ $r_{2,4} = 0,230$	$q_{3,5} = 0,131$ $r_{3,5} = 0,208$	$q_{4,6} = 0,123$ $r_{4,6} = 0,192$		
$q_{0,3} = 0,850$ $r_{0,3} = 1,108$	$q_{1,4} = 0,217$ $r_{1,4} = 0,400$	$q_{2,5} = 0,199$ $r_{2,5} = 0,371$	$q_{3,6} = 0,177$ $r_{3,6} = 0,327$			
$q_{0,4} = 0,904$ $r_{0,4} = 1,304$	$q_{1,5} = 0,267$ $r_{1,5} = 0,577$	$q_{2,6} = 0,245$ $r_{2,6} = 0,532$				
$q_{0,5} = 0,954$ $r_{0,5} = 1,531$	$q_{1,6} = 0,313$ $r_{1,6} = 0,742$					
$q_{0,6} = 1,000$ $r_{0,6} = 1,742$						

Здесь минимальная вероятность получается во второй строке ($r_{1,2} + r_{3,6}$) при значении $k = 3$, следовательно, корневой вершиной дерева $t_{1,6}$ с поддеревьями $t_{1,2}$ и $t_{3,6}$ будет b_3 . Итак, все внутренние вершины являются корнями своих поддеревьев; пользуясь вычислениями r_{ij} , выпишем их:

$$\begin{aligned} b_1: t_{0,6} &= t_{0,0} + t_{1,6}, & b_2: t_{1,2} &= t_{1,1} + t_{2,2}, & b_3: t_{1,6} &= t_{1,2} + t_{3,6}, \\ b_4: t_{3,6} &= t_{3,3} + t_{4,4}, & b_5: t_{3,6} &= t_{3,4} + t_{5,6}, & b_6: t_{5,6} &= t_{5,5} + t_{6,6}. \end{aligned}$$

После этого можно приступить к вычерчиванию бинарного дерева оптимального поиска (рис. 3.38).

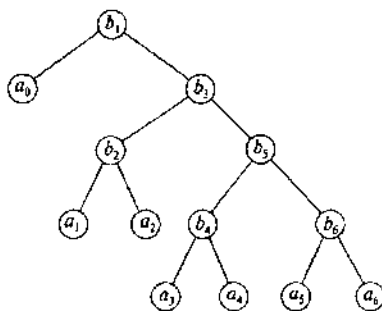


Рис. 3.38

Вершины построенного нами дерева можно было бы закодировать. Однако, с точки зрения теории кодирования, получающийся при этом код не был бы префиксным. Тем не менее среднюю длину кодового слова и здесь рассчитать возможно:

$$l = \sum_{i=0}^n l_i p(a_i) + \sum_{j=1}^n (l_j + 1) p(b_j),$$

где l_i — длина пути до внешней вершины a_i , l_j — длина пути до внутренней вершины b_j .

Если все вычисления проделаны верно, то средняя длина кодового слова l должна в точности совпасть со стоимостью поиска по

дереву $t_{0,6}$: $l = r_{0,6}$, что в нашем случае имеет место. Данное равенство играет роль проверочного соотношения.

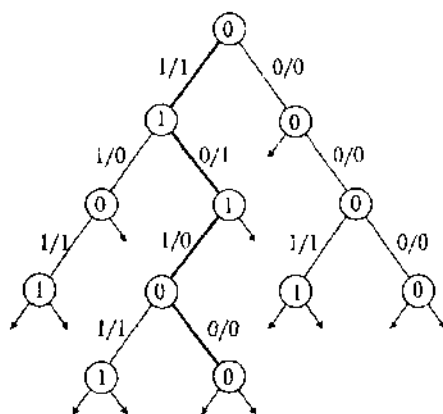


Рис. 3.39

Теперь рассмотрим рис. 3.39, где изображено бесконечное бинарное дерево, переводящее входную последовательность из нулей и единиц в выходную. Дерево имеет два типа вершин — 0 и 1, а каждое ребро снабжено дробью: числитель означает входной символ, знаменатель — выходной; концевые ребра оканчиваются стрелками, указывающими на возможное продолжение ветвей. Жирной линией выделена входная последовательность $x = 1010$, которая преобразуется в выходную $y = 1100$.

Бесконечным бинарным деревом задается автомат A , который в зависимости от входного символа может оказаться в одном из двух состояний. Начальным состоянием является $q = 0$. Если на входе автомата окажется $x = 0$, он не меняет своего первоначального состояния $q = 0$, а на выходе появляется $y = 0$. Если на входе $x = 1$, автомат переходит в состояние $q = 1$, а на выходе будет $y = 1$. Оказавшись в состоянии $q = 1$, автомат ведет себя следующим образом: если $x = 0$, то $y = 1$ и $q = 1$; если $x = 1$, то $y = 0$ и $q = 0$.

В общем случае автомат A можно задать четырьмя способами:

1) Один из способов как раз изображен на рис. 3.39, т.е. с помощью достаточного фрагмента бесконечного дерева, вершинами которого являются состояния автомата, а на ребрах указываются входные и выходные символы. Это, очевидно, наиболее громоздкое представление автомата.

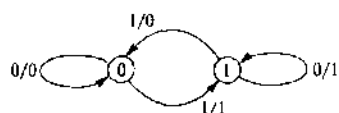


Рис. 3.40

2) Бесконечному дереву отвечает более компактный сильно связанный орграф (рис. 3.40).

3) Аналитическая форма задания автомата осуществляется двумя функциями: функцией переходов $q' = \phi(x, q)$; функцией выходов $y = \psi(x, q)$. Конкретный вид этих функций в нашем случае очень прост — сложение аргументов по mod (2): $q' = x + q$, $y = x + q$. Но, в общем, вместо операции «+» здесь может оказаться любая — дизъюнкция, импликация и т.д.

4) Функции можно задать с помощью таблицы, где в заголовке указываются: по горизонтали — входные символы x , по вертикали — исходные состояния автомата q ; в клетках таблицы на первом месте — новое состояние q' , на втором месте после запятой — выходной символ y . Для нашего примера будем иметь табл. 3.18.

Наш конкретный автомат A обладает одним замечательным свойством: он реагирует на четность числа единиц, поданных на его вход. Пусть в качестве начального состояния будет $q = 0$, в на вход подается бесконечная последовательность x из 0 и 1 (табл. 3.19). Тогда нечетное количество единиц на входе автомата A будет отмечаться единицами на выходе (y_0). Если же в качестве начального со-

стояния выбрать $q = 1$, то нечетное число единиц на входе будет отмечаться уже нулями на выходе (y_1).

Рассмотрим еще один простой пример автомата, когда функция переходов принимает значение входного символа ($q' = x$), а функция выходов — значение состояния ($y = q$). Таблица функций такого автомата представлена табл. 3.20, а реакция на входную последовательность для различных начальных его состояниях — табл. 3.21.

Таблица 3.18

q/x	0	1
0	0, 0	1, 1
1	1, 1	0, 0

Таблица 3.19

x	0 0 1 1 0 1 0 0 0 1 0 1 1 ...
y_0	0 0 1 0 0 1 1 1 1 0 0 1 0 ...
y_1	1 1 0 1 1 0 0 0 0 1 1 0 1 ...

Таблица 3.20

q/x	0	1
0	0, 0	1, 0
1	0, 1	1, 1

Таблица 3.21

x	0 0 1 1 0 1 0 0 0 1 0 1 1 ...
y_0	0 0 0 1 1 0 1 0 0 0 1 0 1 ...
y_1	1 0 0 1 1 0 1 0 0 0 1 0 1 ...

Из табл. 3.21 видно, что автомат на выходе независимо от своего начального состояния просто сдвигает все входные символы на одну позицию вправо. Его называют *автоматом задержки* на один такт. Сильно связанный орграф такого автомата показан на рис. 3.41.

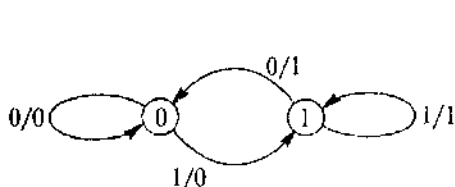


Рис. 3.41

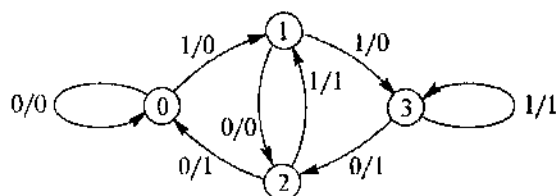


Рис. 3.42

Как видно из рисунка, орграф автомата задержки обладает элементарной группой симметрии относительно перестановки состояний, а также входных и выходных символов 0 и 1. Любопытно построить автомат задержки на два такта: будет ли его орграф обладать симметричными свойствами? Ответ окажется утвердительным (рис. 3.42), хотя число его состояний возрастает до 4, а число дуг — до 8 (табл. 3.22).

Таблица 3.22

q/x	0	1
0	0, 0	1, 0
1	2, 0	3, 0
2	0, 1	1, 1
3	2, 1	3, 1

Автомат задержки на три такта также обладает элементарной симметрией и состоит уже из 8 состояний и 16 дуг (рис. 3.43). Симметрия означает неизменность рисунка при действии на состояния элементарной подстановкой (07)(16)(25)(34) и при одновременной смене входных и выходных символов на противоположные, при этом направление дуг остается прежним, т.е. дуга, идущая из вершины 3 в вершину 7, сохраняет свое направление и после перестановки состояний, но ей присваивается характеристика «вход/выход» 0/1 вместо 1/0 и т.д.

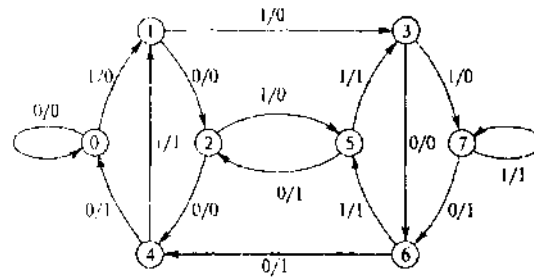


Рис. 3.43

Три последних орграфа являются *эйлеровыми*, так как для них существуют *полные контуры*, включающие все дуги по одному разу. Причиной тому является то, что для каждой вершины число выходящих и входящих дуг четно. Этого факта достаточно, чтобы орграф был эйлеровым. Обход орграфа, изображенного на рис. 3.41, по эйлерову контуру сопровождается выходной последовательностью 0011, если обход начать с петли, или 0110, если сначала идти в вершину 1. Однако это две одинаковых последовательности, сдвинутые на позицию относительно друг друга. Поэтому их принимают за одну и считают, что в этом графе существует только один эйлеров контур. Для орграфа, изображенного на рис. 3.42, существуют два эйлеровых контура с выходными последовательностями 00010111 и 00011101. Наконец, орграф (рис. 3.43) имеет уже 16 эйлеровых обходов; приведем один из них: 0000100101101011.

Если величину задержки обозначить как t , то получим следующие комбинаторные формулы: число вершин в орграфе автомата задержки равно $n = 2^t$; число ребер — $m = 2^{t+1}$; число эйлеровых контуров — $N = 2^n/m$. Три последних орграфа соответствуют значениям $t = 1, 2, 3$. При отсутствии задержки, т.е. при $t = 0$, орграф представлен одной вершиной с двумя петлями — 0/0 и 1/1. Для этого орграфа выполняется одно из важнейших свойств всего ряда автоматов задержки, а именно: для каждой вершины (а здесь она одна) имеются две входящие и две выходящие дуги. Если орграф без задержки ($t = 0$) обозначим как G_0 , а с задержками ($t = 1, 2, 3, \dots$) как G_1, G_2, G_3 и т.д., то в этих обозначениях каждый последующий орграф G_{t+1} является *реберным* по отношению к предыдущему G_t . Условимся орграф G_{t+1} называть *реберным*, если каждой дуге e_j орграфа G_t соответствует вершина q_j в G_{t+1} . Кроме того, если e_1 — дуга орграфа G_t , начало которой есть конец дуги e_0 , то в G_{t+1} имеется дуга q_0 с началом в вершине q_0 и концом в вершине q_1 . Именно при этих условиях из орграфа G_0 путем удвоения числа вершин и дуг получается орграф G_1 ; из G_1 строится G_2 и т.д.

Теперь перейдем от рассмотрения автоматов задержки к другому типу автоматов. До сих пор рассмотренные нами автоматы имели *сильно связанные орграфы*, т.е. эти автоматы могли из любого своего состояния перейти в любое другое, минуя какие то промежуточные. А возможно ли создать автомат, когда ка-

кое-либо состояние становится недостижимым, например, из начального? Да, возможно, в частности, таковым является автомат со следующими функциями переходов и выходов:

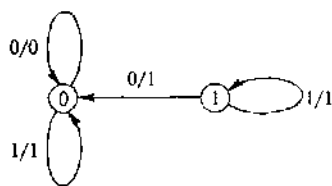


Рис. 3.44

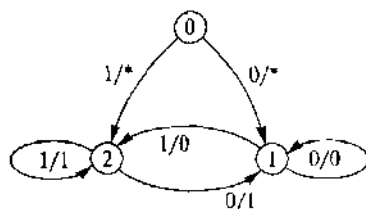


Рис. 3.45

$$q' = x \wedge q, \quad y = x \vee q.$$

Данный автомат описывается просто *связанным* орграфом, для которого вершина 1 является недостижимой из вершины 0 (рис. 3.44).

Существует большая группа автоматов, в частности, *распознавательных*, которые после первого входного символа никогда больше не возвращаются в свое начальное состояние. Элементарным *распознавателем* будет автомат задержки, изображенный на рис. 3.41, если к нему добавить еще одну вершину без входящих в нее дуг (рис. 3.45). Этот автомат распознает четыре типа векторов: 00, 11, 10 и 01. Когда на входе автомата появляется последний символ вектора, на выходе формируется символ 1 или 0: 00 → 0, 11 → 1, 10 → 1, 01 → 0.

Данный автомат можно переделать так, чтобы он распознавал только две последовательности — 11 и 00. Для этого нужно изменить характеристики дуг «вход/выход» 1/0 и 0/1 на 1/* и 0/*. Тогда на выходе получим следующую реакцию на входные векторы: 00 → 0, 11 → 1, 10 → *, 01 → *, что продемонстрировано табл. 3.23.

Таблица 3.23

x	0	0	1	1	0	1	0	0	0	1	0	1	1	0	0	1	0	0	...
y	*	0	*	1	*	*	0	0	*	*	*	1	1	*	0	*	*	0	...

Распознаватель трех единиц (отмечается 1) и трех нулей (отмечается 0) задан табл. 3.24, а графически — с помощью рис. 3.46; на все другие входные последовательности этот автомат реагирует символом «*». Орграф для распознавания четырех единиц и нулей будет состоять уже из семи вершин, но по-прежнему он будет подчиняться симметрии относительно вертикали и в свое начальное состояние $q = 0$ он не возвратится.

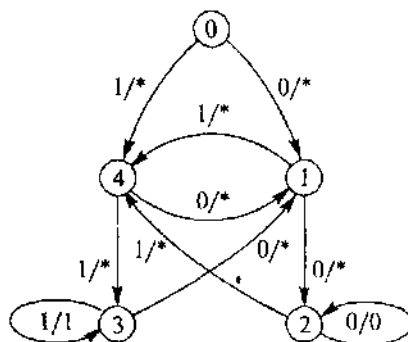


Рис. 3.46

Табл. 3.25 задает распознаватель следующей системы векторов: 000 → 0, 111 → 1, 001 → 1, 110 → 0, на все остальные последовательности из 0 и 1 автомат реагирует «*». Табл. 3.26 определяет автомат для распознавания таких последовательностей: 000 → 0, 111 → 1, 001 → 1, 1100 → 0, 1101 → 1. Имея определенный опыт в проектировании распознавателей, можно создать автомат для регистрации любой последовательности.

Обратимся к синтезу нового класса автоматов — *преобразователей*. Покажем, как можно построить автомат A , который способен преобразовывать одну систему последовательностей в другую:

$$y_i = A(x_i).$$

Таблица 3.24

q/x	0	1
0	1, *	4, *
1	2, *	4, *
2	2, 0	4, *
3	1, *	3, 1
4	1, *	3, *

Таблица 3.25

q/x	0	1
0	1, *	4, *
1	2, *	4, *
2	2, 0	4, 1
3	1, 0	3, 1
4	1, *	3, *

Таблица 3.26

q/x	0	1
0	1, *	4, *
1	2, *	4, *
2	2, 0	4, 1
3	2, *	3, 1
4	1, *	3, *

С этой целью зададимся конкретным списком кодовых векторов — входных x_i и выходных y_i :

$$\begin{aligned} y_1 = A(10) &= 01, & y_4 = A(001) &= 101, & y_7 = A(01001) &= 11110, \\ y_2 = A(000) &= 101, & y_5 = A(011) &= 110, & y_8 = A(11010) &= 01010, \\ y_3 = A(111) &= 011, & y_6 = A(1100) &= 0101, & y_9 = A(110110) &= 010111. \end{aligned}$$

Построение автомата A начнем с вычерчивания бинарного дерева, отвечающего указанным входным и выходным символам (рис. 3.47).

В этом дереве неизвестные пока состояния автомата A обозначены числами, начиная с 0 и кончая 19. Далее руководствуемся следующим правилом: если корень q дерева T_q поместить в вершину q' и при этом реберные характеристики «вход/выход» поддерева $T_{q'}$ целиком совпадут с реберными характеристиками исходного дерева T_q (факт эквивалентности характеристик дуг двух деревьев обозначим как $T_q \approx T_{q'}$), то будем считать состояния q и q' *эквивалентными* ($q \approx q'$). Процедура установления эквивалентных состояний начинаем с корня 0 и далее пойдем согласно нумерации вершин.

Состояния 0, 1 и 2, судя по характеристикам дуг, явно неэквивалентны. Если в вершину 3 поместить корневую вершину 2, то совмещенные дуги рассматриваемых деревьев T_3 и T_2 будут иметь одинаковые характеристики «вход/выход», т.е. $T_3 \approx T_2$, следовательно, состояние $3 \approx 2$. Это обстоятельство автоматически влечет за собой эквивалентность еще двух концевых вершин — $7 \approx 5$, $8 \approx 6$.

