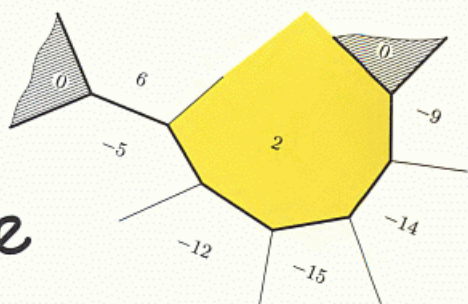


Квадратичные формы, данные нам в ощущениях



Дж. Конвей

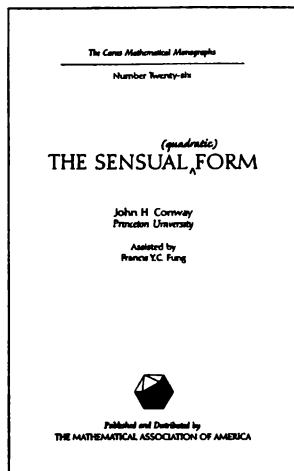
данные нам

**КВАДРАТИЧНЫЕ
ФОРМЫ
В ОЩУЩЕНИЯХ**

*Перевод с английского
С. М. Львовского
под редакцией
В. В. Доценко*

Москва
Издательство МЦНМО
2008

УДК 511.6+512.647.2
ББК 22.132+22.14
К64



Конвей Дж.

К64 Квадратичные формы, данные нам в ощущениях / Перевод с англ. С. М. Львовского. — М.: МЦНМО, 2008. — 144 с.: ил.

ISBN 978-5-94057-268-8

Книга содержит нестандартное изложение различных аспектов теории целочисленных и рациональных квадратичных форм, включая теорему Минковского–Хассе. И студенты старших курсов, и аспиранты, и научные работники найдут в книге много интересного; этим категориям читателей книга и адресована.

ББК 22.132+22.14

Конвей Джон

Квадратичные формы, данные нам в ощущениях

Техн. редактор: *Д. Е. Щербаков*

Лицензия ИД № 01335 от 24/III 2000 года. Подписано в печать 18/III 2008 года.

Формат 60 × 88 ¹/₁₆. Физ. печ. л. 9. Усл. печ. л. 8,82.

Бумага офсетная. Печать офсетная. Гарнитура Computer Modern.

Тираж 1000 экз. Заказ № 89-08

Издательство Московского центра непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11. Тел. 241 74 83.

First published in the United States
under the title:

The Sensual (quadratic) Form

© 1997 by the Mathematical Association
of America, Washington, D. C.

© 2008, МЦНМО, перевод на русский язык

ISBN 0-88385-030-3 (англ.)

ISBN 978-5-94057-268-8 (рус.)

Оглавление

Предисловие	4
К читателю	7
Лекция 1. Можно ли увидеть значения $3x^2 + 6xy - 5y^2$? . . .	8
Добавление. $\text{PSL}_2(\mathbb{Z})$ и дроби Фарея	32
Лекция 2. Можно ли услышать форму решетки?	38
Добавление. Кнезеровский метод склейки: унимодулярные решетки	54
Лекция 3. А можно ли ее форму нащупать?	62
Добавление. Как нащупать форму четырехмерной решетки	83
Лекция 4. Простые ароматы	88
Добавление. Еще об инвариантах; p -адические числа .	111
Постскриптум. Вкус теории чисел	120
Библиография	135
Предметный указатель	139

Предисловие

Эта небольшая книжка основана на Хедриковских лекциях (Earle Raymond Hedrick Lectures), прочитанных мною на совместных заседаниях Американского математического общества и Математической ассоциации Америки в Ороно (штат Мэн) 7–9 августа 1991 года. Я интересуюсь квадратичными формами уже много лет, и тем не менее я все время узнаю новые и простые подходы к их пониманию. Благодаря «топокарте» из лекции 1 вся теория бинарных квадратичных форм становится настолько простой, что пропадает даже необходимость размышлять или доказывать теоремы — достаточно просто посмотреть! В некотором смысле специалистам что-то подобное было известно и раньше, но почему же они пользовались этим только в аналитической теории, а не с самого начала?

Если знаменитый вопрос Марка Каца «Можно ли услышать форму барабана?» применить к n -мерным тороидальным «барабанам», то возникает вопрос о том, какие свойства квадратичных форм определяются числами, которые они представляют. Иными словами: что мы знаем о решетке, если мы знаем количество векторов каждой заданной длины?

Коль скоро в ход уже пошли зрение и слух, я решил, что основной идеей лекций будет то, что надо пытаться воспринимать квадратичную форму всеми органами чувств; отсюда и «ощущения» из заглавия моих Хедриковских лекций, и темы первых двух из них.

Я не смог выбрать единую тему для третьей лекции даже к тому моменту, когда ее надо было уже читать. Поэтому в конце концов я разделил ее на два получасовых рассказа: один про форму области Вороного для данной решетки, другой — про теорию Минковского–Хассе. В книге каждый из этих рассказов превратился в полноценную лекцию.

Исследование области Вороного было легко связать с осязанием. Обоняние было введено мной в игру, когда я стал рассматривать p -адические инварианты как запахи отдельных цветов в букете. После этого естественно было завершить книгу постскриптумом, дающим читателю возможность попробовать на вкус теорию чисел.

Эту книгу не следует рассматривать как серьезный учебник по теории квадратичных форм — скорее это сборник эссе, посвященных интересующим меня отдельным аспектам этой теории. В учебнике,

который я должен был бы написать, теория приведения по Минковскому обсуждалась бы, бесспорно, более подробно; кроме того, туда бы вошла и аналитическая теория квадратичных форм, и гауссова группа бинарных форм с композицией в качестве операции.

Изложение в этой книге отличается от традиционных во многих аспектах. «Топокарта» из лекции 1 является новой, так же как «конормы», использующиеся в ней же и в лекции 3, « p -избыток» и « p -сигнатура» из лекции 4, а также гауссовы средние, с помощью которых доказывается их инвариантность. p -избыток одномерной формы $[a]$ представляет собой квадратичную функцию от a , соответствующая которой симметрическая билинейная функция есть символ Гильберта $(a, b)_p$.

Это, кстати, напомнило мне о том, что многие снисходительно улыбаются всякий раз, как я упоминаю о -1 как о простом числе, и по-прежнему обозначают это число взрослым, как они считают, знаком ∞ . Посмотрим, однако, на следующие утверждения:

Всякое ненулевое рациональное число единственным образом разлагается в произведение степеней простых чисел p .

Если p и q — различные нечетные простые числа, то $\left(\frac{p}{q}\right)$ и $\left(\frac{q}{p}\right)$ отличаются тогда и только тогда, когда $p \equiv q \equiv -1 \pmod{4}$.

Имеется инвариант, называемый p -сигнатурой, в определении которого участвует суммирование p -частей чисел.

Если существуют целые p -адические корневые векторы норм k и kp , то p лежит в спинорном ядре.

В каждом из этих утверждений допускается равенство $p = -1$, и ни одному из них не удастся даже придать смысл, если мы будем пользоваться этим нелепым обозначением « ∞ », так что теперь я буду снисходительно улыбаться в ответ!

Нил Слоун и я сотрудничаем много лет; большинство идей, содержащихся в этой книге, впервые в том или ином виде появились в наших многочисленных статьях или же в нашей книге «Упаковки шаров, решетки и группы». Отсылаем интересующегося читателя к этим текстам, в которых многие вопросы, обсуждающиеся здесь, рассматриваются более подробно. Я обязан Нилу гораздо больше, чем это видно из предисловия!

Я благодарен Леонарду Гиллману и Математической ассоциации Америки за то, что они пригласили меня прочитать Хедриковские лекции 1991 года. Дональд Альберс предложил опубликовать записки этих лекций в серии «Carus Mathematical Monographs», так что

именно ему книга в конечном счете обязана своим существованием. Я благодарен Марджори Сенешаль из редколлегии этой серии за постоянный интерес к книге.

Если эта книга оказалась удобочитаемой, то благодарить за это надо в значительной степени редактора Джулиану Давидофф, тщательно проработавшую текст и внесшую множество полезных предложений. Благодаря ее своевременному вмешательству оказалось возможным возобновить работу над книгой; я глубоко благодарен ей за постоянную поддержку.

И более всего я благодарен Фрэнсису Фунгу за предложение помочь мне в подготовке записок. Его помощь перешла в очень удачное сотрудничество. Фрэнсис всегда стремился включить в книгу побольше материала и в любой момент был готов помочь мне с его записью. Его идеи всегда оказывались уместны; он превратил груды бумаги в книгу, которую вы держите в руках.

Дж. Х. Конвей,
Принстон, Нью-Джерси

К читателю

Изложение в этих заметках является замкнутым; они должны быть доступны математически образованному читателю, не имеющему специальных познаний в теории квадратичных форм. Небольшие исключения не прерывают нить изложения. В добавлениях к лекциям обсуждаются некоторые дополнительные вопросы, и тут иногда требуется больше предварительных знаний.

Материал расположен таким образом, что трудность его постепенно возрастает по мере удаления от начала книги: лекции 1 и 2 можно освоить без особого труда, а вот читателю, который пожелает во всех подробностях разобраться в лекции 4, придется потрудиться.

Поскольку очень много материала в книге изложено по-новому, трудности при ее изучении не всегда легко преодолимы с помощью чтения стандартных учебников. Я надеюсь, что труд, затраченный на чтение книги, окупится и что даже специалисты по квадратичным формам найдут в ней какие-то новые идеи.

Л Е К Ц И Я 1

Можно ли увидеть значения $3x^2 + 6xy - 5y^2$?

Вступление

С этого вопроса начнется наше знакомство с теорией квадратичных форм. Теория эта старая: уже в вышедшей в 1798 году книге А.-М. Лежандра «*Essai sur la théorie des nombres*» [32] содержится ее большая часть, а Карл Фридрих Гаусс в своем монументальном труде «*Disquisitiones Arithmeticae*» [20] (1801) практически завершил эту теорию. В настоящей лекции мы расскажем о новом, очень наглядном, методе представления значений произвольной бинарной квадратичной формы. Он позволит нам просто и элегантно расклассифицировать целые бинарные квадратичные формы и ответить на некоторые из основных вопросов про эти формы.

Что такое квадратичная форма?

Перед тем как начать, неплохо сказать вам, что означают слова «квадратичная форма». В общем случае *квадратичная форма* — это просто однородный многочлен степени 2 от нескольких переменных, то есть выражение наподобие

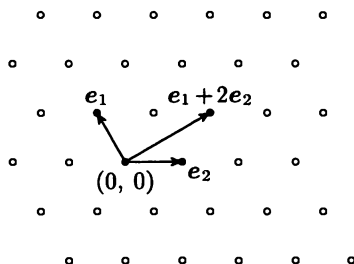
$$3x^2 + 6xy + y^2 - 5yz + z^2,$$

в котором каждое слагаемое имеет степень 2 (и тем самым нет ни линейных, ни постоянных членов). В этой лекции мы будем иметь дело только с целыми квадратичными формами от двух переменных (бинарными формами) вроде $3x^2 + 6xy - 5y^2$, где x, y и коэффициенты — целые числа.

Если $f(x, y) = 3x^2 + 6xy - 5y^2$, то легко видеть, что $f(1, 1) = 3 + 6 - 5 = 4$ является значением формы f . Предположим, однако, что нам хочется выяснить, можно ли найти такую пару (x, y) , что $f(x, y) = 7$. Понять это с ходу не так-то просто, и ясно, что невозможно перебрать все упорядоченные пары (x, y) .

Можно получить больше информации, если немного изменить точку зрения. Мы определили f как функцию от упорядоченной пары (x, y) , но можно было бы с тем же успехом рассматривать ее как

функцию от двумерного вектора $v = xe_1 + ye_2$, где e_1 и e_2 — два линейно независимых вектора. Линейные комбинации с целыми коэффициентами образуют плоскую решетку, как на рисунке ниже; векторы из этой решетки можно складывать и вычитать.



Базисом решетки называется пара векторов решетки наподобие e_1 и e_2 (в старших размерностях — последовательность векторов), обладающая тем свойством, что всякий вектор решетки единственным образом записывается в виде линейной комбинации векторов из базиса с целыми коэффициентами. Разумеется, одну и ту же решетку можно породить многими различными базисами: возьмите, например, $e_1 + e_2$ и e_2 . Итак, бинарная квадратичная форма — это некоторая функция на плоской решетке.

На самом деле функция f является квадратичной формой тогда и только тогда, когда:

- 1) скаляры ведут себя квадратично, т. е. $f(av) = a^2 f(v)$;
- 2) функция $B(v, w) = f(v + w) - f(v) - f(w)$ является симметрической билинейной формой; это означает, что

$$B(w, v) = B(v, w)$$

и

$$B(\lambda u + \mu v, w) = \lambda B(u, w) + \mu B(v, w).$$

В (2×2) -случае бинарную форму $ax^2 + hxy + by^2$ можно более наглядно записать в виде

$$ax^2 + \frac{h}{2}xy + \frac{h}{2}yx + by^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & h/2 \\ h/2 & b \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Тогда соответствующая билинейная форма имеет вид

$$2ax_1x_2 + hx_1y_2 + hy_1x_2 + 2by_1y_2 = 2 \begin{pmatrix} x_1 & y_1 \end{pmatrix} \begin{pmatrix} a & h/2 \\ h/2 & b \end{pmatrix} \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}.$$

Важно сознавать, что от решеток, о которых мы до сих пор говорили, до геометрии еще далеко: мы имели дело только с их аддитивной структурой. (Специалист может рассматривать их как двумерные $\mathbb{Z}$ -модули.)

Два типа целочисленности

Соотношение между коэффициентами в квадратичной форме $ax^2 + hxy + by^2$ и элементами матрицы

$$\begin{pmatrix} a & h/2 \\ h/2 & b \end{pmatrix}$$

приводит к двум различным пониманиям термина «целая квадратичная форма» (эта двусмысленность преследовала наш предмет, начиная с его младенчества). Мы будем говорить, что квадратичная форма является *целой*, если целочисленны ее значения при целых значениях переменных — форма $ax^2 + hxy + by^2$ удовлетворяет этому условию в точности тогда, когда a , h и b — целые числа. Мы будем говорить, что квадратичная форма *матрично целочисленна*, если целочисленны элементы соответствующей матрицы — форма $ax^2 + hxy + by^2$ удовлетворяет этому условию, если целыми числами являются a , $h/2$ и b .

В теории чисел часто приходится иметь дело с представлением чисел формами, так что целые формы тут особенно важны. В геометрических или алгебраических контекстах может быть важна и целочисленность скалярных произведений, так что в этом случае обычно требуется матричная целочисленность.

Определитель решетки — это определитель матрицы, столбцы которой суть координаты базисных векторов. Поскольку определитель матрицы целой формы не всегда является целым числом, некоторые авторы пользуются его модификацией, называемой *дискриминантом* (см., например, [49]). Поскольку при сравнении форм разных размерностей работа с дискриминантом легко приводит к путанице, мы постараемся не пользоваться этим понятием. Например, в дальнейшем нам встретится хорошо известная последовательность решеток $A_0, A_1, A_2, \dots$, определители которых равны

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \dots,$$

в то время как дискриминанты (при стандартном определении) имеют вид

$$1, 1, -3, -2, 5, 3, -7, -4, 9, 5, -11, \dots!$$

Эквивалентность

Две квадратичные формы, выглядящие совершенно по-разному, могут быть по существу одинаковы. Будем называть две формы (целочисленно) эквивалентными, если они представляют одну и ту же функцию на решетке, но, возможно, в двух разных базисах. Точнее говоря, формы $ax^2 + hxy + by^2$ и $AX^2 + HXY + BY^2$ называются целочисленно эквивалентными, если первая из них имеет вид $f(xe_1 + ye_2)$, а вторая — $f(Xf_1 + Yf_2)$, где $\{e_1, e_2\}$ и $\{f_1, f_2\}$ — два базиса одной и той же решетки.

Из этого, в частности, следует, что когда переменные пробегает целые числа, обе формы принимают те же самые значения. Если, например,

$$e_1 = f_2, \quad e_2 = -f_1 - f_2,$$

то

$$xe_1 + ye_2 = -yf_1 + (x-y)f_2 = wf_1 + zf_2,$$

так что

$$2x^2 - 4xy + 3y^2 = 2(x-y)^2 + y^2 = 2z^2 + w^2,$$

где $z = x - y$ и $w = -y$. Если x и y независимо пробегает все целые числа, то это же верно и применительно к z и w ; поэтому значения, принимаемые формами $2x^2 - 4xy + 3y^2$ и $2z^2 + w^2$, одни и те же.

В матричных обозначениях имеем

$$\begin{pmatrix} w \\ z \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

так что

$$(w \ z) = (x \ y) \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

и

$$2z^2 + w^2 = (w \ z) \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} w \\ z \end{pmatrix} = (x \ y) \begin{pmatrix} 2 & -2 \\ -2 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 2x^2 - 4xy + 3y^2.$$

Более общим образом, матрицы A и B представляют одну и ту же форму относительно различных базисов тогда и только тогда, когда существует матрица M , для которой $M^T A M = B$, причем элементы матриц M и M^{-1} целочисленны (или, что равносильно, элементы матрицы M целочисленны и $\det(M) = \pm 1$.) В частности, мы видим, что определитель формы не зависит от выбора базиса: $\det(B) = \det(A)(\det(M))^2 = \det(A)$.

Примитивные векторы, базисы и супербазисы, строгое и нестрогое

Чтобы понять квадратичную форму, надо поелику возможно исследовать ее свойства, не зависящие от базиса. наших рассмотрения будут состоять в тщательном изучении трех понятий: примитивных векторов, базисов и супербазисов.

Поскольку $f(kv) = k^2 f(v)$, мы видим, что для того, чтобы исследовать значения f на всех векторах, достаточно изучить ее значения на *примитивных векторах*, т. е. векторах, не имеющих вида kv ни для какого целого $k > 1$. Далее, поскольку $f(-v) = f(v)$, часто будет удобно мыслить v и $-v$ как «один и тот же» вектор. *Строгим вектором* будет называться примитивный вектор v , мыслимый как отличный от $-v$, а *нестрогим вектором* будет называться пара $\pm v$, где v — строгий вектор.

Точно так же *строгим базисом* называется такая упорядоченная пара векторов (e_1, e_2) , что в виде их линейной комбинации с целыми коэффициентами представляется любой вектор решетки. *Нестрогий базис* — это множество $\{\pm e_1, \pm e_2\}$, получаемое из строгого базиса.

Наконец, *строгий супербазис* — это упорядоченная тройка (e_1, e_2, e_3) , для которой $e_1 + e_2 + e_3 = 0$ и (e_1, e_2) — строгий базис (из строгих векторов), а *нестрогий супербазис* — это множество $\{\pm e_1, \pm e_2, \pm e_3\}$, где (e_1, e_2, e_3) — строгий супербазис. С этого момента мы будем, без дальнейших оговорок, пользоваться «нестрогими» понятиями. Заметим, что все векторы, входящие в базис или супербазис, являются примитивными; обратно, всякий примитивный вектор входит в некоторый базис.

Соотношение между базисами и супербазисами

Ясно, что всякий супербазис

$$\{\pm e_1, \pm e_2, \pm e_3\}$$

содержит в точности три базиса

$$\{\pm e_1, \pm e_2\}, \quad \{\pm e_1, \pm e_3\}, \quad \{\pm e_2, \pm e_3\}.$$

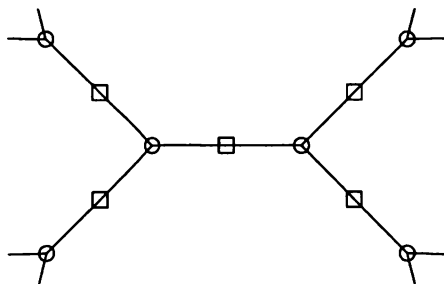
С другой стороны, всякий базис $\{\pm e_1, \pm e_2\}$ содержится в точности в двух супербазисах:

$$\{\pm e_1, \pm e_2, \pm(e_1 + e_2)\}, \quad \{\pm e_1, \pm e_2, \pm(e_1 - e_2)\}$$

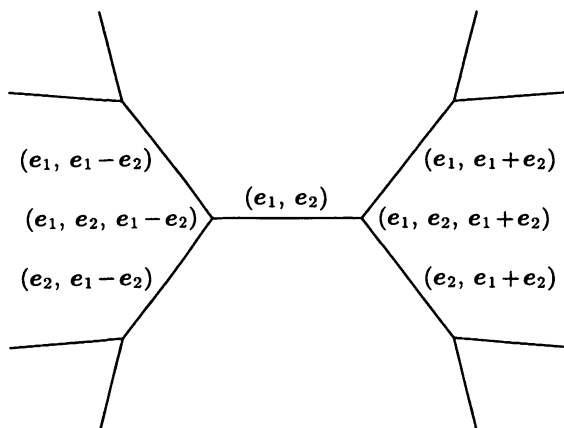
(заметьте, что это действительно супербазисы).

Топография базисов и супербазисов

Связи между базисами и супербазисами можно изобразить на картинке. Давайте нарисуем граф, на котором каждый супербазис (○) соединен с тремя содержащимися в нем базисами (□).



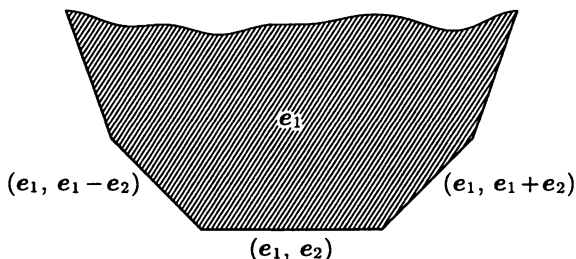
Поскольку каждый базис содержится ровно в двух супербазисах, можно изобразить такую *топокарту*, на которой каждому базису соответствует ребро, а каждому супербазису — вершина:



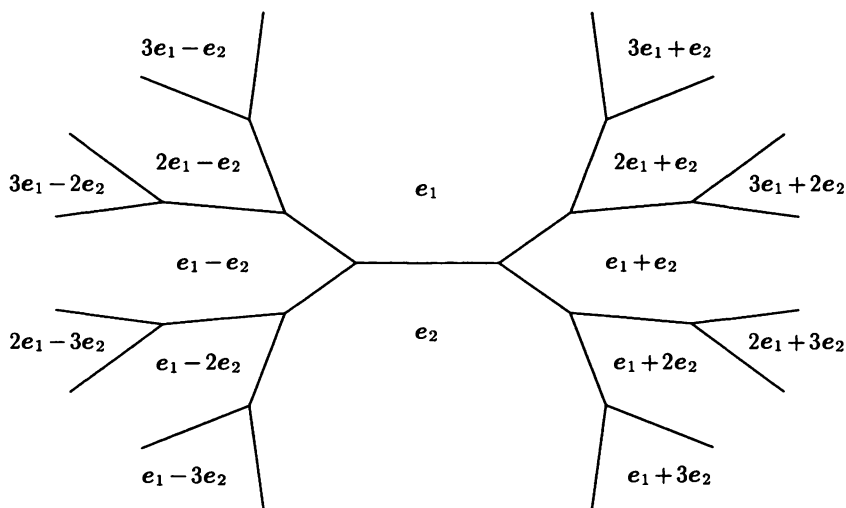
Где на топокарте расположены примитивные векторы?

Если $\pm e_1$ входит в базис $\{\pm e_1, \pm e_2\}$, входящий, в свою очередь, в супербазис $\{\pm e_1, \pm e_2, \pm e_3\}$, то, кроме этого, e_1 входит в только

один из двух остальных базисов, содержащихся в этом супербазисе, а именно, в $\{\pm e_1, \pm e_3\}$. Стало быть, на нашей картинке (где мы опускаем знаки $\pm$) вершины и ребра, содержащие e_1 , образуют несамопересекающуюся ломаную. Следовательно, мы можем добавить к нашей топокарте область, ограниченную этой ломаной, и отождествить эту область с $\pm e_1$ (так что наша топокарта станет более похожей на настоящую). Если разметить таким образом все области на топокарте,



то каждой области будет соответствовать нестрогий вектор $\pm v$ (мы обычно будем опускать знак); два вектора, граничащие по ребру, образуют (нестрогий) базис, а три вектора, сходящиеся в одной точке, образуют (нестрогий) супербазис.



Нормы векторов

До сих пор, работая с топокартой, мы даже не упоминали о значениях формы f (так что вид топокарты от f не зависит). Теперь зафиксируем конкретную квадратичную форму f и будем называть число $f(v)$ (для этой f) *нормой* вектора v .

Правило арифметической прогрессии

Пусть нам известны значения квадратичной формы f на трех векторах $\{e_1, e_2, e_3\}$ из некоторого супербазиса. Как найти значения в других точках? Воспользуемся формулой

$$f(v_1 + v_2) + f(v_1 - v_2) = 2[f(v_1) + f(v_2)],$$

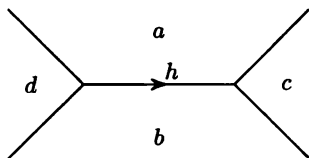
которая по существу эквивалентна хорошо известной теореме Аполлония из планиметрии. Чтобы проверить эту формулу, обозначим через $B(v_1, v_2)$ билинейную форму, ассоциированную с f . Тогда имеем

$$\begin{aligned} f(v_1 + v_2) + f(v_1 - v_2) &= f(v_1) + f(v_2) + B(v_1, v_2) + \\ &\quad + f(v_1) + f(v_2) - B(v_1, v_2) = 2[f(v_1) + f(v_2)]. \end{aligned}$$

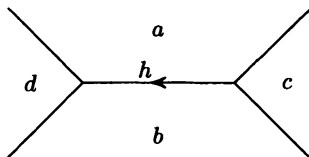
Из доказанной формулы явствует, что если

$$a = f(v_1), \quad b = f(v_2), \quad c = f(v_1 + v_2), \quad d = f(v_1 - v_2)$$

суть значения f на четырех областях, примыкающих к данному ребру на топокарте, то числа $d, a + b$ и c образуют арифметическую прогрессию (разность которой мы будем обозначать через h). Мы будем называть эту закономерность *правилом арифметической прогрессии*. Далее, на каждом ориентированном ребре мы напишем число h (разность арифметической прогрессии). Можно выбирать ориентацию ребер таким образом, чтобы не получалось отрицательных значений h , а если $h = 0$, то мы будем, как правило, опускать стрелку. Короче говоря, рисунок



означает, что $c = (a + b) + h$, $d = (a + b) - h$ (см. [41], [48], [22]), в то время как рисунок



означает, что $c = (a + b) - h$, $d = (a + b) + h$.

Запись квадратичных форм в базисе

Пусть теперь нам даны значения квадратичной формы f на супербазисе:

$$f(e_1) = a, \quad f(e_2) = b, \quad f(e_1 + e_2) = c.$$

Если теперь

$$v = xe_1 + ye_2,$$

то

$$f(v) = f(x, y) = ax^2 + (c - a - b)xy + by^2,$$

поскольку эта функция — единственная однородная квадратичная функция, для которой

$$f(1, 0) = a, \quad f(0, 1) = b \quad \text{и} \quad f(1, 1) = c.$$

Заметим, что коэффициент при xy совпадает с числом h , являющимся разностью той прогрессии, о которой шла речь в правиле арифметической прогрессии.

Итак, если нам даны супербазис и три целых числа a , b и c , то можно найти целую квадратичную форму, принимающую значения a , b и c на этом супербазисе.

Далее, матричное представление формы f в базисе, соответствующем горизонтальному ребру на рисунке на с. 16, имеет вид

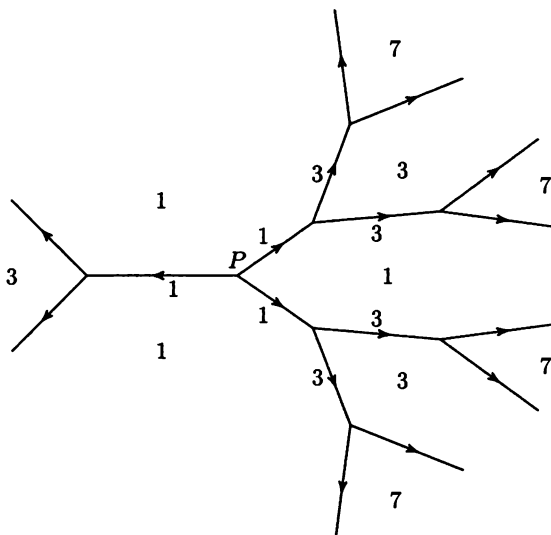
$$(x \ y) \begin{pmatrix} a & h/2 \\ h/2 & b \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

так что определитель формы f равен $ab - (h/2)^2$. Напомним, что поскольку определитель матрицы обратимой замены базиса равен ± 1 , определитель является инвариантом относительно целочисленной эквивалентности.

Древесное свойство

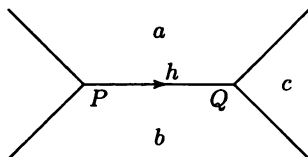
Оказывается, что наша топокарта является *деревом*, то есть связным графом без циклов. Мы докажем это в настоящем и следующем разделах.

Почему отсутствуют циклы? Построим форму, принимающую значения 1, 1, 1 на супербазисе, соответствующем вершине P .



Похоже, что числа возрастают по мере удаления от P . Будет ли так и дальше?

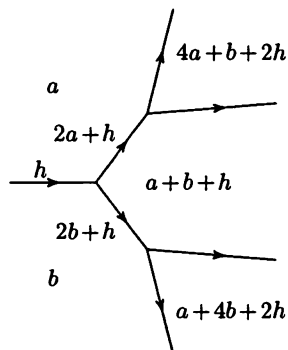
Лемма о возрастании. Пусть числа a , b и h на рисунке положительны. Тогда число c , соответствующее третьей из областей с вершиной в Q , также положительно, и стрелки на двух остальных ребрах, выходящих из Q , направлены прочь от Q .



Доказательство. Число c равно $a + b + h$ ввиду правила арифметической прогрессии. Поэтому одно из ребер, выходящих из Q ,

граничит с областями с надписями a и $a+b+h$, и сумма этих чисел равна $b+(2a+h)$. Поскольку это ребро отходит от области с надписью b , на ребре должно быть написано число $2a+h$.

Аналогично устанавливаем, что надпись на другом ребре есть $2b+h$. Стало быть, если имеется стрелка, ведущая из P в Q и граничащая с положительными числами, то стрелки, исходящие из Q , также будут окружены положительными числами, и притом большими. Значит, если мы выйдем из P в этом направлении, то мы в P никогда



не вернемся, поскольку встречающиеся по дороге числа будут только увеличиваться. $\square$

А теперь сделаем такое важное замечание: форма топокарты не зависит от квадратичной формы, она зависит только от базисов и супербазисов в решетке $\mathbb{Z}^2$, рассматриваемой исключительно как группа. Поэтому доказательство показывает, что цикла не получится *ни для какой* квадратичной формы, хотя мы установили это обстоятельство с помощью некоторой конкретной формы.

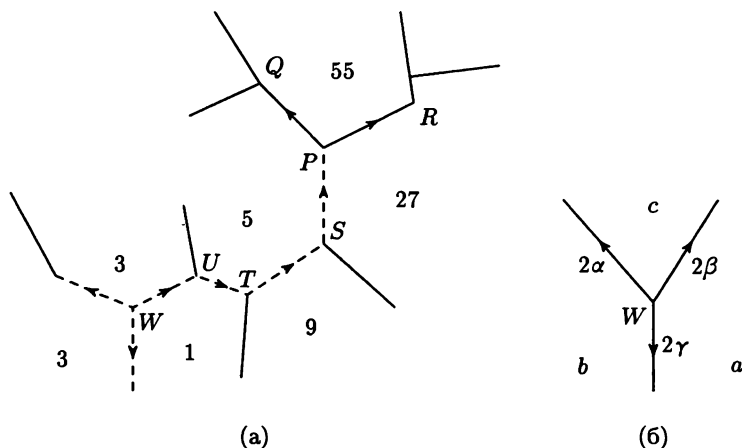
Связна ли топокарта? До сих пор мы рисовали только ее часть, получающуюся, если начать с какой-то одной вершины; могли бы существовать еще какие-то супербазисы, до которых таким способом добраться невозможно. В следующем разделе мы увидим, что это не так; для этого нам придется доказать лемму о положительно определенных формах.

