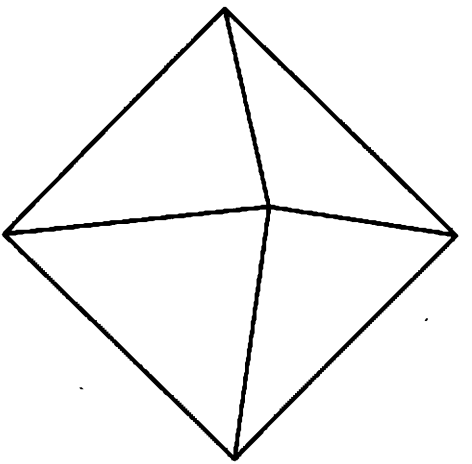
Джон Х. Конвей
Дерек А. Смит

О кватернионах и октавах

об их геометрии,
арифметике
и симметриях



John H. Conway
Derek A. Smith

On Quaternions and Octonions:
Their Geometry, Arithmetic, and Symmetry

A K Peters
Natick, Massachusetts

Джон Х. Конвей
Дерек А. Смит

О кватернионах и октавах,
об их геометрии, арифметике и симметриях

Перевод с английского
С. М. Львовского

под редакцией
В. В. Доценко

Москва
Издательство МЦНМО
2009

УДК 512
ББК 22.14
К64

Конвей Дж., Смит Д.

К64 О кватернионах и октавах, об их геометрии, арифметике и симметриях / Пер. с англ. С. М. Львовского. — М.: МЦНМО, 2009. — 184 с.

ISBN 978-5-94057-517-7

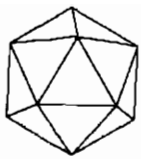
Эта небольшая монография посвящена самым разнообразным геометрическим и арифметическим свойствам алгебр кватернионов и октав (чисел Кэли). В числе прочего, излагаются общая теория композиционных алгебр и теория тройственности, рассказывается о связи октав с лупами Муфанг, изучаются свойства кватернионных и октавных аналогов гауссовых целых чисел. Значительная часть материала книги не была до сих пор отражена в литературе на русском языке.

Для студентов, аспирантов и научных работников.

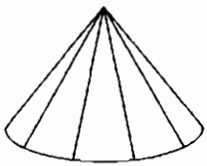
ББК 22.14

ISBN 1-56881-134-9 (англ.)
ISBN 978-5-94057-517-7

Эта книга посвящается
Лилиан Смит и Гарету Конвею,
без которых мы бы завершили работу
гораздо быстрее



Оглавление



Предисловие

Перед вами — книга о геометрии и арифметике алгебр кватернионов и октав. Благодаря тому, что эти алгебры тесно связаны со специальными свойствами геометрии некоторых евклидовых пространств, они помогают понять свойства групп симметрий в малых размерностях. Например, имеется связь между трех- и четырехмерными группами, объясняемая при помощи кватернионов, поскольку поворот в трехмерном пространстве можно задать с помощью одного кватерниона, а в четырехмерном — с помощью пары кватернионов. Устроена эта связь довольно сложно: в ней участвуют соответствия, при которых два элемента соответствуют одному.

С кватернионами знакомы многие; поэтому в части, посвященной кватернионам, мы предполагаем у читателя такое знакомство и рассказываем, как использовать кватернионы для классификации конечных групп в размерностях 3 и 4 (по аналогии с тем, как с помощью комплексных чисел перечисляются группы в размерности 2). В заключение этой части мы обсуждаем, какие свойства гурвицевых целых кватернионов можно установить геометрически, и, в частности, доказываем теорему об однозначном разложении.

Основная тема части, посвященной октавам, — замечательная «симметрия тройственности». Поскольку, однако, свойства октав не столь хорошо известны, начинаем мы с того, что доказываем знаменитую теорему Гурвица, утверждающую, что $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ и $\mathbb{O}$ — единственные композиционные алгебры, так как при этом получается также и наилучший метод построения этих алгебр. Пользуясь методами этого доказательства, мы показываем, что эти алгебры задают лупы Муфанг; мы рассматриваем лупы Муфанг таким образом, чтобы при приложении нашей теории к случаю восьмимерной ортогональной группы проявилась тройственность.

До последнего времени исследование арифметики целых октав, начатое Диксоном, Бруком и Коксетером, продвинулось не слишком дале-

ко. В заключительных главах нашей книги мы улучшаем эту ситуацию в нескольких аспектах. С помощью метода, принадлежащего Рему, мы развиваем новую теорию разложения на множители для целых октав. Мы описываем также действие их группы автоморфизмов на некоторых важных подкольцах и устанавливаем, что максимальные подгруппы являются стабилизаторами некоторых из этих подколец. В одном из случаев нам приходится редуцировать целые октавы по модулю 2.

Завершается книга очень короткой главой, посвященной знаменитой октавной проективной плоскости.

Чтобы получить свойства алгебр над произвольным полем при минимальных предположениях наподобие альтернативности, нужны весьма сложные рассуждения. Чтобы доказательства были попроще, мы сочли нужным исходить из свойства «быть композиционной алгеброй» и ограничиться классическими алгебрами над полем действительных чисел.

Программисты компьютерных игр и авиадиспетчеры широко используют кватернионы, поскольку с их помощью можно находить композиции поворотов с минимумом вычислений. Мы позволили себе обойти молчанием эти и другие практические приложения, поскольку о них подробно рассказано в недавно вышедшей книге Кюйперса [29].

Мы благодарим Джона Баэза, Уоррена Смита, Дэниэла Олкока, Уоррена Джонсона и Мохаммеда Абусаида за полезные замечания касательно различных мест в книге. Дерек благодарен «Academic Research Committee at Lafayette College» за предоставление летней стипендии. Алиса и Клаус Питерс оказались самыми лучшими издателями, каких только можно представить. Мы благодарны им, а также Джонатану Питерсу, Хезер Холкоум, Даррену Уозерспуну, Ариэлю Джаффе и Сюзанне Питерс за работу над этой книгой. Наконец, мы благодарим наших жен Барбару и Диану за терпение.

Джон Конвей, Дерек Смит
Ноябрь 2002

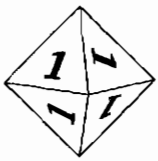
Комплексные числа и их приложения к одно- и двумерной геометрии

Мы полагаем, что с действительными-то числами вы точно знакомы. *Комплексные числа* суть формальные выражения вида $x_0 + x_1 i$ (где x_0, x_1 действительны), операции над которыми определены так:

$$(x_0 + x_1 i) + (y_0 + y_1 i) = (x_0 + y_0) + (x_1 + y_1)i,$$
$$(x_0 + x_1 i)(y_0 + y_1 i) = (x_0 y_0 - x_1 y_1) + (x_0 y_1 + x_1 y_0)i;$$

иными словами, комплексные числа — это алгебра над действительными числами с образующей i, удовлетворяющей соотношению

$$i^2 = -1.$$



Введение

§ 1.1. Алгебра действительных чисел $\mathbb{R}$

После древних греков (а также геометров последующих эпох) принято параметризовать евклидову прямую с помощью алгебры $\mathbb{R}$ действительных чисел. При такой параметризации расстояние между a и b равно $|a-b|$ — абсолютной величине их разности, которую можно также записать в виде $\sqrt{(a-b)^2}$. Важным свойством $\mathbb{R}^1$ является то, что $|xy|=|x||y|$.

Изометрии $\mathbb{R}^1$ (т. е. отображения, сохраняющие расстояния) суть

$$\textit{переносы } x\to k+x \quad \text{и} \quad \textit{отражения } x\to k-x.$$

Стало быть, одномерная ортогональная группа GO_1 состоит из двух изометрий $x\to\pm x$, оставляющих на месте начало координат.

Множество действительных чисел $\mathbb{R}$ содержит множество рациональных чисел $\mathbb{Q}$ и, в частности, множество целых чисел $\mathbb{Z}$, являющиеся предметом изучения теории чисел. В частности, для целых чисел выполнена теорема об однозначном разложении (которая была по существу открыта тем же Евклидом), традиционная формулировка которой состоит в том, что всякое целое положительное число является произведением (положительных) простых чисел, причем это разложение единственно с точностью до порядка сомножителей.

Для целей данной книги лучше отбросить условие положительности; тогда утверждение будет состоять в том, что всякое положительное или отрицательное целое число является произведением положительных или отрицательных простых чисел, причем разложение однозначно с точностью до порядка сомножителей и изменения знаков.

Мы приведем краткий набросок традиционного доказательства, в котором существенно используется то обстоятельство, что всякое число $n\in\mathbb{Z}$ можно разделить с остатком на любое ненулевое число d таким

образом, чтобы остаток r был строго меньше, чем делитель. (На самом деле можно добиться выполнения неравенства $|r| \leqslant \frac{1}{2}|d|$; см. рис. 1.1.)

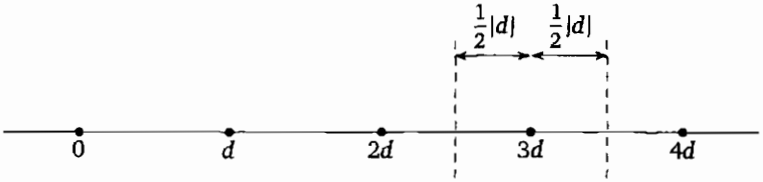


Рис. 1.1. Максимальный остаток для $\mathbb{Z}$

Идеалом в $\mathbb{Z}$ называется подмножество $\mathscr{I}$, обладающее следующими свойствами:

— $0 \in \mathscr{I}$;

— сумма любых двух элементов из $\mathscr{I}$ лежит в $\mathscr{I}$;

— целочисленное кратное произвольного элемента из $\mathscr{I}$ также лежит в $\mathscr{I}$.

Идеал называется *главным*, если он состоит из всех кратных некоторого фиксированного числа g, называемого образующей.

Теперь мы имеем следующий факт.

Лемма 1. *Всякий идеал в $\mathbb{Z}$ является главным.*

Доказательство. Идеал $\{0\}$ является главным. Если $\mathscr{I} \neq \{0\}$, то пусть d — ненулевой элемент $\mathscr{I}$ с наименьшей абсолютной величиной. Покажем, что $\mathscr{I}$ состоит из кратных d. В самом деле, если $\mathscr{I}$ содержит какое-нибудь еще целое число (обозначим его n), то можно записать равенство

$$n = qd + r, \quad \text{где} \quad 0 \leqslant r < |d|.$$

Поскольку, однако, n и d лежат в идеале, то в нем лежит и число r, абсолютная величина которого меньше, чем у d, — противоречие. □

Из этой леммы мы выведем следующую лемму.

Лемма 2. *Если p — простое число, то p делит произведение двух чисел тогда и только тогда, когда оно делит один из сомножителей.*

Доказательство. Предположим, что p делит ab. Тогда идеал, состоящий из чисел вида $mp + na$, обязан быть главным идеалом, образующая которого g должна быть делителем p, так что можно считать, что она равна p или 1. Если, однако, $g = p$, то p делит a, а если $g = 1$, то отсюда следует, что $1 = mp + na$ для некоторых m и n, так что $b = mpb + nab$, что делится на p. □

Из этих двух лемм теорема и следует, поскольку если $p_1 p_2 \ldots$ и $q_1 q_2 \ldots$ — два разложения одного и того числа на простые множите-

ли, то можно заключить, что q_1 должно делить одно из p_i (пусть это будет p_1) и тем самым совпадать с этим p_1 с точностью до знака. Сокращая на p_1, получаем, что q_2 должно с точностью до знака совпадать, скажем, с p_2, и т. д.

§ 1.2. Высшие размерности

Результаты, с которых начинается первая глава, относятся к одномерному пространству $\mathbb{R}^1$ и его подрешетке $\mathbb{Z}$. Цель этой книги — обобщить эти результаты на некоторые высшие размерности.

В главе 2 разбирается двумерный случай: мы обсудим планиметрию в терминах алгебры комплексных чисел $\mathbb{C}$ и скажем кое-что про две самые знаменитые арифметики комплексных чисел: кольцо $\mathbb{Z}[i]$ гауссовых целых чисел и кольцо $\mathbb{Z}[\omega]$ эйзенштейновых целых чисел.

Замечательно, что для подобного обсуждения трехмерной геометрии требуется четырехмерная алгебра — алгебра *кватернионов*. Именно поэтому открыть их было непросто, как видно по фрагменту из книги Баэза, который мы приводим ниже.

В главе 3 мы определяем алгебру $\mathbb{H}$ кватернионов и используем ее для перечисления всех конечных групп трехмерных изометрий. В главе 4 мы делаем то же самое для четырехмерного пространства, что применительно к кватернионам, разумеется, вполне естественно.

В нескольких следующих главах соответствие между номером главы и размерностью нарушается. В главе 5 обсуждается, что́ применительно к кватерниону означает слово «целый». Мы увидим, что для гурвицевых целых выполнен некоторый вариант теоремы об однозначном разложении и что в этом отношении они лучше, чем более наивные липшицевы целые.

Какие еще алгебры обладают свойствами, аналогичными свойствам кватернионов? Оказывается, наиболее важным является тождество $[xy] = [x][y]$, определяющее «композиционные алгебры». В главе 6 мы доказываем замечательный результат Гурвица, гласящий, что список композиционных алгебр исчерпывается знаменитыми алгебрами в размерностях 1, 2, 4 и 8. Оказывается, умножение в восьмимерной *алгебре октав* $\mathbb{O}$ не является ассоциативным, но удовлетворяет условиям Муфанг, являющимся интересной заменой ассоциативности. В главе 7 мы объясняем, каким образом условия Муфанг можно рассматривать как условие симметрии.

В главе 8, аналогичной главе 4, обсуждаются октавы и восьмимерная геометрия. Мы обсуждаем замечательную картановскую трой-

ственность на PSO_8 и выводим с ее помощью «теорему о семи сомножителях».

В главе 9, являющейся аналогом главы 5, изучается правильное определение целости для октав, а затем для целых октав развивается правильная теория разложения. В следующих двух главах очень подробно изучаются автоморфизмы целых октав. В главе 10 исследуются единицы, а в главе 11 показывается, как можно получить дополнительную информацию, работая по модулю 2.

Наконец, в главе 12 октавы используются для построения чрезвычайно интересной проективной плоскости.

§ 1.3. Ортогональные группы

Полная ортогональная группа GO_n есть множество всех изометрий n-мерного евклидова пространства $\mathbb{R}^n$, оставляющих на месте начало координат. Приведенная ниже лемма утверждает, что GO_n порождена отражениями.

Лемма 3. *Всякий элемент* $\alpha \in GO_n$, *оставляющий на месте все точки* k*-мерного подпространства, является произведением не более чем* $n-k$ *отражений.*

Доказательство. Рассмотрим вектор v, не являющийся неподвижным относительно α; пусть $v \to w$. Тогда отражение относительно $v-w$ переводит w обратно в v (см. рис. 1.2) и при этом оставляет на месте всякий вектор u, неподвижный относительно α (поскольку $v-w$ ортогонален к u, так как $[u, v] = [u, w]$). □

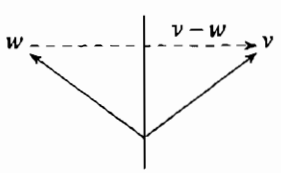


Рис. 1.2. *Отражение относительно* $v-w$

Будем считать, что читатель знаком с понятием определителя. Поскольку определитель отражения равен -1, определитель всякого элемента из GO_n равен ± 1, а элементы с определителем $+1$ образуют подгруппу индекса 2 — *специальную ортогональную группу* SO_n. Произведение любых двух отражений (скажем, относительно r и s) есть простой поворот: плоскость $\langle r, s\rangle$ поворачивается на некоторый угол, а все точки ортогонального к ней $(n-2)$-мерного пространства остаются на

месте. Собирая отражения в пары, получаем, что SO_n порождена этими простыми поворотами.

Если, наконец, в GO_n или SO_n пренебречь разницей между α и $-\alpha$, то мы получим группы PGO_n и PSO_n — *проективную ортогональную группу* и *проективную специальную ортогональную группу*. Соотношения между группами GO_n, SO_n, PGO_n и PSO_n зависят от четности размерности; они обсуждаются в главах 3 и 4.

Следствием существования комплексных чисел является то, что SO_2 и PSO_2 коммутативны; из существования кватернионов вытекает, что $PSO_4 \simeq PSO_3 \times PSO_3$; из существования октав вытекает, что PSO_8 обладает автоморфизмом порядка 3 — «автоморфизмом тройственности».

§ 1.4. История кватернионов и октав

Задумывая эту книгу, мы собирались поместить в этой главе наше собственное изложение истории предмета. Времени на это у нас не хватило, но, к счастью, нас спас Джон Баэз. С его разрешения приводим выдержку из его статьи [5].

Большинство математиков знакомы с историей о том, как Гамильтон изобрел кватернионы. В 1835 году, в возрасте 30 лет, он научился работать с комплексными числами как с парами действительных. Вдохновленный этой связью между $\mathbb{C}$ и двумерной геометрией, он в течение многих лет пытался изобрести бóльшую алгебру, которая играла бы аналогичную роль в трехмерной геометрии. То, что он искал, на современном языке, похоже, называлось бы трехмерной нормированной алгеброй с делением. Его поиски достигли своего апогея в октябре 1843 года. Позже он писал сыну: «Каждое утро в начале этого месяца ты и твой младший брат Уильям Эдвин, который был тогда совсем маленьким, спрашивали меня, когда я спускался к завтраку: „Папа, ты уже научился *умножать тройки*?“. Я же, увы, всякий раз грустно качал головой и отвечал: „Нет, я умею их только складывать и вычитать“». Проблема была, конечно, в том, что трехмерной нормированной алгебры с делением не существует, и на самом деле ему была нужна четырехмерная алгебра.

И вот наконец 16 октября 1843 года, прогуливаясь с женой вдоль Королевского канала по дороге на заседание Королевской ирландской академии в Дублине, он совершил свое эпохальное открытие: «Можно сказать, я здесь и сейчас почувствовал, как электрическая цепь мысли замкнулась, и засверкавшие искры были фундаментальными соотношениями на i, j и k ровно в том виде, в каком я их с тех пор использовал». Тогда же Гамильтон совершил знаменитый акт математического вандализма — он вырезал эти соотношения на каменных перилах моста Брум:

$$i^2 = j^2 = k^2 = ijk = -1.$$

Одна из причин, по которой эта история столь хорошо известна, состоит в том, что с этого момента и до конца своей жизни Гамильтон был одержим идеей исследования кватернионов и применения их к геометрии (см. [21], [24]). И в течение некоторого времени кватернионы действительно были в моде. В Дублине они в обязательном порядке входили в программу экзаменов, а в некоторых американских университетах кватернионы были единственным изучавшимся разделом высшей математики. Многое из того, что мы сейчас делаем со скалярами и векторами в $\mathbb{R}^3$, делалось тогда с помощью вещественных и мнимых кватернионов. Возникла целая школа «кватерниощиков», которую после смерти Гамильтона возглавляли Питер Тэйт из Эдинбурга и Бенджамин Пирс из Гарварда. Тэйт написал о кватернионах восемь книг, в которых особое внимание уделялось приложениям к физике. Когда Гиббс изобрел современные обозначения для скалярного и векторного произведений, Тэйт обозвал их «уроддами-гермафродитами». Развернулась горячая полемика, в ходе которой такие знаменитости, как Кельвин и Хевисайд, разражались убийственными инвективами в адрес кватернионов. В конце концов кватернионы были побеждены и приобрели несколько дурную репутацию, от которой они в полной мере так и не избавились [12].

Менее общеизвестна история открытия октав Джоном Т. Грейвзом, товарищем Гамильтона по колледжу. Именно интерес Грейвза к алгебре первоначально побудил Гамильтона к размышлениям о комплексных числах и тройках чисел. На следующий же день после своей судьбоносной прогулки Гамильтон послал Грейвзу письмо на восьми страницах, в котором рассказывалось о кватернионах. В ответе, датированном 26 октября, Грейвз с похвалой отзывается о смелости гамильтоновской идеи, но при этом прибавляет: «Все-таки нечто в этой системе меня смущает. Мне пока что неясно, до какой степени мы обладаем свободой создавать новые мнимости и наделять их сверхъестественными свойствами». Он задает вопрос: «Если Вы в состоянии создать с помощью своей алхимии три фунта золота, зачем же на этом останавливаться?»

И тут Грейвз сам принялся за работу над своим собственным золотом! 26 декабря он послал Гамильтону письмо с описанием новой восьмимерной алгебры, которую он назвал октавами. Он показал, что октавы образуют нормированную алгебру с делением, и использовал октавы для доказательства того, что произведение двух сумм восьми полных квадратов также является суммой восьми полных квадратов («теорема о восьми квадратах», [23]).

В январе 1844 года Грейвз посылает Гамильтону три письма, в которых и дальше распространяется о своем открытии. Он рассматривает возможность построения общей теории «2^n-ионов» и пытается построить 16-мерную нормированную алгебру с делением, но при этом, как он пишет, «встречается с неожиданными трудностями» и начинает сомневаться в возможности такого построения. Гамильтон пообещал Грейвзу объявить о его открытии, но, будучи поглощенным работой с кватернионами, он постоянно это откладывает. В июле он пишет Грейвзу письмо, в котором указывает, что октавы неассоциативны: «$A \cdot BC = AB \cdot C = ABC$, если A, B и C — кватернионы, но с твоими октавами в общем случае это не так». На самом деле примерно в это время

Гамильтон первым использовал термин «ассоциативность», так что октавы, возможно, сыграли свою роль при возникновении и прояснении концепции ассоциативности.

Между тем юный Артур Кэли, только что окончивший Кембридж, размышлял о кватернионах с того самого момента, когда Гамильтон объявил об их существовании. Кажется, он пытался найти связи между кватернионами и гиперэллиптическими функциями. В марте 1845 года он опубликовал в журнале «Philosophical magazine» статью, озаглавленную «Об эллиптических функциях Якоби: ответ преподобному Б. Бронуину; и о кватернионах». Основная часть этой статьи представляла собой попытку опровергнуть статью, указывающую на ошибки в работе Кэли, посвященной эллиптическим функциям. Похоже, что только в последний момент Кэли добавил к статье краткое описание октав. Надо сказать, в этой статье было столько ошибок, что ее даже не воспроизвели в его собрании сочинений — за исключением части, посвященной октавам [10].

Расстроенный тем, что его обошли с публикацией, Грейвз добавил к своей собственной статье, принятой к печати в следующем номере того же журнала, постскриптум, в котором утверждал, что знал про октавы начиная с Рождества 1843 года; 14 июля 1847 года Гамильтон представил в «Труды» Королевской ирландской академии короткую заметку, утверждающую приоритет Грейвза. Увы, было уже поздно: октавы стали известны под именем чисел Кэли. Мало того, позднее Грейвз обнаружил, что его теорема о восьми квадратах была открыта К. Ф. Дегеном еще в 1818 году (см. [13], [14]).

Но почему же октавы прозябали в такой безвестности по сравнению с кватернионами? Помимо малопочтенных обстоятельств их рождения, свою роль сыграло то, что у них не было такого неутомимого пропагандиста, как Гамильтон. А уж это, в свою очередь, наверняка объясняется тем, что у них не было никаких ясных приложений к геометрии и физике. Единичные кватернионы образуют группу SU_2, являющуюся двулистным накрытием группы поворотов SO_3. Благодаря этому кватернионы очень удобны при работе с поворотами и моментом количества движения, особенно в контексте квантовой механики; в наши дни мы рассматриваем это обстоятельство как частный случай теории алгебр Клиффорда. Большинство из нас не придают теперь кватернионам той вселенской значимости, на которой настаивал Гамильтон, но кватернионы хорошо укладываются в наше понимание вещей. А вот про октавы этого не скажешь.

Наши попытки понять «вселенскую значимость» октав привели к появлению этой книги.

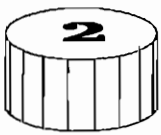
Добавим к баэзовскому краткому историческому очерку, что хотя Гамильтон, похоже, действительно был первым, кто построил кватернионы как алгебру, у кватернионов есть и более ранняя история, начинающаяся с открытия Эйлером в 1748 году тождества с четырьмя квадратами (которое кватернионы и определяет). Кроме того, О. Родригес

в своих исследованиях, увенчавшихся в 1840 году блестящей статьей [38], параметризовал общий поворот с помощью четырех параметров (часто они ошибочно называются параметрами Эйлера—Родригеса), являющихся фактически координатами соответствующего кватерниона. Это позволяет рассматривать его как предвестника идей Гамильтона, поскольку приводимое им правило умножения совпадает с датируемой 1843 годом формулой Гамильтона для произведения двух кватернионов. Более полное описание исследований Родригеса см. в книге С. Альтмана [3].

Из более поздних исследований, имеющих отношение к материалу этой книги, отметим следующие: гурвицеву характеризацию композиционных алгебр [26]; работу Диксона (см. [15]), включающую его конструкцию удвоения и обсуждение понятия «целости»; геометрические (Кокстер, [11]) и арифметические (Ранкин, [36]) исследования целых октав О. И здесь, и в других местах в этой книге мы приводим очень мало ссылок и исторических замечаний. Интересующегося читателя отсылаем к сайту

`http://www.akpeters.com/QANDO`,

содержащему дополнительные библиографические указания и гиперссылку на сетевую версию статьи Баэза.



Комплексные числа и двумерная геометрия

Мы предполагаем, что наш читатель знаком с алгеброй комплексных чисел. В этой главе мы сосредоточимся на их связи с геометрией евклидовой плоскости: это послужит прелюдией к аналогичным приложениям кватернионов и октав к евклидовым пространствам большей размерности. Мы обсудим также арифметику двух наиболее интересных подколец в кольце комплексных чисел: колец гауссовых и эйзенштейновых чисел.

§ 2.1. Повороты и отражения

Геометрические свойства комплексных чисел вытекают из того обстоятельства, что они образуют композиционную алгебру относительно евклидовой нормы

$$N(x+iy)=x^2+y^2,$$

что означает, что

$$N(z_1z_2)=N(z_1)N(z_2).$$

Из этого следует, что при умножении на фиксированное (ненулевое) число z_0 все длины умножаются на $\sqrt{N(z_0)}$; иными словами, такое умножение является евклидовым подобием (рис. 2.1).

В том важном случае, когда $N(z_0)=1$, отображение $z\to z_0z$ является евклидовым движением, или *изометрией*. Более того, до всякого такого «единичного комплексного числа» z_0 можно добраться из 1 по непрерывному пути, идущему полностью по единичным числам (рис. 2.2), так что это движение можно получить непрерывной деформацией из тождественного. Такие движения называются *поворотами*.

Стандартная формула для поворота

$$x'=x\cos\theta-y\sin\theta,$$
$$y'=x\sin\theta+y\cos\theta$$

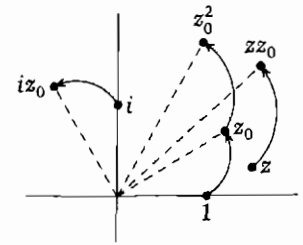


Рис. 2.1. Евклидово подобие $z \to zz_0$

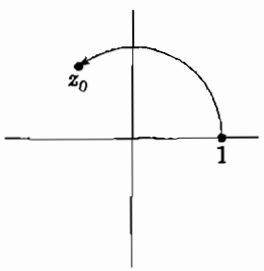


Рис. 2.2. Евклидово движение можно соединить путем с тождественным отображением

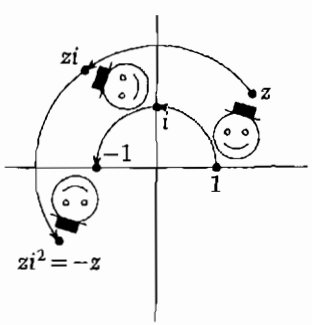


Рис. 2.3. Евклидов поворот $z \to zi$

немедленно вытекает из правила умножения

$$(\cos\theta + i\sin\theta)(x+iy) = \\ = (x\cos\theta - y\sin\theta) + i(x\sin\theta + y\cos\theta)$$

и определений тригонометрических функций (рис. 2.3).

А вот *отражения* — это другой тип евклидовых движений; примером такого движения служит отображение

$$x' = x,$$
$$y' = -y,$$

соответствующее комплексному сопряжению

$$\overline{x+iy} = x - iy.$$

Теорема 1. *Если u — единичное комплексное число, то отображение $z \to uz$ является поворотом, а отображение $z \to u\bar{z}$ является отражением.*

Матрицы этих отображений суть

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix},$$

а их определители равны 1 и -1, так что преобразования лежат в SO_2 и $GO_2 \setminus SO_2$ соответственно.

Более того, всякий элемент (a_{ij}) двумерной ортогональной группы GO_2 принадлежит к одному из этих двух типов. В самом деле, первое из условий ортогональности, а именно $a_{11}^2 + a_{12}^2 = 1$, влечет равенства $a_{11} = \cos\theta$, $a_{12} = \sin\theta$ для некоторого θ, а из остальных условий вытекает, что $a_{21} = \mp\sin\theta$, $a_{22} = \pm\cos\theta$.

Итак, мы описали двумерные ортогональные группы.

Теорема 2. *SO_2 состоит из умножений $z \to uz$ на единичные комплексные числа, а GO_2 состоит из тех же умножений вкупе с $z \to u\bar{z}$.*

Из этой теоремы следует топологическое описание SO_2 как окружности, состоящей из вещественных углов θ, рассматриваемых по модулю 2π. Группа GO_2 имеет две компоненты, каждая из которых является окружностью.

§ 2.2. Конечные подгруппы в GO_2 и SO_2

Рассмотрим наименьшее положительное θ, для которого поворот на θ принадлежит заданной конечной подгруппе $G \subset SO_2$. Это θ имеет вид $\frac{2\pi}{m}$, поскольку если m — наименьшее целое положительное число, для которого $m\theta \geqslant 2\pi$, то должно выполняться равенство $m\theta = 2\pi$, поскольку в противном случае, если $m\theta = 2\pi + \theta'$, то $0 < \theta' < \theta$.

Стало быть, группа G порождена поворотом на $2\pi/m$, поскольку если она содержит поворот на любой другой угол θ, то θ можно представить в виде кратного $2\pi/m$ плюс положительный угол-«остаток» φ, строго меньший, чем $2\pi/m$, — противоречие. Такая группа называется поворотной, или хиральной, точечной группой; в «орбифолдной нотации» (см. приложение) она обозначается $m\bullet$.

Итак, мы доказали вот что.

Теорема 3. *Всякая конечная подгруппа в SO_2 есть группа $m\bullet$, состоящая из поворотов на углы, кратные $2\pi/m$.*

Подгруппы в SO_2 называются *хиральными* (от слова, означающего «рука»), поскольку, действуя на двумерных объектах, они не могут перевести правую руку в левую (рис. 2.4). Соответственно, подгруппы в GO_2, не содержащиеся в SO_2, называются *ахиральными*, поскольку они переводят одну руку в другую (рис. 2.5).

Добавляя отражение относительно любой прямой, проходящей через начало координат, мы получим ахиральную точечную группу, обо-

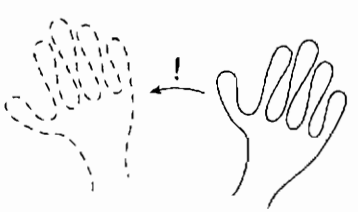


Рис. 2.4. Двумерная хиральность

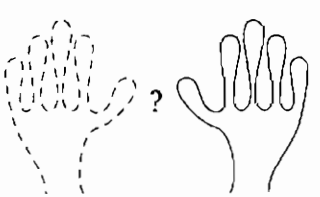


Рис. 2.5. Двумерная ахиральность

значаемую в орбифолдной нотации через $*m\bullet$. Легко видеть, что имеет место такой факт.

Теорема 4. *Общая конечная подгруппа в* GO_2 *есть* $*m\bullet$.

В самом деле, ее хиральная подгруппа индекса 2 должна иметь вид $m\bullet$ для некоторого m.

§ 2.3. Гауссовы целые числа

Гаусс ввел для комплексных чисел понятие, аналогичное понятию целости для действительных чисел. Именно, комплексное число $x+iy$ называется *гауссовым целым*, если его действительная и мнимая части — обыкновенные целые числа. Гауссовы числа образуют кольцо, поскольку сумма, разность и произведение двух гауссовых чисел — тоже гауссово целое.

Геометрически гауссовы числа образуют квадратную решетку (см. рис. 2.6), на которой два ближайших числа отличаются на одну из гауссовых единиц $1, -1, i, -i$.

Возможно, самое интересное свойство гауссовых чисел — теорема об однозначном разложении на множители.

Теорема 5. *Всякое ненулевое гауссово число, отличное от единиц, имеет разложение* $\pi_1\pi_2\ldots\pi_k$ *на гауссовы простые. От каждого такого*

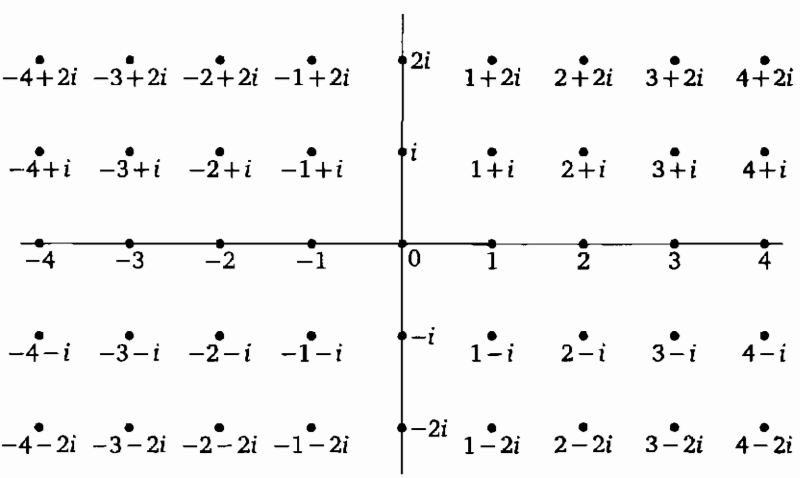


Рис. 2.6. Гауссовы целые числа

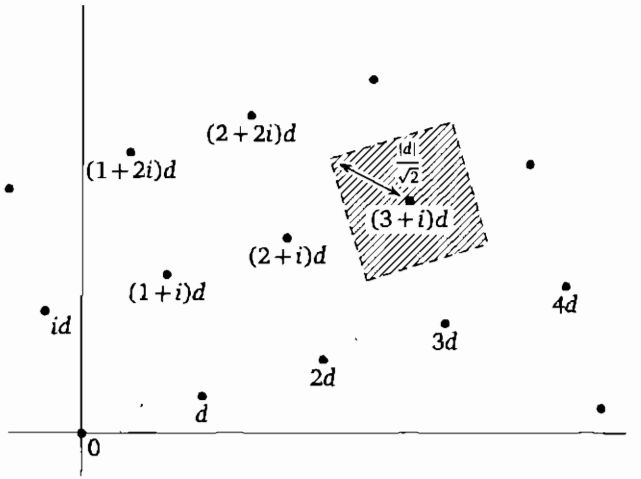


Рис. 2.7. Максимальный остаток для гауссовых чисел

разложения можно перейти к любому другому с помощью следующих операций:

— *перестановка простых множителей;*

— *перенос единиц: замена* π_s, π_{s+1} *на* $\pi_s u$, $\bar{u}\pi_{s+1}$.

Здесь *гауссовым простым* называется гауссово целое число, которое обладает тем свойством, что при любом его разложении на два множителя *один из сомножителей является единицей*[1].

Когда мы в главе 1 доказывали теорему об однозначном разложении для обыкновенных целых чисел, мы пользовались только тем, что одно число можно поделить на другое и получить остаток, меньший делителя. Если разрешить отрицательные остатки, то можно оказаться на расстоянии, не превосходящем $\frac{1}{2}|d|$, от кратного числа d, на которое мы делим (см. рис. 1.1, на котором $|d|$ — расстояние от нуля до d).

Рис. 2.7 показывает, почему всякое гауссово целое число находится на расстоянии, не превосходящем $|d|/\sqrt{2}$, от кратного данного гауссова числа d. Поскольку $1/\sqrt{2}$ меньше единицы, остаток меньше по размеру, чем делитель, так что наше доказательство единственности разложения проходит и для гауссовых целых.

Единицы кольца гауссовых целых — корни четвертой степени из единицы. Ученик Гаусса Эйзенштейн предложил другую числовую си-

[1] В авторский текст внесены некоторые уточнения. — *Прим. перев.*

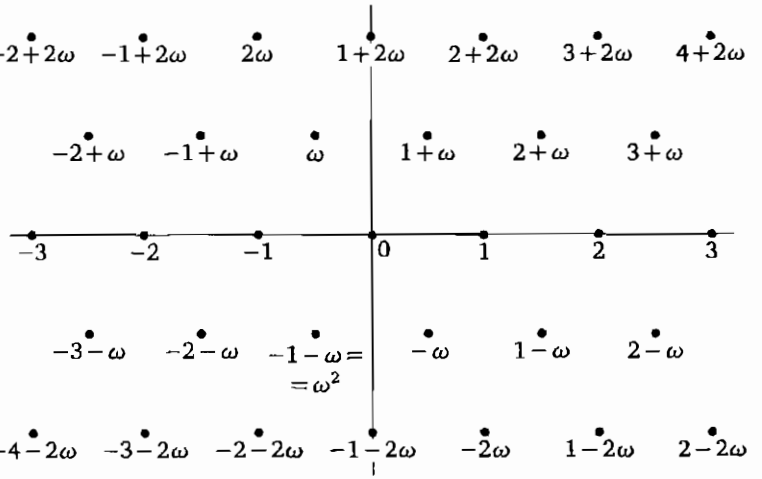


Рис. 2.8. Эйзенштейновы целые числа

стему, в которой используются корни из единицы третьей и шестой степени. Это *эйзенштейновы целые числа*, являющиеся суммами вида $a+b\omega$ (a, $b\in\mathbb{Z}$), где $\omega=(-1+i\sqrt{3})/2$ — один из корней уравнения $x^3=1$ (два других корня суть 1 и $\omega^2=(-1-i\sqrt{3})/2$). Эйзенштейновы числа образуют треугольную решетку (рис. 2.8). Рис 2.9 аналогичен рис. 2.7; он показывает, что всякое целое эйзенштейново число отстоит на расстояние $\frac{1}{\sqrt{3}}|d|$ от некоторого кратного данного эйзенштейнова целого, так что и для этих чисел имеет место однозначность разложения на простые множители.

§ 2.4. Клейновы целые числа

Имеется знаменитая теорема, доказанная К. Хегнером и передоказанная А. Бейкером и Х. М. Старком, которая утверждает, что существует только девять мнимых квадратичных полей, а именно поля с дискриминантами[1]

$$3,\ 4,\ 7,\ 8,\ 11,\ 19,\ 43,\ 67,\ 163.$$

После чисел Эйзенштейна (дискриминант 3) и Гаусса (дискриминант 4), простейшее кольцо называется *клейновым*; оно состоит из

[1]Здесь и ниже автор меняет знак дискриминанта по сравнению с традиционным определением. — *Прим. перев.*

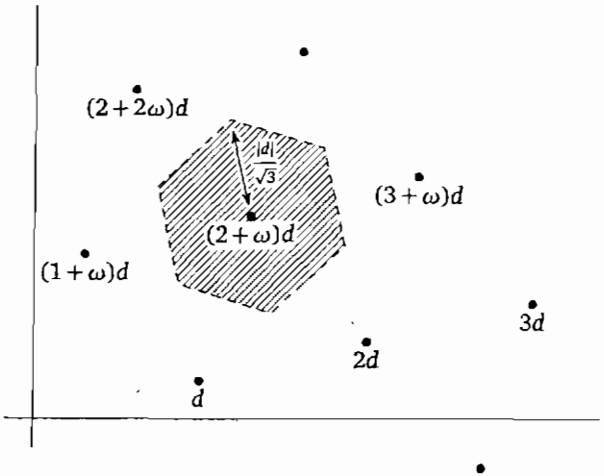


Рис. 2.9. Максимальный остаток для эйзенштейновых чисел

чисел вида $a+b\lambda$ $(a, b\in\mathbb{Z})$, где $\lambda=\frac{-1+\sqrt{-7}}{2}$ (рис. 2.10). Наиболее важные особенности этого кольца состоят в том, что в нем есть всего две единицы ±1 и что 2 разлагается в произведение $\lambda\mu$, где $\mu=\frac{-1-\sqrt{-7}}{2}$.

Приложение
Двумерные пространственные группы

В основной части этой главы мы уже обсудили двумерные точечные группы. Сейчас мы вкратце обсудим 17 двумерных пространственных групп, поскольку их теория тесно связана с теорией трехмерных точечных групп, о которой пойдет речь в следующей главе.

В *орбифолдной нотации* эти 17 групп имеют такой вид:

*632, 632;

*442, 4*2, 442;

*333, 3*3, 333;

*2222, 2*22, 22*, 22×, 2222;

**, *×, ××, ∘.

Здесь

— цифра $A\geqslant 2$, перед которой не стоит звездочка, обозначает тип точки с локальной симметрией типа $A\bullet$;

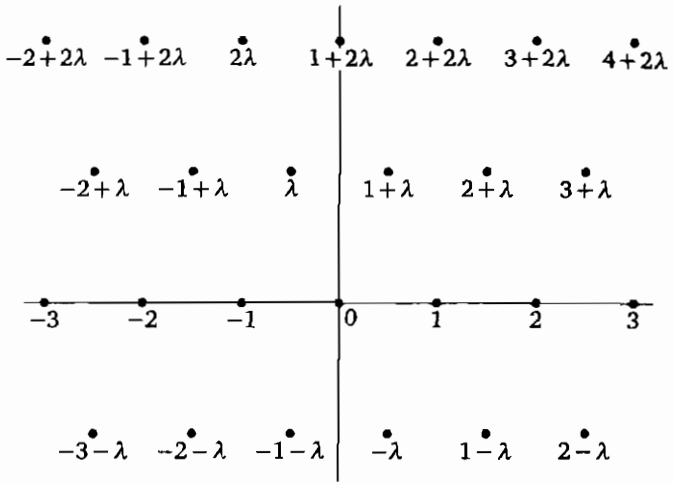


Рис. 2.10. Клейново кольцо

— последовательность цифр $a_1 \geqslant 2$, $a_2 \geqslant 2$, ..., $a_k \geqslant 2$ обозначает тип калейдоскопа, т. е. связной системы прямых-зеркал, на которых расположены различные типы точек с локальными симметриями $*a_1\bullet$, $*a_2\bullet$, ..., $*a_k\bullet$;

— символ $\times$ обозначает «чудо», т. е. наличие обращающего ориентацию пути, не пересекающего ни одного зеркала;

— символ $\circ$ обозначает «странность», т. е. повторение мотива, не встречавшегося ранее.

(Более точных определений мы здесь не даем.)

У каждого из этих значков есть своя стоимость:

Значок	Стоимость
A	$(A-1)/A$
$*$	1
a_i после звездочки	$(a_i-1)/2a_i$
$\times$	1
$\circ$	2

«Волшебная теорема» утверждает, что вышеперечисленные 17 групп — в точности те, общая стоимость которых равна 2.

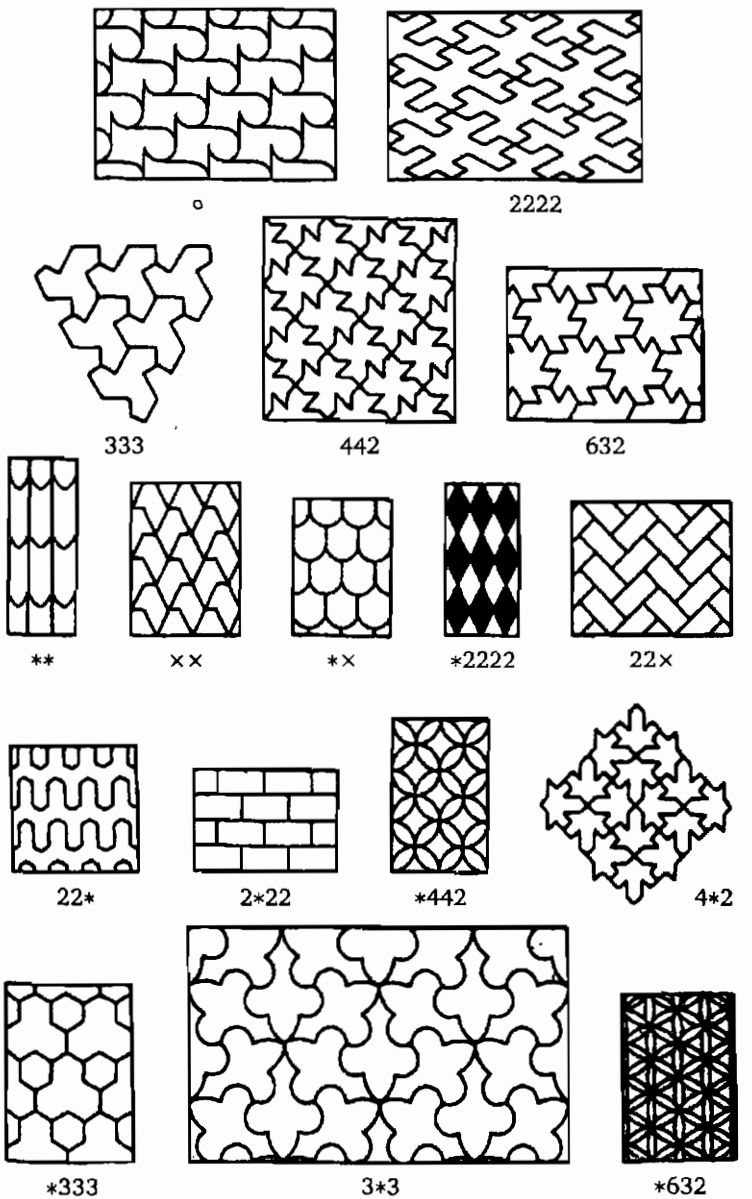


Рис. 2.11. Мы воспроизводим иллюстрацию Д. Пойа 1924 года, на которой представлены 17 различных групп симметрий плоскости; обозначения для групп записаны в орбифолдной нотации

Доказательство «волшебной теоремы» связывает эти значки со свойствами *орбифолда* — плоскости, рассматриваемой по модулю действия группы. При такой интерпретации $*a_1a_2...a_k$ обозначает границу с k углами $\frac{\pi}{a_1}$, $\frac{\pi}{a_2}$, ..., $\frac{\pi}{a_k}$, цифра A (не после звездочки) соответствует конической точке с углом $\frac{2\pi}{A}$, $\times$ — это кросс-кэп, а $\circ$ — это ручка.