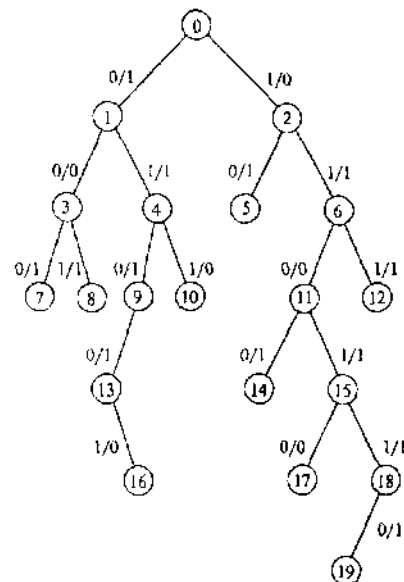


Рис. 3.47

Нелишним будет проверить на конкретных преобразованиях кодовых векторов x в y (табл. 3.28).

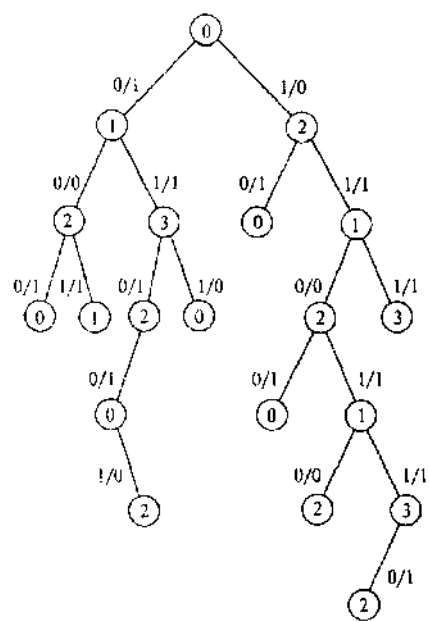


Рис. 3.49

Таблица 3.27

q/x	0	1
0	1, 1	2, 0
1	2, 0	3, 1
2	0, 1	1, 1
3	2, 1	0, 0

Таблица 3.28

x	10	000	111	...	01001	11010	110110
y	01	101	011	...	11110	01010	010111
a	20	123	213	...	13202	21212	212132

В отличие от автоматов-распознавателей, работающих с бесконечной последовательностью символов, автоматы-преобразователи трансформируют конечные кодовые векторы, причем первый символ входного вектора должен поступать тогда, когда автомат находится в начальном состоянии.

Изучим *проблему эквивалентности состояний* автоматов несколько под иным углом зрения. На рис. 3.51а изображен автомат A , внешне сильно отличающийся от автомата A' , изображенного на рис. 3.51б. Между тем их реакции (y) на входные последовательности из 0, 1 и 2 (x) абсолютно одинаковы (табл. 3.29).

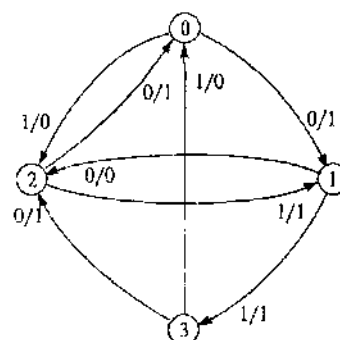


Рис. 3.50

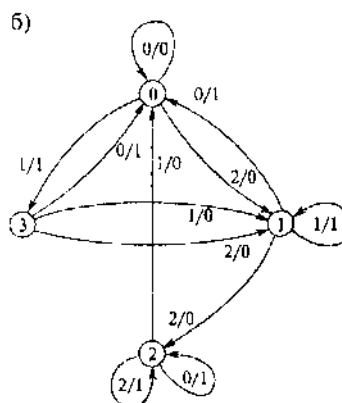
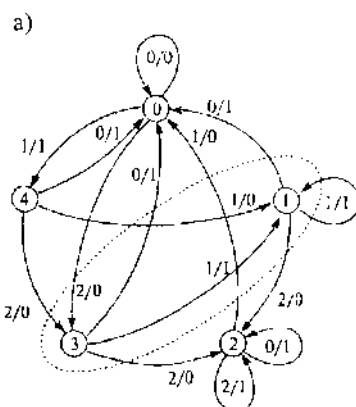


Рис. 3.51

Установить причину такого поведения автоматов помогут таблицы переходов и выходов для A (табл. 3.30) и для A' (табл. 3.31). Из табл. 3.30 видно, что состояния 1 и 3 для автомата A одинаковы. Поэтому строку, отвечающую состоянию 3, из этой таблицы можно просто вычеркнуть, а цифры 3 и 4 заменить на 1 и 3, соответственно. Тогда табл. 3.30 переходит в табл. 3.31, которая представляет переходы и выходы как будто бы совершенно другого автомата A' .

Таблица 3.29

x	0	1	2	2	0	1	1	1	2	1	2	0	1	...
y	0	1	0	0	1	0	1	0	0	0	0	1	1	...
q	0	4	3	2	2	0	4	1	2	0	3	0	4	...
q'	0	3	1	2	2	0	3	1	2	0	1	0	3	...

Таблица 3.30

q/x	0	1	2
0	0, 0	4, 1	3, 0
1	0, 1	1, 1	2, 0
2	2, 1	0, 0	2, 1
3	0, 1	1, 1	2, 0
4	0, 1	1, 0	3, 0

Таблица 3.31

q/x	0	1	2
0	0, 0	3, 1	1, 0
1	0, 1	1, 1	2, 0
2	2, 1	0, 0	2, 1
3	0, 1	1, 0	1, 0

Рассмотрим более сложную ситуацию. Табл. 3.32 задает функции переходов и выходов сложного автомата, принимающего десять различных состояний. Все строки таблицы различны, однако может случиться так, что некоторые из состояний окажутся эквивалентными. Тогда при одинаковом обозначении эквивалентных состояний в таблице появятся и одинаковые строки. Остается только выяснить, какие именно состояния эквивалентны.

Таблица 3.32

q/x	0	1	2	C_i
0	1, 1	0, 1	1, 0	C_0
1	5, 0	3, 1	8, 1	C_1
2	1, 0	6, 0	9, 1	C_2
3	9, 1	6, 1	4, 0	C_0
4	7, 0	3, 0	9, 1	C_2
5	7, 0	8, 0	3, 1	C_2
6	3, 1	9, 1	2, 0	C_0
7	5, 0	6, 1	8, 1	C_1
8	8, 1	0, 1	2, 0	C_0
9	6, 1	3, 1	4, 0	C_0

Прежде разобьем все состояния на *предварительные* классы эквивалентности (C_i), исходя из одинаковости выходных символов (классы C_i проставлены в последнем столбце табл. 3.32). Теперь по отдельности рассмотрим каждый из классов. Для этого пять строк класса C_0 оформим табл. 3.33, в которой вместо выходного символа будем указывать класс эквивалентности состояния.

Таблица 3.33

q/x	0	1	2	C_i
0	1, C_1	0, C_0	1, C_1	C_0
3	9, C_0	6, C_0	4, C_2	C_3
6	3, C_3	3, C_0	2, C_2	C_3
8	8, C_3	0, C_0	2, C_2	C_3
9	6, C_3	3, C_0	4, C_2	C_3

Первая строка табл. 3.33 по принадлежности состояний классам эквивалентности отличается от всех остальных строк. Значит, состояние 0 образует свой собственный класс эквивалентности, за которым мы оставим обозначение C_0 ; состояния же 3, 6, 8 и 9 будут принадлежать другому классу — C_3 (см. последний

столбец табл. 3.33). Согласно новому делению на классы, четыре состояния класса C_3 вновь оформим табл. 3.34, где после каждого переходного состояния укажем его класс. В результате получим отличную от других строку для состояния 8, которое мы отнесем к классу C_4 .

Наконец, табл. 3.35 говорит нам о том, что состояния 3, 6 и 9 действительно эквивалентны, поскольку все состояния, стоящие по строкам, принадлежат одним и тем же классам.

Таблица 3.34

q/x	0	1	2	C_i
3	9, C_3	6, C_3	4, C_2	C_3
6	3, C_3	3, C_3	2, C_2	C_3
8	8, C_3	0, C_0	2, C_2	C_4
9	6, C_3	3, C_3	4, C_2	C_3

Таблица 3.35

q/x	0	1	2	C_i
3	9, C_3	6, C_3	4, C_2	C_3
6	3, C_3	3, C_3	2, C_2	C_3
9	6, C_3	3, C_3	4, C_2	C_3

Переходим к анализу класса C_1 (табл. 3.36). Здесь все строки таблицы по принадлежности переходных состояний классам эквивалентности одинаковые, значит, исходные состояния 1 и 7 принадлежат одному классу эквивалентности.

При рассмотрении табл. 3.37, где выписаны состояния 2, 4 и 5 класса C_2 , обнаруживается неэквивалентное состояние 5, которое образует свой индивидуальный класс C_5 .

Таблица 3.36

q/x	0	1	2	C_i
1	5, C_2	3, C_3	8, C_4	C_1
7	5, C_2	6, C_3	8, C_4	C_1

Таблица 3.37

q/x	0	1	2	C_i
2	1, C_1	6, C_3	9, C_3	C_2
4	7, C_1	3, C_3	9, C_3	C_2
5	7, C_1	8, C_4	3, C_3	C_5

Таким образом, окончательно десять исходных состояний распались на шесть классов эквивалентности:

$$C_0 = \{0\}, C_1 = \{1, 7\}, C_2 = \{2, 4\}, C_3 = \{3, 6, 9\}, C_4 = \{8\}, C_5 = \{5\}.$$

Следовательно, исходная таблица переходов и выходов (табл. 3.32), куда входило десять состояний, может быть сокращена до шести состояний (табл. 3.38), при этом функция автомата по преобразованию входных последовательностей в выходные не меняется. Шесть новых состояний получили свои обозначения от индексов своих классов эквивалентности.

Таблица 3.38

q/x	0	1	2	C_i
0	1, 1	0, 1	1, 0	C_0
1	5, 0	3, 1	4, 1	C_1
2	1, 0	3, 0	3, 1	C_2
3	1, 0	4, 0	3, 1	C_3
4	4, 1	0, 1	2, 0	C_4
5	1, 0	4, 0	3, 1	C_5

При проектировании автоматов могут появиться эквивалентные (лишние) состояния, которые на практике приводят к перерасходу материальных средств. Но зададимся вопросом: какую функциональную нагрузку несет на себе понятие *состояние*? Ведь автомат-преобразователь, который можно назвать автоматом типа «вход — выход — состояние», просто трансформирует входные сообщения (x_i) в выходные (y_i); участие третьей компоненты — состояние (q_i) — здесь не нужно.

Оказывается, понятие состояния возникло в связи с реализацией автоматов на конкретных устройствах — *триггерах*, которые могут находиться в одном из двух состояний — 0 или 1. Автомат с большим числом состояний имеет множество триггеров и их состояния тесным образом увязаны с поступающими на вход и снимаемыми с выхода сигналами. Но вне проблем реализации это понятие излишне. Автомат A считается аналитически заданным, если задан список сообщений: $y_i = A(x_i)$. При графическом же отображении автомата типа «вход — выход» должны фигурировать только входные и выходные символы. Договоримся у дуг писать входные символы, в узлах — выходные. Начальное «состояние» оставим пустым. Тогда списку из девяти слов будет отвечать бинарное дерево (рис. 3.52), напоминающее бинарные деревья, которые мы строили для кодов Фано (3.35) и Хаффмана (3.36). Деревья же Фано и Хаффмана по сути являются автоматами типа «вход».

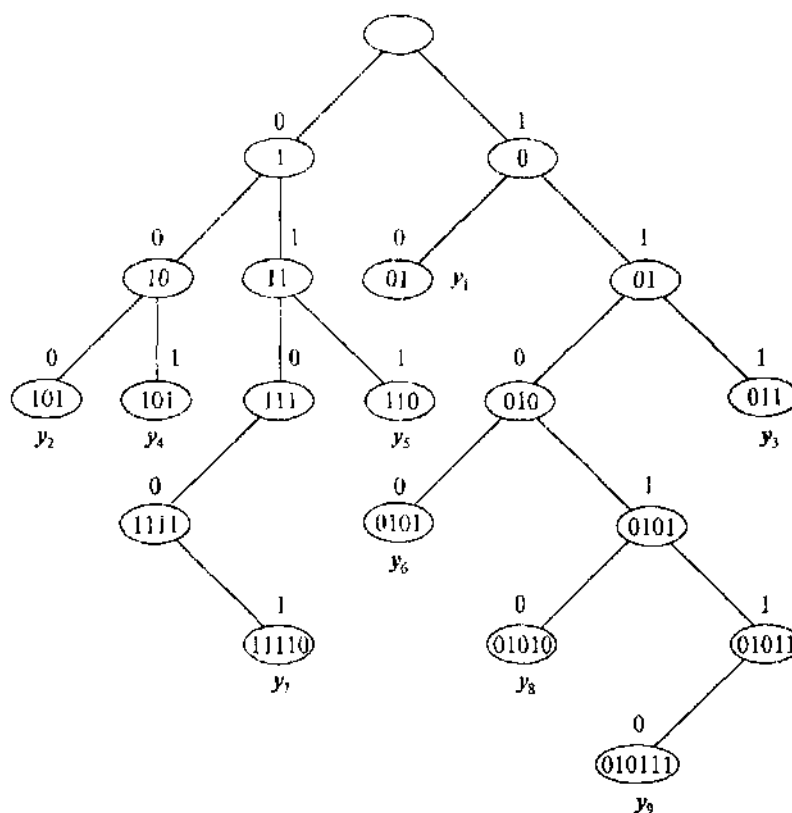


Рис. 3.52

Дерево, изображенное на рис. 3.52, имеет вершины с одинаковым набором символов: 01, 101 и 0101. Такие вершины можно объединять. Однако наибольший эффект от объединения вершин будет тогда, когда сообщения (символы, слова, предложения, события) образуют *замкнутое* множество.

Основным свойством *группы*, как известно, является замкнутость. Автомат «вход — выход», представляющий группу, является сильно связанным орграфом. Табл. 3.39, как часть таблицы перемножения элементов кватерниона (табл. 2.23), является таблицей автомата «вход — выход». В качестве входных сообщений здесь выбраны образующие a и b , а в роли выходных выступают все восемь элементов кватерниона, включая образующие.

Таблица 3.39

q/x	a	b
e	a	b
a	a^2	ab
a^2	a^3	b^3
a^3	e	ba
b	ba	a^2
b^3	ab	e
ab	b	a^3
ba	b^3	a

Табл. 3.39 определяет *симметричную* структуру сильно связанного орграфа (рис. 3.53).

Поставим на место элемента e элемент b . Тогда дуги орграфа сами укажут новый порядок расстановки остальных элементов (рис. 3.54).

Чтобы убедиться в том, что вершины данного орграфа подчиняются группе подстановок кватерниона, нужно вместо тождественного элемента e последовательно подставлять все другие элементы группы, не меняя расположения и характеристик дуг. Для удобства написания подстановок все вершины орграфа

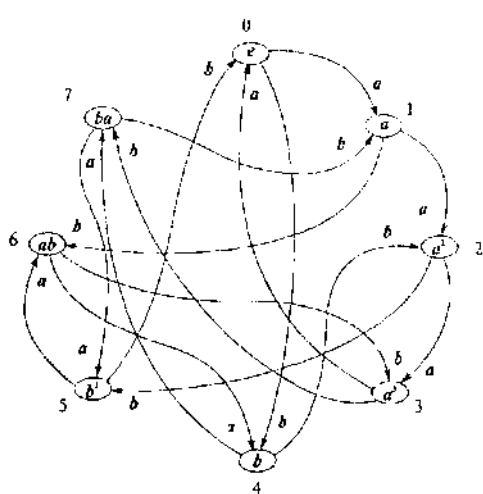


Рис. 3.53

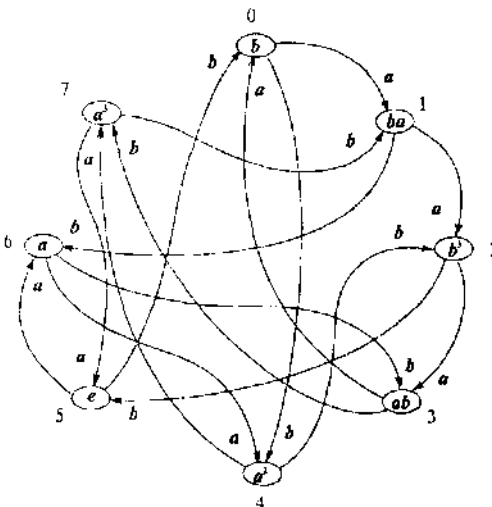


Рис. 3.54

пронумеруем. После расстановки «выходных сообщений» (рис. 3.54) легко записать соответствующую элементу b подстановку. Если вместо e подставить элемент a , получим подстановку еще одной образующей:

$$a = (0123)(4657), \quad b = (0425)(1736).$$

Для каждой группы подстановок можно вычертить свой сильно связанный орграф, который одновременно представляет собой автомат-преобразователь типа «вход — выход». Трудно придумать более наглядную форму графического изображения группы, демонстрирующую ее природу замкнутости. Она совершенно не похожа на те геометрические интерпретации, которые мы давали в разделе «Группы». Действительно, разве есть что-нибудь общее между орграфом, изображенным на рис. 3.55, и изображением тетраэдра или изображением решетки его подгрупп?