Колодцы для положительно определенных форм

Форма f называется *положительно полуопределенной*, если $f(v) \geq 0$ для всех v , и *положительно определенной*, если $f(v) > 0$ для

всех $v \neq 0$. Аналогично определяются отрицательно полуопределенные и отрицательно определенные формы.

Посмотрим на топокарту формы (положительно определенной), принимающей на некотором супербазис значения 5, 27 и 55. Лемма о возрастании показывает, что если выходить из P через Q или R , то числа будут увеличиваться. Поэтому мы лучше опустимся в вершину S , значения в которой равны 5, 9 и 27. Продолжая этот процесс, будем двигаться против течения вдоль пути $STUW$, отмеченного на рисунке пунктиром.



В точке W мы остановимся, поскольку на всех трех ребрах с вершиной W стрелки указывают прочь от W . Будем называть супербазис W на рис. (б) *колодцем*, если всем трем отметкам 2α , 2β и 2γ на сходящихся в нем ребрах соответствуют стрелки, указывающие прочь от W . Если a , b и c — значения f на этом супербазисе, то из правила арифметической прогрессии следует, что

$$2\alpha = b + c - a, \quad 2\beta = c + a - b, \quad 2\gamma = a + b - c,$$

так что

$$a = \beta + \gamma, \quad b = \alpha + \gamma, \quad c = \beta + \alpha.$$

Из вышеприведенной конструкции вытекает, что у всякой положительно определенной целой формы существует колодец.

Лемма о колодце. Пусть дан колодец для положительно определенной квадратичной формы, или, равносильно, супербазис,

окруженный тремя положительными числами, удовлетворяющими «неравенству треугольника», т. е. $a + b \geq c$, $a + c \geq b$, $b + c \geq a$. Тогда три вектора этого супербазиса суть три примитивных вектора с наименьшей нормой (т. е. f принимает на них наименьшие значения).

Доказательство. Обозначим через α , β и γ неотрицательные числа

$$\alpha = \frac{b+c-a}{2}, \quad \beta = \frac{c+a-b}{2}, \quad \gamma = \frac{a+b-c}{2}.$$

Запишем произвольный вектор v в виде

$$v = m_1 e_1 + m_2 e_2 + m_3 e_3;$$

давайте выясним, как f выражается через m_i . Поскольку $e_1 + e_2 + e_3 = 0$, вектор v равен также

$$(m_1 - k)e_1 + (m_2 - k)e_2 + (m_3 - k)e_3,$$

так что f может зависеть только от разностей между m_i .

Однако линейные комбинации выражений

$$(m_2 - m_3)^2, \quad (m_1 - m_3)^2 \quad \text{и} \quad (m_1 - m_2)^2$$

образуют трехмерное пространство квадратичных форм. Следовательно, если какие-нибудь два из m_i совпадают, то v является кратным третьего базисного вектора. Стало быть, мы можем считать, что все m_i различны.

Далее, можно проверить, что выполняется следующая *формула Зеллинга*:

$$f(v) = \alpha(m_2 - m_3)^2 + \beta(m_1 - m_3)^2 + \gamma(m_1 - m_2)^2.$$

(Формула выполнена, поскольку правая часть является квадратичной формой, совпадающей с f на супербазисе e_1, e_2, e_3 ; или можно просто сравнить матрицы двух квадратичных форм в данном базисе.) Если v не кратно ни одному из e_i , то все разности $m_i - m_j$ отличны от нуля, так что $f(v) \geq \alpha + \beta + \gamma$, что не меньше каждой из сумм $a = \beta + \gamma$, $b = \alpha + \gamma$, $c = \alpha + \beta$. Если ни одно из чисел α, β и γ не обращается в нуль, то неравенство будет строгим. Стало быть, значения, принимаемые на колоде, суть три наименьших примитивных значения формы, а если α, β и γ отличны от нуля, то значения на любом другом векторе будут строго больше. $\square$

Формула Зеллинга [41] была обобщена на произвольную размерность Вороным [48]: если $e_0, e_1, \dots, e_n$ — супербазис, для которого

$e_i \cdot e_j = p_{ij}$, то $f(\sum m_i e_i) = \sum_{i < j} p_{ij} (m_i - m_j)^2$. (См. также [14] по поводу дальнейших подробностей.)

Топокарта связна

Чтобы убедиться, что топокарта связна, выберем положительно определенную квадратичную форму, имеющую в некотором супербазисе колодец, для которого $\alpha = \beta = \gamma = 1$. Идя против течения, мы получаем, что всякая компонента топокарты должна содержать колодец, на трех векторах которого достигаются три наименьших примитивных значения формы. Этот колодец может быть только «нашим» колодцем, так что и компонента должна быть «нашей» компонентой; этим доказана связность топокарты.

Конормы, вонормы, простые и двойные колодцы

Числа a , b и c будут называться *вонормами* формы f («нормами Вороного» — это нормы векторов Вороного формы f , которые будут формально определены в третьей лекции). Числа α , β и γ называются *конормами* формы f (их также называют параметрами Зеллинга, но в старших размерностях это не одно и то же). Каждая из этих троек чисел определяется по другой:

$$a = \beta + \gamma, \quad b = \alpha + \gamma, \quad c = \beta + \alpha$$

и

$$\alpha = \frac{b+c-a}{2}, \quad \beta = \frac{c+a-b}{2}, \quad \gamma = \frac{a+b-c}{2}.$$

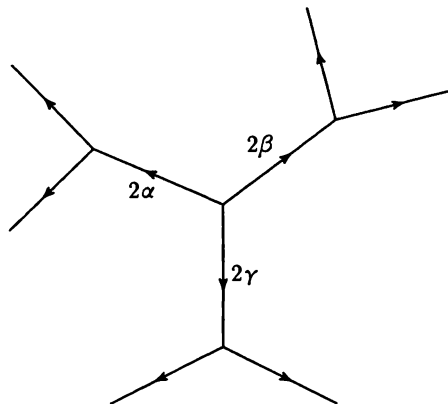
Мы видели, что если α , β и γ положительны, то колодец единствен. На рисунке ниже отметки на всех стрелках строго положительны и стрелки направлены прочь от колодца. Такой колодец мы будем называть *простым*.

Если колодец простым не является, то без потери общности можно считать, что $\alpha = b$, $\beta = a$, $\gamma = 0$, и формула Зеллинга принимает вид

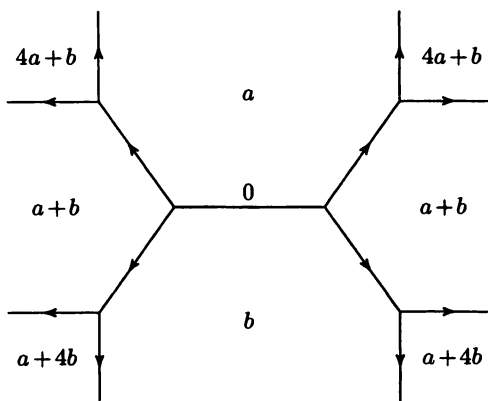
$$f(v) = b(m_2 - m_3)^2 + a(m_1 - m_3)^2.$$

Стало быть, значение f на векторе $m_1 e_1 + m_2 e_2$ есть $am_1^2 + bm_2^2$, значения на четырех нестрогих векторах

$$\pm e_1, \quad \pm e_2, \quad \pm(e_1 + e_2), \quad \pm(e_1 - e_2)$$



Простой колодец



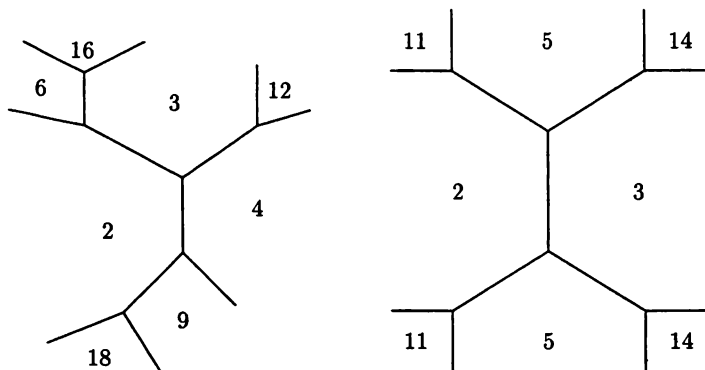
Двойной колодец

суть

$$a, \quad b, \quad a+b, \quad a+b,$$

а значения на всех остальных векторах строго больше. На приведенном рисунке ребро, граничащее с a и b , имеет на каждом конце по колодезю, и на нем нет стрелки (или есть стрелка с нулевой отметкой). На каждом из остальных ребер имеется стрелка, указывающая прочь от этого ребра. Такой колодец мы будем называть *двойным*.

На приведенных ниже рисунках изображены квадратичные формы, имеющие простой и двойной колодец соответственно.



Классификация форм по знакам

Оказывается, разумно разбить бинарные целые квадратичные формы на классы в соответствии с тем, какие значения они принимают на ненулевых примитивных векторах.

(+)-*формы*: это те самые положительно определенные формы, которые мы только что обсуждали. Их наименьшие значения окружают простой или двойной колодец, и их значения растут по мере удаления от колодца.

(-)-*формы*: разумеется, отрицательно определенные квадратичные формы очень похожи на положительно определенные.

(±)-*формы*: это важное семейство; мы обсудим их топокарты в следующем разделе. Как мы увидим, для них существует периодическая «река», разделяющая положительные и отрицательные значения формы.

0-форма: если форма принимает только значение 0, то ее топокарта состоит из бесконечного количества «озер», помеченных нулем.

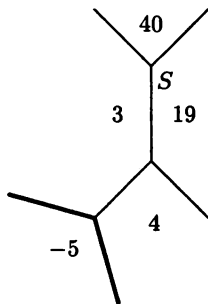
(0+)-формы: форма, принимающая только нулевые и положительные значения, эквивалентна кратному формы x^2 . Мы увидим, что ее значения возрастают по мере удаления от единственного озера (значение 0), окруженного областями с одним и тем же значением.

(0-)-формы аналогичны **(0+)-формам**.

(0±)-формы. Это — последний случай. Мы покажем, что в этом случае имеются два различных «озера» со значением 0, соединенные конечной рекой, разделяющей положительные и отрицательные значения.

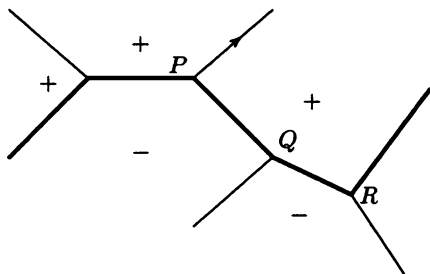
Неопределенные формы, не представляющие нуль: река

Именно такой будет форма $\begin{pmatrix} a & h \\ h & b \end{pmatrix}$, если ее определитель отрицателен, но не является противоположным к полному квадрату. Топокарта такой формы обязательно содержит ребро, непосредственно граничащее как с положительным, так и с отрицательным значениями (поскольку топокарта связна, мы можем пройти из области, где форма положительна, в область, где она отрицательна, а нуль форма не представляет). На практике, если нам дан супербазис S , все значения в котором положительны, мы можем добраться до такого ребра, идя против течения, как на рисунке.



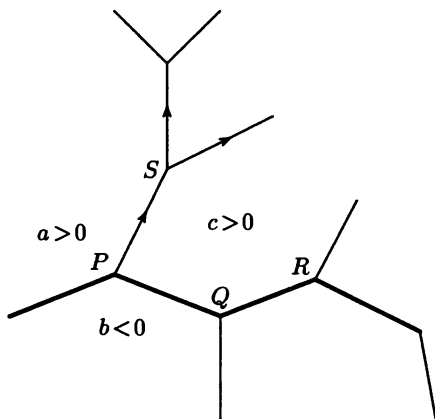
Изображая такие формы, мы будем использовать жирные линии для ребер, отделяющих положительные числа от отрицательных; такие ребра будем называть *участками реки*. Если a принимает отрицательное значение на супербазисе P , а b — положительное (т. е.

имеется участок реки), то третье значение c должно быть либо положительным, либо отрицательным, и тем самым из P выходит еще один участок реки (обозначим его PQ).



Итак, всякий участок реки стыкуется (на каждом из концов) с другим участком реки. Стало быть, получаем ломаную $PQR\dots$, разделяющую положительные и отрицательные числа; назовем ее *рекой*.

Лемма о возрастании показывает, что если удаляться от реки в положительную сторону, то значения будут все время увеличиваться (поскольку на идущем непосредственно от реки ребре, таком, как PS на рисунке ниже, будет стоять числовая отметка $h = c + a - b$, где $a > 0$, $b < 0$, $c > 0$). Аналогичным образом, если мы уходим от реки в другую сторону, то отрицательные значения продолжают уменьшаться.

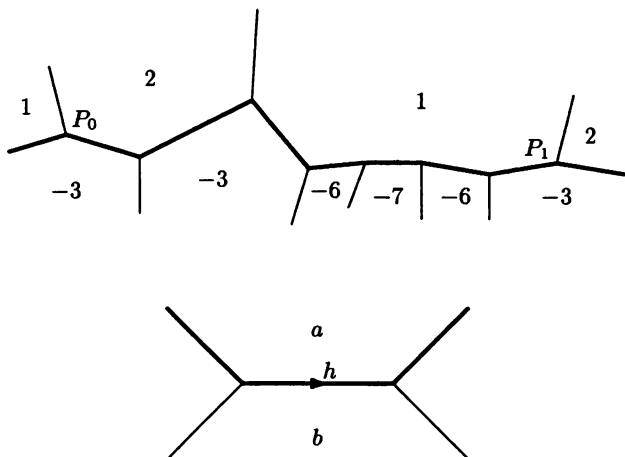


Иными словами: если удаляться от реки, то значения будут расти по абсолютной величине. Заметим, что отсюда вытекает единственность

реки: топокарта связна, а уходя от реки, можно встретить значения только одного знака, так что на другую реку мы никак не попадем.

У целых форм имеются периодические реки

Рассмотрим форму $x^2 + 6xy - 3y^2$; если идти вдоль реки, начав с супербазиса P_0 , окруженного числами 1, 2 и -3 , то мы наткнемся на другой супербазис P_1 , окруженный точно теми же числами. Мы покажем, что если коэффициенты a , h и b у $(\pm)$ -формы $ax^2 + hxy + by^2$ — целые числа, то река будет обязательно периодична, как в этом примере. Определитель данной формы равен $d = ab - (h/2)^2$.



Если базис соответствует участку реки, то ровно одно из двух чисел a и b будет отрицательно, так что ab отрицательно и $|d| = (h/2)^2 + |ab|$. Следовательно, $|h/2| < \sqrt{|d|}$ и $|ab| = |d| - (h/2)^2$, так что для значений a , b и h есть лишь конечное число возможностей. Однако же a , b и h определяют все прочие числовые отметки, а для вершин, лежащих на отрезках реки, имеется лишь конечное число возможных троек (a, b, h) . Поэтому у каких-то двух участков реки должно быть одно и то же окружение, и тем самым река периодична (поскольку значения a , b и h для любого участка реки определяют всю топокарту).

Так можем ли мы все-таки увидеть значения формы

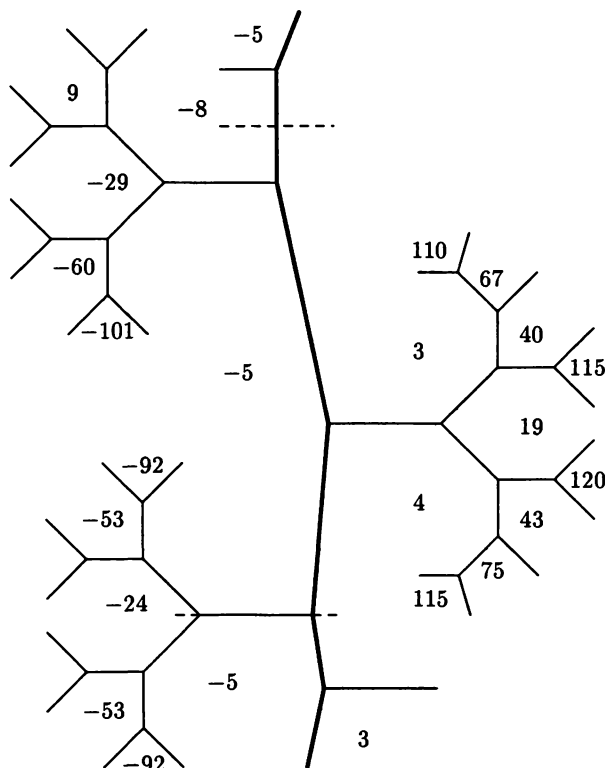
$$f(x, y) = 3x^2 + 6xy - 5y^2?$$

Для этой формы имеем $f(1, 0) = 3$, $f(0, 1) = -5$, $f(1, 1) = 4$. Итак, начнем с superbазиса с отметкой $(4, 3, -5)$ и отправимся в путешествие по реке.

На левом берегу этой замечательной реки мы видим, что отрицательные примитивные значения

$$-5, -8, -24, -29, -53, -60, -69, -92, -101, \dots$$

получаются, по существу, из деревьев двух видов (верхнего дерева и его образа при осевой симметрии).



Положительные примитивные значения

$$3, 4, 19, 40, 43, 67, 75, 110, 115, 120, \dots$$

примостились между ветвями деревьев, по существу, одного вида (и их зеркальными образами). Если еще умножить эти числа на

всевозможные квадраты, то мы получим все значения, принимаемые формой. В частности, мы видим, что диофантовы уравнения

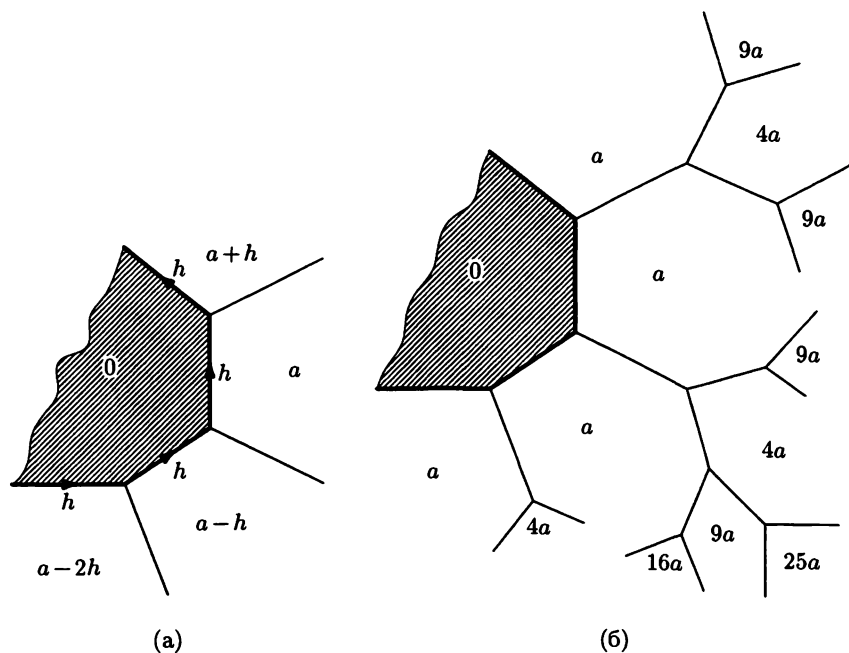
$$3x^2 + 6xy - 5y^2 = 7 \quad \text{и} \quad 3x^2 + 6xy - 5y^2 = -100$$

неразрешимы в целых числах.

Из того же рисунка видно, какова группа изометрий формы f (состоящая, по определению, из сохраняющих f линейных преобразований): это бесконечная диэдральная группа, порожденная отражениями от двух пунктирных прямых; одна из них делит пополам ребро, разделяющее области со значениями -8 и 3 , другая проходит между двумя областями со значением -5 .

Полуопределенные формы

Озеро — это область, соответствующая вектору, на котором форма представляет нуль. Из правила арифметической прогрессии вытекает, что значения на областях, граничащих с озером, образуют бесконечную арифметическую прогрессию, как на рис. (а).



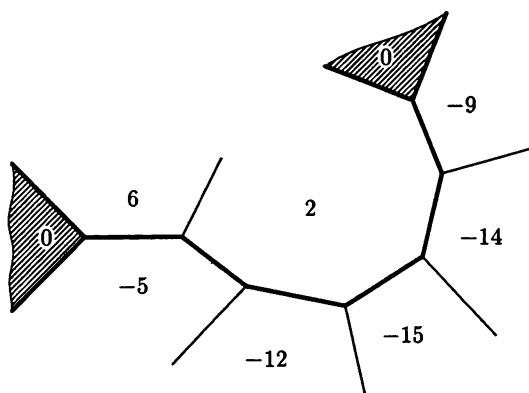
У 0-формы все значения равны нулю, и топокарта — это просто бесконечный набор озер. Далее, $(0+)$ -форма представляет только нуль и положительные числа. Для такой формы арифметическая прогрессия вокруг озера должна иметь нулевую разность (иначе она будет содержать отрицательное число). Стало быть, такая форма — это кратное формы x^2 , как на рис. (б). Аналогично обстоит дело с $(0-)$ -формами.

Неопределенные формы, представляющие нуль

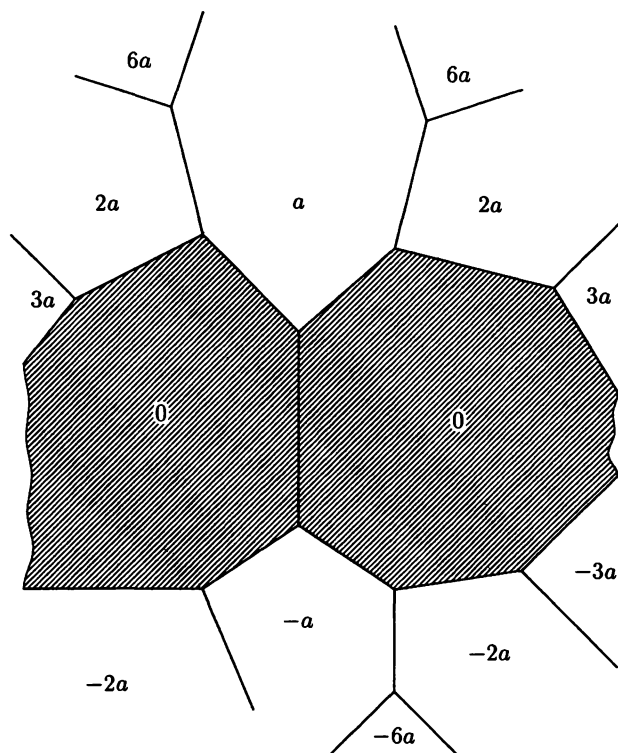
Перейдем наконец к интересному случаю $(0\pm)$ -форм, представляющих числа любого знака, в том числе нуль.

В этом случае у нас имеется озеро и непостоянная арифметическая прогрессия, члены которой в каком-то месте на берегу озера обязаны менять знак. Если знак меняется непосредственно с положительного на отрицательный, то это происходит на участке некоторой реки, вытекающей из озера. Для целой формы эта река обязана впадать в другое озеро, поскольку если бы она была бесконечной, то в силу нашего предыдущего рассуждения она была бы и периодической.

В примере ниже мы выходим из супербазиса с отметкой $(0, 6, -5)$ и доходим до супербазиса $(2, -9, 0)$.



В одном особом случае река имеет нулевую длину. Так происходит, если в арифметической прогрессии содержится число 0. Тогда форма эквивалентна xy , а на топокарте мы видим два озера, примыкающие друг к другу по общему участку берега — «дамбе», с одного конца от которой расположены положительные значения, а с другого — отрицательные.



Форма с дамбой

На прощанье

«Топокарта», описанная в этой лекции, доставляет очень яркое и наглядное представление всего множества значений квадратичной формы. Это представление полезно не только для понимания ситуации: теоремы, которые ранее доказывались алгебраически или арифметически, теперь становятся настолько очевидными, что и в доказательстве перестают нуждаться. Возможно, наиболее важной является следующая теорема, резюмирующая содержание этой лекции:

Теорема. Для данных целых чисел a , b , h и n вопрос о том, имеет ли диофантово уравнение

$$ax^2 + hxy + by^2 = n$$

решения в целых числах (x, y) , а также проблема нахождения таких решений алгоритмически разрешимы. Можно также эффективно решить задачу эквивалентности таких форм и найти их группы изометрий.

На этом завершается наша классификация целых бинарных квадратичных форм. На следующей лекции мы сосредоточим внимание на решетках высших размерностей, связанных с положительно определенными формами через свою функцию длины.

В дальнейшем мы еще вернемся к конормам, конормам и таинственным соотношениям между ними, наподобие $\gamma = \frac{a+b-c}{2}$.

ДОБАВЛЕНИЕ

$\mathrm{PSL}_2(\mathbb{Z})$ и дроби Фарея

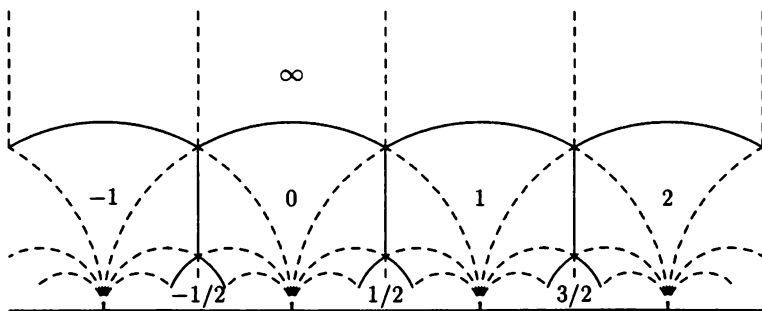
Вступление

В добавлениях к нашим лекциям мы будем рассматривать дополнительные подробности, затрагивать некоторые дополнительные темы или просто рассматривать идеи, изложенные в лекциях, в другом ракурсе. Время от времени мы будем предполагать, что читатель отчасти знаком с более стандартными изложениями предмета.

Предметом первой лекции была, по сути дела, группа $\mathrm{PSL}_2(\mathbb{Z})$, которую можно рассматривать как множество отображений верхней полуплоскости в себя, задаваемых формулами вида

$$z \mapsto \frac{az+b}{cz+d} \quad (a, b, c, d \in \mathbb{Z} : ad-bc=1).$$

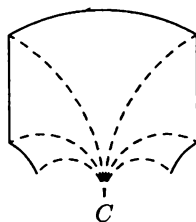
Интересно посмотреть, как наша топокарта изображается на верхней полуплоскости $H = \{x+iy : y > 0\}$.



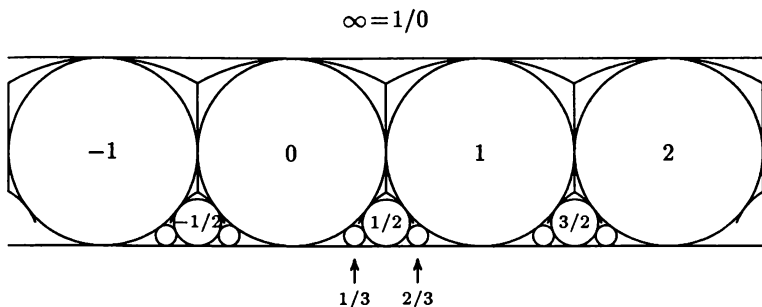
На рисунке H разбита на фундаментальные области группы $\mathrm{PSL}_2(\mathbb{Z}) = \Gamma$. Участки границ областей, изображенные сплошными линиями, образуют дерево, вершины и ребра которого соответствуют superbазисам и базисам для $\mathbb{Z}^2$. Каждая из областей на нашей топокарте состоит из «вееров» фундаментальных областей.

Изобразим один такой веер отдельно.

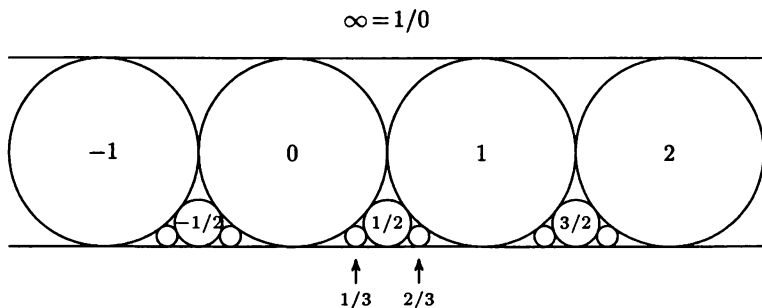
Веер, помеченный дробью p/q , есть область, соответствующая примитивному вектору $(p, q) \in \mathbb{Z}^2$. Оказывается, что центр C этого веера есть рациональное число p/q . Заметим, что поскольку $(-p)/(-q)$ — то же рациональное число, что и p/q , примитивные векторы $(-p, -q)$ и (p, q) автоматически соответствуют одному и тому же вееру.



Геометрия этой картины (иными словами, геометрия Лобачевского) доставляет дополнительную информацию. В вееры можно вписать окружности (см. рисунок):

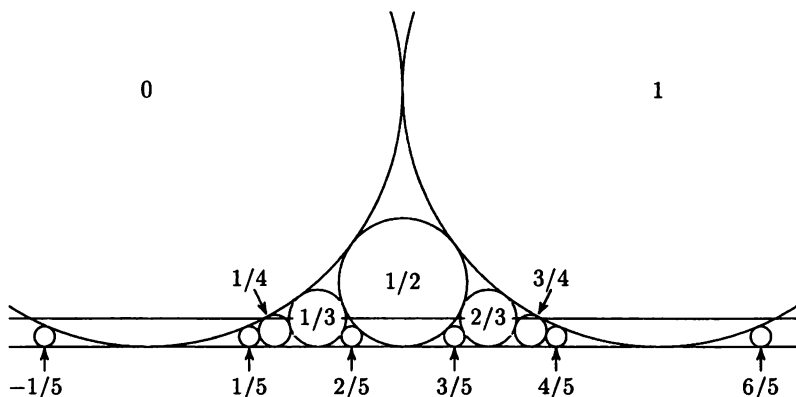


Изобразим эти окружности отдельно:

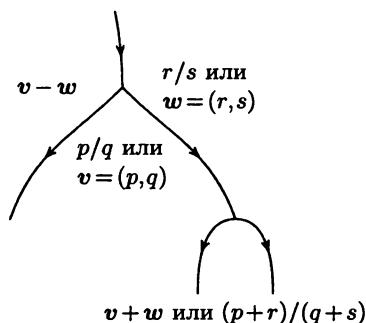


Эти окружности обычно называются *кругами Форда*. «Круг» Форда для $\infty = 1/0$ есть горизонтальная прямая, расположенная на высоте 1. Круг Форда, соответствующий числу p/q , есть окружность диаметром $1/q^2$, касающаяся действительной оси в точке p/q . Ряд Фарея

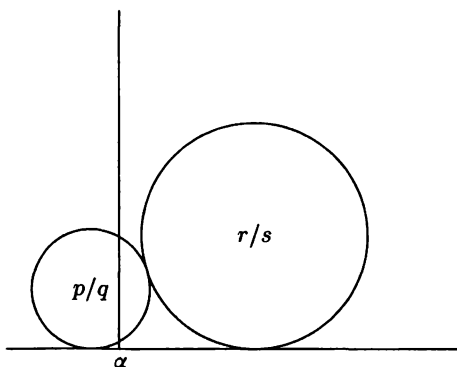
порядка d состоит из всех рациональных чисел со знаменателем, не превосходящим d . Эти числа соответствуют кругам Форда, пересекающим всякую горизонтальную прямую L , расположенную на высоте от $1/d^2$ до $1/(d+1)^2$. Например, для прямой, изображенной на нижеследующем рисунке, мы получаем ряд Фарея порядка 4, то есть $0/1, 1/4, 1/3, 1/2, 2/3, 3/4, 1/1$.