Кватернионы и их приложения к трех- и четырехмерной геометрии

Кватернионы — это формальные выражения вида $x_0+x_1i+x_2j+x_3k$ (где x_0, x_1, x_2, x_3 действительны), над которыми проводятся операции по следующим правилам:

$$(x_0+x_1i+x_2j+x_3k)+(y_0+y_1i+y_2j+y_3k)=$$
$$=(x_0+y_0)+(x_1+y_1)i+(x_2+y_2)j+(x_3+y_3)k;$$

$$(x_0+x_1i+x_2j+x_3k)(y_0+y_1i+y_2j+y_3k)=$$
$$=(x_0y_0-x_1y_1-x_2y_2-x_3y_3)+$$
$$+(x_0y_1+x_1y_0+x_2y_3-x_3y_2)i+$$
$$+(x_0y_2-x_1y_3+x_2y_0+x_3y_1)j+$$
$$+(x_0y_3+x_1y_2-x_2y_1+x_3y_0)k;$$

иными словами, кватернионы образуют алгебру над действительными числами, порожденную базисными единицами i, j и k, удовлетворяющими знаменитым уравнениям Гамильтона

$$ij=k,\quad jk=i,\quad ki=j,$$
$$ji=-k,\quad kj=-i,\quad ik=-j,$$
$$i^2=j^2=k^2=-1.$$

Кватернионы и трехмерные группы

В предыдущей главе мы перечислили все конечные подгруппы в SO_2 и GO_2 и связали их с комплексными числами. В этой главе наша цель — перечислить все конечные группы в SO_3 и GO_3 и связать их с кватернионами.

§ 3.1. Кватернионы и трехмерные повороты

Как связаны кватернионы с трехмерной геометрией? В конечном счете эта связь проистекает из того факта, что норма произведения кватернионов равна произведению норм. Отсюда следует, что

$$N(q_1 v q_2) = N(q_1)N(v)N(q_2),$$

и тем самым отображение $v \to q_1 v q_2$ есть подобие четырехмерного евклидова пространства, умножающее длины на $\sqrt{N(q_1)N(q_2)}$; это подобие является движением, если $N(q_1)N(q_2) = 1$. Если это движение сохраняет $e = 1$, то оно переводит в себя трехмерное пространство, ортогональное к e, типичный элемент которого есть вектор вида $xi + yj + zk$ («без действительной части»); мы будем называть такие кватернионы *векторами* (трехмерными). Поскольку e сохраняется, если $q_1 q_2 = 1$, получаем следующую теорему.

Теорема 1. *Отображение* $[q]\colon v \to q^{-1}vq$ *является движением трехмерного евклидова пространства.*

На самом деле такое движение является *простым поворотом*, т. е. оно оставляет на месте некоторый вектор (в размерности n простой поворот оставляет на месте элементы $(n-2)$-мерного пространства). Точнее говоря, в приложении к этой главе мы покажем, что если $q = r(\cos\theta + u\sin\theta)$, где u — единичный трехмерный вектор, то $[q]$ является поворотом относительно u на угол 2θ.

Поскольку всякий простой поворот имеет такой вид при подходящих u и θ, отсюда немедленно вытекает следующая теорема.

Теорема 2 (Эйлера о поворотах). *Произведение двух простых поворотов является простым поворотом.*

В самом деле, произведение простых поворотов

$$x \to q_1^{-1} x q_1 \quad \text{и} \quad x \to q_2^{-1} x q_2$$

есть $x \to (q_1 q_2)^{-1} x (q_1 q_2)$, что также является простым поворотом. Мы дадим геометрическое доказательство теоремы Эйлера в следующем параграфе.

Поскольку в главе 1 мы показали, что специальная ортогональная группа порождена простыми поворотами, справедлива такая теорема.

Теорема 3. *Всякий элемент SO_3 является простым поворотом и имеет вид $x \to q^{-1} x q$, где q — некоторый кватернион.*

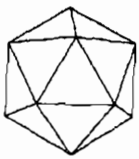
Сразу видно, что при таком соответствии между кватернионами и поворотами одному повороту соответствует бесконечно много кватернионов, поскольку, конечно, все ненулевые скалярные кратные данного кватерниона соответствуют одному и тому же повороту. Мы уменьшим эту неопределенность, потребовав, чтобы q был единичным кватернионом; при этом одному повороту будут соответствовать два кватерниона, поскольку двум противоположным единичным кватернионам q и $-q$ соответствует один и тот же поворот.

Теорема 4. *Отображение, переводящее q в сопряжение $[q]\colon x \to q^{-1} x q$, является гомоморфизмом из группы единичных кватернионов в SO_3, при котором одному элементу SO_3 соответствуют два кватерниона.*

На традиционном языке это означает, что множество единичных кватернионов является «двулистным накрытием» группы SO_3; это накрытие называется *спинорной группой* Spin_3. Спинорные группы существуют во всех размерностях, но общего определения мы не приводим, поскольку это увело бы нас слишком далеко в сторону. В последующих главах мы встретимся еще с тремя спинорными группами: Spin_4, Spin_7 и Spin_8.

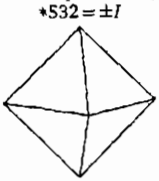
Один из тонких моментов нашего предмета состоит в том, что в нем встречаются несколько различных «2-1-отображений» (отображений, при которых у каждого элемента два прообраза). Так, мы видели, что два единичных кватерниона $+q$ и $-q$ задают одно и то же трехмерное движение $[q]\colon x \to \bar{q} x q$. Однако же два n-мерных движения $+g, -g \in \mathrm{GO}_n$ задают одно и то же проективное движение $[g] \in \mathrm{PGO}_n$. Результат последовательного применения этих двух операций к q мы будем обозначать $[\![q]\!]$, а не $[[q]]$.

В оставшейся части этой главы мы описываем конечные подгруппы в GO_3 (см. рис. 3.1) и то, как они представляются с помощью ква-

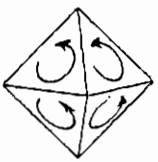


Голоикосаэдральная группа
$*532 = \pm I$

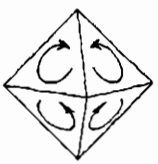
Хироикосаэдральная группа
$532 = +I$



Голооктаэдральная группа
$*432 = \pm O$



Хирооктаэдральная группа
$432 = +O$

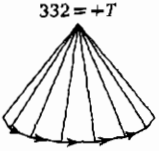


Пиритоэдральная группа
$3*2 = \pm T$

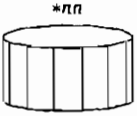
Голотетраэдральная группа
$*332 = TO$

Хиротетраэдральная группа
$332 = +T$

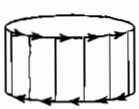
Голопирамидальная группа
$*nn$



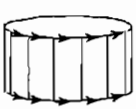
Хиропирамидальная группа
nn



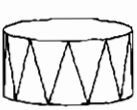
Голопризматическая группа
$*22n = \pm D(n)/DD(2n)$



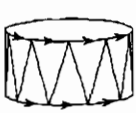
Хиропризматическая группа
$22n = D(n)$
= хиро-антипризматическая группа



Пропризматическая группа
$n* = \pm C(n)/CC(2n)$



Голо-антипризматическая
группа $2*n = DD(2n)/\pm D(n)$



Про-антипризматическая
группа $n\times = CC(2n)/\pm C(n)$

Рис. 3.1. Связь трехмерных групп с полиэдрами

тернионов. Начнем мы с того, что изложим в следующем параграфе некоторые полезные сведения из сферической геометрии.

§ 3.2. Немного сферической геометрии

Начнем с такой теоремы.

Теорема 5. *Всякая конечная группа движений n-мерного евклидова пространства имеет неподвижную точку.*

В самом деле, если $P_1, P_2, \ldots, P_N$ — образы произвольной точки P_1, то точка $\frac{1}{N}(P_1 + P_2 + \ldots + P_N)$ очевидным образом неподвижна.

Итак, с этого момента мы будем считать, что интересующая нас конечная группа имеет начало координат неподвижной точкой, а описывать группу мы будем в терминах ее действия на единичной сфере.

Теорема 6. *Произведение простых поворотов относительно вершин сферического треугольника на углы, равные удвоенным углам этого треугольника (при выборе знаков как на рис. 3.2) является тождественным преобразованием.*

В самом деле, если P, Q и R — отражения от сторон треугольника, то три поворота имеют вид PQ, QR и RP (где PQ означает «сначала P, затем Q»), откуда

$$PQ \cdot QR \cdot RP = PQ^2R^2P = PP = 1.$$

В частности, коль скоро мы всегда можем «дополнить до треугольника» поворот относительно точки A (на угол 2α) и поворот относительно точки B (на угол 2β), как на рис. 3.3, мы получаем геометрическое доказательство теоремы Эйлера о поворотах.

Итак, группа, порожденная простыми поворотами, состоит из одних простых поворотов. Такие *группы поворотов* будут наиболее важны в дальнейшем; далее мы увидим, что каждую из них можно породить двумя поворотами.

Группа отражений — это группа, порожденная отражениями.

Теорема 7. *Всякая группа, порожденная двумя поворотами R_1 и R_2, является подгруппой индекса 2 в некоторой группе отражений.*

Мы получим искомую группу отражений из данной группы поворотов, добавив к этой последней элемент M, являющийся отражением относительно плоскости, содержащей оси поворотов R_1 и R_2. Получающаяся группа действительно является группой отражений, поскольку можно записать равенства $R_1 = MM_1$, $R_2 = MM_2$, где M_1 и M_2 — еще два отражения, равные MR_1 и MR_2 соответственно. Всякий элемент в этой группе отражений можно записать как слово в алфавите

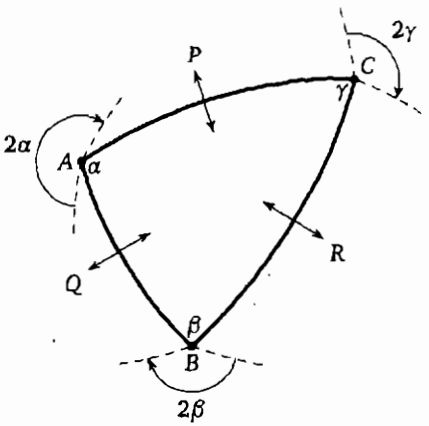


Рис. 3.2. PQ — поворот относительно A на угол 2α, QR — поворот относительно B на угол 2β, RP — поворот относительно C на угол 2γ; направления поворотов указаны на рисунке

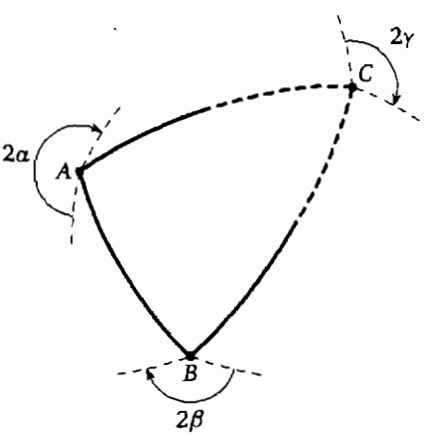


Рис. 3.3. Произведение поворотов относительно A на угол 2α и относительно B на угол 2β — дополняющий треугольник поворот относительно C на угол -2γ

$\{R_1, R_1^{-1}, R_2, R_2^{-1}, M\}$, причем можно, пользуясь соотношениями $R_1M = MR_1^{-1}$ и $R_2M = MR_2^{-1}$, перенести все вхождения M в начало формулы, а затем, пользуясь соотношением $M^2 = 1$, привести к виду w или Mw, где w лежит в подгруппе, порожденной R_1 и R_2.

Теорема 8. *Всякая конечная группа отражений порождена отражениями относительно сторон выпуклого сферического многоугольника с углами вида* $\frac{\pi}{n}$.

В самом деле, посмотрим, что высекается на единичной сфере неподвижными плоскостями всех отражений. Ясно, что они разбивают сферу на некоторое количество выпуклых многоугольников. Кроме того, если у этих многоугольников имеется общая сторона, то они переходят друг в друга при отражении относительно этой стороны. Это показывает, что все многоугольники конгруэнтны и что отражения, соответствующие одному из них, порождают отражения, соответствующие его соседу; итерируя, получаем, что они порождают всю группу.

В орбифолдной нотации группа, порожденная отражениями от сторон многоугольника с углами $\frac{\pi}{a}, \frac{\pi}{b}, \ldots, \frac{\pi}{z}$, обозначается $*ab\ldots z$. Мы позволим себе при необходимости добавлять или удалять цифры 1 в таких символах, поскольку при этом упрощаются общие формулировки.

Теорема 9 (о сферическом избытке).

$$A+B+C=\pi+\triangle,$$
$$A+B+C+D=2\pi+\square,$$
$$A+B+C+D+E=3\pi+\pentagon,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots,$$

где через $\triangle$ ($\square$, $\pentagon$, ...) *обозначена площадь треугольника (четырехугольника, пятиугольника...) с углами A, B, C (D, E, ...).*

Доказательство. На рис. 3.4 показано, как свести общий случай к случаю треугольника; доказательство для треугольника представлено на рис. 3.5 и 3.6. □

§ 3.3. Перечисление групп поворотов

Сначала перечислим соответствующие группы отражений.

Теорема 10. *Всякая конечная группа отражений принадлежит к одному из следующих типов:*

$$*532, \quad *432, \quad *332, \quad *22n, \quad *nn \quad (n \geqslant 1).$$

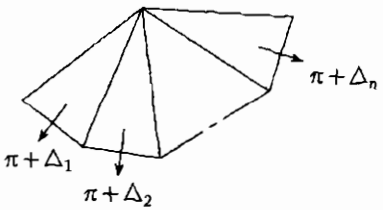


Рис. 3.4. Триангуляция многоугольника и сумма его углов

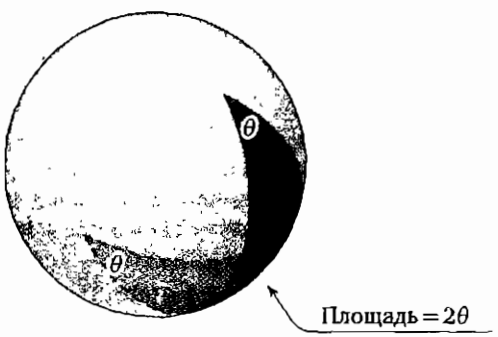


Рис. 3.5. Очевидно, что площадь этой лунки пропорциональна θ; она равна 2θ, поскольку площадь сферы равна 4π

В самом деле, в нашей ситуации сумма углов k-угольника не превосходит $\frac{k\pi}{2}$, но в силу предыдущей теоремы она должна быть больше, чем $(k-2)\pi$, так что $k \leqslant 3$.

Если теперь $k=3$, то наибольший угол должен равняться $\frac{\pi}{2}$ (в противном случае сумма углов будет не превосходить $\frac{\pi}{3}+\frac{\pi}{3}+\frac{\pi}{3}=\pi$), следующий по величине угол должен равняться $\frac{\pi}{2}$ или $\frac{\pi}{3}$ (иначе сумма углов будет не превосходить $\frac{\pi}{2}+\frac{\pi}{4}+\frac{\pi}{4}=\pi$), и наконец, если два наибольших угла равны $\frac{\pi}{2}$ и $\frac{\pi}{3}$, то третий угол должен быть не меньше чем $\frac{\pi}{5}$ (иначе сумма углов будет не превосходить $\frac{\pi}{2}+\frac{\pi}{3}+\frac{\pi}{6}=\pi$). Отсюда получаются случаи $*22n$, $*233$, $*234$ и $*235$.

Если $k=2$, то многоугольник представляет собой лунку из двух больших кругов, два угла которой равны друг другу; если они равны $\frac{\pi}{n}$, то группа есть $*nn$ (это включает и случай $n=1$, когда «многоугольник» представляет собой полусферу).

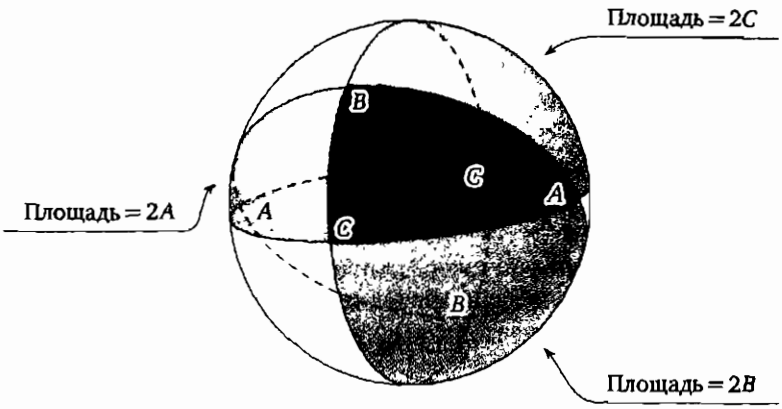


Рис. 3.6. Сфера (общей площадью 4π) разбита на восемь треугольников, причем общая площадь четырех затемненных треугольников равна 2π (поскольку такова же сумма площадей треугольников, им противоположных). Сумма площадей трех затемненных лунок равна $2A+2B+2C$, и эта сумма равна $2\pi+2\Delta$, поскольку общий треугольник с площадью Δ считается трижды

Ключевую роль в этой главе играет следующий факт.

Теорема 11. *Конечные группы поворотов суть*

$$532, \quad 432, \quad 332, \quad 22n, \quad nn \quad (n \geqslant 1).$$

В самом деле, приведенное выше рассуждение показывает, что утверждение верно для групп, порожденных не более чем двумя поворотами.

Может ли существовать группа G, которую двумя поворотами породить нельзя? Нет, поскольку любые два отражения из группы порождают одну из групп, перечисленных выше, что ограничивает сверху расстояния между центрами поворотов, и тогда центр нового поворота окажется недопустимо близок к центру одного из уже имеющихся (см. рис. 3.7).

Итак, мы нашли бесконечно много групп, но нам будет удобнее ссылаться на них как на «пять групп» (две из которых зависят от параметра).

§ 3.4. Обсуждение групп

Первые три группы называются *группами многогранников*, поскольку они состоят из поворотов, переводящих в себя подходящий пра-

вильный многогранник; две остальные группы называются *осевыми группами поворотов*, поскольку они оставляют на месте целую ось.

Как абстрактные группы они изоморфны различным хорошо известным группам $G(n)$ — подгруппам группы перестановок n символов (рис. 3.8). Эти группы таковы:

$532 = I = I_{60} \simeq A(5)$ — *группа икосаэдра*;
$432 = O = O_{24} \simeq S(4)$ — *группа октаэдра*;
$332 = T = T_{12} \simeq A(4)$ — *группа тетраэдра*;
$22n = D = D_{2n} \simeq D(n)$ — *диэдральная группа*;
$nn = C = C_n \simeq C(n)$ — *циклическая группа*.

Эти традиционные названия могут привести к путанице. В дальнейшем мы снабдим их префиксом «хиро-», чтобы отличить их от «голо»-групп, являющихся полными группами симметрий соответствующих многогранников.

В литературе наблюдается некоторая путаница с обозначениями, поскольку специалисты по теории групп обычно обозначают через D_{2n} диэдральную группу порядка $2n$, а в обозначениях, предпочитаемых геометрами, указывается параметр n. Поскольку мы и геометры, и специалисты по теории групп, мы будем обозначать ее и так, и этак: иногда D_{2n}, а иногда и $D(n)$.

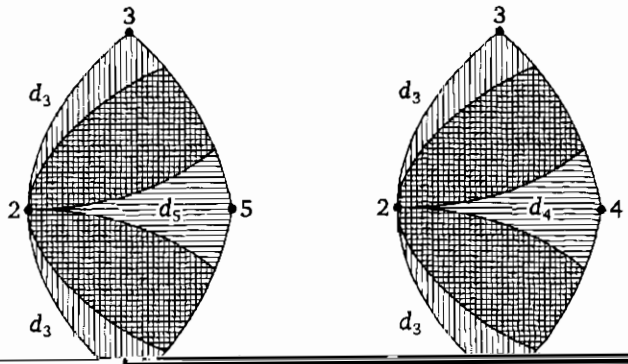
§ 3.5. Конечные группы кватернионов

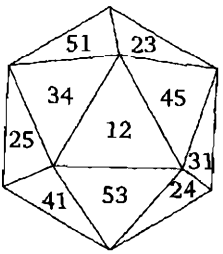
Сделаем небольшое отступление и перечислим конечные группы кватернионов. Отображение, переводящее единичный кватернион q в поворот $[q]: x \to \bar{q}xq$ (и переводящее два кватерниона в один поворот), переводит конечную группу Q кватернионов в группу $[Q] = \{[q] \mid q \in Q\}$, которая должна быть одной из групп C, D, T, O или I. Порядок группы Q будет либо в два раза больше, чем порядок группы $[Q]$ (если -1 лежит в Q), либо совпадать с ним (в противном случае).

Случаи, в которых $-1 \in Q$, обозначим через $2C_n$, $2D_n$, $2T$, $2O$, $2I$, где через $2G$ обозначено $\{q \mid [q] \in G\}$. Если $-1 \notin Q$, то G не может содержать поворот g порядка 2, поскольку если $[q] = g$, то $q^2 = -1$ должно лежать в Q; этому условию удовлетворяют только группы C_n (с нечетным n), являющиеся образами группы Q порядка n (например, $\langle e^{2\pi i/n} \rangle$), которую мы обозначим $1C_n$. Подведем итоги.

Теорема 12. *Конечные группы кватернионов суть*

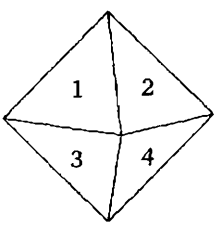
$$2I,\ 2O,\ 2T,\ 2D_{2n},\ 2C_n,\ 1C_n \quad (n \text{ нечетно}).$$


3
d_3
2
d_5
5
d_3
3
d_3
2
d_4
4
d_3



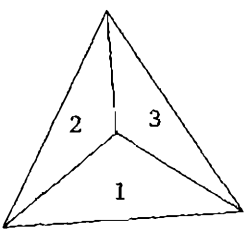
На грани, противоположной к ij, написано ji

Группа икосаэдра I состоит из поворотов, переводящих в себя икосаэдр. Если написать на гранях пары чисел от 1 до 5, как показано на рисунке, то получится изоморфизм этой группы с группой $A(5)$ — знакопеременной группой на пяти символах.



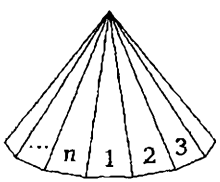
Надписи на противоположных гранях совпадают

Группа октаэдра O изоморфна $S(4)$.



На задней грани написано 4

Группа тетраэдра T изоморфна $A(4)$.



Пирамида

Циклическая группа $C = C_n$ изоморфна $C(n)$.

Диэдральная группа $D = D_{2n}$ состоит из поворотов, переводящих в себя призму, прямоугольные грани которой занумерованы числами $1, \ldots, n$. Эта группа изоморфна $D(n) = \langle (1\,2 \ldots n), (1\,n)(2\,n-1) \ldots \rangle$.

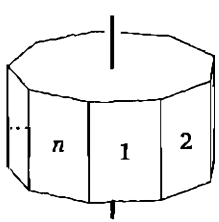


Рис. 3.8. Группы многогранников и осевые группы поворотов изоморфны различным $G(n)$, являющимся группами перестановок n символов

Образующие этих групп приведены ниже:

$$
\begin{aligned}
2I &= \langle i_I, \omega \rangle, & i_I &= \frac{i+\sigma j+\tau k}{2},\ \sigma = \frac{\sqrt{5}-1}{2},\ \tau = \frac{\sqrt{5}+1}{2},\\
2O &= \langle i_O, \omega \rangle, \quad \text{где} & i_O &= \frac{j+k}{\sqrt{2}},\ \omega = \frac{-1+i+j+k}{2},\\
2T &= \langle i_T, \omega \rangle, & i_T &= i,\\
2D_{2n} &= \langle e_n, j \rangle, & e_n &= e^{\pi i/n}.\\
2C_n &= \langle e_n \rangle,\\
1C_n &= \langle e_{n/2} \rangle,
\end{aligned}
$$

§ 3.6. Хиральное и ахиральное, диплоидное и гаплоидное

Термин «хиральный» (*происходящий* от греческого слова, означающего «рука») был введен в научный обиход не позднее 1896 года лордом Кельвином; он предназначался для наименования объектов, которые нельзя совместить со своим зеркальным отражением. Для остальных объектов использовались термины «ахиральный» или «амфихиральный» (двуручный).

Мы будем использовать эти термины не только для самих объектов, но и для их групп симметрий. Тем самым группа симметрий называется *хиральной*, если все входящие в нее преобразования являются движениями, сохраняющими ориентацию, и *ахиральной* в противном случае[1].

Все симметрии конечного физического объекта оставляют на месте его центр *тяжести*; если принять этот последний за начало координат, то симметрии будут представляться ортогональными матрицами, определители которых обязательно равны ± 1. Группа хиральна, если каждый из этих определителей равен $+1$, и ахиральна, если в ней есть элемент с определителем -1.

Для обозначения понятия, двойственного к хиральности, мы позаимствуем парочку терминов у биологов. Будем говорить, что группа является *диплоидной* («составленной из пар»), если она содержит центральную симметрию $-1\colon x \to -x$, поскольку матрицы в такую группу входят парами $\pm g$. Все остальные группы называются *гаплоидными* («составленными из единичных объектов»).

[1]Мы будем придерживаться этой стандартной терминологии, невзирая на то обстоятельство, что каждая из трехмерных «хиральных групп» совпадает со своим зеркальным образом. Мы обсудим это подробнее в главе 4.

По отношению к введенным понятиям все группы должны были бы делиться на четыре класса: хиральные диплоидные, хиральные гаплоидные, ахиральные диплоидные и ахиральные гаплоидные. Один из этих классов, однако же, не встречается: коль скоро мы работаем в нечетной размерности, центральная симметрия -1 имеет определитель -1, так что диплоидная группа должна быть ахиральной. Стало быть, имеется только три класса:

— *диплоидные* группы (с неизбежностью ахиральные);

— *хиральные* группы (с неизбежностью гаплоидные);

— *гибридные* группы (т. е. ахиральные, но гаплоидные).

На нескольких следующих страницах мы воспользуемся этими терминами для классификации групп.

§ 3.7. Проективные, или эллиптические, группы

При *проективном* подходе два элемента отождествляются, если один из них получается из другого с помощью умножения на скаляр. В нашем случае этот множитель может быть равен только ± 1, так что при проективном подходе мы заменяем $+g$ и $-g$ на один и тот же элемент $[g]$.

Напомним, что n-мерная полная ортогональная группа GO_n состоит из всех ортогональных $(n \times n)$-матриц, или, что равносильно, из всех движений n-мерного евклидова пространства, оставляющих на месте начало координат, в то время как n-мерная специальная ортогональная группа SO_n состоит из всех элементов GO_n с определителем 1. При проективном подходе из этих групп получаются PGO_n и PSO_n — n-мерные проективная ортогональная и проективная специальная ортогональная группы.

Впрочем, если n нечетно, то $\det(-1) = -1$, откуда следует, что $\mathrm{PGO}_n = \mathrm{PSO}_n$ и $\mathrm{PSO}_n \simeq \mathrm{SO}_n$. Так получается по той причине, что только один из двух элементов g и $-g$ имеет определитель 1, так что образ каждого из таких элементов при проективизации есть образ «положительного» элемента, а при проективизации группы SO_n ничего отождествлять не требуется. Применяя это соображение к конечным подгруппам, получаем следующий результат.

Теорема 13. *Конечные подгруппы в группе* $\mathrm{PGO}_3 = \mathrm{PSO}_3$ *суть*

$$[I_{60}], \quad [O_{24}], \quad [T_{12}], \quad [D_{2n}], \quad [C_n].$$

Типичный элемент $[g]$ каждой из этих групп представляется парой противоположных матриц: одна из них имеет определитель 1, и мы обозначим ее g, а вторая, обозначаемая $-g$, имеет определитель -1.

Зная проективные группы, мы можем перечислить все конечные подгруппы в GO_3 способом, описанным в следующем параграфе.

§ 3.8. Проективные группы расскажут нам все

Хиральные группы. Каждая из таких групп состоит из элементов вида $+g$, где $[g]$ пробегает некоторую проективную группу $[G]$. Мы будем обозначать такие группы через $+G$. Возможные случаи таковы:

$+C$ — *циклическая* группа поворотов;
$+D$ — *диэдральная* группа поворотов;
$+T$ — *тетраэдральная* группа поворотов;
$+O$ — *октаэдральная* группа поворотов;
$+I$ — *икосаэдральная* группа поворотов.

На языке кватернионов: $+G$ состоит из отображений $x \to q^{-1}xq$, где $q \in 2G$.

Диплоидные группы. Такие группы должны состоять из пар элементов $+g$, $-g$, где $[g] \in [G]$. Мы будем обозначать такие группы через $\pm G$. Возможные случаи таковы:

$\pm C$ — *диплоциклическая* группа;
$\pm D$ — *диплодиэдральная* группа;
$\pm T$ — *диплотетраэдральная* группа;
$\pm O$ — *диплооктаэдральная* группа;
$\pm I$ — *диплоикосаэдральная* группа.

Группа $\pm G$ состоит из отображений $x \to \pm q^{-1}xq$, где $q \in 2G$.

Устройство *гибридных* групп является более тонким. Имеется проективная группа $[G]$, получаемая отбрасыванием знаков, и для каждого из элементов группы $[G]$ надо выбрать знак. Именно, знак будет положителен для некоторой подгруппы $[H]$, содержащей половину элементов группы $[G]$, и отрицателен для остальных элементов.

Стало быть, задание гибридной группы равносильно заданию пары $([H], [G])$ проективных групп, а именно, группы $[G]$, получающейся из гибридной группы при проективизации, и ее «половинки»: подгруппы $[H]$ индекса 2, элементам которой приписывается знак $+$. Формальным обозначением для такой группы будет «$+H-G$», что означает, что эта группа состоит из $+h$ для $[h] \in [H]$ и $-g$ для $[g]$, лежащих в остальной части группы $[G]$. Часто мы будем пользоваться неформальным

сокращенным обозначением HG. Возможные случаи таковы:

$+C_n - C_{2n} = CC_{2n} = CC(2n)$ — *циклоциклическая* группа;
$+C_n - D_{2n} = CD_{2n} = CD(n)$ — *циклодиэдральная* группа;
$+D_{2n} - D_{4n} = DD_{4n} = DD(2n)$ — *диэдро-диэдральная* группа;
$+T_{12} - O_{24} = TO$ — *тетраоктаэдральная* группа.

Группа $+H - G$ состоит из отображений $x \to +q^{-1}xq$ для $q \in 2H$ и $x \to -q^{-1}xq$ для $q \in 2G \setminus 2H$.

По используемым нами обозначениям легко восстановить структуру подгруппы как абстрактной группы, так что мы будем называть такую систему обозначений *алгебраической нотацией*. Правило таково: группы $+G$ и HG изоморфны G, а группа $\pm G$ изоморфна $C_2 \times G$.

§ 3.9. Геометрическое описание групп

На рис. 3.1 все группы описаны через знакомые нам многогранники. В верхней половине рисунка мы видим полные (голо-) и состоящие только из поворотов (хиро-) группы симметрий икосаэдра ($\pm I = *532$, $+I = 532$), октаэдра ($\pm O = *432$, $+O = 432$) и тетраэдра ($TO = *332$, $+T = 332$), а также диплотетраэдральную группу, чаще называемую *пиритоэдральной*, поскольку такой симметрией часто обладают кристаллы железного пирита. В нижней половине рисунка представлены голо-

хироикосаэдральная	532	$= +I$
голоикосаэдральная	*532	$= \pm I$
хирооктаэдральная	432	$= +O$
голооктаэдральная	*432	$= \pm O$
хиротетраэдральная	332	$= +T$
голотетраэдральная	*332	$= TO$
пиритоэдральная	3*2	$= \pm T$
		четное/нечетное
(*n*-угольная) *хиропризматическая*	22*n*	$= +D(n)$
(*n*-угольная) *голопризматическая*	*22*n*	$= \pm D(n)$ $/DD(2n)$
(*n*-угольная) *голо-антипризматическая*	2**n*	$= DD(2n)/\pm D(n)$
(*n*-угольная) *хиропирамидальная*	*nn*	$= +C(n)$
(*n*-угольная) *голопирамидальная*	**nn*	$= CD(n)$
(*n*-угольная) *пропризматическая*	*n**	$= \pm C(n)$ $/CC(2n)$
(*n*-угольная) *про-антипризматическая*	*n*×	$= CC(2n)/\pm C(n)$

Табл. 3.1. Словарь групп

и хирогруппы призм ($*22n$ и $22n$), антипризм ($2*n$ и $2nn$) и пирамид ($*nn$ и nn), а также пропризматические ($n*$) и про-антипризматические ($n\times$), получаемые из призматических и антипризматических при сохранении направления вращения относительно главных осей.

В таблице 3.1 указаны все соответствия между этими названиями и обозначениями в орбифолдной и алгебраической нотациях, а в таблице 3.2 группы расположены по возрастанию порядка. Имеется неприятная «двойственность» между геометрическими и алгебраическими обозначениями, проистекающая из того обстоятельства, что геометры предпочитают добавлять к группам поворотов отражения, а не более простую с алгебраической точки зрения центральную симметрию $-\mathbf{1}$. Поэтому в нашей таблице в некоторых местах через косую черту указаны «четное» и «нечетное» обозначения, наподобие обозначения $\pm D(n)/DD(2n)$ для $*22n$, означающего, что данная группа есть $\pm D(n)$ при четном n и $DD(2n)$ при нечетном n.

Между группами имеется много включений малого индекса; все включения индекса 2 приведены на рис. 3.9 и 3.10.

Приложение
Отображение $v \to \bar{q}vq$ является простым поворотом

Докажем это сначала для случая, когда ось совпадает с направлением вектора i, так что $q = \cos\theta + i\sin\theta$. Если при этом $v = xi + yj + zk$, то

$$\bar{q}vq = \bar{q}(xi)q + \bar{q}(yj + zk)q = xi + \bar{q}^2(yj + zk),$$

поскольку $iq = qi$, в то время как $jq = \bar{q}j$ и $kq = \bar{q}k$. Записывая правую часть этого равенства в виде

$$xi + (\cos(2\theta) - i\sin(2\theta))(y + zi)j,$$

получаем, что все точки одномерного пространства, порожденного i, остаются на месте, в то время как двумерное пространство, порожденное j и k, поворачивается на 2θ.

Из конструкции кватернионов, которую мы приведем в главе 6, фактически будет следовать, что всякий единичный мнимый кватернион можно обозначить через i, всякий перпендикулярный ему кватернион — через j, а произведение этих двух — через k. Мы, впрочем, и без ссылок на эту главу убедимся сейчас, что у кватернионов имеется достаточно симметрий, чтобы перевести всякий мнимый единичный вектор $u = li + mj + nk$ в i. В самом деле, поворотом описанного выше типа (относительно i) можно обратить в нуль коэффициент при k, после чего аналогичным поворотом вокруг k можно обнулить и коэффициент при j.

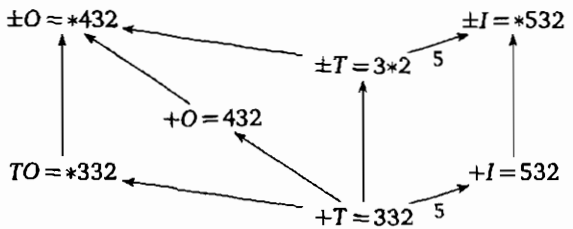


Рис. 3.9. Включения малого индекса между группами многогранников (всюду, где индекс не указан, он равен двум)

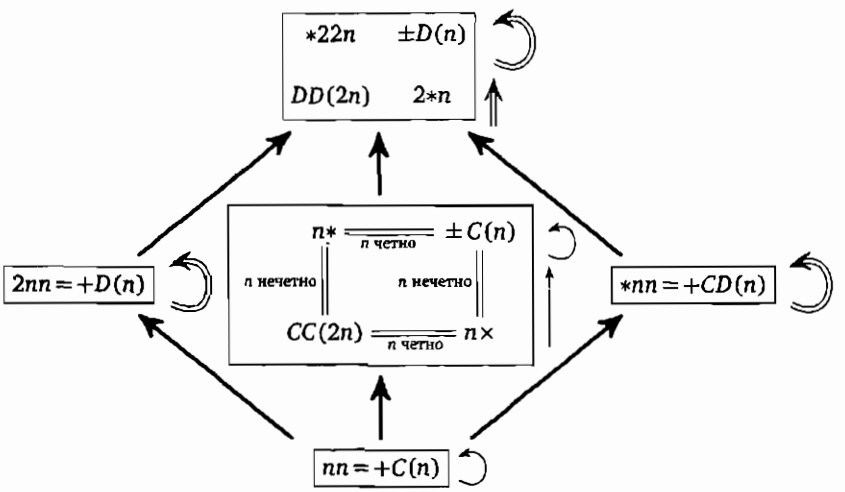


Рис. 3.10. Включения индекса 2 между аксиальными группами. Такого рода включения между группами с одним и тем же n обозначены жирными стрелками: каждая группа из верхнего прямоугольника содержит какую-то группу из нижнего (соответствующую ей группу, если это имеет смысл). Включения индекса 2 между группами, одна из которых характеризуется параметром n, а другая — параметром $n = \frac{m}{2}$, обозначены светлыми стрелками справа от прямоугольников. Например, группа $*22n$ содержит и $*22m$, и $2*m$ (каждую из них дважды, поскольку стрелки двойные)

1	1	$C_1 = 1$					
3_1	2	$C_2 = 22$	$\pm C_1 = \times$	$CC_2 = *$			$CD_2 = *$
1	3	$C_3 = 33$					
5_2	4	$C_4 = 44$	$2\times = CC_4$	$2* = \pm C_2$			$CD_4 = *22$
1	5	$C_5 = 55$					
5_2	6	$C_6 = 66$	$\pm C_3 = 3\times$	$CC_6 = 3*$			$CD_6 = *33$
1	7	$C_7 = 77$					
7_4	8	$C_8 = 88$	$4\times = CC_8$	$4* = \pm C_4$			$CD_8 = *44$
1	9	$C_9 = 99$					
5_2	10	$C_{10} = 10\,10$	$\pm C_5 = 5\times$	$CC_{10} = 5*$			$CD_{10} = *55$
1	11	$C_{11} = 11\,11$					
8_4	12	$C_{12} = 12\,12$	$6\times = CC_{12}$	$6* = \pm C_6$			$CD_{12} = *66$
1	13	$C_{13} = 13\,13$					
5_2	14	$C_{14} = 14\,14$	$\pm C_7 = 7\times$	$CC_{14} = 7*$			$CD_{14} = *77$
1	15	$C_{15} = 15\,15$					
7_4	16	$C_{16} = 16\,16$	$8\times = CC_{16}$	$8* = \pm C_8$			$CD_{16} = *88$
1	17	$C_{17} = 17\,17$					
5_2	18	$C_{18} = 18\,18$	$\pm C_9 = 9\times$	$CC_{18} = 9*$			$CD_{18} = *99$
1	19	$C_{19} = 19\,19$					
7_3	20	$C_{20} = 20\,20$	$10\times = CC_{20}$	$10* = \pm C_{10}$			$CD_{20} = *10\,10$
1	21	$C_{21} = 21\,21$					
5_2	22	$C_{22} = 22\,22$	$\pm C_{11} = 11\times$	$CC_{22} = 11*$			$CD_{22} = *11\,11$
1	23	$C_{23} = 23\,23$					
10_6	24	$C_{24} = 24\,24$	$12\times = CC_{24}$	$12* = \pm C_{12}$			$CD_{24} = *12\,12$
1	27	$C_{27} = 27\,27$					
5_2	30	$C_{30} = 30\,30$	$\pm C_{15} = 15\times$	$CC_{30} = 15*$			$CD_{30} = *15\,15$
1	33	$C_{33} = 33\,33$					
7_3	36	$C_{36} = 36\,36$	$18\times = CC_{36}$	$18* = \pm C_{18}$			$CD_{36} = *18\,18$
1	39	$C_{39} = 39\,39$					
5_2	42	$C_{42} = 42\,42$	$\pm C_{21} = 21\times$	$CC_{42} = 21*$			$CD_{42} = *21\,21$
1	45	$C_{45} = 45\,45$					
8_5	48	$C_{48} = 48\,48$	$24\times = CC_{48}$	$24* = \pm C_{24}$			$CD_{48} = *24\,24$
1	51	$C_{51} = 51\,51$					
5_2	54	$C_{54} = 54\,54$	$\pm C_{27} = 27\times$	$CC_{54} = 27*$			$CD_{54} = *27\,27$
1	57	$C_{57} = 57\,57$					
8_4	60	$C_{60} = 60\,60$	$30\times = CC_{60}$	$30* = \pm C_{30}$			$CD_{60} = *30\,30$
1	75	$C_{75} = 75\,75$					
5_2	90	$C_{90} = 90\,90$	$\pm C_{45} = 45\times$	$CC_{90} = 45*$			$CD_{90} = *45\,45$
1	105	$C_{105} = 105\,105$					
8_5	120	$C_{120} = 120\,120$	$60\times = CC_{120}$	$60* = \pm C_{60}$			$CD_{120} = *60\,60$
			C		$2\times C$		D

Табл. 3.2. Классификация групп по порядку. Перед числом, обозначающим порядок группы, указано количество групп этого порядка, а в нижнем индексе к этому числу — число таких групп с точностью до изоморфизма. Волнистые линии разделяют группы различной структуры (см. нижнюю строку таблицы). Строки для порядков $8n$, $8n+1$, ..., $8n+7$, не включенные в таблицу, — такие же, как для порядков 16, 17, ..., 23

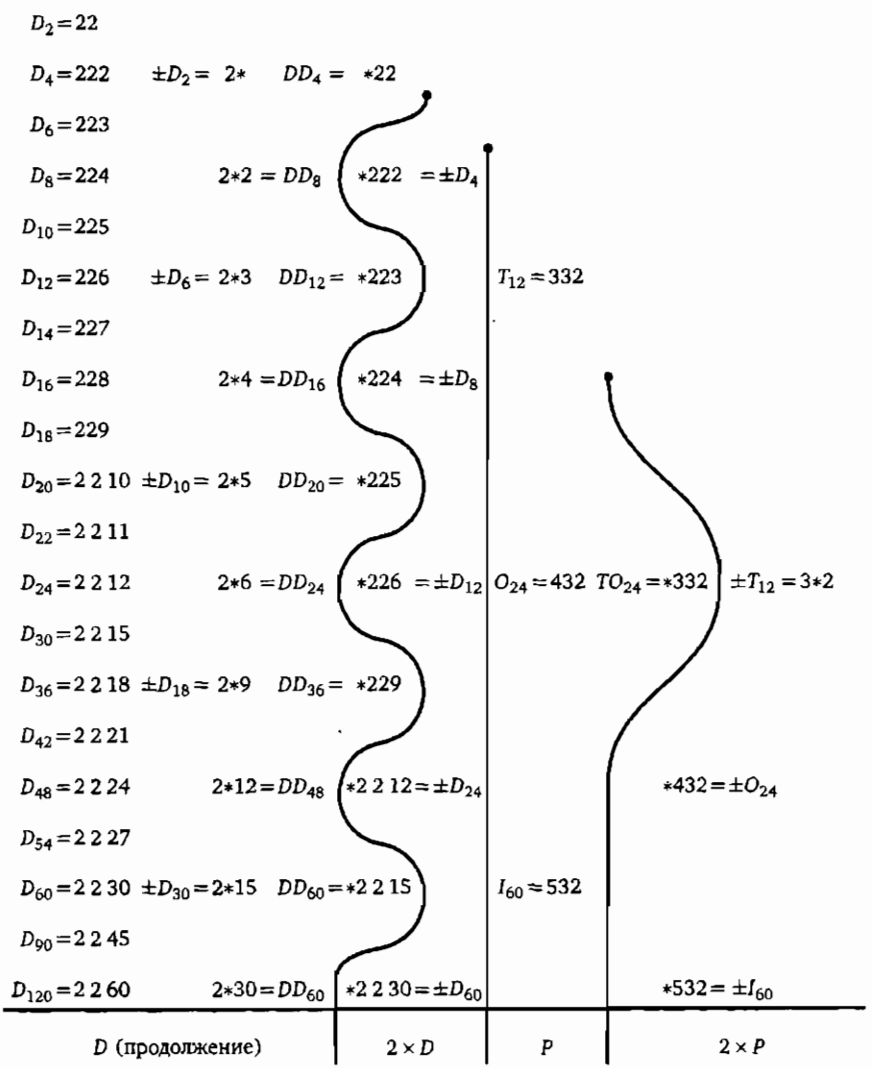
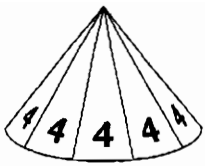


Табл. 3.2 (продолжение)



Кватернионы и четырехмерные группы

§ 4.1. Введение

В главе 3 мы использовали тот факт, что всякое трехмерное ортогональное отображение имеет вид

$$x \to \bar{q}xq \quad \text{или} \quad -\bar{q}xq = \bar{q}\bar{x}q,$$

в зависимости от того, хирально они или ахирально. Первая цель этой главы — установить, что всякое ортогональное отображение в размерности 4 имеет вид

$$x \to \bar{l}xr \quad \text{или} \quad \bar{l}\bar{x}r,$$

где l и r — единичные кватернионы.

В главе 6 мы увидим, что в любой композиционной алгебре отображение

$$x \to -q\bar{x}q$$

(где q — произвольный единичный кватернион) является отражением в гиперплоскости, перпендикулярной q (в дальнейшем мы будем называть такое отображение отражением относительно q). Впрочем, нам нет нужды ссылаться на этот результат, поскольку в кватернионном случае мы можем проверить это непосредственно. Именно, это отображение действует по правилу

$$uq \to -q\bar{q}\bar{u}q = -\bar{u}q,$$

откуда следует, что q переходит в $-q$, а iq, jq и kq переходят в себя.

В главе 1 мы показали, что всякая евклидова симметрия есть произведение отражений. Следовательно, произведение n отражений имеет вид

$$x \to \pm q_n q_{n-1} \cdots q_1 (x \text{ или } \bar{x}) q_1 q_2 \cdots q_n$$

и тем самым приводится к виду

$$[l, r]: x \to \bar{l}xr \quad \text{(если } n \text{ четно)}$$

или

$$*[l, r]: x \to \bar{l}\bar{x}r \quad \text{(если } n \text{ нечетно)},$$

где l и r — единичные кватернионы, а звездочка во второй формуле обозначает кватернионное сопряжение.