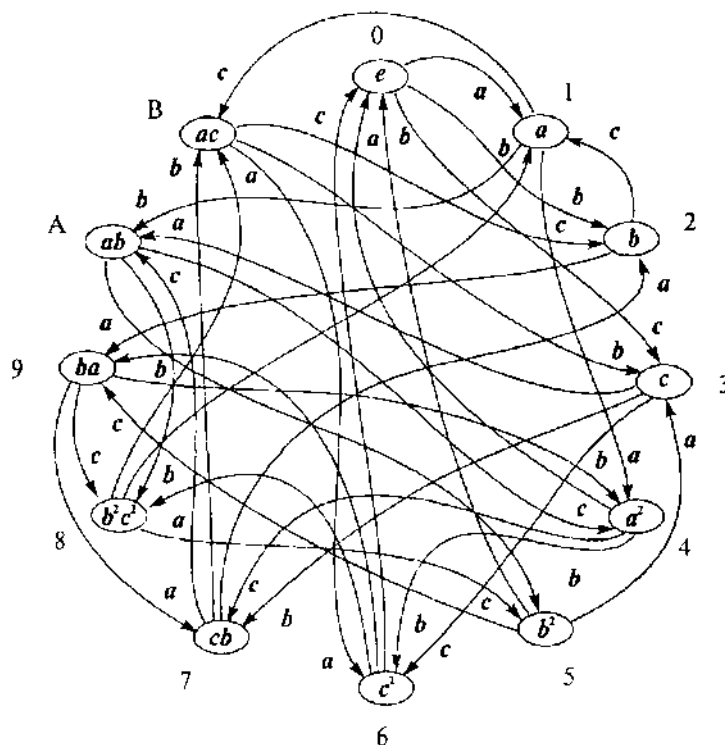


Рис. 3.55

Та легкость, с которой получаются *регулярные* подстановки группы тетраэдра T , записанные с помощью орграфа (рис. 3.55), ставит *автоматное* представление группы T вне конкуренции с ее *геометрическим* и *решетчатым* представлениями. Выпишем регулярные подстановки трех образующих группы тетраэдра T :

$$a = (014)(2A6)(3B7)(589), \quad b = (025)(193)(47A)(6B8), \quad c = (036)(1A8)(279)(45B).$$

Табл. 3.40 является таблицей «вход — выход» для автомата, представляющего группу тетраэдра с тремя «входными сообщениями».

Однако мы хорошо помним, что группу T можно получить и с помощью двух образующих — a, b . Следовательно, существует иная таблица «вход — выход» (табл. 3.41), которой будет отвечать и несколько другой орграф. В последнем случае из каждой вершины будут выходить (и соответственно, входить) не по три, а только по две дуги. Такой орграф можно получить из того, что изображено на рис. 3.55, путем удаления всех дуг с входной характеристикой c .

Таблица 3.40

№	($j \dots$)	q/x	a	b	c
0	(0)	e	a	b	c
1	(012)	a	a^2	ab	ac
2	(123)	b	ba	b^2	a
3	(013)	c	ab	cb	c^2
4	(021)	a^2	e	c^2	cb
5	(132)	b^2	c	e	ba
6	(031)	c^2	b^2c^2	ba	e
7	(023)	cb	b	ac	ab
8	(032)	b^2c^2	ac	a	b^2
9	(01)(23)	ba	cb	a^2	b^2c^2
A	(02)(13)	ab	b^2	b^2c^2	a^2
B	(03)(12)	ac	c^2	c	b

Таблица 3.41

№	($j \dots$)	q/x	a	b
0	(0)	e	a	b
1	(012)	a	a^2	ab
2	(123)	b	ba	b^2
3	(013)	b^2a	ab	ba^2
4	(021)	a^2	e	a^2b
5	(132)	b^2	b^2a	e
6	(031)	a^2b	ab^2	ba
7	(023)	ba^2	b	ab^2a
8	(032)	ab^2	ab^2a	a
9	(01)(23)	ba	ba^2	a^2
A	(02)(13)	ab	b^2	ab^2
B	(03)(12)	ab^2a	a^2b	b^2a

Мы также знаем, что для любой группы по числу образующих имеется нижняя граница, но нет верхней, т.е. количество образующих для кватерниона может быть равно восьми, а для тетраэдра двенадцати. Отсюда автоматные представления кватерниона (рис. 3.53) и тетраэдра (рис. 3.55) далеко не единственны. Вместо *регулярного* орграфа группу может представлять *полный* орграф.

В заключение этого подраздела рассмотрим несколько примеров из теории порождающих грамматик. Возьмем простое предложение:

Маленький мальчик играет в мяч.

Если воспользоваться компьютерным переводчиком Stylus v. 2.5, то получим следующий английский эквивалент:

The small boy plays in a ball.

Но обратный перевод с использованием Stylus по смыслу даст несколько другую фразу:

Маленький мальчик играет в шаре.

Обратимся к формальной стороне дела. Исходную фразу можно представить *порождающим деревом* (рис. 3.56). Ситуация напоминает ту, с которой мы имели дело в разделе «Логика» (п. 1.10), когда составляли ПРОЛОГ-программы. В нашем случае можно обойтись без предикатов, а также вместо записи $y \leftarrow x$ использовать $x \rightarrow y$, которая читается более естественно: « x заменить на y ». Программа:

1) предложение $\Rightarrow$ группа подлежащего, группа сказуемого.

2) группа подлежащего $\Rightarrow$ определение, подлежащее.

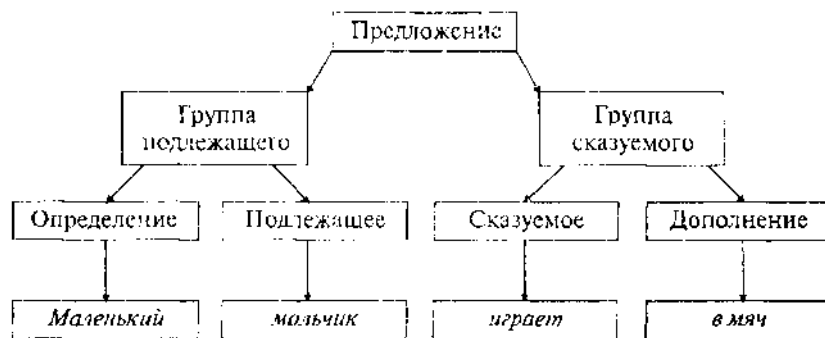


Рис. 3.56

3) группа сказуемого $\Rightarrow$ сказуемое, дополнение.

4) дополнение $\rightarrow$ в мяч.

5) дополнение $\rightarrow$ в шаре.

6) сказуемое $\rightarrow$ играет.

7) подлежащее $\rightarrow$ мальчик.

8) подлежащее $\rightarrow$ мальчика.

9) определение $\rightarrow$ маленький.

10) определение $\rightarrow$ крохотный.

11) определение $\Rightarrow$ низкий.

Система приоритетов Stylus устроена так, что из предложенного набора синонимов были выбраны слова под номерами 5, 7 и 9, вместо 4, 7 и 9; существовали и другие варианты.

Теперь, обобщив приведенный пример, дадим формальное определение *порождающей грамматики*. Порождающей грамматикой G называется семейство четырех множеств:

$$G = \{V, W, S, P\},$$

где V — основной или предметный словарь;

W — вспомогательный или синтаксический словарь;

S — начальное или корневое слово, причем S берется из W ;

P — список логических правил вывода или подстановок.

В предыдущем примере мы имели:

$V = \{\text{крохотный, маленький, низкий, мальчик, мальчика, играет, в шаре, в мяч}\};$

$W = \{\text{предложение, группа подлежащего, группа сказуемого, подлежащее, сказуемое, определение, дополнение}\};$

$S = \text{предложение};$

$P = \{ 1) \text{ предложение} \Rightarrow \text{группа подлежащего, группа сказуемого. ...}$

11) определение $\rightarrow$ низкий\}.

Языком $L(G)$, сформированным под воздействием порождающей грамматики G , называется множество предметных слов V , выведенных из корня S с использованием правил P .

Вернемся к нашему примеру. Если убрать запятые между синтаксическими словами и ввести их в качестве разделителя между правилами, то вышеприведенная программа будет иметь вид:

- 1) $S \Rightarrow AB$, 2) $A \Rightarrow CD$, 3) $B \Rightarrow EF$, 4) $F \rightarrow a$, 5) $F \rightarrow b$, 6) $F \Rightarrow c$,
7) $D \Rightarrow d$, 8) $D \Rightarrow e$, 9) $C \Rightarrow f$, 10) $C \Rightarrow g$, 11) $C \Rightarrow h$.

При этом были введены для синтаксических слов большие латинские буквы, а для предметных — малые. Язык нашего примера ограничен двенадцатью предложениями, которые продиктованы *порождающим автоматом* типа «правило — выход». Граф этого автомата представляет собой дерево. Мы не станем вычерчивать его целиком, а приведем лишь две ветви, одна из которых отвечает возможному ходу вывода предложения «Маленький мальчик играет в мяч» (рис. 3.57а), другая — «Маленький мальчик играет в шаре» (рис. 3.57б).

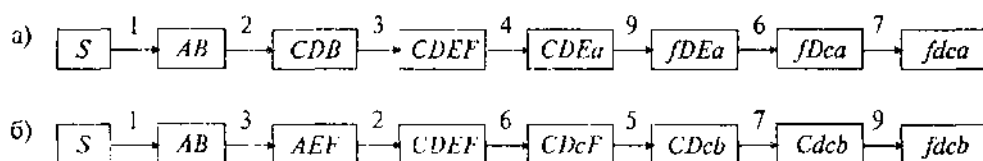


Рис. 3.57

Никаких *входных слов* здесь нет, но есть *выходные предложения* и *правила их вывода*. Дуги автомата снабжены номерами, отвечающими порождающим правилам. Каждая дуга играет роль имплицитной логической связи « $\Rightarrow$ », с помощью которой осуществляется вставка нужного слова. Дерево порождающего автомата — это наиболее приемлемая форма представления процесса формирования грамматических предложений.

С помощью автомата «правило — выход» можно генерировать кодовые слова. Грейбах предложил восемь правил для вывода всевозможных кодовых слов с одинаковым числом 0 и 1:

- 1) $S \Rightarrow 0B$, 3) $A \Rightarrow 0$, 5) $A \Rightarrow 1AA$, 7) $A \Rightarrow 0S$,
2) $S \Rightarrow 1A$, 4) $B \Rightarrow 1$, 6) $B \Rightarrow 0BB$, 8) $B \Rightarrow 1S$.

Здесь по-прежнему большие латинские буквы обозначают вспомогательные переменные, а числа 0 и 1 являются предметными символами. На рис. 3.58 показан вывод двух слов — 011100 и 1001:

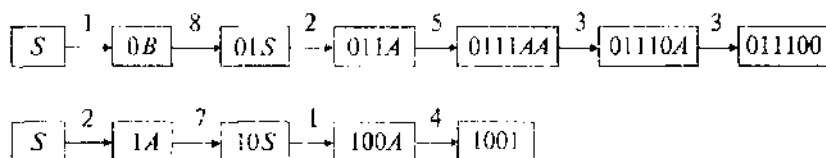


Рис. 3.58

Эти примеры еще раз говорят в пользу того, что граф, подобно тени, следует за объективным процессом, который он представляет. Стоит процедуре чуть измениться, и прежние графические формы, столь хорошо иллюстрирующие взаимосвязь отдельных фаз, вдруг отказываются работать.

Всякий граф есть автомат для получения каких-то выходных сообщений по заданным параметрам. В зависимости от этих исходных параметров нужно выбирать и тип автомата. Если параметрами для выходных сообщений служат только входные символы (кодирование по Фано и Хаффману), удобно использовать граф-автомат, типа «вход»; если каждый входной символ преобразуется в определенный выходной, можно использовать граф-автомат типа «вход — выход» или «вход — выход — состояние»; если в роли входного слова (символа) выступает одно корневое, из которого затем по заданным правилам порождаются выходные сообщения, тогда эффективнее всего использовать граф-автомат типа «правило — выход».

Заключение

Возможные подходы к исследуемому объекту

Небольшой заключительный раздел мы хотели бы посвятить отдельно *конструктивному подходу*, для чего вспомним историю математики, какой она была в Египте четыре тысячи лет назад. Дело в том, что счет древних египтян удивительным образом совпадает с процедурой, осуществляемой современными компьютерами, которые ничего не *доказывают*, а просто *вычисляют* по заданным алгоритмам. Это совпадение требует от нас самого пристального внимания.

Как известно, греки дали миру *аксиоматический метод* и вообще ввели *логику доказательства* математических положений. Римляне перенесли эту культуру ума на социальную почву — так возникло знаменитое *Римское право*. Почему же египтяне пошли по пути *конструирования*? Какая из стратегий более продуктивна — египетская или греческая? Мы свой выбор сделали, осталось убедить читателя выбрать единственно правильный путь.

Нам кажется, что аксиоматическая форма представления знаний консервативна и даже догматична в принципе. Она предполагает незыблемость определенной совокупности положений, на которой выстроена статичная концепция. Сегодняшние конструктивные формы мобильны, чего никак нельзя сказать про вычислительные алгоритмы древних египтян. Но эта консервативность, похоже, типична для древних цивилизаций. Знаменитый магический квадрат 3×3 , для которого сумма чисел по столбцам, строкам и диагоналям равна 15, высеченный на панцире черепахи что-то около пяти тысяч лет назад, благополучно дошел до нас (табл. 1). Но почему после открытия этого квадрата ни один китаец не подумал над аналогичным квадратом 4×4 ? Ведь желание превзойти предшественника является неиссякаемой природой творчества человека. Казалось бы, сегодня все дошедшие до нас панцири должны быть исписаны этими квадратами. Однако мы наблюдаем иную картину, значит, огромный Китай удовлетворился достигнутым. Его больше привлекали трещинки на панцире, чтобы по ним угадывать судьбу, чем поиск математических закономерностей. Сегодня существует компьютерная программа для составления таких квадратов. К счастью, лет десять назад, ваш покорный слуга о ней ничего не слышал и убил два-три дня кряду на составление магического квадрата 10×10 (табл. 2). Ничто так не развивает конструктивное мышление, как решение подобных задач! Читатель может легко убедиться в этом, если возьмется вручную составить магический квадрат 11×11 .

Таблица 1

4	9	2
3	5	7
8	1	6

Таблица 2

71	32	17	83	13	81	24	79	70	29
98	1	84	13	82	20	77	22	99	4
5	96	63	40	54	47	62	37	11	90
95	6	52	43	56	48	60	44	92	9
7	94	49	58	45	53	41	57	13	88
93	8	66	33	55	46	67	36	87	14
12	89	39	64	42	59	38	61	15	86
91	10	34	65	51	50	35	68	85	16
31	72	23	80	25	75	27	73	30	69
2	97	78	21	76	26	74	28	3	100

Графические объекты могут реально существовать, но быть в силу тех или иных причин невидимыми человеком. Актуализация этих математических объектов через их визуализацию не связана с формально-логическими приемами мышления. Больше того, математика и логика в известном смысле противостоят друг другу. Предметом логики является мышление субъекта, которое разворачивается во времени, линейно и последовательно; предметом математики является независимая от мышления структура объекта, которая существует как некая пространственная данность вся целиком. В таком виде математическая структура не может проникнуть в наше сознание и должна быть последовательно деструктурирована. Эта миссия лежит на логике. Можно сказать, что через логику субъекта становится доступна математика объекта.

Математика — это средство описания абстрактных структурных моделей и функциональных зависимостей. Она предоставляет некоторые количественные отношения, выраженные уравнением или тождеством, т.е. определенной формой *эквивалентности*. Мы уже говорили, что при переходе от левой части уравнения к правой не происходит приращения принципиально нового знания: та информация, которая содержится в его левой части, будет содержаться и в правой. Прежде чем вложить информацию в левую часть уравнения, ее нужно увидеть, т.е. она добывается органами зрения, а не говорения. Логический же вывод подчиняется отношению *порядка*, которое соответствует операции импликации типа «если *A*, то *B*». Это отношение тесно связано с причинно-следственным отношением, которое носит объясняющий характер и передается словами: «*A* является достаточным основанием для *B*», «*B*, потому что *A*», «*A* влечет *B*», «*B* при условии выполнения *A*», «из *A* следует *B*» и т.д. Здесь уже «истинная» информация заключения *B* по существу превосходит «истинную» информацию исходной посылки *A*. Нарастание этой информации происходит в процессе рассуждения. Создается впечатление, что мы способны познать мир только усилием мысли. Такая ошибка возникла из-за отсутствия принципиального разграничения между информацией субъекта и объекта теории, т.е. из-за смещения позиций *наблюдателя* (естествоиспытателя, пристально изучающего объект) и *метанаблюдателя* (оторванного от жизни философа), о чем мы говорили в подразделе, посвященном парадоксу лжеца. В действительности же, истинная информация о мире свернута в наших знаках *A* и *B*. Эти две буквы сжигают все мосты между нами и реальным миром вещей. Эфемерное кружево слов, как бы восхитительно оно не блистало, никакого отношения к исследуемым предметам не имеет.

Логика — это наука доказательства, а при доказательстве мы всегда имеем в виду кого-то другого или других: для нас самих доказываемое всегда представляется чем-то очевидным. Таким образом, логика есть убедительное средство передачи информации от нас к другим людям. Значит, логика есть особая языковая форма. Описание объективного мира прежде всего осуществляется посредством обыкновенного языка общения, а затем уже математически. Поэтому логика как таковая выступает в форме *логики высказываний*. Именно эта логика исторически возникла первой в виде *силлогистики* Аристотеля, которая без изменений благополучно просуществовала вплоть до XX века.

В различные периоды истории науки роль логики менялась. Были периоды, когда в ней видели основное средство познания мира. В связи с этим можно вспомнить схоластиков, Гегеля, а из недавнего прошлого позитивистов и марксистов, которые слишком мало обращали внимание на онтологическую картину мира и целиком посвящали себя исследованию исключительно логических и гносеологических проблем. Априорно, только из глубин своего ума они думали черпать новые знания. Между тем, сама логика есть лишь орудие познания реальности, но не сам объективный мир. Под *доказательством* понимают логически обоснованный формализм и, таким образом, «теория доказательства» становится разделом логики, изучающей различного рода суждения или умозаключения. Логика по преимуществу и в главной своей части есть язык рассуждений. В очень малой степени она апеллирует к зрительному образу и реальному предмету: только символы объектов и только действия над этими символами относятся к логике. В доказательствах намеренно используются ригористические языковые средства, создающие впечатление безупречной строгости. Например, вместо слова «равно» употребляется словосочетание «тождественно равно», вместо «тогда, когда...» — «тогда и только тогда, когда...» и т.д. Это похоже на то, как говорят в суде: «клянусь говорить правду и только правду». Зачастую за доказательство принимается некий текст, просто снабженный подзаголовком — «Доказательство». Для некоторых сам этот термин является волшебным.