«Правило медианты» для рядов Фарея гласит, что первая дробь, появляющаяся между соседними дробями p/q и r/s при увеличении числа d , есть их *медианта* $(p+r)/(q+s)$. Смысл операции, сопоставляющей двум дробям их медианту, проясняется, если вспомнить, что дроби p/q соответствует вектор (p, q) . На топокарте эта ситуация выглядит так:



Из топокарты ясно, что если области по две стороны от некоторого ребра имеют отметки p/q и r/s , то отметки областей, примыкающих



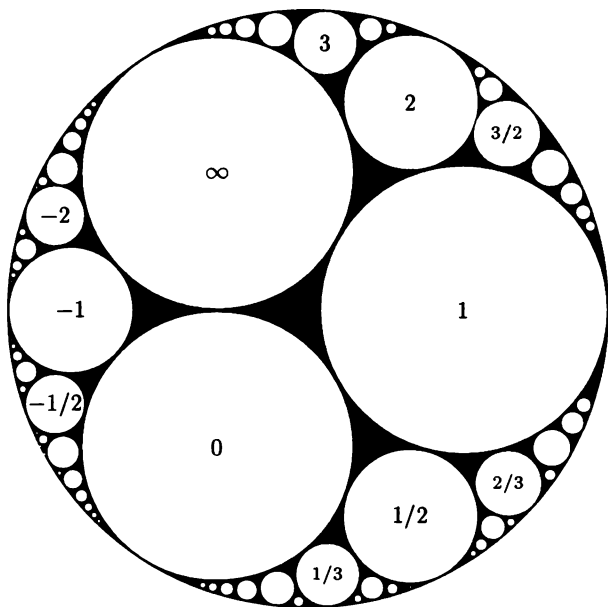
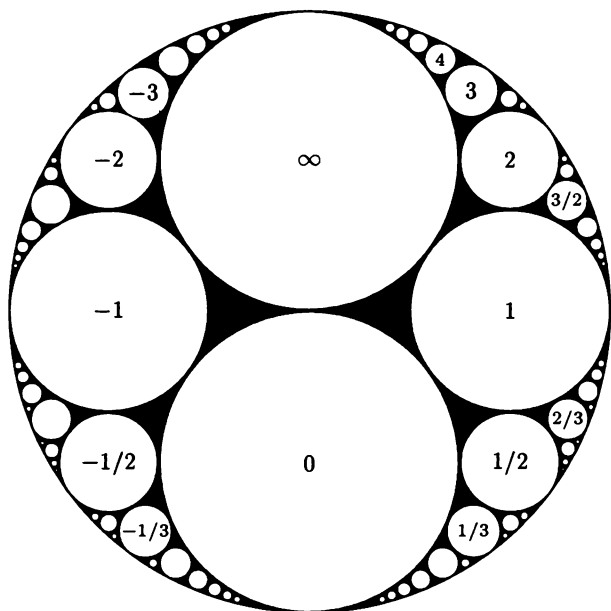
к концам этого ребра, будут $(p \pm r)/(q \pm s)$, так что первой из дробей, расположенных между p/q и r/s и имеющих больший знаменатель, будет и в самом деле их медианта $(p+r)/(q+s)$.

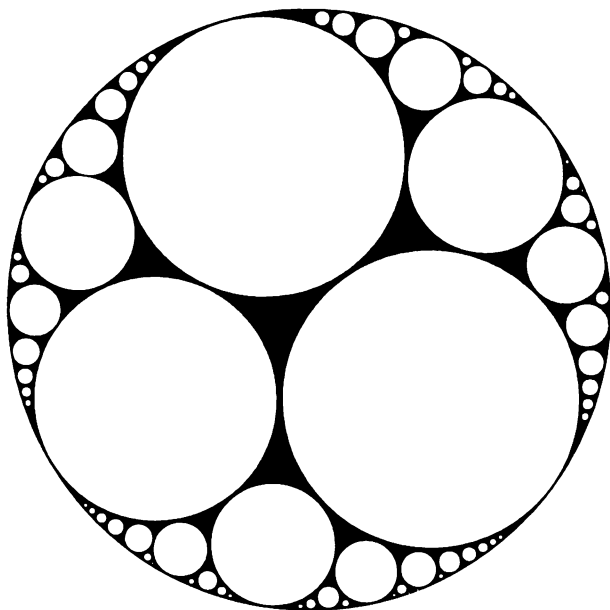
Некоторые теоремы о диофантовых приближениях также становятся очевидными. Например, для всякого иррационального действительного числа α существует бесконечно много рациональных чисел p/q , для которых $\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{2q^2}$.

В самом деле, если взять две соседние окружности p/q и r/s , у которых точки касания с $\mathbb{R}$ лежат по разные стороны от α , то вертикальная прямая, проходящая через α , должна пересекаться по крайней мере с одной из этих окружностей. Если эта прямая пересекает круг Форда для p/q , то $\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{2q^2}$.

Представить себе зрительно действие $SL_2(\mathbb{Z})$ и $GL_2(\mathbb{Z})$ на рациональных числах будет проще, если с помощью конформного отображения $z \mapsto \frac{z-i}{z+i}$ отобразить верхнюю полуплоскость на круг Пуанкаре, как на следующих трех рисунках. При этом круги Форда переходят в окружности, касающиеся границы. Группа $GL_2(\mathbb{Z})$ состоит из всех симметрий фигуры, а $SL_2(\mathbb{Z})$ — только из «вращений».

На первом из рисунков изображена подгруппа в $GL_2(\mathbb{Z})$ порядка 4, порожденная преобразованиями $t \mapsto -t$ и $t \mapsto 1/t$, а на втором — подгруппа порядка 6, порожденная $t \mapsto 1/t$ и $t \mapsto 1-t$. На самом деле $GL_2(\mathbb{Z})$ является свободным произведением этих двух подгрупп, амальгамированным по их общей подгруппе порядка 2. (Если говорить о подгруппах, состоящих из вращений, то $SL_2(\mathbb{Z})$ является свободным произведением подгрупп порядка 2 и 3.)





На первых двух рисунках изображены некоторые конечные подгруппы в $\mathrm{PGL}_2(\mathbb{Z})$, порожденные евклидовыми изометриями. На самом деле, однако, все симметрии представляются изометриями в геометрии Лобачевского. Группа $\mathrm{PGL}_2(\mathbb{Z})$ есть полная группа симметрий конфигурации окружностей бесконечного радиуса (они называются *орициклами*), образующей упаковку на плоскости Лобачевского. Для каждого рационального числа p/q имеется свой орицикл, касающийся границы (отождествляемой с действительной осью) в точке p/q . Мы уже видели эту ситуацию на рисунках, подчеркивающих наличие некоторых специальных подгрупп; орициклы, изображенные на нашем последнем рисунке, никакой особой симметрией не обладают.

Л Е К Ц И Я 2

Можно ли услышать форму решетки?

Вступление

Название этой лекции призвано напомнить знаменитый вопрос Марка Каца: «Можно ли услышать форму барабана?». Статья Каца [24] привлекла широкое внимание к важной старой задаче, впервые сформулированной около ста лет тому назад. На физическом языке ее можно сформулировать так: «Определяют ли основные частоты колебаний форму барабана?». Разумеется, эта задача является чисто математической: можно ли по собственным значениям лапласиана для задачи Дирихле в плоской области определить форму этой области?

Когда я думал, как озаглавить лекции, на которых основана эта книга, эта задача еще оставалась нерешенной, но к тому времени, когда эти лекции читались, появилось решение, принадлежащее Каролине Гордон, Веббу и Вольперту (Gordon C., Webb D., Wolpert S.), которые, в свою очередь, пользовались предшествовавшими работами Сунады и Бузера (Sunada T., Buser P.).

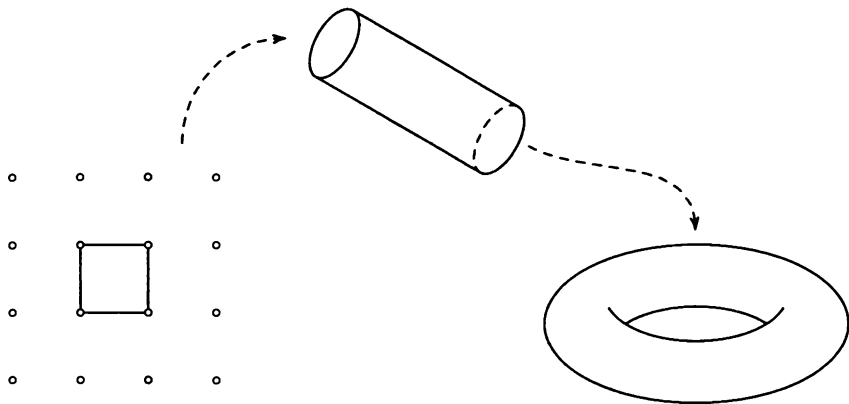
Узнать, что классическая задача решена, всегда радостно, а в данном случае решение можно изложить особенно просто, так что, хотя это и слабо связано с основной темой данных лекций, мы приведем здесь простое решение задачи Каца.

То, что решение искали столь долго, было, возможно, и к лучшему, поскольку в процессе работы над задачей было создано много интересного. В частности, можно рассматривать эту задачу для произвольных римановых многообразий (поверхностей произвольной размерности с произвольной метрикой). Вскоре после лекции Каца Дж. Милнор нашел первые контрпримеры к задаче в этой обобщенной постановке; именно, он построил два 16-мерных тора, «звучащих одинаково» (в том смысле, что собственные значения их лапласианов совпадают), хотя форма этих торов разная [3].

Изоспектральные решетки

Какое все это имеет отношение к решеткам? Решетка $L \subset \mathbb{R}^n$ — это множество целых линейных комбинаций n линейно независимых

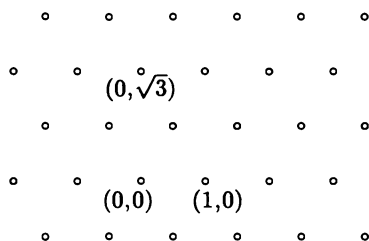
векторов $v_1, v_2, \dots, v_n$. Если в евклидовом пространстве дана решетка, то можно «свернуть» пространство вокруг нее и получить фактор-многообразие. Например, если рассмотреть $\mathbb{Z}^2$ в евклидовом пространстве $\mathbb{R}^2$ и отождествить всякие две точки в $\mathbb{R}^2$, разность которых принадлежит решетке $\mathbb{Z}^2$, то факторпространство $\mathbb{R}^2/\mathbb{Z}^2$ будет (как читатель, вероятно, знает) тором. Аналогичным образом можно строить многомерные торы как факторы других евклидовых пространств по содержащимся в них решеткам.



Эти торы являются римановыми многообразиями, поскольку они «наследуют» метрику евклидова пространства. Так вот, в $\mathbb{R}^{16}$ имеются две неизометричные решетки, а именно $E_8 \oplus E_8$ и D_{16}^+ , для которых торы, являющиеся факторами по ним, *изоспектральны*, то есть «звучат одинаково». Так получается потому, что, как оказывается, спектр фактора по решетке полностью определяется количеством векторов решетки с данной длиной [19], и тем самым так называемой *тэта-функцией решетки*:

$$\Theta_L(q) = \sum_l a_l q^l, \quad q = e^{2\pi iz},$$

где a_l — число векторов в L , у которых квадрат длины равен l . Имея в виду этот результат, естественно сказать, что свойство решеток является *слышимым*, если оно определяется тэта-функцией решетки. Например, в шестиугольной решетке имеется один вектор v , у которого квадрат длины (или *норма*) $N(v)$ равен нулю, шесть векторов с нормой 1, шесть с нормой 3, шесть с нормой 4, двенадцать



с нормой 7 и т. д., так что тэта-функция этой решетки имеет вид

$$1 + 6q + 6q^3 + 6q^4 + 12q^7 + \dots$$

Основная задача этой главы — выяснить, в каких размерностях можно найти две неизометричные решетки с одинаковой тэта-функцией, или, равносильно, с одинаковым количеством векторов каждой данной длины. Это чисто геометрическая задача, хоть возникла она и в аналитическом контексте; в следующем разделе мы увидим, как в рассуждении Милнора используются аналитические идеи.

Пример Милнора

Известно, что тэта-функции четных унимодулярных решеток (т. е. решеток, в которых все квадраты длин являются четными числами и в которых на единицу объема приходится одна точка) имеют чрезвычайно специальный вид: эти функции являются *модулярными формами* относительно полной модулярной группы $\mathrm{PSL}_2(\mathbb{Z}) = \Gamma$. Это означает, что

$$\Theta\left(\frac{az+b}{cz+d}\right) = (cz+d)^{n/2} \Theta(z)$$

для всякой целочисленной (2×2) -матрицы $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ с определителем 1; здесь n — размерность решетки. Оказывается, что в 16-мерном случае такая функция единственна с точностью до постоянного множителя: это функция

$$\Theta(q) = 1 + 480 \sum_n \sigma_7(n) q^{2n},$$

где $\sigma_7(n)$ — сумма седьмых степеней делителей числа n . Стало быть, у всякой 16-мерной четной унимодулярной решетки тэта-функция должна быть именно такова (поскольку коэффициент при q^0 обязан

быть равен единице). Витт показал (см. [50]), что существуют ровно две четные унимодулярные 16-мерные решетки; в наши дни они обычно обозначаются через $E_8 \oplus E_8$ и D_{16}^+ . Значит, два найденных Милнром 16-мерных тора, а именно,

$$\mathbb{R}^{16}/E_8 \oplus E_8 \quad \text{и} \quad \mathbb{R}^{16}/D_{16}^+,$$

изоспектральны. Тем самым форму 16-мерного многообразия услышать невозможно. Рассматривая другие пары решеток с совпадающими тэта-функциями, можно построить изоспектральные торы в других размерностях. В нескольких последующих разделах мы опишем некоторые из использующихся при этом решеток.

16-мерные решетки

Решетка корней D_n состоит из векторов $(x_1, x_2, \dots, x_n)$, для которых x_i — целые числа с четной суммой. n -мерной ромбической упаковкой D_n^+ называется объединение решетки D_n и ее смежного класса $D_n + \left(\frac{1}{2}, \frac{1}{2}, \dots, \frac{1}{2}\right)$. Ромбическая упаковка D_3^+ — это кристаллическая решетка алмаза. Множество D_n^+ может быть решеткой только при четном n , поскольку при нечетном n вектор $\left(\frac{1}{2}, \frac{1}{2}, \dots, \frac{1}{2}\right) + \left(\frac{1}{2}, \frac{1}{2}, \dots, \frac{1}{2}\right) = (1, 1, \dots, 1)$ не лежит в D_n^+ . Если n четно, то D_n^+ является решеткой, и эта решетка является четной унимодулярной, если n делится на 8. В общем случае у D_n^+ имеются только очевидные симметрии: мы можем переставлять координаты произвольным образом, и мы можем одновременно менять знак у четного числа координат. Если, однако, $n=8$, то симметрий у решетки будет больше, так что в этом случае имеет смысл обозначать ее по-другому: не D_8^+ , а E_8 (это решетка корней алгебры Ли типа E_8). Две изоспектральные решетки в размерности 16 суть $E_8 \oplus E_8$ и D_{16}^+ .

В конце этой книги мы докажем, что четные унимодулярные решетки существуют только в размерностях, кратных 8. В размерности 8 есть только решетка E_8^+ , а в размерности 16 — две вышеописанные решетки $E_8 \oplus E_8$ и D_{16}^+ . В добавлении к этой лекции мы обсудим случай размерности 24.

Тэта-функции решеток D_n и D_n^+ выписать легко. Три якобиевых тэта-константы определяются следующим образом:

$$\vartheta_3 = \sum q^{k^2}, \quad \vartheta_4 = \sum (-1)^k q^{k^2}, \quad \vartheta_2 = \sum q^{(k+1/2)^2};$$

суммирование распространено на все целые числа k , причем $q = \exp(2\pi iz)$.

Теперь заметим, что тэта-функция кубической решетки I_n (или $\mathbb{Z}^n$), состоящей из всех векторов $(x_1, x_2, \dots, x_n)$ с целыми x_i , есть ϑ_3^n , и что ϑ_4^n получится из тэта-функции той же решетки, если изменить знак у всех слагаемых, соответствующих векторам с нечетной нормой. Следовательно, тэта-функция решетки D_n есть $\frac{1}{2}(\vartheta_3^n + \vartheta_4^n)$.

Аналогичным образом убеждаемся, что тэта-функции множеств

$$I_n + \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \dots\right) \quad \text{и} \quad D_n + \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \dots\right)$$

суть ϑ_2^n и $\frac{1}{2}\vartheta_2^n$ соответственно. Стало быть, тэта-функция D_n^+ есть $\frac{1}{2}(\vartheta_2^n + \vartheta_3^n + \vartheta_4^n)$.

Далее, решетка D_4^+ порождена четырьмя попарно ортогональными векторами

$$\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right), \left(\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}\right), \left(\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, -\frac{1}{2}\right), \left(\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}\right);$$

стало быть, она изоморфна I_4 , так что, рассмотрев тэта-функции, получаем, что

$$\vartheta_3^4 = \frac{1}{2}(\vartheta_2^4 + \vartheta_3^4 + \vartheta_4^4),$$

или

$$\vartheta_3^4 = \vartheta_2^4 + \vartheta_4^4;$$

это соотношение получил Якоби.

Теперь читатель сможет самостоятельно убедиться, что тэта-функции

$$\frac{1}{2}(\vartheta_2^{16} + \vartheta_3^{16} + \vartheta_4^{16}) \quad \text{и} \quad \left(\frac{1}{2}(\vartheta_2^8 + \vartheta_3^8 + \vartheta_4^8)\right)^2,$$

отвечающие решеткам D_{16}^+ и $E_8 \oplus E_8$ соответственно, совпадают; для этого нужно исключить ϑ_3 из обоих выражений, пользуясь соотношением Якоби.

12-мерные и 8-мерные примеры

Вскоре после появления милноровского примера Кнезер [27] снизил размерность с 16 до 12. Решетки D_{16}^+ и $E_8 \oplus E_8$ не только имеют

одинаковое число векторов каждой данной длины; они также имеют одинаковое количество двумерных подрешеток каждого заданного типа. На самом деле для каждой подрешетки размерности, меньшей 4, две эти решетки содержат по одинаковому количеству таких подрешеток, так что они изоспектральны в очень сильном смысле. Беря подрешетки, ортогональные к подрешеткам, изоморфным D_4 , Кнезер нашел изоспектральную пару двенадцатимерных решеток, а именно D_{12} и $E_8 \oplus D_4$.

Некоторое время спустя Китаока [26] понизил размерность и далее, построив две изоспектральные решетки размерности 8 (с определителем 81).

У п р а ж н е н и е. Найдите тэта-функции решеток D_{12} и $E_8 \oplus D_4$ и воспользуйтесь соотношением Якоби, чтобы убедиться, что они совпадают.

Шестимерные кубическая и изокубическая решетки

Нил Слоун очень любит два описанных ниже кода. Цифры в таблицах — целые числа по модулю 2 (так что C_1 и C_2 — двоичные коды). Каждый из кодов C_1 и C_2 состоит из восьми символов:

C_1	C_2
0 0 0 0 0 0	0 0 0 0 0 0
1 1 0 0 0 0	1 0 1 0 0 0
0 0 1 1 0 0	0 0 1 0 1 0
0 0 0 0 1 1	1 0 0 0 1 0
0 0 1 1 1 1	0 1 0 1 1 1
1 1 0 0 1 1	1 1 0 1 0 1
1 1 1 1 0 0	0 1 1 1 0 1
1 1 1 1 1 1	1 1 1 1 1 1

Эти коды линейны: сумма двух слов в каждом из этих кодов также принадлежит этому коду. Более того, у них совпадает распределение весов: в них есть одно слово веса 0, три слова веса 2, три слова веса 4 и одно слово веса 6 (*весом* слова называется число его ненулевых элементов). Тем не менее эти изоспектральные коды неизоморфны, поскольку сумма слов веса 2 в C_1 есть 1 1 1 1 1 1, а в C_2 эта сумма есть 0 0 0 0 0 0.

Теперь по этим кодам мы можем построить неизометричные изоспектральные решетки L_1 и L_2 ; для этого определим L_i как множество тех векторов, редукция которых по модулю 2 лежит в C_i .

(Какие решетки называются *неизометричными*, будет ясно в конце этого раздела.)

Имеется простое взаимно однозначное соответствие между C_1 и C_2 , сохраняющее веса: если слово из кода C_1 содержит ровно два элемента некоторой данной четности, то второй из этих элементов надо поменять местами со следующим в строке (за шестым элементом следует первый). Вот пример:

$$(1, 1, 0, 0, 0, 0) \rightarrow (1, 0, 1, 0, 0, 0).$$

В точности то же правило доставляет сохраняющее длины соответствие между векторами решеток L_1 и L_2 :

$$(3, 5, 0, 2, 4, 6) \rightarrow (3, 0, 5, 2, 4, 6).$$

Векторы, в которых все координаты имеют одну и ту же четность, остаются на месте.

Из этого соответствия ясно, что решетки L_1 и L_2 имеют одинаковое количество векторов каждой заданной длины.

Замечательно, что L_1 получается изменением масштаба из шестимерной кубической решетки! В самом деле, L_1 порождается своими кратчайшими векторами, а именно векторами

$$\begin{aligned} v_1 &= (1, 1, 0, 0, 0, 0), & v_2 &= (1, -1, 0, 0, 0, 0), & v_3 &= (0, 0, 1, 1, 0, 0), \\ v_4 &= (0, 0, 1, -1, 0, 0), & v_5 &= (0, 0, 0, 0, 1, 1), & v_6 &= (0, 0, 0, 0, 1, -1) \end{aligned}$$

и противоположными к ним. Поскольку $v_1, v_2, \dots, v_6$ — попарно ортогональные векторы одинаковой длины, решетка L_1 действительно геометрически подобна кубической. В решетке L_2 , которую мы будем называть *изокубической*, кратчайшие векторы суть

$$\begin{aligned} w_1 &= (1, 0, 1, 0, 0, 0), & w_2 &= (1, 0, -1, 0, 0, 0), & w_3 &= (0, 0, 1, 0, 1, 0), \\ w_4 &= (0, 0, 1, 0, -1, 0), & w_5 &= (1, 0, 0, 0, 1, 0), & w_6 &= (1, 0, 0, 0, -1, 0) \end{aligned}$$

и противоположные к ним.

Заметим, что $w_2 \cdot w_3 = -1$, и w_2 и w_3 не ортогональны, так что решетка L_1 не изометрична решетке L_2 . Значит, в размерности 6 (и выше) невозможно даже услышать, имеет ли решетка такую же форму, как кубическая.

Пятимерные примеры

В добавлении к этой лекции мы докажем, что кубичность решетки является слышимой в размерностях 5 и ниже. Тем не менее, форма

решетки может слышимой и не быть: если в вышеописанных кубической и исокубической решетках взять подрешетки, состоящие из векторов, ортогональных к $(1, 1, 1, 1, 1, 1)$, то мы получим две различные, но одинаково звучащие пятимерные решетки.

Кстати, эти примеры отнюдь не являются изолированными. В определение этих решеток можно ввести варьирующиеся параметры и получить бесконечные семейства изоспектральных решеток.

Последние новости: четырехмерные примеры

В дальнейшем, ближе к нашему времени, Шиман [38] нашел с помощью компьютера некоторые четырехмерные примеры. В тот момент, когда читались эти лекции, структура этих примеров была совершенно непонятна. Однако же, в результате изучения первого из этих примеров Нил Слоун и я нашли особенно простое четырехпараметрическое семейство примеров, которые мы назвали *тетрапешетками* (tetralattices). Это название призвано указывать на связь с *тетракодом* — тернарным кодом длины 9, состоящим из следующих слов:

$$(0, 0, 0, 0), \quad \pm(0, 1, 1, 1), \quad \pm(1, 0, 1, -1), \\ \pm(1, -1, 0, 1), \quad \pm(1, 1, -1, 0).$$

Пусть e_a, e_b, e_c и e_d — четыре попарно ортогональных вектора различных длин, для которых

$$e_a \cdot e_a = \frac{1}{12}a, \quad e_b \cdot e_b = \frac{1}{12}b, \quad e_c \cdot e_c = \frac{1}{12}c, \quad e_d \cdot e_d = \frac{1}{12}d.$$

Будем писать $[w, x, y, z]$ вместо $we_a + xe_b + ye_c + ze_d$; определим решетку $L^+ = L^+(a, b, c, d)$ как решетку, порожденную векторами

$$v_1^+ = [+3, -1, -1, -1], \quad v_2^+ = [+1, +3, +1, -1], \\ v_3^+ = [+1, -1, +3, +1], \quad v_4^+ = [+1, +1, -1, +3].$$

Определим также решетку $L^- = L^-(a, b, c, d)$, заменив $+3$ на -3 в определении L^+ ; получится решетка, порожденная векторами

$$v_1^- = [-3, -1, -1, -1], \quad v_2^- = [+1, -3, +1, -1], \\ v_3^- = [+1, -1, -3, +1], \quad v_4^- = [+1, +1, -1, -3].$$

При редукции любого вектора любой тетрарешетки по модулю 3 мы получим слово, принадлежащее тетракоду, и всякое ненулевое слово из тетракода получается редукцией по модулю 3 из одного из четырех базисных векторов или противоположных к ним. Например, $v_1^+ + v_2^+ = [4, 2, 0, -2] \equiv [1, -1, 0, 1] \pmod{3}$, и это слово из тетракода получается редукцией по модулю 3 из v_3^+ .

Ядром этого отображения из L^+ на тетракод является подрешетка индекса 9, которую мы обозначим M^+ . Решетка M^+ состоит из векторов, все координаты которых делятся на 3. Например,

$$v_1^+ + v_2^+ - v_3^+ = [3, 3, -3, -3] \in M^+.$$

Легко проверить, что решетка M^+ порождается теми из векторов $[\pm 3, \pm 3, \pm 3, \pm 3]$, у которых четно число знаков «-» (таких векторов восемь штук). Точно так же решетка L^- содержит подрешетку M^- индекса 9, порожденную векторами $[\pm 3, \pm 3, \pm 3, \pm 3]$ с нечетным числом знаков «-».

Представители смежных классов L^ε по M^ε суть

$$0, \pm v_1^\varepsilon, \pm v_2^\varepsilon, \pm v_3^\varepsilon, \pm v_4^\varepsilon.$$

Далее, ясно, что решетки M^+ и M^- изометричны (изометрия получится, если изменить знак какой-нибудь одной из координат). Аналогичным образом решетки $M^+ + v_i^+$ и $M^+ - v_i^+$ изометричны решеткам $M^- + v_i^-$ и $M^- - v_i^-$. Объединив эти наблюдения, можно получить простое правило, дающее взаимно однозначное и сохраняющее длины соответствие между L^+ и L^- : *поменять знак первой из делящихся на 3 координат*. Многие из примеров Шимана являются частными случаями этой конструкции; его первая пара из спектральных решеток с определителем $1729 = 7 \times 13 \times 19$ есть $L^+(1, 7, 13, 19)$ и $L^-(1, 7, 13, 19)$. Тем не менее, имеются и другие четырехмерные примеры, не входящие в это семейство.

Мы считаем, что если числа a, b, c и d все различны, то решетки $L^+(a, b, c, d)$ и $L^-(a, b, c, d)$ неизометричны. Это легко проверить для целых a, b, c и d в случае, когда определитель $abcd$ меньше, чем 10^4 . Найдем, например, все решения уравнений $x^2 + 7y^2 + 13z^2 + 19w^2 = 48$ и $x^2 + 7y^2 + 13z^2 + 19w^2 = 96$, чтобы найти все возможные векторы с нормами 4 и 8 в $L^+(1, 7, 13, 19)$ и $L^-(1, 7, 13, 19)$. Оказывается, что $\pm v_1^+$ и $\pm v_2^+$ суть единственные векторы с нормами 4 и 8 соответственно в $L^+(1, 7, 13, 19)$, а $\pm v_1^-$ и $\pm v_2^-$ суть единственные такие векторы в $L^-(1, 7, 13, 19)$. Поскольку $v_1^+ \cdot v_2^+ = 1$, а $v_1^- \cdot v_2^- = 2$, эти решетки не могут быть изометричны. Дальнейшие подробности см. в [8].

Экстренное сообщение! Что в размерностях 2 и 3?

Если нам известны длины всех векторов решетки, то мы можем узнать и длины примитивных векторов, поскольку вклад в тэта-функцию решетки кратных примитивного вектора v с нормой n , т. е.

$$\pm v, \pm 2v, \pm 3v, \pm 4v, \dots,$$

есть

$$2q^n + 2q^{4n} + 2q^{9n} + 2q^{16n} + \dots$$

Отсюда можно вывести, что если тэта-функция есть $1 + 2 \sum a_n q^n$, то число пар $\pm v$ примитивных векторов с нормой n есть

$$\sum_{d|n} \mu(d) a_{n/d^2},$$

где $\mu(d)$ — функция Мёбиуса.

Однако же в первой лекции мы показали, что для двумерной решетки нормы трех кратчайших примитивных векторов суть значения соответствующей квадратичной формы на некотором супербазисе. Следовательно, в двумерном случае тэта-функция решетки определяет ее размер.

Вопрос о том, так ли это в трехмерном случае, оставался открытым в течение многих лет. Когда эта книга писалась, мы получили сообщение о том, что Шиман показал (с помощью обширных компьютерных вычислений), что в трехмерном случае форма решетки слышима, так что и в этой размерности примеров нет.

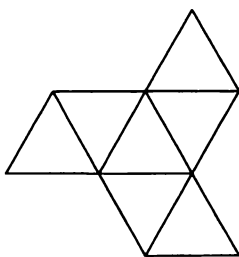
Нет, форму барабана услышать нельзя!

Хотя два тора, получаемые из двух разных двумерных решеток, не могут звучать одинаково, существуют две одинаково звучащие многоугольные области. Мы дадим очень простое доказательство этого факта, рассчитанное на читателей, понимающих используемые термины.

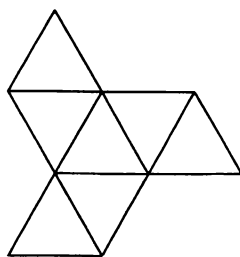
Когда в 1965 году Марк Кац спросил, можно ли услышать форму барабана, он спрашивал, существуют ли две неизометричные изоспектральные плоские области. В течение последующих 25 лет было найдено множество примеров изоспектральных многообразий, чья размерность, топология и свойства кривизны постепенно приближались к соответствующим свойствам плоскости. Недавно Гордон, Вебб и Вольперт привели, наконец, примеры с плоскими областями. В этом

разделе, содержание которого основано на [2], мы приводим простой пример вместе с принадлежащим Бузеру простым доказательством.

Рассмотрим две области (а) и (б), имеющие форму пропеллера:

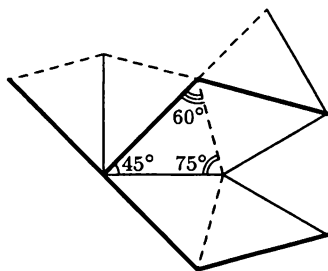


(а)

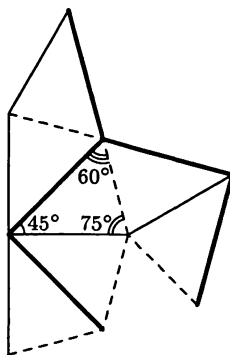


(б)

Наши примеры получаются из (а) и (б) заменой равносторонних треугольников на остроугольные разносторонние (одинаковой формы) таким образом, чтобы всякие два треугольника, имеющие общую сторону, были симметричны относительно этой стороны, как на рисунках (в) и (г) ниже (где приведены треугольники с углами 45° , 60° и 75°). По ходу доказательства мы увидим, что треугольники действи-

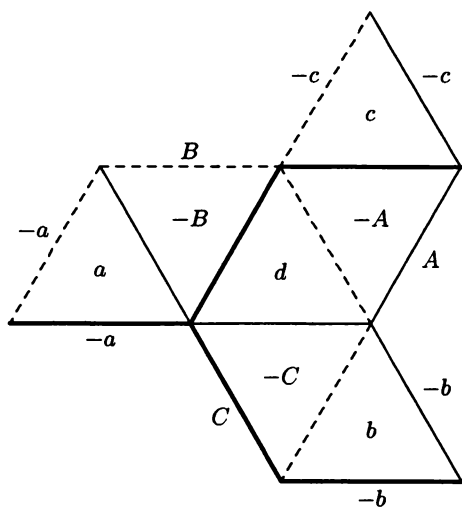


(в)



(г)

тельно являются разносторонними, но на рисунках мы будем изображать их в виде равносторонних треугольников, чтобы отразить симметрию рассуждения, и только три разных стороны треугольника будем изображать разными линиями.