§ 4.2. Два отображения

Мы получили обобщение трехмерных результатов, поскольку ясно, что наши отображения сохраняют единицу тогда и только тогда, когда $l = r = q$, так что отображения из главы 3 суть

$$[q] = [q, q] \quad \text{и} \quad *[q] = *[q, q].$$

В предыдущей главе мы установили, что при отображении, ставящем в соответствие единичному кватерниону q элемент SO_3, действующий по правилу

$$[q]: x \to \bar{q}xq,$$

у каждого элемента есть два прообраза, поскольку единственное возможное совпадение — это $[-q] = [q]$. Наше новое отображение из упорядоченных пар единичных кватернионов[1] в элементы SO_4 обладает аналогичным свойством, поскольку единственное возможное совпадение — это

$$[-l, -r] = [l, r].$$

(Отображение вида $[l, r]$, являющееся тождественным, должно сохранять единицу, так что из трехмерного результата вытекает, что единственная нетривиальная пара с таким свойством есть $[-1, -1]$.)

При проективизации слияний будет немного больше, поскольку ввиду равенств

$$[-l, -r] = [l, r], \quad [-l, r] = [l, -r] = -[l, r]$$

четырем выражениям $[\pm l, \pm r]$ соответствует одно и то же отображение проективных пространств. В соответствии с нашим соглашением, по которому через $[x]$ обозначается функция, удовлетворяющая только условию $[-x] = [x]$, мы для отображения в проективную группу будем использовать обозначение $[\![l, r]\!]$ (вместо $[[l, r]]$).

[1] Они образуют группу, изоморфную четырехмерной *спинорной* группе Spin_4.

§ 4.3. Обозначения для групп

Не вдаваясь прямо сейчас в подробности, скажем, что наше обозначение для типичной четырехмерной хиральной группы будет иметь вид

$$\tfrac{1}{f}[\![L \times R]\!], \quad \pm\tfrac{1}{f}[L \times R] \quad \text{или} \quad +\tfrac{1}{f}[L \times R]$$

в проективном, диплоидном или гаплоидном случаях соответственно, причем L и R здесь — трехмерные хиральные группы. Эти обозначения удачны в том отношении, что, например, обозначение $\pm\frac{1}{f}[L \times R]$ наталкивает на верный вывод, что эта группа содержит $\frac{1}{f}$ от всех элементов вида $\pm[l, r]$ при всех выборах знаков. В частности, порядки этих групп суть

$$\frac{|L| \times |R|}{f}, \quad 2\frac{|L| \times |R|}{f} \quad \text{и} \quad \frac{|L| \times |R|}{f}$$

соответственно.

Группа $\frac{1}{f}[\![L \times R]\!]$ состоит из элементов вида $[\![l, r]\!]$, для которых $l \in 2L$, $r \in 2R$ и $l^\alpha = r^\beta$, где α и β — гомоморфизмы этих групп на одну и ту же конечную группу F порядка f. Соответствующая диплоидная группа $\pm\frac{1}{f}[L \times R]$ состоит из пар элементов $\pm[l, r]$, удовлетворяющих тем же условиям, а в гаплоидной группе (если таковая существует) для каждой пары выбирается один из двух знаков.

Если какая-нибудь из вышеописанных групп имеет индекс 2 в ахиральной группе, то L и R должны быть группой одного типа (обозначим ее Q), и наше обозначение для большей группы будет иметь вид

$$\tfrac{1}{f}[\![Q \times Q]\!] \cdot 2, \quad \pm\tfrac{1}{f}[Q \times Q] \cdot 2 \quad \text{или} \quad +\tfrac{1}{f}[Q \times Q] \cdot 2;$$

порядки таких групп равны

$$2\frac{|Q|^2}{f}, \quad 4\frac{|Q|^2}{f} \quad \text{и} \quad 2\frac{|Q|^2}{f}$$

соответственно.

Обычно гомоморфизмы α и β однозначно определяются уже по группам L и R и числу f. В тех случаях, когда это не так, мы будем добавлять к L и R дополнительные значки. Именно, будем иногда добавлять число в скобках в качестве верхнего индекса, или будем проводить черту над обозначением группы, чтобы указать на менее очевидный из двух возможных случаев, или будем позволять себе опускать $\frac{1}{f}$, (s) или (t), если f, s или t равно 1. В ахиральных случаях

Группа	Образующие
$\pm[I\times O]$	$[i_I,1],[\omega,1],[1,i_O],[1,\omega]$;
$\pm[I\times T]$	$[i_I,1],[\omega,1],[1,i],[1,\omega]$;
$\pm[I\times D_{2n}]$	$[i_I,1],[\omega,1],[1,e_n],[1,j]$;
$\pm[I\times C_n]$	$[i_I,1],[\omega,1],[1,e_n]$;
$\pm[O\times T]$	$[i_O,1],[\omega,1],[1,i],[1,\omega]$;
$\pm[O\times D_{2n}]$	$[i_O,1],[\omega,1],[1,e_n],[1,j]$;
$\pm\frac{1}{2}[O\times D_{2n}]$	$[i,1],[\omega,1],[1,e_n];[i_O,j]$
$\pm\frac{1}{2}[O\times \bar{D}_{4n}]$	$[i,1],[\omega,1],[1,e_n],[1,j];[i_O,e_{2n}]$
$\pm\frac{1}{6}[O\times D_{6n}]$	$[i,1],[j,1],[1,e_n];[i_O,j],[\omega,e_{3n}]$
$\pm[O\times C_{2n}]$	$[i_O,1],[\omega,1],[1,e_n]$;
$\pm\frac{1}{2}[O\times C_{2n}]$	$[i,1],[\omega,1],[1,e_n];[i_O,e_{2n}]$
$\pm[T\times D_{2n}]$	$[i,1],[\omega,1],[1,e_n],[1,j]$;
$\pm[T\times C_n]$	$[i,1],[\omega,1],[1,e_n]$;
$\pm\frac{1}{3}[T\times C_{3n}]$	$[i,1],[1,e_n];[\omega,e_{3n}]$
$\pm\frac{1}{2}[D_{2m}\times \bar{D}_{4n}]$	$[e_m,1],[1,e_n],[1,j];[j,e_{2n}]$
$\pm[D_{2m}\times C_n]$	$[e_m,1],[j,1],[1,e_n]$;
$\pm\frac{1}{2}[D_{2m}\times C_{2n}]$	$[e_m,1],[1,e_n];[j,e_{2n}]$
$+\frac{1}{2}[D_{2m}\times C_{2n}]$	$-,-;+$
$\pm\frac{1}{2}[\bar{D}_{4m}\times C_{2n}]$	$[e_m,1],[j,1],[1,e_n];[e_{2m},e_{2n}]$

Табл. 4.1. Хиральные группы I. В этой таблице содержится большинство «метахиральных» групп (см. § 4.6; некоторые другие можно найти в последних строках таблицы 4.2)

различные возможные выборы элемента $*[a,b]$, добавляемого к хиральной группе, различаются с помощью индексов или вертикальной черты у завершающей обозначение цифры 2. Точный смысл индексов и черты должен быть ясен из приведенных в таблицах 4.1—4.3 (в которых все интересующие нас группы перечислены) списков пар кватернионов, порождающих группы.

Классификация проводится с помощью (простой) теории подгрупп $G\subset A\times B$ в прямом произведении двух групп, развитой Гурса в 1889 году [20] для этой самой цели. Именно, элементы $l\in A$ (соответствен-

но $r \in B$), для которых существует элемент $(l, r) \in G$, образуют подгруппу $L \subset A$ (соответственно $R \subset B$); мы будем называть эти подгруппы левой и правой. Элементы l (соответственно r), для которых $(l, 1) \in G$ (соответственно $(1, r) \in G$), образуют нормальные подгруппы $L_0 \subset A$ и $R_0 \subset B$, которые мы будем называть левым и правым ядром соответственно.

Если теперь $l_0 \in L_0$, $r_0 \in R_0$, то

$$(l, r) \in G \iff (ll_0, rr_0) \in G,$$

так что условие «$(l, r) \in G$» зависит только от классов l и r по модулю L_0 и R_0. Более того, это условие задает изоморфизм между левой факторгруппой L/L_0 и правой факторгруппой R/R_0, так что эти группы должны быть изоморфны одной и той же группе F. Если порядок группы F равен f, то группа G будет иметь индекс f в $L \times R$.

Поскольку типичный элемент $[\![l, r]\!]$ в четырехмерной проективной группе PSO_4 не зависит от знаков l и r, он определяется парой соответствующих элементов $[l], [r] \in PSO_3$, откуда $PSO_4 \simeq PSO_3 \times PSO_3$. Согласно теории Гурса, типичная конечная подгруппа в PSO_4 имеет тогда вид

$$\{[\![l, r]\!] \mid [l] \in L, [r] \in R, \alpha([l]) = \beta([r])\},$$

где L и R — конечные подгруппы в PSO_3, а α и β — гомоморфизмы из этих групп на одну и ту же абстрактную группу F. Ничто не мешает считать, что α и β определены на соответствующих кватернионных группах $2L$ и $2R$ и содержат -1 в своих ядрах. Все это показывает, что группы вида $\frac{1}{f}[\![L \times R]\!]$ — это еще не все проективные хиральные группы и что доказательства в остальных случаях аналогичны (в гаплоидных случаях надо рассмотреть подгруппу в $2L \times 2R$, состоящую из элементов, для которых $[l, r]$ лежит в группе).

Мы только что убедились, что с помощью кватернионов можно получить короткую и элегантную полную классификацию четырехмерных групп. Если, однако, группа нам задана геометрически, а не через кватернионы, то найти ее в этой кватернионной классификации (или, наоборот, дать геометрическое описание группы из наших таблиц) может быть непросто. В следующем параграфе рассматривается важный частный случай.

§ 4.4. Кокстеровские обозначения для групп многогранников

Широко используются обозначения Кокстера для правильных многогранников и соответствующих групп (полученные путем адаптации обозначений Шлефли). В этом параграфе мы немного расширим его

Группа	Образующие	Кокстеровское обозначение
$\pm[I\times I]$	$[i_I,1],[\omega,1],[1,i_I],[1,\omega];$	$[3,3,5]^+$
$\pm\frac{1}{60}[I\times I]$	$;[\omega,\omega],[i_I,i_I]$	$2.[3,5]^+$
$+\frac{1}{60}[I\times I]$	$;\ +\ ,\ +$	$[3,5]^+$
$\pm\frac{1}{60}[I\times\bar{I}]$	$;[\omega,\omega],[i_I,i'_I]$	$2.[3,3,3]^+$
$+\frac{1}{60}[I\times\bar{I}]$	$;\ +\ ,\ +$	$[3,3,3]^+$
$\pm[O\times O]$	$[i_O,1],[\omega,1],[1,i_O],[1,\omega];$	$[3,4,3]^+:2$
$\pm\frac{1}{2}[O\times O]$	$[i,1],[\omega,1],[1,i],[1,\omega];[i_O,i_O]$	$[3,4,3]^+$
$\pm\frac{1}{6}[O\times O]$	$[i,1],[j,1],[1,i],[1,j];[\omega,\omega],[i_O,i_O]$	$[3,3,4]^+$
$\pm\frac{1}{24}[O\times O]$	$;[\omega,\omega],[i_O,i_O]$	$2.[3,4]^+$
$+\frac{1}{24}[O\times O]$	$;\ +\ ,\ +$	$[3,4]^+$
$+\frac{1}{24}[O\times\bar{O}]$	$;\ +\ ,\ -$	$[2,3,3]^+$
$\pm[T\times T]$	$[i,1],[\omega,1],[1,i],[1,\omega];$	$[^+3,4,3^+]$
$\pm\frac{1}{3}[T\times T]$	$[i,1],[j,1],[1,i],[1,j];[\omega,\omega]$	$[^+3,3,4^+]$
$\simeq\pm\frac{1}{3}[T\times\bar{T}]$	$[i,1],[j,1],[1,i],[1,j];[\omega,\bar{\omega}]$	$[^+3,3,4^+]$
$\pm\frac{1}{12}[T\times T]$	$;[\omega,\omega],[i,i]$	$2.[3,3]^+$
$\simeq\pm\frac{1}{12}[T\times\bar{T}]$	$;[\omega,\bar{\omega}],[i,-i]$	$2.[3,3]^+$
$+\frac{1}{12}[T\times T]$	$;\ +\ ,\ +$	$[3,3]^+$
$\simeq+\frac{1}{12}[T\times\bar{T}]$	$;\ +\ ,\ +$	$[3,3]^+$
$\pm[D_{2m}\times D_{2n}]$	$[e_m,1],[j,1],[1,e_n],[1,j];$	
$\pm\frac{1}{2}[\bar{D}_{4m}\times\bar{D}_{4n}]$	$[e_m,1],[j,1],[1,e_n],[1,j];[e_{2m},e_{2n}]$	
$\pm\frac{1}{4}[D_{4m}\times\bar{D}_{4n}]$	$[e_m,1],[1,e_n];[e_{2m},j];[j,e_{2n}]$	Условия:
$+\frac{1}{4}[D_{4m}\times\bar{D}_{4n}]$	$-\ ,-\ ;\ +\ ,\ +$	m,n нечетны
$\pm\frac{1}{2f}[D_{2mf}\times D^{(s)}_{2nf}]$	$[e_m,1],[1,e_n];[e_{mf},e^s_{nf}],[j,j]$	$(s,f)=1$
$+\frac{1}{2f}[D_{2mf}\times D^{(s)}_{2nf}]$	$-\ ,-\ ;+\ ,\ +$	m,n нечетны, $(s,2f)=1$
$\pm\frac{1}{f}[C_{mf}\times C^{(s)}_{nf}]$	$[e_m,1],[1,e_n];[e_{mf},e^s_{nf}]$	$(s,f)=1$
$+\frac{1}{f}[C_{mf}\times C^{(s)}_{nf}]$	$-\ ,-\ ;\ +$	m,n нечетны, $(s,2f)=1$

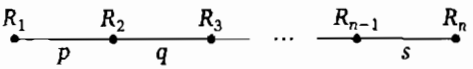
Табл. 4.2. Хиральные группы II. Большинство этих групп «ортохиральны»; в последних строках несколько групп «парахиральны». Образующие надо брать с обоими знаками во всех случаях, кроме гаплоидных; в гаплоидных случаях мы указываем только выбор знаков. Смысл кокстеровских обозначений разъясняется в § 4.4

Группа	Дополнительный элемент	Кокстеровское обозначение
$\pm[I\times I]\cdot 2$	$*$	$[3,3,5]$
$\pm\frac{1}{60}[I\times I]\cdot 2$	$*$	$2.[3,5]$
$+\frac{1}{60}[I\times I]\cdot 2_3$ или 2_1	$*$ или $-*$	$[3,5]$ или $[3,5]^\circ$
$\pm\frac{1}{60}[I\times \bar{I}]\cdot 2$	$*$	$2.[3,3,3]$
$+\frac{1}{60}[I\times \bar{I}]\cdot 2_3$ или 2_1	$*$ или $-*$	$[3,3,3]^\circ$ или $[3,3,3]$
$\pm[O\times O]\cdot 2$	$*$	$[3,4,3]:2$
$\pm\frac{1}{2}[O\times O]\cdot 2$ или $\bar{2}$	$*$ или $*[1,i_O]$	$[3,4,3]$ или $[3,4,3]^{+,}\cdot 2$
$\pm\frac{1}{6}[O\times O]\cdot 2$	$*$	$[3,3,4]$
$\pm\frac{1}{24}[O\times O]\cdot 2$	$*$	$2.[3,4]$
$+\frac{1}{24}[O\times O]\cdot 2_3$ или 2_1	$*$ или $-*$	$[3,4]$ или $[3,4]^\circ$
$+\frac{1}{24}[O\times \bar{O}]\cdot 2_3$ или 2_1	$*$ или $-*$	$[2,3,3]^\circ$ или $[2,3,3]$
$\pm[T\times T]\cdot 2$	$*$	$[3,4,3^+]$
$\pm\frac{1}{3}[T\times T]\cdot 2$	$*$	$[^+3,3,4]$
$\pm[T\times \bar{T}]\cdot 2$	$*$	$[3,3,4^+]$
$\pm\frac{1}{12}[T\times T]\cdot 2$	$*$	$2.[^+3,4]$
$\pm\frac{1}{12}[T\times \bar{T}]\cdot 2$	$*$	$2.[3,3]$
$+\frac{1}{12}[T\times T]\cdot 2_3$ или 2_1	$*$ или $-*$	$[^+3,4]$ или $[^+3,4]^\circ$
$+\frac{1}{12}[T\times \bar{T}]\cdot 2_3$ или 2_1	$*$ или $-*$	$[3,3]^\circ$ или $[3,3]$
$\pm[D_{2n}\times D_{2n}]\cdot 2$	$*$	
$\pm\frac{1}{2}[\bar{D}_{4n}\times \bar{D}_{4n}]\cdot 2$ или $\bar{2}$	$*$ или $*[1,e_{2n}]$	
$\pm\frac{1}{4}[D_{4n}\times \bar{D}_{4n}]\cdot 2$	$*$	Условия:
$+\frac{1}{4}[D_{4n}\times \bar{D}_{4n}]\cdot 2_3$ или 2_1	$*$ или $-*$	n нечетно
$\pm\frac{1}{2f}[D_{2nf}\times D^{(s)}_{2nf}]\cdot 2^{(\alpha,\beta)}$ или $\bar{2}$	$*[e^{\alpha}_{2nf}, e^{\alpha s+\beta f}_{2nf}]$ или $*[1,j]$	См. приложение к этой главе
$+\frac{1}{2f}[D_{2nf}\times D^{(s)}_{2nf}]\cdot 2^{(\alpha,\beta)}$ или $\bar{2}$	$*[e^{\alpha}_{2nf}, e^{\alpha s+\beta f}_{2nf}]$ или $*[1,j]$	
$\pm\frac{1}{f}[C_{nf}\times C^{(s)}_{nf}]\cdot 2^{(\gamma)}$	$*[1, e^{\gamma(f,s+1)}_{2nf}]$	
$+\frac{1}{f}[C_{nf}\times C^{(s)}_{nf}]\cdot 2^{(\gamma)}$	$*[1, e^{\gamma(f,s+1)}_{2nf}]$	

Табл. 4.3. Ахиральные группы. Условия на параметр, налагаемые в последних четырех строках, см. в приложении на с. 67

систему обозначений, чтобы иметь возможность назвать все «полиэдральные» группы, приведенные также в таблицах 4.2 и 4.3.

Кокстер обозначает через $[p, q, \ldots, r, s]$ группу симметрий n-мерного многогранника $\{p, q, \ldots, r, s\}$; эта группа порождена отражениями $R_1, \ldots, R_n$, соответствующими вершинам n-вершинной диаграммы



В таких обозначениях группа задается соотношениями

$$1 = R_1^2 = (R_1R_2)^p = R_2^2 = (R_2R_3)^q = \ldots = R_{n-1}^2 = (R_{n-1}R_n)^s = R_n^2 = (R_iR_j)^2,$$

$j > i+1$. В этой группе содержится очевидная подгруппа $[p, q, \ldots, r, s]^+$ индекса 2, состоящая из слов четной длины в алфавите $R_1, \ldots, R_n$.

Если ровно одно из чисел $p, q, \ldots, r, s$ является четным (пусть, например, это будет число, расположенное между R_k и R_{k+1}), то есть еще подгруппы

$$[{}^+p, q, \ldots, r, s] \quad \text{и} \quad [p, q, \ldots, r, s^+],$$

состоящие из слов, в которые

$$R_1, \ldots, R_k \quad \text{и} \quad R_{k+1}, \ldots, R_n$$

соответственно входят четное число раз. Их пересечение — подгруппа $[{}^+p, q, \ldots, r, s^+]$ индекса 4, состоящая из слов, в которые и $R_1, \ldots, R_k$, и $R_{k+1}, \ldots, R_n$ входят четное число раз. Мы слегка модифицировали обозначения Кокстера: он пишет $[p^+, \ldots]$, когда мы пишем $[{}^+p, \ldots]$, и пользуется только некоторыми частными случаями.

Чтобы получились изящные обозначения для всех «групп многогранников» в размерности 4, мы дополняем кокстеровские обозначения следующим образом. Через G° мы обозначаем группу, «противоположную» к G, то есть группу, получаемую из G заменой каждого элемента $g \in G$ на $+g$ или $-g$, в зависимости от того, равняется $\det g$ единице или минус единице; добавление префикса «2.» к обозначению группы обозначает удвоение группы с помощью добавления -1, а добавление суффикса «:2» или «·2» означает некоторое другое удвоение, расщепленное или нерасщепленное соответственно.

§ 4.5. Более ранние классификации

У классификации наших групп имеется большая история, начинающаяся с классификации эллиптических групп, проведенной Гурса в 1889 году. В 1931 году Трельфалль и Зейферт [40] перечислили все группы и обнаружили некоторые их применения в топологии. Стандартной

ссылкой по-английски была маленькая изящная книга Дю Валя «Homographies, Quaternions, and Rotations» [41].

Надо, однако, отметить, что в списках Гурса и Дю Валя имеется пробел, а также что в некотором важном смысле *все* эти классификации являются незавершенными. Список Зейферта и Трельфалля действительно содержит все группы, но про каждую из групп, входящих в этот список, неизвестно, сколько раз она там упомянута, поскольку *отсутствует* полный список эквивалентностей между группами, зависящими от параметров. Ранее в литературе вопрос ставился только в работе Хёрли [25], посвященной кристаллографическим группам, где эти группы классифицировались с помощью введенных ad hoc инвариантов. В книге [7] ее авторы (Браун, Бюлов, Нойбюзер, Вондрачек и Цассенхауз) используют инварианты, введенные Хёрли, для классификации четырехмерных пространственных групп.

То обстоятельство, что проблема не вполне тривиальна, иллюстрируется тем фактом, что при всех допустимых значениях h и k группы, которые Дю Валь обозначает через

$$(D_{\frac{1}{2}nr}/C_n; D_{\frac{1}{2}nr}/C_n)^{\star}_{s,h,k-},$$

будут геометрически изоморфны! В наших обозначениях (в которых смысл числовых параметров иной) это группа $\pm\frac{1}{2f}[D_{2nf}\times D^{(s)}_{2nf}]\cdot\overline{2}$.

§ 4.6. Замечание о хиральности

Вопрос о хиральности является более тонким, чем кажется. Мы уже упоминали о том, что когда мы говорим, что группа симметрий некоторого объекта «хиральна», имеется в виду, что хирален *сам этот объект*. В размерности три все конечные подгруппы ортогональной группы, в том числе и «хиральные», совпадают со своими зеркальными образами.

Тем не менее, среди 219 кристаллографических групп в размерности 3 имеется 11 не совпадающих со своими зеркальными образами (по каковой причине некоторые авторы пишут, что общее число кристаллографических групп равно 230). Такие группы называются *метахиральными*. Метахиральность часто встречается у подгрупп четырехмерной ортогональной группы, поскольку каждая из групп $\pm\frac{1}{f}[L\times R]$ или $+\frac{1}{f}[L\times R]$, где $L\neq R$, очевидным образом метахиральна.

Есть, однако, и еще один интересный эффект, впервые проявляющийся в размерности 4. В меньших размерностях всякая хиральная

группа, не являющаяся метахиральной, является хиральной частью некоторой ахиральной группы. Мы называем такие группы «ортодоксально хиральными», или *ортохиральными*. По-другому можно сказать так: можно наложить соответствующий хиральный объект на его зеркальный образ и получить в результате ахиральный объект.

В размерности 4 это верно уже не всегда; группы, для которых это неверно, мы называем *парахиральными*. Например, парахиральная группа $\pm\frac{1}{7}[C_7 \times C_7^{(2)}]$ является подгруппой индекса 14 в ахиральной группе $\pm[C_7 \times C_7] \cdot 2$, но не в хиральной части какой бы то ни было ахиральной группы, поскольку ее зеркальный образ есть $\pm\frac{1}{7}[C_7 \times C_7^{(4)}]$.

Некоторые химики проводят еще одно различие: между «хиральностью ботинок» и «хиральностью картофелин». Мы не ожидаем ни от ботинок, ни от картофелин, что они окажутся ахиральными, но при этом мы говорим о левом и правом ботинке, но не о «левой или правой картофелине». Почему так получается?

Причина в том, что картофелину можно непрерывно продеформировать в свое зеркальное отражение так, чтобы в процессе деформации она все время оставалась хиральной. Топологи называют такую деформацию «изотопией» (внутри класса хиральных объектов), так что хиральность «как у ботинок» мы будем называть *изохиральностью* (хиральностью даже с учетом изотопий).

В размерности 2 класс хиральных (т. е. разносторонних) треугольников изохирален, поскольку длины сторон возрастают либо против часовой стрелки (для «левых» треугольников), либо по часовой стрелке (для «правых»). В размерности 3 хиральные тетраэдры не являются изохиральными, поскольку все хиральные тетраэдры изотопны внутри этого класса.

Приложение
Полнота таблиц

Мы установим эту полноту, показав, что в них учтены все возможные пары гомоморфизмов из L и R на одну и ту же абстрактную конечную группу F. Поскольку, впрочем,

$$[l, r]^{[l_1, r_1]} = [l^{l_1}, r^{r_1}],$$

можно заменять L и R независимо одну от другой на сопряженные подгруппы, так что достаточно работать только с точностью до «геометрической эквивалентности».

Полнота таблиц 4.1 и 4.2

Теперь легко перечислить нормальные подгруппы трехмерных хиральных групп. За одним исключением, для каждого возможного порядка такая группа единственна. Порядки таковы:

$$\begin{aligned} 1, 4, 12 &\quad \text{в } T \\ 1, 4, 12, 24 &\quad \text{в } O \\ 1, 60 &\quad \text{в } I \\ m, \text{ где } m|n, &\quad \text{в } C_n \text{ или } D_n. \end{aligned}$$

Исключение[1] состоит в том, что группа D_{2n} содержит две нормальные подгруппы порядка $2n$, а именно C_{2n} и D_n. Стало быть, ядра гомоморфизмов α и β полностью определяются индексом f, кроме двух случаев с D_{2n}, когда n четно, а $f = 2$:

$$\text{запись } \tfrac{1}{2}[\ldots D_{2n}\ldots] \text{ означает, что ядро} = C_n;$$

$$\text{запись } \tfrac{1}{2}[\ldots \bar{D}_{2n}\ldots] \text{ означает, что ядро} = D_n.$$

Тем не менее имеются случаи, когда различные гомоморфизмы имеют одно и то же ядро; причина здесь в том, что F обладает автоморфизмом, не индуцированным никаким элементом GO_3 (тем самым этот автоморфизм с неизбежностью должен быть внешним). Легко проверить, что эти случаи таковы:

Наши обозначения	Описание автоморфизма
$\frac{1}{60}[\ldots \bar{I}\ldots]$	расширяет A_5 до S_5
$+\frac{1}{24}[\ldots \bar{O}\ldots]$	умножает на -1 элементы[2] $2S_4 \setminus 2A_4$
$\frac{1}{4}[\ldots \bar{D}\ldots]$	сдвигает «циклическую часть»[3]
$\frac{1}{f}[\ldots D_{nf}^{(s)}\ldots]$, $\frac{1}{f}[\ldots C_{nf}^{(s)}\ldots]$	возведение в степень s на циклической части

[1] Здесь в авторский текст были внесены некоторые изменения. — *Прим. ред.*

[2] К проективному и диплоидному случаям не относится.

[3] Гурса, а вслед за ним и Дю Валь, пропустили группу $\frac{1}{4}[D_{4m} \times \bar{D}_{4n}]$, обязанную своим существованием тому обстоятельству, что автоморфизмы группы $F \simeq D_4$ могут произвольным образом переставлять неединичные элементы, в отличие от случая бо́льших D_{2k}, у которых «циклическая часть» C_k однозначно определена.

В таблице 4.2 имеются три группы, для которых мы приводим альтернативное обозначение с участием $\bar{T}$. Это повторение упрощает таблицу 4.3.

Полнота таблицы 4.3

Группы из этой таблицы строятся из своих «половинок» H, соответствующих какому-то изоморфизму $L/L_0 \simeq R/R_0$, с помощью добавления некоторого элемента $*[a, b]$, который должен нормализовать H. Мы покажем, что (за счет некоторых модификаций) дополнительный элемент можно привести к виду $*[1, c]$, а также что (без всяких модификаций) c можно умножить на элемент из R_0 или подвергнуть сопряжению с помощью элемента из R с тем, чтобы в конце концов c попал в множество элементов из R, оставляемых на месте (по модулю R_0) данным изоморфизмом (поскольку $(*[1, c])^2 = [c, c]$ должно лежать в H).

В самом деле, при сопряжении с помощью $[1, a]$ элемент $*[a, b]$ заменяется на

$$(*[a, b])^{[1,a]} = [1, \bar{a}]*[a, b][1, a] = *[\bar{a}a, ba] = *[1, c];$$

при этом $[l, r]$ заменится на $[l, \bar{a}ra]$, и тем самым изоморфизм заменится на геометрически эквивалентный. Если $r_0 \in R_0$, то $*[1, cr_0]$ задает ту же группу, что $*[l_1, cr_1]$ для произвольного $[l_1, r_1] \in H$; при сопряжении с помощью $[1, l_1]$, где $l_1 \in R$ — произвольный элемент, это сводится к $*[1, cr_1l_1]$; при этом r в паре $[l, r]$ заменяется на $\bar{l}_1 r l_1$.

С помощью этих преобразований всегда можно привести дополнительный элемент к виду

$$*[1, \pm 1] = * \text{ или } -*,$$

которому соответствуют обозначения $\cdot 2_3$ или $\cdot 2_1$ (нижний индекс указывает размерность пространства, умножаемого на -1). Исключения — случаи «$D \times D$» и «$C \times C$», для которых в таблице 4.3 перечислены все значения c, а также еще два случая, а именно

$$\pm\frac{1}{2}[O \times O] \cdot \bar{2} \quad \text{и} \quad \pm\frac{1}{4}[\bar{D}_{4n} \times \bar{D}_{4n}] \cdot \bar{2};$$

в этих случаях можно положить $c = i_O$ и $c = e_{2n}$ соответственно.

Как мы уже отмечали, приведение к форме $*[1, c]$ происходит за счет замены изоморфизма на геометрически эквивалентный, а в $(T \times T)$-случае при этом иногда приходится заменять тождественный изоморфизм на изоморфизм, обозначенный нами через $\bar{T}$, а именно

$$\omega \to \bar{\omega} \quad \text{и} \quad i \to \bar{i} = -i.$$

Последние восемь строк в таблице 4.3

В случае $\pm[D\times D]\cdot 2$ мы начнем с того, что дополнительный элемент $*[a,b]$ можно привести по модулю H и что он должен нормализовать H, а тем самым и E — подгруппу элементов в H вида $[e^{\gamma}, e^{\delta}]$ (поскольку $E\subset H$ является характеристической подгруппой всегда, кроме простых случаев, в которых $f\leqslant 2$, — их мы не рассматриваем). Стало быть, можно считать, что a и b лежат в $e^{\mathbb{R}}(1$ или $j)$; поэтому (так как $[j,j]\in H$) можно считать, что $*[a,b]=*[e^{\lambda}, e^{\mu}]$ (получается группа $\pm[D\times D]\cdot 2^{\langle\alpha,\beta\rangle}$) или $*[a,b]=*[e^{\lambda}, e^{\mu}j]$ (получается[1] $\pm[D\times D]\cdot\overline{2}$). В первом случае должно выполняться включение

$$[j,j]^{*[e^{\lambda},e^{\mu}]}=[j,j]^{[e^{\lambda},e^{\mu}]}=[je^{2\lambda}, je^{2\mu}]\in H,$$

откуда следует, что $\lambda=\dfrac{\alpha}{2}$ и $\mu=\dfrac{\alpha s+\beta f}{2}$, где $\alpha,\beta\in\mathbb{Z}$. Поскольку квадрат этого элемента лежит в H, получаем, что $\alpha g+\beta f\equiv 0\pmod 2$.

Группа G не изменится, если прибавить 2 к α или β, поскольку $[e,e^{s}]$, $[1,e^{f}]\in H$. По аналогичным причинам, хоть s изначально определено только по модулю f, равенство

$$*[e^{\alpha/2}, e^{(\alpha s+\beta f)/2}]=*[e^{\alpha/2}, e^{(\alpha(s+f)+(\beta-\alpha)f)/2}]$$

показывает, что

$$\langle s,\alpha,\beta\rangle\approx\langle s+f,\alpha,\beta-\alpha\rangle,$$

так что можно теперь считать, что s определено по модулю $2f$. Поскольку $[e^{s},s]=[e,e^{s}]^{*[a,b]}$ и $[e,e^{s^2}]$ лежат в H, для некоторого $g\in\mathbb{Z}$ должно выполняться равенство $s^2=fg+1$.

Чтобы выяснить, какие получающиеся группы совпадают, мы должны перебрать все элементы, переводящие данную группу $\langle s,\alpha,\beta\rangle$ в подобную группу $\langle s',\alpha',\beta'\rangle$. Элемент, осуществляющий такое преобразование, можно привести по модулю H; с учетом $*$ и $[1,j]$ (переводящих $\langle s,\alpha,\beta\rangle$ в себя или в $\langle -s,\alpha,-\beta\rangle$), можно считать, что этот элемент нормализует H и тем самым имеет вид $[e^{a/2}, e^{(as+bf)/2}]$, где $a,b\in\mathbb{Z}$. Преобразование с помощью такого элемента прибавляет кратное пары (f,g) (возможно, нечетное) к (α,β), так что единственное дополнительное соотношение есть $\langle s,\alpha,\beta\rangle\approx\langle s,\alpha+f,\beta+g\rangle$.

---

[1] Во втором случае можно упростить группу, выбрав новые образующие. Именно, сопряжение на $[1,e^{\lambda}]$ оставляет на месте E и заменяет $*[e^{\lambda}, e^{\mu}j]$ на $*[1,e^{\mu-\lambda}j]=*[1,J]$; после этого можно подставить J вместо j, поскольку $(*[1,J])^2=[J,J]$ должно лежать в H.

Итак, для групп $\pm[D\times D]\cdot 2^{(\alpha,\beta)}$ имеем следующее:

Параметры	Условия	Совпадения
$\alpha \pmod 2$	$s^2=fg+1$	$\langle s,\alpha,\beta\rangle\approx$
$\beta \pmod 2$	$\alpha g+\beta f\equiv 0 \pmod 2$	$\approx\langle -s,\alpha,-\beta\rangle\approx$
$s \pmod{2f}$		$\approx\langle s+f,\alpha,\beta-\alpha\rangle\approx$
		$\approx\langle s,\alpha+f,\beta+g\rangle,$

тогда как для $\pm[D\times D^{(s)}]\cdot\overline{2}$ имеем

Параметры	Условия	Совпадения
$s \pmod f$	$s^2=fg-1$	$\langle s\rangle\approx\langle -s\rangle.$

Совпадения для остальных случаев собраны в следующую таблицу.

Группа	Параметры	Условия	Совпадения
$+[D\times D^{(s)}]\cdot 2^{(\alpha,\beta)}$	$\alpha \pmod 2$	$s^2=fg+1$	$\langle s,\alpha,\beta\rangle\approx$
	$\beta \pmod 4$	$\alpha g\equiv 0 \pmod 4$	$\approx\langle -s,\alpha,-\beta\rangle\approx$
	$s \pmod{4f}$	n нечетно, g четно	$\approx\langle s+2f,\alpha,\beta-2\alpha\rangle\approx$
			$\approx\langle s,\alpha,\beta+2h\rangle$
$+[D\times D]\cdot\overline{2}$	$s \pmod{2f}$	$s^2=fg-1$, $g=2h$ четно	$\langle s\rangle\approx\langle -s\rangle$
$\pm[C\times C]\cdot 2^{(\gamma)}$	$s \pmod f$	$s^2=fg-1$	$\langle s,\gamma\rangle\approx$
	$\gamma \pmod 2$	$(g,s-1)\gamma\equiv 0 \pmod 2$	$\approx\langle s,-\gamma\rangle$
	$*[\mathbf{1},e^{\gamma(f,s+1)/2}]$	$(f,s+1)\gamma\equiv 0 \pmod 2$	
		g четно	
$+[C\times C]\cdot 2^{(\gamma)}$	$s \pmod{2f}$	$s^2=fg-1$	$\langle s,\gamma\rangle\approx$
	$\gamma \pmod{2d}$	$(g,s-1)\gamma\equiv 0 \pmod 2$	$\approx\langle s,-\gamma\rangle$
	$*[1,e^{\gamma(f,s+1)/2}]$	$(f,s+1)\gamma\equiv 0 \pmod 2$	
	$d=\dfrac{(2f,s+1)}{(f,s+1)}$	n нечетно, $g=2h$ четно	

В таблице 4.4 собрана информация про ахиральные группы из последних четырех строк таблицы 4.3. В последних восьми строках таблицы 4.3 можно всюду заменять D_2 на C_2 и $\bar{D}_4$ на D_4.

f, g четны	$\cdot 2^{(0,0)}, \cdot 2^{(0,1)}, \cdot 2^{(1,0)}, \cdot 2^{(1,1)}$ и $\cdot\overline{2}$	
иначе	$\cdot 2$ и $\cdot\overline{2}$	
f, h четны	$\cdot 2^{(0,0)}, \cdot 2^{(0,2)}, \cdot 2^{(1,0)}, \cdot 2^{(1,2)}$ и $\cdot\overline{2}$	
иначе	$\cdot 2$ и $\cdot\overline{2}$	
g четно	$\cdot 2^{(0)}, \cdot 2^{(d)}$ и $\cdot\overline{2}$	
иначе	$\cdot 2$ и $\cdot\overline{2}$	
h четно	$\cdot 2^{(0)}, \cdot 2^{(d)}$ и $\cdot\overline{2}$	$d = \frac{(2f, s+1)}{(f, s+1)}$
иначе	$\cdot 2$ и $\cdot\overline{2}$	

Табл. 4.4. Различные ахиральные группы

Гурвицевы целые кватернионы

§ 5.1. Гурвицевы целые кватернионы

Какие кватернионы $q = a + bi + cj + dk$ следует считать *целыми*? Одна очевидная возможность — имитировать определение гауссовых целых чисел и потребовать, чтобы a, b, c и d были обычными целыми числами. Говоря технически, мы называем кватернион $a + bi + cj + dk$ *липшицевым целым*, если и только если $a, b, c, d \in \mathbb{Z}$. Это условие равносильно тому, что $q = z_1 + z_2 j$, где z_1 и z_2 — гауссовы целые. Позднее, однако, Гурвиц предложил другое определение, при котором свойства целых кватернионов оказываются более приятными. Мы будем говорить, что $a + bi + cj + dk$ является *гурвицевым целым*, если a, b, c и d либо все лежат в $\mathbb{Z}$, либо все лежат в $\mathbb{Z} + \frac{1}{2}$.

Когда мы в главе 2 изучали арифметику гауссовых целых, важную роль играло «деление с остатком»: возможность поделить произвольное (гауссово) целое число Z на произвольное ненулевое z, получив целое частное Q и остаток R, который будет строго меньше делителя. Напомним, как это доказывалось: если $Z/z = a + bi$ и если положить $Q = A + Bi$, где A и B — целые числа, ближайшие к a и b, то

$$R/z = Z/z - Q = (a - A) + (b - B)i,$$

так что

$$N(R/z) = (a - A)^2 + (b - B)^2 \leqslant (1/2)^2 + (1/2)^2 = 1/2 < 1.$$

Если, однако, Z и $z \neq 0$ — липшицевы целые кватернионы, причем $q = Zz^{-1} = a + bi + cj + dk$, и если A, B, C и D — целые числа, ближайшие к a, b, c и d, то, полагая $Q = A + Bi + Cj + Dk$ и $R = Z - qz$, имеем

$$N(Rz^{-1}) = (a - A)^2 + \ldots + (d - D)^2 \leqslant (1/2)^2 + \ldots + (1/2)^2 = 1,$$

из чего следует только неравенство $N(R) \leqslant N(z)$. К сожалению, то обстоятельство, что неравенство является нестрогим, оказывается кри-

тически важным, поскольку в рассуждении используется спуск по величине норм.

Заметим, что случай $N(R)=N(z)$ возникает, только если

$$|a-A|=|b-B|=|c-C|=|d-D|=1/2,$$

то есть когда a, b, c и d лежат в $\mathbb{Z}+\frac{1}{2}$. Именно поэтому гурвицево определение более удачно: если Z и $z\neq 0$ суть гурвицевы целые кватернионы, а q, Q и R определяются так же, как выше, то либо

$$Z=Qz+R, \quad \text{где } N(R)<N(z),$$

либо

$$N(R)=N(z),$$

и из приведенного выше рассуждения следует, что q является гурвицевым целым и $Z=qz+0$ (где $N(0)<N(z)$).

Мы доказали следующее: гурвицевы целые (в отличие от липшицевых) обладают «свойством деления с остатком». Поэтому с гурвицевыми целыми H работать проще, чем с лишпицевыми целыми L, и утверждения про L обычно выводят из утверждений про H.

§ 5.2. Простые и единицы

Перейдем к теории разложения гурвицевых целых на простые множители. Простое гурвицево целое P — это гурвицево целое, норма которого является рациональным простым числом p. Подобно тому, как $p=p\times 1$ и $p=1\times p$ — единственные способы разложить p в произведение двух рациональных простых, единственно возможные разложения P в произведение двух гурвицевых простых должны иметь вид

$$P=P'\times U \quad \text{или} \quad P=V\times P'',$$

где $N(P')=N(P'')=p$ и $N(U)=N(V)=1$. Стало быть, нам надо также изучить *гурвицевы единицы*, т. е. гурвицевы целые с нормой 1.

Теорема 1. *Имеется в точности* 24 *гурвицевых единицы:* 8 *липшицевых единиц* ± 1, $\pm i$, $\pm j$, $\pm k$ *и еще* 16 *единиц вида* $\pm\frac{1}{2}\pm\frac{1}{2}i\pm\frac{1}{2}j\pm\frac{1}{2}k$.

Доказательство. У липшицевой единицы одно из чисел $|a|$, $|b|$, $|c|$ или $|d|$ должно быть не меньше единицы, так что из равенства $a^2+b^2+c^2+d^2=1$ вытекает, что эта координата равна ± 1, а остальные — нулю. В остальных случаях все числа $|a|$, $|b|$, $|c|$ и $|d|$ должны быть $\geqslant\frac{1}{2}$, а поскольку $a^2+b^2+c^2+d^2=1$, все эти числа равны $\pm\frac{1}{2}$. □

Гурвицевы единицы полностью решают проблему разложения гурвицева простого. Именно, если P — гурвицево простое, то всякое разложение P в произведение гурвицевых целых имеет вид

$$P = PU^{-1} \times U \quad \text{или} \quad P = V \times V^{-1}P,$$

где U и V пробегают все 24 гурвицевы единицы. Этими разложениями все исчерпывается, поскольку мы уже показали, что один из сомножителей должен быть единицей, а второй сомножитель однозначно определяется первым; выписанные разложения законны, поскольку если U и V — единицы, то U^{-1} и V^{-1} — тоже единицы, так что PU^{-1} и $V^{-1}P$ — гурвицевы целые.

Разложение гурвицева целого на простые существенно зависит от того, является ли это гурвицево число импримитивным (т. е. делится ли оно на какое-то натуральное число $n > 1$). В примитивном случае имеем следующий факт.

Теорема 2. *Пусть Q — примитивное гурвицево целое с нормой q. Тогда всякому разложению $q = p_0 p_1 \ldots p_k$ в произведение простых рациональных чисел соответствует разложение*

$$Q = P_0 P_1 \ldots P_k$$

в произведение гурвицевых простых, для которого $N(P_0) = p_0$, ..., $N(P_k) = p_k$. Мы будем говорить, что разложение $Q = P_0 P_1 \ldots P_k$ моделируется разложением $N(Q) = p_0 p_1 \ldots p_k$. Более того, если разложение $Q = P_0 P_1 \ldots P_k$ моделируется разложением $p_0 p_1 \ldots p_k$, то все прочие разложения числа Q имеют вид

$$Q = P_0 U_1 \cdot U_1^{-1} P_1 U_2 \cdot \ldots \cdot U_k^{-1} P_k;$$

иными словами, разложение по данной модели единственно с точностью до переноса единиц.

Так, примитивный гурвицев кватернион с нормой 60 имеет, с точностью до переноса единиц, ровно 12 разложений на простые кватернионы; это разложения, моделируемые следующими 12 разложениями нормы в произведение рациональных простых:

$$2 \cdot 2 \cdot 3 \cdot 5, \quad 2 \cdot 2 \cdot 5 \cdot 3, \quad 2 \cdot 3 \cdot 2 \cdot 5, \quad 2 \cdot 5 \cdot 2 \cdot 3, \quad 2 \cdot 3 \cdot 5 \cdot 2, \quad 2 \cdot 5 \cdot 3 \cdot 2,$$
$$3 \cdot 2 \cdot 2 \cdot 5, \quad 5 \cdot 2 \cdot 2 \cdot 3, \quad 3 \cdot 2 \cdot 5 \cdot 2, \quad 5 \cdot 2 \cdot 3 \cdot 2, \quad 3 \cdot 5 \cdot 2 \cdot 2, \quad 5 \cdot 3 \cdot 2 \cdot 2.$$

Общее количество разложений будет равно $24^3 \times 12 = 165888$, поскольку мы можем переносить любую из 24 единиц в трех местах.

Доказательство. В этом месте мы сменим обозначения и будем писать $[x]$ вместо $N(x)$, а соответствующее скалярное произведение

обозначать через $[x, y]$. Идеал $p_0\mathsf{H}+Q\mathsf{H}$ должен быть главным, так что имеем

$$p_0\mathsf{H}+Q\mathsf{H}=P_0\mathsf{H}$$

для некоторого P_0; поскольку $[P_0]$ должно быть делителем числа $[p_0]=p_0^2$, получаем, что $[P_0]$ должно равняться 1, p_0 или p_0^2.

Если $[P_0]=1$, то $p_0\mathsf{H}+Q\mathsf{H}$ совпадает со всем H, что невозможно, поскольку норма элемента p_0a+Qb равна

$$[p_0a]+2[p_0a, Qb]+[Qb]=p_0^2[a]+2p_0[a, Qb]+p_0\ldots p_k[b],$$

что делится на p_0. Не может норма P_0 равняться и p_0^2, поскольку из того, что P_0 делит p_0, вытекает, что $p_0=P_0U$, где U — единица (так как $[U]=1$), и отсюда следует, что Q делится на p_0 (поскольку это верно для $P_0=p_0U^{-1}$). Единственная остающаяся возможность состоит в том, что $[P_0]=p_0$, так что P_0 — гурвицево простое, делящее Q.