Между прочим, русское слово «доказать» и близкие к нему по смыслу «указать», «показать», «выказать» образованы от глагола «казать», т.е., по Далю, «давать видеть», «являть» (*Казаная девка олово, неказаная золото*). Другой ряд слов: «сказать», «высказать», «приказать», также образованный от глагола «казать», имеет вторичное значение в славянских языках, смысл которых состоит в «проговаривании» уже *указанной* ситуации. Таким образом, получается, что логика высказываний еще дальше уводит нас от исторических корней термина «доказать», этимология же возвращает нас не только к истории, но и к смысловым глубинам этого понятия. Группы и графы свидетельствуют, что истинное доказательство только-то и связано с непосредственным видением или представлением, но никак не с декларированием слов. Существование математического факта можно считать установленным, если получена соответствующая ему конструкция в виде формул, таблиц и рисунков. Скрытая истина устанавливается на основе открытой истины, некой видимой данности.

Прежде чем реальность будет представлена в виде математических формул, она должна быть описана с помощью модели; именно на основе этих моделей производятся необходимые вычисления. С нашей точки зрения, всю математику, как науку о количественных отношениях и пространственных формах, по-

лезно было бы разделить на две области — *конструктивную* и *доказательную* (последнюю можно называть *логической* или *формальной*). Теорема Ферма убеждает нас, какие порой колоссальные усилия уходят на доказательства индуктивно открытых истин. Строгость, которой кичится математика, часто оборачивается какой-то особой интеллектуальной формой мазохизма, или во всяком случае, некой психической аномальностью. Психология до сих пор является наукой темной, тем не менее обратимся к некоторым ее аспектам, которые, думается, будут не совсем ошибочными.

Представление, как элемент психической деятельности, тяготеет к пространственной, структурной организации, понятие — к временной, функциональной; представления даны нам в основном через зрительные образы, понятия — через словесные определения. Понятия и представления тесно взаимосвязаны: вслед за названным словом в памяти всплывает зрительный образ. Если каналы поступления чувственной информации от внешнего мира полностью блокированы, то представления могут быть столь отчетливы, что, кажется, идут извне, а не изнутри. Так, субъективные события, имеющие место при галлюцинациях и во сне, принимаются за объективные. Однако вещи, данные в представлениях, могут сильно отличаться от вещей, данных непосредственно в ощущениях. Кроме того, не все, что дано в определениях, можно представить образно. Например, вообразить себе остроугольный или тупоугольный треугольник можно, но треугольник вообще — нельзя, хотя определение его существует. В процессе познания вещи часть знаний приходится на понятия об этой вещи (функциональные элементы), а часть — на представления о ней (структурные элементы).

Есть люди, которые воспринимают мир в основном через дефиниции (определения) и символы. В дефинициях фигурирует преимущественно то, что установлено в опыте. У других больше развито образное мышление, при котором каждое явление не просто обозначается, а воссоздается по существу, то есть имитируется. Здесь имеется множество искусственно введенных пространственных элементов — конструктов. Отсюда возникают и два вида научных концепций — *феноменологический* и *конструктивный*. При феноменологическом методе отход от зарегистрированных в опыте данных минимален, всякое теоретизирование воспринимается неохотно, результаты представляются в виде законов, которые выражены в функциональных зависимостях, куда должны входить только экспериментально найденные параметры. Конструктивисты, напротив, апеллируют в основном к имитационным моделям, без которых, как они считают, не может быть полноценной теории. Предложенные ими математические выражения обычно получены из их искусственных моделей, поэтому в них часто входят параметры абстрактных моделей, а не экспериментально измеренные. Типичными феноменалистами были Аристотель, Оствальд, Эйнштейн, а типичными конструктивистами — Демокрит, Френель, Максвелл.

Такая классификация хороша в естествознании, но не в математике, хотя математический конструктивизм ничем особенным не отличается от естественно-научного и этим он нас привлекает. Все же в математике существует иное деление, а именно: на *конструктивистов* и *формалистов*. В этой науке, как принято считать, не может быть феноменологического подхода, поскольку получается, что все ее «феномены» взяты из головы. Математик всегда, как модно сейчас го-

ворить, имеет дело с виртуальной реальностью. Поэтому те, кто склонен мыслить феноменологически, кажется, должны будут перебежать в стан конструктивистов, а те, кто был бы в естествознании конструктивистом, встанут в стройные ряды формалистов. Кому, как не любителям искусственных построений реальности, заняться убедительными логическими схемами доказательств. Однако в жизни дело обстоит ровно наоборот. Максвелл со своими многочисленными моделями эфира — лучший претендент на роль лидера в лагере математиков-конструктивистов, а знаменитый Эйнштейн со своей теорией относительности мог бы возглавить огромный в нынешние времена отряд математиков-формалистов. Почему так, а не иначе?

Дело все в том, что Максвелла интересовала объективная реальность, а для Эйнштейна справедлива жизненная формула прагматичного позитивиста: уравнение работает, значит оно верно. Если эфир нас в чем-то не устраивает, долой его, обойдемся и без него. А то, что электромагнитным волнам без светоносной среды негде распространяться, никого не должно волновать. Главное, чтобы в данный момент, на данном участке науки дела шли успешно. Сегодня из всех книг и учебников исчез вывод знаменитых четырех уравнений Максвелла. А ведь он целиком опирался на механические модели эфира, которые возникли на базе бесчисленных, тщательно записанных протоколов электромагнитных опытов Фарадея. Кто об этом сейчас помнит и кому нужен этот вывод? Всем важно, чтобы формула работала. Сейчас нас спрашивают: «Уравнения Эйнштейна удовлетворяют непосредственно наблюдаемым фактам?». И мы дружно отвечаем: «Да, конечно!». «Чего же вы хотите?». Нам кажется, что фактор времени здесь вновь дает о себе знать. Феноменалисты всегда спешат выдать готовую формулу. Классическая физика создавалась медленно, в течение нескольких столетий. Нынешняя же радикальная трансформация естествознания протекла почти мгновенно, в течение одного-двух десятков лет.

Не станем углубляться в спор между конструктивистами и феноменалистами, работающими в области естествознания — это длинная песня. Заметим лишь, что начался он еще в античные времена между теми, кто отстаивал теорию атома, связанную с пространственной моделью строения вещества, и теми, кто придерживался качественного взгляда на мир, кто ощущал теплоту, холод, влажность и сухость, т.е. придерживался теории четырех элементов. Учение Аристотеля о четырех свойствах материи в Средние века, превратившись в алхимию и схоластику, захватило все плацдармы легальной науки, атомистика же Демокрита и Архимеда ушла в подполье или осталась на ее задворках. В Новое время об атомах вспомнили и конструктивный дух, возрожденный Коперником, Галилеем, Кеплером и Ньютоном, снова стал господствующим в науке. Однако к началу XX века он угас во второй раз, феноменалисты вновь стали править балом. Ныне физика лежит на боку, ее основной вес в естествознании незначительный, все заняты биологией, а точнее, геной инженерией.

В чем же состоят главные аргументы формалистов от математики, к которым прежде всего нужно отнести Давида Гильберта? Они хотели превратить всю математику в единую систему символов, за которыми не было бы никакого содержания. Реальный мир всегда мешал формалистам, и они всячески пытались избавиться от него. Мечтая об идеальной логической оболочке, они стремились исключить любые противоречия, коих в жизни, конечно, немало. Всеобщность

и универсальность также является характерной чертой их доктрин. Формалисты никогда не устраивали какие-то там конкретные математические объекты, они хватались за «основания математики». И абстрактная, оторванная от реальности символика позволяла создать видимость больших достижений в этом придуманном ими мире.

Формалисты критикуют конструктивизм за то, что можно было бы назвать *естественнонаучной компонентой математического знания*. Они ни на минуту не хотят покидать почву формальной логики. Обращение к содержательной стороне дела рассматривается ими как преступление. Эта содержательная компонента, разумеется, всегда разрушает созданную ими логическую связанность. Но когда конструктивист берется за строительство того или иного объекта, формалист предупреждает, что действия его противоречат «основаниям математики». Такая их критика может быть подтверждена следующими знаменательными словами¹:

Характерной особенностью формальной аксиоматики — в отличие от содержательной — является необходимость *установления ее непротиворечивости*. Между тем содержательная аксиоматика вводит свои понятия со ссылкой на имеющийся у нас опыт, а свои основные положения либо считает очевидными фактами, в которых можно непосредственно убедиться, либо формулирует их как итог определенного опыта и тем самым выражает нашу уверенность в том, что нам удалось напасть на след законов природы, а заодно и наше намерение подкрепить эту уверенность успехом развиваемой теории.

Формалисты презрительно относятся к конструктивистам, рассматривая содержательный аспект реального мира как вынужденное «дополнение». Тем самым они походят на безгрешных ангелов, для которых материальная плоть может лишь обременять их идеальное существование. Формалисты исповедуют принцип «отброшенной лестницы», которую, однажды использовав для подъема наверх, можно затем отбросить за ненадобностью. Эта жизненная позиция чувствуется в следующих словах²:

Формальная аксиоматика по необходимости нуждается в содержательной как в своем дополнении, поскольку именно эта последняя поначалу руководит нами в процессе выбора соответствующего формализма, а затем, когда формальная теория уже имеется в нашем распоряжении, она подсказывает нам, как эта теория должна быть применена к рассматриваемой области действительности.

Похоже, амбиции формалистов выходят далеко за пределы традиционной области математики. Эти слобы гнушаются анализировать не только конкретные объекты, с которыми имели дело Ньютон, Эйлер, Лагранж, Даламбер и Гаусс, но считают ниже своего достоинства опускаться до арифметики и алгебры³:

Осуществленное нами рассмотрение начал арифметики и алгебры было предпринято с целью продемонстрировать, как на практике применяются и используются прямые содержательные рассуждения, совершающиеся в виде мысленных экспериментов над наглядно представимыми объектами и не зависящие от предположений аксиоматического характера.

¹ Д. Гильберт, П. Бернайс. Основания математики. — М.: Наука, 1979 с. 24.

² Там же, с. 25.

³ Там же, с. 59.

Людям, далеким от всякой математики, например философам, очень нравятся «глобальные» рассуждения формалистов. Их приводит в умиление положение о том, что число точек на линии равно числу точек на плоскости или в объеме. Теорией Кантора, говорят они, нельзя забивать гвозди, но она восхитительна. Мы же, напротив, не склонны доверять теориям, которые опираются только на манипуляцию символами, и прежде всего, символами, обозначающими бесконечность. Впрочем, символы могут быть разными.

И *понятия*, и *представления* выражаются через определенные системы символов. Но для символов представлений важны пространственные характеристики (форма, размеры, композиционные соотношения) — только в этом случае геометрия форм образует адекватную модель. Например, важно, чтобы электроны обозначались шарами (а не эллипсоидами или кубами), однородное магнитное поле — параллельными силовыми линиями определенной плотности, орбиты планет — правильными эллипсами, зонные структуры полупроводников должны иметь конкретную ширину и очередность. Символы, отражающие понятия, должны быть компактны, легко узнаваемы и без труда воспроизводимы. Так, символами служат слова обыкновенного языка общения, специальные научные термины, многочисленные математические символы, обозначения химических элементов. Неразвитая символика сдерживает любой научно-познавательный процесс. Из истории науки хорошо известно, что введение специальной символики позволило Лагранжу и Гильберту значительно продвинуть вперед геометрическую, а значит исключительно конструктивную, механику Ньютона.

Однако символ в науке не должен существовать совершенно обособленно от соответствующей пространственно-временной формы. Манипуляция слишком специализированными терминами или иностранными словами приводит только к путанице. Хорошо изученные объекты имеют отчетливую функциональную и структурную форму. Таковыми являются гелиоцентрическая модель Солнечной системы, оболочечная структура атома, капельная модель экситонной жидкости, сферический кристалл фуллерена, периодическая таблица Менделеева, классификация живых организмов, клетка органической материи, структура молекулы ДНК, схема геологической периодизации истории Земли и многое другое.

Строго дедуктивные умозаключения противны духу творчества, поскольку они зачастую разрушительно действуют на процессы синтетического мышления; новое знание появляется часто вопреки логике, в результате некой благоприятной мутации. На уровне идеи математическая структура чаще всего возникает в нашем сознании помимо логики и даже вопреки ей, когда многие необходимые звенья для правильного вывода отсутствуют. Затем уже этой *индивидуальной* идее сообщается общезначимая логическая форма, чтобы она могла быть воспринята *коллективным* сознанием. Конструктивная идеология прекрасно изложена в книге Джорджа Пойа «Математика и правдоподобные рассуждения» (М., 1975), которую бы мы настоятельно рекомендовали читателю. Не станем пересказывать ее содержание, напомним, что наша книга в какой-то мере, пусть в самой незначительной, дополнит ее. После этого вступления к нашему Заключению, перейдем, наконец, к египтянам.

Итак, мы сказали, что египтяне *вычисляли* истины, а не *доказывали* их. Первое, к чему они пришли, были дроби, наиболее распространенные среди них — $1/2, 1/3, 1/4, 1/6, 2/3, 3/4, 4/5$. Дробными величинами измерялись длины, площади, объемы, веса, периоды времени, музыкальные интервалы и пр. Дошедший до нас папирус Ринда, датированный примерно 2000 г. до Р.Х., начинается с так называемой *канонической таблицы* представления дробей вида $2/n$ суммой дробей вида $1/k$ (табл. 3). В ней указаны нечетные знаменатели дроби вида $2/n$, изменяющиеся от 3 до 101, и два, три или четыре знаменателя дроби вида $1/k$. Приведем примеры разложения дробей $2/n$ на сумму дробей $1/k$:

$$\begin{aligned} 2/3 &= 1/2 + 1/6, \quad 2/5 = 1/3 + 1/15, \quad 2/7 = 1/4 + 1/28, \dots, \\ 2/13 &= 1/8 + 1/52 + 1/104, \quad 2/15 = 1/10 + 1/30, \dots, \\ 2/101 &= 1/101 + 1/202 + 1/303 + 1/606. \end{aligned}$$

Таблица 3

n	k	n	k	n	k
3	2, 6	37	24, 111, 296	71	40, 568, 710
5	3, 15	39	26, 78	73	60, 219, 292, 365
7	4, 28	41	24, 246, 328	75	50, 150
9	6, 18	43	42, 86, 129, 301	77	44, 308
11	6, 66	45	30, 90	79	60, 237, 316, 790
13	8, 52, 104	47	30, 141, 470	81	54, 162
15	10, 30	49	28, 196	83	60, 332, 415, 498
17	12, 51, 68	51	34, 102	85	51, 255
19	12, 76, 114	53	30, 318, 795	87	58, 174
21	14, 42	55	30, 330	89	60, 356, 534, 890
23	12, 276	57	38, 114	91	70, 130
25	15, 75	59	36, 236, 531	93	62, 186
27	18, 54	61	40, 244, 488, 610	95	60, 380, 570
29	24, 58, 174, 282	63	42, 126	97	56, 679, 776
31	20, 124, 155	65	39, 195	99	66, 198
33	22, 66	67	40, 335, 536	101	101, 202, 303, 606
35	30, 42	69	46, 138		

Далее в папирусе Ринда приводятся условия и решения свыше 80 различных задач; при решении некоторых из них египтяне использовали данные разложения. Однако почему из бесчисленного множества разложений дроби $2/n$ на сумму дробей вида $1/k$ приведены именно эти, сказать трудно. Например, легко доказать, что любая дробь $2/n$ разлагается на две компоненты вида $1/k$:

$$\frac{2}{n} = \frac{1}{(n+1)/2} + \frac{1}{n(n+1)/2}.$$

В частности, первые три разложения удовлетворяют этой формуле. Но зачем понадобилось менять эту процедуру для других 46 значений n (исключение составляет еще дробь с $n = 23$), непонятно.

Больше того, каноническое разложение, которым египтяне пользовались на протяжении многих веков, вдруг в какое-то время подвергалось изменениям. Например, существует глиняная табличка, относящаяся примерно к раннему периоду Нового царства (1500 год до Р.Х.), в которой уже вместо двучленного разложения дроби $2/7$ использовалось трехчленное:

$$2/7 = 1/6 + 1/14 + 1/21.$$

Все это очень трудно объяснить, хотя недостатка в гипотезах мы сегодня не испытываем.

Что представляют собой эти задачи? Немало из них относятся к типу «аха». Последнее слово можно переводить как «куча» или «множество», т.е. то неизвестное количество, которое необходимо найти и которое мы, люди 2000 года, обозначаем как x . Вот, например, как выглядят условие и решение задачи № 26: «Аха и ее четвертая часть вместе дают 15». Далее древнеегипетский писец папируса Ринда предлагал алгоритм решения: «Считай с 4; от них ты должен взять четверть, а именно — 1; вместе — 5». Затем нужно было произвести еще два действия: деление — $15/5 = 3$ и умножение — $3 \cdot 4 = 12$. Таким образом, находилась неизвестная «аха», т.е. $x = 12$.

Сегодня эту задачу мы решали бы путем составления уравнения и решения его относительно x :

$$x + (1/4) \cdot x = (5/4) \cdot x = 15, \quad x = (15/5) \cdot 4 = 3 \cdot 4 = 12.$$

Древний же египтянин использовал так называемый метод «ложного положения», которым пользовались и европейские математики в Средние века. Здесь положение x занимает некоторое число 4, от которого легко подсчитывается четвертая часть. Вместо 4 можно было бы взять, скажем, 8. Тогда четвертая часть равнялась бы 2, что в сумме с 8 давало бы 10. Но результат, предложенный данным алгоритмом, окажется тем же, т.е. $x = (15/10) \cdot 8 = 12$.

Приведем задачу из Московского папируса, который так же, как и папирус Ринда, написан в эпоху Среднего царства, но в котором число задач в четыре раза меньше, чем в папирусе, хранящимся в Лондоне, т.е. свыше 20 штук (кстати, размеры папирусов также отличаются примерно в 4 раза: папирус Ринда имеет площадь $525 \times 33 \text{ см}^2$, а Московский — $544 \times 8 \text{ см}^2$).

Итак, задача № 19 из папируса, находящегося в Пушкинском музее в Москве:

1 плюс 1/2 аха вместе с 4 дают 10. Что есть аха? Подсчитай число, на которое 10 превышает 4. Получишь 6. Сколько раз надо взять 1 + 1/2, чтобы получить 1? Это число равно 2/3. Возьми 2/3 от 6. Получишь 4. Ответ найден верно.