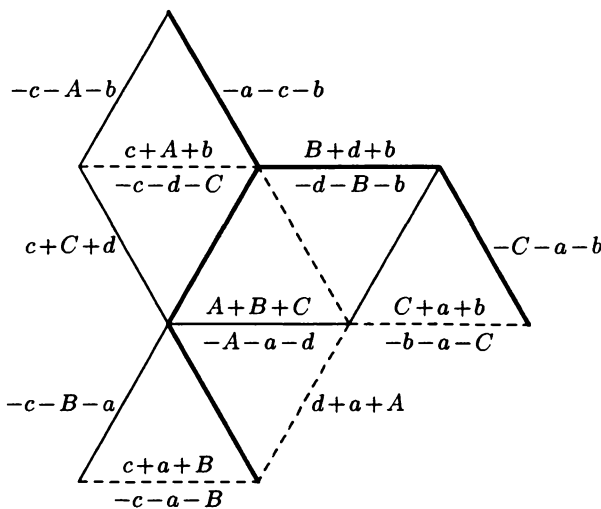


(д)

Пусть теперь λ — произвольное действительное число и $\varphi = \varphi(x)$ — произвольная собственная функция задачи Дирихле для левостороннего пропеллера, изображенного на рис. (д); пусть соответствующее собственное значение равно λ . Обозначим ограничения φ на семь треугольников, составляющих этот пропеллер, через $a, b, c, d, -A, -B$ и $-C$.

Граничное условие задачи Дирихле состоит в том, что φ должна быть нулем на каждом из граничных отрезков. Ввиду принципа симметрии это эквивалентно тому, что φ меняет знак при ее продолжении (как гладкой собственной функции) через любой граничный отрезок, что также показано на рис. (д).

На рис. (е) мы показываем, как, исходя из φ , найти другую собственную функцию с собственным значением λ , на сей раз для правостороннего пропеллера. В центральный треугольник поместим функцию $A(x) + B(x) + C(x)$. Из (д) видно, что функции $A(x), B(x)$ и $C(x)$ непрерывно продолжаются через пунктирные линии до функций $-d(x), -B(x)$ и $-b(x)$ соответственно, так что их сумма, как показано на рисунке, продолжается до $-[d(x) + B(x) + b(x)]$. Читателю предлагается аналогичным образом проверить, что эта функция продолжается через толстую сплошную линию до функции $B(x) + d(x) + b(x)$



(e)

(противоположной ей), а через тонкую сплошную линию — до функции $C(x) + a(x) + b(x)$, которая, в свою очередь, продолжается через толстую или пунктирную линию до противоположной себе, как это показано на рис. (e).

Этих результатов (и их аналогов, получаемых с помощью симметрии) достаточно, чтобы показать, что функция на рис. (e) есть собственная функция с собственным значением λ , обращающаяся в нуль на каждом граничном отрезке правостороннего пропеллера.

Итак, мы определили линейное отображение из собственного подпространства для левостороннего пропеллера, соответствующего собственному значению λ , в аналогичное подпространство для правостороннего пропеллера; поскольку можно определить и обратное отображение, получаем, что размерности этих собственных подпространств равны, так что два пропеллера изоспектральны относительно задачи Дирихле. Они также изоспектральны для задачи Неймана (производная по нормали к границе должна обращаться в нуль на границе): доказательство аналогично приведенному выше, но каждый знак «-» надо заменить на «+».

Доказательства такого типа, использующие принцип симметрии, принадлежат Петеру Бузеру. Наши «пропеллеры», возможно, являются простейшими известными примерами.

Что можно услышать у решетки?

Мы назвали *слышимыми* те свойства решетки, которые определяются ее тэта-функцией

$$\vartheta_L(z) = \sum_{v \in L} q^{N(v)}, \quad q = e^{2\pi iz},$$

где $N(v)$ — квадрат длины v . Теперь заметим, что геометрически определитель d решетки — квадрат объема фундаментального параллелепипеда. Отсюда следует, что число точек решетки внутри большого шара примерно равно объему шара, деленному на $\sqrt{d}$, так что (поскольку для всякого R мы можем «услышать» число таких v , что $N(v) < R$):

Определитель решетки является слышимым.

Двойственная решетка L^* определяется как множество векторов в вещественном векторном пространстве, порожденном L , обладающих тем свойством, что их внутреннее произведение со всяким вектором из L является целым числом. Имеется следующая формула Якоби, связывающая тэта-функции для L и L^* :

$$\vartheta_{L^*}(z) = (\det L)^{1/2} \left(\frac{i}{z}\right)^{n/2} \vartheta_L\left(-\frac{1}{z}\right);$$

из этой формулы следует, что

Тэта-функция решетки L^ слышима.*

Гауссовы средние

Имеются и другие очень важные инварианты, являющиеся слышимыми. Если f — квадратичная форма, соответствующая L , то ее *гауссово среднее* равно, по определению, среднему значению чисел

$$e^{2\pi i N(v)},$$

взятому по всем $v \in L^*$, где L^* — двойственная решетка.¹

Поскольку речь идет о среднем значении бесконечного множества комплексных чисел, при формальном определении тут требуется известная аккуратность. Для целочисленных решеток, однако, проблем не возникает, поскольку указанные комплексные числа зависят от точки решетки периодически. Это происходит потому, что если решетка

¹ В лекции 4 мы слегка изменим это определение.

L целочисленна, то она является подрешеткой в L^* , и нормы векторов v и $v+w$ из L^* , разность которых есть вектор $w \in L$, отличаются на целое число $2(v, w) + N(w)$, так что слагаемые в гауссовом среднем, отвечающие v и $v+w$, совпадают. Стало быть, гауссово среднее для целочисленной решетки — то же самое, что среднее значение чисел

$$e^{2\pi i N(v)},$$

взятое по множеству векторов v , являющихся представителями элементов двойственной факторгруппы L^*/L , то есть некоторой конечной группы.

Прямая сумма $f \oplus g$ квадратичных форм f и g с матрицами M и N есть квадратичная форма с матрицей

$$\begin{pmatrix} M & 0 \\ 0 & N \end{pmatrix}.$$

Полезным свойством гауссовых средних является тот факт, что гауссово среднее формы $f \oplus g$ есть произведение гауссовых средних для f и g . Благодаря этому нам будет легко посчитать гауссово среднее для форм вида

$$\text{diag}[1, 1, \dots, p, p, \dots, p^2, \dots] \quad (p \text{ нечетно}).$$

(В дальнейшем мы будем опускать diag в таких обозначениях.) Ввиду мультипликативности гауссовых средних нам достаточно посчитать гауссово среднее для одномерной формы $[p^k]$. Разумеется, гауссово среднее для формы $[1]$ равно 1.

Согласно знаменитой теореме Гаусса, значение суммы

$$\sum_{0 \leq n < p} e^{2\pi i n^2/p}$$

равно $\sqrt{p}$ или $i\sqrt{p}$, в зависимости от того, сравнимо p с 1 или -1 по модулю 4. Поскольку гауссово среднее для $[p]$ есть среднее значение слагаемых в этой сумме, среднее равно $(1 \text{ или } i)/\sqrt{p}$.

Чтобы увидеть, что происходит со степенями p , посмотрим на гауссово среднее для $[9]$. Поскольку квадраты чисел 0, 1, 2, 3, 4, 5, 6, 7, 8 равны 0, 1, 4, 0, 7, 7, 0, 4, 1 по модулю 9, гауссово среднее есть среднее чисел

$$1, \varepsilon, \varepsilon^4, 1, \varepsilon^7, \varepsilon^7, 1, \varepsilon^4, \varepsilon \quad (\varepsilon = e^{2\pi i/9}),$$

и это среднее равно $(1+1+1)/9=1/3$, поскольку

$$\varepsilon + \varepsilon^4 + \varepsilon^7 = \varepsilon(1 + \varepsilon^3 + \varepsilon^6) = 0.$$

Аналогичным образом находим, что гауссово среднее для $[p^{2k}]$ есть $1/p^k$, а гауссово среднее для $[p^{2k+1}]$ есть $(1 \text{ или } i)/p^{k+1/2}$, а точнее говоря — среднее для $[p]$, деленное на p^k .

Соберем полученные результаты:

Теорема. Гауссово среднее формы f , являющейся суммой n экземпляров формы $[1]$, n' экземпляров формы $[p]$, n'' экземпляров формы $[p^2]$, ..., есть

$$1^n \times \left(\frac{1}{\sqrt{p}}\right)^{n'} \times \left(\frac{1}{\sqrt{p^2}}\right)^{n''} \times \dots,$$

помноженное на некоторый корень четвертой степени из единицы.

Разумеется, выражение, приведенное в формулировке этой теоремы, есть $1/\sqrt{\det(f)}$. Теперь посмотрим, что будет, если поделить f на степень p . Поскольку

$$e^{2\pi i p} = e^{2\pi i p^2} = \dots = 1,$$

гауссовы средние форм

$$[1/p], [1/p^2], [1/p^3], \dots$$

все равны единице. Следовательно, гауссово среднее формы f/p есть

$$1^{n'} \times \left(\frac{1}{\sqrt{p}}\right)^{n''} \times \left(\frac{1}{\sqrt{p^2}}\right)^{n'''} \times \dots,$$

гауссово среднее для f/p^2 есть

$$1^{n''} \times \left(\frac{1}{\sqrt{p}}\right)^{n'''} \times \dots,$$

и так далее (все эти значения надо умножить на подходящий корень четвертой степени из единицы). Поскольку все эти числа слышимы, получаем следующий результат:

Теорема. Если p нечетно, то для форм вида $[1, 1, \dots, p, p, \dots, p^2, \dots, p^k]$ слышимы числа $n, n', n'', \dots$ (количество единиц, количество p , количество $p^2, \dots$).

Мы вернемся к этой теме (для более общих форм) после лекции 4. Числа $n, n', n'', \dots$ являются показателями в определяемом там p -адическом символе, а из корней четвертой степени из единицы мы получим знаки, входящие в этот символ. Окажется, что p -адические символы из этой лекции слышимы для нечетного p , но не для $p=2$.

ДОБАВЛЕНИЕ

Кнезеровский метод склейки: унимодулярные решетки

Вступление

Главной темой этой книги является классификация квадратичных форм; последняя лекция представляла собой отступление, важность которого выяснится только впоследствии. В первой лекции мы классифицировали двумерные формы, в третьей будем классифицировать знакоопределенные трехмерные формы, а в четвертой мы будем классифицировать неопределенные формы во всех размерностях, превосходящих 2.

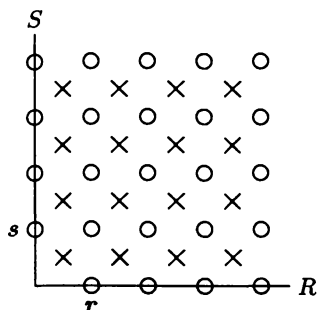
Нет никакой надежды на классификацию положительно определенных квадратичных форм во всех размерностях. Тем не менее Кнезер нашел много целых решеток с маленьким определителем с помощью «склеивания» решеток корней друг с дружкой (или решетки с собой). В милноровских тороидальных «барабанах» использовались 16-мерные четные унимодулярные решетки E_8^2 и D_{16}^+ . Более ярким приложением была принадлежащая Нимейеру полная классификация 24-мерных четных унимодулярных решеток.

Пример склейки

Мы продемонстрируем *метод склейки* на простом примере. Пусть R и S — две ортогональные одномерные решетки на плоскости, порожденные векторами $\mathbf{r}$ и $\mathbf{s}$ соответственно, для которых $N(\mathbf{r}) = \mathbf{r} \cdot \mathbf{r} = 2$, $N(\mathbf{s}) = \mathbf{s} \cdot \mathbf{s} = 2$ и $\mathbf{r} \cdot \mathbf{s} = 0$.

Поискем двумерную целую решетку L , строго содержащую $R \oplus S$. Всякий вектор $\mathbf{y} \in L$ должен иметь вид $\mathbf{y} = \lambda \mathbf{r} + \mu \mathbf{s}$, где $\mathbf{y} \cdot \mathbf{r} = \lambda \mathbf{r} \cdot \mathbf{r} = 2\lambda$ и $\mathbf{y} \cdot \mathbf{s} = \mu \mathbf{s} \cdot \mathbf{s} = 2\mu$ должны быть целыми числами, так что λ и μ должны быть полуцелыми. Другое ограничение состоит в том, что число $\mathbf{y} \cdot \mathbf{y} = 2\lambda^2 + 2\mu^2$ должно быть целым. По модулю $R \oplus S$ для $\mathbf{y}$ имеется

только одна нетривиальная возможность, а именно, $\mathbf{y} = \frac{1}{2}\mathbf{r} + \frac{1}{2}\mathbf{s}$. Мы



будем говорить, что решетка L , порожденная этим вектором y , а также R и S , получена путем *склеивания* решеток R и S с помощью клеевого вектора y . На рисунке кружками помечены точки из $R \oplus S$, а крестиками — остальные точки решетки L .

Тем же методом можно воспользоваться для склеивания любого количества целочисленных решеток $L_1, L_2, \dots$

$\dots, L_k$, в результате которого получается

целочисленная решетка L , содержащая $L_1 \oplus L_2 \oplus \dots \oplus L_k$. Решетка L порождена $L_1, L_2, \dots, L_k$ и различными клеевыми векторами, которые могут быть записаны в виде $y_1 + y_2 + \dots + y_k$, где y_i лежит в вещественном пространстве, порожденном L_i , причем его скалярное произведение с любым элементом L_i является целым. Роль играют только значения y_i по модулю L_i . Возможные значения y_i , соответствующие элементам двойственной факторгруппы L_i^*/L_i , будут называться *клеевыми векторами* для L_i .

Решетки корней

Имеется специальный класс решеток — так называемые *решетки корней*, — особенно хорошо приспособленных к склейке. Опишем кратко эти решетки и их клеевые векторы.

Решетка A_n состоит из всех векторов $(x_0, x_1, \dots, x_n)$, координаты которых — $n+1$ целое число с нулевой суммой. Например, A_2 — это двумерная решетка, порожденная векторами $(1, -1, 0)$ и $(0, 1, -1)$. Стало быть, ее клеевые векторы будут иметь вид (x, y, z) , где $x+y+z=0$, но x, y и z не обязаны быть целыми числами. Один из таких векторов имеет вид $(2/3, -1/3, -1/3)$. Для произвольного n ненулевые клеевые векторы в A_n имеют вид

$$[i] = \left(\left(\frac{j}{n+1} \right)^i, \left(\frac{-i}{n+1} \right)^j \right), \quad 1 \leq i \leq n, \quad i+j=n+1.$$

Двойственная факторгруппа A_n^*/A_n есть циклическая группа порядка $n+1$.

Мы уже встречались с решеткой корней D_n , состоящей из целочисленных векторов $(x_1, x_2, \dots, x_n)$ с четной суммой координат. (Эту

решетку можно назвать «шахматной», поскольку она содержит в точности по одному вектору для каждого «черного поля» на n -мерной шахматной доске.) Ее отличные от нуля клеевые векторы суть

$$[1] = \left(\frac{1}{2}, \frac{1}{2}, \dots, \frac{1}{2}\right), \quad [2] = (0, \dots, 0, 1), \quad [3] = \left(\frac{1}{2}, \frac{1}{2}, \dots, \frac{1}{2}, -\frac{1}{2}\right).$$

Двойственная факторгруппа D_n^*/D_n имеет порядок 4; она циклична, только если n нечетно.

Решетка E_8 состоит из векторов $(x_1, x_2, \dots, x_8)$, координаты которых являются либо все целыми, либо все полуцелыми, и при этом сумма координат четна. Для E_8 нетривиальных клеевых векторов нет, и двойственная факторгруппа E_8^*/E_8 тривиальна.

Решетка E_7 состоит из тех векторов в E_8 , для которых $x_1 + \dots + x_8 = 0$. Единственный отличный от нуля клеевой вектор есть

$$[1] = \left(\frac{1}{4}, \dots, \frac{1}{4}, -\frac{3}{4}, -\frac{3}{4}\right),$$

и группа E_7^*/E_7 имеет порядок 2.

Решетка E_6 состоит из тех векторов в E_8 , для которых $x_1 + x_8 = x_2 + \dots + x_7 = 0$. Отличные от нуля клеевые векторы суть

$$[1] = \left(0, -\frac{2}{3}, -\frac{2}{3}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, 0\right) \quad \text{и} \quad [2] = -[1],$$

и группа E_6^*/E_6 имеет порядок 3.

Разумеется, нулевой вектор $[0]$ является клеевым вектором в любом случае.

Склеивание решеток

Мы сейчас введем удобное обозначение для решеток, полученных в результате склейки. Пусть $X_m, Y_n, \dots$ — решетки корней размерностей $m, n, \dots$. Обозначим теперь через

$$X_m Y_n \dots [ab \dots, a'b' \dots, \dots]$$

решетку, полученную присоединением клеевых векторов

$$\begin{aligned} &[a] + [b] + \dots, \\ &[a'] + [b'] + \dots, \\ &\dots\dots\dots \end{aligned}$$

к $X_m \oplus Y_n \oplus \dots$

Например, одна из нимейеровских 24-мерных решеток обозначается $A_{11}D_7E_6[1, 1, 1]$. Вспомним, что

$$[1] \text{ для } A_{11} \text{ есть } \left(\frac{11}{12}, \frac{-1}{12}, \dots, \frac{-1}{12}\right);$$

$$[1] \text{ для } D_7 \text{ есть } \left(\frac{1}{2}, \dots, \frac{1}{2}\right);$$

$$[1] \text{ для } E_6 \text{ есть } \left(0, -\frac{2}{3}, -\frac{2}{3}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, 0\right).$$

Стало быть, $A_{11}D_7E_6[1, 1, 1]$ — это решетка, порожденная $A_{11} \oplus D_7 \oplus E_6$ и вектором

$$\left(\frac{11}{12}, \left(\frac{-1}{12}\right)^{11}, \left(\frac{1}{2}\right)^7, 0, -\frac{2}{3}, -\frac{2}{3}, \left(\frac{1}{3}\right)^4, 0\right).$$

Можно обозначить эту решетку и просто $(A_{11}D_7E_6)^+$, если нет необходимости более точно указывать клеевые векторы. Тогда плюс означает просто «вместе с некоторыми клеевыми векторами».

Решетки Нимейера

Таким способом можно описать много интересных решеток. В размерности 8 есть только одна четная унимодулярная решетка, а именно E_8 . Во второй лекции мы видели, что в размерности 16 таких решеток всего две, а именно D_{16}^+ и $E_8 \oplus E_8$; в наших нынешних обозначениях это решетки $D_{16}[1]$ и $E_8E_8[0, 0]$ соответственно. В общем случае мы будем писать $(X_mY_n\dots)^+$ для обозначения результата присоединения некоторых не указанных явно клеевых векторов к решетке $X_m \oplus Y_n \oplus \dots$

Нимейер решил поставленную Виттом старую задачу перечисления всех четных унимодулярных 24-мерных решеток. Список этих решеток приведен в нижеследующей таблице. Круглые скобки в обозначениях для клеевого вектора означают, что наряду с указанным вектором имеются в виду и все векторы, полученные с помощью циклических перестановок координат, взятых в скобки. Последняя решетка A_{24} — замечательная решетка, открытая Джоном Личем; к сожалению, у нас нет возможности обсудить ее здесь.

Тем же методом можно перечислять и другие решетки. Например, все унимодулярные решетки размерности, не превосходящей 16, являются прямыми суммами решеток

$$I_1, E_8, D_{12}[1], E_7^2[11], A_{15}[4], D_8^2[(12)], D_{16}[1],$$

где I_1 — одномерная решетка, порожденная вектором с нормой 1.

Решетка	Клей (запятые опущены)
$(D_{24})^+$	[1]
$(D_{16}E_8)^+$	[10]
E_8^3	[000]
$(A_{24})^+$	[5]
$(D_1 2^2)^+$	[12, 21]
$(A_{17}E_7)^+$	[31]
$(D_{10}E_7^2)^+$	[110, 301]
$(A_{15}D_9)^+$	[21]
$(D_8^3)^+$	[(122)]
$(A_{12}^2)^+$	[15]
$(A_{11}D_7E_6)^+$	[11]
$(E_6^4)^+$	[1(012)]
$(A_9^2D_6)^+$	[240, 501, 053]
$(D_6^4)^+$	[четные перестановки (0123)]
$(A_8^3)^+$	[(114)]
$(A_7^2D_5^2)^+$	[1112, 1721]
$(A_6^4)^+$	[1(216)]
$(A_4^4D_4)^+$	[2(024)0, 33001, 30302, 30033]
$(D_4^6)^+$	[111111, 0(02332)]
$(A_4^6)^+$	[1(01441)]
$(A_3^8)^+$	[3(2001011)]
$(A_2^{12})^+$	[2(11211122212)]
$(A_1^{24})^+$	[1(00000101001100110101111)]
Λ_{24}	методом склейки не строится

Лемма Витта о решетках корней

В качестве еще одной иллюстрации полезности понятия склейки мы докажем изящную лемму Витта, утверждающую, что всякая целочисленная решетка, порожденная векторами с нормой 2, является прямой суммой решеток корней A_n , D_n и E_n .

Достаточно доказать, что неразложимая решетка, порожденная векторами с нормой 2, есть A_n , D_n или E_n . Пусть L — неразложимая решетка, являющаяся контрпримером к этому утверждению; рассмотрим максимальную решетку корней X_n , содержащуюся в L . Существует вектор с нормой 2, лежащий в L , но не в X_n , и кроме того, существует вектор с такой нормой, не ортогональный к X_n (в противном случае L была бы разложима). Этот вектор v равен $v_1 + v_2$, где $v_1 \neq 0$ лежит в пространстве, порожденном X_n (он «горизонта-

лен»), вектор v_2 ортогонален к этому пространству («вертикален»), и $N(v_1) + N(v_2) = 2$. Кроме того, скалярные произведения v_1 со всеми векторами из X_n целочисленны, поскольку v_2 в эти произведения вклада не дает.

Стало быть, мы можем применить склейку: v_1 должен быть клеевым вектором для X_n , и мы склеиваем X_n с решеткой, порожденной v_2 . В каждом из возможных случаев мы увидим, что в результате склейки также получится решетка корней, что будет противоречить максимальности X_n .

В качестве примера рассмотрим решетку, порожденную A_9 и некоторым вектором $v = v_1 + v_2$ с нормой 2. Вектор v_1 должен быть клеевым вектором для A_9 с нормой, не превосходящей 2. Так может быть только в следующих случаях: $v_1 = [1]$ или $[9]$ (с нормой $9/10$) склеивается с v_2 с нормой $11/10$, или же $v_1 = [2]$ или $[8]$ (с нормой $16/10$) склеивается с v_2 (с нормой $4/10$). Стало быть, имеются ровно две такие решетки, которые тем самым должны быть изометричны с A_{10} или D_{10} , поскольку обе содержат A_9 .

Если, в большей общности, X_n вкладывается таким образом в $(n+1)$ -мерную решетку Y_{n+1} , то отношение определителей этих решеток будет $N(v_2) = 2 - N(v_1)$. Нам уже известны некоторые из возникающих при этом случаев:

		$N(v_2)$	$N(v_1)$	Клей
A_{n+1} из A_n		$(n+2)/(n+1)$	$n/(n+1)$	[1] или [n]
D_{n+1} из D_n		1	1	[2]
E_6 из A_5		$3/6=1/2$	$3/2$	[3]
E_6 из D_5		$3/4$	$5/4$	[1] или [3]
E_7 из A_6		$2/7$	$12/7$	[3] или [4]
E_7 из D_6		$2/4=1/2$	$3/2$	[1] или [3]
E_7 из E_6		$2/3$	$4/3$	[1] или [2]
E_8 из A_7		$1/8$	$15/8$	[3] или [5]
E_8 из D_7		$1/4$	$7/4$	[1] или [3]
E_8 из E_7		$1/2$	$3/2$	[1]

Использованный нами клеевой вектор v_1 имеет известную норму h , и в последнем столбце мы перечислили все возможности для вектора v_1 , норма которого теперь известна. Список полон, поскольку можно проверить, что в него включены все клеевые векторы с нормой, меньшей 2.

Если же вкладывать X_n в решетку Y_n , также являющуюся n -мерной, то $N(v_2)$ будет равно нулю, а $N(v_1)$ будет равно 2. Некоторые из

тех случаев, которые, как мы знаем, возможны, приведены в следующей таблице:

	$N(v_2)$	$N(v_1)$	Клей
E_7 из A_7	0	2	[4]
E_8 из A_8	0	2	[3] или [6]
E_8 из D_8	0	2	[1] или [3]

Опять клеевой вектор v_1 полностью определен своей нормой 2, и приведены все возможные клеевые векторы с такой нормой.

Поскольку всякая целочисленная решетка, порожденная векторами нормы 2, получается последовательными расширениями указанного типа с клеевыми векторами нормы, не превосходящей 2, и поскольку каждый такой клеевой вектор появляется в одном из расширений, дающих решетку корней, в результате *всякого* такого расширения получается решетка корней.

Разумеется, именно благодаря лемме Витта решетки корней являются столь полезными для построения других целочисленных решеток с малым определителем. Суть здесь в том, что в такой решетке, скорее всего, будет много векторов с нормой 1 или 2, которые будут порождать прямую сумму кубической решетки I_n с одной из этих решеток корней.

Кубичность слышима в низких размерностях

Мы докажем с помощью леммы Витта высказанное ранее в тексте утверждение о том, что кубичность является слышимым свойством в размерностях, не превосходящих 5.

С помощью изменения масштаба переведем пятимерную кубическую решетку в решетку

$$L = A_1 \oplus A_1 \oplus A_1 \oplus A_1 \oplus A_1,$$

нормы векторов которой являются четными целыми числами. Решетка L' , звучащая так же, как L , будет обладать тем же свойством и тем самым будет четной целочисленной решеткой, содержащей 10 векторов $\pm v_1, \pm v_2, \pm v_3, \pm v_4, \pm v_5$, имеющих норму 2. Согласно лемме Витта, эти векторы порождают решетку, являющуюся прямой суммой решеток корней; такой решеткой может быть либо все та же

$$A_1 \oplus A_1 \oplus A_1 \oplus A_1 \oplus A_1$$

(и в этом случае $L' = L$), либо

$$A_2 \oplus A_1 \oplus A_1.$$

Стало быть, если $L' \neq L$, то L' получается склеиванием из некоторой решетки вида

$$L'' = A_2 \oplus A_1 \oplus A_1 \oplus L_1,$$

где L_1 — одномерная решетка, порожденная кратчайшим вектором из L'' , ортогональным к $A_2 \oplus A_1 \oplus A_1$ (мы предполагаем, что этот вектор имеет норму n).

Однако же определитель решетки L'' равен $3 \times 2 \times 2 \times n$, что должно быть равно $32d^2$, где d — индекс L'' в L' . Значит, d делится на 3, так что L' должна содержать клеевой вектор порядка 3 по модулю L'' . Однако же с точностью до знака единственный клеевой вектор порядка 3 для $A_2 \oplus A_1 \oplus A_1$ есть $[1] \oplus [0] \oplus [0]$, имеющий норму $2/3$, а для L_1 единственный такой вектор есть $v/3$, имеющий норму $n/9$. Стало быть, $2/3 + n/9$ должно быть целым числом, что противоречит установленному выше равенству $12n = 32d^2$.

Лекция 3

А можно ли ее форму нащупать?

Геометрия или арифметика?

Когда в первой лекции мы обсуждали бинарные квадратичные формы, было заметно существенное различие между случаями определенных и неопределенных форм. Оно сохраняется и в высших размерностях. Значения положительно определенной формы лучше всего представлять себе как квадраты длин векторов решетки, и мы классифицируем такие решетки с помощью геометрического анализа их формы.

В неопределенном случае, если размерность равна по крайней мере 3, имеется принадлежащая Эйхлеру полная классификация с помощью арифметического инварианта, называемого спинорным родом; этот последний, в свою очередь, определяется через более простой и более важный инвариант, называемый родом.

В своих Хедриковских лекциях я совместил две эти очень разные темы в рамках одной лекции; в печатном издании мне представляется более правильным их разделить. Эта лекция будет в основном посвящена геометрической классификации трехмерных решеток с помощью так называемых областей Вороного. Обсуждение арифметических вопросов, после которого мы опишем теорему Эйхлера, откладывается до следующей, четвертой лекции.

Область Вороного

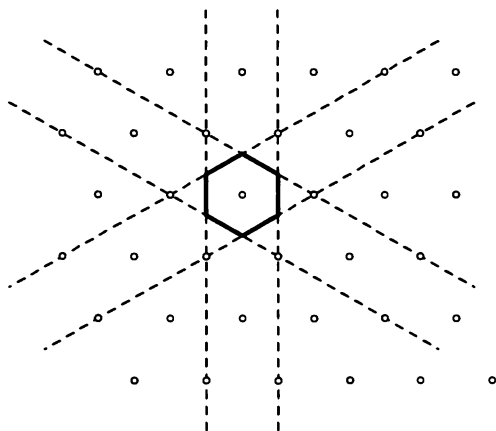
Вспомним, что, как мы установили в первой лекции, положительно определенную бинарную форму можно задать либо с помощью трех чисел α , β и γ , называемых конормами, либо с помощью трех других чисел a , b и c , называемых вонормами. Сейчас мы дадим геометрическую интерпретацию этих чисел и приведем обобщение на высшие размерности.

При обсуждении этих вопросов необходимо иметь в виду два обстоятельства. Во-первых, у нас есть правило перехода от греческих букв к латинским: $a = \beta + \gamma$, $b = \alpha + \gamma$ и $c = \alpha + \beta$, так что $\alpha = \frac{1}{2}(b + c - a)$ и т. д. Далее, если e_1 , e_2 , e_3 — супербазис колодца, то он обладает

тем свойством, что $e_i \cdot e_j \leq 0$; будем говорить, что это *тупоугольный супербазис*. Мы получим аналогичные результаты для трехмерных решеток.

Геометрическая интерпретация вонорм такова: в общем случае они являются нормами некоторых векторов, называемых векторами Вороного. В размерностях 2 и 3 вонормы по существу совпадают с некоторыми параметрами, введенными Зеллингом в 1874 году, а именно, с абсолютными величинами скалярных произведений пар векторов из тупоугольного супербазиса. Векторы Вороного связаны с важной областью, называемой областью Вороного (или областью Дирихле, или зоной Бриллюэна).

Сопоставим каждой точке решетки множество точек пространства, расположенных от нее не дальше, чем от любой другой точки решетки. При этом получится замощение пространства областями, называемыми *областями Вороного*. Вот как выглядит область Вороного для шестиугольной решетки:

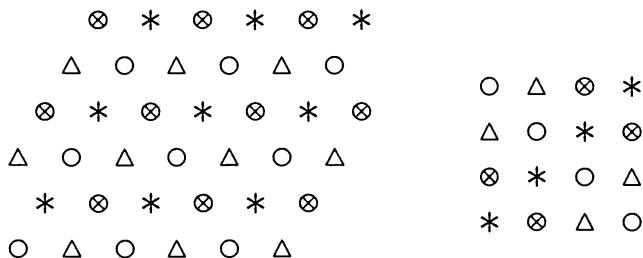


Область Вороного, содержащая начало координат, получается как результат серии состязаний между началом координат и всеми остальными точками v , принадлежащими решетке; результат каждого состязания определяется гиперплоскостью, являющейся срединным перпендикуляром к отрезку, соединяющему 0 и v ; начало координат побеждает в одной из получающихся при этом полуплоскостей, а область Вороного есть пересечение этих полуплоскостей:

$$H(v) = \left\{ x : x \cdot v \leq \frac{1}{2} v \cdot v \right\}.$$

Впрочем, большинство этих гиперплоскостей в задании области Вороного роли не играют, поскольку они слишком далеки от начала координат. Те из них, которые существенны для задания области, получаются из некоторых векторов, которые мы будем называть *векторами Вороного в строгом смысле*. Имеется красивая теорема Вороного, утверждающая следующее: v является вектором Вороного для L тогда и только тогда, когда $\pm v$ — в точности кратчайшие векторы в своем смежном классе по модулю $2L$. В самом деле, если w — другой вектор в этом смежном классе, длина которого не превосходит длины v , то гиперплоскость $H(v)$ не играет роли при задании области, поскольку она содержит пересечение гиперплоскостей $H\left(\frac{1}{2}(v+w)\right)$ и $H\left(\frac{1}{2}(v-w)\right)$. Если же $H(v)$ не играет роли, то так получается потому, что $\frac{1}{2}v$ лежит вне или на границе некоторой гиперплоскости $H(x)$, т. е. $\frac{1}{2}v \cdot x \geq \frac{1}{2}x \cdot x$, так что $N(v-2x) \leq N(v)$.