Итак, имеем $Q=P_0Q_1$, где $[Q_1]=p_1\ldots p_k$ и P_0 определено однозначно с точностью до умножения справа на единицу. Повторяя это рассуждение, получаем аналогичные разложения

$$Q_1=P_1Q_2, \quad Q_2=P_2Q_3, \quad \ldots,$$

где P_1, P_2, ... — гурвицевы простые с нормами p_1, p_2, ... Отсюда получаем разложение $Q=P_0P_1\ldots P_kQ'$, в котором Q' должно быть единицей (и тем самым может быть включено в P_k). По ходу рассуждения мы убедились и в том, что разложение единственно с точностью до переноса единиц. □

§ 5.3. Кватернионное разложение обычных простых чисел

Перед тем как продолжить наши рассмотрения, нам нужно изучить кватернионные разложения целых рациональных чисел и, в частности, рациональных простых чисел p. Напомним, что

(i) *квадратичный вычет* r удовлетворяет сравнению $r\equiv a^2 \pmod p$ для некоторого $a\not\equiv 0 \pmod p$,

в то время как *квадратичные невычеты* суть все остальные числа, не сравнимые с 0 по модулю p. Мы покажем, что

(ii) всякий квадратичный невычет n удовлетворяет сравнению $n\equiv a^2+b^2 \pmod p$ для некоторых $a, b\not\equiv 0 \pmod p$

и что

(iii) $0\equiv a^2+b^2+c^2 \pmod p$ для некоторых $a, b, c\not\equiv 0 \pmod p$.

Поскольку все квадратичные невычеты можно получить из одного невычета умножением на всевозможные вычеты, достаточно доказать (ii) для числа n, являющегося наименьшим квадратичным невычетом. Такое n имеет вид $r+1$, где r — квадратичный вычет, так что из $r \equiv a^2 \pmod p$ вытекает, что $n \equiv a^2 + 1^2 \pmod p$. Чтобы доказать (iii), заметим, что $0 = -1 + 1^2$, и это сравнимо с суммой $\leqslant 3$ квадратов (включая 1^2), поскольку -1 сравнимо с суммой $\leqslant 2$ квадратов. Теперь мы можем доказать следующее утверждение.

Теорема 3. *Всякое рациональное простое число p допускает хотя бы одно кватернионное разложение*

$$p = P_0\bar{P}_0.$$

Доказательство. Поскольку $x^2 \equiv (p-x)^2 \pmod p$, в (iii) можно предположить, что $0 \leqslant a, b, c \leqslant p/2$; тем самым существует разложение $a^2+b^2+c^2 = mp$, где $0 < m < p$, и кватернион $Q = a + bi + cj$ с нормой mp. Если теперь $p\mathsf{H} + Q\mathsf{H} = P_0\mathsf{H}$, то, как и раньше, имеем $[P_0] = p$.

На самом деле разложений числа p имеется столько же, сколько есть кватернионов с нормой p. Аналитическими методами можно установить, что это количество равно $24(p+1)$, если $p > 2$, и 24, если $p = 2$. □

Как обстоит дело с единственностью разложения кватерниона Q, если он импримитивен? Предположим, что у кватерниона Q с нормой $2^{n_0}p_1^{n_1}p_2^{n_2}\ldots p_k^{n_k}$ наибольший общий делитель координат есть целое число $2^{s_0}p_1^{s_1}p_2^{s_2}\ldots p_k^{s_k}$. Тогда ответ на заданный вопрос дается следующей теоремой.

Теорема 4. *Число разложений (считаемых с точностью до переноса единиц), моделируемых данным разложением числа $N(Q)$ на простые множители, равно произведению*

$$\prod_{i \geqslant 1} C_{n_i, s_i}(p_i),$$

то есть произведению значений «усеченных многочленов Каталана» в участвующих в разложении простых числах.

Первые несколько многочленов Каталана имеют вид

$$\begin{aligned} C_0(x) = C_1(x) &= 1, \\ C_2(x) &= x+1, \\ C_3(x) &= 2x+1, \\ C_4(x) &= 2x^2+3x+1; \end{aligned}$$

коэффициенты этих многочленов можно увидеть на «треугольнике Каталана» (рис. 5.1; см. также [22]). Усеченный многочлен Каталана

×														
	1													
×		1												
	1		1											
×		2		1										
	2		3		1									
×		5		4		1								
	5		9		5		1							
×		14		14		6		1						
	14		28		20		7		1					
×		42		48		27		8		1				

Рис. 5.1. Треугольник Каталана строится так же, как треугольник Паскаля, но никакое число не может появиться левее вертикальной черты

$C_{n,s}(x)$ представляет собой сумму одночленов степени $\leqslant s$, входящих в $C_n(x)$.

Доказательство. Достаточно рассматривать разложения вида

$$Q = P_1 P_2 \ldots P_n,$$

где все P_i имеют одну и ту же простую норму p.

Предположим теперь, что кватернион Q (имеющий норму p^n) делится на p^s, но не на p^{s+1}, и запишем равенство $Q = p^s P$. Поскольку P примитивен, у него имеется разложение

$$P = P_1' P_2' \ldots P_{n-2s}',$$

единственное с точностью до переноса единиц.

Мы сошлемся на тот факт, что (с точностью до умножения справа на единицу) имеется ровно $p+1$ кватернион с нормой p, и зададимся вопросом, совпадают ли P_1 и P_1' (опять-таки с точностью до умножения справа на единицу). В том единственном случае, если это действительно так, задача сводится к вопросу о разложении кватерниона с нормой p^{n-1}, который по-прежнему делится на p^s, но не на бóльшую степень p; согласно предположению индукции, число решений этой задачи равно $C_{n-1,s}(p)$. В каждом из тех p случаев, когда P_1 не совпадает с P_1', задача сводится к вопросу о разложении кватерниона с нормой p^{n-1}, делящегося на p^{s-1}, но не на бóльшую степень p; каждый из этих случаев дает тем самым $C_{n-1,s-1}(p)$ решений. Стало быть,

получаем рекуррентное соотношение

$$C_{n,s}(p) = C_{n-1,s}(p) + pC_{n-1,s-1}(p),$$

задающее многочлены Каталана. Например, задача о разложении кватерниона с нормой p^7, делящегося на p^2, но не на p^3, сводится к задаче о разложении кватерниона с нормой p^6, делящегося на p^2, но не p^3 (всего $C_{6,2} = 9p^2 + 5p + 1$ решений) и к p задачам о разложении кватерниона с нормой p^6, делящегося на p, но не на p^2 (у каждой по $C_{6,1} = 5p + 1$ решений). В сумме действительно получается

$$9p^2 + 5p + 1 + p(5p + 1) = 14p^2 + 6p + 1 = C_{7,2}(p). \qquad \square$$

Для кватерниона с нормой $p^m q^n \ldots$ и наибольшим общим делителем координат $p^s q^t \ldots$ мы получаем то же количество возможностей для сомножителей с нормой p, независимо от того, где они расположены, так что общее количество разложений с точностью до переноса единиц равно произведению количеств таких разложений для отдельных простых множителей.

§ 5.4. Задача о метакоммутировании

Даже разложение целых рациональных чисел не единственно: например,

$$60 = 2 \cdot 2 \cdot 3 \cdot 5 = 2 \cdot 3 \cdot 5 \cdot 2 = (-3) \cdot 2 \cdot 5 \cdot (-2) = \ldots$$

Тем не менее, мы справедливо считаем разложение единственным, поскольку все такие разложения легко получаются одно из другого.

Теорему 2 обычно называют теоремой об однозначном разложении для примитивных (гурвицевых) кватернионов, и она действительно заслуживает такого названия, пока речь идет о разложениях по данной модели, поскольку любые два такие разложения получаются одно из другого с помощью понятной операции переноса единиц (в импримитивном случае к ней надо добавить еще рекомбинацию — см. ниже).

Однако же, чтобы иметь возможность говорить о подлинной единственности для разложения гурвицевых целых, следовало бы решить следующую задачу, которую мы назовем *задачей о метакоммутировании*: как по разложению PQ, моделируемому разложением pq, найти разложение $Q'P'$, моделируемое разложением qp? Похоже, эта трудная задача нигде в литературе не ставилась.

Существует три основных способа изменить разложение на простые. Мы уже имели дело с переносом единиц, заменяющим PQ на

$PU \cdot \bar{U}Q$. Возможна также *рекомбинация*, при которой пара сопряженных простых $P\bar{P}$ (с нормой p) заменяется на любую другую пару $P'\bar{P}'$ (с той же нормой). Наконец, всякое произведение PQ двух различных гурвицевых простых с нормами p и q можно разложить по-новому в произведение $Q'P'$ гурвицевых простых с нормами q и p; мы назовем эту операцию *метакоммутированием* простых P и Q; новое разложение $Q'P'$ единственно с точностью до переноса единиц. Нетрудно видеть, что любые два разложения одного и того же кватерниона на простые множители можно получить друг из друга с помощью последовательного выполнения преобразований этих трех типов.

§ 5.5. Разложение липшицевых целых

Чтобы разобраться с разложением липшицевых целых, надо понять, как они связаны с гурвицевыми (и с аддитивной, и с мультипликативной точки зрения).

С геометрической точки зрения множество липшицевых целых L представляет собой четырехмерную кубическую решетку I_4. В множество чисел Гурвица вложены еще две решетки, изоморфные I_4, а именно[1] $\omega\mathsf{L} = I_4'$ и $\bar{\omega}\mathsf{L} = I_4''$. Пересечение этих трех кубических решеток (совпадающее с пересечением любых двух из них) есть

$$\mathsf{L} \cap \omega\mathsf{L} \cap \bar{\omega}\mathsf{L} = D_4$$

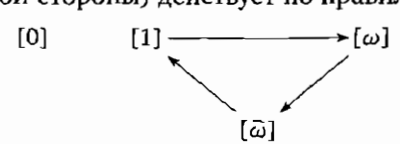
(четырехмерная «ортоплектическая решетка», она же решетка корней типа D_4). Решетка чисел Гурвица есть объединение этих трех решеток:

$$\mathsf{H} = \mathsf{L} \cup \omega\mathsf{L} \cup \bar{\omega}\mathsf{L} = D_4^*;$$

обозначение объясняется тем, что эта решетка действительно двойственна к D_4.

Заметим, что D_4 как аддитивная группа имеет четыре смежных класса в D_4^*, а именно $[0]$, $[1]$, $[\omega]$ и $[\bar{\omega}]$; решетки, упоминавшиеся нами, представляют собой различные объединения этих смежных классов (рис. 5.2).

При рассмотрении мультипликативной структуры важно, что умножение на ω (с любой стороны) действует по правилу



[1] Здесь и далее $\omega = \frac{1}{2}(-1 + i + j + k)$. — *Прим. ред.*

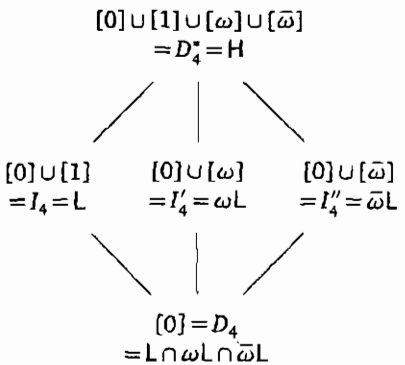


Рис. 5.2. Включения между подрешетками в H

и тем самым оставляет на месте D_4 и D_4^*, но циклически переставляет I_4, I_4' и I_4''.

Гурвицевы целые с четной нормой — это в точности элементы класса смежности [0]; на самом деле они останутся в этом классе и после умножения на ω или $\bar{\omega}$ (с любой стороны). Гурвицево целое Q с нечетной нормой лежит в [1], $[\omega]$ или $[\bar{\omega}]$; равносильное утверждение: ровно одно из Q, ωQ и $\bar{\omega}Q$ лежит в [1].

Подсчет количества липшицевых разложений

Приведенные выше рассмотрения позволяют доказать следующий факт.

Лемма 1. *Всякое разложение липшицева целого в произведение гурвицевых можно с помощью переноса единиц перевести в разложение липшицева целого в произведение липшицевых.*

Поскольку единицы, которые мы будем переносить, суть степени ω, не являющегося липшицевым целым, из этой леммы следует, что разложение липшицевых целых свойством единственности заведомо не обладает.

Доказательство. Посмотрим, как «сдвиг омеги»

$$\alpha = \beta\gamma \to \alpha = \beta\omega \cdot \bar{\omega}\gamma$$

влияет на двучленное разложение липшицева целого α. Поскольку α лежит в [0] или [1], на рис. 5.3 перечислены все возможные смежные классы, в которые могут попасть β и γ; в каждой тройке присутствует разложение, в котором оба множителя липшицевы. □

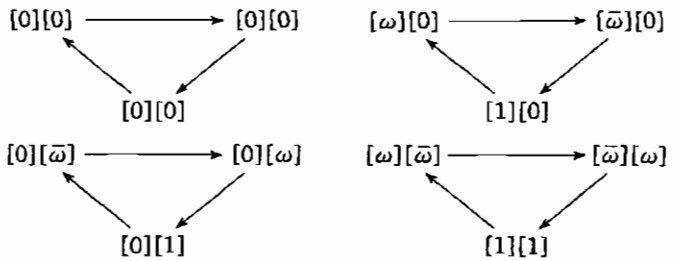


Рис. 5.3. Сдвиг омеги: $\beta\gamma \to \beta\omega \cdot \bar{\omega}\gamma$

С помощью более тщательного анализа можно получить следующий результат.

ТЕОРЕМА 5. *Число липшицевых разложений, получающихся переносом единиц из*

$$P_1P_2\ldots P_k,$$

равно $8^{k-1}3^{l-1}$, *где* l — *число сомножителей с четной нормой.*

В самом деле, мы можем передвигать любую из восьми липшицевых единиц между соседними множителями p_i и p_{i+1}, ..., p_k, а для случая, когда оба множителя имеют четную норму, у нас есть еще три степени ω.

Октавы и их приложения к семи- и восьмимерной геометрии

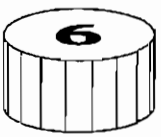
Октавы — это формальные выражения

$$x_\infty + x_0 i_0 + x_1 i_1 + x_2 i_2 + x_3 i_3 + x_4 i_4 + x_5 i_5 + x_6 i_6$$

(все x_t действительны); они образуют алгебру над действительными числами, с образующими $i_0, \ldots, i_6$, удовлетворяющими соотношениям

$$i_n^2 = -1,$$
$$i_{n+1} i_{n+2} = i_{n+4} = -i_{n+2} i_{n+1},$$
$$i_{n+2} i_{n+4} = i_{n+1} = -i_{n+4} i_{n+2},$$
$$i_{n+4} i_{n+1} = i_{n+2} = -i_{n+1} i_{n+4}$$

(индексы рассматриваются как вычеты по модулю 7).



Композиционные алгебры

В главе 2 мы проинтерпретировали тождество с двумя квадратами

$$(x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2 = (x_1^2 + x_2^2)(y_1^2 + y_2^2)$$

как утверждение о том, что в алгебре комплексных чисел норма произведения равна произведению норм; мы будем записывать это тождество в виде[1]

$$[z_1z_2] = [z_1][z_2].$$

В главах 3 и 4 мы существенно пользовались аналогичным результатом для алгебры кватернионов.

В этой главе мы докажем знаменитую теорему Гурвица, утверждающую, что всякая алгебра с таким «композиционным свойством» совпадает с одной из хорошо известных алгебр в размерностях 1, 2, 4 и 8 (совпадает *в точности*, если у алгебры есть единица по умножению, и *с точностью до изотопии* в противном случае). Предположим для начала, что у алгебры есть двусторонняя единица 1, так что $1x = x = x1$, и положим, как обычно,

$$[x, y] = \frac{[x+y] - [x] - [y]}{2}$$

(мы работаем над полем действительных чисел, где 2 обратимо). Мы будем неоднократно пользоваться тем обстоятельством, что если $[x, t] = [y, t]$ для всех t, то $x = y$.

§ 6.1. Свойства умножения

Начнем с того, что выведем некоторые следствия из *композиционного свойства*

$$[xy] = [x][y]. \qquad \text{(M1)}$$

[1] В этой главе мы пользуемся квадратными скобками для обозначения норм и скалярных произведений; разумеется, не следует путать эти обозначения с обозначениями для некоторых отображений в предыдущих главах.

Правило масштабирования:

$$[xy, xz] = [x][y, z] \quad (\text{и } [xz, yz] = [x, y][z]). \tag{M2}$$

Доказательство. Заменяя y на $y+z$ в (M1), получаем

$$[xy] + [xz] + 2[xy, xz] \overset{\text{M1}}{=} [x]([y] + 2[y, z] + [z]);$$

остается привести подобные и поделить на два. □

Правило обмена:

$$[xy, uz] = 2[x, u][y, z] - [xz, uy]. \tag{M3}$$

Доказательство. Заменяя x на $x+u$ в (M2), получаем

$$[xy, xz] + [xy, uz] + [uy, xz] + [uy, uz] \overset{\text{M2}}{=} ([x] + 2[x, u] + [u])[y, z];$$

теперь приводим подобные и группируем слагаемые. □

§ 6.2. Свойства сопряжения

Теперь мы докажем три правила, в которых участвует сопряжение $\bar{x} = 2[x, 1] - x$.

Правила косы:

$$[xy, z] = [y, \bar{x}z] \quad (\text{и } [xy, z] = [z, z\bar{y}]). \tag{C1}$$

Доказательство. Полагая $u = 1$ в (M3), получаем

$$2[x, 1][y, z] - [xz, y] = [y, (2[x, 1] - x)z].$$ □

(Название этого правила поясняется на рис. 6.1)

Двойное сопряжение:

$$\bar{\bar{x}} = x. \tag{C2}$$

Доказательство. Положим $y = 1$ и $z = t$ и применим дважды (C1); получим, что

$$[x, t] = [x1, t] = [1, \bar{x}t] = [\bar{\bar{x}}1, t] = [\bar{\bar{x}}, t]$$

для всех t. □

Сопряжение и умножение:

$$\overline{xy} = \bar{y}\bar{x}. \tag{C3}$$

Доказательство. Применяя правило (C1), получаем:

$$[\bar{y}\bar{x}, t] = [\bar{x}, yt] = [\bar{x}\bar{t}, y] = [\bar{t}, xy] = [\bar{t}, xy \cdot 1] = [\bar{t}\overline{xy}, 1] = [\overline{xy}, t].$$ □

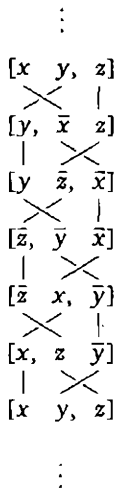


Рис. 6.1. Правило косы связывает между собой шесть скалярных произведений

§ 6.3. Свойства удвоения

Пусть теперь через H обозначена n-мерная подалгебра, содержащая 1, и пусть i — единичный вектор, ортогональный к H; буквами $a, b, c, \ldots$ будут обозначаться элементы алгебры H. Имеем $\bar{i} = -i$ и $[i, a] = 0$ (благодаря этим равенствам у нас при применении правила обмена будет часто обращаться в нуль слагаемое $2[x, u][y, z]$). Наши следующие три правила объясняют, как устроены скалярное произведение, сопряжение и умножение на алгебре $H + iH$ — «диксоновском удвоении» алгебры H.

Скалярное произведение на удвоении:

$$[a + ib, c + id] = [a, c] + [b, d]. \tag{D1}$$

Доказательство. Это вытекает из трех равенств:

$$[a, id] = [a\bar{d}, i] = 0, \quad [ib, c] = [i, c\bar{b}] = 0, \quad [ib, id] = [i][b, d] = [b, d]. \qquad \square$$

Сопряжение на удвоении:

$$\overline{a + ib} = \bar{a} - ib \tag{D2}$$

(так что $ib = -\overline{ib} = -\bar{b}\bar{i} = \bar{b}i$).

Доказательство. $\overline{ib} = 2[ib, 1] - ib = -ib.$ $\square$

Умножение на удвоении:

$$(a+ib)(c+id)=(ac-d\bar{b})+i(cb+\bar{a}d). \tag{D3}$$

Доказательство. Это вытекает из трех равенств:

$$[a\cdot id,t]\overset{C1}{=}[id,\bar{a}t]\overset{M3}{=}0-[it,\bar{a}d]\overset{C1}{=}[t,i\cdot\bar{a}d];$$

$$[ib\cdot c,t]\overset{C1}{=}[ib,t\bar{c}]\overset{D2}{=}[\bar{b}i,t\bar{c}]\overset{M3}{=}0-[\bar{b}\bar{c},ti]\overset{C1}{=}[\bar{b}\bar{c}\cdot i,t]\overset{D2}{=}[i\cdot cb,t];$$

$$[ib\cdot id,t]\overset{C1}{=}-[ib,t\cdot id]\overset{M3}{=}0+[i\cdot id,tb]\overset{C1}{=}$$
$$\overset{C1}{=}-[id,i\cdot tb]\overset{M2}{=}-[i][d,tb]\overset{C1}{=}[-d\bar{b},t].$$ □

§ 6.4. Завершение доказательства теоремы Гурвица

Вычисления из предыдущего параграфа показывают, что если наша композиционная алгебра Z содержит собственную подалгебру, то она содержит и ее диксоновское удвоение. Следовательно, если Z конечномерна, то она должна получаться с помощью последовательных удвоений из своей наименьшей подалгебры $\mathbb{R}$; в частности, Z должна быть удвоением некоторой алгебры Y, а та, в свою очередь, должна быть удвоением некоторой алгебры X, и так далее. Покажем теперь, что свойство «быть композиционной алгеброй» может пережить не более трех операций удвоения.

Когда алгебра $Z=Y+i_ZY$ является композиционной? Ровно тогда, когда для любых $a, b, c, d\in Y$ имеем

$$[a+i_Zb][c+i_Zd]=[(ac-d\bar{b})+i_Z(cb+\bar{a}d)].$$

Поскольку, однако, это равенство расписывается в виде

$$[a][c]+[a][d]+[b][c]+[b][d]=$$
$$=[ac]-2[ac,d\bar{b}]+[d\bar{b}]+[cb]+2[cb,\bar{a}d]+[\bar{a}d],$$

равенство выполняется тогда и только тогда, когда

$$[ac,d\bar{b}]=[cb,\bar{a}d],$$

или, что равносильно, когда

$$[ac\cdot b,d]=[a\cdot cb,d],$$

и это верно тогда и только тогда, когда $ac\cdot b=a\cdot cb$ для всех $a, b, c\in Y$.

Итак, ответ на первый вопрос таков.

Лемма 1. *Z является композиционной алгеброй тогда и только тогда, когда Y является ассоциативной композиционной алгеброй.*

Когда $Y = X + i_Y X$ является ассоциативной композиционной алгеброй? Очевидно, что при этом алгебра X также должна обладать этими свойствами; поскольку, однако, $i_Y b \cdot c = i_Y \cdot cb$ для всех $b, c \in X$, должно выполняться тождество $bc = cb$, то есть X должна быть коммутативна.

С другой стороны, если $a, b, c, d, e, f \in X$, то

$$\begin{aligned}(a+i_Y b)(c+i_Y d)\cdot(e+i_Y f) &= [(ac-d\bar{b})+i_Y(cb+\bar{a}d)](e+i_Y f) = \\ &= (ac-d\bar{b})e - f(\bar{b}\bar{c}+\bar{d}a)+i_Y[e(cb+\bar{a}d)+(\bar{c}\bar{a}-b\bar{d})f] = \\ &= [ac\cdot e - d\bar{b}\cdot e - f\cdot\bar{b}\bar{c} - f\cdot\bar{d}a] + i_Y[e\cdot cb + e\cdot\bar{a}d + \bar{c}\bar{a}\cdot f - b\bar{d}\cdot f]\end{aligned}$$

и

$$\begin{aligned}(a+i_Y b)\cdot(c+i_Y d)(e+i_Y f) &= (a+i_Y b)[(ce-f\bar{d})+i_Y(ed+\bar{c}f)] = \\ &= a(ce-f\bar{d}) - (ed+\bar{c}f)\bar{b} + i_Y[(ce-f\bar{d})b+\bar{a}(ed+\bar{c}f)] = \\ &= [a\cdot ce - a\cdot f\bar{d} - ed\cdot\bar{b} - \bar{c}f\cdot\bar{b}] + i_Y[ce\cdot b - f\bar{d}\cdot b + \bar{a}\cdot ed + \bar{a}\cdot\bar{c}f];\end{aligned}$$

если X коммутативна и ассоциативна, то эти выражения совпадают.

Стало быть, верно следующее утверждение.

Лемма 2. *Y является ассоциативной композиционной алгеброй тогда и только тогда, когда X является коммутативной и ассоциативной композиционной алгеброй.*

Когда $X = W + i_X W$ является коммутативной и ассоциативной композиционной алгеброй? Пусть $a, b, c, d, e \in W$. Поскольку $ie = \bar{e}i$, необходимо, чтобы $e = \bar{e}$ для всех $e \in W$; иными словами, сопряжение на W должно быть тривиально.

Однако же

$$(a+i_X b)(c+i_X d) = (ac-d\bar{b}) + i_X(cb+\bar{a}d)$$

и

$$(c+i_X d)(a+i_X b) = (ca-b\bar{d}) + i_X(ad+\bar{c}b),$$

и эти выражения совпадают, если W коммутативна с тривиальным сопряжением. Таким образом, получаем лемму.

Лемма 3. *X является коммутативной и ассоциативной композиционной алгеброй тогда и только тогда, когда W — коммутативная ассоциативная композиционная алгебра с тривиальным сопряжением.*

Следовательно, мы доказали такую теорему.

Теорема 1 (Гурвиц). *$\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ и $\mathbb{O}$ — единственные возможные композиционные алгебры.*

В самом деле, $\mathbb{R}$ — коммутативная и ассоциативная композиционная алгебра с тривиальным сопряжением. Значит, $\mathbb{C}$ — коммутативная и ассоциативная композиционная алгебра *с нетривиальным сопряжением*. Значит, $\mathbb{H}$ — ассоциативная композиционная алгебра, *не являющаяся коммутативной*. Значит, $\mathbb{O}$ — композиционная алгебра, *не являющаяся ассоциативной*, а ее диксоновское удвоение композиционной алгеброй уже не будет.

Мы доказали знаменитую теорему Гурвица, гласящую, что всякая композиционная алгебра с единицей на вещественном евклидовом пространстве является одной из четырех перечисленных алгебр. Покажем теперь, что с точностью до изотопии это утверждение верно и для алгебр без единицы.

В произвольной композиционной алгебре выберем элементы u и v с нормой 1. Тогда отображения $x \to xv$ и $y \to uy$ являются ортогональными преобразованиями, так что у них имеются обратные α и β. Зададим теперь новое умножение по правилу $x \star y = x^{\alpha} y^{\beta}$. Тогда

$$[x \star y] = [x^{\alpha} y^{\beta}] = [x^{\alpha}][y^{\beta}] = [x][y],$$

умножение $\star$ также задает структуру композиционной алгебры; поскольку

$$uv \star uy = (uv)^{\alpha}(uy)^{\beta} = uy,$$
$$xv \star uv = (xv)^{\alpha}(uv)^{\beta} = xv,$$

элемент uv является двусторонней единицей относительно нового умножения[1].

§ 6.5. Другие свойства алгебр

Положим $x^{-1} = \bar{x}/[x]$, где $x \neq 0$.

Правила обращения: $\bar{x} \cdot xy = [x]y \approx yx \cdot \bar{x}$, или, что равносильно, $x^{-1} \cdot xy = y = yx \cdot x^{-1}$.

Доказательство. $[\bar{x} \cdot xy, t] = [xy, xt] = [x][y, t] = [[x]y, t]$. □

Закон альтернативности: $x \cdot xy = x^2 y$ и $yx \cdot x = yx^2$.

Доказательство. Подставьте $\bar{x} = 2[x, 1] - x$ в тождество $\bar{x} \cdot xy = \bar{x}x \cdot y$. □

Замечание. На самом деле теорема Брука—Клейнфельда [8] характеризует наши алгебры именно исходя из свойства альтернативно-

[1] На языке следующей главы это означает, что всякий элемент с нормой 1 можно перевести в единицу с помощью изотопии, так что монотопии на таких элементах транзитивны (что является характеристическим свойством луп Муфанг).

сти. Иногда тождество

$$xy \cdot x = x \cdot yx$$

называется третьим законом альтернативности. Мы докажем его сразу после того, как установим следующие

Правила Муфанг: $xy \cdot zx = x(yz) \cdot x = x \cdot (yz)x$.

Доказательство.

$$\begin{aligned}[xy \cdot zx, t] = [xy, t \cdot \bar{x}\bar{z}] &= 2[x, t][y, \bar{x}\bar{z}] - [x \cdot \bar{x}\bar{z}, ty] = \\ &= 2[x, t][yz, \bar{x}] - [\bar{x}\bar{z}, \bar{x} \cdot ty] = \\ &= 2[yz, \bar{x}][x, t] - [x][\bar{z}\bar{y}, t] = \\ &= 2[x, \overline{yz}][x, t] - [x][\overline{yz}, t].\end{aligned}$$

Стало быть, $xy \cdot zx = 2[x, \overline{yz}]x - [x]\overline{yz}$ зависит только от x и yz. Следовательно, можно заменить y и z на два любых других элемента с тем же произведением и получить, что

$$xy \cdot zx = x(yz) \cdot 1x = x(yz) \cdot x \quad \text{и} \quad xy \cdot zx = x1 \cdot (yz)x = x \cdot (yz)x. \qquad \square$$

Поскольку $y1 = 1y = y$, мы получаем и третий закон альтернативности:

$$xy \cdot x = xy \cdot 1x = x1 \cdot yx = x \cdot yx.$$

Как сообщил нам Смит (W. D. Smith), Шефером (R. D. Schafer) доказано, что *всякая* алгебра, получаемая из $\mathbb{R}$ с помощью итерации диксоновских удвоений, обладает свойством ассоциативности степеней, удовлетворяет тождествам $(ab)a = a(ba)$ и $(ab)a^2 = a(ba^2)$, и всякий элемент такой алгебры удовлетворяет некоторому квадратному уравнению. Смит также отмечает, что «вещественные части» октав ассоциативны: $[ab \cdot c, 1] = [a \cdot bc, 1]$.

§ 6.6. Отображения L_x, R_x и B_x

Ввиду отсутствия ассоциативности стоит поизучать операторы умножения. Определим операторы соответственно левого, правого и двустороннего умножения по формулам

$$L_x : y \to xy, \quad R_x : y \to yx, \quad B_x : y \to xyx.$$

Третий закон альтернативности показывает, что отображение B_x корректно определено и является произведением L_x и R_x (в любом порядке):

$$y^{L_x R_x} = xy \cdot x = y^{B_x} = x \cdot yx = y^{R_x L_x}.$$

Мы покажем также, что у B_x имеется геометрическая интерпретация в терминах отражений. В самом деле, если сравнить нашу формулу

$$xy \cdot zx = 2[x, \overline{yz}]x - [x]\overline{yz}$$

с обычным выражением

$$\mathrm{ref}(x): t \to t - \frac{2[x,t]}{[x]}x$$

для отражения относительно вектора x, получаем, что

$$xy \cdot zx = -[x](\overline{yz})^{\mathrm{ref}(x)} = [x](yz)^{\mathrm{ref}(1)\cdot\mathrm{ref}(x)},$$

так что B_x только на скалярный множитель отличается от $\mathrm{ref}(1)\cdot\mathrm{ref}(x)$.

Посмотрим на закон ассоциативности повнимательнее. Если записать его в виде

$$(yz)^{L_x} = y^{L_x}z, \quad (yz)^{R_x} = yz^{R_x},$$

то видно, что он утверждает, что применение оператора левого или правого умножения к произведению двух элементов равносильно применению этого оператора к одному из сомножителей. Правило же Муфанг для двустороннего умножения $xy \cdot zx = x(yz)x$, будучи записанным в виде $(yz)^{B_x} = y^{L_x}z^{R_x}$, означает, что вместо применения оператора двустороннего умножения к произведению достаточно применить операторы левого и правого умножения к двум сомножителям.

Существуют еще два правила Муфанг; обычно они записываются в виде

$$x(y \cdot xz) = xyx \cdot z \quad \text{и} \quad (yx \cdot z)x = y \cdot xzx,$$

и в таком виде ими пользоваться неудобно. Мы предпочитаем записывать их в эквивалентной форме («левое и правое муфангово правило умножения»)

$$x(yz) = xyx \cdot x^{-1}z \quad \text{и} \quad (yz)x = yx^{-1} \cdot xzx;$$

при этом становится ясно, как они заменяют ассоциативность, поскольку в такой форме они показывают, как заменить левое или правое умножение на произведение умножениями на отдельные сомножители:

$$(yz)^{L_x} = y^{B_x}z^{L_{x^{-1}}} \quad \text{и} \quad (yz)^{R_x} = y^{R_{x^{-1}}}z^{B_x}.$$

Мы еще не доказали, что в наших алгебрах выполняются эти два новых правила Муфанг. Мы сделаем это в следующей главе, когда покажем (с помощью правил обращения), что все три правила Муфанг равносильны.

§ 6.7. Координаты в кватернионах и октавах

Давайте теперь восстановим классические определения алгебр из нашего описания в терминах диксоновского удвоения. Заметим, что два единичных элемента, ортогональных к 1 и друг к другу (обозначим их i и j), обладают тем свойством, что $iji = j$, поскольку $B_i = \mathrm{ref}(1)\cdot\mathrm{ref}(i)$ очевидным образом оставляет на месте j. Стало быть,

$$ij = k \;\Rightarrow\; ki = j \quad \text{и аналогично} \quad ij = k \;\Rightarrow\; jk = i.$$

Кроме того,

$$k^2 = ijij = jj = -1$$

и

$$ji = \bar{j}\bar{i} = \bar{k} = -k.$$

Если обозначить через i тот единичный элемент, с присоединением которого $\mathbb{R}$ расширяется до $\mathbb{C}$, то получаем знаменитые соотношения Гамильтона

$$i^2 = j^2 = k^2 = -1,$$
$$ij = k,\ jk = i,\ ki = j,$$
$$ji = -k,\ kj = -i,\ ik = -j.$$

Для октав мы найдем семь единичных элементов $i_0, \ldots, i_6$, для которых перестановки

$$\alpha\colon i_n \to i_{n+1}, \quad \beta\colon i_n \to i_{2n}$$

(индексы — вычеты по модулю 7) сохраняют умножение. Для этого переобозначим единицы нашей исходной кватернионной подалгебры

$$i = i_1, \quad j = i_2, \quad k = i_4,$$

а затем, воспользовавшись единичным элементом i_0, положим $i_0 i_n = i_{3n}$, так что

$$i_0 i_1 = i_3, \quad i_0 i_2 = i_6, \quad i_0 i_4 = i_5.$$

Вспомним теперь, что если b и c лежат в кватернионной подалгебре $\langle 1, i_1, i_2, i_4\rangle$, то $i_0 b\cdot c = i_0\cdot cb$. Отсюда вытекает, что

$$i_6 i_1 = i_0 i_2 \cdot i_1 = i_0 \cdot i_1 i_2 = i_0 i_4 = i_5,$$
$$i_5 i_2 = i_0 i_4 \cdot i_2 = i_0 \cdot i_2 i_4 = i_0 i_1 = i_3,$$
$$i_3 i_4 = i_0 i_1 \cdot i_4 = i_0 \cdot i_4 i_1 = i_0 i_2 = i_6;$$

стало быть, i_x, i_y и i_z ведут себя как гамильтоновы i, j и k для каждой из семи «кватернионных троек» индексов

$$xyz = 124, 235, 346, 450, 561, 602, 013.$$

Поскольку все такие тройки имеют вид

$$i_{n+1}, i_{n+2}, i_{n+4}$$

(индексы — вычеты по модулю 7), наше утверждение про $i_0, \ldots, i_6$ выполнено.

§ 6.8. Симметрии и октавы: диассоциативность

Приведенное выше рассуждение дает нам также некоторую информацию о группе автоморфизмов октав. Именно, всякий единичный элемент, ортогональный к 1, может играть роль i_1; всякий единичный элемент, ортогональный к 1 и i_1, может играть роль i_2; и всякий единичный элемент, ортогональный к 1, i_1, i_2 и $i_1 i_2$, может играть роль i_0.

Точнее говоря, если j_1 — произвольный единичный элемент, ортогональный к 1, j_2 — произвольный единичный элемент, ортогональный к 1 и j_1, и, наконец, j_0 — произвольный единичный элемент, ортогональный к 1, j_1, j_2 и $j_1 j_2$, то существует один и только один автоморфизм, переводящий i_1 в j_1, i_2 в j_2 и i_0 в j_0. При этом j_1 пробегает точки на единичной сфере в семимерном пространстве, ортогональном к 1, элемент j_2 пробегает точки на единичной сфере в шестимерном пространстве, ортогональном к 1 и j_1, а элемент j_0 пробегает точки на единичной сфере в четырехмерном пространстве, ортогональном к 1, j_1, j_2 и $j_1 j_2$. Эти сферы являются многообразиями размерностей 6, 5 и 3, так что найденные нами симметрии образуют непрерывную группу размерности $6 + 5 + 3 = 14$. В стандартных обозначениях теории групп Ли эта группа Ли называется группой G_2. Мы продолжим обсуждение G_2 в главе 8.

Сейчас мы воспользуемся G_2 для доказательства артиновской «диассоциативности» октав.

Теорема 2. *Алгебра, порожденная любыми двумя октавами, ассоциативна.*

В самом деле, с точностью до автоморфизма октав можно считать, что первый из этих элементов имеет вид $x + i_1 y$, а второй $X + i_1 Y + i_2 Z$, так что они оба лежат в кватернионной подалгебре $\langle 1, i_1, i_2, i_4 \rangle$.

§ 6.9. Алгебры над другими полями

Основное внимание в этой книге мы уделяем композиционным алгебрам относительно стандартной положительно определенной квадратичной формы $x_1^2 + x_2^2 + \ldots + x_n^2$ над действительными числами. Тем

не менее доказательства в этой главе проходят почти без изменений для случая композиционных алгебр относительно произвольной невырожденной квадратичной формы над всеми полями характеристики, отличной от 2.

Напомним, что квадратичная форма $[x]$ называется *невырожденной*, если соответствующая билинейная форма удовлетворяет условию

$$([x,t]=0 \text{ для всех } t) \;\Rightarrow\; x=0.$$

Этого достаточно, чтобы обосновать те наши рассуждения, в которых равенство $x=y$ выводилось из того, что $[x,t]=[y,t]$ для всех t. Единственное изменение состоит в том, что нельзя гарантировать, что найдется ортогональный к H элемент, имеющий норму 1. Следовательно, надо позволить дополнительному элементу i иметь произвольную норму α; при этом правила удвоения примут вид

$$(a+ib)(c+id)=(ac-\alpha d\bar{b})+i(cb+\bar{a}d)$$

и $[a+ib]=[a]+\alpha[b]$.

На самом деле эти рассуждения работают и в характеристике 2, в каковом случае удвоение можно продолжать до бесконечности; см. Альберт [1] (а также Капланский [27]). Проблема тут возникает не с алгебрами, а с квадратичными формами: не всегда можно найти базис из попарно ортогональных векторов. Тем не менее, диксоновское удвоение алгебры H можно определить и с помощью i, не являющегося ортогональным к H: формулы при это станут более сложными, но структура рассуждения не изменится.

В одном важном отношении эти более общие алгебры могут отличаться от стандартных: в них могут существовать ненулевые элементы, не имеющие обратного. Именно, даже у невырожденной квадратичной формы может существовать (а над конечным полем — и обязательно будет существовать) ненулевой элемент x, для которого $[x]=0$.

§ 6.10. Тождества с одним, двумя, четырьмя и восемью квадратами

Существование четырех алгебр $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ и $\mathbb{O}$ равносильно существованию следующих тождеств с N квадратами, где $N=1,2,4,8$:

$$x_1^2y_1^2=(x_1y_1)^2;$$

$$(x_1^2+x_2^2)(y_1^2+y_2^2)=(x_1y_1-x_2y_2)^2+(x_1y_2+x_2y_1)^2;$$

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)=$$

$$= (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 +$$
$$+ (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2 +$$
$$+ (x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2)^2 +$$
$$+ (x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1)^2;$$

$$(x_\infty^2 + x_0^2 + \ldots + x_6^2)(y_\infty^2 + y_0^2 + \ldots + y_6^2) =$$
$$= (x_\infty y_\infty - x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6)^2 +$$
$$+ (x_\infty y_0 + x_0y_\infty + x_1y_3 + x_2y_6 + x_4y_5 - x_3y_1 - x_6y_2 - x_5y_4)^2 +$$
$$+ (x_\infty y_1 + x_1y_\infty + x_2y_4 + x_3y_0 + x_5y_6 - x_4y_2 - x_0y_3 - x_6y_5)^2 +$$
$$+ (x_\infty y_2 + x_2y_\infty + x_3y_5 + x_4y_1 + x_6y_0 - x_5y_3 - x_1y_4 - x_0y_6)^2 +$$
$$+ (x_\infty y_3 + x_3y_\infty + x_4y_6 + x_5y_2 + x_0y_1 - x_6y_4 - x_2y_5 - x_1y_0)^2 +$$
$$+ (x_\infty y_4 + x_4y_\infty + x_5y_0 + x_6y_3 + x_1y_2 - x_0y_5 - x_3y_6 - x_2y_1)^2 +$$
$$+ (x_\infty y_5 + x_5y_\infty + x_6y_1 + x_0y_4 + x_2y_3 - x_1y_6 - x_4y_0 - x_3y_2)^2 +$$
$$+ (x_\infty y_6 + x_6y_\infty + x_0y_2 + x_1y_5 + x_3y_4 - x_2y_0 - x_5y_1 - x_4y_3)^2.$$

Теорема Гурвица утверждает, что тождество вида

$$(x_1^2 + \ldots + x_N^2)(y_1^2 + \ldots + y_N^2) = z_1^2 + \ldots + z_N^2,$$

в котором z_k — билинейные функции от x_i и y_j, может существовать только при $N = 1, 2, 4$ или 8 (и в этих случаях оно «изотопно» одному из выписанных).

§ 6.11. Высшие тождества с квадратами: теория Пфистера

В свете всего сказанного большой неожиданностью оказалось следующее утверждение, доказанное А. Пфистером [34] в 1967 году.

Теорема 3. *Над любым полем и для любого n произведение двух сумм 2^n квадратов является суммой 2^n квадратов.*

Пфистер вывел эту теорему из того факта, что как только N является степенью двойки, существует тождество с N квадратами

$$(x_1^2 + \ldots + x_N^2)(y_1^2 + \ldots + y_N^2) = z_1^2 + \ldots + z_N^2,$$

в котором z_k являются рациональными функциями от x_i и y_j (и если характеристика отлична от 2, то такое тождество существует, только если N является степенью двойки). На самом деле z_k всегда можно выбрать линейными по x_i (или по y_j).

Кажется, не общеизвестно, что такие тождества можно получить с помощью различных модификаций диксоновского удвоения[1]. Например, можно получить тождество с 16 квадратами (для упорядоченных пар октав $a+ib$ и $c+id$) из «определения»

$$(a+ib)(c+id)=ab\cdot b^{-1}c-d\bar{b}+i(cb-\bar{a}d)=$$
$$=X+iY,$$

где при $b=0$ выражение $ab\cdot b^{-1}c$ следует понимать как ac.

В самом деле, норма правой части равна

$$[X]+[Y]=[ab\cdot b^{-1}c]+[d\bar{b}]+[cb]+[\bar{a}d]-2[ab\cdot b^{-1}c,d\bar{b}]+2[cb,\bar{a}d],$$

что совпадает с

$$[a][c]+[d][b]+[c][b]+[a][d]=([a]+[b])([c]+[d]),$$

поскольку слагаемые со скалярными произведениями сокращаются:

$$[ab\cdot b^{-1}c,d\bar{b}]=[(ab\cdot b^{-1}c)b,d]=[a\cdot cb,d]=[cb,\bar{a}d].$$

В среднем равенстве мы воспользовались правилом Муфанг (глава 7):

$$(xy)z=xz^{-1}\cdot zyz.$$

В формуле

$$(a+ib)(c+id)=(ac-d\bar{b})+i(cb+\bar{a}d),$$

с помощью которой получаются тождества с 16 квадратами, можно аналогичным образом заменять не только ac, но и $\bar{d}b$, cb, $\bar{a}d$. В приложении 1 к этой главе приводятся некоторые способы таких замен, которые можно итерировать бесконечно и получать тождества с 2^n квадратами для всех n. Одна из этих замен равносильна формуле, приведенной Уорреном Смитом:

$$(a+bi)(c+di)=(ac-\overline{\bar{b}d})+(b\bar{c}+\overline{b(\bar{a}\cdot\overline{\bar{b}^{-1}d})})i.$$

Пфистер пошел и дальше, создав целую теорию сумм квадратов и других мультипликативных квадратичных форм. Мы ограничимся одним простым результатом.

Теорема 4. *Если в поле $\mathbb{F}$ элемент -1 может быть представлен в виде суммы N квадратов, то наименьшее значение N, при котором такое представление возможно, является степенью двойки.*

[1]Пфистер первоначально получал свои тождества по-другому.

(Пфистер называет это наименьшее значение «уровнем» (Stufe) поля $\mathbb{F}$.)

В самом деле, предположим, что -1 является суммой 2^n+k квадратов, где $0<k<2^n$:

$$-1=x_1^2+\ldots+x_{2^n}^2+y_1^2+\ldots+y_k^2;$$

предположим также, что -1 не является суммой меньшего количества квадратов (так что $-1=x_1^2+\ldots+x_{2^n}^2\neq 0$). Запишем это равенство в виде

$$-(x_1^2+\ldots+x_{2^n}^2)=y_1^2+\ldots+y_k^2+1^2=y_1^2+\ldots+y_{2^n}^2$$

(мы положили $y_{k+1}=1$, остальные «новые» игреки равны нулю). Умножая это равенство на $s=x_1^2+\ldots+x_{2^n}^2$, получаем равенство вида

$$-s^2=(x_1^2+\ldots+x_{2^n}^2)(y_1^2+\ldots+y_{2^n}^2)=z_1^2+\ldots+z_{2^n}^2$$

(мы воспользовались тождеством с 2^n квадратами); отсюда следует, что

$$-1=(z_1/s)^2+\ldots+(z_{2^n}/s)^2,$$

и получаем противоречие.[1]

Приложение 1
О диксоновском удвоении

Диксоновское правило удвоения встречается в литературе в двух видах:

$$(a+ib)(c+id)=(ac-d\bar{b})+i(cb+\bar{a}d)$$

и

$$(a+bi)(c+di)=(ac-\bar{d}b)+(da+b\bar{c})i;$$

мы будем называть их левосторонней и правосторонней версиями. Чтобы запомнить эти формулы, можно заметить, что в левосторонней версии буквы идут в порядке $(a\ c\ b)$ и $(\bar{a}\ d\ \bar{b})$, начиная с самой левой буквы a, а в правосторонней версии — в порядке $(d\ a\ c)$ и $(\bar{d}\ b\ \bar{c})$, начиная с самой правой буквы d.