В данном случае древнеегипетский математик решал уравнение $x + (1/2) \cdot x + 4 = 10$ примерно так же, как это сделали бы мы сегодня, т.е. без всякого «ложного положения»:

$$(3/2) \cdot x = 10 - 4 = 6, \quad x = 6 \cdot (2/3) = 4.$$

Задача № 32 папируса Ринда демонстрирует алгоритм перемножения двух чисел, а именно: $12 \cdot 12$, который практически ничем не отличается от алгоритма, используемого в компьютерах, поскольку основывается он на представлении чисел в двоичной системе счисления. Алгоритм оформлен в виде табл. 4, в левой части которой он представлен на языке древнеегипетских иероглифов, в правой же части записан арабскими цифрами.

Древнеегипетские иероглифы читаются справа налево, причем символ I означает единицу, O — 10, S — 100; «РЕЗУЛЬТАТ» изображался в виде свернутого папируса с печатью наверху. Правая часть таблицы является зеркальным отображением левой с той только разницей, что все иероглифы переведены на современный язык. Первый множитель составлялся из определенного набора степеней 2; в данном случае — $12 = 4 + 8 = 2^2 + 2^3$ (цифры 4 и 8 писец отмечал косой черточкой в виде апострофа). Второй столбец чисел начинался со значения второго множителя, который у нас равен тоже 12. Последующие числа получаются путем удвоения предыдущих. Результат находится как сумма чисел второго столбца, взятых из отмеченных апострофом строк, т.е. $144 = 48 + 96$.

Таблица 4

2000 год до Р.Х.		2000 год после Р.Х.	
II O	I	1	12
IIII O O	II	2	24
IIII O O	IIII	4	48
IIII O O			
II O O O O O	IIII	8	96
II O O O O	IIII		
		РЕЗУЛЬТАТ	
IIII O O O O S		144	

Забота о воспитании и обучении молодых людей в Древнем Египте лежала на жрецах. Знания — это сила и власть. Вполне естественно, что жреческая каста не слишком стремилась к просвещению широких масс населения, ибо, в противном случае, при рабовладельческом укладе жизни возникла бы опасность потери управления в обществе. Поэтому многие знания передавались из «уст в уши» без какой-либо записи на материальных носителях. Если последние и использовались, то только для фиксации трудно запоминаемой информации, как в случае с каноническим разложением дробей вида $2/n$. Это мы говорим к тому, что в папирусе Ринда есть иероглифический текст, который трудно назвать задачей. Непосвященному сложно было догадаться, о чем, собственно, идет речь. Но мы, просвещенные люди, живущие в открытом обществе, легко понимаем суть дела. Итак, расшифровка иероглифов даст следующий набор слов и чисел:

« Лестница

Дом	7
Кошка	49
Мышь	343
Колос	2401
Зерно	16807

1	2801
2	5602
4	11204

Вместе 19607 »

Здесь речь идет о сумме пяти членов геометрической прогрессии:

$$7 + 7^2 + 7^3 + 7^4 + 7^5 = 19607.$$

Египетский жрец геометрическую прогрессию обозначил иероглифом «лестница». Устный текст для этой задачи мог бы звучать приблизительно так:

Представьте себе улицу, где стоят семь домов. В каждом доме проживает по семь кошек. Каждая кошка съедает по семь мышей. Каждая мышь съедает по семь колосков. На каждом колоске находится по семь зерен. Требуется определить размер «кучи».

В папирусе приводятся все пять степеней семерки, три промежуточных и одна окончательная суммы. Посвященный в тайны арифметического счета должен был уметь составлять таблицы типа табл. 5, в которой все очень хорошо видно: в последней строке приведены степени числа 7, в последнем столбце — промежуточные и окончательные суммы; используемый алгоритм счета тот же самый, что и в задаче № 32, т.е. бинарный.

Таблица 5

1	7	49	343	2401	2801
2	14	98	686	4802	5602
4	28	196	1372	9604	11204
7	49	343	2401	16807	19607

Мы говорили в определении науки математики, помимо количественных отношений, еще и о пространственных формах. В самом деле, *пространственным формам* математики во все времена и во всех странах уделяли самое пристальное внимание. Посмотрим, как эта сторона дела освещалась в древнеегипетских папирусах. Но прежде заметим, что в Древнем Египте различалось три вида письма. В Древнем царстве (3000–2000 гг. до Р.Х.) использовалось *иероглифическое письмо*. Писцов тогда было немного и все надписи они тщательно прорисовывали. Набор художественных картинок передавал содержание примерно так же, как в наше время комиксы. В Среднем царстве (2000–1500 гг. до Р.Х.) было уже распространено так называемое *иератическое письмо*, при котором детально прорисованные иероглифические изображения заменялись на упрощенные эскизы. Сами же иероглифы использовались только в особо торжественных случаях, например, они наносились на крышки саркофагов усопших важных персон. В Новом царстве (1500–1000 гг. до Р.Х.) плоды просвещения дали о себе знать. Огромная масса не слишком старательных писцов пользовалась уже *демотическим письмом*, при котором стилизованное иератическое письмо заменялось на еще более упрощенную скорописную символику.

И.И. Перепелкин выполнил иероглифический перевод содержания задачи № 14 Московского папируса, написанный иератическим письмом. Эта задача включала в себя схематический рисунок (рис. 1), позволяющий нам сориентироваться в отношении того, каким образом древнеегипетские математики обращались с пространственными формами. Содержание задачи сводится к примеру вычисления объема (*V*) усеченной пирамиды с квадратным основанием, когда высота (*h*) и стороны нижнего (*a*) и верхнего (*b*) квадратов заданы в конкретных числах. Его можно передать следующими словами:

Если тебе дана пирамида без вершины в 6 локтей в высоту, в 4 локтя по нижней стороне и в 2 локтя по верхней стороне, то вычисления начни с нижней стороны, которую возведи в квадрат; получишь 16; затем умножь 4 на 2; получишь 8; далее возьми 2 и возведи в квадрат; получишь 4; сложи вместе три числа — 16, 8 и 4; получишь 28; возьми треть от 6; получишь 2; перемножь это 2 с числом 28; получишь 56. Ты нашел верно.

Как видим, автор этого алгоритма рекомендует нам последовательно придерживаться школьной формулы вычисления, а именно:

$$V = (a^2 + a \cdot b + b^2) \cdot h / 3. \quad (1)$$

Схема (рис. 1), которой была снабжена задача, в лаконичной форме дублировала подробный алгоритмический текст задачи.

Напомним, что все записанные на ней числа и действия с ними нужно прочитывать справа налево. На схеме, помимо известного нам иероглифа «результат», имеются еще два — «шагающие ноги», призванного символизировать математические действия сложения и возведения в квадрат (что также сводится к сложению; иероглиф «шагающие ноги» можно было бы передать английским словом «go», который на русский язык может переводиться не только как «иди», но и более широко как «начинай действовать»), и «рот, откусывающий часть от целого» (в нашем случае «откусывается» треть от шести, т.е. двойка).

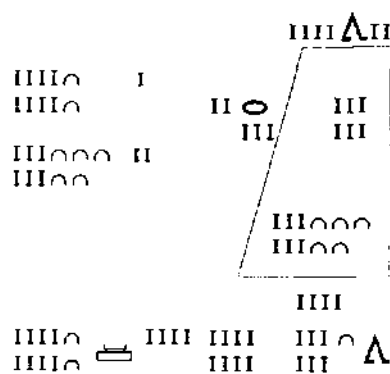


Рис. 1

Самое первое стоящее над пирамидой число указывает сторону верхнего сечения и тут же оно возводится в квадрат (возможно, автор желал тем самым показать, что рассматривается именно объемная фигура, а не плоская трапеция, как это может показаться на первый взгляд). Под нижним основанием пирамиды стоит четверка, указывающая сторону еще одного квадрата. Внутри пирамиды написаны два числа: первое 6, которое указывает высоту пирамиды, второе 56 — объем пирамиды. На одной строке с 6 автор записал математическое действие — «откусывание одной трети от шести» — и тут же помещен результат этого действия — 2. Слева от изображения пирамиды записано бинарное перемножение двух чисел — $28 \cdot 2 = 56$. В самом низу рисунка показано, как получается число 28; оно получается путем сложения 16, 8 и 4.

В изложенной задаче прежде всего поражает формула (1), по которой следует алгоритм решения. Если отбросить экзотические предположения, связанные, например, с посещением страны древних пирамид инопланетными пришельцами, которые могли бы подсказать формулу, то всякий историк науки обязан попытаться воспроизвести ход мысли древних математиков. Понятно, что без моделирования пространственными формами выражение (1) не получить.

Существуют два варианта рассуждений. Первый основывается на том факте, что в Московском папирусе как будто бы изображена прямоугольная усеченная пирамида. В этом случае можно произвести ее разрез на четыре части, как это

показано на рис. 2а, высчитать объем каждой части и затем произвести сложение. Результирующая формула будет иметь вид:

$$V = b^2 h + b(a - b) \cdot h + (a - b)^2 h / 3. \quad (2)$$

Здесь нужно заметить, что формула для объема пирамиды общего вида была известна, видимо, с очень древних времен. Этот объем равен одной трети от произведения площади основания пирамиды на ее высоту. Во всяком случае, ее несложно найти эмпирическим путем, как это сделал, в частности, Демокрит. Он составлял из «атомов», т.е. маленьких кубиков,

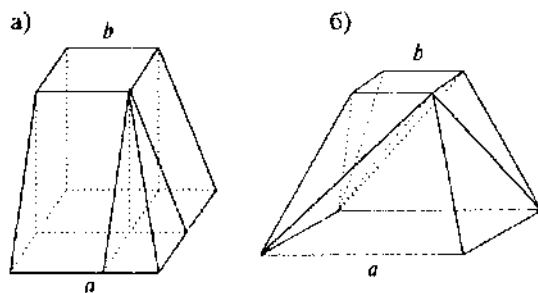


Рис. 2

сначала пирамиду, а потом из тех же самых «атомов» и на том же самом основании прямую призму, которая всегда оказывалась на две трети ниже высоты пирамиды. Аналогичным методом пользовался Архимед, когда он подсчитывал площади криволинейных геометрических фигур: он их взвешивал, помещал в ванны с водой и по произведенным физическим действиям судил о геометрических свойствах этих фигур.

Поэтому последнее слагаемое в выражении (2) не вызывает вопросов. Но они тут же появятся, если данное выражение сравнить с выражением (1). Почему алгоритм рассматриваемой задачи из папируса не выстроен сразу по формуле (2)? Ведь невозможно себе представить, чтобы древнеегипетские математики могли произвести сложные алгебраические преобразования от формулы (2) к формуле (1). Они оперировали только конкретными числами и ни о каких буквенных преобразованиях не могли и подумать (хотя бы потому, что тогда не было самого алфавита).

Более правдоподобным вариантом рассуждения древних кажется второй. Усеченную пирамиду, выделенную, например, из сырой глины (причем обязательно прямоугольной формы), можно было бы разрезать, как это показано на рис. 2б. Тогда формула объема, выраженная через сумму ее составляющих, будет выглядеть уже несколько ближе к алгоритмической формуле (1):

$$V = a^2 h / 3 + b^2 h / 3 + 2(a \cdot h / 2) \cdot b / 3. \quad (3)$$

Многовековое обращение с конкретными числами не могло не привести внимательного человека к мысли о справедливости коммутативного и дистрибутивного законов:

$$a \cdot b = b \cdot a, \quad a \cdot d + b \cdot d + c \cdot d = (a + b + c) \cdot d.$$

Это значит, что путь от формулы (3) к формуле (1) существовал и он носил явно конструктивный характер: без манипуляции пространственными образами здесь не обошлось. Египетских жрецов не заботили доказательства, они думали только о вычислении подтверждаемого практикой результата. Какова принципиальная разница между ними?

Для раскрытия природы доказательства и исчисления обратимся сначала к школьной формуле:

$$(a + b)^2 = a^2 + 2ab + b^2.$$

Она имеет по крайней мере два сильно различающихся обоснования:

а) *символьное* — $(a + b)^2 = (a + b)(a + b) = a^2 + ab + ba + b^2$.

б) *образное* — смотри рис. 3!

В символьном доказательстве формулы квадратичного бинома многое подразумевается и не все прописывается в явном виде. В самом деле, действия над буквами a и b не столь очевидны, как это может показаться с первого взгляда. В частности, требуется еще обосновать, что квадрат скобки равен произведению двух скобок и что скобки перемножаются так, как это показано; что ab равно ba и что сумма $ab + ab$ может быть представлена как $2ab$. Однако мы отлично знаем, что под буквами a и b подразумеваются некие числа, которые, как показал многотысячелетний опыт человечества, подчиняются всем упомянутым правилам.

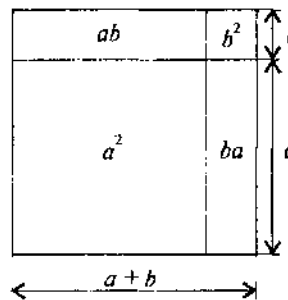


Рис. 3

Наше символьное доказательство есть не что иное, как сокращенная форма записи исчисления чисел. Для какого-нибудь инопланетянина запись $(3 + 4)^2 = 3^2 + 2 \cdot 3 \cdot 4 + 4^2$ выглядят совершенно одинаково по сравнению с предыдущей, хотя в первом случае под a и b мы подразумеваем абстрактные символы, принимающие любые числовые значения, во втором — конкретные числа. Впрочем, конкретность символов 3 и 4 относительна, так как они, в свою очередь, являются довольно сильным абстрактным нововведением по сравнению с более древней записью этих же самых математических объектов — III и IV. Таким образом, формула квадратичного бинома в действительности представляет собой свернутый в плотную символьную упаковку наш долгий индуктивный опыт работы со счетными объектами.

Тот же жизненный опыт по измерению площадей земельных участков привел нас к геометрической форме доказательства выражения для квадратичного бинома. Возможно, какой-нибудь дотошный формалист заявит нам, что мы своим рис. 3 не представили никакого доказательства. Он потребует введения таких понятий как *конгруэнтность*, т.е. совместимость геометрических фигур при их перемещении в пространстве, а также специальных определений примерно такого типа: *прямая линия не имеет толщины*. В противном случае, скажет он, мы не сможем убедить читателя в том, что при наложении четырех фигур, обозначенных как a^2 , b^2 , ab и ba , на квадрат $(a + b)^2$ не произойдет пересечений в местах наложения линий. Это будет означать, в свою очередь, что левая часть рассматриваемого выражения не равна правой. На что какой-нибудь нижегородский крестьянин резонно заметит: «Да неужто ячменные поля двигать можно?» — И будет прав, так как нет в существе своем разницы между доказательствами равенства, скажем, двух прямоугольников ab и ba , т.е. коммутативности величин a и b , путем совмещения фигур или путем сбора одинакового урожая ячменя с двух указанных полей. В обоих случаях мы имеем дело с человеческим опытом, отлитым в различные жизненные формы.

Графическое доказательство (б) несколько не хуже символического (а). Какие символы мы введем, какую словесную дорожку протопчем к заветной формуле — не столь уж важно. Можно просто указать пальцем на рисунок — «Вот!», или сказать: «Смотри рис. 3!», т.е. сделать нечто, что привлечет внимание всякого желающего знать, как можно развернуть квадратичный бином, на некий объект, для которого указанная формула справедлива. Как нам удастся донести ее читателям: будет ли это интересно и убедительно, или же скучно и путано, — вещь второстепенная. Разумеется, хорошо, если это сделано грамотно, общепризнанными методами и хуже, когда формула сваливается на нас как бы с потолка. Но нет более неприятной ситуации, чем иметь дело со схоластикой, при которой не существует никакой объективной реальности, а есть лишь спекуляция на искусственно введенных символах и дефинициях.

В подтверждение сказанному о приоритете объекта, представляющего данное символическое выражение, над субъективными средствами его доказательства продолжим наш пример в сторону увеличения степени бинома. Для кубического бинома —

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

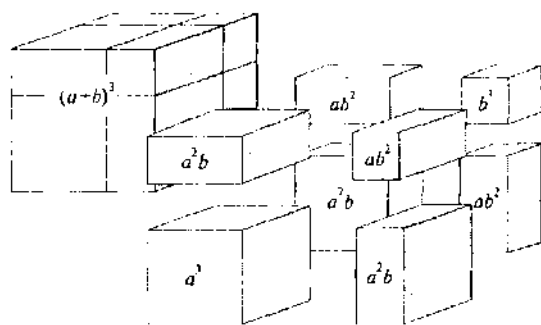


Рис. 4

также имеются две формы обоснования; образная показана на рис. 4.

Для тетрабинома, в силу своеобразия восприятия человеком физического пространства, графический объект пропадает, хотя символический вывод формулы продолжает существовать. Нижеследующая формула безупречно отражает действия с числами.

$$(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.$$

Возникшую ситуацию можно сравнить с восприятием человеком электромагнитных или звуковых колебаний. Глаз или ухо улавливают их в узких диапазонах. Если колебания выходят за пределы этих диапазонов, человек перестает воспринимать их. Всякая раскраска в цветные тона ультрафиолетового или инфракрасного излучения будет субъективна и ложна, располагай мы при этом миллионами цветовых оттенков.

Но не видеть математический объект человек может не только из-за своих *физических* ограничений. До Пифагора греки не подозревали о существовании несоизмеримых отрезков, что равносильно восприятию ими только рациональных чисел. Затем, за счет введения иррациональностей, диапазон чисел расширился, но сфера построения геометрических рисунков оставалась ограниченной инструментами — циркулем и линейкой. Декарт снял эти ограничения, и математическому анализу подверглись новые графические объекты — циклоида, астроида, кардиоида и пр. Хотя и в античной геометрии использовался инструмент под названием конхоидограф, сконструированный Никомедом (250—150 гг. до Р.Х.)

для решения задачи о делении произвольного угла на три равные части («задача трисекции угла»). Конхоиду Никомеда нельзя было вычертить с помощью циркуля и линейки, однако анализ ее в античное время являлся скорее исключением, чем правилом. В XIX веке числовая шкала, благодаря введению трансцендентных и мнимых чисел, еще расширилась. Комплексное число и кватернион так же, как и понятия о рациональности, иррациональности, трансцендентности, связаны с геометрическими образами. Сегодня мы можем говорить совершенно об экзотических числах; с некоторыми из них мы уже познакомились. Но вернемся к нашим баранам.