Решетка $2L$ состоит из удвоенных векторов решетки L . В двумерном случае у решетки L имеется четыре класса смежности по модулю $2L$; мы сопоставим им четыре «масти» $\circ$, $\triangle$, $\otimes$ и $*$; два вектора имеют одну масть тогда и только тогда, когда их разность есть удвоенный вектор из L . Стало быть, факторгруппа $L/2L$ есть в точности множество мастей $\{\circ, \triangle, \otimes, *\}$, на котором введена групповая операция.

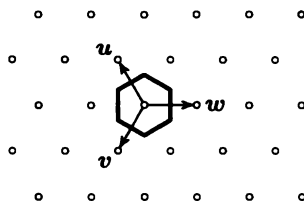


$L/2L$ и ее групповая структура

Двумерные области Вороного

У большинства двумерных решеток область Вороного является шестиугольником с шестью векторами Вороного $\pm u$, $\pm v$ и $\pm w$,

удовлетворяющими соотношению $u + v + w = 0$; выглядит она примерно так:



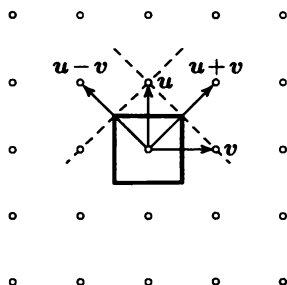
В этом случае конормы a , b и c — это просто нормы векторов u , v и w :

$$u \cdot u = a, \quad v \cdot v = b, \quad w \cdot w = c.$$

Конормы противоположны скалярным произведениям этих векторов:

$$v \cdot w = -\alpha, \quad w \cdot u = -\beta, \quad u \cdot v = -\gamma.$$

Пусть теперь у нас имеется прямоугольная решетка со сторонами, параллельными векторам u и v . Тогда имеется ровно четыре вектора Вороного $\pm u$ и $\pm v$, поскольку они являются кратчайшими векторами в своих смежных классах, а в остающемся смежном классе имеются четыре вектора равной длины ($u + v$, $u - v$ и противоположные к ним). Из рисунка видно, что гиперплоскости, соответствующие этим векторам, для задания области Вороного не нужны, поскольку они проходят через вершины под углом к осям. Стало быть, $u + v$ и $u - v$ не являются векторами Вороного в строгом смысле; но поскольку они почти что необходимы, мы назовем их (и противоположные к ним) *векторами Вороного в нестрогом смысле*.



Вонормы

Пусть L — произвольная решетка. Тогда *вонорма* смежного класса L по $2L$ есть норма вектора, кратчайшего в этом смежном классе. Ста-ло быть, вонормы (нормы Вороного) суть нормы векторов Вороного (в строгом и нестрогом смысле). Для каждой масти имеется ровно одна вонорма. Мы будем считать нулевую вонорму (из тривиального смежного класса) «несобственной» и не будем, как правило, принимать ее во внимание. У n -мерной решетки имеется $2^n - 1$ собственных вонорм.

Теперь посмотрим еще раз на то, что происходило в первой лекции. У положительно определенной бинарной квадратичной формы (а тем самым и у двумерной решетки) имеется либо простой, либо двойной колодец. Простой колодец соответствует шестиугольной области Вороного со «строго тупоугольным» супербазисом $\pm e_1, \pm e_2, \pm e_3$; это означает, что $e_i \cdot e_j < 0$ при $i \neq j$. В этом случае имеющиеся $2^2 - 1 = 3$ вонормы суть $N(e_1)$, $N(e_2)$ и $N(e_3)$, а конормы равны $-e_2 \cdot e_3$, $-e_3 \cdot e_1$ и $-e_1 \cdot e_2$.

Двойной колодец соответствует прямоугольной области Вороного с базисом $\pm e_1, \pm e_2$ из перпендикулярных векторов. Следовательно, у нас действительно есть два «нестрого тупоугольных» супербазиса:

$$\{\pm e_1, \pm e_2, \pm(e_1 + e_2)\} \quad \text{и} \quad \{\pm e_1, \pm e_2, \pm(e_1 - e_2)\}.$$

В этом случае три вонормы равны $a = N(e_1)$, $b = N(e_2)$ и $a + b = N(e_1 \pm e_2)$, а конормы равны b , a и 0 .

Характеры и конормы

А как же обстоит дело с загадочными соотношениями

$$\alpha = \frac{b + c - a}{2}?$$

Конормы в размерности n суть некоторые числа, выражаемые через вонормы с помощью обобщения этой формулы, в котором участвуют *вещественные характеры* решетки L . Такой характер — это отображение $\chi: L \rightarrow \{\pm 1\}$, удовлетворяющее тождеству $\chi(v + w) = \chi(v) \times \chi(w)$. Мы обычно будем вместо $+1$ и -1 писать просто $+$ и $-$. Мы не будем также рассматривать «несобственный» характер, все значения которого равны $+$.

У двумерной решетки имеются три собственных характера (см. таблицу ниже). Пространство вонорм состоит из мастей $\{O, \Delta, \otimes, *\}$.

Стало быть, *вономра* как функция $vo(\text{масть})$ действительно определена на пространстве *воном* и принимает значения 0, a , b и c . Обычно мы будем игнорировать «несобственную масть».

В приведенной ниже таблице проиллюстрировано вычисление конорм («сопряженных норм») для каждого собственного характера. *Конорма* для данного характера χ определяется как число¹

$$-\frac{1}{2^{n-1}} \sum \chi(\text{масть}) vo(\text{масть}).$$

У двумерной решетки имеются четыре масти, и тем самым четыре *вономы* (три из них собственные), и три собственных характера и *конормы*, как в приведенной ниже таблице.

масти:		○	△	⊗	*		
вономы:		0	a	b	c		
характеры	} :	{	+	+	−	−	→ $\alpha = -1/2(a - b - c)$
и			+	−	+	−	→ $\beta = -1/2(b - c - a)$
конормы			+	−	−	+	→ $\gamma = -1/2(c - a - b)$

Пространство *воном* и пространство *конорм*

В двумерном случае *вономы* заданы на «прямой *воном*», состоящей из трех точек:

$$a \text{ ————— } b \text{ ————— } c.$$

Точки этой прямой соответствуют трем нетривиальным элементам группы $L/2L$.

Конормы определены на «двойственной» прямой, называемой *прямой конорм*:

$$\alpha \text{ ————— } \beta \text{ ————— } \gamma.$$

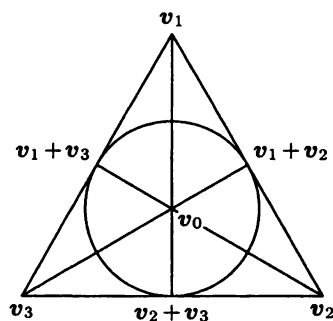
Точки этой прямой соответствуют трем нетривиальным характеристам группы $L/2L$.

Плоскость Фано: подготовка к трехмерному случаю

В трехмерном случае $L/2L$ — группа порядка 8 (изоморфная $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$). Стало быть, имеется восемь мастей, из них семь

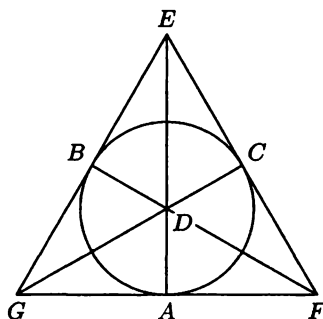
¹Приведенная ниже формула означает, что *конормы* являются (с точностью до постоянного множителя) «конечным преобразованием Фурье» *воном*.

собственных. Семь мастей пространства вонорм образуют проективную плоскость. Это — так называемая плоскость Фано, на которой имеется семь «точек» и семь прямых (на каждой из которых лежат три точки), обладающих тем свойством, что всякие две точки лежат на ровно одной прямой. Это можно изобразить так:

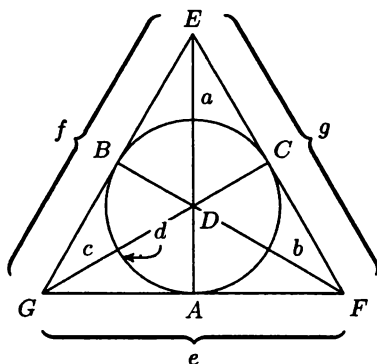


Каждой точке на этой плоскости соответствует одна вонорма. Каждой же прямой на этой плоскости соответствует один характер, принимающий значение «+» на трех точках этой прямой (и в нуле) и значение «-» в четырех точках, не лежащих на прямой. Тем самым пространство, на котором определены конормы, является в сущности двойственной проективной плоскостью.

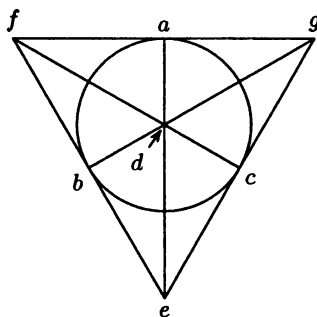
Обсудим вкратце двойственность для плоскости Фано. Обозначим точки буквами A, B, C, D, E, F и G :



Обозначим теперь прямые буквами a, b, c, d, e, f и g (например, f — прямая, проходящая через G, B и E):



Построим теперь новую плоскость Фано, в которой точки обозначены буквами a, b, c, d, e, f и g , а три точки коллинеарны тогда и только тогда, когда три соответствующие прямые на исходной плоскости проходят через одну точку (конкурrentны):



Три конкурrentные прямые на этом рисунке соответствуют трем коллинеарным точкам на исходном рисунке.

Вонормы и конормы для трехмерных решеток

У трехмерной решетки имеется восемь мастей O, A, B, C, D, E, F и G . Следовательно, собственные вонормы $vo(A), vo(B), \dots, vo(G)$ суть нормы кратчайших векторов соответствующих мастей. Имеется восемь характеров $\chi_0, \chi_a, \chi_b, \dots, \chi_g$ и семь собственных характеров, соответствующих прямым на плоскости вонорм (и тем самым семи прямым на плоскости конорм). Например, χ_a — это характер, прини-

мающий значение «+» в точке O и в точках A , D и E , лежащих на прямой a , и принимающий значение «-» в остальных четырех точках.

В размерности 3 конорма характера χ задается формулой

$$\text{co}(\chi) = -\frac{1}{4} \sum_{\text{по всем мастям}} \chi(\text{масть}) \text{vo}(\text{масть}).$$

Иными словами, конорма, соответствующая данной прямой, есть

$$\frac{1}{4}(\text{сумма воном точек вне прямой}) - \\ - \frac{1}{4}(\text{сумма воном точек на прямой}).$$

Имеется также формула для выражения воном через конормы:

$$\text{vo}(\text{масть}) = \sum_{\chi(\text{масть})=-1} \text{co}(\chi);$$

в правой части стоит сумма конорм всех характеров, принимающих значение -1 на данной масти (геометрически: сумма конорм всех прямых, проходящих через соответствующую точку на плоскости воном).

Тупоугольные супербазисы

Оказывается, что, как и в рассмотренном в первой лекции двумерном случае, у всякой трехмерной решетки есть хотя бы один тупоугольный супербазис, а в общем случае такой базис ровно один. В размерности n тупоугольный супербазис (если он существует) состоит из $n+1$ вектора $v_0, v_1, \dots, v_n$ с нулевой суммой, для которых $v_i \cdot v_j \leq 0$ при $i \neq j$. Положим теперь $p_{ij} = -v_i \cdot v_j$. Опять имеет место формула Зеллинга: норма данного вектора

$$v = m_0 v_0 + m_1 v_1 + \dots + m_n v_n$$

равна

$$N(v) = \sum_{0 \leq i < j \leq n} p_{ij} (m_i - m_j)^2.$$

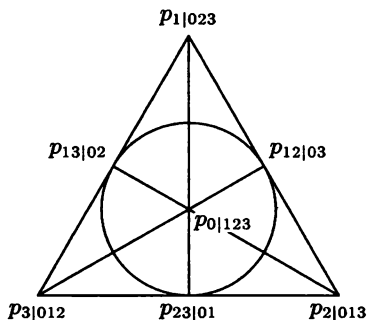
Если мы прибавим к m_i четные целые числа, то к v прибавится элемент решетки $2L$. Поэтому при поиске кратчайших векторов в данном классе смежности можно заменить все четные m_i на 0 и все

нечетные m_j на 1. Стало быть, векторы Вороного — это в точности те векторы, для которых $m_i = 0$ или 1, то есть (в трехмерном случае)

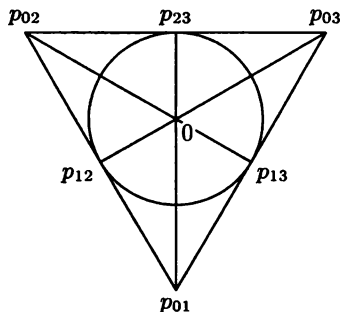
$$\pm v_1, \pm v_2, \pm v_3, \pm v_0, \pm(v_1 + v_2), \pm(v_2 + v_3), \pm(v_1 + v_3).$$

Отметим, что, например, $v_0 + v_3 = -(v_1 + v_2)$, так что для каждой из семи нетривиальных мастей в пространстве воном имеет ровно два представителя.

Далее, норма вектора v_i есть $p_{ij} + p_{ik} + p_{il}$, что вкратце будет записываться как $p_{i|jkl}$, где j, k и l — остальные три индекса, а норма вектора $v_i + v_j$ есть $p_{ik} + p_{il} + p_{jk} + p_{jl}$, что сокращенно будет записываться как $p_{ij|kl}$. В пространстве воном эти нормы располагаются так:



Мы покажем, что в случае, когда имеется тупоугольный супербазис со скалярными произведениями $-p_{ij}$, конормами будут просто числа p_{ij} и нуль. В трехмерном случае их можно нанести на двойственную плоскость Фано:



Например, конорма, соответствующая прямой f , проходящей через v_1 и v_3 , есть

$$\begin{aligned} \text{co}(\chi_f) = & -\frac{1}{4} \sum_{\text{масти}} \chi_f(\text{масть}) \text{vo}(\text{масть}) = -\frac{1}{4} (N(v_1 + v_3) + N(v_3) + \\ & + N(v_1) - N(v_1 + v_2) - N(v_0) - N(v_2 + v_3) - N(v_2)) = -\frac{1}{4} (p_{13|02} + \\ & + p_{3|012} + p_{1|023} - p_{12|03} - p_{0|123} - p_{01|23} - p_{2|013}) = -\frac{1}{4} (-4p_{02}) = p_{02}. \end{aligned}$$

Аналогичное вычисление показывает, что средняя конорма равна нулю.

Тупоугольные супербазисы в размерности 3

Мы докажем, что у всякой трехмерной решетки имеется тупоугольный супербазис. Описанный выше супербазис является тупоугольным тогда и только тогда, когда все p_{ij} положительны. Возьмем теперь решетку L и будем ее деформировать, пока в точности одно из чисел p_{ij} не станет отрицательным. Пусть, например, $p_{13} = -\epsilon$.

Заметим, что из неравенства $p_{13} < 0$ вытекает, что $v_1 - v_3$ короче, чем $v_1 + v_3$; поскольку остальные p_{ij} положительны, можно проверить, пользуясь формулой Зеллинга, что каждый из остальных шести векторов по-прежнему является кратчайшим в своей масти. Определим теперь новый, «смежный», супербазис

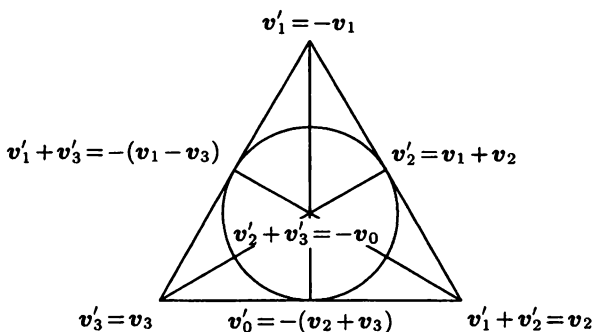
$$v'_0 = v_0 + v_1, \quad v'_1 = -v_1, \quad v'_2 = v_1 + v_2, \quad v'_3 = v_3.$$

Оказывается, этот супербазис является тупоугольным, если только ϵ столь мало, что $p_{ij} - \epsilon$ неотрицательны. Векторы Вороного будут иметь следующий вид:

$$\begin{aligned} v'_0 = v_0 + v_1 = & -(v_2 + v_3), \quad v'_1 = -v_1, \quad v'_2 = v_1 + v_2, \quad v'_3 = v_3, \\ v'_1 + v'_2 = & v_2, \quad v'_2 + v'_3 = (v_1 + v_2 + v_3) = -v_0, \quad v'_1 + v'_3 = -(v_1 - v_3). \end{aligned}$$

Как видим, слово «смежный» вполне удачно, поскольку шесть из этих векторов Вороного совпадают (с точностью до знака) со старыми. Интересно представить себе тупоугольный супербазис как что-то вроде изогнутой упругой пластины: если продеформировать решетку далее, чем до критической конфигурации, то пластина со щелчком перейдет в смежный супербазис.

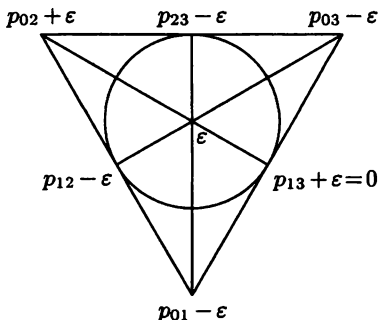
Поскольку изменилась (на 4ϵ) только одна конорма, а именно $N(v_1 - v_3) = N(v_1 + v_3) - 4\epsilon$, новые конормы можно найти следующим



образом: прибавим ε ко всем числам, лежащим на прямой, проходящей через p_{13} и 0, и вычтем ε из всех чисел, не лежащих на этой прямой. Например, «левая верхняя» конорма на приведенном ниже рисунке есть

$$-\frac{1}{4}(N(v_1 - v_3) + N(v_3) + N(-v_1) - \\ - N(v_1 + v_2) - N(v_0) - N(-(v_2 + v_3)) - N(v_2)),$$

а поскольку $N(v_1 - v_3) = N(v_1 + v_3) - 4\varepsilon$, это число равно $p_{02} + \varepsilon$.



Из этих рассуждений вытекает, что у всякой трехмерной решетки L есть тупоугольный супербазис. В самом деле, пусть L_0 — решетка с тупоугольным супербазисом. Будем ее деформировать в решетку L , пока одно из чисел p_{ij} не станет отрицательным и супербазис не перейдет в смежный. Будем продолжать этот процесс, пока не дойдем

от L_0 до L . Поскольку на каждом шаге у нас имелся тупоугольный супербазис, описанный процесс приводит к нахождению тупоугольного супербазиса решетки L .

Пример

На практике мы переходим от нетупоугольного супербазиса к тупоугольному, следя за изменением скалярных произведений векторов, входящих в супербазис. Лучше работать с числами, противоположными этим скалярным произведениям, поскольку в момент, когда мы доберемся до тупоугольного супербазиса, эти числа будут конормами решетки.

Рассмотрим решетку L_0 , характеризующуюся следующей матрицей скалярных произведений для базиса v_1, v_2, v_3 :

$$\begin{pmatrix} 3 & 1 & 1 \\ 1 & 4 & 2 \\ 1 & 2 & 5 \end{pmatrix}.$$

Добавим вектор v_0 , для которого $v_1 + v_2 + v_3 + v_0 = 0$; матрица при этом расширится таким образом, что сумма всех столбцов и сумма всех строк будут нулевыми векторами:

$$\begin{pmatrix} 3 & 1 & 1 & -5 \\ 1 & 4 & 2 & -7 \\ 1 & 2 & 5 & -8 \\ -5 & -7 & -8 & 20 \end{pmatrix}.$$

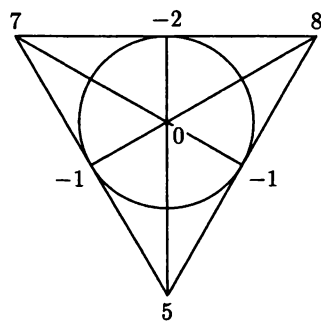
Поскольку некоторые из скалярных произведений положительны, этот супербазис тупоугольным не является. Равносильное утверждение состоит в том, что некоторые из чисел p_{ij} отрицательны:

$$p_{01} = 5, \quad p_{02} = 7, \quad p_{03} = 8, \quad p_{12} = -1, \quad p_{13} = -1, \quad p_{23} = 2.$$

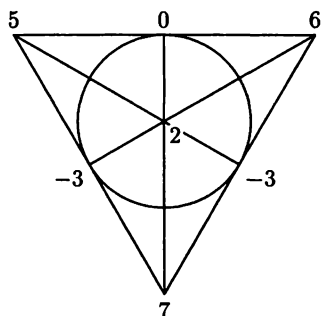
Выпишем все же эти «виртуальные конормы» на нашей двойственной плоскости Фано — см. рис. (а).

Из наших рассуждений в предыдущем параграфе вытекает, что мы можем добраться до соответствующих чисел в смежном супербазисе, прибавляя ϵ к трем числам, лежащим на прямой, соединяющей $-\epsilon$ и нуль, и вычитая ϵ из четырех чисел, не лежащих на этой прямой.

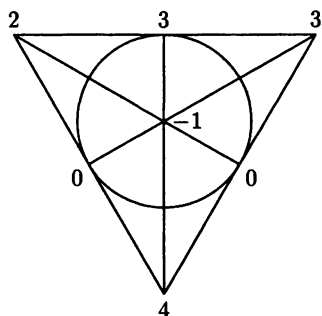
Если сделать это с вертикальной прямой на рис. (а), то получится рис. (б), на котором по-прежнему присутствуют два отрицательных числа. Поэтому мы повторим процесс для «круглой» прямой на этом рисунке и получим рисунок (в). Еще две такие операции дают рисунки (г) и (д), и на этом процесс завершается: коль скоро отрицательных



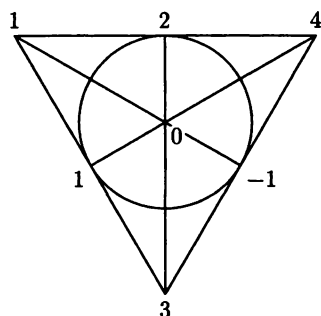
(a)



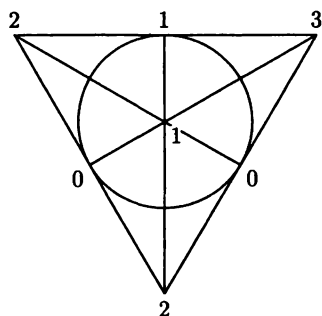
(б)



(в)



(г)



(д)

чисел нет, мы получили диаграмму конорм для тупоугольного супербазиса. Этот алгоритм всегда завершается, поскольку на каждом шаге уменьшается одна из «виртуальных конорм».

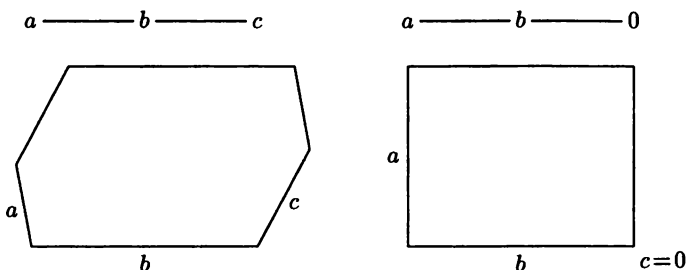
Конормы и параметры Зеллинга

Поскольку у трехмерной решетки всегда есть тупоугольный супербазис, получаем, что одна из конорм равна нулю, а остальные суть параметры Зеллинга p_{ij} для некоторого тупоугольного супербазиса. Стало быть, в этой размерности наша теория оказывается очень похожей на теорию, развитую Зеллингом в 1874 году и обобщенную позднее Вороным и Делоне на старшие размерности. Тем не менее, то, что мы добавляем еще и число 0, является значительным усовершенствованием: наше определение показывает, что семь конорм (в отличие от шести параметров Зеллинга) непрерывно зависят от решетки. Конормы также в некотором смысле инвариантны (параметры Зеллинга инвариантными в этом смысле не являются): две решетки, описываемые с помощью конорм, эквивалентны тогда и только тогда, когда их конормы отличаются на автоморфизм плоскости Фано.

Пять видов области Вороного

В двумерном случае мы выяснили, что форма области Вороного зависит только от количества 0-конорм.

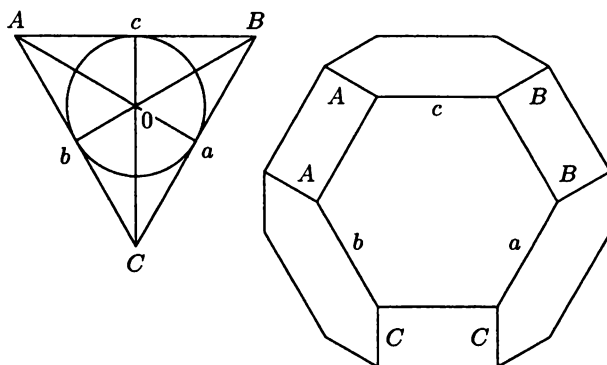
Три строго положительных конормы a , b и c дают шестиугольную область Вороного, вырождающуюся в прямоугольник, если $c=0$. (Две и более конормы обращаться в нуль не могут.)



В размерности 3 различные виды области Вороного также определяются тем, какие конормы равны нулю, с учетом того обстоятельства, что носитель функции конорм не может содержаться в прямой

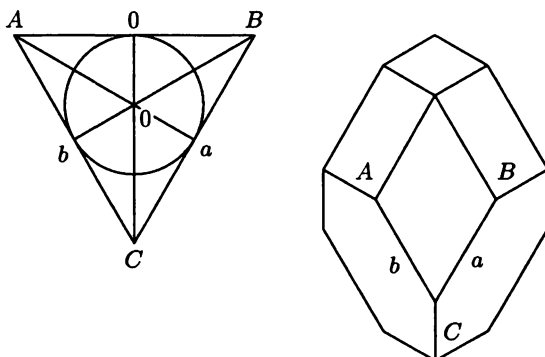
(в противном случае конорма этой прямой будет равна нулю). Имеется всего пять возможностей для такого обращения в нуль; мы их сейчас опишем.

Если имеются шесть ненулевых конорм a, b, c, A, B, C , то область Вороного представляет собой усеченный октаэдр (см. рисунок).

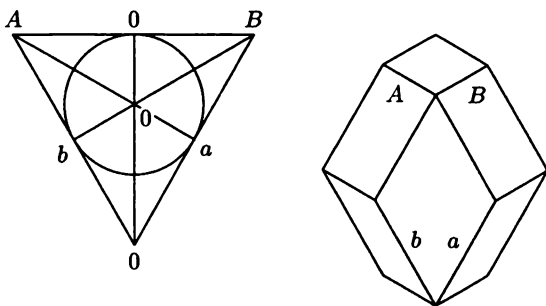


У этого многогранника имеется шесть классов параллельных ребер, соответствующих шести конормам, также обозначенным на рисунке.

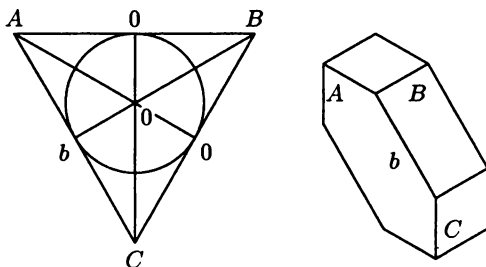
Если положить $c=0$, то все соответствующие ребра (на рисунке они горизонтальны) стянутся в точки, и мы получим многогранник, который иногда называют удлинненным додекаэдром; мы предпочитаем называть его *гексаромбическим додекаэдром*. У него четыре шестиугольные грани и восемь ромбических.



Третья возможность — это *ромбододекаэдр*, получаемый, если положить также $C=0$ (вертикальные ребра стягиваются). Теперь три обращающиеся в нуль конормы лежат на прямой в пространстве конорм.

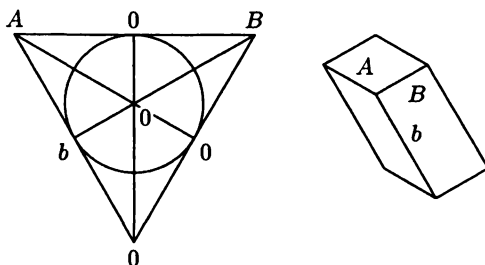


Если вместо этого стянуть a -ребра гексаромбического додекаэдра, то получится четвертый возможный вид области Вороного — шестигульная призма. Она характеризуется тем, что три нулевые конормы не лежат на одной прямой. Носитель конормы состоит из прямой и точки, не лежащей на этой прямой.



Наконец, если стянуть либо a -ребра ромбододекаэдра, либо C -ребра шестигульной призмы, то получим последнюю из возможных ячеек — прямоугольный параллелепипед.

Когда какая-то конорма обращается в нуль, соответствующие ребра (все имеющие одно направление) стягиваются в точку, поскольку в формулу для квадрата их длины эта конорма входит в качестве множителя. Прочие ребра и углы в многограннике при этом также претерпевают некоторые неочевидные изменения; для простоты мы на рисунках это обстоятельство проигнорировали. Надо также иметь



в виду, что под «ромбами» в названиях многогранников подразумеваются параллелограммы.

Итак, мы видим, как найти область Вороного двух- или трехмерной решетки, исходя из конорм. В добавлении мы вкратце опишем, как обстоит дело в размерности 4.

Решетки, соответствующие упаковкам сфер

Решетки, имеющие наименьший детерминант для данной минимальной нормы, называются *упаковками сфер*, поскольку они задают плотнейшие решеточные упаковки равных сфер. Если минимальная норма равна 2, то такие решетки известны вплоть до размерности 8: это решетки корней

$$A_0, A_1, A_2, D_3, D_4, D_5, E_6, E_7, E_8.$$

В размерности < 3 все просто; случай размерности 3 был разобран Гауссом [21] в 1831 году, случай размерностей 4 и 5 — Коркиным и Золотарёвым [28] в 70-х годах XIX века, а с размерностями 6, 7 и 8 разобрался Бlichфельд [4] к 1935 году. Рассуждения Бlichфельда были упрощены Морделлом [35], показавшим, что случай размерности 8 легко вывести из случая размерности 7, и Ветчинкиным [47]; вычисления, тем не менее, по-прежнему остаются очень запутанными (см. подробности в [11]). Мы приведем краткие наброски доказательств для $n = 2, 3$.

Если у двумерной решетки три конормы равны 2 (мы предположили, что это — минимальное значение), то форма решетки однозначно определена: это A_2 . Если же мы будем только требовать, чтобы значение 2 принимали не более чем две конормы, то появляется переменный параметр, и легко показать, что определитель можно уменьшить, сокращая третью конорму.

При $n=3$ аналогичное рассуждение показывает, что для минимальности определителя нужно, чтобы не менее шести конорм равнялись 2, поскольку матрица зависит от шести параметров. Но в этом случае последняя конорма должна равняться 4 (чтобы одна из конорм равнялась нулю), и этим решетка опять-таки определена однозначно: это решетка D_3 (изоморфная A_3).

Приведение по Минковскому

Коль скоро мы так подробно обсудили приведение двух- и трехмерных решеток по Вороному, представляется разумным по крайней мере упомянуть более известное понятие приведения по Минковскому.

Целочисленный базис $e_1, e_2, \dots, e_n$ называется *приведенным по Минковскому* базисом для f , если для каждого i значение $f(e_i)$ является наименьшим среди значений $f(e'_i)$ для всех целочисленных базисов $e_1, e_2, \dots, e_{i-1}, e'_i, e'_{i+1}, \dots, e'_n$. Положительно определенная форма f называется *приведенной по Минковскому*, если она задается матрицей относительно некоторого базиса, приведенного по Минковскому. Условие приведенности сводится к конечному числу неравенств

на элементы матрицы. Для бинарной формы $\begin{pmatrix} a & h \\ h & b \end{pmatrix}$ эти условия имеют вид

$$|2h| \leq a \leq b.$$

Для тернарной формы

$$\begin{pmatrix} a & h & g \\ h & b & f \\ g & f & c \end{pmatrix}$$

это условия

$$a \leq b \leq c, \\ 2|h| \leq a, \quad 2|g| \leq a, \quad 2|f| \leq b$$

и

$$2|h \pm g \pm f| \leq a + b.$$

При увеличении размерности число неравенств очень быстро растет; они выписаны в явном виде только до размерностей, не превосходящих 7.