[1] В действительности дело обстоит чуть менее тривиально. Рациональные функции в тождестве для сумм 2^n квадратов имеют знаменатели, которые могут обратиться в нуль при подстановке фиксированных элементов $x_1, \ldots, y_{2^n}$ основного поля. Формальное обоснование требует, в каком-то смысле, построения для каждой точки (x, y) варианта этого тождества, для которого правая часть определена в (x, y). Оказывается, это возможно; подробности см. в монографии Пфистера и Альбрехта (Pfister, Albrecht. Quadratic forms with applications to algebraic geometry and topology. London Mathematical Society Lecture Note Series, 217. Cambridge University Press, Cambridge, 1995). — *Прим. ред.*

Формулы, задающие расширение октав до 16-мерных систем «седенионов», получаются из этих формул с помощью «вытягивания» одной из букв из действительной или мнимой части. Так, в левосторонней версии мы можем заменить $(ac-d\bar{b})$ на любое из следующих выражений:

$$a(c-a^{-1}d\cdot\bar{b}),\ (a-d\cdot\bar{b}c^{-1})c,\ d(d^{-1}a\cdot c-\bar{b}),\ (a\cdot c\bar{b}^{-1}-d)\bar{b}^{-1}$$

или заменить $(cb+\bar{a}d)$ на любое из следующих выражений:

$$c(b+c^{-1}\bar{a}\cdot d),\ (c+\bar{a}\cdot db^{-1})b,\ \bar{a}(\bar{a}^{-1}c\cdot b+d),\ (c\cdot bd^{-1}+\bar{a})d.$$

Эти законы умножения можно сгруппировать в четыре «сопряженные» пары, каждая из которых состоит из леволинейного умножения $\{x\}y$ и праволинейного умножения $x\{y\}$, связанных соотношением

$$\overline{x\{y\}}=\{\bar{y}\}\bar{x}.$$

Тут подразумевается, что формула задает функцию, линейную относительно всех переменных в скобках. Чтобы получить «произвольнионы» (т. е. 2^n-ионы для произвольного n), достаточно взять подходящие переменные в фигурные скобки, например, так:

$$(a+ib)\{c+id\}=a(\{c\}-a^{-1}\{d\}\cdot\bar{b})+(\{c\}b+\bar{a}\{d\})i.$$

Четыре пары умножений изотопны. Например, i, умноженное на произведение x и y, есть другое произведение ix и y.

Мы благодарны Уоррену Смиту (Warren Smith), подробно исследовавшему такие законы умножения.

Приложение 2
Что сохраняет кватернионную подалгебру?

Автоморфизмы (или «симметрии»), сохраняющие кватернионную подалгебру H, хорошо описываются на языке главы 4. Как обычно, будем считать, что i — фиксированный единичный вектор, ортогональный к H, и будем записывать произвольную октаву в виде $x+iy$, где $x, y\in H$ — как при диксоновском удвоении. Тогда имеет место следующее утверждение.

Теорема 5. *Автоморфизмы октав, переводящие H в себя, образуют группу, изоморфную SO_4. Общий автоморфизм*[1] $[u,v]=[-u,-v]$ *параметризуется двумя единичными элементами $u, v\in H$; он действует по правилу* $x+iy\to\bar{u}xu+i\cdot\bar{u}yv$.

[1]Мы возвращаемся к обозначениям, в которых $[u,v]$ — общий элемент SO_4.

Доказательство. Любой автоморфизм алгебры H очевидным образом продолжается на ее диксоновское удвоение. Поскольку всякий такой автоморфизм есть лежащее в SO_3 отображение $x \to \bar{u}xu$, он индуцирует автоморфизм

$$[u,u]: x+iy \to \bar{u}xu + i\cdot\bar{u}yu.$$

По модулю таких автоморфизмов достаточно рассмотреть такие, что оставляют на месте каждый элемент из H. Если такой автоморфизм переводит i в I, то $x+iy$ он переводит в $x+Iy$. Но тогда можно записать равенство $I=iv$ для некоторого единичного элемента $v\in H$; после этого ясно, что отображение

$$[1,v]: x+iy \to x+i\cdot yv$$

обладает нужным свойством, поскольку $i\cdot yv = iv\cdot y$ ввиду (D3).

Найденные нами автоморфизмы вида $[u,u]$ и $[1,v]$ порождают все симметрии вида $[u,v]$ (так как $[u,v]=[u,u][1,\bar{u}v]$). □

Симметрии вида $[u,1]$, $[1,v]$ и $[u,u]$ обладают очень разными свойствами. Наиболее важны *квазисопряжения* $Q_u=[u,1]$. Важность этих отображений прояснится, если сменить обозначения: если положить $X=x$, $Y=iy$, то

$$[u,1]: X+Y \to \bar{u}Xu + uY$$

(поскольку $uY = u\cdot iy = i\cdot\bar{u}y$ ввиду (D3)), что показывает, что $[u,1]$ не зависит от выбора i. Этот автоморфизм зависит, однако, от выбора подалгебры H, содержащей u. Полное название для этого автоморфизма — *квазисопряжение с помощью u относительно подалгебры H*. Квазисопряжения относительно данной H образуют нормальную подгруппу в группе автоморфизмов, сохраняющую H.

Следующие по важности симметрии — *H-стабилизаторы* $S_v=[1,v]$. Как и следует из их названия, они сохраняют каждый элемент в H и образуют нормальную подгруппу. К сожалению, параметр v, задающий данный H-стабилизатор, зависит не только от H, но и от i.

Диагональные симметрии $D_u=[u,u]$ являются наименее важными, поскольку диагональность симметрии может не сохраниться после применения другой симметрии: сопряженный к $[u,u]$ с помощью $[a,b]$ есть $[u^a,u^b]$, и этот автоморфизм может уже не быть диагональным. С алгебраической точки зрения это означает, что диагональные симметрии образуют подгруппу, не являющуюся нормальной.

Мы будем пользоваться этими идеями в главе 10.

Лупы Муфанг

§ 7.1. Лупы с обращением

Лупой с обращением называется множество с отмеченным элементом 1, бинарной операцией xy и унарной операцией («обращением») $^{-1}$, удовлетворяющими тождествам

$$x1 = x = 1x,$$
$$x^{-1}(xy) = y = (yx)x^{-1},$$
$$(x^{-1})^{-1} = x$$

для всех x и y. (Скоро станет понятно, почему мы записываем обратный элемент как x^{-1}, а не x^{-1}).

Основная тема этой главы — то обстоятельство, что основное соотношение $xy = z$ можно записать шестью способами (рис. 7.1). Мы будем говорить, что эти соотношения образуют *шестерку*.

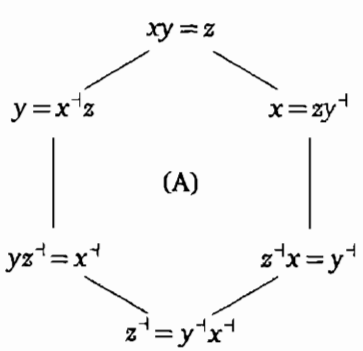


Рис. 7.1. Дуплексная форма основной шестерки

Поскольку эквивалентность

$$yz^{\dashv} = x^{\dashv} \iff z^{\dashv}x = y^{\dashv}$$

можно записать в виде

$$(yz^{\dashv})x = 1 \iff y(z^{\dashv}x) = 1,$$

мы видим, что соотношения $(XY)Z = 1$ и $X(YZ) = 1$ равносильны и могут тем самым записываться без скобок, как $XYZ = 1$.

Будем называть $xy = z$ и $xyz^{\dashv} = 1$ *дуплексной* и *триплексной* формами основного соотношения. Если перевести шесть соотношений на рис. 7.1 в триплексную форму и заменить z на $z^{\dashv}$, то их симметрия станет более понятной (рис. 7.2).

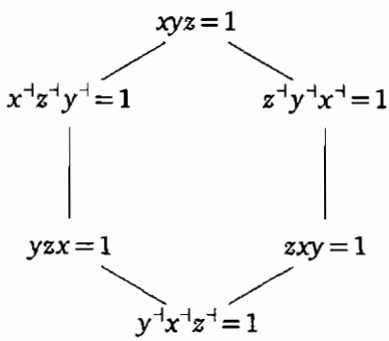


Рис. 7.2. Триплексная форма основной шестерки

§ 7.2. Изотопии

Изотопией лупы с обращением называется тройка обратимых отображений, сохраняющих основное соотношение. Для изотопии удобно использовать два типа обозначений в зависимости от того, в дуплексной или триплексной форме записано соотношение. Мы будем писать $(\alpha, \beta \mid \gamma)$ в значении $x^{\alpha}y^{\beta} = (xy)^{\gamma}$; мы будем писать (α, β, γ) в значении $xyz = 1 \Rightarrow x^{\alpha}y^{\beta}z^{\gamma} = 1$.

Если $(\alpha, \beta \mid \gamma)$ — изотопия, записанная в дуплексной форме, то

$$xyz = 1 \Rightarrow xy = z^{\dashv} \Rightarrow x^{\alpha}y^{\beta} = z^{\dashv\gamma} \Rightarrow x^{\alpha}y^{\beta}z^{\dashv\gamma\dashv} = 1,$$

так что $(\alpha, \beta, \dashv\gamma\dashv)$ — запись той же изотопии в триплексной форме.

Применяя $(\alpha, \beta \mid \gamma)$ к шестерке (A), получаем шестерку (B), которая упрощается до (C) (рис. 7.3).

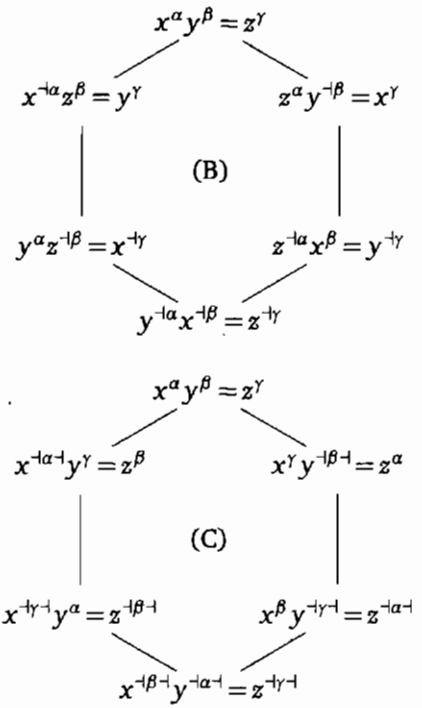


Рис. 7.3. Упрощение шестерки изотопий: (B) упрощается до (C)

Стало быть, если $(\alpha, \beta \mid \gamma)$ является изотопией, то таковы же и все члены шестерки (D) (рис. 7.4). Опять-таки симметрия становится более заметной, если перевести (D) в триплексную форму (E) (заменяя γ на $\dashv\gamma\dashv$).

§ 7.3. Монотопии и их сателлиты

Будем называть *монотопией* любое из трех отображений, составляющих изотопию. Из шестерок (D) и (E) видно, что определение не зависит от того, какое из трех отображений выбрать.

Итак, если γ — монотопия, то существуют отображения α и β, для которых

$$xy = z \;\Rightarrow\; x^\alpha y^\beta = z^\gamma.$$

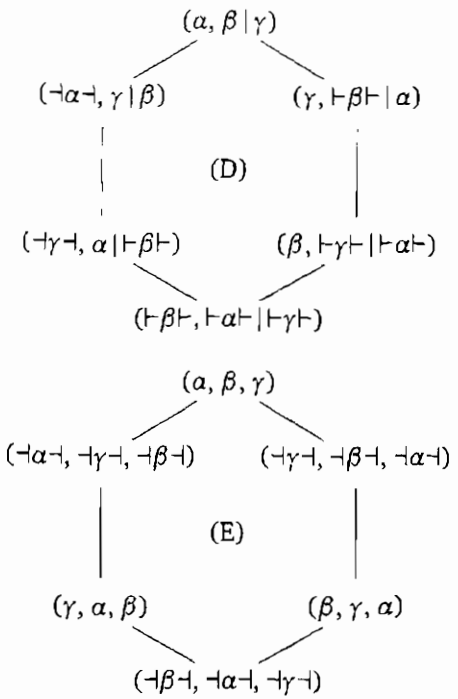


Рис. 7.4. Изотопии в дуплексной и триплексной формах: (D) переходит в (E)

В частности,

$$z^{\alpha}1^{\beta}=z^{\gamma}, \quad \text{так что} \quad z^{\alpha}=z^{\gamma}1^{\beta\dashv}=z^{\gamma}b,$$
$$1^{\alpha}z^{\beta}=z^{\gamma}, \quad \text{так что} \quad z^{\beta}=1^{\alpha\dashv}z^{\gamma}=az^{\gamma}.$$

Стало быть, γ является монотопией тогда и только тогда, когда в лупе имеются элементы b и a, для которых $(xy)^{\gamma}=x^{\gamma}b\cdot ay^{\gamma}$. Мы будем называть a и b парой *сателлитов* (companions) изотопии γ. Наши формулы показывают, что монотопии очень близки к изоморфизмам (автоморфизм — это просто монотопия, у которой 1, 1 является парой сателлитов).

В общем случае определение элементов a и b показывает, что три отображения, составляющие изотопию, очень тесно связаны. На языке операторов левого и правого умножения

$$L_a: x\to ax, \quad R_b: x\to xb$$

эта связь выражается формулами $\alpha=\gamma R_b$, $\beta=\gamma L_a$.

На самом деле, однако, можно сказать и больше! Рассмотрим отношение двух соседних изотопий из (D):

$$(\alpha, \beta \mid \gamma)^{-1} \cdot (\dashv\alpha\dashv, \gamma \mid \beta) = (\alpha^{-1}\dashv\alpha\dashv, \beta^{-1}\gamma \mid \gamma^{-1}\beta).$$

Тогда, поскольку $\gamma^{-1}\beta = \mathsf{L}_a$, так что $\beta^{-1}\gamma = (\mathsf{L}_a)^{-1} = \mathsf{L}_{a^\dashv}$, эта изотопия имеет следующий специальный вид:

$$(\alpha^{-1}\dashv\alpha\dashv, \mathsf{L}_{a^\dashv} \mid \mathsf{L}_a).$$

Применяя эту изотопию к xa, получаем:

$$a(xa) = x^{\alpha^{-1}\dashv\alpha\dashv} \cdot a^\dashv a = x^{\alpha^{-1}\dashv\alpha\dashv}.$$

Отсюда вытекает, что отображение $\alpha^{-1}\dashv\alpha\dashv$ переводит x в $a(xa)$ и что

$$a(xa) \cdot a^\dashv y = a(xy),$$

а в частности и что

$$a(xa) \cdot a^\dashv = ax,$$

так что

$$a(xa) = (ax)a.$$

Это позволяет нам пользоваться стандартным обозначением B_a для отображения, переводящего x в $a(xa) = (ax)a$, так что наша изотопия есть $(\mathsf{B}_a, \mathsf{L}_{a^\dashv} \mid \mathsf{L}_a)$. Как и всякая изотопия, она включается в шестерку;

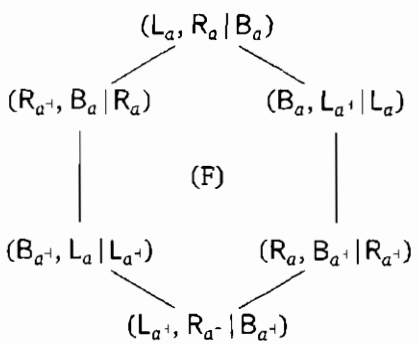


Рис. 7.5. Шестерка изотопий, включающая L_a, R_a, B_a

ее полная шестерка (F) представлена на рис. 7.5; при ее построении мы пользуемся равенствами

$$\dashv\mathsf{L}_a\dashv = \mathsf{R}_{a^\dashv}, \quad \dashv\mathsf{R}_a\dashv = \mathsf{L}_{a^\dashv} \quad \text{и} \quad \dashv\mathsf{B}_a\dashv = \mathsf{B}_{a^\dashv}.$$

Поскольку эта шестерка симметрична относительно замены a на $a^\dashv$, мы доказали следующий факт.

Теорема 1. *Если a — образ 1 при некоторой монотопии, то имеют место все изотопии из шестерки* (F), *так что L_a, $L_{a^{-1}}$, R_a, $R_{a^{-1}}$, B_a и $B_{a^{-1}}$ являются монотопиями. В частности, если существует какая-нибудь монотопия, переводящая 1 в a, то L_a и R_a также являются такими монотопиями.*

Отсюда, в свою очередь, вытекает теорема, объясняющая смысл правил Муфанг.

Теорема 2. *Монотопии транзитивны тогда и только тогда, когда выполнено правило Муфанг*

$$zx \cdot yz = z(xy)z.$$

Доказательство. В этом случае $(L_z, R_z \mid B_z)$ должно быть изотопией для всякого z. □

Лупа, удовлетворяющая этому условию, называется *лупой Муфанг* (неформально — «мупой»).

Мартин Либек [31] показал, что всякая конечная простая лупа Муфанг, не являющаяся группой, состоит из элементов с нормой 1 в алгебре октав по модулю p, рассматриваемых по модулю скаляров.

§ 7.4. Различные формы правил Муфанг

Будучи примененными к xy, шесть изотопий из (F) становятся эквивалентными трем правилам:

$$z(xy)z = zx \cdot yz \quad \text{— правило Муфанг (двустороннее);}$$
$$z(xy) = zxz \cdot z^{-1}y \quad \text{— левое правило Муфанг;}$$
$$(xy)z = xz^{-1} \cdot zyz \quad \text{— правое правило Муфанг}$$

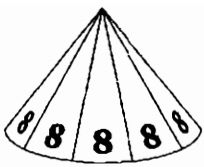
(здесь z — это a или a^{-1}). Второе и третье правила в традиционной записи выглядят немного иначе:

$$z(x(zt)) = zxz \cdot t,$$
$$((tz)y)z = t \cdot zyz.$$

Эти формулы получатся, если подставить $y = zt$ и $x = tz$ в левое и правое правило Муфанг соответственно.

Лупы Муфанг называются так в честь Рут Муфанг, открывшей их в связи с введением координат на некоторых проективных плоскостях (см. [33]). В некотором смысле, однако, это не было их первым появлением в математике, поскольку ненулевые вещественные октавы образуют архетипическую лупу Муфанг. Более того, мы выдвигаем гипотезу, что лупа, порожденная n общими вещественными октавами, является свободной лупой Муфанг с n образующими.

Разумеется, правила Муфанг можно рассматривать как ослабленные формы ассоциативности. И в самом деле, одна из самых знаменитых теорем о таких лупах — это теорема Артина о диассоциативности, утверждающая, что всякая лупа Муфанг с двумя образующими является ассоциативной. Мы, однако, убедились, что есть и более важная причина изучать абстрактные лупы Муфанг — это то, что монотопии на них транзитивны. Мы будем использовать некоторые части этой теории (в частности, свойства сателлитов) в следующей главе.



Октавы и восьмимерная геометрия

Мы знаем, что умножениями на единичные комплексные числа или кватернионы порождаются ортогональные группы SO_2 и SO_4 соответственно, а в этой главе мы докажем, что умножения на единичные октавы порождают группу SO_8.

Тем не менее, между этими тремя случаями имеются различия, связанные с тем, имеет ли место коммутативность или ассоциативность. Закон ассоциативности, записанный в виде

$$L_{xy} = L_y L_x, \quad R_{xy} = R_x R_y$$

(где x и y — единицы), говорит нам, что произведение двух левых (или двух правых) умножений — также умножение, так что в тех случаях, когда ассоциативность есть, левые или правые умножения образуют подгруппы в специальных ортогональных группах.

В комплексном случае коммутативность (т. е. $L_x = R_x$) говорит нам, что эти группы совпадают (и являются полной группой SO_2). В кватернионном случае как левая, так и правая группа являются собственными подгруппами, и мы видели в главе 4, что всякий элемент из SO_4 является произведением левого и правого умножений. Поскольку для октав ассоциативность нарушается, мы больше не можем сказать, что произведение двух умножений одного вида также является умножением. Мы увидим в этой главе, что октавные умножения каждого из видов порождают всю группу SO_8.

§ 8.1. Изотопии и SO_8

Начнем с того, что докажем, что октавы строго неассоциативны в следующем смысле.

Теорема 1. *Если $x(ry) = (xr)y$ для всех октав x и y, то октава r вещественна.*

В самом деле, $(i_1 i_0)i_2 = -i_1(i_0 i_2)$, так что если $(i_1 r)i_2 = i_1(r i_2)$, то коэффициент при i_0 у r должен равняться нулю, и то же верно применительно к коэффициентам при i_n, где $1 \leqslant n \leqslant 6$, поскольку $(i_{n+1} i_n)i_{n+2} = -i_{n+1}(i_n i_{n+2})$.

Из этой теоремы следует, что определенные в главе 7 сателлиты по существу единственны.

Теорема 2. *Если a, b — пара сателлитов монотопии γ, то любая другая пара сателлитов этой монотопии имеет вид $ar, r^{-1}b$, где r вещественно.*

Доказательство. Если A, B — другая пара сателлитов, то для всех x и y выполнено тождество

$$x^\gamma a \cdot b y^\gamma = x^\gamma A \cdot B y^\gamma.$$

Положив $x^\gamma = X$, $y^\gamma = Y$, это тождество можно переписать в виде

$$Xa \cdot bY = XA \cdot BY$$

(для произвольных X и Y). Пусть $A = ar$; полагая в этом тождестве $X = a^{-1}$, $Y = 1$, получаем, что $b = rB$, так что $b = r^{-1}B$, и тождество принимает вид

$$Xa \cdot bY = X(ar) \cdot (r^{-1}b)Y \quad \text{для всех } X \text{ и } Y.$$

Полагая в этом тождестве $Y = (r^{-1}b)^{-1} = b^{-1}r$, получаем, что $(Xa)r = X(ar)$; полагая $X = (ar)^{-1} = r^{-1}a^{-1}$, получаем, что $r^{-1}(bY) = (r^{-1}b)Y$, так что тождество превращается в такое:

$$Xa \cdot bY = (Xa)r \cdot r^{-1}(bY).$$

Полагая, наконец, $Xa = x$, $bY = ry$, получаем, что

$$x(ry) = (xr)y$$

для всех x и y; значит, r вещественно, чем доказательство и завершается. □

Теперь мы можем применить эти результаты к SO_8.

Теорема 3. *Пусть $\gamma \in \mathrm{SO}_8$. Тогда существуют такие $\alpha, \beta \in \mathrm{SO}_8$, что $(\alpha, \beta \mid \gamma)$ является изотопией (и тем самым γ является монотопией). Более того, α и β определены однозначно с точностью до знака: единственная возможная другая пара есть $-\alpha, -\beta$.*

Мы докажем эту теорему с помощью следующей леммы.

Лемма 1. *Операции* $\mathrm{ref}(1)\,\mathrm{ref}(a)$ *и* $\mathrm{ref}(a)\,\mathrm{ref}(1)$ *являются двусторонними умножениями на единичные октавы.*

Доказательство. Отображения не изменятся, если мы умножим a на подходящий скаляр, чтобы норма стала равна единице. А в этом случае первое из этих отображений есть B_a (как мы выяснили в главе 6), а второе — обратное к нему отображение $\mathsf{B}_{a^{-1}} = \mathsf{B}_{\bar{a}}$. □

Доказательство теоремы. Можно представить γ в виде произведения четного числа отражений:

$$\gamma = \mathrm{ref}(a_1)\,\mathrm{ref}(b_1)\,\mathrm{ref}(a_2)\,\mathrm{ref}(b_2)\ldots\mathrm{ref}(a_{2n})\,\mathrm{ref}(b_{2n}).$$

Однако же

$$\mathrm{ref}(a_i)\,\mathrm{ref}(b_i) = \mathrm{ref}(a_i)\,\mathrm{ref}(1)\,\mathrm{ref}(1)\,\mathrm{ref}(b_i)$$

есть произведение двух двусторонних умножений на единичную октаву. Следовательно, γ есть произведение $2n$ таких двусторонних умножений (обозначим их $\mathsf{B}_{c_1}\mathsf{B}_{c_2}\ldots\mathsf{B}_{c_{2n}}$). Тогда

$$(\alpha, \beta \,|\, \gamma) = (\mathsf{L}_{c_1}\ldots\mathsf{L}_{c_{2n}}, \mathsf{R}_{c_1}\ldots\mathsf{R}_{c_{2n}} \,|\, \mathsf{B}_{c_1}\ldots\mathsf{B}_{c_{2n}})$$

является искомой изотопией (поскольку $c_1, \ldots, c_{2n}$ — единичные октавы, α и β действительно лежат в SO_8). Наконец, мы знаем, что α и β единственны с точностью до умножения на скаляры, и единственный нетривиальный скаляр, умножение на который не выводит за пределы SO_8, есть -1, так что единственная другая изотопия есть

$$(-\alpha, -\beta \,|\, \gamma) = (\alpha, \beta \,|\, \gamma).$$ □

§ 8.2. Ортогональные изотопии и группа Spin

В предыдущих рассуждениях было удобно пользоваться изотопиями в дуплексной форме $(\alpha, \beta \,|\, \gamma)$; поскольку теперь мы подходим к тройственности, нам будет удобнее перейти к триплексной форме (α, β, γ), в которой найденные нами изотопии принимают вид

$$(\mathsf{L}_a\mathsf{L}_b\ldots, \mathsf{R}_a\mathsf{R}_b\ldots, \mathsf{B}_{\bar{a}}\mathsf{B}_{\bar{b}}\ldots).$$

Мы будем говорить, что (α, β, γ) — *ортогональная изотопия*, если три входящие в нее монотопии α, β и γ лежат в SO_8. Мы показали, что группа ортогональных изотопий является двулистным накрытием группы SO_8; мы будем называть это накрытие *спинорной группой* Spin_8. Читатель, знакомый с обычным определением спинорных групп, узнает ее сразу. Как мы отмечали в главе 3, в этой книге мы предпочитаем не давать общего определения спинорных групп.

§ 8.3. Тройственность

Из нашего определения спинорной группы легко вытекает следующее утверждение.

Теорема 4. *Спинорная группа обладает внешним автоморфизмом порядка 3; именно, это автоморфизм, действующий по правилу* $(\alpha, \beta, \gamma) \to (\beta, \gamma, \alpha)$.

Доказательство. Ясно, что это автоморфизм. Автоморфизм является внешним (т. е. не является сопряжением вида $g \to h^{-1}gh$), поскольку образы в SO_8 у связанных тройственностью элементов

$$(L_{i_0}, R_{i_0}, B_{i_0} \simeq B_{\tilde{i}_0}) \quad \text{и} \quad (R_{i_0}, B_{i_0}, L_{i_0})$$

не являются сопряженными (B_{i_0} оставляет неподвижными точки 6-мерного пространства, тогда как L_{i_0} неподвижных точек не имеет). □

Специальная ортогональная группа SO_8 тройственностью не обладает, поскольку α и β определяются по γ только с точностью до знака. Тем не менее, верно следующее.

Теорема 5. *Проективная специальная ортогональная группа* PSO_8 *обладает автоморфизмом тройственности.*

В самом деле, если $\varphi \in SO_8$, то положим $[\varphi] = \{+\varphi, -\varphi\}$, так что $[\varphi] \in PSO_8$. Ясно, что множество троек $([\alpha], [\beta], [\gamma])$, происходящих из ортогональных изотопий (α, β, γ), изоморфно PSO_8 (поскольку на сей раз $[\alpha]$ и $[\beta]$ однозначно определяются по $[\gamma]$) и тем самым обладает автоморфизмом тройственности

$$([\alpha], [\beta], [\gamma]) \to ([\beta], [\gamma], [\alpha]).$$

Тройственность на PSO_8 для всякой единичной октавы u действует по формуле

$$[L_u] \to [R_u] \to [B_{\bar{u}}] \to [L_u].$$

§ 8.4. Семь правых как одно левое

Вот немедленное следствие тройственности.

Теорема 6. *Группа* SO_8 *порождена левыми умножениями на октавные единицы (а также правыми умножениями на октавные единицы).*

Доказательство. SO_8 порождена двусторонними умножениями; применяя тройственность, получаем, что она также порождена левыми (а кроме того, и правыми) умножениями. □

В частности, всякое левое умножение можно представить в виде произведения правых, и обратно. Сколько правых умножений нужно,

чтобы получить левое умножение L_x? Ответ дается следующей теоремой.

Теорема 7 (о семи сомножителях). *Всякий элемент группы SO_8 является произведением не более чем семи левых (или не более чем семи правых) умножений.*

Эта оценка неулучшаема.

Теорема 8. *Общее левое умножение является произведением семи, но не меньшего количества, правых умножений.*

Доказательство. Если $\alpha \in SO_8$, то $\mathrm{ref}(1)\cdot\alpha$ лежит в $GO_8 \setminus SO_8$ и тем самым является произведением не более чем семи отражений. Стало быть,

$$\alpha = \mathrm{ref}(1)\,\mathrm{ref}(u_1)\,\mathrm{ref}(u_2)\ldots\mathrm{ref}(u_7),$$

что можно записать в виде произведения семи двусторонних умножений

$$\alpha = B_{u_1}B_{\bar{u}_2}B_{u_3}B_{\bar{u}_4}B_{u_5}B_{\bar{u}_6}B_{u_7},$$

поскольку

$$\mathrm{ref}(u)\,\mathrm{ref}(v) = \mathrm{ref}(u)\,\mathrm{ref}(1)\,\mathrm{ref}(1)\,\mathrm{ref}(v) = B_{\bar{u}}B_v.$$

Ввиду тройственности α тогда является и произведением семи левых умножений или семи правых умножений. В частности, всякое левое умножение есть произведение семи правых умножений; например, имеем

$$L_{i_0} = R_{i_{\bar{2}\bar{6}\bar{4}\bar{5}}}R_{i_{\bar{2}\bar{6}\bar{4}\bar{5}}}R_{i_6}R_{i_5}R_{i_{\infty\bar{0}\bar{1}\bar{3}}}R_{i_{\infty\bar{0}\bar{1}\bar{3}}}R_{i_3}$$

и

$$L_{i_{\infty 365}} = R_{i_0}R_{i_{\bar{0}\bar{1}\bar{2}\bar{4}}}R_{i_{0\bar{1}\bar{2}\bar{4}}}R_{i_{\bar{0}\bar{1}\bar{2}\bar{4}}}R_{i_{\infty\bar{6}\bar{4}\bar{1}}}R_{i_{\infty\bar{5}\bar{1}\bar{2}}}R_{i_{\infty\bar{3}\bar{2}\bar{4}}};$$

мы будем пользоваться этими равенствами в главе 9.

С другой стороны, если u — единичный элемент, отличный от ± 1, то L_u нельзя представить в виде произведения шести правых умножений на единичные элементы, так как в таком случае R_u было бы произведением соответствующих шести двусторонних умножений на единицы, а тем самым и шести отражений, и, стало быть, имело бы неподвижный вектор, что не так.

Поскольку положительные скалярные множители можно включить в сомножители при умножении любого из трех типов, нам нет нужды ограничиваться единичными элементами: L_x может быть произведением шести правых умножений, только если x вещественно. □

§ 8.5. Другие теоремы об умножении

Что происходит с произведениями умножений разных типов? Если каждая из букв X, Y и Z обозначает одну из букв L, R и B, то, например, через XYZX мы обозначим множество элементов из SO_8, представимых в виде $X_aY_bZ_cX_d$, где a, b, c и d — произвольные единичные октавы.

Теорема 9. *Размерности указанных ниже множеств таковы, как в следующей таблице:*

X	XX	XXX	XXXX	XXXXX	XXXXXX	XXXXXXX
7	13	18	22	25	27	28

XY	XXY	XXXY	XXXXY
14	20	25	28

Доказательство. Поскольку октавное сопряжение переставляет L и R, оставляя на месте B, в то время как тройственность переставляет по кругу L, R и B, можно считать, что $X=B$ и $Y=R$. Теперь числа в верхней строке получаются с помощью того соображения, что множество произведений n преобразований типа B есть множество произведений n отражений, если n четно, или то же множество, помноженное на ref(1), если n нечетно.

Покажем теперь, что размерности множеств XY, XXY и XXXY на 7 больше, чем множеств X, XX и XXX соответственно. Это немедленно следует из того факта, что равенство

$$B_aB_bB_cR_d = B_{a'}B_{b'}B_{c'}R_{d'}$$

влечет равенство $d=d'$ (и тем самым $B_aB_bB_c = B_{a'}B_{b'}B_{c'}$). Это же, в свою очередь, верно потому, что из выписанного равенства вытекает, что $R_{d'}R_{\bar{d}}$ лежит в BBBBBB и тем самым имеет двумерное неподвижное пространство; если $e\neq 0$ лежит в этом пространстве, то $(ed')\bar{d}=e$, так что $ed'=ed$, откуда $d'=d$.

Из аналогичного равенства

$$B_aB_bB_cB_dR_e = B_{a'}B_{b'}B_{c'}B_{d'}R_{e'}$$

вытекает только тривиальное

$$R_{e'}R_{\bar{e}}\in \mathrm{BBBBBBBB},$$

из которого $e'=e$ не следует. Тем не менее, можно все-таки подсчитать размерность пространства BBBBR (которая равна не 29, а 28), подсчитав размерность множества таких равенств. Подробности мы опустим. □

Много других смешанных произведений сводятся к описанным в теореме 9 благодаря следующему факту.

Лемма 2. *Имеют место равенства*

$$\mathsf{LR}=\mathsf{RB}=\mathsf{BL},$$
$$\mathsf{RL}=\mathsf{LB}=\mathsf{BR}.$$

Например, из этих равенств вытекает, что $\mathsf{BLL}=\mathsf{LRL}=\mathsf{LLB}$, что показывает (двумя способами), что размерность множества LRL равна 20.

Доказательство. Тождества

$$\mathsf{L}_a\mathsf{R}_b=\mathsf{R}_{b\bar{a}}\mathsf{B}_a=\mathsf{B}_b\mathsf{L}_{a\bar{b}},$$
$$\mathsf{R}_a\mathsf{L}_b=\mathsf{B}_b\mathsf{R}_{\bar{b}a}=\mathsf{L}_{\bar{a}b}\mathsf{B}_a$$

вытекают из правил Муфанг. □

На самом деле единственное множество длины $\leqslant 4$, не покрываемое нашей теоремой, есть XXYY (LLRR, RRLL, RRBB, BBRR, BBLL и LLBB — одно и то же множество ввиду леммы 2); не покрываемые теоремой множества длины 5 и более, скорее всего, совпадают со всей группой. Именно, мы выдвигаем следующую гипотезу:

Гипотеза о пяти умножениях. *Пусть* V, W, X, Y, Z — *произвольные* 5 *букв из множества* {L, R, B}, *причем не все эти буквы одинаковы. Тогда множество* VWXYZ *содержит все элементы группы* SO_8.

Наша лемма показывает, что все случаи можно свести к случаю XXXXY, про который мы уже знаем, что он имеет нужную размерность 28, так что остается совсем немного.

§ 8.6. Три семимерные группы в одной восьмимерной

Лучший способ понять взаимосвязь Spin_8 и SO_8 — воспользоваться двулистным накрытием, сопоставляющим тройке ее последнюю компоненту:

$$\begin{array}{l}(\alpha,\beta,\gamma)\searrow\\ \qquad\qquad\gamma.\\ (-\alpha,-\beta,\gamma)\nearrow\end{array}$$

Технически говоря, речь идет о восьмимерном представлении Spin_8.

Семимерная спинорная группа Spin_7 есть прообраз SO_7 при этом отображении: тройки (α,β,γ), для которых γ оставляет 1 на месте, образуют группы Spin_7. Ясно, что если потребовать вместо этого, чтобы единицу сохраняла α или β, то мы получим в Spin_8 еще две подгруппы, изоморфные Spin_7.

Все эти три группы имеют восьмимерные представления, получаемые ограничением представления, указанного выше, и эти три пред-

ставления очень различны. Одно из них приводимо (поскольку 1 сохраняется) и не является точным (поскольку $(-1,-1,1)$ лежит в ядре). Два другие представления являются и неприводимыми, и точными. Дело в том, что, с одной стороны, $(-1,-1,1)$ — единственный нетривиальный элемент ядра — не лежит ни в одной из этих групп, а с другой стороны, эти группы транзитивны на единичном шаре. Чтобы в этом убедиться, достаточно рассмотреть изотопию

$$(\alpha,\beta,\gamma)=(R_{\bar{u}},B_u,L_{\bar{u}})(B_{\bar{u}},L_u,R_u),$$

в которой $\gamma: x\to\bar{u}xu$ сохраняет 1, в то время как α и β переводят 1 в $\bar{u}^3$ и u^3, и это может быть произвольная единичная октава.

Теорема 10. *Пересечение любых двух из этих трех* Spin_7*, вложенных в* Spin_8*, совпадает с пересечением всех трех. Это пересечение есть группа автоморфизмов октав.*

Доказательство. Применяя α, β и γ к равенству $1\cdot 1\cdot 1=1$, получаем, что $1^\alpha 1^\beta 1^\gamma=1$, так что если любые два из преобразований α, β и γ сохраняют 1, то таково же и третье. Если теперь a и b — сателлиты γ, так что $\alpha=\gamma R_a$, $\beta=\gamma L_b$, то отсюда следует, что $a=b=1$ и тем самым γ — изоморфизм. □

Построенная нами группа является группой Ли, обычно обозначаемой G_2. Это самая маленькая из пяти «исключительных» групп Ли.

На рис. 8.1 изображены взаимосвязи между группами, о которых шла речь. Чтобы спуститься на этом рисунке на один шаг, надо потребовать, чтобы одно из преобразований α, β или γ сохраняло 1; при этом размерность уменьшается на 7, поскольку преобразование могло перевести 1 в любую точку на семимерной сфере.

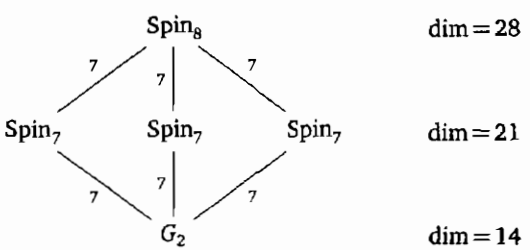


Рис. 8.1. Группа G_2 — группа автоморфизмов октав — является пересечением любых двух Spin_7, вложенных в Spin_8

Элементы группы Spin_8 группируются в четверки

$$(\alpha,\beta,\gamma),\quad(\alpha,-\beta,-\gamma),\quad(-\alpha,\beta,-\gamma),\quad(-\alpha,-\beta,\gamma),$$

являющиеся классами смежности по ее центру

$$(1,1,1),\quad (1,-1,-1),\quad (-1,1,-1),\quad (-1,-1,1).$$

Отображение $(\alpha,\beta,\gamma)\to\gamma$ из Spin_8 на SO_8 скрадывает эту симметрию, объединяя элементы этих четверок в две пары:

$$\begin{array}{ccc}(\alpha,\beta,\gamma)\searrow & & (\alpha,-\beta,-\gamma)\searrow\\ & \gamma; & \qquad -\gamma.\\ (-\alpha,-\beta,\gamma)\nearrow & & (-\alpha,\beta,-\gamma)\nearrow\end{array}$$

Можно восстановить симметрию, перейдя к PSO_8, в которой γ и $-\gamma$ отождествляются в $[\gamma]$:

$$\begin{array}{ccc}(\alpha,\beta,\gamma)\searrow & & \swarrow(\alpha,-\beta,-\gamma)\\ & [\gamma] & \\ (-\alpha,-\beta,\gamma)\nearrow & & \nwarrow(-\alpha,\beta,-\gamma).\end{array}$$

Стало быть, у групп Spin_8 и PSO_8 есть симметрия тройственности, отсутствующая у SO_8. Мы продолжим обсуждение этого в следующем параграфе.

§ 8.7. О сателлитах

Сопоставляя различные результаты из этой и предыдущей глав, получаем следующую теорему.

Теорема 11. *Для всякого элемента $\gamma\in\mathrm{SO}_8$ существуют две единичных октавы a и b, называемых его* сателлитами, *для которых*

$$(xy)^\gamma = x^\gamma a\cdot by^\gamma.$$

Сателлиты определены однозначно с точностью до изменения знака; единственная возможная вторая пара сателлитов есть $(-a,-b)$.

Нетрудно вывести «правило умножения» для сателлитов.

Теорема 12. *Если сателлиты элементов γ и δ суть (a,b) и (c,d) соответственно, то сателлиты для $\gamma\delta$ суть $(cd\cdot a^\delta c, db^\delta\cdot cd)$.*

Доказательство.

$$\begin{aligned}(xy)^{\gamma\delta} &= (x^\gamma a\cdot by^\gamma)^\delta =\\ &= (x^\gamma a)^\delta c\cdot d(by^\gamma)^\delta =\\ &= ((x^{\gamma\delta}c)(da^\delta))c\cdot d((b^\delta c)(dy^{\gamma\delta}) =\\ &= ((x^{\gamma\delta}c)(da^\delta)c)((d(b^\delta c)d)y^{\gamma\delta}) =\\ &= (x^{\gamma\delta}(cd\cdot a^\delta c))((db^\delta\cdot cd)y^{\gamma\delta}).\end{aligned}$$

Первые три равенства получаются из определения сателлитов, два последние — из правил Муфанг. □

С помощью этой теоремы мы можем найти сателлитов для любой комбинации левых, правых и двусторонних умножений, если начать со следующего факта.

ТЕОРЕМА 13. *Сателлиты преобразований* L_a, R_a *и* B_a *суть*

$$(a, a^{-2}), \quad (a^{-2}, a) \quad \text{и} \quad (a^{-1}, a^{-1})$$

соответственно.

ДОКАЗАТЕЛЬСТВО.

$$\begin{aligned} a(xy) &= axa \cdot a^{-1}y = (ax \cdot a)(a^{-2} \cdot ay), \\ (xy)a &= x^{-1}a \cdot aya = (xa \cdot a^{-2})(a \cdot ya), \\ a(xy)a &= ax \cdot ya = (axa \cdot a^{-1})(a^{-1} \cdot axa). \end{aligned}$$ □

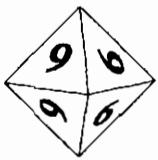
В теории групп отображение $T_a: x \to a^{-1}xa$, называемое *сопряжением* с помощью a, важно потому, что представляет собой автоморфизм. С октавами это верно не всегда, но мы знаем (см. Цорн [44]) все случаи, когда это так.

ТЕОРЕМА 14. *Сопряжение* T_a *является автоморфизмом тогда и только тогда, когда* a^3 *вещественно.*

ДОКАЗАТЕЛЬСТВО. Нижеследующее вычисление показывает, что сателлитами T_a являются a^{-3} и a^3 (в последнем равенстве дважды используется диассоциативность):

$$\begin{aligned} a^{-1}(xy)a &= (a^{-1}xa^{-1} \cdot ay)a = \\ &= (a^{-1}xa^{-1} \cdot a^{-1})(a(ay)a) = \\ &= (a^{-1}xa \cdot a^{-3})(a^3 \cdot a^{-1}ya). \end{aligned}$$ □

В частности, T_ω, где $\omega = -\frac{1}{2} + \frac{1}{2}i_1 + \frac{1}{2}i_2 + \frac{1}{2}i_4$, является автоморфизмом октав, и даже целых октав, которые мы определим в следующей главе.



Октавные целые O

В этой главе мы сначала находим правильный способ определить «целые октавы» и исследуем геометрию образуемой ими очень интересной решетки E_8. Мы доказываем, что кольцо «октавных целых» $O = O^8$ обладает евклидовым свойством — возможностью деления с остатком, при котором остаток будет меньше делителя. К сожалению, это не ведет к ожидаемой теории идеалов и однозначного разложения, поскольку, как мы покажем, идеалы в O довольно тривиальны. И наконец, мы излагаем новую теорию, впервые публикующуюся в этой книге, которая существенно проясняет как арифметику, так и геометрию делителей произвольной целой октавы. Эта теория была вдохновлена принадлежащим Рему (H. P. Rehm) открытием новой формы алгоритма Евклида.

Элементы кольца O назывались целыми числами Кэли со времен одноименной статьи Кокстера [11]. Позднее Кокстер отмечал следующее: «Если бы я сначала прочитал „Историю октав" Ван дер Блея [42], я бы назвал свою статью „Целые октавы"». Мы будем называть элементы кольца O (аналогичные гурвицевым целым кватернионам) октавными целыми; в знак признания заслуг Грейвза, мы будем называть «грейвзовыми целыми октавами» аналог липшицевых целых.

§ 9.1. Определение целости

В главе 5 мы ввели два понятия целого кватерниона, по Липшицу и по Гурвицу; зададимся теперь вопросом, в каком случае целой можно считать октаву. В наши дни алгебраисты понимают «целое» как принадлежащее некоторому *максимальному порядку* (понятие введено Диксоном, который использовал термин «арифметика»).

Понятие *порядка* первоначально появилось в связи с полями алгебраических чисел (т. е. конечных расширений поля рациональных

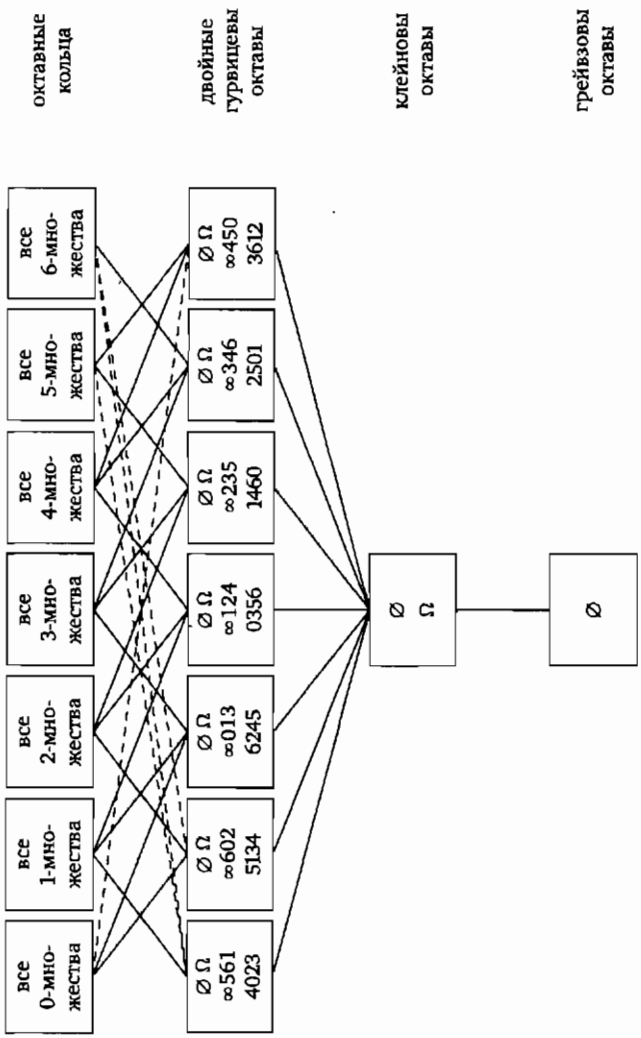


Рис. 9.1. 16 порядков, содержащих грейвзовы октавы G^8

чисел); в этом контексте оно означает кольцо, всякий элемент которого удовлетворяет уравнению вида

$$x^n + c_{n-1}x^{n-1} + \ldots + c_0 = 0,$$

где $c_{n-1}, \ldots, c_0 \in \mathbb{Z}$. Диксон называл *арифметикой* максимальный порядок.