Вывод формул разложения квадратичного и кубического биномов — и символичный, и геометрический — относится к конструктивному виду. Их трудно отнести к полноценным формам *доказательства*, поскольку в них практически отсутствует логика в том ее понимании, о котором здесь говорилось. Такого рода получение знания мы называем *исчислением*. В основе всякого исчисления, естественно, лежит процедура счета, которая в применении к более сложным математическим объектам, чем натуральный ряд чисел, трансформируется в специальные алгоритмы. В качестве объектов реальности могут выступать отдельные предложения и целые тексты. В этом случае мы будем иметь дело с *исчислением высказываний*, т.е., собственно, с *математикой*. Если высказывания перестают быть предметом исследования и становятся инструментом субъекта теории, то мы имеем дело с *логикой* как таковой.

В математических доказательствах логика и исчисление присутствуют в различных пропорциях; их, порой, трудно отделить друг от друга. В одном случае все доказательство может состоять из одноактового представления объекта, как мы уже знаем на примере рис. 3 и рис. 4. В других случаях, доказательство выстраивается в форме некоторой совокупности суждений, которая направлена не на получение *количественного* результата, а в сторону установления факта *существования* того или иного объекта или обнаружения логического *противоречия*. В двух нижеприведенных доказательствах присутствует именно такая организация вывода.

Первый пример взят из далекого прошлого. Рассмотрим, каким образом пифагорейцы доказывали иррациональность числа $\sqrt{2}$, т.е. устанавливали факт невозможности его рационального соотношения с единицей.

Пусть, рассуждали они, имеет место пропорция:

$$1 : \sqrt{2} = a : b.$$

Тогда $b^2 = 2 \cdot a^2$. Отсюда видно, что b^2 четно. Четный квадрат может дать только четное основание, значит, b четно. Предположим, что $b = 2 \cdot c$. Из исходной пропорции и четности числа b вытекает нечетность числа a . Но подставим последнее равенство в предыдущее: $4 \cdot c^2 = 2 \cdot a^2$ или $a^2 = 2 \cdot c^2$, т.е. a — четно. Возникло противоречие: целое число может быть либо четным, либо нечетным. Таким образом, число $\sqrt{2}$ иррационально.

Второе доказательство относится к нашим дням. Оно взято из книги Драгина А.Г. «Математический интуиционизм. Введение в теорию доказательств» (М., 1979, с. 15–16).

Теорема. Существуют два иррациональных действительных числа a и b такие, что a^b рационально.

Доказательство. Рассмотрим число $\sqrt{2}^{\sqrt{2}}$. Если это число рационально, то теорема доказана: достаточно положить $a = \sqrt{2}$, $b = \sqrt{2}$. Если же $\sqrt{2}^{\sqrt{2}}$ иррационально, то нужные a и b вновь можно найти: достаточно взять $a = \sqrt{2}^{\sqrt{2}}$ и $b = \sqrt{2}$. В этом случае $a^b = 2$. Таким образом, при любых обстоятельствах нужные a и b существуют.

Обращаем внимание на то, что во втором доказательстве отсутствует попытка установления факта рациональности или иррациональности чисел a и b . Перед нами типичное логическое доказательство на существование. В первом же доказательстве процедура исчисления присутствует несколько в большей степени, чем во втором.

Сильно ошибаются те, кто думает, что с помощью формально-логического вывода можно добыть принципиально новые знания. Мы уже говорили, что логические доказательства нужны математикам скорее для убеждения коллег в своей правоте. В среде математиков существует негласное правило: приступай к поиску доказательства только после того, как убедился в истинности предложения. Это очень здравый совет. Аксиомы, леммы и теоремы — все равно, что юридические нормы, регулирующие отношения людей в обществе: они должны быть завершенными, непротиворечивыми, лаконичными и общепризнанными, чтобы не вызывать путаницы. Если же вы хотите проникнуть в реальный мир математики и познать объективную красоту формул, лучше воспользоваться эффективными вычислительными процедурами.

Чтобы лучше усвоить эту важную мысль, докажем несколькими способами следующее элементарное равенство:

$$1 + 2 + 3 + \dots + n = n(n + 1)/2. \quad (4)$$

Доказательство 1 (по индукции).

Формула (4) верна, если она верна для $n = 1$, $n = k$, $n = k + 1$. Для первых двух значений n имеем

$$1 = 1 \cdot (1 + 1)/2, \quad 1 + 2 + 3 + \dots + k = k \cdot (k + 1)/2.$$

К левой и правой частям последнего равенства прибавим член ряда $(k + 1)$:

$$1 + 2 + 3 + \dots + k + (k + 1) = k \cdot (k + 1)/2 + (k + 1).$$

Правую часть нетрудно представить в виде

$$(k + 1)(k + 2)/2,$$

что соответствует формуле (4) при третьем значении n . Теперь у нас появилась уверенность в том, что эта формула будет работать при любых целых значениях n . Однако мы остались в полном неведении относительно того, откуда взялась формула.

Очень легко устанавливается, что сумма нечетных чисел равна квадрату числа слагаемых:

$$1 + 3 + 5 + \dots + (2n - 1) = n^2. \quad (5)$$

Действительно, последовательно увеличивая длину суммируемого ряда, мы быстро улавливаем закономерность:

$$1^2 = 1^2, \quad 1 + 3 = 4 = 2^2, \quad 1 + 3 + 5 = 9 = 3^2, \quad 1 + 3 + 5 + 7 = 16 = 4^2, \dots$$

Сравнительно просто находится формула для суммы кубов натурального ряда:

$$1^3 + 2^3 + 3^3 + \dots + n^3 = [n(n+1)/2]^2. \quad (6)$$

Она вытекает из следующих сумм:

$$1^3 = 1^2, \quad 1^3 + 2^3 = 9 = 3^2, \quad 1^3 + 2^3 + 3^3 = 36 = 6^2, \\ 1^3 + 2^3 + 3^3 + 4^3 = 100 = 10^2, \dots$$

Но попробуйте подобрать формулу для суммы квадратов натурального ряда —

$$1^2 = 1, \quad 1^2 + 2^2 = 5, \quad 1^2 + 2^2 + 3^2 = 14, \\ 1^2 + 2^2 + 3^2 + 4^2 = 30, \quad 1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 55, \dots$$

Это сделать уже не просто. Поэтому ценны именно те математические методы, которые не только *подтверждают*, но и *выводят* формулу.

Доказательство 2 (для суммы арифметической прогрессии).

Операция сложения подчиняется коммутативному закону. Сложение членов ряда произведем парами, элементы которых равноудалены от концов ряда. Пусть число элементов в ряду будет сначала четным, т.е. $n = 2k$, тогда

$$1 + 2 + 3 + \dots + (2k-2) + (2k-1) + 2k = \\ = [1 + 2k] + [2 + (2k-1)] + [3 + (2k-2)] + \dots + [k + (2k - (k-1))] = \\ = [1 + 2k] + [1 + 2k] + [1 + 2k] + \dots + [1 + 2k] = [1 + 2k]k = n(n+1)/2.$$

Пусть число элементов в ряду нечетно, $n = 2k + 1$, тогда

$$1 + 2 + 3 + \dots + k + (k+1) + (k+2) + \dots + (2k-1) + 2k + (2k+1) = \\ = [1 + (2k+1)] + [2 + 2k] + [3 + (2k-1)] + \dots + [k + (k+2)] + (k+1) = \\ = [2 + 2k] + [2 + 2k] + [2 + 2k] + \dots + [2 + 2k] + (k+1) = \\ = [2 + 2k]k + (k+1) = (k+1)(2k+1).$$

При $k = (n-1)/2$ получим $n(n-1)/2$.

Подобное доказательство справедливо для всех рядов $a_1, a_2, a_3, \dots, a_n$ вида

$$a_1, \quad a_1 + d, \quad a_1 + 2d, \dots, \quad a_1 + (n-1)d,$$

которые называются *арифметическими прогрессиями*. Разность (d) и первый член (a_1) арифметической прогрессии могут быть любыми действительными числами, но число элементов в ряду по-прежнему равно либо четному, либо нечетному целому. Поэтому суммы пар равноудаленных элементов, равные $2a_1 + (n-1)d$, нужно рассматривать для четного и нечетного числа n . В обоих случаях результат сводится к формуле:

$$\sum_{i=1}^n a_i = (a_1 + a_n)n/2. \quad (7)$$

Формула (7) переходит в формулу (4) при подстановке $a_1 = 1$ и $a_n = n$.

Последнюю формулу легко понять, если понимается следующий факт:

$$(a_1 + a_n)/2 = (a_2 + a_{n-1})/2 = (a_3 + a_{n-2})/2 = \dots = (a_{n/2} + a_{n-n/2})/2,$$

т.е. среднее арифметическое двух равноудаленных от концов ряда элементов всегда равно одному и тому же числу — *центру арифметической прогрессии*. Если число элементов прогрессии нечетно ($n = 2k + 1$), то центр арифметической про-

грессии совпадает с центральным членом ряда (a_{k+1}); если число элементов четно ($n = 2k$), то центр равен среднеарифметическому двух срединных элементов $(a_k + a_{k+1})/2$. В частности, для нечетного $n = 5$ имеем

$$1 + 2 + 3 + 4 + 5 = (1 + 5)5/2 = 15;$$

центр арифметической прогрессии приходится на элемент 3: $(1 + 5)/2 = (2 + 4)/2 = 3$. Для четного $n = 6$ имеем

$$1 + 2 + 3 + 4 + 5 + 6 = (1 + 6)6/2 = 21;$$

центр равен

$$(1 + 6)/2 = (2 + 5)/2 = (3 + 4)/2 = 3,5.$$

Таким образом, второе доказательство дало нам больше, чем мы рассчитывали: мы не только подтвердили и вывели формулу (4), но и нашли существенно более общую формулу (7). Так, если нам дана арифметическая прогрессия с параметрами: $a_1 = -2,54$, $d = 0,127$, $n = 57$, то, воспользовавшись формулой (4), можно без труда подсчитать сумму (S) всех ее 57 элементов:

$$\begin{aligned} S &= \sum_{i=1}^n a_i = (a_1 + a_n)n/2 = [2a_1 + (n-1)d]n/2 = \\ &= [2 \cdot (-2,54) + 56 \cdot 0,127] \cdot 57/2 = 57,912. \end{aligned}$$

Несколько иной взгляд на сумму S приходит к нам, если члены арифметической прогрессии расположить по следующей схеме:

$$\begin{array}{cccccc} & & & & d & \dots \\ & & & & d & d \\ & & & d & d & d \\ & & d & d & d & d \\ d & d & d & d & d & \dots \\ a_1 & a_1 & a_1 & a_1 & a_1 & \dots \end{array}$$

Тогда S можно представить как сумму двух составляющих S_1 и S_2 :

$$S = S_1 + S_2 = 57,912.$$

$$S_1 = n \cdot a_1 = 57 \cdot (-2,54) = -144,78,$$

$$S_2 = n \cdot (n-1) \cdot d/2 = 57 \cdot 56 \cdot 0,127 = 202,692.$$

Здесь для подсчета второй составляющей (S_2) используется формула (4).

Доказательство 3 (связанное с биномиальным разложением).

В биномиальное разложение $(x+1)^2 = 1 + 2x + x^2$ или $(x+1)^2 - x^2 = 1 + 2x$ вместо x поочередно будем подставлять числа 1, 2, 3, ..., n . В результате получим следующую систему равенств:

$$\begin{aligned} 2^2 - 1^2 &= 1 + 2 \cdot 1, \\ 3^2 - 2^2 &= 1 + 2 \cdot 2, \\ 4^2 - 3^2 &= 1 + 2 \cdot 3, \\ &\dots \\ (n+1)^2 - n^2 &= 1 + 2 \cdot n. \end{aligned}$$

Произведем сложение правых и левых частей этих равенств, получим выражение:

$$(n+1)^2 - 1 = n + 2 \cdot (1 + 2 + 3 + \dots + n).$$

После очевидных преобразований приходим к (4).

Данную методику вывода можно распространить на сумму квадратов, кубов и более высоких степеней чисел натурального ряда. В самом деле, возьмем кубический бином:

$$(x+1)^3 - x^3 = 1 + 3x + 3x^2.$$

Поочередно присвоим x числа $1, 2, 3, \dots, n$, а затем, производя те же самые операции, что и в предыдущем случае, найдем ранее найденную формулу для суммы квадратов натурального ряда:

$$\begin{aligned} (n+1)^3 - 1 &= n + 3 \cdot n(n+1)/2 + 3 \cdot (1^2 + 2^2 + \dots + n^2); \\ 1^2 + 2^2 + \dots + n^2 &= n^3/3 + n^2/2 + n/6 = n \cdot (n+1) \cdot (2n+1)/6. \end{aligned} \quad (8)$$

Используя тетрабином $(x+1)^4$, находим (6) и т.д.

При доказательстве формулы (4) необязательно ограничиваться только символической манипуляцией. Ниже рассматриваются еще три способа доказательства, где существенную роль играют операции с графическими объектами.

Доказательство 4 (связанное с представлением целых чисел геометрическими точками).

Поставим каждому целому числу натурального ряда соответствующую совокупность точек на плоскости. Тогда сумма числовых рядов представит перед нашим взором в виде некоторого множества точек, образующих треугольник (рис. 5).

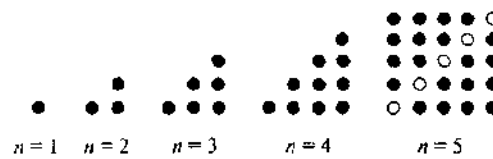


Рис. 5

На рис. 5 для случая $n=5$ показано, каким образом можно было бы подсчитать число точек в треугольнике. Для этого необходимо произвести следующие алгоритмические операции:

- 1) подсчитать число точек в квадрате: $n \cdot n$;
- 2) вычесть из полученного числа точки, стоящие на диагонали: $n \cdot n - n = n \cdot (n-1)$;
- 3) результат разделить пополам: $n \cdot (n-1)/2$;
- 4) к последнему числу прибавить ранее вычитенные диагональные точки: $n \cdot (n-1)/2 + n = n \cdot (n+1)/2$.

Однако с помощью точек трудно вывести следующую формулу для сумм, т.е. формулу суммы сумм:

$$1 + 3 + 6 + 10 + \dots + n \cdot (n+1)/2 = n \cdot (n+1) \cdot (n+2)/6. \quad (9)$$

Подставляя в формулу (9) $n=1, 2, 3, 4, \dots$, будем получать числа — 1, 4, 10, 20, ..., которые можно проиллюстрировать точками в пространстве, а именно, пирамидами (рис. 6). Но вывести непосредственно из рисунка правую часть формулы (9), оставаясь в пределах разумного числа алгоритмических процедур, практически невозможно.

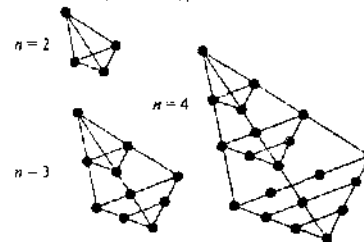


Рис. 6

Доказательство 5 (связанное с вычислением площади под прямой $y = x$).

На рис. 7 изображены координатные оси и прямая $y = x$. На прямой возьмем точку M и от нее на обе оси проведем перпендикуляры MM_x и MM_y . Отрезки OM_x и OM_y поделим на n частей, при этом длину каждой части примем за a , так что

$$OM_x = OM_y = na.$$

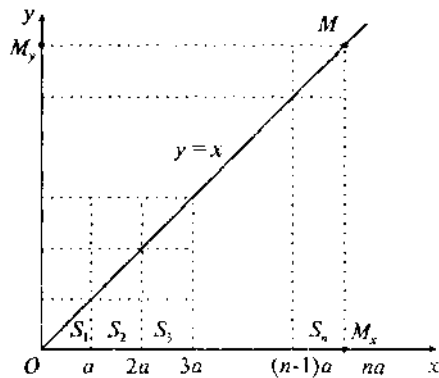


Рис. 7

Наконец, избавившись от a^2 , находим формулу (4):

$$1 + 2 + 3 + \dots + n = n^2/2 + n/2 = n(n+1)/2.$$

Кажется, что эту методику можно было бы распространить на параболу $y = x^2$ (рис. 8) с целью выведения формулы (8).

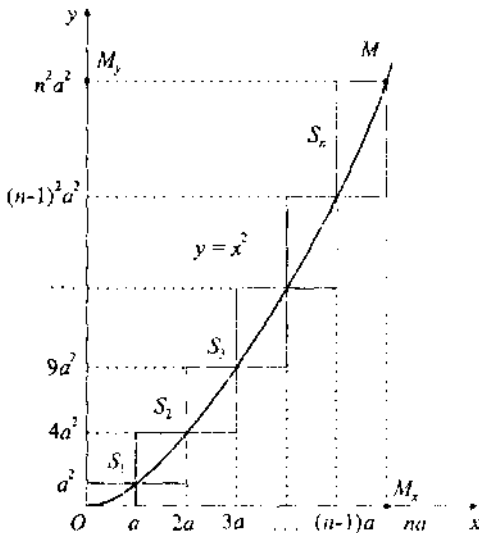


Рис. 8

Но этого не удастся сделать. Площадь под параболой, как известно из интегрального исчисления, равна одной трети площади прямоугольника OM_yMM_x , т.е. $n^3a^3/3$. Чтобы ее вычислить, напротив, требуется именно знать формулу (8), но никак не наоборот.

С помощью рис. 8 удастся еще вывести формулу (5) для линейного ряда чисел. Действительно, площадь прямоугольников S_i равна:

$$S_1 = a^3, \quad S_2 = 3a^3, \quad S_3 = 5a^3, \quad \dots, \\ S_n = (2n - 1)a^3.$$

Если затемненные прямоугольники составить один под другим, получится крайняя правая вертикальная полоса, площадь которой равна:

$$\sum_{i=1}^n S_i = a^3 + 3a^3 + 5a^3 + \dots + (2n - 1)a^3 = n^2a^3.$$

Избавившись в этом выражении от a^3 , можно найти формулу (5). Таким образом, сфера расширения методики вывода здесь, как и в предыдущем случае, оказывается весьма ограниченной.