Малая мафусаилова форма

С помощью условий Минковского доказываются многие теоремы теории чисел. В качестве примера мы воспользуемся ими для доказательства следующего забавного факта:

Т е о р е м а. *Малая мафусаилова форма*

$$F(x, y, z) = x^2 + 2y^2 + yz + 4z^2$$

представляет все целые числа от 1 до 30, но не представляет 31. Всякая целая положительно определенная тернарная форма G , неэквивалентная этой форме F , не представляет какое-нибудь целое число от 1 до 30.

Д о к а з а т е л ь с т в о. Из топокарты (см. ниже) следует, что числа

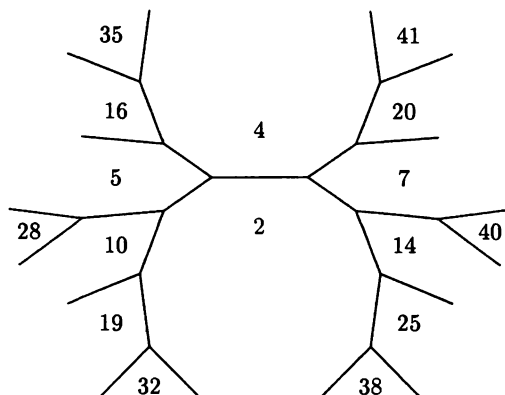
2, 4, 5, 7, 10, 14, 16, 19, 20, 25, 28, 32

суть наименьшие примитивные значения формы $2y^2 + yz + 4z^2$; умножая их на квадраты, получим, что числа в верхней строке суть все значения этой формы, не превосходящие 32.

0	2	4	5	7	8	10	14	16	18	19	20	25	28	32
1	3	5	6	8	9	11	15	17	19	20	21	26	29	
4	6	8	9	11	12	14	18	20	22	23	24	29	32	
9	11	13	14	16	17	19	23	25	27	28	29			
16	18	20	21	23	24	26	30	32						
25	27	29	30	32										

Остальные строки получены из первой прибавлением квадратов; в целом таблица показывает, что наша малая мафусаилова форма представляет все целые числа от 0 до 32, кроме 31.

Чтобы показать, что ни для какой другой формы G так не получится, предположим, что матрица для формы G есть общая (3×3) -матрица, приведенная по Минковскому (см. выше). Поскольку G представляет 1, получаем, что a должно равняться 1. Поскольку, однако, G представляет 2, получаем, что $b \leq 2$. Теперь можно перебрать все возможные бинарные подформы $\begin{pmatrix} a & h \\ h & b \end{pmatrix}$ и убедиться, что каждая из них не представляет некоторого числа $m \leq 5$; следовательно, у формы G должно быть $c \leq 5$. Неравенства Минковского показывают, что имеется только конечное число форм G , удовлетворяющих всем этим условиям; мы можем их перебрать и убедиться, что каждая из таких форм, не эквивалентных форме F , не представляет какое-нибудь число, меньшее 31. $\square$



Это рассуждение не объясняет, *почему* всякая положительно определенная целая тернарная форма обязана не представлять какое-то целое число. В постскрипуме мы увидим, что даже над рациональными числами положительно определенная тернарная форма какое-то целое число обязательно не представляет.

На прощанье

В этой лекции мы обобщили на трехмерный случай наше исследование положительно определенных бинарных квадратичных форм. В размерности 4 ситуация, как мы увидим в добавлении к лекции, становится ощутимо более сложной. Вместо всего одной «примитивной» (общей) формы области Вороного имеются целых три, только одна из которых имеет тупоугольный супербазис. Общее число видов возрастает с 5 до 52. В размерности 5 имеется 222 примитивных вида и чрезвычайно большое (до сих пор неизвестное) количество других видов.

Что же касается классификации целых положительно определенных квадратичных форм, то приведение по Минковскому оказывается очень полезным до размерности 8 включительно; до размерности 24 можно еще кое-что контролировать с помощью метода склейки, описанного в добавлении ко второй лекции. В более высоких размерностях такие формы перестают поддаваться классификации. С другой стороны, неопределенные формы ранга 3 и выше допускают полную классификацию с помощью совершенно других методов, как мы увидим в следующей лекции.

Д О Б А В Л Е Н И Е

Как нащупать форму четырехмерной решетки

Конормы и параметры Зеллинга

В основной части лекции мы показали, что в размерностях 2 и 3 вид области Вороного определяется расположением нулевых конорм. В размерности два область прямоугольна или шестиугольна в зависимости от того, есть нулевая конорма или такой нет. В размерности 3 зависимость формы области Вороного от числа нулевых конорм такова:

1	усеченный октаэдр;
2	гексаромбический додекаэдр;
3 (на одной прямой)	ромбододекаэдр;
3 (не на одной прямой)	шестиугольная призма;
4	прямоугольный параллелепипед.

Однако же всерьез конормы вступают в свои права только для четырехмерных решеток. С их помощью получается простое описание 52 типов решеток, найденное Делоне [15] с исправлениями Штогри-на [45].

По некоторому совпадению, в малых размерностях конормы практически эквивалентны параметрам Зеллинга. Именно, у решетки размерности

$$1, 2, 3, 4, 5, \dots, n, \dots$$

имеется

$$1, 3, 7, 15, 31, \dots, 2^n - 1, \dots$$

конорм, но всего лишь

$$1, 3, 6, 10, 15, \dots, \frac{n(n+1)}{2}, \dots$$

параметров Зеллинга.

В размерностях 1 и 2 конормы суть в точности параметры Зеллинга, а в размерности 3 конормы представляют собой параметры Зеллинга, к которым добавлен нуль. То же самое происходит с *некоторыми* решетками в любой размерности: если у решетки есть тупоугольный супербазис, то ее конормы суть параметры Зеллинга, к которым добавлены нули.

Четырехмерные графовые решетки

Шестнадцать четырехмерных решеток следующим образом параметризуются некоторыми подграфами полного графа K_5 на пяти вершинах. Вершины $\alpha, \beta, \gamma, \delta$ и ε суть пять характеров, произведение которых есть тривиальный характер; и мы имеем

$$\text{co}(\alpha) = \text{co}(\beta) = \text{co}(\gamma) = \text{co}(\delta) = \text{co}(\varepsilon) = 0$$

и $\text{co}(\lambda\mu) \neq 0$ тогда и только тогда, когда λ и μ соединены в графе ребром.

Кроме этого, есть еще ровно один случай, в котором возникают нулевые конормы. Он соответствует полному двудольному графу $K_{3,3}$ с шестью вершинами α, β, γ и $\delta, \varepsilon, \zeta$. В этом случае характеры $\alpha\beta\gamma$ и $\delta\varepsilon\zeta$ тривиальны, и имеем в точности шесть нулевых конорм:

$$\text{co}(\alpha) = \text{co}(\beta) = \text{co}(\gamma) = \text{co}(\delta) = \text{co}(\varepsilon) = \text{co}(\zeta) = 0.$$

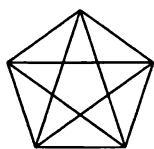
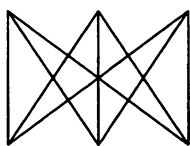
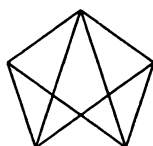
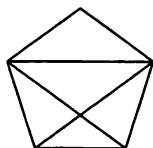
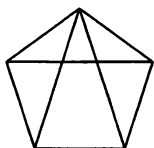
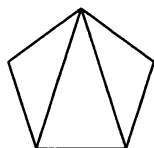
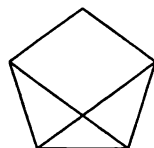
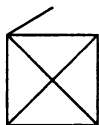
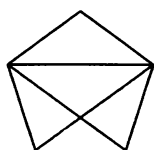
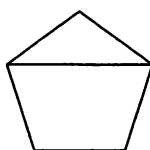
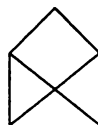
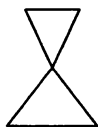
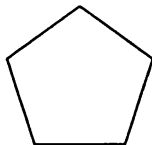
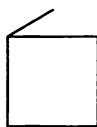
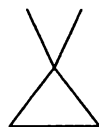
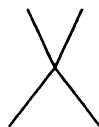
В каждом из этих семнадцати случаев мы можем указать точную форму решетки, надписав на ребрах соответствующего графа значения конорм. В нижеследующей таблице мы перечисляем эти семнадцать «графовых» решеток, указывая для них число определяющих их независимых параметров (по одному параметру для каждой ненулевой конормы). На рисунке на следующей странице изображены графы, соответствующие решеткам.

число параметров	решетки
10	K_5
9	$K_{3,3}, K_5 - 1$
8	$K_5 - 2, K_5 - 1 - 1$
7	$K_5 - 3, K_5 - 2 - 1, K_4 + 1, C_{2221}$
6	$K_4, C_{321}, C_{222}, C_3 + C_3$
5	$C_5, C_4 + 1, C_3 + 1 + 1$
4	$1 + 1 + 1 + 1$

Остальные четырехмерные решетки

Если нулевых конорм нет, то оказывается, что в точности три конормы отрицательны, причем эти отрицательные значения совпадают. Пусть, скажем, эти конормы суть α, β и γ , причем

$$\text{co}(\alpha) = \text{co}(\beta) = \text{co}(\gamma) = -p.$$

 K_5  $K_{3,3}$  $K_5 - 1$  $K_5 - 2$  $K_5 - 1 - 1$  $K_5 - 3$  $K_5 - 2 - 1$  $K_4 + 1$  C_{2221}  K_4  C_{321}  C_{222}  $C_3 + C_3$  C_5  $C_4 + 1$  $C_3 + 1 + 1$  $1 + 1 + 1 + 1$

Кроме того, оказывается, что $\alpha\beta\gamma$ — тривиальный характер. Тогда можно расположить (нетривиальные) характеры в виде таблицы

	α	β	γ
δ	$\alpha\delta$	$\beta\delta$	$\gamma\delta$
ε	$\alpha\varepsilon$	$\beta\varepsilon$	$\gamma\varepsilon$
ζ	$\alpha\zeta$	$\beta\zeta$	$\gamma\zeta$

причем можно считать, что характер $\delta\varepsilon\zeta$ тривиален. Ввиду нашего соглашения все три конормы в верхней строке имеют значение $-p$. Замечательно, что в каждой из остальных трех строк минимальная конорма равна p . Все 35 решеток классифицируются по расположе-

нию этих минимумов. Мы будем говорить, что решетка имеет тип rst , если минимум в этих строках достигается r , s и t раз.

При данных r , s и t конормы, равные p , могут располагаться несколькими неэквивалентными способами. Вот, например, как они расположены у нескольких решеток типа 322:

$$\begin{array}{ccc} \begin{bmatrix} & -p & -p & -p \\ p & p & & \\ p & p & & \\ p & p & & \end{bmatrix} & \begin{bmatrix} & -p & -p & -p \\ p & p & & p \\ p & p & & \\ & & p & p \end{bmatrix} & \begin{bmatrix} & -p & -p & -p \\ & p & p & p \\ p & p & & \\ p & & & p \end{bmatrix} \\ 322+ & 322- & 322' \end{array}$$

Для всякой решетки типа 322 обозначим характеры с конормой p через, скажем, $\delta_1, \delta_2, \delta_3; \varepsilon_1, \varepsilon_2; \zeta_1, \zeta_2$.

Цифра 2 соответствует паре характеров из одной строки, произведение которых является каким-то характером из первой строки. Если два или более из чисел rst равны 2, то мы добавляем штрихи в знак того, что соответствующие произведения характеров различны. Например, в первых двух наших примерах имеем $\varepsilon_1 \varepsilon_2 = \zeta_1 \zeta_2 = \alpha$, и штрихи не нужны, а вот в третьем примере $\varepsilon_1 \varepsilon_2 = \alpha$, но $\zeta_1 \zeta_2 = \beta$, откуда и обозначение 322'.

Впрочем, невзирая на отсутствие штрихов, первые два случая комбинаторно различны: в случае 322+ характеры

$$\delta_1 \varepsilon_1 \zeta_1, \quad \delta_1 \varepsilon_2 \zeta_2, \quad \delta_2 \varepsilon_1 \zeta_2, \quad \delta_2 \varepsilon_2 \zeta_1$$

все тривиальны, а в случае 322- имеются только две тривиальные тройки:

$$\delta_3 \varepsilon_1 \zeta_2, \quad \delta_3 \varepsilon_2 \zeta_1.$$

В общем случае мы ставим знак + или - в зависимости от того, будет число троек ijk , для которых $\delta_i \varepsilon_j \zeta_k$ — тривиальный характер, больше или меньше «ожидаемого» числа ijk .

Перечислим теперь 35 неграфовых случаев, сгруппированных по числу независимых параметров, определяющих решетку:

Число параметров	Решетки
10	111+, 111-
9	211+, 211-
8	311+, 311-, 221+, 221-, 22'1
7	411, 321+, 321-, 222+, 222-, 222', 22'2''

Число параметров	Решетки
6	421, 331+, 331-, 322+, 322-, 322'
5	431, 422, 422', 332+, 332-
4	441, 432, 333+, 333-
3	442, 433
2	443
1	444

Как видим, только в трех случаях (K_5 , 111+, 111-) достигается максимальное число параметров, равное 10. Вороной называл такие общие случаи *примитивными*. В размерности 5 количество примитивных случаев равно уже 222; они были перечислены Барановским и Рышковым в 1973 году (исправления позднее внес Энгель). В примитивном случае область Вороного имеет максимально возможное число граней, а именно $2(2^n - 1)$. Впрочем, в размерности 4 область Вороного для типа $K_{3,3}$ также имеет 30 граней, а в размерности 5 имеются три непримитивные решетки, области Вороного которых имеют тем не менее по 62 грани.

Л Е К Ц И Я 4

Простые ароматы

Введение

В лекции 3 мы расклассифицировали определенные формы в размерности ≤ 3 с помощью метода, равносильного геометрическому исследованию их ячеек Вороного. Однако же по своей глубинной сути квадратичные формы являются арифметическими объектами. Рассматривая сравнения по модулю степеней простых чисел, можно выписать арифметические инварианты, говорящие о форме очень многое: с помощью этих инвариантов полностью решается проблема рациональной эквивалентности любых форм.

Поле $\mathbb{Q}$ рациональных чисел можно расширять до больших полей $\mathbb{Q}_p$ — «полей p -адических чисел», по одному для каждого простого числа p . Хотя p -адические числа традиционно относятся к основам этой теории, в лекции мы ими на самом деле не пользуемся. Читатель, заинтересованный в более глубоком понимании предмета, найдет обсуждение p -адических чисел в добавлении.

Квадратичную форму над $\mathbb{Q}$ можно уподобить букету цветов, в котором каждый цветок представляет собой форму над одним из полей $\mathbb{Q}_p$. По запахам этих цветов мы сможем восстановить структуру рациональной формы.

В первой половине этой лекции мы приводим полную теорию рациональной эквивалентности квадратичных форм. Вторая половина, в которой изложение более подробно, посвящена целочисленным инвариантам. В ней приводится новое доказательство инвариантности, использующее введенное в лекции 2 понятие слышимости.

Эквивалентность над $\mathbb{Q}$; диагонализация

Если допустить преобразования с рациональными коэффициентами (например, замену базисного вектора e_1 на $e_2 - \frac{3}{2}e_1$), то задача

об эквивалентности форм упрощается. Пусть, например, матрица

$$\begin{matrix} & e_1 & e_2 & e_3 & e_4 \\ \begin{matrix} e_1 \\ e_2 \\ e_3 \\ e_4 \end{matrix} & \begin{pmatrix} 2 & 3 & 4 & 5 \\ 3 & 6 & 7 & 8 \\ 4 & 7 & 9 & 10 \\ 5 & 8 & 10 & 11 \end{pmatrix} \end{matrix}$$

представляет четырехмерную квадратичную форму, которую мы хотим диагонализировать. Лучше всего представлять себе, что в матрице представлены скалярные произведения четырех базисных векторов e_1, e_2, e_3, e_4 (см. выше); мы хотим найти базис из четырех попарно ортогональных векторов.

Для этого рассмотрим сначала промежуточный базис, состоящий из вектора $e'_1 = e_1$ и трех векторов

$$e'_2 = e_2 - \frac{3}{2}e_1, \quad e'_3 = e_3 - 2e_1, \quad e'_4 = e_4 - \frac{5}{2}e_1,$$

ортогональных к e_1 . Скалярные произведения этих векторов с исходными образуют матрицу

$$\begin{matrix} & e_1 & e_2 & e_3 & e_4 \\ \begin{matrix} e'_1 \\ e'_2 \\ e'_3 \\ e'_4 \end{matrix} & \begin{pmatrix} 2 & 3 & 4 & 5 \\ 0 & 3/2 & 1 & 1/2 \\ 0 & 1 & 1 & 0 \\ 0 & 1/2 & 0 & -3/2 \end{pmatrix} \end{matrix},$$

полученную из исходной с помощью вычитания первой строки, умноженной на $3/2$, из второй строки, вычитания удвоенной первой строки из третьей строки и вычитания первой строки, умноженной на $5/2$, из четвертой строки. Чтобы получить скалярные произведения новых векторов друг с другом, надо произвести аналогичные операции со столбцами (сводящиеся к тому, что три элемента матрицы заменяются на нули):

$$\begin{matrix} & e'_1 & e'_2 & e'_3 & e'_4 \\ \begin{matrix} e'_1 \\ e'_2 \\ e'_3 \\ e'_4 \end{matrix} & \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 3/2 & 1 & 1/2 \\ 0 & 1 & 1 & 0 \\ 0 & 1/2 & 0 & -3/2 \end{pmatrix} \end{matrix}.$$

Итак, первый шаг диагонализации завершен. Поскольку следующий диагональный элемент, а именно $3/2$, отличен от нуля, мы можем продолжать в том же духе, вычитая кратные второй строки из третьей

и четвертой строк и проводя аналогичные операции над столбцами; в результате получится матрица

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3/2 & 0 & 0 \\ 0 & 0 & 1/3 & -1/3 \\ 0 & 0 & -1/3 & -5/3 \end{pmatrix},$$

которая на следующем шаге станет уже диагональной:

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3/2 & 0 & 0 \\ 0 & 0 & 1/3 & 0 \\ 0 & 0 & 0 & -2 \end{pmatrix}.$$

На каждом из этих шагов матрица формы умножается справа на некоторую рациональную матрицу, а затем слева на транспонированную к ней. Стало быть, мы доказали, что для некоторой матрицы M имеем

$$M^t \cdot \begin{pmatrix} 2 & 3 & 4 & 5 \\ 3 & 6 & 7 & 8 \\ 4 & 7 & 9 & 10 \\ 5 & 8 & 10 & 11 \end{pmatrix} \cdot M = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3/2 & 0 & 0 \\ 0 & 0 & 1/3 & 0 \\ 0 & 0 & 0 & -2 \end{pmatrix}.$$

Иными словами, наша форма рационально эквивалентна форме вида $\text{diag} \left[2, \frac{3}{2}, \frac{1}{3}, -2 \right]$; мы будем сокращенно писать просто $\left[2, \frac{3}{2}, \frac{1}{3}, -2 \right]$.

Тот же подход работает для всякой формы, имеющей хоть один ненулевой элемент на диагонали. Если все диагональные элементы равны нулю, но какой-то внедиагональный элемент a_{ij} от нуля отличен, модифицируем матрицу с помощью следующего трюка: прибавим j -ю строку к i -й, а затем j -й столбец к i -му — в результате получится ненулевой диагональный элемент $2a_{ij}$. Если же ненулевых элементов у матрицы нет, то она уже диагональна. Итак, мы показали, что над рациональными числами всякую квадратичную форму можно диагонализировать.

Проблема инварианта

Пусть, однако, в нашем примере мы начали с правого нижнего элемента и организовали нули в нижней строке и правом столбце; тогда получится матрица

$$\begin{pmatrix} -3/11 & -7/11 & -6/11 & 0 \\ -7/11 & 2/11 & -3/11 & 0 \\ -6/11 & -3/11 & -1/11 & 0 \\ 0 & 0 & 0 & 11 \end{pmatrix};$$

продолжая далее снизу вверх, мы придем в конце концов к матрице

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1/11 & 0 \\ 0 & 0 & 0 & 11 \end{pmatrix}.$$

Стало быть, мы доказали, что

$$\left[2, \frac{3}{2}, \frac{1}{3}, -2\right] = \left[2, 1, -\frac{1}{11}, 11\right],$$

где знак равенства обозначает рациональную эквивалентность.

Нам нужно уметь выяснять, в каком случае две диагональные формы эквивалентны над рациональными числами. Такие эквивалентности вовсе не самоочевидны: $2x^2 + 2y^2$ равно $(x+y)^2 + (x-y)^2$ и тем самым эквивалентно $x^2 + y^2$, что, в свою очередь, эквивалентно $5x^2 + 5y^2$, но не $3x^2 + 3y^2$!

Мы найдем ответ на такие вопросы с помощью инвариантов

$$\sigma_{-1}, \sigma_2, \sigma_3, \sigma_5, \sigma_7, \dots,$$

называемых *p-адическими сигнатурами*, вкупе с определителем формы. Заметим, что сам по себе определитель инвариантом формы, собственно говоря, не является: инвариантен определитель, рассматриваемый с точностью до умножения на ненулевые квадраты рациональных чисел.

Сигнатура σ_p определяет то, что мы назвали во введении «запахом» формы над $\mathbb{Q}_p$. Это название уместно, потому что термин «сигнатура» действительно употребляется в парфюмерии!

Сигнатуры квадратичной формы

Всякое ненулевое рациональное число можно единственным способом разложить в произведение степеней простых чисел. Например,

$$-4\frac{1}{2} = (-1) \times 2^{-1} \times 3^2.$$

Отметим, что мы рассматриваем (-1) как простое число наравне с остальными, но это простое число имеет только две степени, 1 и -1 , так что это простое число порядка 2.

Если число разложено в произведение степеней простых, то входящая в это произведение степень p называется *p-частью* числа. Мы определим *p-сигнатуры* через эти *p-части*. Например, обычная сигнатура, введенная Сильвестром, есть сумма (-1) -частей диагональных

элементов. Обозначим ее через σ_{-1} ; покажем, как определить аналогичные сигнатуры σ_p для остальных простых чисел. Поскольку диагональные элементы можно умножать на ненулевые квадраты, будем считать, что эти элементы являются целыми числами.

Итак, пусть f — диагональная форма с целыми коэффициентами. Чтобы определить $\sigma_p(f)$, где p — нечетное простое число, сложим p -части коэффициентов и прибавим к сумме по четверке за каждый p -адический антиквадрат. Здесь число $a = p^r a'$ называется p -адическим антиквадратом, если p нечетно, а a' не является квадратичным вычетом по модулю p (так что a не является квадратом сразу по двум причинам: его p -часть не является квадратом, а все остальное не является квадратом даже по модулю p). При $p \neq -1$ эти сигнатуры определены только по модулю 8.

Например, 3-сигнатура формы $[10, -9, 21, 6]$ есть

$$\begin{array}{r} 1+9+3+3 \\ +4 \end{array}$$

(то есть $4 \pmod{8}$), поскольку 6 есть 3-адический антиквадрат. Для той же формы 5-сигнатура есть

$$\begin{array}{r} 5+1+1+1 \\ +4, \end{array}$$

то есть опять-таки $4 \pmod{8}$. А вот 7-сигнатура этой формы равна

$$\begin{array}{r} 1+1+7+1 \\ +4, \end{array}$$

то есть $6 \pmod{8}$.

2-сигнатура, или *нечетность*, формы получается, напротив, если сложить нечетные части коэффициентов, включая знаки (при $p=2$ всё всегда вверх ногами), а затем прибавить по четверке за каждый элемент вида $2^{\text{нечетное}}(8k \pm 3)$, являющийся 2-адическим антиквадратом.

Например, 2-сигнатура все той же формы есть

$$\begin{array}{r} 5-9+21+3 \\ +4 \qquad +4, \end{array}$$

то есть $4 \pmod{8}$.

Наконец, (-1) -сигнатура этой формы равна, разумеется,

$$1-1+1+1,$$

то есть целому числу 2. Важно помнить, что только (-1) -сигнатура является целым числом; все остальные сигнатуры определены только по модулю 8.

Теорема Минковского–Хассе и глобальное соотношение

Определенные выше сигнатуры полностью решают проблему эквивалентности. *Две формы одной размерности f и g рационально эквивалентны тогда и только тогда, когда равны их определители (по модулю квадратов) и равны их p -сигнатуры для всех простых $p = -1, 2, 3, 5, \dots$* Это — знаменитая теорема Минковского–Хассе, переформулированная несколько нетрадиционным образом. Проверим с помощью этой теоремы установленную нами эквивалентность форм

$$\left[2, \frac{3}{2}, \frac{1}{3}, 2\right] \quad \text{и} \quad \left[2, 1, -\frac{1}{11}, 11\right].$$

Умножая на квадраты, получим эквивалентные формы

$$[2, 6, 3, -2] \quad \text{и} \quad [2, 1, -11, 11].$$

Подсчитаем их сигнатуры:

$$\begin{aligned} \sigma_2: \quad & \frac{1+3+3-1}{+4} \equiv 2 \equiv 1+1-11+11, \\ \sigma_{-1}: \quad & 1+1+1-1 = 2 = 1+1-1+1, \\ \sigma_3: \quad & \frac{1+3+3+1}{+4} \equiv 4 \equiv 1+1+1+1, \\ \sigma_{11}: \quad & 1+1+1+1 \equiv 4 \equiv \frac{1+1+11+11}{+4} \end{aligned}$$

и

$$\sigma_p: \quad 1+1+1+1 \equiv 4 \equiv 1+1+1+1$$

для всех прочих p (все сравнения берутся по модулю 8).

На самом деле наша « p -адическая сигнатура» инвариантна относительно преобразований над большим полем $\mathbb{Q}_p$ (полем p -адических чисел), так что из нашей формулировки вытекает стандартная

Т е о р е м а. *Две квадратичные формы f и g эквивалентны над $\mathbb{Q}$ тогда и только тогда, когда они эквивалентны над $\mathbb{Q}_p$ для всех простых чисел p (включая -1).*

p -адические структуры для различных p являются почти (хотя и не вполне) независимыми. Оказывается, что между ними имеет-ся ровно одно соотношение, которое мы будем называть *глобальным*

соотношением (обычно оно встречается в виде «формулы произведения»). Чтобы сформулировать это соотношение, немного модифицируем наши инварианты: определим p -избытки формы f , обозначаемые $e_p(f)$, так:

$$e_p(f) = \sigma_p(f) - \dim(f), \quad \text{если } p \neq 2;$$

$$e_2(f) = \dim(f) - \sigma_2(f).$$

Глобальное соотношение состоит в следующем.

Теорема. Сумма p -избытков по всем p (включая -1) делится на 8.

По существу, это единственное соотношение между определителем и p -избытками. В самом деле, предположим, что для каждого p существует форма с заданным значением d и заданным p -избытком. Тогда мы покажем в постскрипуме, что (единственная) рациональная форма, достигающая всех этих значений одновременно, существует в точности тогда, когда выполнено глобальное соотношение.

В нескольких последующих параграфах мы докажем теорему Минковского–Хассе с помощью последовательных редукций.

Редукция к случаю тривиальных инвариантов

Мы сейчас покажем, что достаточно рассматривать только формы с *тривиальными инвариантами*, т.е. формы, определитель которых является квадратом, а все размерности и p -сигнатуры кратны 8.

В следующих параграфах мы покажем, что форма с тривиальными инвариантами эквивалентна форме вида

$$[\pm 1, \pm 1, \dots, \pm 1].$$

Эта редукция использует результат, называемый *теоремой Витта о сокращении*, который утверждает, что если форма h невырождена и при этом $h \oplus f$ эквивалентна $h \oplus g$ (над полем характеристики, отличной от 2), то f и g эквивалентны. Если инварианты форм f и g совпадают, то формы

$$g \oplus g \oplus g \oplus g \oplus g \oplus g \oplus g \oplus f$$

и

$$g \oplus g \oplus g \oplus g \oplus g \oplus g \oplus g$$

имеют одинаковые (тривиальные) инварианты, так что из сформулированного выше утверждения вытекает, что они эквивалентны, а из теоремы Витта тогда следует, что эквивалентны f и g .

Доказательство теоремы Витта о сокращении

При доказательстве теоремы Витта достаточно рассмотреть случай одномерной формы h , то есть доказать, что если

$$[a, b, c, \dots] = [a, b', c', \dots]$$

и $a \neq 0$, то

$$[b, c, \dots] = [b', c', \dots].$$

Первое из этих равенств означает, что в пространстве, порожденном ортогональными векторами $e_1, e_2, e_3, \dots$, для которых

$$e_1 \cdot e_1 = a, \quad e_2 \cdot e_2 = b, \quad e_3 \cdot e_3 = c, \quad \dots,$$

имеется и базис из ортогональных векторов $e'_1, e'_2, \dots$, для которых

$$e'_1 \cdot e'_1 = a, \quad e'_2 \cdot e'_2 = b', \quad e'_3 \cdot e'_3 = c',$$

Нам достаточно найти изометрию этого пространства, переводящую e_1 в e'_1 , поскольку эта изометрия с неизбежностью переведет подпространство $\langle e_2, e_3, \dots \rangle$, ортогональное к e_1 , в подпространство $\langle e'_2, e'_3, \dots \rangle$, ортогональное к e'_1 . Как известно, отражение от гиперплоскости, перпендикулярной вектору r , задается формулой

$$x \mapsto x - \frac{2(x, r)}{(r, r)} r.$$

Легко проверить, что это преобразование сохраняет нашу квадратичную форму (x, x) . Если $r = e_1 - e'_1$, то это отражение действительно переводит e_1 в e'_1 . Впрочем, не все так просто: отражения возможны только относительно векторов ненулевой длины, тогда как форма, с которой мы работаем, может быть неопределенной, так что может случиться, что нормы некоторых ненулевых векторов равны нулю. Однако же если норма r равна нулю, то можно провести отражение относительно вектора $s = e_1 + e'_1$ (при этом e_1 перейдет в $-e'_1$), а затем умножить на -1 . Оба числа (r, r) и (s, s) равняться нулю не могут, поскольку ввиду тождества Аполлония имеем

$$(r, r) + (s, s) = 2(e_1, e_1) + 2(e'_1, e'_1) = 4a \neq 0.$$

Заменяем p -члены

Итак, мы можем предполагать, что форма имеет тривиальные инварианты; мы хотим, чтобы все элементы матрицы равнялись ± 1 . На

самом деле мы найдем соответствующее преобразование не для самой f , а для подходящей прямой суммы

$$f \oplus [\pm 1, \pm 1, \dots, \pm 1],$$

а затем заключим с помощью теоремы Витта, что такое преобразование существует и для f . Пусть f имеет диагональный вид со свободными от квадратов коэффициентами, и пусть p — наибольшее из простых чисел, делящих какой-либо из коэффициентов. Назовем p -членами диагональные элементы вида

$$pq_0q_1q_2\dots q_t \quad (-1 \leq q_i < p).$$

Первым делом мы упростим такой p -член, заменив его сомножитель $q_0q_1q_2\dots q_t$ на нечто более удобоваримое.

Лемма о замене. Пусть $p \geq 3$. Тогда для данного p -члена

$$pq_0q_1q_2q_3\dots q_t = pqt \quad (-1 \leq q < p)$$

и данного числа q' при выполнении условий

$$-1 \leq q < p, \quad -1 \leq q' < p,$$

$$qq' \text{ сравнимо с квадратом по модулю } p$$

можно заменить коэффициенты pqt , 1 , -1 на $pq't$, $*$, $*$, где простые делители чисел, обозначенных звездочками, меньше, чем p .