Например, в $\mathbb{Q}(\sqrt{-3})$ число $a + b\sqrt{-3}$ удовлетворяет уравнению $x^2 - 2ax + (a^2 + 3b^2) = 0$, так что кольцо $\mathbb{Q}[\sqrt{-3}]$ (состоящее из чисел вида $a + b\sqrt{-3}$, где $a, b \in \mathbb{Z}$)[1], бесспорно, является порядком. Однако же большее кольцо эйзенштейновых целых (для которых $2a, a + b \in \mathbb{Z}$) также является порядком, так что $\mathbb{Q}[\sqrt{-3}]$ не является *максимальным* порядком, то есть арифметикой.

Той же терминологией мы будем пользоваться и для «кольца» рациональных октав $\mathbb{Q}(i_0, i_1, i_2, i_3, i_4, i_5, i_6)$, хотя оно и не является ассоциативным. Поскольку минимальный многочлен элемента $\alpha = a_\infty + a_0 i_0 + \ldots + a_6 i_6$ есть

$$x^2 - 2a_\infty x + (a_\infty^2 + a_0^2 + \ldots + a_6^2) = 0,$$

условие состоит в том, что «след» $2a_\infty$ и «норма» $a_\infty^2 + a_0^2 + \ldots + a_6^2$ должны быть обычными целыми числами для любого элемента, принадлежащего порядку (или арифметике) в $\mathbb{Q}(i_0, i_1, i_2, i_3, i_4, i_5, i_6)$.

§ 9.2. На пути к октавным целым

Самый очевидный порядок в $\mathbb{Q}(i_0, i_1, i_2, i_3, i_4, i_5, i_6)$ состоит из октав, у которых все координаты являются обычными целыми числами; мы назовем их *грейвзовыми октавами* или *грейвзовыми целыми*. В этом параграфе мы докажем следующий факт.

Теорема 1. *Всякий порядок, содержащий грейвзовы целые, является одной из* 16 *систем, перечисленных на рис.* 9.1.

В дальнейшем нам будут неоднократно встречаться октавы α, все координаты которых лежат в $\frac{1}{2}\mathbb{Z}$. Номера координат такой октавы, не являющихся целыми числами, образуют множество, которое мы будем называть *полуцелым множеством* (halving-set) октавы α.

Лемма 1. *Если α принадлежит порядку, содержащему грейвзовы целые, то для всякой его компоненты a_r число $2a_r$ является целым, и число элементов всякого полуцелого множества (обозначим его m) делится на* 4.

[1] Обычно это кольцо обозначают $\mathbb{Z}[\sqrt{-3}]$. — *Прим. перев.*

Доказательство. Для доказательства первого утверждения достаточно умножить α на i_r. Для доказательства второго утверждения заметим, что

$$a_\infty^2 + \ldots + a_6^2 \equiv \frac{m}{4} \pmod 1. \qquad \square$$

Имея в виду эту лемму, введем следующие обозначения. Положим

$$i_{abcd} = \frac{i_a + i_b + i_c + i_d}{2}$$

и будем ставить черточки над индексами для обозначения вычитания (вместо сложения):

$$i_{a\bar{b}c\bar{d}} = \frac{i_a - i_b + i_c - i_d}{2}.$$

Мы можем задать каждый из 16 порядков, указав, каковы его полуцелые множества. Мультипликативная структура октав сама по себе задает выделенное семейство четверок индексов, а именно четверки, соответствующие кватернионным подалгебрам, а также их дополнения. Эти четверки, вместе с пустым множеством и множеством, состоящим из всех индексов, образуют 16 множеств, которые мы будем называть *∞-множествами*:

$\varnothing$	$\infty 124$	$\infty 235$	$\infty 346$	$\infty 450$	$\infty 561$	$\infty 602$	$\infty 013$
$\Omega = \infty 0123456$	0356	0146	0125	1236	0234	1345	2456

Октава, полуцелое множество которой является ∞-множеством, называется *∞-целой*, или *целой по Кирмзе*, в честь Кирмзе (J. Kirmse), полагавшего (что естественно, но ошибочно), что эти октавы образуют максимальный порядок[1].

Тем не менее, Кокстер обнаружил, что *множество ∞-целых не является мультипликативно замкнутым*. Например, произведение ∞-целых чисел $i_{\infty 026}$ и $i_{\infty 013}$ есть i_{0235}, и это не есть ∞-целое; произведение же этого числа с ∞-целым $i_{\infty 235}$ есть число

$$-\frac{3}{4} + \frac{1}{4}(i_0 - i_1 + i_2 + i_3 - i_4 + i_5 + i_6)$$

с минимальным многочленом $x^2 + \frac{3}{2}x + 1$, и это число никак не является целым.

Необходимая поправка была сделана Диксоном (позднее это было переоткрыто и дополнено Бруком). Мы определим *n-множества* и *n-целые* ($n = 0, \ldots, 6$), переставив ∞ и n в определении ∞-множеств и ∞-целых.

Теперь имеем следующую лемму.

[1]Эта совершенно естественная мысль посещала и других людей, так что удобно дать ей стандартное название «ошибка Кирмзе». Произведение двух случайно выбранных целых по Кирмзе чисел оказывается целым по Кирмзе более чем в трети случаев.

Лемма 2. *Множество n-целых чисел мультипликативно замкнуто для каждого* $n=0,\ldots,6$.

Доказательство. Семь множеств очевидным образом изоморфны, так что мы проверим утверждение только для 0-целых, для которых полуцелые множества имеют вид

$\varnothing$	0124	0235	0346	∞450	0561	∞602	∞013
$\Omega=\infty$0123456	∞356	∞146	∞125	1236	∞234	1345	2456

Из этой таблицы явствует, что 0-целые порождены элементами $i_{\infty 356}$, i_{0235}, i_{0463} и i_{0156} над грейвзовыми целыми, причем таблица умножения этих образующих выглядит так:

	$i_{\infty 356}$	i_{0235}	i_{0463}	i_{0156}
$i_{\infty 356}$	$i_{\overline{\infty}356}$	$i_{\overline{\infty}234}$	$i_{\overline{\infty}461}$	$i_{\overline{\infty}152}$
i_{0235}	$i_{\overline{\infty}0\overline{4}5}$	-1	$i_{\overline{\infty}1\overline{2}5}$	$i_{\overline{\infty}\overline{4}1\overline{6}}$
i_{0463}	$i_{\overline{\infty}0\overline{1}3}$	$i_{\overline{\infty}\overline{1}2\overline{5}}$	-1	$i_{\overline{\infty}2\overline{4}3}$
i_{0156}	$i_{\overline{\infty}0\overline{2}6}$	$i_{\overline{\infty}\overline{4}1\overline{6}}$	$i_{\overline{\infty}\overline{2}4\overline{3}}$	-1

□

Порядки, о которых идет речь в лемме 2, — это семь из шестнадцати порядков из теоремы 1, а именно семь максимальных порядков (см. рис. 9.1). Попарные пересечения этих семи порядков (совпадающие также с некоторыми пересечениями по три) — это семь «двойных гурвицевых колец». (Полуцелые множества $\varnothing$, Ω, $\infty 124$ и 0356 для типичного такого кольца показывают, что двойные гурвицевы кольца получаются удвоением из кольца гурвицевых кватернионов.) Пересечение всех семи максимальных порядков, совпадающее с пересечением любых двух двойных гурвицевых колец, будет называться *клейновыми октавами*, поскольку они получаются из грейвзовых целых октав добавлением элемента $\frac{1}{2}(1+i_0+\ldots+i_6)$, каковой, имея вид $\frac{1}{2}(1+\sqrt{-7})$, является «клейновым» целым (см. главу 2).

Завершим теперь доказательство теоремы 1. Мы видим, что всякое допустимое полуцелое множество является n-множеством для некоторого $n\neq\infty$, поскольку на рис. 9.2 представлены все множества из 0, 4 или 8 индексов. Мы будем называть n-множество *внутренним* или *внешним* в соответствии с тем, является оно также ∞-множеством или нет.

Сначала разберемся с внешними n-множествами.

∞124	0356
∞235	1460
∞346	2501
∞450	3612
∞561	4023
∞602	5134
∞013	6245
∅	Ω

∞-множества

0124	**∞356**
0235	**146∞**
0346	**25∞1**
∞045	3612
0561	**4∞23**
∞062	5134
∞013	6245
∅	Ω

0-множества

∞124	0356
1235	**∞460**
1346	**250∞**
1450	**36∞2**
∞561	4023
1602	**5∞34**
∞013	6245
∅	Ω

1-множества

∞124	0356
∞235	1460
2346	**∞501**
2450	**361∞**
2561	**40∞3**
∞602	5134
2013	**6∞45**
∅	Ω

2-множества

3124	**0∞56**
∞235	1460
∞346	2501
3450	**∞612**
3561	**402∞**
3602	**51∞4**
∞013	6245
∅	Ω

3-множества

∞124	0356
4235	**1∞60**
∞346	2501
∞450	3612
4561	**∞023**
4602	**513∞**
4013	**62∞5**
∅	Ω

4-множества

5124	**03∞6**
∞235	1460
5346	**2∞01**
∞450	3612
∞561	4023
5602	**∞134**
5013	**624∞**
∅	Ω

5-множества

6124	**035∞**
6235	**14∞0**
∞346	2501
6450	**3∞12**
∞561	4023
∞602	5134
6013	**∞245**
∅	Ω

6-множества

Рис. 9.2. Все n-множества; внешние множества выделены жирным шрифтом

Лемма 3. *Всякая октава α, у которой полуцелое множество является внешним n-множеством, порождает над грейвзовыми октавами кольцо всех n-целых.*

Доказательство. Можно считать, что полуцелое множество является одним из восьми внешних 0-множеств. Вычитая подходящее грейвзово целое, можно привести α к виду

$$\alpha = \frac{1}{2}(\pm i_a \pm i_b \pm i_c \pm i_d)$$

(выбор знаков неважен ввиду возможности прибавить грейвзово целое). Теперь на рис. 9.3 видно, как умножение на три грейвзовы единицы связывает между собой все восемь внешних 0-множеств. Поскольку каждое внутреннее 0-множество является суммой двух внешних, получающиеся при таких умножениях октавы аддитивно порождают все 0-целые. ❑

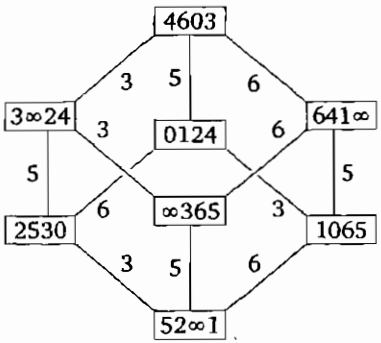


Рис. 9.3. Восемь внешних 0-множеств, связанных умножением на i_3, i_5 и i_6 (знаки мы игнорируем)

Теперь займемся внутренними n-множествами, являющимися заодно и ∞-множествами.

Лемма 4. (i) *Если у двух целых октав полуцелые множества являются взаимно дополнительными четырехэлементными ∞-множествами, то каждая из этих октав лежит в кольце, порожденном другой над грейвзовыми целыми.*

(ii) *Две октавы, чьи полуцелые множества являются различными недополнительными четырехэлементными ∞-множествами, порождают над грейвзовыми целыми кольцо n-целых для некоторого n (см. рис. 9.4).*

Доказательство. (i) Левое умножение на i_0 переводит элемент $\frac{1}{2}(i_\infty + i_1 + i_2 + i_4)$ в $\frac{1}{2}(i_0 + i_3 + i_6 + i_5)$ и т. д.

(ii) Ввиду (i) можно считать, что оба множества содержат ∞, так что одно получается из другого прибавлением к индексам чисел 1, 2 или 4 (по модулю 7); не ограничивая общности, можно считать, что прибавляется 1, поскольку имеется симметрия $\beta = (i_1 i_2 i_4)(i_3 i_6 i_5)$, удваивающая индексы. Стало быть, опять-таки без потери общности, можно считать, что два полуцелых множества — это $\infty 602$ и $\infty 013$, а мы уже видели, что произведение $i_{\infty 602}$ и $i_{\infty 013}$ имеет полуцелым множеством 0235, а это внешнее 0-множество. □

Теперь легко доказать, что всякий порядок, содержащий грейвзовы целые, является одним из перечисленных шестнадцати. Если он не совпадает ни с грейвзовыми, ни с клейновыми октавами, то в нем должен присутствовать элемент с четырехэлементным полуцелым множеством, а следовательно, и с дополнительным к нему полуцелым

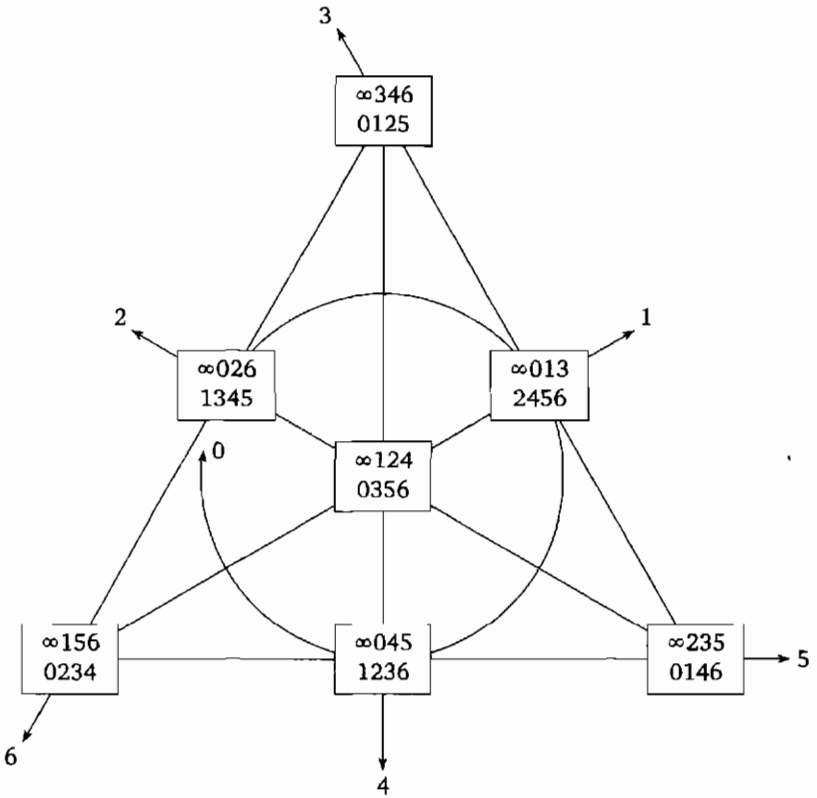


Рис. 9.4. Если две «точки» на этой «плоскости» лежат на «прямой», обозначенной символом n, то октавы с соответствующими полуцелыми множествами порождают кольцо n-целых

множеством, а также с множествами $\varnothing$ и Ω. Если никаких других полуцелых множеств не имеется, то это двойное гурвицево кольцо. В противном случае должно встретиться либо внешнее множество, либо два различных недополнительных внутренних множества, и тогда кольцо содержит все кольцо n-целых для некоторого n.

Если порядок строго больше, чем такое кольцо, то это же рассуждение показывает, что он содержит кольца n-целых для двух различных значений n. Применяя при необходимости симметрию β, удваивающую индексы, можно считать, что эти два значения n отличаются на 2, так что без потери общности можно предполагать, что порядок со-

держит 0-целое $i_{\infty 235}$ и 2-целое i_{0235}, произведение которых, как мы видели, целым не является.

§ 9.3. Решетка E_8 (Коркин, Золотарев, Госсет)

Зафиксируем теперь один из семи максимальных порядков: будем называть *целыми октавами* 0-целые. Геометрически целые октавы O^8 образуют хорошо известную и очень интересную решетку, которая обычно называется *решеткой корней* E_8 (или *решеткой Госсета*, в честь Торольда Госсета, исследовавшего ее геометрию [19])[1].

Арифметические свойства этой решетки также много изучались. Упомянем следующий результат из аналитической теории квадратичных форм: число векторов из E_8 с нормой $2n > 0$ равно 240, умноженному на сумму кубов делителей числа n. В следующих параграфах мы дадим новое простое геометрическое определение этой решетки и воспользуемся им для доказательства того, что октавы обладают «свойством деления с остатком».

9.3.1. *Симплектическая решетка* A_n

Правильным симплексом (n-мерным) называется выпуклая оболочка $n+1$ точек, находящихся на равных расстояниях друг от друга. n-мерная *симплектическая решетка* A_n порождена векторами, нарисованными на ребрах симплекса. Если в качестве вершин выбрать точки

$$v_i = (0, 0, \ldots, \overset{i}{1}, \ldots, 0, 0)$$

в $(n+1)$-мерном пространстве, то образующими решетки будут

$$v_i - v_j = (0, 0, \ldots, \overset{i}{1}, \ldots, \overset{j}{-1}, \ldots, 0, 0);$$

при этом A_{n+1} отождествляется с множеством $(n+1)$-мерных векторов $(x_0, \ldots, x_n)$ с целочисленными координатами, сумма которых равна нулю.

---

[1]Эта решетка также является единственной «четной унимодулярной» решеткой в размерности 8; именно в этом качестве ее существование было доказано в 1867 году Смитом [39]. Коркин и Золотарев [28] построили ее в явном виде в 1877 году в ходе своих исследований по упаковкам сфер. Блихфельд [6] доказал в 1935 году, что эта решетка действительно задает плотнейшую упаковку сфер в размерности 8.

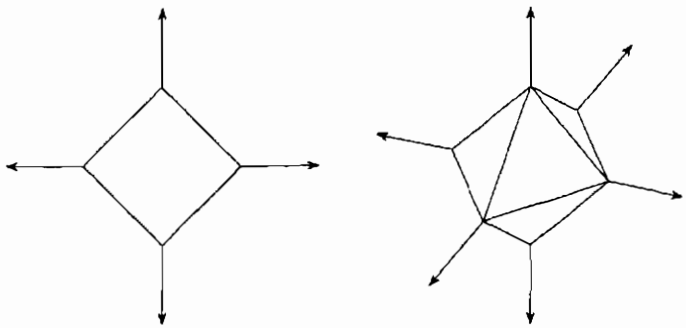


Рис. 9.5. Двумерный ортоплекс является квадратом. Его четыре ребра соответствуют четырем квадрантам на плоскости. Трехмерный ортоплекс — это правильный октаэдр. Его восемь треугольных граней соответствуют восьми октантам, на которые делится пространство

9.3.2. *Ортоплектическая решетка* D_n

Мы будем называть *правильным ортоплексом* аналог двумерного квадрата и трехмерного октаэдра (рис. 9.5). Его вершины $(\pm 1^1, 0^{n-1})$ суть концы единичных векторов, направленных вдоль осей ортонормальной системы координат; он содержит по одной (симплициальной) клетке для каждого из ортантов в n-мерном пространстве (так что «ортоплекс» — это сокращение от «ортантный комплекс»)[1].

Назовем n-мерной *ортоплектической решеткой* D_n решетку, порожденную векторами, нарисованными на ребрах правильного n-мерного ортоплекса. Если в качестве вершин ортоплекса выбрать

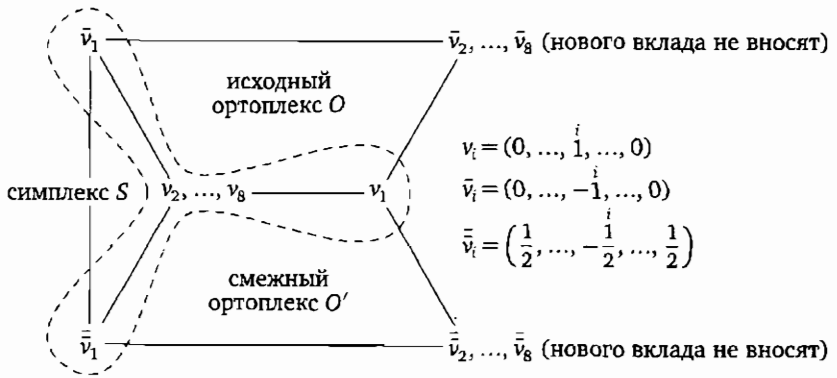
$$v_i = (0, 0, \ldots, \overset{i}{1}, \ldots, 0, 0) \quad \text{и} \quad \bar{v}_i = (0, 0, \ldots, \overset{i}{-1}, \ldots, 0, 0) \quad (i = 1, \ldots, n),$$

то образующими D_n будут все векторы $(\pm 1^2, 0^{n-2})$ и D_n отождествится с решеткой векторов $(x_1, \ldots, x_n)$ с целыми координатами, сумма которых четна.

9.3.3. *Определение решетки* E_8

Мы определим E_8 как решетку $\langle S, O \rangle$, порожденную векторами, нарисованными на ребрах восьмимерного симплекса S и смежного с ним ортоплекса O. Из рис. 9.6 видно следующее:

[1]Автор упоминает также еще один английский термин для этого многогранника: cross polytope. — *Прим. перев.*



Вершины ортоплекса O суть $\nu_1, \ldots, \nu_8, \bar{\nu}_1, \ldots, \bar{\nu}_8$, центр — в точке (0^8).

Вершины ортоплекса O' суть $\nu_1, \ldots, \nu_8, \bar{\bar{\nu}}_1, \ldots, \bar{\bar{\nu}}_8$, центр — в точке $\left(\frac{1}{4}^8\right)$.

Вершины симплекса S суть $\bar{\nu}_1, \bar{\bar{\nu}}_1, \nu_2, \ldots, \nu_8$, центр — в точке $\left(-\frac{1}{6}, \frac{1}{6}^7\right)$.

Рис. 9.6. Все три решетки $\langle S, O\rangle$, $\langle S, O'\rangle$ и $\langle O, O'\rangle$ совпадают с решеткой, порожденной разностями десяти векторов $\bar{\nu}_1, \bar{\bar{\nu}}_1, \nu_1, \nu_2, \ldots, \nu_8$ (это следует из равенств $\nu_1 + \bar{\nu}_1 = \ldots = \nu_8 + \bar{\nu}_8$ и $\nu_1 + \bar{\bar{\nu}}_1 = \ldots = \nu_8 + \bar{\bar{\nu}}_8$)

— E_8 содержит и A_8, и D_8. Как мы увидим, индекс подрешетки A_8 равен 3, а индекс подрешетки D_8 равен 2.

— Если O' — ортоплекс, построенный на соседней грани симплекса S, то $\langle S, O\rangle = \langle S, O'\rangle$, так что наша конструкция обладает всеми симметриями симплекса S: решетка E_8 порождена ребрами симплекса S вкупе с ребрами ортоплекса, построенного на любой из его девяти граней.

— Если, напротив, O' — ортоплекс, построенный на соседней грани ортоплекса O, то $\langle S, O\rangle$ совпадает с решеткой $\langle O, O'\rangle$, порожденной ребрами ортоплексов O и O', симметричных относительно плоскости, разделяющей O и O'. Поэтому в данном случае у нас в два раза меньше симметрии, чем в случае O: решетка E_8 порождена ребрами ортоплекса O, симплекса S, построенного на любой из его 128 граней, и ортоплекса O', полученного из O отражением относительно любой из остальных граней.

Из рис. 9.6 также видно, что восьмимерное пространство, содержащее E_8, покрывается симплексами и ортоплексами, эквивалентными упомянутым выше относительно симметрий. В самом деле, половина граней ортоплекса является гранями эквивалентных ортоплексов, а вторая половина — гранями симплексов, тогда как перейдя через

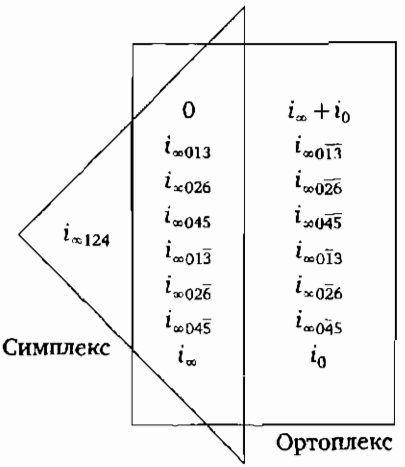


Рис. 9.7. Октавные целые порождают решетку E_8

любую грань симплекса, мы попадаем в ортоплекс. Отсюда получаем следующий факт.

Лемма 5. *Пусть α — произвольная точка восьмимерного пространства. Тогда в решетке E_8 существует такая точка β, что $[\alpha - \beta] \leqslant 1$.*

В самом деле, α лежит либо в симплексе, либо в ортоплексе, так что ее расстояние до решетки не превосходит расстояния до центра этого многогранника.

Чтобы показать, что октавные целые содержат решетку, пропорциональную решетке E_8, достаточно найти среди них вершины симплекса и смежного ему ортоплекса. Как это делается, показано на рис. 9.7. Поскольку нормы этих векторов в два раза меньше, чем нормы векторов построенной нами E_8, можно переформулировать лемму 5 таким образом.

Лемма 6. *Для всякой вещественной октавы α существует октавное целое β, для которого $[\alpha - \beta] \leqslant \frac{1}{2}$.*

§ 9.4. Деление с остатком и идеалы

Применяя лемму 6 к $\delta^{-1}\alpha$ (или к $\alpha\delta^{-1}$), немедленно получаем следующее утверждение.

Теорема 2. *Если α и δ — октавные целые, причем $\delta \neq 0$, то имеет место равенство $\alpha = \delta\beta + \rho$ (а также[1] $\alpha = \beta\delta + \rho$), где $[\rho] \leqslant \frac{1}{2}[\delta]$.*

Поскольку, в частности, $[\rho] < [\delta]$, получаем обычным образом такой результат.

Теорема 3. *Всякий левый или правый идеал в O^8 является главным.*

Обычно идеалами интересуются по той причине, что они используются в стандартных доказательствах теорем о разложении на множители. В некоммутативных кольцах понятия левого и правого идеала не совпадают. Кольцо O^8, однако, является особенным.

Лемма 7. *Всякий идеал в O^8 является двусторонним.*

Доказательство. Всякий правый идеал $\mathcal{I}$ замкнут относительно правого умножения. В главе 8 мы показали, что левые умножения на единичные октавы i_0 и $i_{\infty 365}$ являются произведениями семи правых умножений на единичные октавы. В главе 10 мы увидим, что отсюда легко следует, что всякое левое умножение на единичную октаву есть произведение семи правых умножений. Следовательно, $\mathcal{I}$ замкнуто относительно умножения на единичные октавы и тем самым на произвольные октавные целые, поскольку всякое октавное целое есть сумма единичных октав. □

Можно сказать и больше.

Теорема 4. *Всякий двусторонний идеал $\Lambda \subset O^8$ есть главный идеал nO^8, порожденный целым рациональным числом n.*

Эта теорема убивает надежду на использование идеалов для доказательства единственности разложения. Она была частично доказана Малером [32]; позднее доказательство было намечено Ван дер Блеем и Спрингером [43] и завершено Ламонтом [30]. Из наших геометрических результатов теорема выводится легко.

Доказательство. Мы воспользуемся тем фактом, что идеал Λ инвариантен относительно двусторонних умножений на единичные октавы, каковые умножения порождают группу всех четных симметрий решетки, пропорциональной решетке E_8. Воспользуемся теперь такой теоремой.

Теорема 5. *Если подрешетка $\Lambda \subset E_8$ инвариантна относительно всех четных автоморфизмов решетки E_8, то $\Lambda = nE_8$.*

Чтобы в этом убедиться, воспользуемся «ортоплектическими» координатами для E_8. Пусть $v_1 = (a\ b\ c\ d\ e\ f\ g\ h)$ — элемент из Λ с наименьшей ненулевой нормой. Покажем сначала, что можно считать, что две из его координат равны нулю. В самом деле, если это не так,

[1] С другими β и ρ, вообще говоря. — *Прим. перев.*

то, применив четную перестановку, можем считать, что g и h — две наименьшие по модулю координаты; теперь существует четная симметрия, переводящая v_1 в $v_2 = (a\ b\ c\ d\ e\ f\ -g\ -h)$, и норма вектора $v_3 = v_1 - v_2 = (0\ 0\ 0\ 0\ 0\ 0\ 2g\ 2h)$ не превосходит норму v_1.

Покажем теперь, что можно также считать, что не более чем одна координата отлична от нуля. В самом деле, в противном случае, если две последние координаты равны нулю, существует четная симметрия (3-цикл), переводящая $v_1' = (a\ b\ c\ d\ e\ f\ 0\ 0)$ в $v_2' = (a\ b\ c\ d\ e\ 0\ f\ 0)$, где f — наименьшая по модулю ненулевая координата, и опять норма вектора $v_3' = v_1' - v_2' = (0\ 0\ 0\ 0\ 0\ f\ -f\ 0)$ не превосходит норму v_1'; это показывает, что в Λ найдется минимальный ненулевой вектор, равный умноженному на f минимальному вектору из E_8; применяя четные симметрии, получаем, что в Λ лежит произведение f на любой минимальный вектор из E_8, так что $\Lambda = fE_8$.

Остается рассмотреть случай, когда у минимального вектора имеется ровно одна ненулевая координата. Но тогда этот (лежащий в E_8) вектор обязан иметь вид $(2f\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$; подходящей четной симметрией это переводится в $(f\ f\ f\ f\ 0\ 0\ 0\ 0)$, и можно снова применить рассуждение из предыдущего абзаца. □

Итак, теория идеалов не поможет в исследовании разложения октав на множители. Более плодотворный подход развивается в следующем параграфе.

§ 9.5. Разложение на множители в O^8

В этом параграфе мы покажем, что примитивное октавное целое ρ с нормой mn имеет в точности 240 левых делителей с нормой m и в точности 240 правых делителей с нормой n, причем каждое из множеств таких делителей геометрически подобно множеству из 240 единиц в O^8. Этот результат[1] аналогичен утверждению про гурвицевы целые из главы 5, с тем исключением, что разложения в O^8 не являются единственными «с точностью до переноса единиц», поскольку O неассоциативно. Более общим образом, мы покажем, что множество левых делителей данной целой октавы геометрически подобно множеству всех целых октав с некоторой фиксированной нормой.

Замечательно, что в рассуждении не используется в полной мере деление с остатком в октавах. Тем не менее, используется соответствующее свойство решетки E_8, так что рассуждение не проходит при более

[1]Первые результаты в этом направлении принадлежат Ранкину и Ламонту. Геометрическое утверждение представляется новым.

наивном понимании целых октав; причины этой неудачи более серьезны, чем в случае с липшицевыми целыми кватернионами.

Мы начнем с того, что опишем интересный «обратный алгоритм Евклида», принадлежащий Рему [37]. Алгоритм состоит из двух этапов: прямого хода и обратного. *Прямой ход* (рис. 9.8) начинается с пары ρ_1, m_1, где ρ_1 — октава, норма которой делится на целое рациональное число m_1; по техническим причинам мы записываем остаток со знаком сопряжения. Мы полагаем $[\rho_1] = m_0 m_1$ и последовательно находим числа m_i и октавы γ_i, ρ_i, как показано на рис. 9.8.

$$\begin{array}{lll}
\rho_1 = \gamma_1 m_1 + \bar{\rho}_2 & [\rho_1] = m_0 m_1 & \\
\rho_2 = \gamma_2 m_2 + \bar{\rho}_3 & [\rho_2] = m_1 m_2 & m_1 > m_2 \\
\vdots & \vdots & \vdots \\
\rho_{N-1} = \gamma_{N-1} m_{N-1} + \bar{\rho}_N & [\rho_{N-1}] m_{N-2} m_{N-1} & m_{N-2} > m_{N-1} \\
\rho_N = \gamma_N m_N & [\rho_N] = m_{N-1} m_N & m_{N-1} > m_N > 0
\end{array}$$

Рис. 9.8. Алгоритм Рема: прямой ход

Объясним вкратце, что происходит. Почему $[\rho_2]$ делится на m_1 (так что $m_2 = [\rho_2]/m_1$ — целое число)? Потому что m_1 делит каждое слагаемое в правой части равенства

$$[\bar{\rho}_2] = [\rho_1 - \gamma_1 m_1] = [\rho_1] + m_1^2 [\gamma_1] - m_1 (2[\rho_1, \gamma_1]).$$

Почему $m_2 < m_1$? Потому что $m_1 m_2 = [\rho_2] \leqslant \frac{m_1^2}{2}$.

Если $m_2 > 0$, то мы можем повторить те же рассуждения применительно к ρ_2 и m_2, получить ρ_3 и $m_3 < m_2$ и так далее. Поскольку начиная с m_1 последовательность m_i является убывающей, в какой-то момент окажется, что $m_{N+1} = 0$, и в нашем распоряжении окажется конечный набор элементов O^8, удовлетворяющих соотношениям на рис. 9.8.

Теперь перейдем к изображенному на рис. 9.9 *обратному ходу* алгоритма, устанавливающему взаимно однозначные соответствия

$$\mu_N \longleftrightarrow \mu_{N-1} \longleftrightarrow \ldots \longleftrightarrow \mu_1 \longleftrightarrow \mu_0,$$

являющиеся на самом деле подобиями, между некоторыми делителями октав ρ_i. Именно, пусть μ_N — произвольный элемент с нормой m_N. Поскольку $\mathbb{O}$ диассоциативно, можно записать равенство

$$\rho_N = \gamma_N m_N = \gamma_N (\mu_N \bar{\mu}_N) = (\gamma_N \mu_N) \bar{\mu}_N.$$

$$
\begin{array}{lll}
 & & [\mu_N] = m_N \\
\rho_N = \mu_{N-1}\bar{\mu}_N & \mu_{N-1} = \gamma_N \mu_N & [\mu_{N-1}] = m_{N-1} \\
\rho_{N-1} = \mu_{N-2}\bar{\mu}_{N-1} & \mu_{N-2} = \gamma_{N-1}\mu_{N-1} + \mu_N & [\mu_{N-2}] = m_{N-2} \\
\rho_{N-2} = \mu_{N-3}\bar{\mu}_{N-2} & \mu_{N-3} = \gamma_{N-2}\mu_{N-2} + \mu_{N-1} & [\mu_{N-3}] = m_{N-3} \\
\vdots & \vdots & \vdots \\
\rho_2 = \mu_1\bar{\mu}_2 & \mu_1 = \gamma_2\mu_2 + \mu_3 & [\mu_1] = m_1 \\
\rho_1 = \mu_0\bar{\mu}_1 & \mu_0 = \gamma_1\mu_1 + \mu_2 & [\mu_0] = m_0
\end{array}
$$

Рис. 9.9. Алгоритм Рема: обратный ход

Положим $\mu_{N-1} = \gamma_N \mu_N$, так что μ_{N-1} — левый делитель ρ_N, имеющий норму m_{N-1}. Тогда $\bar{\mu}_{N-1}$ является правым делителем и у $\bar{\rho}_N$, и у m_{N-1}, а значит, и у ρ_{N-1}, поскольку

$$
\begin{aligned}
\rho_{N-1} = \gamma_{N-1} m_{N-1} + \bar{\rho}_N &= (\gamma_{N-1}\mu_{N-1})\bar{\mu}_{N-1} + \mu_N \bar{\mu}_{N-1} = \\
&= (\gamma_{N-1}\mu_{N-1} + \mu_N)\bar{\mu}_{N-1}.
\end{aligned}
$$

Полагая $\mu_{N-2} = \gamma_{N-1}\mu_{N-1} + \mu_N$, находим левый делитель октавы ρ_{N-1}, имеющий норму m_{N-2}. Мы можем продолжать эту процедуру, пока не дойдем до μ_0, являющегося левым делителем $\rho = \rho_1$ с нормой $m = m_0$ и до соответствующего правого делителя $\bar{\mu}_1$ с нормой $n = m_1$. Весь процесс изображен на рис. 9.9; можно сказать, что мы идем снизу вверх по левому столбцу рис. 9.8, по ходу дела проводя разложение.

Заметим, что на этапе алгоритма, представленном на рис. 9.8, умножение в алгебре октав практически не используется. Более того, на рис. 9.9 произведения трех элементов встречаются только в тех случаях, когда все три элемента лежат в одной ассоциативной подалгебре.

9.5.1. *Структура множеств делителей*

Теперь мы можем описать множества всех левых и правых делителей октавы $\rho = \rho_1$, имеющих норму $m = m_0$ и $n = m_1$. Мы увидим, что размер этих множеств совпадает с количеством октавных целых μ_N, норма которых равна целому числу m_N из последней строки на рис. 9.8. Для геометрического описания этих множеств мы воспользуемся следующей леммой.

Лемма 8. *Пусть октавное целое γ разлагается двумя способами: $\gamma = \alpha\beta = \alpha'\beta'$, где $[\alpha] = [\alpha'] \neq 0$ и $[\beta] = [\beta'] \neq 0$. Тогда угол между α и α' (обозначим его θ_a) равен углу между β и β' (обозначим его θ_b).*

Доказательство. Рассматривая скалярное произведение γ и $\alpha\beta'$, получаем

$$[\alpha][\beta, \beta'] = [\alpha\beta, \alpha\beta'] = [\gamma, \alpha\beta'] = [\alpha'\beta', \alpha\beta'] = [\alpha', \alpha][\beta'],$$

откуда имеем

$$\cos\theta_a = \frac{[\alpha, \alpha']}{[\alpha]} = \frac{[\beta, \beta']}{[\beta']} = \cos\theta_b. \qquad \square$$

Пусть через $\{\mu_N\}, \{\mu_{N-1}\}, \ldots, \{\mu_0\}$ обозначены все множества μ_k, возникающие на обратном ходе алгоритма Рема (рис. 9.9). Мы показали, что $\{\mu_N\}$ есть множество всех октавных целых с нормой m_N. Оно очевидным образом подобно сопряженному множеству $\{\bar{\mu}_N\}$; можно также получить этот результат, положив $\gamma = m_N$ в лемме 8. Мы будем обозначать это подобие следующим образом:

$$\{\mu_N\} \overset{m_N}{\sim} \{\bar{\mu}_N\}.$$

Аналогичным образом, полагая по очереди $\gamma = \rho_i$ и $\gamma = m_i$, получаем подобия

$$\{\bar{\mu}_N\} \overset{\rho_N}{\sim} \{\mu_{N-1}\} \overset{m_{N-1}}{\sim} \{\bar{\mu}_{N-1}\} \overset{\rho_{N-1}}{\sim} \ldots \overset{m_1}{\sim} \{\bar{\mu}_1\} \overset{\rho_1}{\sim} \{\mu_0\}.$$

Однако $\{\mu_0\}$ и $\{\bar{\mu}_1\}$ суть в точности множества левых и правых делителей октавы ρ_1 с нормой n. Тем самым мы приходим к следующей теореме.

Теорема 6. *Пусть $\rho = \rho_1$ — октавное целое с нормой mn, где m и n — целые положительные числа. Пусть d — целое число, являющееся наибольшим общим делителем ρ, m и n. Тогда множество левых делителей (μ_0) октавы ρ с нормой m и множество правых делителей $(\bar{\mu}_1)$ октавы ρ с нормой n геометрически подобны множеству всех октавных целых (μ_N) с нормой $d = m_N$.*

Доказательство. Почти все мы уже сделали, осталось уточнить норму, то есть найти m_N. Будем обозначать через н.о.д.$(\eta_1, \ldots, \eta_k)$ наибольшее целое рациональное число, являющееся общим делителем элементов $\eta_1, \ldots, \eta_k \in O^8$. Имеем следующую лемму.

Лемма 9. *Если $1 \leqslant i \leqslant N$, положим $d_i =$ н.о.д.(ρ_i, m_{i-1}, m_i). Тогда $d_i = d_{i+1}$ при $1 \leqslant i \leqslant N-1$.*

Доказательство леммы. Заметим, что d_i делит $\bar{\rho}_{i+1} = \rho_i - \gamma_i m_i$, поскольку d_i делит ρ_i и m_i; стало быть, d_i делит ρ_{i+1}. Кроме того, d_i по определению делит m_i. Наконец, d_i делит и m_{i+1}, поскольку d_i делит

каждое слагаемое во второй строке равенства

$$m_{i+1}=\frac{[\bar{\rho}_{i+1}]}{m_i}=\left(\frac{1}{m_i}\right)([\rho_i]+m_i^2[\gamma_i]-m_i(2[\gamma_i,\rho_i]))=$$
$$=m_{i-1}+m_i[\gamma_i]-2[\gamma_i,\rho_i].$$

Стало быть, d_i делит d_{i+1}; аналогичное рассуждение показывает, что d_{i+1} делит d_i, так что $d_i=d_{i+1}$. □

Из доказанного наша теорема сразу следует, поскольку

$$d_N=\text{н.о.д.}(\rho_N,m_{N-1},m_N)=m_N$$

и тем самым

$$m_N=d_1=\text{н.о.д.}(\rho_1,m_0,m_1)=\text{н.о.д.}(\rho,m,n)=d.$$ □

С помощью этой теоремы можно найти число разложений на более чем два сомножителя с произвольными нормами и «отношением к импримитивности». В следующем параграфе обсуждается только разложение на простые.

§ 9.6. Число разложений на простые

В главе 5 мы нашли количество разложений кватерниона на простые множители, моделируемых на данном разложении его нормы. Например, с точностью до переноса единиц существует ровно 12 разложений на простые множители у примитивного числа Гурвица с нормой 60; они моделируются на следующих разложениях числа 60 в произведение простых рациональных чисел:

$$2\cdot2\cdot3\cdot5,\quad 2\cdot2\cdot5\cdot3,\quad 2\cdot3\cdot2\cdot5,\quad 2\cdot5\cdot2\cdot3,\quad 2\cdot3\cdot5\cdot2,\quad 2\cdot5\cdot3\cdot2,$$
$$3\cdot2\cdot2\cdot5,\quad 5\cdot2\cdot2\cdot3,\quad 3\cdot2\cdot5\cdot2,\quad 5\cdot2\cdot3\cdot2,\quad 3\cdot5\cdot2\cdot2,\quad 5\cdot3\cdot2\cdot2.$$

Поскольку для октав ассоциативность не имеет место, ситуация меняется в двух отношениях. Во-первых, теперь имеется $5\times12=60$ разложений числа 60 в произведение обычных простых чисел:

$$60=((2\cdot2)3)5=(2(2\cdot3))5=(2\cdot2)(3\cdot5)=2((2\cdot3)5)=2(2(3\cdot5))=$$
$$=((2\cdot2)5)3=(2(2\cdot5))3=\ldots$$

Во-вторых, разложения октавы Q, моделируемые на одном и том же разложении нормы, больше не обязаны получаться одно из другого с помощью переноса единиц, поскольку $\alpha u\cdot u^{-1}\beta$ не обязано равняться $\alpha\beta$.

Будем поэтому называть преобразование, затрагивающее только два соседних множителя, *метапереносом*, поскольку оно «имитирует»

перенос единиц. Заметим, что количество разложений вида $\beta u \cdot u^{-1}\gamma$, получаемых переносом единиц из $\beta\gamma$, равно количеству единиц, а множество левых сомножителей вида βu геометрически подобно множеству единиц u. Из нашей теоремы о разложениях на два множителя легко вытекает следующее.

Теорема 7. *Количество разложений примитивного октавного целого (например, $Q=((P_1P_2)(P_3(P_4\ldots P_k))))$, моделируемых на данном разложении его нормы, равно 240^{k-1}. Более того, если зафиксировать все простые, кроме P_i и P_j, то множества возможных значений P_i и P_j геометрически подобны множеству из 240 единиц.*

Что будет, если октава не обязательно примитивна?

Теорема 8. *Октава с нормой $p_1^{n_1}\ldots p_k^{n_k}$, делящаяся на $p_1^{s_1}\ldots p_k^{s_k}$, но не более того, имеет в точности*

$$240^{n-1}\prod C_{n_i,s_i}(p_i^3)$$

разложений на простые по данной модели. Здесь «усеченные многочлены Каталана» $C_{n,s}(x)$ определены в главе 5, а $n=n_1+\ldots+n_k$.

Доказательство. Как и в случае кватернионов, достаточно сосредоточить внимание на одном рациональном простом числе p. Для разложений вида

$$P_1(P_2(\ldots(P_{n-1}P_n)\ldots))$$

рассуждение будет точно таким же, как в главе 5, с теми отличиями, что мы не можем работать с точностью до переноса единиц и поэтому должны добавлять множители 240 по мере их появления, а также что p надо заменить на p^3, поскольку имеется $240(p^3+1)$ октав с нормой p (число 2 особым статусом более не обладает).

Аналогичное рассуждение применимо и к разложениям вида

$$P_1((P_2P_3)P_4),$$

которые можно получить, добавляя множители по одному. Чтобы разобраться с разложениями, не имеющими такого вида, например,

$$(P_1P_2)(P_3P_4),$$

можно воспользоваться «леммой о мета-ассоциативности», утверждающей, что имеется одинаковое количество разложений вида $(AB)C$ и $A'(B'C')$, если в каждой из пар (A, A'), (B, B') и (C, C') оба элемента имеют одинаковую норму и делятся на те же целые рациональные числа. Детали мы опускаем. □

Если модель не фиксирована, то общее количество разложений на простые равно произведению 240^{n-1} на следующие числа:

— $C_{n_1,s_1}(p_1^3)\ldots C_{n_k,s_k}(p_k^3)$ — произведение чисел, дающих количество разложений по данной модели с точностью до метапереноса;

— мультиномиальный коэффициент $\binom{n}{n_1,\ldots,n_k}$, дающий количество способов упорядочить простые множители в данной модели;

— число Каталана C_{n-1}, дающее количество расстановок скобок.

(Чтобы получить из этой формулы соответствующий результат для кватернионов, надо заменить 240 на 24 и p_i^3 на p_i, а также опустить множители C_{n-1}, поскольку имеет место ассоциативность.)

Вряд ли можно утверждать, что разложение октав на простые единственно, пока мы не решили сформулированные ниже задачи о метапереносе, метакоммутировании и мета-ассоциативности. Тем не менее Ранкин и Ламонт отмечают, что разложение на простые множители примитивной октавы с нечетной нормой можно сделать единственным, если дополнительно потребовать, чтобы сомножители были сравнимы по модулю 2 с заданными единицами.