Доказательство 6 (связанное с представлением о полном графе).

Каждое ребро графа соединяет две точки, но любая вершина графа может быть инцидентна нескольким ребрам. В связи с этим вводят понятие о *валентности* или *степени* связанности данной вершины с другими вершинами. Понятно, что на каждое ребро приходится по две валентности. Поэтому число ребер равно половине суммы степеней всех вершин:

$$m = \frac{1}{2} \sum_{i=1}^n d(i), \quad (10)$$

где m — число ребер, n — число вершин, $d(i)$ — валентность i -ой вершины.

Формула (10) вытекает непосредственно из геометрического образа графа и только что введенных понятий. Произвольно вычерченный граф (рис. 9) подчиняется этому соотношению:

$$14 = (2 + 5 + 6 + 3 + 4 + 3 + 5)/2.$$

Граф называется *полным*, если каждая его вершина связана ребрами со всеми остальными вершинами. На рис. 10 представлены первые четыре полных графа G_n .

Для полных графов формулу (10) можно упростить, заменив сумму произведением двух величин: числа вершин (n) и валентностью одной из вершин ($d = n - 1$):

$$m = nd/2 = n(n - 1)/2.$$

Так, для последнего графа G_5 , изображенного на рис. 10, число ребер равно $10 = 5 \cdot 4/2$; для следующего графа G_6 будем иметь $15 = 6 \cdot 5/2$ и т.д.

Переходя от вершины к вершине и последовательно вычеркивая ребро за ребром, как показано на рис. 10, мы можем подсчитать число m иначе, а именно как сумму чисел от 1 до $n - 1$. Например, для G_5 получим $10 = 1 + 2 + 3 + 4$, для $G_6 = 15 = 1 + 2 + 3 + 4 + 5$ и т.д. Отсюда возникает система равенств: $5 \cdot 4/2 = 1 + 2 + 3 + 4$, $6 \cdot 5/2 = 1 + 2 + 3 + 4 + 5$ и т.д., которая при обобщении порождает формулу (4), записанную не для n слагаемых, а для $n - 1$:

$$1 + 2 + 3 + \dots + (n - 1) = n(n - 1)/2,$$

что, однако, не меняет ее сущности.

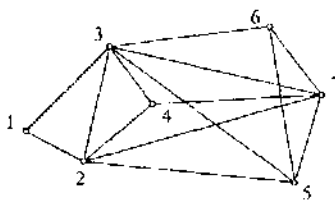


Рис. 9

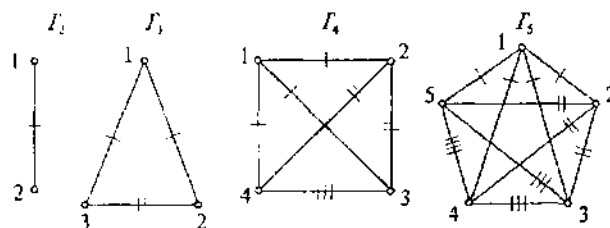


Рис. 10

Итак, мы рассмотрели шесть различных способов доказательства справедливости одной и той же достаточно элементарной формулы. Какие же выводы в связи с этим можно было бы сделать?

Во-первых, нет никаких оснований считать какой-либо вывод более строгим, более убедительным или более исчерпывающим. В математике, как и в юриспруденции, ни одно из доказательств не имеет преимущественного значения. Они все имеют равное право на существование: вывод формулы (4) с помощью графических образов (точек, площадей или ребер графа) ничем не хуже вывода этой формулы на основе чисто символьных процедур на основе представлений об арифметической прогрессии или биноме.

Однако, и это во-вторых, графические способы вывода не имеют продолжения. Они ограничиваются доказательством данной конкретной формулы. Их методики не экстраполируются на другие подобные случаи. Графические образы позволяют «видеть» элементарные формулы (4) и (5), но они не дают «увидеть» чуть более сложные формулы (8) и (9). Тем не менее, особо подчеркнем, не нужно пренебрегать пространственными объектами, коль скоро их удастся привлечь к анализу той или иной математической ситуации, поскольку рисунки сообщают абстрактным знаниям ту степень *репрезентативности*, которая как нельзя лучше способствует их усвоению.

В юриспруденции в качестве аргументов могут выступать показания свидетелей и вещественные улики. В математике графические образы можно отнести по юридической терминологии к вещественным, т.е. к аргументам прямого действия.

Основная же наша мысль состоит в третьем выводе, который вытекает из представленных здесь доказательств формулы (4). Задумаемся, а почему, собственно, символьные доказательства (второе и третье) оказались столь эффективны? Вышло так, что аналитическая методика обоснования формулы (4) оказалась значительно ценнее самой формулы, поскольку она дала ключ к открытию новых формул. Не потому ли, что ряды различных арифметических прогрессий и ряды от разворачивания биномов различной степени сами задают определенного рода *регулярные процедуры*, подчиняющиеся простой алгоритмизации. Отсюда напрашивается еще более эффективная методика продуцирования новых формул, при которой числовые ряды (если речь идет о них) возникают не от случая к случаю, а путем направленного *конструирования*. Такой конструктивизм приведет нас к методу *исчисления* рядов, когда истинность формулы устанавливается ее единственным атрибутом — местом в бесконечном ряду подобных формул. Это избавляет нас от громоздкой процедуры ее специального обоснования логическими методами.

Рассмотрим табл. 6, в которой приведены так называемые *арифметические ряды*, дающие коэффициенты разложения бинома Ньютона n -ой степени:

$$(1+x)^n = 1 + nx + \frac{n(n-1)}{2!}x^2 + \frac{n(n-1)(n-2)}{3!}x^3 + \dots + \frac{n!x^k}{(n-k)!k!} + \dots \quad (11)$$

Таблица 6

	q_0	q_1	q_2	q_3	q_4	q_5	q_6	q_7	q_8	...
p_0	1	1	1	1	1	1	1	1	1	...
p_1	1	2	3	4	5	6	7	8	9	...
p_2	1	3	6	10	15	21	28	36	45	...
p_3	1	4	10	20	35	56	84	120	165	...
p_4	1	5	15	35	70	126	210	330	495	...
p_5	1	6	21	56	126	252	462	792	1287	...
p_6	1	7	28	84	210	462	924	1716	3003	...
p_7	1	8	36	120	330	792	1716	3432	6435	...
p_8	1	9	45	165	495	1287	3003	6435	12870	...
...	...	...	...	...	...	...	...	...	...	...

Биномиальные коэффициенты для $n = 1, 2, 3, \dots$ выставлены в косые ряды, начиная с верхнего левого угла табл. 6, а именно: $\{1, 1\}$, $\{1, 2, 1\}$, $\{1, 3, 3, 1\}$ и т.д. (они раскрашены в одинаковые белые или серые тона). Сумма биномиальных коэффициентов дает соответствующую степень 2, что вытекает из формулы (11) при подстановке $x = 1$:

$$1 + 1 = 2^1, \quad 1 + 2 + 1 = 2^2, \quad 1 + 3 + 3 + 1 = 2^3, \dots$$

Элементы табл. 6 обладают другими замечательными свойствами: каждый последующий элемент таблицы складывается из двух предыдущих, стоящих на предыдущей строке и в предыдущем столбце, например: $56 = 35 + 21$, $6435 = 3003 + 3432$ и т.д. Кроме того, любой элемент получается в результате сложения всех предшествующих ему элементов либо на предыдущей строке, либо в предыдущем столбце, например:

$$\begin{aligned} 495 &= 1 + 8 + 36 + 120 + 330, \\ 495 &= 1 + 4 + 10 + 20 + 35 + 56 + 84 + 120 + 165, \\ 3003 &= 1 + 8 + 36 + 120 + 330 + 792 + 1716, \\ 3003 &= 1 + 6 + 21 + 56 + 126 + 252 + 462 + 792 + 1287. \end{aligned}$$

Такая регулярность построения таблицы приводит к закономерностям в формулах для получения последовательностей чисел по горизонтальным (p_i) и вертикальным (q_i) рядам:

$$\begin{aligned} p_0 &= q_0 = 1, \\ p_1 &= q_1 = n/1!, \\ p_2 &= q_2 = n(n+1)/2!, \\ p_3 &= q_3 = n(n+1)(n+2)/3!, \\ p_4 &= q_4 = n(n+1)(n+2)(n+3)/4!, \quad \dots \end{aligned} \tag{12}$$

Видно, что формулы (12) для горизонтальных и вертикальных рядов отличаются от диагональных формул для биномиальных коэффициентов (11) только знаком, стоящим внутри каждой скобки.

Кто-то, возможно, посчитает *индуктивный* способ установления формул (12) недостаточным и попытается найти им подкрепление в каком-нибудь аналитическом выводе, например, из формул (11) или из двух вышеприведенных свойств таблицы. Это не означает, что данные математики излишне обеспоко-

ны своей профессиональной репутацией. Очень может быть, что они искренне заинтересованы побольше узнать об объективном устройстве числовых рядов. Поиск объективно существующих, но пока неизвестных нам, связей в действительности далек от формально-логического манипулирования символами. Так или иначе он будет походить скорее на методику исчисления.

Табл. 6 мы строили элемент за элементом, ряд за рядом по строго определенным законам. Нарушение этих закономерностей в 10 или 10^{10} рядах невозможно (если только мы сами этого не захотим), а значит, невозможен сбой формул для p_{10} или $p_{10^{10}}$. Сумма чисел натурального ряда, т.е. наша исходная формула (4), отвечает строке p_2 или, что то же самое, столбцу q_2 табл. 6. Успех этой формулы и ее символическое представление, помимо всего прочего, обеспечиваются еще и тем местом, которое отведено числам, стоящим в соответствующей строке и столбце. Формуле (9), которую мы не смогли доказать графическими способами, естественным образом отводятся следующие строка (p_3) и столбец (q_3). Так возникает целый каскад единообразных формул.

Чтобы найти формулу для сумм квадратов, которые дают последовательность чисел 1, 5, 14, 30, 55, и т.д. (ее мы тоже не смогли определить), нужно построить новую таблицу арифметических рядов, где бы в качестве одной из строк выступал квадратичный ряд. Нам посчастливилось открыть закономерность для сумм кубов (формула (6)), но как быть с суммами чисел, возведенных в четвертую, пятую и другие высшие степени? Здесь нет иного пути, как только последовательное конструирование таблиц арифметических рядов. К этому конструированию мы сейчас приступим, но прежде сделаем небольшое замечание в отношении табл. 6.

Если элементы арифметического ряда p_n обозначить через $a_1, a_2, a_3, \dots$, элементы ряда p_{n-1} через $b_1, b_2, b_3, \dots$, элементы ряда p_{n-2} через $c_1, c_2, c_3, \dots$ и т.д., то можно составить систему разностей 1-го порядка: $b_1 - a_1 = 0, b_2 - a_2 = a_1, b_3 - a_3 = a_2, \dots$, разностей 2-го порядка: $c_1 - b_1 = 0, c_2 - b_2 = b_1, c_3 - b_3 = b_2, \dots$ и т.д. Известно, что именно операция вычитания лежит в основе процедуры *дифференцирования*. Если, к примеру, взять производную от целочисленной квадратичной функции p_2 , то в результате получим линейную функцию:

$$\frac{dp_2}{dn} = \frac{d(n(n+1)/2)}{dn} = n + \frac{1}{2}.$$

В нашем случае при переходе от третьей ко второй строке так же происходит понижение степени полинома, но уже без добавления константы $1/2$, что можно записать как

$$d(p_2) = p_1 = n.$$

Движение по таблице снизу вверх и справа налево отвечает природе *дифференцирования*. Обратное движение по таблице, связанное с суммированием ее элементов, соответствует *интегрированию*:

$$d(p_n) = p_{n-1}, \quad d(q_n) = q_{n-1}, \quad \int (p_n) = p_{n+1}, \quad \int (q_n) = q_{n+1}.$$

Важно понять, что природа этих двух важнейших операций математического анализа в первую очередь лежит на элементарных арифметических операциях вычитания и сложения, и только во вторую очередь на операции предельного перехода

к бесконечно малым разностям ($\Delta x \rightarrow 0$) или к бесконечно большому числу деления ($n \rightarrow \infty$).

Теперь перейдем к рассмотрению табл. 7, которая уже не симметрична относительно своей диагонали. Ее строительство началось с третьей строки p_2 , где записаны квадраты чисел натурального ряда. Остальные элементы вычисляются из знакомого нам принципа: каждый последующий элемент складывается из двух предшествующих, например: $9 = 2 + 7$, $9438 = 5148 + 4290$ и т.д. В табл. 7, для всех элементов выполняются те же самые соотношения, что и для табл. 6, в частности:

$$\begin{aligned}660 &= 1 + 9 + 44 + 156 + 450, \\660 &= 2 + 7 + 16 + 30 + 50 + 77 + 112 + 156 + 210, \\4719 &= 2 + 15 + 64 + 204 + 540 + 1254 + 2640, \\4719 &= 1 + 7 + 27 + 77 + 182 + 378 + 714 + 1254 + 2079.\end{aligned}$$

Формулы, по которым вычисляются элементы горизонтальных и вертикальных рядов будут такими:

$$\begin{aligned}p_0 &= 2, & q_0 &= 1, \\p_1 &= (2n-1)/1!, & q_1 &= (n+1)/1!, \\p_2 &= n(2n+0)/2! = n^2, & q_2 &= n(n+3)/2!, \\p_3 &= n(n+1)(2n+1)/3!, & q_3 &= n(n+1)(n+5)/3!, \\p_4 &= n(n+1)(n+2)(2n+2)/4!, & q_4 &= n(n+1)(n+2)(n+7)/4!, \\p_5 &= n(n+1)(n+2)(n+3)(2n+3)/5!, \dots & q_5 &= n(n+1)(n+2)(n+3)(n+9)/5!, \dots\end{aligned}$$

Таблица 7

	q_0	q_1	q_2	q_3	q_4	q_5	q_6	q_7	q_8	...
p_0	—	2	2	2	2	2	2	2	2	...
p_1	1	3	5	7	9	11	13	15	17	...
p_2	1	4	9	16	25	36	49	64	81	...
p_3	1	5	14	30	55	91	140	204	285	...
p_4	1	6	20	50	105	195	336	540	825	...
p_5	1	7	27	77	182	378	714	1254	2079	...
p_6	1	8	35	112	294	672	1386	2640	4719	...
p_7	1	9	44	156	450	1122	2508	5148	9867	...
p_8	1	10	54	210	660	1782	4290	9438	19305	...

Числа, стоящие в «диагональных» рядах, начиная с верхнего левого угла табл. 7, также представляют собой коэффициенты регулярных полиномов либо r_i , либо s_i вида:

$$\begin{aligned}r_1 &= x + 2, & s_1 &= 2x + 1, \\r_2 &= (x + 1)(x + 2), & s_2 &= (x + 1)(2x + 1), \\r_3 &= (x + 1)^2(x + 2), & s_3 &= (x + 1)^2(2x + 1), \\r_4 &= (x + 1)^3(x + 2), \dots & s_4 &= (x + 1)^3(2x + 1), \dots\end{aligned}$$

Если в r - и s -полиномах раскрыть скобки, то перед различными степенями x как раз и будут стоять указанные коэффициенты. Для этих коэффициентов выполняются следующие вполне понятные соотношения:

$$1 + 2 = 3 \cdot 2^0, \quad 1 + 3 = 2 + 3 \cdot 2^1, \quad 1 + 4 + 5 + 2 = 3 \cdot 2^2, \dots$$

В связи с общим видом табл. 7 заметим, что представляют определенный интерес именно несимметричные таблицы, так как если бы первый столбец табл. 7 состоял из 2, то мы вновь имели бы дело с предыдущим случаем, отображенным табл. 6, у которой все элементы были бы умножены на 2. Аналогичная ситуация возникнет при $p_0 = q_0 = 3$ и т.д.

Наконец, рассмотрим табл. 8, в четвертой строке которой стоят кубы чисел натурального ряда. Строение этой таблицы аналогично строению табл. 7. Для ее элементов выполняются знакомые нам соотношения, в частности: $127 = 36 + 91$, $2892 = 1296 + 1596$, ..., $574 = 1 + 10 + 46 + 146 + 371$ и т.д. Горизонтальные и вертикальные ряды чисел удовлетворяют системе формул:

$$\begin{aligned} p_0 &= 6, & q_0 &= 1, \\ p_1 &= 6n + 6, & q_1 &= n + 5, \\ p_2 &= 3n^2 + 3n + 1, & q_2 &= (n^2 + 9n + 2)/2!, \\ p_3 &= n^3, & q_3 &= n(n^2 + 15n + 20)/3!, \\ p_4 &= [n(n+1)/2]^2 + n(n+1)(6n^2 + 6n + 0)/4!, & q_4 &= n(n+1)(n^2 + 21n + 50)/4!, \\ p_5 &= n(n+1)(n+2)(6n^2 + 12n + 2)/5!, \\ q_5 &= n(n+1)(n+2)(n^2 + 27n + 92)/5!, \\ p_6 &= n(n+1)(n+2)(n+3)(6n^2 + 18n + 6)/6!, \\ q_6 &= n(n+1)(n+2)(n+3)(n^2 + 33n + 146)/6!, \dots \\ p_7 &= n(n+1)(n+2)(n+3)(n+4)(6n^2 + 24n + 12)/7!, \dots \end{aligned}$$

Таблица 8

	q_0	q_1	q_2	q_3	q_4	q_5	q_6	q_7	q_8	...
p_0	—	—	6	6	6	6	6	6	6	...
p_1	—	6	12	18	24	30	36	42	48	...
p_2	1	7	19	37	61	91	127	169	217	...
p_3	1	8	27	64	125	216	343	512	729	...
p_4	1	9	36	100	225	441	784	1296	2025	...
p_5	1	10	46	146	371	812	1596	2892	4917	...
p_6	1	11	57	203	574	1386	2982	5874	10791	...
p_7	1	12	69	272	846	2232	5214	11088	21879	...
p_8	1	13	82	354	1200	3432	8646	19734	41613	...
...	...	...	...	...	...	...	...	...	...	...