Доказательство. Существует целое число x , для которого

$$qq' \equiv x^2 \pmod{p}$$

и $|x| < \frac{1}{2}p$. Тогда можно записать равенство $qq' = x^2 - py$, где $-p^2 < py < p^2$, так что $|y| < p$. Следовательно,

$$pqt \left(\frac{q'}{x}\right)^2 + yq't \left(\frac{p}{x}\right)^2 = pq't.$$

Стало быть, форма $[pqt, yq't]$ представляет $pq't$, так что

$$[pqt, yq't] = [pq't, *],$$

причем из рассмотрения определителя вытекает, что число $*$ должно быть равно произведению yqt на полный квадрат. Кроме того, форма $[1, -1]$, то есть $x^2 - y^2$, представляет все числа, так что то же рассуждение показывает, что

$$[-1, 1] = [m, -m]$$

для всякого $m \neq 0$.

Следовательно, форма

$$[pqt, 1, -1]$$

рационально эквивалентна форме

$$[pqt, yq't, -yq't],$$

а эта последняя, в свою очередь, эквивалентна форме

$$[pq't, yqt, -yq't],$$

что и требовалось. □

Заключительный удар

Пусть теперь $u = r + 1$ — наименьший квадратичный невычет по модулю p . Тогда для данного p -члена $pq_0q_1q_2\dots q_s$ мы можем последовательно заменить каждое из q_i на 1 или u и тем самым заменить весь p -член на p или pu , поскольку квадраты можно отбрасывать.

Однако форма $[p, pr]$ представляет число pu и тем самым эквивалентна $[pu, pru]$. Число же $r = u - 1$ является квадратичным вычетом (в силу выбора u) и тем самым может быть заменено на 1. Стало быть, с помощью таких последовательных замен мы можем заменить пару p -членов p, p на p, pr , затем на pu, pru , а затем и на pu, pu .

Короче говоря, мы можем заменить пару p -членов p, p на pu, pu или наоборот. Отсюда вытекает следующее утверждение:

Лемма о свободе. Один из двух данных p -членов можно выбрать по своему усмотрению.

В самом деле, если они совпадают, то можно произвести замену, а если они различны, то можно поменять их местами. □

Заметим теперь, что в силу предположения хотя бы один p -член у нас есть, а поскольку определитель является квадратом, таких членов не менее двух. Первый из этих членов можно выбирать произвольно; пусть он равен $-p$. Если имеется три или более p -членов, сделаем второй из них равным p , а затем избавимся от двух p -членов, пользуясь эквивалентностью $[p, -p] = [1, -1]$.

В оставшемся случае, когда p -членов ровно два, они имеют вид либо $-p, p$ (и тогда от них можно избавиться), либо $-p, pu$. Однако же очевидно, что p -сигнатуры в этих двух случаях отличаются на 4, и поскольку в случае $-p, p$ сигнатура тривиальна, второй случай встретиться не может.

Подытожим: если число p , являющееся наибольшим из простых делителей коэффициентов, больше или равно 3, то мы можем избавиться от всех p -членов. Стало быть, в конечном счете все сводится к случаю $p=2$, где рассуждение даже проще.

Именно, мы можем уничтожить все 2-члены (количество которых должно быть четно) с помощью эквивалентностей

$$[2, 2] = [1, 1],$$

$$[2, -2] = [1, -1],$$

$$[-2, -2] = [-1, -1].$$

Значит, в конце концов мы приходим к случаю $p=-1$ и приведем f к требуемому виду

$$[\pm 1, \pm 1, \dots, \pm 1].$$

Если теперь формы f и g имеют одинаковые инварианты (включая σ_{-1}), то

$$g \oplus g \oplus g \oplus g \oplus g \oplus g \oplus g \oplus f$$

и

$$g \oplus g \oplus g \oplus g \oplus g \oplus g \oplus g \oplus g$$

имеют одинаковые (тривиальные) инварианты, так что они обе могут быть приведены к форме такого вида. Более того, это будет *та же самая* форма, поскольку ранг и сигнатура этих форм совпадают. Теперь можно применить теорему Витта о сокращении и заключить, что f и g эквивалентны.

Другие версии теоремы Минковского–Хассе

Большинство авторов вместо наших сигнатур пользуются инвариантами, принимающими только значения 1 и -1 , но в литературе встречается такое количество разных инвариантов этого типа, что немудрено запутаться. Представляется, что четыре таких инварианта заслуживают специальных названий: это *единица Минковского*

$$C_p(f) = \left(\frac{b_1}{p}\right) \left(\frac{-b_2}{p}\right) \left(\frac{b_3}{p}\right) \left(\frac{-b_4}{p}\right) \dots,$$

сопряженная единица Минковского

$$C_p(-f) = \left(\frac{-b_1}{p}\right) \left(\frac{b_2}{p}\right) \left(\frac{-b_3}{p}\right) \left(\frac{b_4}{p}\right) \dots,$$

неполное гильбертово произведение¹

$$(f)_p = \prod_{i < j} (a_i, a_j)_p$$

и полное гильбертово произведение

$$(f)_p^* = \prod_{i \leq j} (a_i, a_j)_p.$$

В этих формулах подразумевается, что форма f есть $[a_1, a_2, a_3, \dots]$, а $b_1, b_2, \dots$ суть p' -части² чисел a_j , делящихся на нечетные степени p .

Символ Лежандра $\left(\frac{b}{p}\right)$ равен 1 или -1 в зависимости от того, является b квадратом по модулю p или нет, а гильбертов символ норменного вычета $(a_i, a_j)_p$ равен по определению 1 или -1 в зависимости от того, совпадают или нет p -сигнатуры форм $[a_i, a_j]$ и $[1, a_i a_j]$.

Возможно, ситуацию прояснит следующее замечание. Для всякой размерности $n > 2$ и определителя d существуют ровно две неэквивалентные формы над $\mathbb{Z}_p$: та, которая первой пришла вам в голову, и еще одна.

Теперь вы можете определить свой личный инвариант, объявив, что он принимает значение $+1$ для формы, которая первой пришла вам в голову, и -1 для другой формы. Если первой вам пришла в голову одна из перечисленных ниже форм, то ваш инвариант совпадает с инвариантом, указанным в соответствующей строке:

$[d_p, d_{p'}, 1, 1, 1, \dots, 1]$	для	$C_p(f)$,
$[-d_p, -d_{p'}, 1, 1, \dots, 1]$	для	$C_p(-f)$,
$[d, 1, 1, \dots, 1]$	для	$(f)_p$,
$[-d, -1, 1, \dots, 1]$	для	$(f)_p^*$.

Инварианты целых форм

На этом пока завершается наше обсуждение рациональных форм. Мы не доказали, что наши p -сигнатуры действительно являются инвариантами (об этом пойдет речь в добавлении к лекции). Не затрагивали мы и вопросов о существовании форм с заданными инвариантами

¹В отечественной литературе оно называется инвариантом Хассе. — Прим. перев.

²Под p' -частью числа m автор понимает результат деления m на максимальную степень p , являющуюся делителем m . — Прим. перев.

или о соотношениях между инвариантами — об этом мы поговорим в постскрипуме. В оставшихся параграфах этой лекции мы построим некоторые инварианты квадратичных форм над целыми числами.

Читатель, желающий сразу перейти к постскрипуму, может это сделать, поскольку теория, к изложению которой мы переходим, в нем не используется.

***p*-адическая диагонализация и *p*-адические символы**

Мы продемонстрировали, как можно диагонализировать любую форму над рациональными числами. Оказывается, что для всякого простого $p \geq 3$ такую диагонализацию можно провести, ни разу не деля на p — при этом получится то, что называется *p-адически целой диагонализацией*. [В добавлении мы увидим, что она соответствует диагонализации над кольцом $\mathbb{Z}_p$ целых *p*-адических чисел.]

При $p = -1$ соответствующее понятие — диагонализация над кольцом $\mathbb{R}$ действительных чисел. [В этом контексте $\mathbb{R}$ обозначается также $\mathbb{Z}_{-1}$ или $\mathbb{Q}_{-1}$. Это хорошо известно из линейной алгебры; сильвестров закон инерции утверждает, что числа n_+ и n_- , то есть количество положительных и отрицательных диагональных коэффициентов, являются инвариантами. Мы будем описывать эту ситуацию в таких терминах: *(-1)-адический символ* есть $(+)^{n_+}(-)^{n_-}$.]

При $p \geq 3$ мы действуем следующим образом. В общем случае, когда степень p , делящая какой-то из диагональных коэффициентов, является наименьшей степенью простого, делящей *какой-нибудь* коэффициент, мы можем начать диагонализацию с этого коэффициента, поскольку делить на p при этом не потребуется. Если наименьшая степень p появляется во внедиагональном коэффициенте a_{ij} , мы можем свести ситуацию к нормальному случаю с помощью того же приема, что при обычной диагонализации формы, прибавив j -й столбец к i -му столбцу и j -ю строку к i -й строке.

Стало быть, для всякого нечетного p мы можем привести форму с помощью *p*-адической диагонализации к виду

$$[a, b, c, \dots, pa', pb', \dots, p^2a'', \dots, \dots],$$

где все числа $a, b, c, \dots, a', b', \dots, a'', \dots$ взаимно просты с p (случай $p = -1$ не исключается; под «взаимно простыми с -1 » числами понимаются числа положительные).

Формы

$$f_1 = [a, b, c, \dots], \quad f_p = [a', b', c', \dots], \quad f_{p^2} = [a'', b'', c'', \dots]$$

называются *жордановыми компонентами* формы f , а разложение

$$f_1 \oplus p f_p \oplus \dots \oplus q f_q \oplus \dots$$

называется ее *жордановым разложением*. Жордановы компоненты являются *p -адическими единичными формами*, иными словами, их определитель не делится на p (а при $p = -1$ они положительно определены).

Оказывается, что при $p \neq 2$ размерности, определители (с точностью до p -адических квадратов, как всегда) и p -сигнатуры жордановых компонент образуют полный набор инвариантов относительно p -адической эквивалентности. Удобно собрать всю эту информацию в *p -адический символ*. Типичный p -адический символ имеет вид наподобие

$$1^{\pm l} p^{\pm k} \dots q^{\pm n} \dots$$

В общем случае мы имеем формальное произведение выражений вида $q^{\pm n}$, где q — степень p , n — размерность f_q , а знак — символ Лежандра $\left(\frac{\det(f_q)}{p}\right)$.

Например, $[1, 2, 3]$ имеет 3-адический символ $1^{-2}3^{+1}$, поскольку 2 является квадратичным невычетом по модулю 3.

2-адическое жорданово разложение; 2-адический символ

При $p = 2$ ситуация становится более сложной. Если существует диагональный элемент, делящийся на наименьшую из возможных степеней двойки, то можно действовать, как и ранее. Если, однако, наименьшая степень двойки встречается только в некотором внедиагональном элементе a_{ij} , то сведение к этому случаю не проходит, поскольку после нашего стандартного трюка на диагонали появится $2a_{ij}$, а не a_{ij} . В таком случае нам остается только смириться с той ситуацией, когда ведущий (2×2) -минор можно привести к виду

$$q \begin{pmatrix} a & h \\ h & b \end{pmatrix}, \quad a \text{ и } b \text{ четны, } h \text{ нечетно,}$$

где q — наименьшая степень двойки, делящая все элементы матрицы.

Вместо того чтобы диагонализировать f , нам придется представлять ее в виде прямой суммы диагональных форм и (2×2) -матриц вышеуказанного вида для различных значений q . Тем не менее, поскольку при этом число $ab - h^2$ нечетно, у нас по-прежнему получится

жорданово разложение

$$f_1 \oplus 2f_2 \oplus 4f_4 \oplus \dots \oplus qf_q \oplus \dots,$$

в котором каждая из f_q является 2-адической единичной формой. Далее, мы можем считать, что либо все диагональные коэффициенты формы f_q четны (форма типа II), либо f_q имеет положительную размерность и имеет нечетный диагональный элемент (форма типа I). Всю эту информацию можно собрать в 2-адическом символе; по определению, это формальное произведение множителей вида

$$q_t^{\pm n},$$

где знак — символ Якоби $\left(\frac{2}{\det(f_q)}\right)$, n — размерность, причем $t = \infty$ для формы f_q типа II и $t = \text{Tr}(f_q) \bmod 8$, если форма f имеет тип I и диагональна.

Полезно заметить, что:

в показателе степени имеем знак +, если $\det(f_q) \equiv \pm 1 \pmod{8}$,
в показателе степени имеем знак —, если $\det(f_q) \equiv \pm 3 \pmod{8}$.

Если, например,

$$f = [1, 3, 5] \oplus 2 \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \oplus 4[1, 1],$$

то 2-адический символ имеет вид

$$1_1^{+3} 2_\infty^{-2} 4_2^{+2},$$

поскольку

$$\begin{array}{lll} 1 \times 3 \times 5 \equiv \pm 1, & \det \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \equiv \pm 3; & 1 \times 1 \equiv \pm 1, \\ 1 + 3 + 5 \equiv 1; & & 1 + 1 \equiv 2, \end{array}$$

где все сравнения — по модулю 8.

Числа, входящие в 2-адический символ, являются инвариантами жордановых компонент f_q . Тут, однако, имеется следующая трудность. При $p=2$ у формы может быть другое жорданово разложение $f'_1 \oplus 2f'_2 \oplus \dots$, и при этом новые жордановы компоненты f'_q не обязаны иметь те же инварианты, что и f_q . Имеются два правила модификации 2-адических символов, позволяющие бороться с этой трудностью.

Правило слияния нечетностей состоит в том, что во всякой цепочке форм $f_q, f_{2q}, f_{4q}, \dots$ (без пропусков), в которой все значения t конечны, мы можем любым образом менять значения t для отдельных форм при условии, что сумма этих значений остается неизменной.

Правило движения знаков утверждает, что мы можем изменить знаки двух форм f_q и $f_{2^r q}$ за счет изменения значений t для некоторых форм при условии, что в цепочке форм

$$f_q, f_{2q}, \dots, f_{2^{r-1}q}, f_{2^r q}$$

никакие две последовательные формы не относятся к типу II.

Именно, в процессе движения от f_q до $f_{2^r q}$ всякий раз, когда мы переходим от f_Q к f_{2Q} , хотя бы одна из этих форм обязана иметь тип I, и при этом мы прибавляем 4 к значению t для встречающихся по дороге нечетных форм. (Мы не можем изменить значение $t = \infty$ для четной формы.)

Имеет место следующий факт: две формы являются 2-адически целочисленно эквивалентными тогда и только тогда, когда их 2-адические символы можно перевести один в другой с помощью описанных выше преобразований.

Род

Говорят, что две целые квадратичные формы относятся к одному роду, если они p -адически эквивалентны для каждого p . Поскольку наш p -адический символ является полным инвариантом относительно p -адической эквивалентности, можно объединить все то, что было сказано об этой эквивалентности, в следующей теореме.

Т е о р е м а. *Две квадратичные формы f и g принадлежат к одному роду тогда и только тогда, когда их p -адические символы совпадают для всех p , включая -1 .*

(Разумеется, «совпадающие 2-адические символы» означает «2-адические символы, которые можно связать с помощью цепочки слияний нечетностей и движений знаков».)

В оставшейся части лекции мы объясняем, как доказывается инвариантность этих символов.

p -адические гауссовы средние

Во второй лекции мы определили инварианты, называемые гауссовыми средними. Для дальнейшего нам будет очень удобно немного изменить их определения и обозначать через $GM(f)$ то, что мы раньше называли гауссовым средним формы $f/2$, т. е. среднее значение чисел

$$e^{\pi i N(v)} \quad (v \in L^*),$$

где L^* — решетка, двойственная к L . Конечно, в этой лекции разумно выделить часть этих средних, инвариантную относительно p -адических целочисленных преобразований для каждого p . Поэтому мы определим также p -адическое гауссово среднее $GM_p(f)$ как среднее p -частей тех же самых чисел

$$e^{\pi i N(v)} \quad (v \in L^*).$$

[Заметим, что всякий корень из единицы α единственным образом представляется в виде произведения двух корней из единицы β и γ , где порядок β является степенью p , а порядок γ взаимно прост с p . Число β называется p -частью корня из единицы α , а число γ — его p' -частью.]

p -адическое гауссово среднее действительно зависит только от класса эквивалентности f над целыми p -адическими числами $\mathbb{Z}_p$. Тем не менее, как мы отмечали в начале лекции, p -адические числа нам на самом деле не нужны. Поэтому мы только вкратце объясним, почему эти средние инвариантны относительно целых p -адических преобразований, т.е. рациональных преобразований, не использующих деления на p . Причина в том, что при таких преобразованиях слагаемые гауссова среднего умножаются только на корни из единицы порядков, взаимно простых с p , а p -части от этого измениться не могут.

Теперь мы покажем, что p -избыток при $p \geq 3$ можно вычислить исходя из p -адических гауссовых средних; отсюда, в частности, будет следовать, что он действительно является p -адическим инвариантом.

Значение вычисленного во второй лекции гауссова среднего для одномерной формы $[p]$ равно 1 или i , деленному на $\sqrt{p}$. Теперь мы, однако, изменили определение, убрав множитель 2 в показателях степени. К каким изменениям это приведет? Ответ для гауссовых сумм хорошо известен: если внести множитель k (взаимно простой с p) в показатель степени, то гауссова сумма умножится на символ Лежандра $\left(\frac{k}{p}\right)$. Поэтому мы можем легко подсчитать новое гауссово среднее для формы $[p]$:

p сравнимо с	1 или 3 или 5 или 7 (mod 8)
старое гауссово среднее	(1 или i или 1 или i) $/\sqrt{p}$
символ $\left(\frac{2}{p}\right)$ равен	1 или -1 или -1 или 1, так что
новое гауссово среднее есть	(1 или $-i$ или -1 или i) $/\sqrt{p}$.

То же самое можно сформулировать и проще:

p -адическое гауссово среднее для формы $[p]$ равно

$$\frac{1}{\zeta^{p-1}\sqrt{p}},$$

где ζ — корень восьмой степени из единицы $(1+i)/\sqrt{2}$ (так что $\zeta^2=i$).

p -адическое гауссово среднее для модифицированной формы $[kp]$, где k взаимно просто с p , получается из этого выражения умножением на $\left(\frac{k}{p}\right)$; можно это записать в виде $1/(\zeta^m\sqrt{p})$, где m равно $p-1$ или $p-1+4$ в зависимости от того, является k квадратом по модулю p или нет.

Однако же это число — не что иное, как p -избыток формы $[kp]$! С помощью аналогичных вычислений для форм $[kp^n]$ получается следующий более общий результат.

Т е о р е м а. p -адическое гауссово среднее диагональной формы

$$f = [a_1, a_2, \dots, pb_1, pb_2, \dots, p^2c_1, \dots]$$

при $p \geq 3$ равно

$$\frac{1}{\zeta^{e_p(f)}\sqrt{\det_p(f)}},$$

где через $\det_p(f)$ обозначена p -часть $\det(f)$.

Поскольку p -адическое гауссово среднее является инвариантом относительно целой p -адической эквивалентности, из этой теоремы получается также инвариантное определение $e_p(f)$; этим доказывается, что $e_p(f)$ есть инвариант формы f , а именно инвариант относительно (рациональных) целых p -адических преобразований.

Слышимость p -адического символа

Мы можем получить больше информации, рассматривая и формы $f/p, f/p^2, \dots$. Именно, p -адическое гауссово среднее для f/p такое же, как для

$$[b_1, b_2, \dots, pc_1, pc_2, \dots, p^2d_1, \dots],$$

поскольку это среднее для $[a_i/p]$ равно 1.

Аналогично устанавливается, что средние для f/p^2 , f/p^3 , ... — такие же, как для форм

$$\begin{aligned}f' &= [b_1, b_2, \dots, pc_1, pc_2, \dots], \\f'' &= [c_1, c_2, \dots, pd_1, \dots], \\f''' &= [d_1, \dots], \\&\dots\dots\dots, \end{aligned}$$

Поэтому при $p \geq 3$ мы можем восстановить значения e_p и $\det_p$ для всех форм f' , f'' , f''' , что достаточно для нахождения p -адического символа.

Чтобы найти q -размерности, поступим так. Найдем, например,

$$\begin{aligned}\det_p(f)/\det_p(f') &= p^{n_1+n_p+\dots}, \\ \det_p(f')/\det_p(f'') &= p^{n_p+n_{p^2}+\dots},\end{aligned}$$

откуда можно найти n_1 . Аналогичным образом можно найти индивидуальные q -размерности и p -избытки. Стало быть, верна следующая теорема:

Теорема. Если p нечетно, то p -адический символ является слышимым инвариантом.

В частности, он действительно является инвариантом!

Случай $p = 2$

При $p = 2$ ситуация возникает очень похожая, но с некоторыми новыми чертами. Рассмотрим сначала 2-адические гауссовы средние для одномерных форм $[2^k]$. Поскольку $e^{\pi i} = -1$, 2-адическое гауссово среднее от формы $[1]$ есть среднее от $(-1)^{m^2}$ по всем целым числам m , что равно нулю. То же происходит и с $[k]$ для произвольного нечетного k .

Для форм $[2k]$ ($k = 1, 3, 5, 7$) получаем среднее от i^{km^2} , т.е.

$$\begin{aligned}k=1: & \quad 1, i, i^4=1, i^9=i, \quad \text{т.е. } (1+i)/2 = \zeta^1/\sqrt{2}; \\ k=3: & \quad 1, -i, 1, -i, \quad \text{т.е. } (1-i)/2 = \zeta^{3+4}/\sqrt{2}; \\ k=5: & \quad 1, i, 1, i, \quad \text{т.е. } (1+i)/2 = \zeta^{5+4}/\sqrt{2}; \\ k=7: & \quad 1, -i, 1, -i, \quad \text{т.е. } (1-i)/2 = \zeta^7/\sqrt{2}.\end{aligned}$$

Проведя аналогичные вычисления для форм

$$[2^n k], \quad 2^n \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad 2^n \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix},$$

получим следующую теорему.

Теорема. 2-адическое гауссово среднее целой формы

$$f = f_1 + 2f_2 + 4f_4 + \dots$$

равно 0, если f_1 имеет тип I, и

$$\frac{\zeta_{\text{нечетность формы } f}}{\sqrt{\det_2(f)}}$$

в противном случае.

Как и при $p \geq 3$, ту же информацию можно получить из форм

$$\begin{aligned} f' &= f_2 + 2f_4 + 4f_8 + \dots, \\ f'' &= f_4 + 2f_8 + \dots, \\ f''' &= f_8 + \dots, \\ &\dots\dots\dots \end{aligned}$$

но если одно из гауссовых средних обращается в нуль, то часть информации пропадает безвозвратно вместе с ним. Впрочем, мы и не должны были надеяться определить нечетности отдельных f_q , благо они не являются инвариантами формы f . Оказывается, что на самом деле выполняется следующее утверждение.

Теорема. По 2-адическим гауссовым средним форм f , $f/2$, $f/4$, ... восстанавливается вся информация, заключенная в 2-адическом символе (кроме, возможно, q -размерностей n_1 , n_2 , n_4 , ...) с точностью до преобразований из правила слияния нечетностей и правила движения знаков.

Уже в следующем параграфе мы увидим, что q -размерности не всегда слышимы, так что мы не можем гарантировать, что их можно восстановить по гауссовым средним. Тем не менее, они бесспорно являются инвариантами формы f (точнее говоря, 2-адическими инвариантами), поскольку они задают структуру 2-части двойственной факторгруппы L^*/L , являющейся прямым произведением n_1 экземпляра группы C_1 , n_2 экземпляров группы C_2 , n_4 экземпляров группы C_4 и т. д. Таким образом, верна следующая теорема.

Теорема. 2-адический символ является (с точностью до слияния нечетностей и движения знаков) инвариантом формы f относительно 2-адической целочисленной эквивалентности.

Как услышать род: игра в прятки

Теперь мы знаем, что мы можем услышать весь род, кроме, возможно, q -размерностей n_q при $p=2$. Тем не менее часть информации

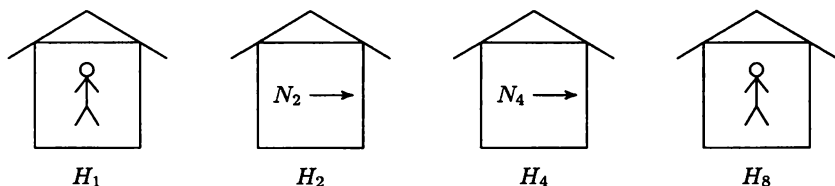
о них является слышимой, и мы покажем, что это позволит нам услышать все эти размерности в случае, когда $n = 4$.

Услышим мы эту информацию, сыграв игру в прятки с командой из n игроков, прячущихся в нескольких домиках (в домике H_q сидят n_q игроков). Каждый домик должен удовлетворять следующему условию: либо в нем виден один из игроков (это домик типа I, и это условие соответствует тому факту, что n_q должно быть положительно, если f_q имеет тип I), либо на нем должна быть вывешена табличка с числом

$$N_q = n_{2q} + 2n_{4q} + 3n_{8q} + 4n_{16q} + \dots,$$

являющимся суммой расстояний от домика до всех игроков, прячущихся в домиках, стоящих правее, чем H_q (в случае типа II; определитель формы $f_q + 2f_{2q} + 4f_{4q} + \dots$ равен 2^{N_q}). Более того, число игроков, прячущихся в любом домике типа II, должно быть четным (оно может быть равно нулю).

Например, на приведенном ниже рисунке изображены первые четыре домика формы, у которой f_1 и f_8 имеют тип I, а f_2 и f_4 имеют тип II.

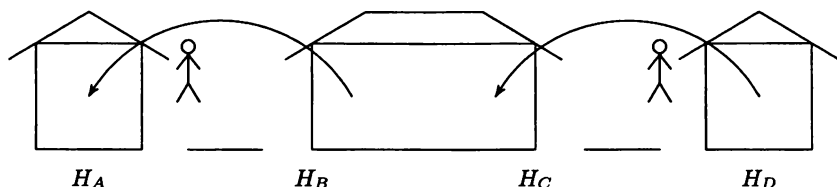


Мы покажем, что если в команде противника всего четыре игрока, то мы можем их найти. Если все домики имеют тип II, то мы знаем все, так что можно считать, что хотя бы один из домиков имеет тип I, так что мы видим хотя бы одного игрока (обозначим домик, в котором мы его видим, через H_q). Если больше ни одного игрока мы не видим, то во всех домиках, кроме H_q , сидит по четному числу игроков (поскольку эти домики имеют тип II), так что и в H_q должно сидеть четное число игроков; тем самым мы обнаружили и второго игрока.

Предположим теперь, что есть два не противоречащих имеющейся у нас информации способа разместить двух остающихся игроков. Тогда можно переместить двух игроков из домиков H_B и H_C в H_A и H_D таким образом, чтобы доступные нам данные не изменились.

Без потери общности можно считать, что

$$H_A < H_B \leq H_C < H_D$$



и должно выполняться равенство $BC = AD$, поскольку определитель меняться не должен. Далее, в каждом из домиков H_A и H_D при одной из этих расстановок укрывается нечетное количество игроков, так что они должны иметь тип I, и то же верно применительно к H_B и H_C , если только это не один и тот же домик. Стало быть, если мы не видим третьего игрока, то H_B и H_C — один и тот же домик типа II, но в этом случае число, написанное на вывешенной на нем табличке, будет различным для двух расстановок игроков. Следовательно, мы всегда можем обнаружить третьего игрока, расположение же четвертого игрока находится после этого из определителя.

Мы доказали теорему, принадлежащую, по моему мнению, Китаоке.

Теорема. В размерности, не превосходящей 4, род квадратичной формы является слышимым инвариантом.

Неслышимость рода в высших размерностях

У кубической и исокубической решеток с минимальной нормой 2, упомянутых в лекции 2, 2-адические символы различны:

$$\begin{array}{ll} 1_{\infty}^0 2_6^6 4_{\infty}^0 & \text{для кубической решетки;} \\ 1_{\infty}^2 2_6^2 4_{\infty}^2 & \text{для исокубической решетки.} \end{array}$$

Подрешетки этих решеток, ортогональные к вектору $(1, 1, 1, 1, 1, 1)$, также имеют разные 2-адические символы:

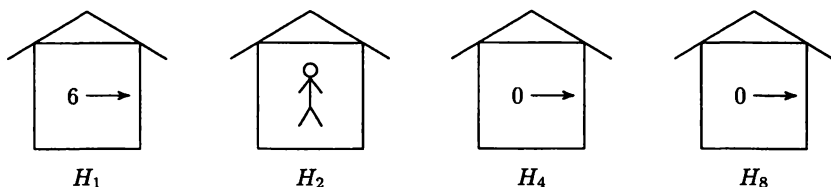
$$1_{\infty}^0 2_3^{-5} 4_{\infty}^0, \quad 1_{\infty}^2 2_3^{-1} 4_{\infty}^2.$$

Следовательно, имеет место следующий факт.

Теорема. В размерности 5 и выше род слышим не всегда.

Я полагаю, что этот результат является новым.

Интересно посмотреть, как именно сможет нас победить команда из шести игроков. И кубической, и изокубической решетке соответствует следующая картинка:



При этом, однако, в случае кубической решетки все шесть игроков прячутся в H_2 , а в случае изокубической решетки по два игрока сидят в каждом из домиков H_1 , H_2 , H_4 . В обоих случаях сумма расстояний от H_1 до игроков, прячущихся правее его, равна 6. Чтобы получить пятимерный пример, удалим одного игрока из H_2 .

ДОБАВЛЕНИЕ

Еще об инвариантах; p -адические числа

Инвариантность p -адических сигнатур

Мы еще не доказали, что p -сигнатуры (или, что равносильно, p -избытки) являются инвариантами относительно рациональной эквивалентности. Мы можем это сделать, показав, что для всякой целой формы F типа II, рационально эквивалентной форме f , p -адическое гауссово среднее формы F равно положительному действительному числу, умноженному на $\zeta^{\sigma_2(f)}$ или $\zeta^{-e_p(f)}$ в зависимости от того, выполнено или нет равенство $p=2$.

Если F_1 и F_2 — две целые формы типа II, эквивалентные f , то можно перейти от одной из них к другой за конечное число шагов, на каждом из которых решетка заменяется на подрешетку простого индекса P либо производится обратная замена.

Для простых чисел p , отличных от P , такая замена просто умножает слагаемые в гауссовом среднем на корни из единицы степени P , что не влияет на p -адическое гауссово среднее или p -избыток. Однако e_P можно вычислить по остальным e_p с помощью доказанного в постскриптуме глобального соотношения, так что с этим тоже все в порядке!

p -адические числа

Гаусс и другие математики уже давно заметили, что некоторые из наиболее интересных свойств квадратичных форм зависят только от значений их коэффициентов по модулю степеней различных простых чисел. К. Гензель нашел очень изящный способ выразить эту мысль с помощью введенных им в обиход колец p -адических чисел.

Мы определим *целое p -адическое число* x как формальное решение совместной системы сравнений

$$x \equiv a_n \pmod{p^n} \quad (n=0, 1, 2, \dots),$$

по одному сравнению на каждую степень p . Условие совместности состоит в том, что каждые два сравнения должны иметь общее решение в обыкновенных целых числах. Например, сравнения $x \equiv 1 \pmod{3}$,

$x \equiv 7 \pmod{9}$ и $x \equiv -2 \pmod{27}$ совместны, поскольку им всем удовлетворяет $x = 25$.

Так определенные p -адические числа образуют кольцо, поскольку их можно складывать, вычитать и умножать. В самом деле, если x и y — два целых p -адических числа, заданных сравнениями

$$x \equiv a_n \pmod{p^n}, \quad y \equiv b_n \pmod{p^n},$$

то $u = x + y$, $v = x - y$, $w = xy$ суть p -адические числа, заданные сравнениями

$$u \equiv a_n + b_n, \quad v \equiv a_n - b_n, \quad w \equiv a_n b_n \pmod{p^n}.$$

Число $1/3$ является целым 2-адическим; оно же является и целым 5-адическим. Чтобы убедиться в этом, заметим, что числа a_n , равные

$$7, 67, 667, 6667, 66667, \dots,$$

после умножения на 3 дают числа

$$21, 201, 2001, 20001, 20001, \dots,$$

сравнимые с единицей по модулю все более высоких степеней двойки и пятерки. Поэтому p -адическое число x , заданное сравнениями $x \equiv a_n \pmod{p^n}$, где p равно 2 или 5, удовлетворяет условию $3x = 1$.

Далее, существует целое 5-адическое число x , для которого $x^2 = -1$, поскольку числа

$$2, 7, 57, 182, \dots$$

(на сей раз закономерность менее очевидна) сравнимы друг с другом, а их квадраты

$$4, 49, 3249, 33124, \dots$$

сравнимы с -1 по модулю возрастающих степеней пятерки.