§ 9.7. «Метазадачи» для разложения октав

Напомним, что мы свели вопрос о единственности разложения гурвицевых кватернионов к *задаче о метакоммутировании*: как связаны разложения PQ и QP, моделируемые на pq и qp? При разложении октав возникает также *задача о мета-ассоциативности*: как связаны разложения $(PQ)R$ и $P'(Q'R')$, моделируемые на $(pq)r$ и $p(qr)$? Кроме того, есть еще и *задача о метапереносе*: как связаны разложения PQ и $P'Q'$, моделируемые на одном и том же pq, коль скоро они больше не связаны через перенос единиц?

Еще один вопрос — понять, как устроено разложение в грейвзовом случае. Следующее утверждение, соответствующее теореме 6, доказано Ч. Фо (C. Feaux) [16].

Теорема 9. *Если p и q — два различных простых числа, то грейвзово целое с нормой pq имеет ровно 16 разложений по модели pq:*

$$P_1Q_1 = (-P_1)(-Q_1) = \ldots = P_8Q_8 = (-P_8)(-Q_8).$$

Более того, множество левых множителей геометрически подобно множеству грейвзовых единиц (иными словами, $P_1,\ldots,P_8$ попарно ортогональны); то же верно и применительно к правым множителям.

Задача о метапереносе в грейвзовом случае состоит в том, что надо выяснить, как получить все эти 16 разложений, начав с одного из них. У нас есть частичный ответ на этот вопрос для случая, когда целая октава лежит в липшицевом подкольце.

Теорема 10. *Если $L=PQ$ и $L=Q'P'$ — разложения липшицева целого $L=a+bi_1+ci_2+di_4$ по моделям pq и qp соответственно, то все грейвзовы разложения октавы L, моделируемые на pq, суть*

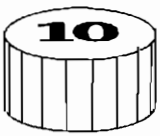
$$PU\cdot\bar{U}Q \quad \text{и} \quad P'V\cdot\bar{V}Q',$$

где U пробегает множество $\{\pm 1, \pm i_1, \pm i_2, \pm i_4\}$, а V пробегает множество $\{\pm i_0, \pm i_3, \pm i_5, \pm i_6\}$.

Доказательство. Это немедленно следует из формулы удвоения

$$(a+i_0b)(c+i_0d)=(ac-d\bar{b})+i_0(cb+\bar{a}d). \qquad \square$$

Итак, в данном случае задача о метапереносе для грейвзовых целых сводится к задаче о метакоммутировании для липшицевых целых.



Автоморфизмы и подкольца в O

В этой главе мы изучим октавные целые более подробно, а затем воспользуемся полученной информацией для нахождения группы автоморфизмов кольца $O = O^8$ и изучения некоторых его подколец.

§ 10.1. 240 октавных единиц

В первом столбце нижеследующей таблички приведены кватернионные тройки abc (для которых i_a, i_b и i_c ведут себя как i, j и k). Если добавить к такой тройке ∞ (или 0), то получится четверка, являющаяся полуцелым множеством для октав; дополнение к такой четверке также является полуцелым множеством.

тройка		
124	0	∞365
235	0	∞461
346	0	∞512
450	∞	6123
561	0	∞234
602	∞	1345
013	∞	2456
четверка		дополнительная четверка

Октавные единицы — это октавные целые, обратные к которым также являются октавными целыми. Сколько всего октавных единиц?

Теорема 1. *Существует ровно* 240 *октавных единиц.*

Доказательство. Единицы могут иметь вид либо

$$\pm 1,\ \pm i_0, \ldots, \pm i_6,$$

либо

$$\frac{1}{2}(\pm i_a \pm i_b \pm i_c \pm i_d),$$

где $abcd$ — одно из 14 четырехэлементных 0-множеств. Поскольку во втором случае знаки можно выбирать шестнадцатью способами, общее количество единиц равно $16+14\cdot 16=240$. □

Немногим сложнее расклассифицировать единицы по (мультипликативному) порядку. Имеется:

по одной единице порядков 1 и 2 (именно, $+1$ и -1);

по 56 единиц каждого из порядков 3 и 6: это единицы вида $\pm\frac{1}{2}(-1\pm\pm i_a\pm i_b\pm i_c)$, где abc имеет вид 356, 146, 125, 450, 234, 602 или 013;

и, наконец, 126 единиц порядка 4: это $\pm i_n$ и $\frac{1}{2}(\pm i_d\pm i_e\pm i_f\pm i_g)$, где $defg$ имеет вид 0124, 0235, 0346, 1236, 0561, 1345 или 2456.

Мы будем обозначать элементы мультипликативных порядков 3 и 4 буквами ω и i соответственно с подходящими нижними индексами; например,

$$\omega_{abc}=\frac{1}{2}(-1+i_a+i_b+i_c),\quad i_{defg}=\frac{1}{2}(i_d+i_e+i_f+i_g);$$

если перед какой-то компонентой стоит знак «минус», то над соответствующей буквой в нижнем индексе будем ставить черточку:

$$\omega_{ab\bar{c}}=\frac{1}{2}(-1+i_a+i_b-i_c),\quad i_{d\bar{e}\bar{f}g}=\frac{1}{2}(i_d-i_e-i_f+i_g).$$

Если мы интересуемся множествами, порождаемыми различными семействами единиц, то взаимно обратные единицы разумно рассматривать вместе. Имея это в виду, можно сказать, что мы изучаем чудовище с 63 парами «глаз» (по-английски eyes — i's) и 28 парами «рук» (по-английски arms, что созвучно с «oms» — сокращением от «omegas»).[1]

§ 10.2. Два типа ортогональности

В нескольких следующих парграфах мы будем изучать группу $\mathrm{Aut}(O)$ кольца O октавных целых. В некотором отношении это дискретный аналог того, чем мы занимались в главе 6. Именно в ней мы выяснили, что группа автоморфизмов вещественных октав есть 14-мерная группа Ли $G_2(\mathbb{R})$, которую мы будем сокращенно обозначать G_2. Как мы увидим, группа автоморфизмов кольца октавных целых — это аналогичная группа $G_2(\mathbb{F}_2)$ над полем $\mathbb{F}_2$ (поле из двух элементов). Специалисты по теории групп обычно обозначают эту группу просто $G_2(2)$.

[1]Мы будем называть эти «глаза» и «руки» соответственно i-единицами и ω-единицами. — *Прим. перев.*

Как правило, дискретная теория параллельна непрерывной, с небольшими отличиями. Например, в непрерывном случае мы выяснили, что всякая единица, ортогональная к 1, неотличима от любой другой такой единицы и что всякая ортогональная пара таких единиц неотличима от любой другой такой пары. Первое из этих двух утверждений остается верным и в дискретном случае, а вот второе — нет. Иными словами, все 126 «глаз» — единиц, ортогональных к 1, — эквивалентны друг другу при действии группы, тогда как пары i, j ортогональных i-единиц разбиваются на два вида. Мы будем говорить, что i и j *четно ортогональны*, если $\frac{1+i+j+ij}{2}$ — тоже октавное целое, и *нечетно ортогональны* в противном случае. При этом будем говорить, что i, j и ij образуют соответственно *четную* или *нечетную* кватернионную тройку.

Октавное целое вида $\frac{1}{2}(\pm i_a \pm i_b \pm i_c \pm i_d)$ мы будем обозначать через i'_{abcd}, где количество знаков «минус» нечетно, через i''_{abcd} — аналогично записываемое октавное целое, если число минусов четно, и через i^*_{abcd} — произвольное октавное целое такого вида.

Лемма 1. *Единица i_0 ортогональна в точности 60 другим i-единицам; при этом она четно ортогональна к 12 из них, а именно к $\pm i_1$, $\pm i_2$, ..., $\pm i_6$, и нечетно ортогональна к 48 из них, а именно к единицам вида i^*_{1236}, i^*_{2465}, i^*_{4153}.*

Доказательство. Поскольку всякая i-единица, отличная от $\pm i_n$, имеет вид i^*_{abcd} и поскольку 1236, 2465 и 4153 — единственные 0-множества, не содержащие ни ∞, ни 0, таких i-единиц действительно именно 60. Что же до типов ортогональности, то благодаря наличию удваивающей индексы симметрии $(i_1 i_2 i_4)(i_3 i_6 i_5)$ достаточно показать, что $j = i_1$ или i_3 четно ортогонально к $i = i_0$ — а это так и есть, поскольку

$$\frac{1+i+j+ij}{2} = \frac{1+i_0 \pm i_1 \pm i_3}{2}$$

лежит в O_8, а также показать, что $j = i^*_{1236}$ нечетно ортогонально к i_0 — а это также верно, поскольку

$$\frac{1+i+(j+ij)}{2} = \frac{1+i_0+(\pm i_{1\text{ или }3} \pm i_{2\text{ или }6})}{2}$$

в O^8 не лежит. □

Начиная с этого момента мы будем работать «с точностью до знака» и тем самым говорить, что имеется ровно шесть i-единиц, четно ортогональных к i_0.

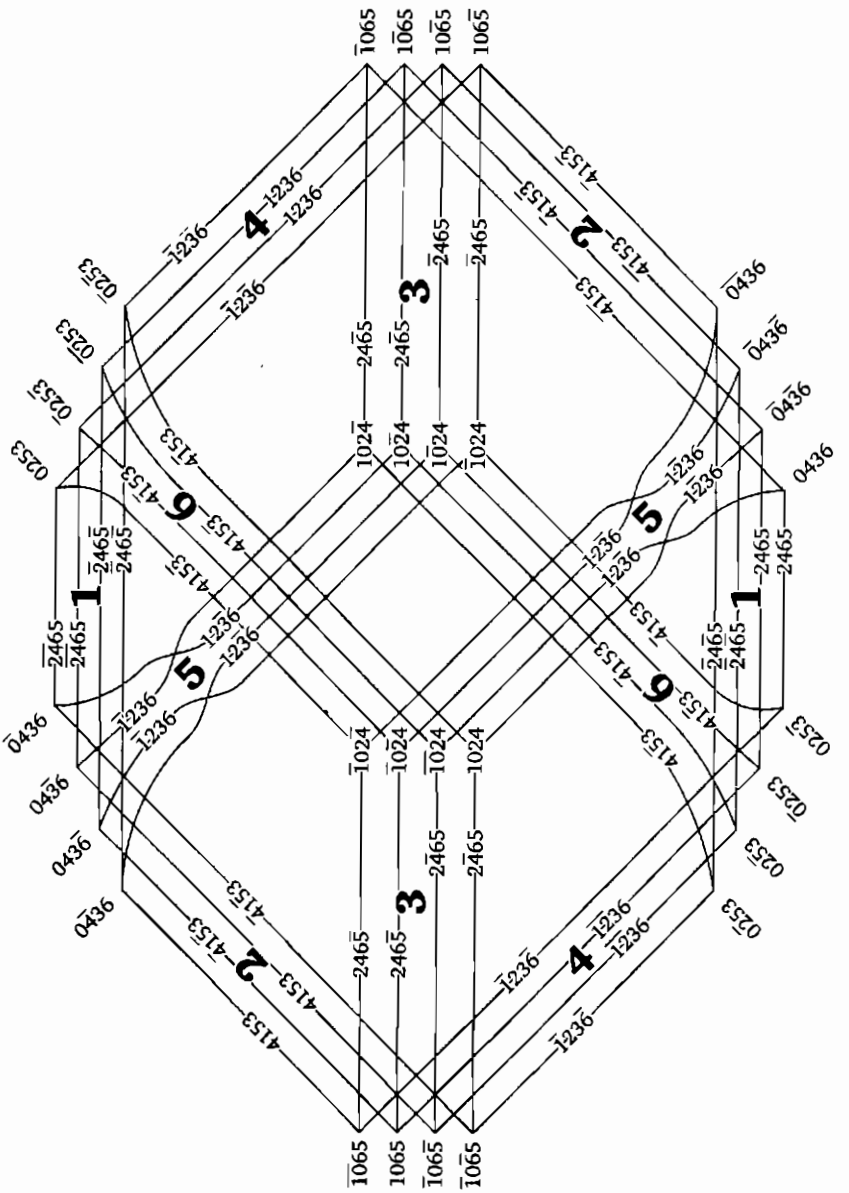


Рис. 10.2. «Дальняя сторона» гипершестиугольника: 48 треугольников

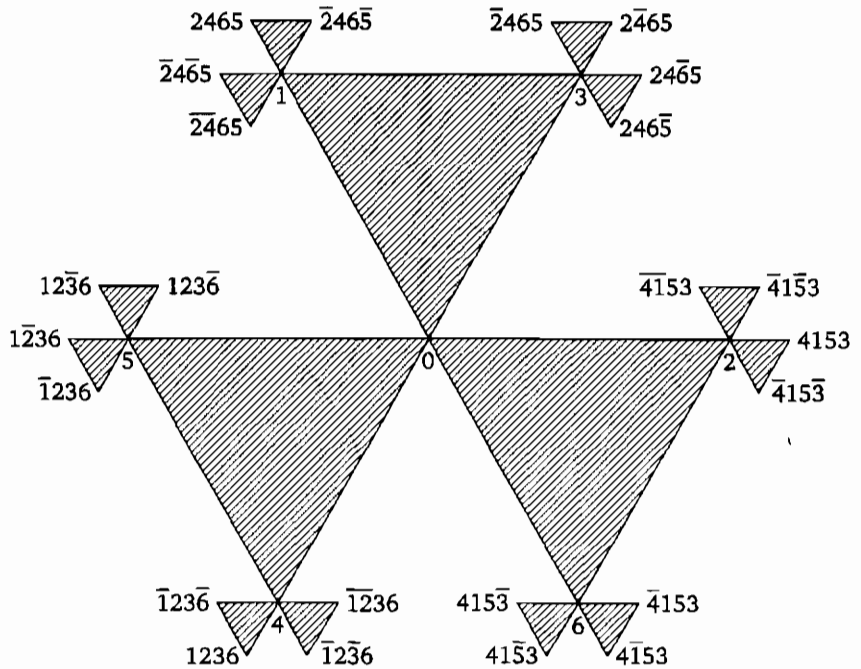


Рис. 10.1. Пятнадцать треугольников гипершестиугольника вблизи вершины i_0 («ближняя сторона»). Каждая внешняя вершина принадлежит еще двум треугольникам; они изображены на рис. 10.2 в виде отрезков

§ 10.3. Группа автоморфизмов кольца O

Если соединить каждую i-единицу с шестью другими i-единицами, четно ортогональными к ней, то получится граф, который мы будем называть гипершестиугольником[1]. На рис. 10.1 изображена часть этого графа, находящаяся вблизи i_0, а на рис. 10.2 — все остальное.

Мы воспользуемся этим графом для доказательства следующей теоремы.

Теорема 2. *Группа* Aut(O) *транзитивна на* i*-единицах.*

Доказательство. Для всякой октавы ω, имеющей порядок 3, отображение $x \mapsto \bar{\omega} x \omega$ является автоморфизмом октавного умножения ввви-

[1]Обычно этот граф называется обобщенным шестиугольником. См. конец этого параграфа.

ду теоремы 14 из главы 8, и этот автоморфизм переводит O в O, если $\omega \in O$. Так что, например, сопряжение на $\omega = \frac{1}{2}(-1+i_0+i_1+i_3)$ является автоморфизмом кольца O, циклически переставляющим i_0, i_1 и i_3.

Точно так же можно построить автоморфизм, переставляющий вершины любого треугольника в гипершестиугольнике; поскольку граф связен, отсюда вытекает транзитивность. □

Что можно сказать про образы i_0, i_1 и i_2 при общем автоморфизме кольца O (обозначим их $i_0^\dagger$, $i_1^\dagger$ и $i_2^\dagger$)? Поскольку i_0 четно ортогонально к i_1 и i_2, а i_1 и i_2 нечетно ортогональны, единицы $i_0^\dagger$, $i_1^\dagger$ и $i_2^\dagger$ должны обладать теми же свойствами. С другой стороны, имеет место такой результат.

Теорема 3. *Если $i_0^\dagger$, $i_1^\dagger$ и $i_2^\dagger$ — три попарно ортогональные i-единицы, причем только ортогональности, в которых участвует $i_0^\dagger$, являются четными, то существует и единствен автоморфизм кольца O, переводящий i_0 в $i_0^\dagger$, i_1 в $i_1^\dagger$ и i_2 в $i_2^\dagger$.*

Доказательство. Единственность получается сразу, поскольку если мы знаем образы i_0, i_1 и i_2, то знаем и образы $i_4 = i_1 i_2$, $i_3 = i_0 i_1$, $i_6 = i_0 i_2$, $i_5 = i_0 i_4$. Для доказательства существования покажем, например, как построить автоморфизм, для которого $i_0^\dagger = i_0$, $i_1^\dagger = i_2$, $i_2^\dagger = i_1$. Тогда имеем

$$\begin{aligned}
i_4^\dagger &= i_1^\dagger i_2^\dagger = i_2 i_1 = -i_4,\\
i_3^\dagger &= i_0^\dagger i_1^\dagger = i_0 i_2 = i_6,\\
i_6^\dagger &= i_0^\dagger i_2^\dagger = i_0 i_1 = i_3,\\
i_5^\dagger &= i_0^\dagger i_4^\dagger = i_0(-i_4) = -i_5,
\end{aligned}$$

так что получается отображение $(i_0)(i_1 i_2)(i_3 i_6)(i_4, -i_4)(i_5, -i_5)$, и легко проверить, что оно является автоморфизмом. Аналогично находятся симметрии

$$\begin{aligned}
&(i_0)(i_1, i_2, i_4)(i_3, i_6, i_5),\\
&(i_0)(i_2)(i_6)(i_1, i_3, -i_1 - i_3)(i_5, i_4, -i_5 - i_4),\\
&(i_0)(i_1)(i_3)(i_2, i_4, -i_2 - i_4), (i_6, i_5, -i_6 - i_5),\\
&(i_0)(i_1)(i_3)(i_2, i_5, -i_2 - i_5)(i_4, i_6, -i_4 - i_6).
\end{aligned}$$

Доказательство в общем случае проходит следующим образом. Прежде всего, ввиду транзитивности все сводится к случаю $i_0^\dagger = i_0$. Далее, $i_1^\dagger$ и $i_2^\dagger$ должны лежать в множестве $\{\pm i_n\}$, поскольку это единственные i-единицы, четно ортогональные к i_0. С помощью вышеуказанных симметрий можно свести $i_1^\dagger$ к i_1 (не трогая i_0) и $i_2^\dagger$ к i_2 (не трогая i_0 и i_1); отсюда теорема и следует. □

Вот непосредственное следствие.

Следствие. *Порядок группы* Aut(O) *равен* 12096.

Доказательство. Единица $i_0^\dagger$ может быть любой из 126 i-единиц. Если теперь $i_0^\dagger = i_0$, то $i_1^\dagger$ может быть любой из $\pm i_1, \ldots, \pm i_6$ (т. е. из двенадцати i-единиц, четно ортогональных к i_0), а если, кроме того, $i_1^\dagger = i_1$, то $i_2^\dagger$ может быть любой из $\pm i_2, \ldots, \pm i_5$ (т. е. из восьми i-единиц, четно ортогональных к i_0 и нечетно ортогональных к i_1). Стало быть, порядок равен

$$126 \times 12 \times 8 = 12096. \qquad \square$$

Теорема 4. *Группа* Aut(O) *транзитивна на:* (1) *четных кватернионных тройках;* (2) *нечетных кватернионных тройках;* (3) *ω-единицах.*

Доказательство. (1) Если $i \to i_0$ и $j \to i_1$, то $k \to i_3$.

(2) Если $i \to i_1$ и $j \to i_2$, то $k \to i_4$.

(3) Достаточно для каждого $\omega = \frac{1}{2}(-1 \pm i_a \pm i_b \pm i_c)$ найти четную кватернионную тройку i, j, k, для которой $\omega = \frac{1}{2}(-1 + i + j + k)$; в качестве таковой можно взять[1] $i = \pm i_a$, $j = i^\omega$, $k = j^\omega$. $\square$

Обычно граф, изображенный на рис. 10.1 и 10.2, называется *обобщенным шестиугольником*, но мы предпочитаем термин «гипершестиугольник». Обычный многоугольник — это связное множество вершин и ребер, в котором каждый объект одного вида инцидентен ровно двум объектам другого вида. Многоугольник называется *n-угольником*, если он содержит по n вершин и ребер, чередующихся друг с другом. Чтобы получить обобщенный n-угольник, надо в этом определении заменить 2 на другое число, в нашем случае 3. Вершины нашего обобщенного шестиугольника суть i-единицы с точностью до знака; его «гиперребра» суть кватернионные тройки i, j, k, составленные из таких i-единиц (опять-таки с точностью до знака).

§ 10.4. Кольца октавных единиц

Кольцом октавных единиц называется подкольцо в O^8, порожденное единицами. В приложении мы докажем следующий факт.

Теорема 5. *С точностью до изоморфизма существует ровно четыре типа целых колец, порожденных элементами нечетного порядка:* G^1,

[1] Не всегда можно положить i, j и k равными $\pm i_a$, $\pm i_b$, $\pm i_c$, поскольку это не обязательно кватернионная тройка. Если $\omega = \omega_{365}$, то рассуждение в тексте дает $i = i_3$, $j = i_{\bar{2}465}$, $k = i_{\bar{2}\bar{4}65}$.

E^2, H^4 и O^8. *При этом все кольца октавных единиц можно получить из этих колец с помощью диксоновского удвоения (см. рис. 10.3).*

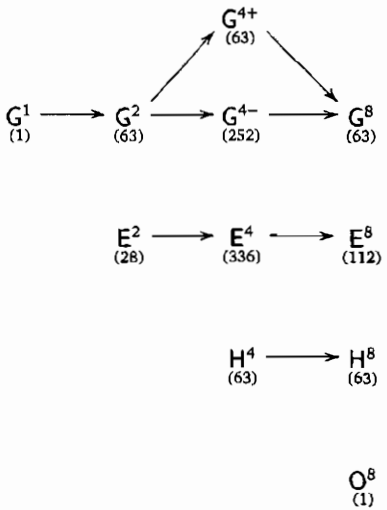


Рис. 10.3. Кольца единиц. Здесь G^1 — обычное кольцо целых чисел $\mathbb{Z}$, E^2 — кольцо эйзенштейновых целых $\mathbb{Z}[\omega]$, порожденное элементом ω, имеющим порядок 3 в O^8, H^4 — гурвицево кольцо $\mathbb{Z}[i, j, k, \frac{1}{2}(-1+i+j+k)]$; наконец, O^8 — все кольцо октавных целых. Стрелка $R^n \to R^{2n}$ означает, что R^{2n} является диксоновским удвоением (R^n, i) для некоторого i, ортогонального к R. Количество колец каждого типа приведено в скобках

Оказывается, что (за одним важным исключением) если два кольца единиц изоморфны как абстрактные кольца, то они связаны симметрией кольца O^8. Исключение состоит в том, что имеется две орбиты абстрактного типа $G^4 = \langle i, j, k\rangle$: орбита, содержащая G^{4+}, если i, j и k четно ортогональны, и G^{4-}, если i, j, k нечетно ортогональны.

Мы вкратце обсудим эти транзитивности в нетривиальных случаях, уделяя особое внимание орбитам, соответствующим максимальным подгруппам. Транзитивность на кольцах типа G^2 и G^8 следует из того, что они находятся во взаимно однозначном соответствии друг с другом[1] и с вершинами гипершестиугольника. Транзитивность на G^{4+},

[1]Если кольцо G^2 порождено некоторой единицей (i), то соответствующее G^8 порождено i-единицами, четно ортогональными к этой i.

H^4 и H^8 вытекает из того, что такие кольца находятся во взаимно однозначном соответствии друг с другом[1] и с «гиперребрами» гипершестиугольника.

Транзитивность на кольцах G^{4-} следует из транзитивности на нечетных кватернионных тройках. Однако же все автоморфизмы, оставляющие на месте тройку $\langle i_1, i_2, i_4\rangle$, оставляют[2] на месте и единицу $\pm i_0$, порождающую вместе с ними G^8; следовательно, эта подгруппа немаксимальна. Заодно мы описали четыре вложения G^{4-} в G^8; например, вышеупомянутое G^8 содержит

$$\langle i_1, i_2, i_4\rangle,\ \langle i_1, i_5, i_6\rangle,\ \langle i_2, i_3, i_5\rangle,\ \langle i_4, i_6, i_3\rangle.$$

Транзитивность на кольцах вида $E^2 = \mathbb{Z}[\omega]$ следует из транзитивности на ω-единицах. Поскольку кольцо типа E^4 или E^8 содержит единственное кольцо типа E^2 (порожденное его элементами нечетного порядка), его стабилизатор не является максимальной подгруппой. Доказательство транзитивности предоставляется заинтересовавшемуся читателю[3].

На рис. 10.4 указаны все включения между этими кольцами единиц (и еще кое-что). Подробнее это обсуждается в следующем параграфе. За двумя исключениями, всякая лупа, порожденная единицами, является лупой единиц одного из этих колец единиц. Исключениями являются тривиальная группа C_1 и группа C_3 порядка 3, порожденная ω. Благодаря тому, что они также присутствуют на рис. 10.4, оказывается, что на этом рисунке перечислены также все включения луп единиц. В главе 11 мы (с помощью рассуждений, использующих редукцию по модулю 2) найдем четыре подкольца K^1, K^2, K^4 и K^8, не являющиеся кольцами единиц; на рис. 10.4 присутствует кольцо K^8.

§ 10.5. Стабилизаторы колец единиц

Ниже мы приводим более подробную информацию. Стабилизаторы общих кватернионных подсистем Q^4, порожденных кватернионными тройками i, j, k, можно описать единым образом, рассматривая Q^8 как диксоновское удвоение $Q^4 + hQ^4$ (где h — «удваивающий» элемент) и

[1] Кольцу $G^{4+} = \langle i, j, k\rangle$ соответствует кольцо $H^4 = \langle i, j, k, \frac{1}{2}(-1+i+j+k)\rangle$, а соответствующее H^8 получается из H^4 присоединением всех ортогональных к нему i-единиц.

[2] Единственные i-единицы, четно ортогональные к i_1, i_2 и i_4, суть $\pm i_0$.

[3] Все 36 $\langle i\rangle$-подпространств, ортогональных к $\langle\omega\rangle$, распадаются на 12 троек. Присоединяя любую из этих троек, получаем E^4; чтобы получить E^8, надо добавить три подходящие тройки.

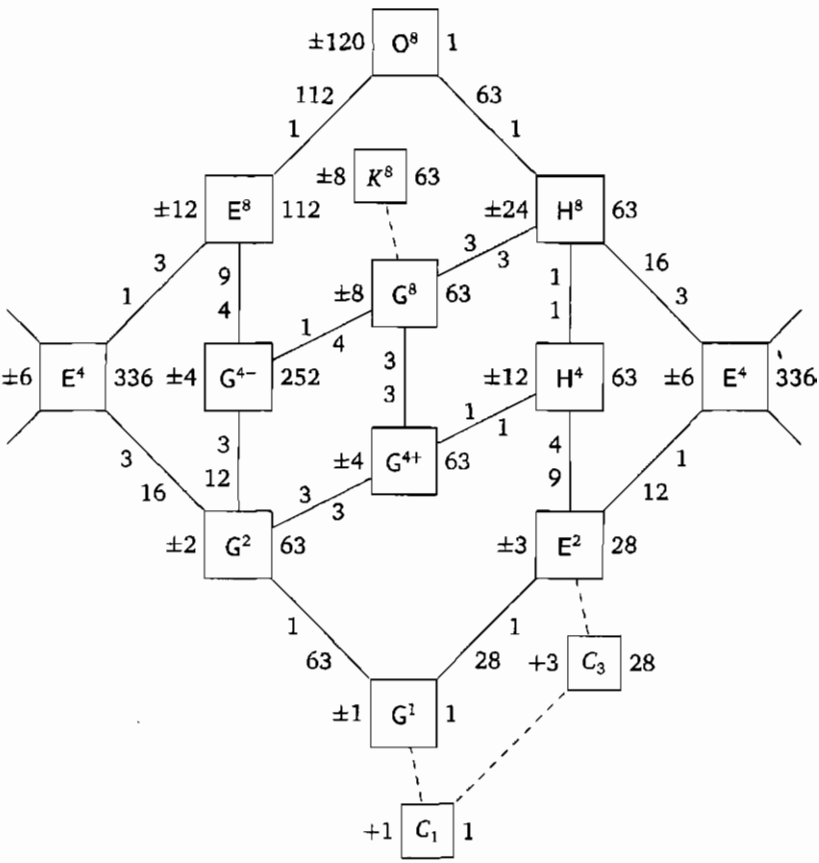


Рис. 10.4. Включения между некоторыми подобъектами в O^8. Если перед прямоугольником стоит $\pm n$, то это означает, что речь идет о кольце, в котором имеется n пар противоположных единиц. Если перед прямоугольником стоит $+n$, то это группа, состоящая из n единиц. Цифра n, стоящая после прямоугольника, означает, что имеется n таких объектов. Надписи на отрезках означают количество включений: например, каждое E^4 содержится в трех H^8, а каждое H^8 содержит 16 экземпляров E^4. Для удобства E^4 нарисовано и справа, и слева

пользуясь идеями из § 6.6 и обозначениями из главы 4. Рассматривать стабилизатор у G^{4+} нет нужды, поскольку стабилизатор этого кольца совпадает со стабилизатором единственного содержащего их H^4. Что же до остальных случаев, то Q^8 порождается Q^4 и единицами, ортогональными к Q^4, так что стабилизатор $\mathrm{Stab}(Q^4)$ содержится в стабилизаторе $\mathrm{Stab}(Q^8)$.

10.5.1. *Подкольцо* G^{4-}

Одно из таких колец порождено элементами $i = i_1$, $j = i_2$, $k = i_4$, для которых подходящее удвоение задается элементом $h = i_0$. В приводимой ниже таблице (в которой указаны только нижние индексы) описано действие образующих группы автоморфизмов на элементы базиса.

	i	j	k	h	hi	hj	hk
$[u,v]$	1	2	4	0	3	6	5
$[\omega,\omega]$	2	4	1	0	6	5	3
$[\zeta,\zeta]$	2	1	$\bar{4}$	0	6	3	$\bar{5}$
$[i,i]$	1	$\bar{2}$	$\bar{4}$	0	3	$\bar{6}$	$\bar{5}$
$[1,-1]$	1	2	4	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{5}$

$$\omega = \frac{-1+i+j+k}{2}$$

$$\zeta = \frac{i+j}{\sqrt{2}}$$

Это действительно образующие, поскольку первые три из них порождают все автоморфизмы кольца $\langle i_1, i_2, i_4\rangle$, так что про остальные образующие можно считать, что они оставляют на месте i_1, i_2 и i_4 и тем самым переводят i_0 в $\pm i_0$, поскольку это единственные i-единицы, четно ортогональные к i_1, i_2 и i_4.

В обозначениях главы 4 стабилизатор кольца G^{4-} есть

$$\pm\frac{1}{24}[O\times O],$$

поскольку в этой группе содержится $-1 = [1,-1]$, а автоморфизмы $[\omega,\omega]$, $[\zeta,\zeta]$ и $[i,i]$ задают тождественный изоморфизм между L и R, изоморфными бинарной группе октаэдра $2O = \langle\omega,\zeta,i\rangle$.

Всякий автоморфизм, сохраняющий G^8 (например, $\langle i_n\rangle$), должен сохранять кольцо G^2 (в данном случае это $\langle i_0\rangle$), порожденное его средним элементом, и обратное также верно, поскольку i-единицы, четно ортогональные к $\pm i_0$, суть прочие $\langle\pm i_n\rangle$. Всякое кольцо $G^{4-} = \langle i,j,k\rangle$

содержит единственное $\mathsf{G}^8 = \langle h, i, j, k\rangle$, получающееся присоединением h — среднего элемента тройки i, j, k. Например, $\mathsf{G}^{4-} = \langle i_1, i_2, i_4\rangle$ содержится в кольце $\mathsf{G}^8 = \langle i_n\rangle$, которое, в свою очередь, содержит ровно четыре кольца типа G^{4-}:

$$\langle i_1, i_2, i_4\rangle,\ \langle i_1, i_5, i_6\rangle,\ \langle i_2, i_3, i_5\rangle,\ \langle i_4, i_6, i_3\rangle.$$

Значит, $\mathrm{Stab}(\mathsf{G}^{4-})$ имеет индекс 4 в группе $\mathrm{Stab}(\mathsf{G}^8) = \mathrm{Stab}(\mathsf{G}^2 = \langle i_0\rangle)$.

10.5.2. *Подкольцо* H^4

В этом случае (например, при $i = i_0$, $j = i_1$, $k = i_3$) можно положить $h = i_6$ и получить следующие автоморфизмы:

	i	j	k	h	hi	hj	hk
$[u, v]$	0	1	3	6	2	5	4
$[\omega, 1]$	1	3	0	$\leftarrow$	6254*		$\rightarrow$
$[\zeta, \zeta]$	$\bar{0}$	3	1	6	$\bar{2}$	4	5
$[k, k]$	$\bar{0}$	$\bar{1}$	3	6	$\bar{2}$	$\bar{5}$	4
$[j, j]$	$\bar{0}$	1	$\bar{3}$	6	$\bar{2}$	5	$\bar{4}$
$[1, -1]$	0	1	3	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{4}$
$[1, i]$	0	1	3	2	$\bar{6}$	$\bar{4}$	5
$[1, j]$	0	1	3	5	4	$\bar{6}$	$\bar{2}$
$[i, k]$	0	1	3	4	$\bar{5}$	2	$\bar{6}$

$$\omega = \frac{-1 + i + j + k}{2}$$

$$\zeta = \frac{j + k}{\sqrt{2}}$$

Они порождают группу вида

$$\pm\tfrac{1}{2}[O \times \bar{D}_8],$$

так как имеется элемент $-1 = [1, -1]$, а единицы i, j, k и ζ порождают группу $2D_8$, которая при присоединении ω превращается в $2O$, причем «правое ядро» не является циклическим. Легко проверить, что это весь стабилизатор, причем эта группа индуцирует все автоморфизмы H^4.

Присоединяя ортогональные единицы, получаем кольцо H^8, стабилизатор которого тот же самый, так как H^4 восстанавливается по H^8 как подкольцо, порожденное элементами порядка 3.

10.5.3. *Подкольцо* E^4

С точностью до знака единицы кольца E^4 суть

$$1,\ \omega,\ \bar{\omega},\ i,\ i'=\omega i,\ i''=\bar{\omega}i,$$

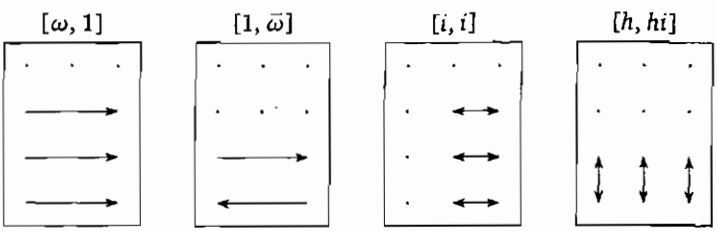
а ортогональные единицы суть

$$j,\ j'=\omega j,\ j''=\bar{\omega}j,\ k,\ k'=\omega k,\ k''=\bar{\omega}k,$$

где i, j и k — нечетная кватернионная тройка и $\omega=\frac{1}{2}(-1+h\sqrt{-3})$. Мы запишем все эти единицы в виде прямоугольной таблицы:

$$\begin{array}{|ccc|}\hline 1 & \omega & \bar{\omega} \\ i & i' & i'' \\ j & j' & j'' \\ k & k' & k'' \\ \hline\end{array}.$$

Имеются четыре автоморфизма, действующие так, как показано на рисунке,



и порождающие группу[1] вида

$$+\frac{1}{4}[D_{12}\times\bar{D}_{12}]$$

в обозначениях главы 4 (поскольку элемент $[1,-1]$ отсутствует и при этом как элементы u, так и элементы v порождают группы D_{12}, отображающиеся на D_4 при факторизации по $\langle\omega\rangle$, причем «циклический смежный класс» $\langle h\rangle$ меняется местами с нециклическим $\langle hi\rangle$). Тот факт, что это весь стабилизатор, вытекает из того, что первое отображение, как легко проверить, порождает стабилизатор E^4, а остальные три порождают все достижимые автоморфизмы E^4.

[1]Интересно отметить, что эта группа не упоминается в [41], поскольку ее эллиптический образ был пропущен в исходной классификации Гурса.

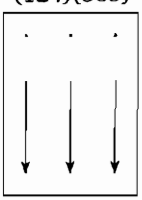
Присоединяя единицы, ортогональные к E^4, мы получаем E^8, стабилизатор которого в три раза больше, как видно из примера

∞	$\overline{\infty}365$	$\overline{\infty 365}$
1	$\overline{0165}$	$0\overline{1}6\overline{5}$
2	$\overline{0253}$	$0\overline{2}5\overline{3}$
4	$\overline{0435}$	$0\overline{4}3\overline{6}$

,

в котором этот автоморфизм имеет вид

(124)(365)



.

Приложение
Доказательство теоремы 5

Мы докажем следующее утверждение.

Теорема 5. *С точностью до изоморфизма существует ровно четыре типа целых колец, порожденных элементами нечетного порядка:* G^1, E^2, H^4 *и* O^8. *При этом все кольца октавных единиц можно получить из этих колец с помощью диксоновского удвоения (см. рис. 10.3).*

Лемма 2. *Всякое кольцо единиц можно получить с помощью диксоновского удвоения из кольца, порожденного* ω*-единицами.*

Доказательство. Пусть X — подкольцо, порожденное ω-единицами. Тогда, очевидно, всякая единица, не лежащая в X, должна быть i-единицей. Однако эта единица должна быть ортогональна ко всякой единице u, лежащей в X (а значит, и ко всему X), так как в противном случае $\pm ui$ будет ω-единицей, не лежащей в X. Следовательно, при ее присоединении к кольцу X получается его диксоновское удвоение (обозначим его Y). Заменяя X на Y и повторяя, если необходимо, это рассуждение, получаем доказательство леммы. □

С учетом леммы теорема сводится к следующей.

Теорема 6. *Существуют только четыре типа колец, порожденных* ω*-единицами, а именно* G^1, E^2, H^4, O^8.

Доказательство. Если кольцо порождено не более чем одним элементом, то очевидно, что это G^1 или E^2. Поскольку $\mathrm{Aut}(O^8)$ дважды

транзитивна на $\langle\omega\rangle$, кольцо, порожденное двумя не равными и не противоположными ω-единицами, опять-таки может иметь только тип H^4. Чтобы завершить доказательство, надо провести несложную проверку того, что если присоединить ω-единицу, не лежащую в H^4, к одному конкретному $\mathsf{H}^4 = \langle i_0, i_1, i_3, \omega_{013}\rangle$, то получится всё O^8. □

Редукция O по модулю 2

§ 11.1. Зачем редуцировать по модулю 2?

Группа $\mathrm{Aut}(\mathrm{O})$, состоящая из автоморфизмов кольца $\mathrm{O} = \mathrm{O}^8$, является почти что *простой*: у нее есть *простая подгруппа индекса* 2. Поскольку простые конечные группы расклассифицированы, встает вопрос, с какой именно простой группой мы имеем дело. Удобнее всего находить ответ с помощью редукции по модулю 2.

Интересные кольца получаются при редукции октавных целых по модулю любого простого числа p (точно так же, как при редукции обычных целых по модулю p получается интересное кольцо, а именно поле). Точное определение: два октавных целых сравнимы по модулю p, если их разность есть p, умноженное на некоторое октавное целое. (Таким образом, октавное целое по модулю p есть не что иное, как элемент кольца $\mathrm{O}/p\mathrm{O}$.)

Конечная группа $G_2(p)$ (более полное обозначение: $G_2(\mathbb{F}_p)$) есть по определению группа автоморфизмов кольца октав по модулю p. Поскольку такие группы не являются предметом нашей книги, мы просто сообщим, что порядок группы $G_2(p)$ равен $p^6(p^2-1)(p^6-1)$. Ясно, что всякий автоморфизм кольца O индуцирует, при редукции по модулю p, элемент группы $G_2(p)$. Отсюда получаем отображение

$$\mathrm{Aut}(\mathrm{O}) \to G_2(p),$$

являющееся на самом деле вложением, поскольку только тождественный автоморфизм кольца O индуцирует тождественный автоморфизм по модулю p. При $p = 2$ это даже изоморфизм, поскольку, ввиду вышеприведенной формулы, порядок группы $G_2(2)$ равен

$$2^6(2^2-1)(2^6-1) = 12096,$$

что совпадает с порядком $\mathrm{Aut}(\mathrm{O})$.

Итак, интересующая нас группа совпадает с $G_2(2)$. Хотя группа $G_2(p)$ обычно проста, при $p=2$ это не так: у нее есть простая подгруппа индекса 2, которая встречается в классификации в другом месте: это группа $U_3(3)$ «унитарных» (3×3)-матриц с элементами из поля порядка 9. Мы будем обозначать эту простую группу через $\mathcal{G}$, а наша $G_2(2)$ будет тогда группой $\mathcal{G}\cdot 2$.

Специалисты по теории групп знают, что лучший способ изучить конечную простую группу — найти ее максимальные подгруппы. В группе $\mathcal{G}$ имеется (с точностью до сопряжения) четыре максимальные подгруппы:

$\mathcal{G}_G$ — стабилизатор одного из 63 гауссовых подколец G^2;

$\mathcal{G}_H$ — стабилизатор одного из 63 гурвицевых подколец H^4;

$\mathcal{G}_E$ — стабилизатор одного из 28 эйзенштейновых подколец E^2;

$\mathcal{G}_K$ — стабилизатор одного из 36 клейновых подколец K^1.

Кроме четырех подгрупп $\mathcal{G}_G\cdot 2$, $\mathcal{G}_H\cdot 2$, $\mathcal{G}_E\cdot 2$ и $\mathcal{G}_K\cdot 2$ группа $\mathcal{G}\cdot 2$ содержит еще только одну максимальную подгруппу, а именно саму $\mathcal{G}$. Только три из этих подгрупп встречались нам в качестве стабилизаторов подколец октавных целых, но все четыре являются стабилизаторами подколец малой размерности в октавных целых по модулю 2.

Чтобы получить первые три группы, надо редуцировать по модулю 2 подкольца $\langle i_0\rangle$, $\langle i_0, i_1, i_3, \omega_{013}\rangle$ и $\langle\omega\rangle$. Четвертая является стабилизатором кольца, порожденного (по модулю 2) клейновым целым λ, имеющим вид $\frac{1}{2}(-1+\sqrt{-7})$. Оказывается, что, кроме того, она оставляет на месте два базиса: «j-репер» $1, j_0, \ldots, j_6$ и «k-репер» $1, k_0, \ldots, k_6$. В таблице 11.1 показано действие всех четырех групп на подалгебрах всех четырех видов.

§ 11.2. Решетка E_8 по модулю 2

При исследовании решетки октавных целых по модулю 2 нам будет важно знать количество октав с данной нормой. Как мы объясняли в главе 9, решетка октавных целых пропорциональна решетке корней E_8, в которой число векторов с данной нормой $n>0$ равно 240, помноженному на сумму кубов делителей числа n.

Поэтому существует в точности	240	2160	6720	...
октавных целых с нормой	1	2	3	...

Впрочем, реально нам нужно только количество *коротких векторов*, т. е. векторов, длина которых не превосходит 2. Чтобы наше из-

	Действие			
	$\mathcal{G}_G$	$\mathcal{G}_H$	$\mathcal{G}_E$	$\mathcal{G}_K$
на 63 кольцах G^2	1 +6 +24 +32 G^2 G^{4+} G^{4-} E^4	3 +12 +48 G^{4+} G^8 H^8	27 +36 H^4 E^4	14 +21 +28 K^2 K^4 E^4
на 63 кольцах H^4	3 +12 +48 G^{4+} G^8 H^8	1 +6 +24 +32 H^4 G^8 H^8 O^8	9 +54 H^4 H^8	21 +42 K^4 H^8
на 28 кольцах E^2	12 +16 H^4 E^4	4 +24 H^4 H^8	1 +27 E^2 H^4	28 E^4
на 36 кольцах K^1 mod 2	8 +12 +16 K^2 K^4 E^4	12 +24 K^4 H^8	36 E^4	1 +14 +21 K^1 K^2 K^4

Табл. 11.1. Под действием группы, сохраняющей подалгебру одного из типов, множество алгебр любого данного типа распадается на орбиты указанных порядков. Две данные алгебры порождают третью, тип которой указан под соответствующим числом

ложение было замкнутым, подсчитаем их непосредственно, исходя из того, какой вид они могут иметь.

$$\begin{array}{lccccc} \text{норма 1:} & (\pm 1^1, 0^7) & \text{и} & \left(\pm\frac{1}{2}^4, 0^4\right) & & \\ \text{количество:} & 2^1 \cdot 8 & + & 2^4 \cdot 14 & = & 240; \end{array}$$

$$\begin{array}{lccccccc} \text{норма 2:} & (\pm 1^2, 0^6) & \text{и} & \left(\pm\frac{1}{2}^4, \pm 1^1, 0^3\right) & \text{и} & \left(\pm\frac{1}{2}^8\right) & & \\ \text{количество:} & 2^2 \cdot 28 & + & 2^5 \cdot 14 \cdot 4 & + & 2^8 & = & 2160. \end{array}$$

Теперь рассмотрим сравнения по модулю 2 между этими короткими векторами.

Лемма 1. *Кроме сравнений $v \equiv -v$, единственные сравнения по модулю 2 между короткими векторами суть сравнения между ортогональными векторами с нормой 2.*

Доказательство. Пусть $v \equiv w$, причем $v \neq \pm w$. Заменив, если нужно, w на $-w$, можно считать, что скалярное произведение $(v, w]$ неотрицательно, так что для норм имеем неравенство

$$[v - w] \leqslant [v] + [w] \leqslant 4,$$

вытекающее из того, что v и w — короткие векторы (см. рис. 11.1). Однако из того, что $v - w \in 2O^8$, вытекает, что $[v - w] \geqslant 4$, так что $[v - w] = 4$, откуда $[v] = [w] = 2$ и $(v, w] = 0$. □

Поскольку в восьмимерном пространстве нельзя найти более восьми попарно ортогональных векторов, в качестве следствия получаем,

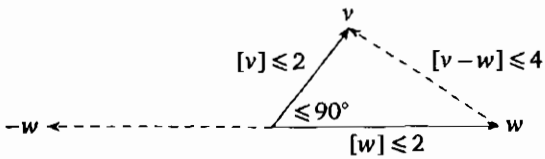


Рис. 11.1. Если $[v, w] \geqslant 0$, то $[v - w] \leqslant 4$

что в любом классе по модулю 2 существует не более шестнадцати векторов с нормой 2. Поэтому число классов, содержащих векторы с нормой 2, не меньше, чем

$$1 + \frac{240}{2} + \frac{2160}{16} = 1 + 120 + 135 = 256 = 2^8.$$

Поскольку $O^8/2O^8$ — восьмимерное пространство над полем из двух элементов, это число совпадает с общим числом классов, так что мы доказали следующий факт.