Ряды p - и q -формул прерываются, когда закономерность их построения становится очевидной. Так, для q -формул определенную сложность вначале представляет поиск коэффициентов в последней скобке. В частности, коэффициенты перед n удовлетворяют простому условию: разности двух соседних коэффициентов дают 6:

$$15 - 9 = 21 - 15 = 27 - 21 = 33 - 27 = \dots = 6.$$

Но свободные члены квадратичной формы удовлетворяют уже более сложной системе равенств:

$$\begin{aligned} 20 - 2 = 18 = 3 \cdot 6, \quad 50 - 20 = 30 = 5 \cdot 6, \\ 92 - 50 = 42 = 7 \cdot 6, \quad 146 - 92 = 54 = 9 \cdot 6, \dots \end{aligned}$$

И все же для решения задачи по отысканию коэффициентов нужна какая-то общая методика, так как даже, например, для третьей строки $\{1, 7, 19, 37, 61, \dots\}$ практически невозможно чисто визуальным путем уловить закономерность получения очередного члена ряда. Такая методика существует. В частности, для p_2 нужно составить систему из трех уравнений и решить ее:

$$\begin{cases} a + b + c = 1, & a = 3, \\ 4a + 2b + c = 7, & b = -3, \\ 9a + 3b + c = 19, & c = 1. \end{cases}$$

Для нахождения коэффициентов p_3 требуется уже решить систему из шести уравнений:

$$\begin{cases} a + b + c + d + e + f = 1, & a = 1/20, \\ 32a + 16b + 8c + 4d + 2e + f = 10, & b = 1/4, \\ 243a + 81b + 27c + 9d + 3e + f = 46, & c = 5/12, \\ 1024a + 256b + 64c + 16d + 4e + f = 146, & d = 1/4, \\ 3125a + 625b + 125c + 25d + 5e + f = 371, & e = 1/30, \\ 7776a + 1296b + 216c + 36d + 6e + f = 812, & f = 0. \end{cases}$$

Затем, после составления полинома

$$n^5/20 + n^4/4 + 5n^3/12 + n^2/4 + n/30 = n(6n^4 + 30n^3 + 50n^2 + 30n + 4)/5!$$

его нужно попытаться упростить, поделив многочлен, стоящий в скобках, на два члена $(n+1)$ и $(n+2)$. В более сложных случаях можно попытаться отыскать корни полиномов. Рассмотрим самый неприятный для нас случай.

Пусть дан числовой ряд:

$$1, 5, 13, 25, 45, 81, 145, 257, 439, \dots,$$

и нужно найти формулу для его n -ого члена.

Взяв первые три элемента, мы можем вычислить подходящий для этой цели полином: $2n^2 - 2n + 1$. Однако при $n = 5$ он дает число 41 вместо 45. Поэтому составим и решим систему из пяти уравнений. Так мы найдем новый полином: $(n^5 - 10n^3 + 47n^2 - 62n + 30)/6$. При $n = 5, 6$ и 7 он нас устраивает, но при $n = 8$ даст число 253 вместо 257. Таким образом, у нас нет никогда уверенности в правильности нахождения полинома для n -ого члена.

К счастью, нам нечего бояться подобной ситуации. Таблицы устроены так, что степень полиномов нарастает равномерно на единицу и все формулы для горизонтальных и вертикальных рядов оказываются взаимосвязанными. Впрочем, для большей уверенности здесь можно воспользоваться приемом, который применялся нами в самом первом доказательстве справедливости формулы (4). Для табл. 8 это означает, что полином p верен, так как он удовлетворяет полиному p_2 :

$$(3n^2 - 3n + 1) + 6(n+1) = 6 - 3(n+1)^2 = 3(n+1) + 1.$$

Полином p_2 верен, так как он удовлетворяет полиному p_3 :

$$n^3 + 3(n+1)^2 = 3(n+1) + 1 = (n+1)^3 \text{ и т.д.}$$

Нахождение r и s -полиномов по табл. 3 не составит большого труда. Первоначальными значениями полиномов являются

$$r_2 = x^2 + 6x + 6, \quad s_2 = 6x^2 + 6x + 1.$$

Далее можно воспользоваться рекуррентными соотношениями:

$$r_{n+1} = (x+1)r_n, \quad s_{n+1} = (x+1)s_n.$$

Суммы коэффициентов полностью расписанных r и s -полиномов удовлетворяют равенствам:

$$1 + 6 + 6 = 13 \cdot 2^0, \quad 1 + 7 + 12 + 6 = 13 \cdot 2^1, \\ 1 + 8 + 19 + 18 + 6 = 13 \cdot 2^2, \dots$$

Несложно написать начало числовой таблицы, где бы задающей строкой был полином $p_4 = n^4$. Для нее первым r -полиномом будет

$$r_3 = x^3 + 14x^2 + 36x + 24.$$

Таблица со строкой $p_5 = n^5$ имеет такой r -полином:

$$r_4 = x^4 + 30x^3 + 150x^2 + 240x + 120.$$

Таким образом, мы имеем следующие ряды чисел:

1						
1	2					
1	6	6				
1	14	36	24			
1	30	150	240	120		
1	62	540	1560	1800	720	
...	...	...	...	...	...	...

Здесь обнаруживаются свои закономерности. Так, второй вертикальный ряд $\{2, 6, 14, 30, 62, \dots\}$ подчиняется простой формуле $2^n - 2$. Первый косой ряд $\{1, 2, 6, 24, 120, 720, \dots\}$ представляет собой последовательные значения факториала $n!$. А сейчас внимание: отношение элементов второго ряда $\{1, 6, 36, 240, 1800, \dots\}$ к соответствующим элементам первого ряда неожиданно дает хорошо знакомый нам ряд, подчиняющийся формуле (4):

$$1/1 = 1, \quad 6/2 = 3, \quad 36/6 = 6, \quad 240/24 = 10, \quad 1800/120 = 15, \dots$$

Так вот, мы утверждаем, что те закономерности, которые проявились во всех вышеприведенных таблицах, можно повернуть в сторону обоснования этой единственной формулы. Правда, мы не знаем, как это сделать. Очевидно, такой путь вычислений будет слишком громоздким. Однако он безусловно существует, коль скоро наша заветная последовательность выдала себя здесь. Еще раз подчеркнем, что к упомянутым здесь закономерностям мы пришли не в результате какого-то логического мышления, а на основе исключительно своих зрительных способностей. Кроме того, мы руководствовались неким свободным конструктивным принципом, который определяется словами: *что будет, если построить таблицу...*

В самом деле, мы смотрим на табл. 8 и замечаем, что она имеет три прочерка в первых своих ячейках по сравнению с одним прочерком в двух предыдущих слу-

чаях. Что будет, если построить таблицу, у которой первая строка состояла бы из шестерок, но имелся бы только один прочерк в первой строке? Такой шаг не является логически обоснованным, скорее это наша прихоть, ведь перед нами распростерто множество дорог, и мы выбираем один путь из большого числа возможных. В результате свободного выбора перед нами оказалась новая таблица чисел — табл. 9.

Таблица 9

	q_0	q_1	q_2	q_3	q_4	q_5	q_6	q_7	q_8	...
p_0	—	6	6	6	6	6	6	6	6	...
p_1	1	7	13	19	25	31	37	43	49	...
p_2	1	8	21	40	65	96	133	176	225	...
p_3	1	9	30	70	135	231	364	540	765	...
p_4	1	10	40	110	245	476	840	1380	2145	...
p_5	1	11	51	161	406	882	1722	3102	5247	...
p_6	1	12	63	224	630	1512	3234	6336	11583	...
p_7	1	13	76	300	930	2442	5676	12012	23595	...
p_8	1	14	90	390	1320	3762	9438	21450	45045	...

Естественно, мы останавливаем свой взор на строке p_3 , где раньше стояли кубы чисел. Сравнивая два ряда чисел: $\{1, 8, 27, 64, 125, 216, 343, 512, 729, \dots\}$ и $\{1, 9, 30, 70, 135, 231, 364, 540, 765, \dots\}$, мы неожиданно для себя открываем хорошо знакомый нам ряд чисел: $\{0, 1, 3, 6, 10, 15, 21, 28, 35, 56, 84, \dots\}$. Конечно, можно было бы обмануть читателя и весь текст изложения построить так, чтобы он с железной необходимостью подводил читателя к формуле (4). Но мы не станем разыгрывать из себя некую логическую машину и признаемся, что все вышло абсолютно случайно.

По инерции мышления мы начинаем образовывать разности между всеми остальными элементами двух таблиц, в результате чего возникает еще одна таблица — табл. 10.

Таблица 10

	q_0	q_1	q_2	q_3	q_4	q_5	q_6	q_7	q_8	...
p_0	—	—	—	0	0	0	0	0	0	...
p_1	—	—	1	1	1	1	1	1	1	...
p_2	—	1	2	3	4	5	6	7	8	...
p_3	0	1	3	6	10	15	21	28	36	...
p_4	0	1	4	10	20	35	56	84	120	...
p_5	0	1	5	15	35	70	126	210	330	...
p_6	0	1	6	21	56	126	252	462	792	...
p_7	0	1	7	28	84	210	462	924	1716	...
p_8	0	1	8	36	120	330	792	1716	3432	...

Табл. 10 отличается от табл. 6 первой строкой и первым столбцом, состоящими из нулей. Теперь к нам пришло понимание того, почему разности между чле-

нами ряда p_3 табл. 9 и табл. 8 получились именно такими. Разумеется, такой результат не был случайным. Можно говорить, что он со всей *логической необходимостью* вытекает из правила сложения таблиц арифметических рядов, хотя на само правило мы наткнулись достаточно случайно.

Если разность между табл. 9 и табл. 8 дала табл. 6, то нельзя ли, например, к табл. 8 соответствующим образом прибавить табл. 7? Да, такой «эксперимент» удастся осуществить, в результате получаем табл. 11.

Таблица 11

	q_0	q_1	q_2	q_3	q_4	q_5	q_6	q_7	q_8	...
p_0	—	—	—	6	6	6	6	6	6	...
p_1	—	—	14	20	26	32	38	44	50	...
p_2	—	8	22	42	68	100	138	182	232	...
p_3	1	9	31	73	141	241	379	561	793	...
p_4	1	10	41	114	255	496	875	1436	2229	...
p_5	1	11	52	166	421	917	1792	3228	5457	...
p_6	1	12	64	230	651	1568	3360	6588	12045	...
p_7	1	13	77	307	958	2526	5886	12474	24519	...
p_8	1	14	91	398	1356	3882	9768	22242	46761	...

Таблица 12

	q_0	q_1	q_2	q_3	q_4	q_5	q_6	q_7	q_8	...
p_0	—	—	—	—	0	0	0	0	0	...
p_1	—	—	—	1	1	1	1	1	1	...
p_2	—	—	1	2	3	4	5	6	7	...
p_3	—	0	1	3	6	10	15	21	28	...
p_4	0	0	1	4	10	20	35	56	84	...
p_5	0	0	1	5	15	35	70	126	210	...
p_6	0	0	1	6	21	56	126	252	462	...
p_7	0	0	1	7	28	84	210	462	924	...
p_8	0	0	1	8	36	120	330	792	1716	...

Вновь устремляем свои взоры на ряд p_3 и вновь сравниваем его с рядом p_3 табл. 9. Разность этих рядов опять порождает ряд $\{0, 0, 1, 3, 6, 10, 15, 21, 28, \dots\}$. Следовательно, табл. 11 отличается от табл. 9 на табл. 6, у которой нулями уже заняты первые два столбца (табл. 12).

Так шаг за шагом к нам приходит глубокое понимание природы таблиц арифметических рядов. Оказывается, каждая такая бесконечная таблица представляет собой цельный математический объект. Эти объекты, как и числа, можно складывать и вычитать. Они поддаются классификации, в частности, по количеству прочерков в левом верхнем углу таблицы, т.е. по числу ячеек, для которых не выполняются провозглашенные ранее принципы образования элементов. К *нулевому классу* можно было бы отнести табл. 6. Это единственная таблица, которая имеет одинаковые формулы для вертикальных и горизонтальных рядов. Она

играет роль единичного элемента в множестве арифметических таблиц. Затем идут таблицы *первого класса* типа табл. 7 и табл. 9. Они отличаются тем, что полиномы, выражающие общие члены горизонтальных и вертикальных последовательностей, имеют действительные корни. Формулы p - и q -полиномов для табл. 7 уже выписывались. Приведем соответствующие формулы для табл. 9:

$$\begin{aligned} p_0 &= 6, \\ p_1 &= (6n - 5)/1!, \\ p_2 &= n(6n - 4)/2!, \\ p_3 &= n(n + 1)(6n - 3)/3!, \\ p_4 &= n(n + 1)(n + 2)(6n - 2)/4!, \\ p_5 &= n(n + 1)(n + 2)(n + 3)(6n - 1)/5!, \\ p_6 &= n(n + 1)(n + 2)(n + 3)(n + 4)(6n - 0)/6!, \\ p_7 &= n(n + 1)(n + 2)(n + 3)(n + 4)(n + 5)(6n + 1)/7!, \\ p_8 &= n(n + 1)(n + 2)(n + 3)(n + 4)(n + 5)(n + 6)(6n + 2)/8!, \\ &\dots \\ q_0 &= 1, \\ q_1 &= (n + 5)/1!, \\ q_2 &= n(n + 11)/2!, \\ q_3 &= n(n + 1)(n + 17)/3!, \\ q_4 &= n(n + 1)(n + 2)(n + 23)/4!, \\ q_5 &= n(n + 1)(n + 2)(n + 3)(n + 29)/5!, \\ &\dots \end{aligned}$$

Сопоставляя эти формулы с формулами для табл. 7, мы легко улавливаем закономерности их написания. Теперь без всяких таблиц мы сможем выписать p - и q -формулы с $p_0 = 3, 4, 5$ и т.д.

Ко *второму классу* таблиц можно отнести табл. 8, которая имеет три ячейки с прочерком и для которой p - и q -полиномы не полностью раскладываются на простые двучлены с действительными корнями. В их состав входят квадратичные сомножители с комплексными корнями. К *третьему классу* относятся таблицы типа табл. 11, у которой уже шесть прочерков. В состав p -полинома у нее входят неразложимые кубы:

$$\begin{aligned} p_3 &= (6n^3 + 6n^2 - 12n + 6)/3!, \\ p_4 &= n(6n^3 + 20n^2 - 6n + 1)/4!, \\ p_5 &= n(n + 1)(6n^3 + 34n^2 + 16n - 4)/5!, \dots \end{aligned}$$

Табл. 10 и табл. 12 дают представление о роли «единичного элемента» в множестве арифметических таблиц и поясняют правила сложения и вычитания со сдвигом на строку или столбец. Мы также припоминаем, что складывать и вычитать можно не только целые положительные числа; следовательно, таблицы могут быть заполнены действительными или комплексными числами. Если читатель захочет, он может остаток своей жизни целиком посвятить изучению свойств этих таблиц: они вполне достойны этого. Что же касается нас, то позвольте закончить этот последний подраздел повторением главного вывода.

Всякий скажет, что таблицы и p , q -формулы ничего общего не имеют с рисунками. Тем не менее, установленные закономерности припили к нам благодаря внимательному *рассматриванию* их. Цифры и буквенные обозначения мы *обозреваем* точно так же, как точки и линии, образующие рисунки, т.е. при рассмотрении тех и других задействованы одни и те же психические механизмы. Через цифры и буквы к нам приходят понятия о числе, формуле и отношениях между ними; через точки и линии — понятия о различных фигурах и тоже отношениях между ними. По формулам и таблицам мы свободно скользим взглядом так же, как по рисункам, и здесь нет места для логики. От формулы к формуле мы нередко приходим через *процедуру вычисления*. Логика, конечно, помогает общаться и делает понятным все то, что затем излагается другим людям, но на этапе исследования или даже первого знакомства с неведомым объектом она плохая помощница. Молодым людям, жаждущим познать истину вещей, нужно усвоить именно *философию конструктивизма*.

Содержание

Предисловие	4
1. Логика	5
1.0. Введение	5
1.1. Операции логики Буля	7
1.2. Формы представления булевых функций	13
1.3. Методы доказательства в логике Буля	21
1.4. Задания на практическую работу по логике Буля	28
1.5. Введение в логику высказываний	34
1.6. Построение доказательств в логике высказываний	39
1.7. Задания на практическую работу по логике высказываний.....	53
1.8. Примеры решения задач	59
1.9. Операции над предикатами и кванторами	65
1.10. Построение доказательств в логике предикатов.....	77
1.11. Задания на практическую работу по логике предикатов.....	85
1.12. Разбор решений задач по логике предикатов.....	89
2. Группы	96
2.0. Введение	96
2.1. Введение понятия группы	97

2.2. Действия с 0,1-матрицами.....	107
2.3. Подстановки	117
2.4. Группы небольших порядков.....	125
2.5. Отношение эквивалентности	134
2.6. Геометрическая интерпретация групповых преобразований.....	143
2.7. Отношение порядка.....	174
2.8. Алгебраические системы.....	204
2.9. Поля многочленов.....	214
2.10. Корректирующие коды.....	224
3. Графы.....	234
3.0. Введение	234
3.1. Цепи	237
3.2. Виды графов. Пути и контуры в графе	264
3.3. Морфология графа.....	273
3.4. Решение задач по теории кодирования, автоматов и языков с использованием графов	292
Заключение	316
1. Возможные подходы к исследуемому объекту.....	316
2. Конструктивизм	323

Учебное издание

Акимов Олег Евгеньевич

Дискретная математика:
логика, группы, графы

Художник *И. Лозинская*
Компьютерная верстка *В. Носенко*

Подписано в печать 14.12.00. Формат 70х100¹/₁₆.
Гарнитура Ньютон. Бумага офсетная. Печать офсетная.
Усл. печ. л. 22,0. Тираж 3000 экз. Заказ 6514

Издательство «Лаборатория Базовых Знаний»
Адрес для переписки: 103473, Москва, а/я 9
Телефон (095)955-0398. E-mail: lbz@aha.ru

Лицензия на издательскую деятельность №066140
от 12 октября 1998 г.

Отпечатано с готовых диапозитивов в полиграфической фирме «Полиграфист».
160001, г. Вологда, ул. Челюскинцев, 3.

САЙТ АВТОРА: <http://sceptic-ratio.narod.ru/index.htm>