Теорема 1. *Всякий класс по модулю 2 содержит короткий вектор. Эти классы таковы: один класс, представленный нулевым вектором; 120 классов, каждый из которых представлен двумя векторами $\pm v$ с нормой 1; 135 классов, каждый из которых представлен репером из шестнадцати векторов $\pm v_1, \ldots, \pm v_8$ с нормой 2. В третьем случае векторы $v_1, \ldots, v_8$ попарно ортогональны, и всякий вектор с нормой 2 лежит в таком реперe.*

Начиная с этого момента мы будем называть такие классы векторами по модулю 2. Если сгруппировать их в соответствии с их мультипликативными свойствами, то получится вот что:

Норма	Тип	Всего
0	один элемент 0	1
1	один элемент ± 1, 63 элемента $\pm i$, 56 элементов $\pm\omega$	120
2	63 элемента $1+i$, 72 элемента λ	135
		$256 = 2^8$

Шестнадцать минимальных представителей вектора типа $1 + i$ — это 4 вектора $\pm 1 \pm i$ и 12 векторов вида $\pm i' \pm i''$. Например, для $1 + i_0$ имеем

$$\pm 1 \pm i_0,\ \pm i_1 \pm i_3,\ \pm i_2 \pm i_6,\ \pm i_4 \pm i_5.$$

С типом λ мы раньше не встречались. Его 16 минимальных представителей имеют вид $\frac{1}{2}(\pm 1 \pm \sqrt{-7})$ для различных октавных квадратных корней из -7. Группа $G_2(2)$ действует транзитивно на 72 элементах λ, но имеется только 36 алгебр $\langle\lambda\rangle$ (mod 2), поскольку алгебра,

порожденная одним таким элементом λ, содержит и второй, а именно $\mu \equiv 1 + \lambda$. Стандартный случай таков:

$$\lambda = i_{\infty 0123456} = \frac{-1 + i_0 + \ldots + i_6}{2}$$

и

$$\mu = i_{\infty 0123456} = \frac{1 + i_0 + \ldots + i_6}{2};$$

16 минимальных представителей элемента μ суть

$$\pm i_{\infty 0123456},\ \pm i_{\infty 01\widetilde{23}\widetilde{456}}$$

и еще 6 аналогичных. Всякий вектор, получаемый сложением ω-единицы с ортогональной к ней i-единицей, есть вектор типа λ, и обратно, всякий вектор типа λ представим в таком виде (многими способами).

Пара λ, μ задает пару координатных реперов $1, j_0, \ldots, j_6$ и $1, k_0, \ldots, k_6$ (и однозначно определяется по этой паре). Элементы j_n и k_m находятся из сравнений

$$j_n\mu \equiv \mu \equiv \mu k_m \quad \text{и} \quad \lambda j_n \equiv \lambda \equiv k_m\lambda$$

и обратно, μ находится из этих сравнений с использованием того факта, что 28 ненулевых значений (по модулю 2), которые принимают 49 произведений $(1 + j_m)(1 + k_n)$, сравнимы с μ.

Эти два базиса переставляются элементом δ, меняющим местами j_m и k_{-m}; его добавление увеличивает порядок группы со 168 до 336. Можно рассматривать k_m как точки на проективной плоскости, а j_n — как прямые (см. рис. 11.2). В свете этого новая группа — расширение группы $L_3(2)$ автоморфизмов этой проективной плоскости с помощью проективной двойственности; эту последнюю группу можно рассматривать как $PGL_2(7)$. Это четвертая максимальная подгруппа в группе $\mathcal{G} \cdot 2$; мы посвятим ей следующий параграф.

§ 11.3. О стабилизаторе $\langle\lambda\rangle$

Будем называть (координатным) *репером* набор из 16 векторов вида $\pm 1, \pm v_0, \pm v_1, \ldots, \pm v_6$, где $1, v_0, v_1, \ldots, v_6$ — попарно ортогональные единицы в O^8. Подобно кватернионным тройкам, реперы тоже могут быть четными и нечетными. *Четный репер* — это репер, содержащий четную кватернионную тройку; в *нечетном репере* все кватернионные тройки нечетны.

Лемма 2. *Всякие две нечетно ортогональные i-единицы принадлежат ровно трем реперам, из которых один четен и два нечетны.*

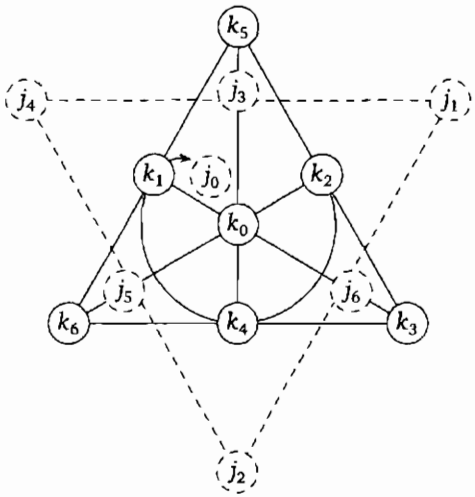


Рис. 11.2. Можно рассматривать k_m как точки проективной плоскости над $\mathbb{F}_2$, а j_n — как прямые (и обратно)

Доказательство. Можно считать, что две единицы — это i_3 и i_5. В обозначениях главы 10 список всех i-единиц, ортогональных к ним, выглядит так:

$$\pm i_6,\ \pm i_0,\ \pm i_1,\ \pm i_2,\ \pm i_4,\ i^*_{0124};$$

из этих векторов можно выбрать только реперы, содержащие ± 1, $\pm i_3$, $\pm i_5$, $\pm i_6$ вкупе с:

$$\underset{(i\text{-репер}),}{\pm i_0,\ \pm i_1,\ \pm i_2,\ \pm i_4} \quad \text{или} \quad \underset{(j\text{-репер}),}{i'_{0124}} \quad \text{или} \quad \underset{(k\text{-репер}).}{i''_{0124}}$$

Поскольку тройка i_0, i_1, i_3 четная, получаем, что i-репер четен. Приводимые ниже вычисления показывают, что j-репер нечетен, а тогда таков же и k-репер, поскольку симметрия, меняющая знаки у i_0, i_3, i_5 и i_6, переставляет j-реперы с k-реперами. □

11.3.1. *Вычисления*

Легче всего увидеть симметрии j-репера, выразив через него все октавные единицы. Положим

$$j_3 = -i_6, \quad j_6 = -i_5, \quad j_5 = -i_3, \quad j_0 = i_{\bar{0}124},$$
$$j_1 = i_{0\bar{1}24}, \quad j_2 = i_{01\bar{2}4}, \quad j_4 = i_{012\bar{4}}.$$

Это преобразование легко обратить: имеем

$$i_3=-j_5,\quad i_6=-j_3,\quad i_5=-j_6,\quad i_0=j_{\bar 0124},$$
$$i_1=j_{0\bar 124},\quad i_2=j_{01\bar 24},\quad i_4=j_{012\bar 4}$$

(тут полезно заметить, что $j_0+j_1=i_2+i_4$, $j_0-j_1=i_1-i_0$ и т. п.).

Теперь легко получаем, что

$$j_0j_1=j_{23\bar 46},\quad j_1j_2=j_{34\bar 50},\quad \ldots,\quad j_6j_0=j_{12\bar 35};$$

эти соотношения замечательным образом инвариантны относительно отображений

$$\alpha:(01\ldots6)\quad\text{и}\quad\beta:(124)(365).$$

Теперь легко заполнить таблицу умножения j_m, пользуясь инвариантностью относительно α и β и тем обстоятельством, что $j_n^2=-1$ и $j_nj_m=\overline{j_mj_n}$:

1	j_0	j_1	j_2	j_3	j_4	j_5	j_6
j_0	-1	$j_{2\bar 463}$	$j_{4\bar 156}$	$j_{\overline{4\bar 156}}$	$j_{1\bar 235}$	$j_{\overline{2\bar 463}}$	$j_{\overline{1\bar 235}}$
j_1	$j_{\overline{23\bar 46}}$	-1	$j_{3\bar 504}$	$j_{5\bar 260}$	$j_{\overline{5\bar 260}}$	$j_{2\bar 346}$	$j_{\overline{3\bar 504}}$
j_2	$j_{\overline{4\bar 615}}$	$j_{\overline{3\bar 450}}$	-1	$j_{4\bar 615}$	$j_{6\bar 301}$	$j_{\overline{6\bar 301}}$	$j_{3\bar 450}$
j_3	$j_{4\bar 561}$	$j_{\overline{5\bar 026}}$	$j_{\overline{4\bar 561}}$	-1	$j_{5\bar 026}$	$j_{\overline{0\bar 412}}$	$j_{\overline{0\bar 412}}$
j_4	$j_{\overline{1\bar 523}}$	$j_{5\bar 602}$	$j_{\overline{6\bar 130}}$	$j_{\overline{5\bar 602}}$	-1	$j_{6\bar 130}$	$j_{1\bar 523}$
j_5	$j_{2\bar 634}$	$j_{\overline{2\bar 634}}$	$j_{6\bar 013}$	$j_{\overline{0\bar 241}}$	$j_{\overline{6\bar 013}}$	-1	$j_{0\bar 241}$
j_6	$j_{1\bar 352}$	$j_{3\bar 045}$	$j_{\overline{3\bar 045}}$	$j_{0\bar 124}$	$j_{\overline{1\bar 352}}$	$j_{\overline{0\bar 124}}$	-1

Оказывается, что всякая симметрия, сохраняющая j-репер, сохраняет и ассоциированный k-репер. Именно, положим

$$k_0=j_{\overline{0\bar 124}}=-i_0,$$
$$k_1=j_{\overline{1\bar 235}}=i_{\bar 1263},$$
$$k_2=j_{\overline{2\bar 346}}=i_{\bar 2456},$$
$$k_3=j_{\overline{3\bar 450}}=i_{\overline{1\bar 263}},$$
$$k_4=j_{\overline{4\bar 561}}=i_{\bar 4135},$$
$$k_5=j_{\overline{5\bar 602}}=i_{\overline{4\bar 135}},$$
$$k_6=j_{\overline{6\bar 013}}=i_{\overline{2\bar 456}}$$

и заметим, что эти элементы инвариантны относительно α и β. Затем подсчитаем произведения

$$k_0k_1=-i_0i_{1\bar 263}=i_{3\bar 621}=j_{04\bar 53}\quad\text{и}\quad j_6k_0=i_{\bar 5}i_{\bar 0}=i_4=j_{012\bar 4};$$

пользуясь α- и β-симметриями, получаем отсюда таблицы 11.2 и 11.3.

1	j_0	j_1	j_2	j_3	j_4	j_5	j_6
j_0	-1	i_{52}	i_{34}	$-i_{24}$	i_{61}	$-i_{12}$	$-i_{41}$
j_1	$-i_{52}$	-1	i_{63}	i_{45}	$-i_{35}$	i_{02}	$-i_{23}$
j_2	$-i_{34}$	$-i_{63}$	-1	i_{04}	i_{56}	$-i_{46}$	i_{13}
j_3	i_{24}	$-i_{45}$	$-i_{04}$	-1	i_{15}	i_{60}	$-i_{50}$
j_4	$-i_{61}$	i_{35}	$-i_{56}$	$-i_{15}$	-1	i_{26}	i_{01}
j_5	i_{12}	$-i_{02}$	i_{46}	$-i_{60}$	$-i_{26}$	-1	i_{30}
j_6	i_{41}	i_{23}	$-i_{13}$	i_{50}	$-i_{01}$	$-i_{30}$	-1

1	k_0	k_1	k_2	k_3	k_4	k_5	k_6
k_0	-1	i_{63}	i_{56}	$-i_{61}$	i_{35}	$-i_{34}$	$-i_{52}$
k_1	$-i_{63}$	-1	i_{04}	i_{60}	$-i_{02}$	i_{46}	$-i_{45}$
k_2	$-i_{56}$	$-i_{04}$	-1	i_{15}	i_{01}	$-i_{13}$	i_{50}
k_3	i_{61}	$-i_{60}$	$-i_{15}$	-1	i_{26}	i_{12}	$-i_{24}$
k_4	$-i_{35}$	i_{02}	$-i_{01}$	$-i_{26}$	-1	i_{30}	i_{23}
k_5	i_{34}	$-i_{46}$	i_{13}	$-i_{12}$	$-i_{30}$	-1	i_{41}
k_6	i_{52}	i_{45}	$-i_{50}$	i_{24}	$-i_{23}$	$-i_{41}$	-1

1	k_0	k_1	k_2	k_3	k_4	k_5	k_6
j_0	ω_{00}	i_{01}	i_{02}	$-\omega_{03}$	i_{04}	$-\omega_{05}$	$-\omega_{06}$
j_1	$-\omega_{10}$	ω_{11}	i_{12}	i_{13}	$-\omega_{14}$	i_{15}	$-\omega_{16}$
j_2	$-\omega_{20}$	$-\omega_{21}$	ω_{22}	i_{23}	i_{24}	$-\omega_{25}$	i_{26}
j_3	i_{30}	$-\omega_{31}$	$-\omega_{32}$	ω_{33}	i_{34}	i_{35}	$-\omega_{36}$
j_4	$-\omega_{40}$	i_{41}	$-\omega_{42}$	$-\omega_{43}$	ω_{44}	i_{45}	i_{46}
j_5	i_{50}	$-\omega_{51}$	i_{52}	$-\omega_{53}$	$-\omega_{54}$	ω_{55}	i_{56}
j_6	i_{60}	i_{61}	$-\omega_{62}$	i_{63}	$-\omega_{64}$	$-\omega_{65}$	ω_{66}

Табл. 11.2. Таблицы умножения для j_n и k_m. По поводу определений см. таблицу 11.3

$abcd$	$j_{\bar{a}bcd}$	$j_{a\bar{b}cd}$	$j_{ab\bar{c}d}$	$j_{abc\bar{d}}$	j_{abcd}	$j_{\bar{a}\bar{b}cd}$	$j_{\bar{a}b\bar{c}d}$	$j_{\bar{a}bc\bar{d}}$
0124	$-k_0$	i_{50}	i_{30}	i_{60}	h_{00}	$-h_{10}$	$-h_{21}$	$-h_{40}$
1235	$-k_1$	i_{61}	i_{41}	i_{01}	h_{11}	$-h_{21}$	$-h_{32}$	$-h_{51}$
2346	$-k_2$	i_{02}	i_{52}	i_{12}	h_{22}	$-h_{32}$	$-h_{43}$	$-h_{62}$
3450	$-k_3$	i_{13}	i_{63}	i_{23}	h_{33}	$-h_{43}$	$-h_{54}$	$-h_{03}$
4561	$-k_4$	i_{24}	i_{04}	i_{34}	h_{44}	$-h_{54}$	$-h_{65}$	$-h_{14}$
5602	$-k_5$	i_{35}	i_{15}	i_{45}	h_{55}	$-h_{65}$	$-h_{06}$	$-h_{25}$
6013	$-k_6$	i_{46}	i_{26}	i_{56}	h_{66}	$-h_{06}$	$-h_{10}$	$-h_{36}$
∞653	ω_{00}	$-\omega_{20}$	$-\omega_{40}$	$-\omega_{10}$	$-\bar{\omega}_{00}$	$\bar{\omega}_{20}$	$\bar{\omega}_{40}$	$\bar{\omega}_{10}$
∞064	ω_{11}	$-\omega_{31}$	$-\omega_{51}$	$-\omega_{21}$	$-\bar{\omega}_{11}$	$\bar{\omega}_{31}$	$\bar{\omega}_{51}$	$\bar{\omega}_{21}$
∞105	ω_{22}	$-\omega_{42}$	$-\omega_{62}$	$-\omega_{32}$	$-\bar{\omega}_{22}$	$\bar{\omega}_{42}$	$\bar{\omega}_{62}$	$\bar{\omega}_{32}$
∞216	ω_{33}	$-\omega_{53}$	$-\omega_{03}$	$-\omega_{43}$	$-\bar{\omega}_{33}$	$\bar{\omega}_{53}$	$\bar{\omega}_{03}$	$\bar{\omega}_{43}$
∞320	ω_{44}	$-\omega_{64}$	$-\omega_{14}$	$-\omega_{54}$	$-\bar{\omega}_{44}$	$\bar{\omega}_{64}$	$\bar{\omega}_{14}$	$\bar{\omega}_{54}$
∞431	ω_{55}	$-\omega_{05}$	$-\omega_{25}$	$-\omega_{65}$	$-\bar{\omega}_{55}$	$\bar{\omega}_{05}$	$\bar{\omega}_{25}$	$\bar{\omega}_{65}$
∞542	ω_{66}	$-\omega_{16}$	$-\omega_{36}$	$-\omega_{06}$	$-\bar{\omega}_{66}$	$\bar{\omega}_{16}$	$\bar{\omega}_{36}$	$\bar{\omega}_{06}$

$$
\begin{aligned}
h_{mm} &= j_m + k_m, \quad m = m & \qquad \omega_{mn} &= -j_m k_n, \quad m > n \\
h_{mn} &= j_m - k_n, \quad m > n & \qquad \omega_{mn} &= \pm j_m k_n, \quad m \geqslant n \\
i_{mn} &= j_m k_n, \quad m < n & \qquad h_{mn} &= j_m \pm k_n, \quad m \geqslant n \\
\omega_{mm} &= j_m k_m, \quad m = m & \qquad i_{mn} &= j_m k_n, \quad m < n
\end{aligned}
$$

Табл. 11.3. Как и в таблице 11.2, мы полагаем $j_m k_n = i_{mn}$, если это произведение является i-единицей; в противном случае $j_m k_m = \omega_{mm}$, $j_m + k_m = h_{mm}$, $j_m k_n = -\omega_{mn}$, $j_m - k_n = h_{mn}$. Обозначения выбраны таким образом, чтобы они были инвариантны по модулю 2 относительно $L_3(2)$

Оказывается, что нечетные реперы можно разделить на два класса: *j-реперы* и *k-реперы*. Автоморфизм либо переводит в себя каждый из этих классов (тогда мы называем этот автоморфизм четным), либо меняет их местами (такие автоморфизмы назовем нечетными).

Симметрии, переводящие в себя данный j-репер, образуют простую группу порядка 168, известную под именем $L_3(2)$ или $L_2(7)$, и, кроме того, они переводят в себя некоторый конкретный k-репер, называемый ассоциированным k-репером. Для стандартной пары ассоциированных реперов эта группа порождена отображениями α, β и γ, действующими так:

$$\left.\begin{matrix}\alpha: & (01\ldots6)\\ \beta: & (124)(365)\end{matrix}\right\} \quad \text{на } j\text{- и } k\text{-индексах;}$$

$$\gamma: \begin{matrix}(56)(14)\varepsilon_{0124} & \text{на } j\text{-индексах;}\\ (12)(36)\varepsilon_{0365} & \text{на } k\text{-индексах.}\end{matrix}$$

Действие группы $\mathscr{G}_K \simeq L_3(2)\cdot 2$ на различных объектах легко усмотреть из таблицы 11.3, в которой указано представление в j-репере для всех 240 единиц ($j_{abcd} = \frac{1}{2}(j_a + j_b + j_c + j_d)$).

§ 11.4. Остальные подкольца по модулю 2

Этот параграф посвящен доказательству того факта, что, с точностью до симметрий, единственные подкольца по модулю 2 в O^8 суть редукции колец единиц по модулю 2 полюс четыре кольца

$$K^1 = \langle\lambda\rangle, \quad K^2 = \langle\lambda, i_0\rangle, \quad K^4 = \langle\lambda, i_0, i_1, i_3\rangle, \quad K^8 = \langle\lambda, i_0, \ldots, i_6\rangle,$$

где $\lambda = \frac{1}{2}(-1 + i_0 + \ldots + i_6)$.

Лемма 3. *Кольцо $\langle\lambda_1, \lambda_2\rangle$, порожденное двумя элементами λ (для которых $\langle\lambda_1\rangle \neq \langle\lambda_2\rangle$), порождено также λ_1 и некоторой i-единицей.*

Доказательство. Мы можем считать, что $\lambda_1 = \left(+\frac{1}{2}^8\right)$, а λ_2 имеет координаты

$$\left(\pm\frac{1}{2}^8\right) \quad \text{или} \quad \left(\pm\frac{1}{2}^4, \pm 1, 0^3\right).$$

В первом случае вектор не меняется по модулю 2, если поменять знаки у любой четверки; поэтому можно считать, что число знаков «−» не превосходит двух, и если их ровно два, то один из них стоит при 1, так что $\lambda_1 - \lambda_2$ имеет вид i или $i+1$. По аналогичным причинам можно считать, что во втором случае имеется не более одного минуса и что

если он есть, то он стоит при $\frac{1}{2}$, так что $\lambda_1 - \lambda_2$ имеет координаты

$$\left(0^4, \pm\tfrac{1}{2}^4\right) \quad \text{или} \quad \left(0^3, 1, \pm\tfrac{1}{2}^4\right)$$

(в зависимости от того, равен коэффициент при 1 нулю или единице). В первом случае разность является i-единицей, а во втором имеет вид либо $1+i$, либо $i+i'$ (что сравнимо с $1+i$ по модулю 2). □

Лемма 4. *Кольцо, порожденное λ и ω-единицей, является кольцом единиц.*

Доказательство. Можно положить

$$\lambda = \left(\pm\tfrac{1}{2}^8\right), \quad \omega = \left(\pm\tfrac{1}{2}^4, 0^4\right),$$

а выбрав подходящего представителя для λ, можно изменить знаки таким образом, чтобы $\lambda - \omega$ имело вид

$$\left(0^4, \pm\tfrac{1}{2}^4\right) \quad \text{или} \quad \left(0^3, \pm 1, \pm\tfrac{1}{2}^4\right),$$

что равно i или $1+i$. Стало быть, $\langle \lambda, \omega \rangle = \langle \omega, i \rangle$ для этого i. □

Объединяя эти две леммы, получаем такой результат.

Теорема 2. *По модулю 2 всякое кольцо, не порожденное единицами, есть кольцо одного из типов K^1, K^2, K^4 или K^8.*

Доказательство. По модулю 2 всякая неединица сравнима с λ или $1+i$, так что можно считать, что все образующие, не являющиеся единицами, имеют вид λ; ввиду леммы 3 можно считать, что такая образующая только одна, а ввиду леммы 4 — что среди образующих нет ω-единиц. Следовательно, часть кольца, порожденная единицами, состоит из 1 и каких-то попарно ортогональных i-единиц.

Теперь можно, не теряя общности, предположить, что одна из наших образующих — это выписанное выше λ. Глядя на правый верхний элемент в таблице 11.1, устанавливаем, что стабилизатор этого λ имеет три орбиты на i-единицах; две из них дают K^2 и K^4, а третья нас не интересует, поскольку она соответствует кольцу E^4, содержащему ω-единицу. Стало быть, можно считать, что всякое не рассмотренное ранее кольцо содержит это λ, элементы 1, i_0, i_1 и i_3, а также четыре i-единицы, ортогональные данным. Эти четыре единицы могут быть либо i_2, i_4, i_5 и i_6, и в этом случае получается K^8, либо i'_{2645} или i''_{2645}, что сводится к предыдущему с помощью симметрий. □

Октавная проективная плоскость $\mathbb{O}P^2$

Эта книга была посвящена «внутренней» теории кватернионов и октав. В число наших основных целей входило представить простое и замкнутое изложение свойств этих алгебр, наиболее естественных арифметик в них и приложений кватернионов и октав к геометрии пространств, которые их содержат. По поводу многочисленных приложений к другим разделам математики и физики мы отсылаем к работам, перечисленным в списке литературы — с надеждой, что наша книга поможет вам в их изучении.

В этой заключительной главе мы вкратце опишем некоторые «внешние» приложения октав.

§ 12.1. Исключительные группы Ли и «магический квадрат» Фрейденталя

Знаменитая классификация компактных полупростых групп Ли (т. е. непрерывных) над вещественными и комплексными[1] числами включает в себя как бесконечные серии (A_n, B_n, C_n и D_n в обозначениях Картана), включающие в себя унитарные, ортогональные и симплектические группы, так и пять «исключительных» групп G_2, F_4, E_6, E_7 и E_8. При этом выяснилось, что исключительные группы тесно связаны с октавами: например, мы видели, что G_2 — группа автоморфизмов октав.

Когда Йордан, фон Нейман и Вигнер в 1934 году расклассифицировали «йордановы алгебры»[2], они нашли «исключительную» алгебру,

---

[1] В комплексном случае речь, конечно, идет о полупростых группах. — *Прим. перев.*

[2] Такие алгебры задаются условиями $a \circ b = b \circ a$ и $a \circ (b \circ a^2) = (a \circ b) \circ a^2$; эти условия выполнены для матриц над ассоциативным кольцом, если положить $A \circ B = \frac{1}{2}(AB + BA)$. Исключительная йорданова алгебра — единственная, которую нельзя получить из ассоциативного кольца.

состоящую из «эрмитовых» (3×3)-матриц над октавами; ее группа автоморфизмов есть F_4.

В 1950-х годах Фрейденталь обнаружил, что над $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ и $\mathbb{O}$ можно определить четыре «геометрии»: эллиптическую и проективную плоскости, пятимерную симплектическую геометрию (они были к тому моменту известны) и найденную им новую «метасимплектическую» геометрию. Автоморфизмы четырех геометрий над четырьмя кольцами образуют знаменитый «магический квадрат» (см. [17] и [18]):

	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{H}$	$\mathbb{O}$
эллиптическая плоскость	B_1	A_2	C_3	F_4
проективная плоскость	A_2	A_2+A_2	A_5	E_6
5-мерная симплектическая геометрия	C_3	A_5	D_6	E_7
метасимплектическая геометрия	F_4	E_6	E_7	E_8

Свойства этих геометрий изучались Ж. Титсом совместно с Фрейденталем.

§ 12.2. Октавная проективная плоскость

Обычное определение *n-мерного проективного пространства* над полем состоит в том, что точки этого пространства суть одномерные подпространства в $(n+1)$-мерном векторном пространстве над полем; тем самым эти точки задаются ненулевыми наборами из $n+1$ элемента $(x_0, x_1, \ldots, x_n)$, причем подразумевается, что для всех $\lambda \neq 0$ координаты $(\lambda x_0, \lambda x_1, \ldots, \lambda x_n)$ представляют одну и ту же точку. При этом k-мерные подпространства в проективном пространстве суть $(k+1)$-мерные подпространства в векторном пространстве, так что, например, типичная гиперплоскость состоит из всех точек $(x_0, x_1, \ldots, x_n)$, удовлетворяющих некоторому линейному уравнению на координаты x_i.

В частности, точки двумерного комплексного проективного пространства параметризуются ненулевыми тройками комплексных чисел (x_0, x_1, x_2), причем подразумевается, что $(\lambda x_0, \lambda x_1, \lambda x_2) = (x_0, x_1, x_2)$ при $\lambda \neq 0$ и что прямые задаются линейными уравнениями на x_0, x_1 и x_2. Если в трехмерном комплексном векторном пространстве задать эрмитово скалярное произведение с помощью обычной эрмитовой формы $\bar{x}_0 x_0 + \bar{x}_1 x_1 + \bar{x}_2 x_2$, то типичная прямая задается уравнением $x_0\bar{y}_0 + x_1\bar{y}_1 + x_2\bar{y}_2 = 0$, т. е. как множество точек (x_0, x_1, x_2), ортогональных к данной точке (y_0, y_1, y_2).

Та же конструкция проходит и для кватернионов, но не для октав. У нее, однако, есть альтернатива, основанная на некоторых идеях из физики, с помощью которой все-таки удается определить двумерное проективное пространство, или проективную плоскость, над $\mathbb{O}$.

Давайте представлять себе точку p комплексной проективной плоскости как оператор проектирования на соответствующее одномерное подпространство в $\mathbb{C}^3$. При $p=(1,0,0)$ это оператор с матрицей

$$e=\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}.$$

В общем случае мы будем требовать, чтобы матрица была *эрмитовой* ($e_{ij}=\bar{e}_{ji}$), *идемпотентной* ($e^2=e$) и *с единичным следом* ($e_{00}+e_{11}+e_{22}=1$). Два одномерных подпространства в $\mathbb{C}^3$ ортогональны тогда и только тогда, когда соответствующие проекторы e и f удовлетворяют условию $e\circ f=0$, где через $e\circ f$ обозначено *йорданово произведение* $\frac{1}{2}(ef+fe)$. Мы определим прямую f на комплексной проективной плоскости как множество точек e, для которых $e\circ f=0$.

Это определение на самом деле обобщается на проективные пространства любой размерности над $\mathbb{R}$, $\mathbb{C}$ и $\mathbb{H}$. Над октавами $\mathbb{O}$, однако же, получается только проективная плоскость, но не пространство более высокой размерности, поскольку для конструкции необходимо, чтобы матрицы образовывали йорданову алгебру. Итак, мы определяем *октавную проективную плоскость* так: ее точки и прямые суть идемпотентные эрмитовы (3×3)-матрицы со следом единица над октавами, причем точка e лежит на прямой f тогда и только тогда, когда $e\circ f=0$.

С математической точки зрения это определение является наиболее удовлетворительным, поскольку из него явствует, что у плоскости имеются по крайней мере все симметрии исключительной йордановой алгебры (эти автоморфизмы образуют группу Ли типа F_4). На самом деле автоморфизмов у плоскости еще больше; именно, они образуют группу Ли E_6, содержащую F_4. Тем не менее работать с таким определением неудобно, так что в следующем параграфе мы докажем эквивалентность этого определения «координатному определению» (принадлежащему Портеусу [35] и Аслаксену [4]), которое менее симметрично, но более привычно и более удобно. Наше обсуждение эквивалентности этого определения фрейденталевскому следует изящной статье Оллкока [2].

§ 12.3. Координаты на $\mathbb{O}P^2$

Благодаря нашей первой лемме мы сможем заменить матрицы на векторы, составленные из октав.

Лемма 1. *Всякую идемпотентную эрмитову* (3×3)*-матрицу со следом единица можно записать в виде* $e_{x_0,x_1,x_2}=(\bar{x}_i x_j)$*, где* (x_0,x_1,x_2) *— вектор с единичной нормой и* x_0 *вещественно.*

Доказательство. Если

$$e=\begin{pmatrix} a & \gamma & \bar{\beta} \\ \bar{\gamma} & b & \alpha \\ \beta & \bar{\alpha} & c \end{pmatrix} \quad \text{и} \quad a+b+c=1,$$

где $a,b,c\in\mathbb{R}$ и $\alpha,\beta,\gamma\in\mathbb{O}$, то условие $e^2=e$ равносильно шести равенствам:

$$\begin{aligned} a&=a^2+[\beta]+[\gamma], & \bar{\gamma}\bar{\beta}&=(1-b-c)\alpha=a\alpha,\\ b&=b^2+[\gamma]+[\alpha] & \bar{\alpha}\bar{\gamma}&=(1-c-a)\beta=b\beta,\\ c&=c^2+[\alpha]+[\beta], & \bar{\beta}\bar{\alpha}&=(1-a-b)\gamma=c\gamma. \end{aligned}$$

Из трех равенств в левом столбце следует, что $a,\ b,\ c\geqslant 0$, а из трех равенств в правом столбце — что

$$[\beta][\gamma]=a^2[\alpha],\quad [\gamma][\alpha]=b^2[\beta],\quad [\alpha][\beta]=c^2[\gamma],$$

так что $[\gamma]=ab$ и $[\beta]=ac$, если $[\alpha][\beta][\gamma]\neq 0$. Если теперь положить

$$\begin{aligned} (x_0,x_1,x_2)&=\left(\sqrt{a},\frac{\gamma}{\sqrt{a}},\frac{\bar{\beta}}{\sqrt{a}}\right), && \text{если } a\neq 0,\\ (x_0,x_1,x_2)&=\left(0,\sqrt{b},\frac{\alpha}{\sqrt{b}}\right), && \text{если } a=0,\ b\neq 0,\\ (x_0,x_1,x_2)&=(0,0,1) && \text{иначе,} \end{aligned}$$

то легко видеть, что (x_0,x_1,x_2) — искомый вектор. □

Разумеется, мы с тем же успехом могли потребовать, чтобы вещественным был x_1 или x_2. Переход в обратную сторону несложен.

Лемма 2. *Если* $(x_0,x_1,x_2)=(r_0,r_1u_1,r_2u_2)$*, где* $r_i\in\mathbb{R}$*, а* u_i *— единичные октавы, то* $e_{x_0,x_1,x_2}=e_{\bar{u}_1x_0,r_1,\bar{u}_1x_2}$.

Доказательство. «Матрицы скалярных произведений»

	r_0	r_1u_1	r_2u_2
r_0	r_0^2	$r_0r_1u_1$	$r_0r_2u_2$
$r_1\bar{u}_1$	$r_0r_1\bar{u}_1$	r_1^2	$r_1r_2\bar{u}_1u_2$
$r_2\bar{u}_2$	$r_0r_2\bar{u}_2$	$r_1r_2\bar{u}_2u_1$	r_2^2

и

	$r_0\bar{u}_1$	r_1	$r_2\bar{u}_1u_2$
$r_0\bar{u}_1$	r_0^2	$r_0r_1u_1$	$r_0r_2u_2$
r_1	$r_0r_1\bar{u}_1$	r_1^2	$r_1r_2\bar{u}_1u_2$
$r_2\bar{u}_2u_1$	$r_0r_2\bar{u}_2$	$r_1r_2\bar{u}_2u_1$	r_2^2

совпадают. □

Теперь покажем, что координатное условие ортогональности выполнено для точки и прямой, имеющих вещественную координату в разных местах.

Лемма 3. *Если x_0 и y_1 вещественны, то для $e=e_{x_0,x_1,x_2}$ и $f=e_{y_0,y_1,y_2}$ имеем*

$$x_0\bar{y}_0+x_1\bar{y}_1+x_2\bar{y}_2=0 \iff e\circ f=0.$$

Доказательство. Если $x_0\bar{y}_0+x_1\bar{y}_1+x_2\bar{y}_2=0$, то имеем, например,

$$(ef)_{02}=\bar{x}_0((x_0\bar{y}_0+x_1\bar{y}_1+x_2\bar{y}_2)y_2)=0,$$

поскольку левая часть равна

$$\bar{x}_0x_0\cdot\bar{y}_0y_2+\bar{x}_0x_1\cdot\bar{y}_1y_2+\bar{x}_0x_2\cdot\bar{y}_2y_2,$$

и в этой сумме слагаемые можно заменить на

$$\bar{x}_0(x_0\bar{y}_0\cdot y_2),\quad \bar{x}_0(x_1\bar{y}_1\cdot y_2)\quad\text{и}\quad \bar{x}_0(x_2\bar{y}_2\cdot y_2)$$

в силу, соответственно, вещественности x_0, вещественности y_1 и, наконец, вещественности $\bar{y}_2y_2$ вкупе с диассоциативностью.

Имеющейся ослабленной ассоциативности как раз хватает для того, чтобы аналогичным образом показать, что все остальные $(ef)_{ij}$ и $(fe)_{ij}$ обращаются в нуль, с тем исключением, что для элементов с индексами 01 и 10 необходимо предварительно привести (x_0, x_1, x_2) к виду (x_0', x_1', x_2'), где x_2' вещественно.

Чтобы доказать обратное, мы с помощью того же метода убедимся, что сумма диагональных элементов матрицы $e\circ f$ (равная нулю) есть

сумма трех действительных чисел

$$\sum_i [\bar{x}_i((x_0\bar{y}_0 + x_1\bar{y}_1 + x_2\bar{y}_2)y_i), 1] =$$

$$= \sum_i [x_0\bar{y}_0 + x_1\bar{y}_1 + x_2\bar{y}_2, x_i\bar{y}_i] = [x_0\bar{y}_0 + x_1\bar{y}_1 + x_2\bar{y}_2],$$

так что $x_0\bar{y}_0 + x_1\bar{y}_1 + x_2\bar{y}_2$ действительно обращается в нуль. □

Наша заключительная лемма обосновывает употребление слов «проективная плоскость»: она показывает, что любые две различные прямые пересекаются ровно в одной точке и что через любые две различные точки проходит ровно одна прямая.

Лемма 4. *Если (y_0, y_1, y_2) и (z_0, z_1, z_2) — два непропорциональных единичных вектора, в которых y_1 и z_1 вещественны, то равенства*

$$x_0\bar{y}_0 + x_1\bar{y}_1 + x_2\bar{y}_2 = 0 \quad и \quad x_0\bar{z}_0 + x_1\bar{z}_1 + x_2\bar{z}_2 = 0$$

вкупе с условием вещественности x_0 определяют (x_0, x_1, x_2) однозначно с точностью до пропорциональности.

Доказательство. Отношение x_0 к x_2 находится с помощью вычитания

$$(x_0\bar{y}_0 + x_1\bar{y}_1 + x_2\bar{y}_2)\bar{z}_1$$

из

$$(x_0\bar{z}_0 + x_1\bar{z}_1 + x_2\bar{z}_2)\bar{y}_1;$$

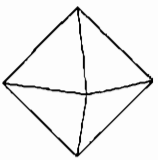
после этого x_1 можно найти из любого из двух уравнений. □

Этим завершается доказательство следующей теоремы.

Теорема 1. *Назовем тройку октав (x_0, x_1, x_2)* специальной, *если хотя бы одна из них вещественна; отождествим (x_0, x_1, x_2) с $(\lambda x_0, \lambda x_1, \lambda x_2)$, если обе тройки специальны, и назовем тройки (x_0, x_1, x_2) и (y_0, y_1, y_2)* ортогональными, *если они имеют вещественные координаты в разных местах и $x_0\bar{y}_0 + x_1\bar{y}_1 + x_2\bar{y}_2 = 0$. Тогда с помощью специальных троек можно параметризовать и точки, и прямые на октавной проективной плоскости; точка и прямая инцидентны тогда и только тогда, когда соответствующие тройки ортогональны.*

Октавная плоскость интересна потому, что она является чрезвычайно симметричным объектом; ее группа автоморфизмов — это 52-мерная группа Ли E_6. Данное нами определение является, для такого замечательного объекта, удивительно простым.

Поскольку, однако, цель этой книги — изучить свойства кватернионов и октав самих по себе, мы ограничимся здесь этим указанием на одно из их приложений.



Литература

[1] A. A. Albert. Quadratic forms permitting composition // Ann. Math. — 1942. — V. 43. — P. 161–177.

[2] D. Allcock. Identifying models of the octave projective plane // Geom. Dedicata. — 1997. — V. 65. — P. 215–217.

[3] S. L. Altmann. Rotations, Quaternions, and Double Groups. — Oxford: Clarendon Press, 1986.

[4] H. Aslaksen. Restricted homogeneous coordiantes for the Cayley projective plane // Geom. Dedicata. — 1991. — V. 40. — P. 245–250.

[5] J. Baez. The octonions // Bull. Amer. Math. Soc. — 2002. — V. 39. — P. 145–205.

[6] H. F. Blichfeldt. The minimum values of positive quadratic forms in six, seven, and eight variables // Math. Z. — 1935. — V. 39. — P. 1–15.

[7] H. Brown, R. Bülow, J. Neubüser, etc. Crystallographic groups of four-dimensional space. New York: John Wiley and Sons, 1978.

[8] R. H. Bruck, E. Kleinfeld. The structure of alternative division rings // Proc. Amer. Math. Soc. — 1951. — V. 2. — P. 878–890.

[9] A. Cayley. On Jacobi's elliptic functions, in reply to the Rev. B. Bronwin; and on quaternions // Phil. Mag. — 1845. — V. 26. — P. 208–211.

[10] A. Cayley. On Jacobi's elliptic functions, in reply to the Rev. B. Bronwin; and on quaternions (appendix only). In: The Collected mathematical papers. — New York: Johnson Reprint Co., 1963. — P. 127.

[11] H. S. M. Coxeter. Integral Cayley numbers // Duke Math J. — 1946. — V. 13. — P. 561–678.

[12] M. J. Crowe. A History of Vector Analysis. — Notre Dame: University of Notre Dame Press, 1963.

[13] C. W. Curtis. The four and eight square problem and division algebras. In: A. Albert, ed. Studies in Modern Algebra. New Jersey: Prentice-Hall, 1963. — P. 100–125.

[14] L. E. Dickson. On quaternions and their generalization and the history of the eight square theorem // Ann. Math. — 1919. — V. 20. — P. 155–171, 297.

[15] L. E. Dickson. Algebras and Their Arithmetics. — Chicago: Univ. of Chicago Press, 1923.

[16] C. J. Feaux. Divisor matrices in the Cayley ring // J. of Number Theory. — 1973. — V. 5. — P. 502–523.

[17] H. Freudenthal. Lie groups in the foundations of geometry //Adv. Math. — 1964. — V. 1. — P. 145–190.

[18] H. Freudenthal. Oktaven, Ausnahmengruppen und Oktavengeometrie // Geometriae Dedicata. — 1985. — V. 19. — P. 7–63. (Имеется перевод: Г. Фрейденталь. Октавы, особые группы и октавная геометрия // Математика (сб. переводов). — 1957. — Т. 1, № 1. — С. 117–153.)

[19] T. Gosset. On the regular and semi-regular figures in space of n dimensions // Messenger Math. — 1900. — V. 29. — P. 43–48.

[20] M. E. Goursat. Sur les substitutions orthogonales et les divisions régulières de l'espace // Ann. Sci. Ec. Norm. Sup. — 1989. — V. 6. — P. 9–102.

[21] R. P. Graves. Life of Sir William Rowan Hamilton. — New York: Arno Press, 1975.

[22] R. Guy. Catwalks, sandsteps, and Pascal pyramids // Journal of Integer Sequences. — 2000. — № 3. — Article 00.1.6.

[23] W. R. Hamilton. The Mathematical Papers of William Rowan Hamilton, App. 3, V. 3. — Cambridge: CUP, 1967. (См. также: У. Гамильтон. Избранные труды. — М.: Наука, 1994.)

[24] T. L. Hankins. Sir William Rowan Hamilton. — Baltimore: Johns Hopkins University Press, 1980.

[25] A. C. Hurley. Finite rotation groups and crystal classes in four dimensions // Proc. of the Cambridge Phil. Soc. — 1951. — P. 650–661.

[26] A. Hurwitz. Über die Komposition der quadratische Formen von beliebig vielen Variabeln // Nachr. Ges. der Wiss. Gött. — 1898. — P. 309–316.

[27] I. Kaplansky. Infinite-dimensional quadratic forms admitting composition // Proc. Amer. Math. Soc. — 1953. — V. 4. — P. 956–960.

[28] A. Korkine, G. Zolotareff. Sur les formes quadratiques positives // Math. Ann. — 1877. — V. 11. — P. 242–292.

[29] J. B. Kuipers. Quaternions and Rotation Sequences. — Princeton: PUP, 2002.

[30] P. J. C. Lamont. Ideals in Cayley's algebra // Indag. Math. — 1963. — V. 25. — P. 394–400.

[31] M. Liebeck. The classification of finite simple Moufang loops // Math. Proc. of the Cambridge Phil. Soc. — 1987. V. 102. — P. 33–47.

[32] K. Mahler. On Ideals in the Cayley–Dickson algebra // Proc. of the Irish academy. — 1942. — V. 48. — P. 123–133.

[33] R. Moufang. Alternativkörper und der Satz vom vollständigen Vierseit (D_9) // Abh. Math. Sem. Univ. Hamburg. — 1933. — V. 9. — P. 207–222.

[34] A. Pfister. Zur Darstellung definiter Funktionen als summe von Quadraten // Inv. Math. — 1967. — V. 4. — P. 229–237.

[35] I. Porteous. Topological Geometry. — Cambridge: CUP, 1981.

[36] R. A. Rankin. A certain class of multiplicative functions // Duke Math. J. — 1946. — V. 13. — P. 281–306.

[37] H. P. Rehm. Prime factorization of integral Cayley octaves // Ann. Fac. Sci. Toulouse. — 1993. — V. 2. — P. 271–289.

[38] O. Rodrigues. Des lois géométriques qui régissent les déplacements d'un système solide dans l'espace, et de la variation des cordonnées provenant de ces déplacements considérés indépendamment des causes qui peuvent les produire // J. Math. Pures et Appl. — 1840. — V. 5. — P. 380–440.

[39] H. J. S. Smith. On the orders and genera of quadratic forms containing more than three indeterminates // Proc. of the Royal Soc. — 1867. — V. 16. — P. 197–208.

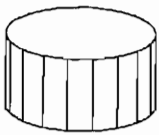
[40] W. Threlfall, H. Seifert. Topologische Untersuchung der Diskontinuitätsbereiche einer Bewegungsgruppen des dreidimensionalen sphärlichen Raumes // Math. Ann. — 1931. — V. 104. — P. 1–70.

[41] P. Du Val. Homographies, Quaternions, and Rotations. — Oxford: OUP, 1964.

[42] F. van der Blij. History of the octaves // Simon Stevin. — 1961. — P. 106–125.

[43] F. van der Blij, T. A. Springer. The arithmetics of octaves and of the group G_2 // Indag. Math. — 1959. — V. 21. — P. 406–418.

[44] M. Zorn. The automorphisms of Cayley's non-associative algebra // Proc. of the Nat. Acad. Sci. — 1935. — V. 21. — P. 355–358.



Предметный указатель

Джон Хортон Конвей
Дерек Алан Смит

О кватернионах и октавах, об их геометрии, арифметике и симметриях

Редактор *Т. Л. Коробкова*
Технический редактор *Д. Е. Щербаков*

Подписано в печать 15/X 2009 года. Формат $60 \times 90\,{}^{1}/_{16}$.
Физ. печ. л. 11,5. Бумага офсетная. Печать офсетная.
Тираж 1000 экз. Заказ № 20041.

Издательство Московского центра
непрерывного математического образования.
119002, Москва, Большой Власьевский пер., 11. Тел. (499) 241 74 83.

Отпечатано по CtP-технологии
в ОАО «Печатный двор» им. А. М. Горького.
197110, Санкт-Петербург, Чкаловский проспект, 15.

Эта небольшая монография посвящена самым разнообразным геометрическим и арифметическим свойствам алгебр кватернионов и октав (чисел Кэли). В числе прочего, излагаются общая теория композиционных алгебр и теория тройственности, рассказывается о связи октав с лупами Муфанг, изучаются свойства кватернионных и октавных аналогов гауссовых целых чисел. Значительная часть материала книги не была до сих пор отражена в литературе на русском языке.

ISBN 978-5-94057-517-7