Более общим образом, если r/s — рациональное число, знаменатель которого не делится на p , то имеется система сравнений

$$x \equiv a_n \pmod{p^n},$$

равносильная $sx \equiv r$, и формальное решение этой системы сравнений есть целое p -адическое число x , удовлетворяющее условию $sx = r$; это число естественно отождествить с рациональным числом r/s . Если же k — произвольный квадратичный вычет по модулю p , то аналогичным способом можно показать, что уравнение $x^2 \equiv k$ разрешимо в целых p -адических числах.

Рациональные p -адические числа определяются точно так же, как целые, но на сей раз в задающих эти числа сравнениях

$$x \equiv a_n \pmod{p^n}$$

числа a_n могут быть произвольными рациональными. Оказывается, что всякое рациональное p -адическое число есть целое p -адическое число, деленное на некоторую степень p .

Мы будем использовать обозначение $\mathbb{Z}_p$ для множества целых p -адических чисел и $\mathbb{Q}_p$ для множества рациональных p -адических чисел. Все вышесказанное относилось к простым числам, отличным от весьма специального простого числа -1 . Имеются другие подходы, при которых естественно считать, что и $\mathbb{Z}_{-1}$, и $\mathbb{Q}_{-1}$ представляют собой кольцо $\mathbb{R}$ целых чисел.

Для читателя, незнакомого с этими понятиями, отметим, что на самом деле в данной книге они не нужны. Мало что будет потеряно, если фразы наподобие «такое-то уравнение разрешимо в целых p -адических числах» заменять на «такое-то уравнение разрешимо по модулю сколь угодно больших степеней p ».

Бинарные формы над $\mathbb{Q}_p$

Неособая бинарная форма с определителем d над любым из полей $\mathbb{Q}$ и $\mathbb{Q}_p$ будет полностью определена, если указать какое-нибудь представляемое ей число. В самом деле, если она представляет число $k \neq 0$, то она эквивалентна форме $[k, dk]$, а если она представляет нуль, то она эквивалентна форме xy , или $[1, -1]$.

Если форма представляет k , то она представляет и все числа вида kx^2 ($x \neq 0$), составляющие класс k по модулю квадратов. Мы будем обозначать классы p -адических чисел по модулю квадратов следующим образом:

$$\begin{array}{ll} +u, -u & \text{при } p = -1, \\ u_1, u_3, u_5, u_7, 2u_1, 2u_3, 2u_5, 2u_7 & \text{при } p = 2, \\ u_+, u_-, pu_+, pu_- & \text{при } p \geq 3. \end{array}$$

Здесь u — класс положительных чисел, u_k — класс 2 -адических чисел по модулю квадратов, состоящий из чисел вида $8n + k$ ($k = 1, 3, 5, 7$), а u_+ и u_- — классы p -адических чисел, состоящие из квадратичных вычетов (т. е. квадратов) и невычетов соответственно.

Поскольку в $\mathbb{Q}_p$ имеется только конечное число классов по модулю квадратов, в любой данной размерности имеется только конечное

число форм. Бинарные формы классифицируются по классу их определителя и представляемым ими числам (представляемым, когда не все переменные равны нулю) следующим образом (в таблице через $p_{\pm}$ обозначено положительное простое число, сравнимое с ± 1 по модулю 4):

p	d	Числа, представимые соответствующими формами	
-1	$+u$	$\{+u\}$	$\{-u\}$
	$-u$	$\{0, +u, -u\}$	
2	u_1	$\{u_1, u_5, 2u_1, 2u_5\}$	$\{u_3, u_7, 2u_3, 2u_7\}$
	u_3	$\{u_1, u_3, u_5, u_7\}$	$\{2u_1, 2u_3, 2u_5, 2u_7\}$
	u_5	$\{u_1, u_5, 2u_3, 2u_7\}$	$\{u_3, u_7, 2u_1, 2u_5\}$
	u_7	$\{0, u_1, u_3, u_5, u_7, 2u_1, 2u_3, 2u_5, 2u_7\}$	
	$2u_1$	$\{u_1, u_3, 2u_1, 2u_3\}$	$\{u_5, u_7, 2u_5, 2u_7\}$
	$2u_3$	$\{u_1, u_7, 2u_3, 2u_5\}$	$\{u_3, u_5, 2u_1, 2u_7\}$
	$2u_5$	$\{u_1, u_3, 2u_5, 2u_7\}$	$\{u_5, u_7, 2u_1, 2u_3\}$
	$2u_7$	$\{u_1, u_7, 2u_1, 2u_7\}$	$\{u_3, u_5, 2u_3, 2u_5\}$
p_+	u_+	$\{0, u_+, u_-, pu_+, pu_-\}$	
	u_-	$\{u_+, u_-\}$	$\{pu_+, pu_-\}$
	pu_+	$\{u_+, pu_+\}$	$\{u_-, pu_-\}$
	pu_-	$\{u_+, pu_-\}$	$\{u_-, pu_+\}$
p_-	u_+	$\{u_+, u_-\}$	$\{pu_+, pu_-\}$
	u_-	$\{0, u_+, u_-, pu_+, pu_-\}$	
	pu_+	$\{u_+, pu_+\}$	$\{u_-, pu_-\}$
	pu_-	$\{u_+, pu_-\}$	$\{u_-, pu_+\}$

Рациональные формы с заданными инвариантами

Как мог заметить читатель, из вышеприведенной таблицы явствует, что если d принадлежит к классу -1 по модулю квадратов, то существует только одна бинарная форма с определителем d , и эта форма представляет все числа. Такие формы называются *бинарными изотропными формами*. Более общо, всякая невырожденная форма, нетривиально представляющая нуль, называется *изотропной*, и легко проверяется, что изотропные формы — это в точности формы вида $[1, -1, *, *, \dots]$. В самом деле, с одной стороны, форма $[1, -1]$ изотропна; с другой стороны, если форма $[a, b, \dots]$ изотропна, то имеется уравнение $ax^2 + by^2 + \dots = 0$, в котором должно присутствовать по крайней мере два ненулевых слагаемых. Но в этом случае вектор v , для которого $f(v) = 0$, можно записать в виде суммы двух

ортогональных векторов с ненулевыми нормами k и $-k$, так что в подходящем базисе f выглядит как $[k, -k, *, *, \dots] = [1, -1, *, *, \dots]$.

Стало быть, над $\mathbb{Q}_p$ имеются две бинарные формы с данным определителем d , кроме случая, когда $-d$ является p -адическим квадратом, в каковом случае имеется только изотропная форма. Выберем теперь для данного рационального числа d по одной из двух форм $f^{(p)}$ с определителем d для каждого p (разумеется, если $-d$ является p -адическим квадратом, то выбора у нас нет). При каких условиях существует рациональная квадратичная форма с определителем d , которая для каждого p будет p -адически эквивалентна форме $f^{(p)}$?

Ответ состоит в том, что такая f существует тогда и только тогда, когда выполняется глобальное соотношение: сумма p -избытков всех форм $f^{(p)}$ равна нулю по модулю 8.

В лежандровском доказательстве теоремы о трех квадратах в соответствующем месте использовался тот факт, что в подходящих арифметических прогрессиях есть простые числа, что было доказано Дирихле только спустя много лет. (Серр в своем «Курсе арифметики» [42] также использует в доказательстве этого факта теорему Дирихле, но, в отличие от большинства остальных авторов, в дальнейшем он приводит ее доказательство!)¹ Мы также не будем нарушать традицию и сошлемся на теорему Дирихле; кроме того, мы воспользуемся глобальным соотношением, доказательство которого будет приведено только в постскрипуме.

Опишем вкратце процедуру построения формы f по формам $f^{(p)}$. В бинарном случае положим искомую форму равной

$$[p_1 p_2 p_3 \dots p_m P, p_1 p_2 \dots p_m P d],$$

где простые числа $p_1, p_2, \dots, p_m$ — это $-1, 2$, простые делители d , а также какие-то из простых чисел, обладающих тем свойством, что заданная p -адическая форма $f^{(p)}$ не эквивалентна $[1, d]$. Число P — это большое простое число, которое будет выбрано позднее. Легко

¹Гаусс нашел доказательство, независимое от теоремы Дирихле и использующее его закон композиции и роды бинарных квадратичных форм над $\mathbb{Z}$. Для тех, кто понимает используемую терминологию, мы приведем краткий набросок доказательства Гаусса. Нам хочется доказать, что род имеет «правильный размер». Однако две формы принадлежат к одному роду тогда и только тогда, когда их частное является квадратом в группе относительно композиции, так что можно доказывать, что ядро отображения возведения в квадрат имеет правильный размер. Формы, лежащие в ядре, хорошо известны — это так называемые *амбивые* формы. Они, грубо говоря, соответствуют разложениям числа d , и имеется «правильное» число таких разложений.

видеть, что можно получить требуемую $f^{(p)}$ за счет включения или не включения p в произведение $p_1 p_2 \dots p_m$ и при этом добиться того, чтобы P было, в зависимости от наших потребностей, квадратичным вычетом или невычетом по модулю p .

Это означает, что мы можем получить требуемые $f^{(p)}$ для всех простых чисел p , кроме, возможно, P . Однако из глобального соотношения вытекает, что тогда и форма $f^{(P)}$ будет такой, как требуется!

Чтобы построить форму старшей размерности

$$f = [a_1, a_2, a_3, \dots]$$

с заданными инвариантами, выберем сначала значения коэффициентов, начиная с a_3 , таким образом, чтобы требуемое значение произведения $a_1 a_2$ не было противоположным p -адическому квадрату для всех тех p , для которых это существенно, а затем с помощью вышеописанного метода найдем бинарную подформу $[a_1, a_2]$.

Целые формы с предписанными инвариантами

С помощью несколько более громоздкого рассуждения можно построить целую форму с заданными p -адическими символами, удовлетворяющими глобальному соотношению. Наиболее простое доказательство опять использует теорему Дирихле, но ценой дополнительных усилий этого можно избежать. Искомую форму можно сделать трехдиагональной: все ненулевые элементы будут у нее сосредоточены на главной диагонали и на двух соседних с ней. В качестве ведущего (левого верхнего) элемента матрицы можно выбрать любое число, примитивно представимое над целыми p -адическими числами для каждого простого p . После этого прочие элементы матрицы выбираются последовательно, по модулю степеней различных простых чисел, с использованием китайской теоремы об остатках. На каждом шаге надо вводить не более одного нового простого числа с использованием теоремы Дирихле. Поведение формы по отношению к последнему из этих простых чисел мы проконтролировать не можем, но оно автоматически является правильным ввиду глобального соотношения.

У этой теории есть важные следствия, относящиеся к представлению чисел целыми формами. Если целое число n представимо формой f над p -адическими числами для всех p , включая -1 , то, хотя число может и не представляться самой формой f , оно представимо какой-то формой из того же рода, что и f . Причина тут в том, что ес-

ли n является примитивно представимым над p -адическими числами для всякого p , то с помощью конструкции, описанной в предыдущем абзаце, получается форма g , лежащая в том же роде, что и f , и имеющая n ведущим элементом своей матрицы; значит, g примитивно представляет число n .

Разумеется, f представляет число n непримитивно тогда и только тогда, когда она представляет какое-то число вида n/k^2 ($k > 1$) примитивно. Если это имеет место в p -адических числах для всякого p , то какая-то форма g из того же рода, что и f , представляет n/k^2 примитивно и тем самым представляет n непримитивно.

Именно эти факты лежат в основе теоремы Лежандра о трех квадратах. В роде формы $f(x, y, z) = x^2 + y^2 + z^2$ имеется только одна форма, так что если число удовлетворяет p -адическим условиям представимости формой f , то оно должно быть представимым самой формой f . Нетривиальные условия получаются только при $p = -1$ и 2 . В постскрипуме мы, тем не менее, дадим полное доказательство теоремы Лежандра, не зависящее от этих рассуждений.

Эквивалентность с несущественным знаменателем

Ортогональная группа квадратичной формы f порождена отражениями в различных векторах v , для которых $f(v) \neq 0$. Пусть $\{-1, 2, \dots, p\}$ — конечное множество простых чисел, включающее в себя $-1, 2$ и все простые делители числа $\det(f)$; будем называть эти простые числа *существенными*. Теорема об аппроксимации утверждает, что если даны целые p -адические автоморфизмы

$$\vartheta^{(-1)}, \vartheta^{(2)}, \dots, \vartheta^{(p)}$$

формы f , имеющие один и тот же (1 или -1) определитель для всех существенных простых, то существует рациональный автоморфизм ϑ , индуцирующий данные $\vartheta^{(p)}$.

Чтобы доказать это утверждение, заметим, что мы можем представить $\vartheta^{(p)}$ в виде произведения отражений в векторах

$$\tau_1^{(p)}, \tau_2^{(p)}, \dots, \tau_k^{(p)},$$

где k — то из чисел n и $n-1$, для которого $(-1)^k$ равно определителю. Положим теперь ϑ равным произведению отражений в рациональных векторах

$$\tau_1, \tau_2, \dots, \tau_k,$$

сравнимых с выписанными выше векторами по модулю достаточно больших степеней соответствующих p .

Мы доказали «принцип эквивалентности с несущественным знаменателем» — если две формы принадлежат одному роду, то они эквивалентны относительно рационального преобразования, матрица которого не содержит в знаменателях существенных простых чисел.

Спинорный род

На рациональной ортогональной группе квадратичной формы f определен, наряду с принимающим значения ± 1 *определителем*, еще один гомоморфизм, а именно *спинорная норма*. Значениями спинорной нормы являются классы рациональных чисел по модулю квадратов. Чтобы определить этот гомоморфизм, достаточно сказать, что спинорная норма отражения в векторе τ равна классу $f(\tau)$ по модулю квадратов (в то время как определитель этого отражения равен -1).

Понятие спинорного рода — это уточнение понятия рода, использующее спинорную норму. Если f и g принадлежат одному роду, то они эквивалентны относительно многих различных рациональных преобразований с несущественным знаменателем. Пусть $S_r(f)$ — класс всех тех форм g , для которых это рациональное преобразование может быть выбрано так, чтобы оно имело определитель 1 и спинорную норму r . Тогда $S_1(f)$ — это *спинорный род* формы f , а *спинорное ядро* — это множество всех таких чисел r , что $S_r(f) = S_1(f)$.

Наше определение спинорного рода представляется наиболее простым. Оно лежит где-то посередине между традиционным (являющимся небольшой модификацией исходного Эйхлеровского определения) и более поздним уотсоновским определением «спинорной эквивалентности».

С нашим определением можно проводить вычисления, если воспользоваться теоремой Уотсона:

Теорема. Пусть f и g — квадратичные формы с одинаковым определителем d , соответствующие решеткам L и M , пересечение которых имеет индекс r в каждой из них. Тогда если r — нечетное число, взаимно простое с d , то g лежит в $S_r(f)$. В частности, f и g принадлежат к одному роду, а если r лежит в спинорном ядре, то они принадлежат и к одному спинорному роду.

Важность спинорного рода подчеркивается следующей теоремой Эйхлера.

Теорема. *Две неопределенные формы ранга ≥ 3 целочисленно эквивалентны тогда и только тогда, когда они принадлежат к одному спинорному роду.*

Определенный нами спинорный род является эффективно вычислимым инвариантом. На практике работают со спинорным ядром, которое можно найти чисто «локальными» вычислениями.

Очень часто спинорный род совпадает с родом, так что наши p -адические символы характеризуют форму с точностью до эквивалентности. Именно, можно показать, что так и будет, если только не окажется, что для некоторого p форму можно диагонализировать, причем таким образом, что все степени p , делящие диагональные элементы, будут различны. Кроме того, для неопределенных форм размерности n с определителем d спинорный род совпадает с родом, если $4^{\lfloor n/2 \rfloor} d$ не делится на $k^{\binom{n}{2}}$ для некоторого не являющегося квадратом натурального k , сравнимого с 0 или 1 по модулю 4. Это — теорема 21 из главы 15 книги [7], в которой приведен также удобный на практике алгоритм вычислений со спинорным родом.

ПОСТСКРИПТУМ

Вкус теории чисел

Три знаменитые теоремы

В этом постскриптуме мы докажем три знаменитые теоремы: небезызвестный квадратичный закон взаимности, теорему о том, что сигнатура четной унимодулярной квадратичной формы кратна восьми, и славную теорему Лежандра о трех квадратах. Мы получим некоторые следствия из теоремы Лежандра, включая универсальность некоторых форм от четырех переменных, а в заключение объясним, почему никакая рациональная положительно определенная тернарная форма универсальной быть не может.

Определение символа Якоби по Золотарёву

Пусть n — нечетное число с разложением на простые множители $n = pqr \dots$; Якоби определил свой символ по формуле

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) \left(\frac{a}{q}\right) \left(\frac{a}{r}\right) \dots,$$

то есть как произведение символов Лежандра. Хотя из его многочисленных свойств явствовало, что символ Якоби — объект весьма естественный, прошло некоторое время, пока Золотарёв не нашел более концептуального определения: $\left(\frac{a}{n}\right)$ — это знак перестановки, реализуемой умножением на a по модулю n . В этом постскриптуме мы будем придерживаться определения Золотарёва.

Напомним, что всякой перестановке π конечного множества можно сопоставить ее *знак*, который равен -1 тогда и только тогда, когда нечетное число циклов перестановки имеет четную длину. Через « $\times a \bmod n$ » будем обозначать перестановку множества $\{0, \dots, n-1\}$, задаваемую умножением на a . Например,

$$\times 3 \bmod 11 = (0)(1, 3, 9, 5, 4)(2, 6, 7, 10, 8).$$

Поскольку циклов четной длины нет, имеем $\left(\frac{3}{11}\right) = +1$.

Такое определение позволяет чрезвычайно просто доказать квадратичный закон взаимности. Замечательно, что в доказательстве не

используются даже понятия простого числа или полного квадрата. Мы будем все же пользоваться тем фактом, что знак перестановки мультипликативен.

Будем говорить, что число *положительно по модулю t* , если оно сравнимо по модулю t с числом, лежащим строго между 0 и $\frac{1}{2}t$, и что оно *отрицательно по модулю t* , если оно сравнимо с числом из интервала $(-\frac{1}{2}t, 0)$. Число $\frac{1}{2}t$ является *неопределенным по модулю t* .

Пять лемм

Начнем с того, что найдем $\left(\frac{-1}{n}\right)$.

Л е м м а 1. $\left(\frac{-1}{n}\right)$ есть знак n по модулю 4.

Иными словами, $\left(\frac{-1}{n}\right)$ равен 1, если $n=4k+1$, и равен -1 , если $n=4k-1$.

Д о к а з а т е л ь с т в о. Это немедленно следует из определения. Например, $\left(\frac{-1}{11}\right)$ и $\left(\frac{-1}{13}\right)$ суть знаки перестановок

$$(0)(1, -1)\dots(5, -5) \quad \text{и} \quad (0)(1, -1)\dots(6, -6)$$

соответственно, то есть -1 в первом случае и 1 во втором, поскольку первая перестановка содержит пять транспозиций, а вторая — шесть.

□

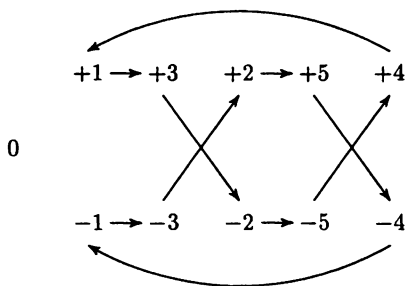
Л е м м а 2. Имеем $\left(\frac{a}{n}\right) = (-1)^s$, где s — «число перемен знака» для отображения $x \mapsto ax \bmod n$, то есть число положительных $k \bmod n$, для которых ak отрицательно по модулю n .

Д о к а з а т е л ь с т в о. Рассмотрим, например, $\left(\frac{3}{11}\right)$. Выпишем числа, переставляемые преобразованием $\times 3 \bmod 11$, вместе со знаками:

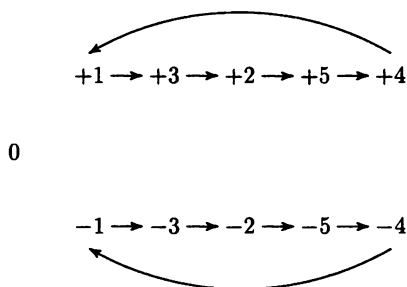
$$(0)(+1, +3, -2, +5, +4)(-1, -3, +2, -5, -4).$$

Из рисунка видно, что число перемен знака ($s=2$) равно числу пересечений стрелок. Тот же рисунок показывает, что перестановка разлагается в произведение перестановок

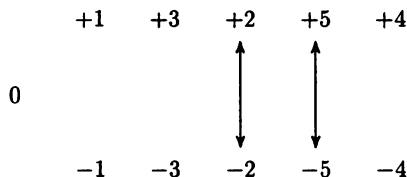
$$(0)(1, 3, 2, 5, 4)(-1, -3, -2, -5, -4) \quad \text{и} \quad (2, -2)(5, -5):$$



получается при умножении



на



Первую из этих перестановок можно было бы назвать «абсолютным умножением на 3», или «умножением на 3, сохраняющим знаки», а во второй подстановке производится необходимая коррекция знаков.

В общем случае абсолютное умножение на $a \bmod n$ является четной подстановкой, поскольку это композиция двух подстановок с абсолютно одинаковым разложением на циклы, а перестановка, корректирующая знаки, состоит из транспозиций и тем самым имеет знак $(-1)^s$. $\square$

Для всякого данного a мы можем найти с помощью этой леммы значение $\left(\frac{a}{n}\right)$ при любых n . Например, $\left(\frac{2}{n}\right) = -1$ или 1 в зависимости от того, сравним n с ± 1 или ± 3 по модулю 8.

Лемма 3. Если $a > 0$, то s равно количеству целых чисел из интервала $(0, n/2)$, лежащих в объединении интервалов вида

$$\left[\left(l - \frac{1}{2}\right) \frac{n}{a}, l \frac{n}{a}\right].$$

Доказательство.

$$\begin{array}{ccccccc}
 0 \times \frac{11}{3} & + & \frac{1}{2} \times \frac{11}{3} & - & 1 \times \frac{11}{3} & + & 1\frac{1}{2} \times \frac{11}{3} \\
 \vdots & & \vdots & & \vdots & & \vdots \\
 \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 3 & & 6 & & 9 & & 15 \\
 \equiv 3 & & \equiv -5 & & \equiv -2 & & \equiv 4 \\
 \vdots & & \vdots & & \vdots & & \vdots \\
 0 \times 11 & + & \frac{1}{2} \times 11 & - & 1 \times 11 & + & 1\frac{1}{2} \times 11 \\
 & & & & & & \text{знак}
 \end{array}
 \begin{array}{c}
 a \\
 \downarrow \\
 ak \pmod{n}
 \end{array}$$

Это сразу видно из рисунка. Пунктирные линии показывают, как меняется знак с плюса на минус, когда ak проходит через число вида $\left(l - \frac{1}{2}\right)n$, и обратно с минуса на плюс, когда ak проходит через число вида ln . $\square$

Лемма 4. (Периодичность символа Якоби как функции от n).

Если $m \equiv \pm n \pmod{4a}$, то $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right)$.

Доказательство. Если прибавить к m или вычесть кратное $4a$, то все концы интервалов в лемме 3 сдвинутся на четное число единиц, так что s изменится на четное число. Кроме того, символ $\left(\frac{a}{-n}\right)$ равен $\left(\frac{a}{n}\right)$, так как умножение на a по модулю $-n$ — то же самое, что умножение на a по модулю n . $\square$

Лемма 5. Если m и n — взаимно простые нечетные числа, сумма которых — положительное число, делящееся на 4, то $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$.

Доказательство. Пусть $m + n = 4a$. Тогда

$$\left(\frac{m}{n}\right) = \left(\frac{4a}{n}\right) = \left(\frac{a}{n}\right) = \left(\frac{a}{m}\right) = \left(\frac{4a}{m}\right) = \left(\frac{n}{m}\right).$$

Эти равенства имеют место, потому что умножение на m по модулю n — то же самое, что умножение на $4a$ по модулю n , а это умножение можно провести, дважды умножив на 2 (что не повлияет на знак), а затем умножив на a . $\square$

Взаимность для символа Якоби

Обычно закон взаимности для символа Якоби формулируется так.

Т е о р е м а. Пусть m и n — два взаимно простых положительных нечетных числа. Тогда $\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right)$ всегда, кроме случая, когда и m , и n отрицательны по модулю 4; в этом последнем случае символы $\left(\frac{m}{n}\right)$ и $\left(\frac{n}{m}\right)$ различны.

Д о к а з а т е л ь с т в о. Легко видеть, что это утверждение содержится в лемме 5. Мы рассмотрим три случая, принимая во внимание тот факт, что $\left(\frac{m}{-n}\right) = \left(\frac{m}{n}\right)$ (поскольку умножение по модулю $-n$ — то же, что умножение по модулю n).

1) *Знаки по модулю 4 различны.* В этом случае теорема сразу следует из леммы 5. Например, $\left(\frac{11}{13}\right) = \left(\frac{13}{11}\right)$, поскольку $11 + 13$ делится на 4.

2) *m и n положительны по модулю 4.* Рассмотрим, например, числа 5 и 13. Лемма 5 в этом случае показывает, что

$$\left(\frac{13}{5}\right) = \left(\frac{13}{-5}\right) = \left(\frac{-5}{13}\right) = +\left(\frac{5}{13}\right),$$

поскольку $13 - 5$ — положительное число, делящееся на 4, а $\left(\frac{-1}{13}\right) = +1$ по лемме 1.

3) *m и n отрицательны по модулю 4.* Рассмотрим, например, 7 и 11. Из леммы 5 получаем, что

$$\left(\frac{11}{7}\right) = \left(\frac{11}{-7}\right) = \left(\frac{-7}{11}\right) = -\left(\frac{7}{11}\right),$$

поскольку $11 - 7$ — положительное число, делящееся на 4, а $\left(\frac{-1}{11}\right) = -1$ по лемме 1. $\square$

Это доказательство в значительной степени снимает покров тайны с закона взаимности благодаря использованию символа Якоби по Золотарёву вместо символа Лежандра. В остальном оно следует доказательству Шольца из вышедшей в 1939 году книги [40].

Символы Лежандра и линейные символы Якоби

Чтобы показать, что из доказанного нами вытекает обычный квадратичный закон взаимности, мы должны показать, что определенный по Золотарёву символ Якоби $\left(\frac{a}{p}\right)$ совпадает с обычным символом Лежандра, если p — нечетное простое число.

Вспомним для этого теорему Эйлера, согласно которой мультипликативная группа целых чисел по модулю p является циклической группой порядка $p-1$. Если теперь обозначить через g образующую этой группы, то перестановка « $\times g \bmod p$ » является $(p-1)$ -циклом, так что $\left(\frac{g^k}{p}\right) = (-1)^k$, чем все и доказано.

Один из традиционных способов записи закона взаимности — формула, утверждающая, что

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}},$$

если m и n взаимно просты.

Чтобы упростить дальнейшую работу с p -сигнатурами и p -избытками, нам будет удобно ввести линейную версию символа Якоби — выражение, принимающее значение в вычетах по модулю 8. Положим

$$\left[\frac{m}{n}\right] = 0 \bmod 8, \quad \text{если} \quad \left(\frac{m}{n}\right) = -1,$$

и

$$\left[\frac{m}{n}\right] = 4 \bmod 8, \quad \text{если} \quad \left(\frac{m}{n}\right) = 1.$$

В этих обозначениях закон взаимности записывается так:

$$\left[\frac{m}{n}\right] + \left[\frac{n}{m}\right] \equiv (m-1)(n-1) \pmod{8}.$$

Глобальное соотношение

В лекции 4 мы определили для рациональной квадратичной формы инварианты σ_p , называемые p -сигнатурами, значения которых — целые числа по модулю 8. Мы также определили p -избыток e_p по формулам

$$e_p(f) = \sigma_p(f) - \dim(f), \quad \text{если } p \neq 2,$$

и

$$e_2(f) = \dim(f) - \sigma_2(f).$$

Поскольку каждое из e_p зависит только от p -адической версии формы, естественно ожидать, что различные e_p будут независимы. Имеется, однако же, замечательное глобальное соотношение:

Сумма всех p -избытков кратна 8.

То же самое соотношение обычно записывали по-другому: оно утверждало, что произведение некоторых инвариантов равно единице, так что стандартное название для этого соотношения — «формула произведения». Как объяснялось в лекции 4, p -сигнатура одномерной формы $[a] = [p^\alpha A]$ равна p^α или $p^\alpha + 4$, причем слагаемое 4 возникает тогда и только тогда, когда a является p -адическим антиквадратом, т. е. когда α нечетно и A является квадратичным невычетом по модулю p . На языке наших линейных символов Якоби можно сказать, что сигнатура равна

$$p^\alpha + \left[\frac{A}{p^\alpha} \right].$$

Понятие p -сигнатуры можно обобщить. Именно, если π — произвольное множество нечетных простых чисел, то определим π -сигнатуру формы $[a]$ как

$$\pi(a) + \left[\frac{\pi'(a)}{\pi(a)} \right],$$

где $\pi(a)$ и $\pi'(a)$ — части числа a , состоящие из простых чисел, входящих в π , и из простых чисел, входящих в множество π' , являющееся дополнением к π , соответственно. Далее, π -избыток получается из π -сигнатуры вычитанием единицы: это, по определению,

$$\pi(a) - 1 + \left[\frac{\pi'(a)}{\pi(a)} \right].$$

π -сигнатура и π -избыток произвольной формы $f = [a, b, c, \dots]$ определяются теперь как суммы

$$\sigma_\pi(f) = \sigma_\pi(a) + \sigma_\pi(b) + \dots$$

и

$$e_\pi(f) = e_\pi(a) + e_\pi(b) + \dots$$

соответственно, так что $e_\pi(f) = \sigma_\pi(f) - \dim(f)$.

Теорема. Пусть π_1 и π_2 — два непересекающихся множества нечетных простых чисел, и пусть π — их объединение. Тогда $e_\pi \equiv e_{\pi_1} + e_{\pi_2} \pmod{8}$.

Доказательство. Пусть $a = P_1 P_2 a$, где через P_1 и P_2 обозначены соответственно P_1 - и P_2 -части числа a . Тогда

$$e_{\pi_1(a)} = (P_1 - 1) + \left[\frac{P_2}{P_1} \right] + \left[\frac{A}{P_1} \right],$$

$$e_{\pi_2(a)} = (P_2 - 1) + \left[\frac{P_1}{P_2} \right] + \left[\frac{A}{P_2} \right],$$

$$e_{\pi(a)} = (P_1 P_2 - 1) + \left[\frac{A}{P_1} \right] + \left[\frac{A}{P_2} \right].$$

Стало быть, теорема немедленно следует из закона взаимности

$$(P_1 - 1)(P_2 - 1) \equiv \left[\frac{P_1}{P_2} \right] + \left[\frac{P_2}{P_1} \right] \pmod{8}. \quad \square$$

А что можно сказать о множествах простых чисел, содержащих 2? Можно сделать так, чтобы аддитивность сохранялась и для таких множеств, если просто положить e_{π} для такого множества равным $-e_{\pi'}$. Это согласуется с данным выше определением 2-избытка.

Итак, мы доказали глобальное соотношение

$$e_{-1}(a) + e_2(a) + e_3(a) + e_5(a) + \dots \equiv 0 \pmod{8}$$

для одномерных форм $[a]$; ввиду аддитивности он верен и для произвольных форм f . Сумма на самом деле является конечной, поскольку все слагаемые в ней, кроме конечного их числа, равны нулю.

Усиленный принцип Минковского–Хассе

Из глобального соотношения и существования рациональных форм с данными инвариантами можно вывести важный факт, называемый иногда усиленным принципом Минковского–Хассе.

Теорема. *Рациональная форма f представляет рациональное число $r \neq 0$ над полем рациональных чисел $\mathbb{Q}$ тогда и только тогда, когда она представляет r над каждым из $\mathbb{Q}_p$ ($p = -1, 2, 3, \dots$).*

Доказательство. Число r представимо над некоторым полем формой f тогда и только тогда, когда над этим полем форма f эквивалентна форме $[r, *, *, \dots]$, или, говоря другими словами, если над этим полем f эквивалентна форме вида $[r] \oplus g$ для некоторой формы g . Стало быть, в условии теоремы сказано, что существуют такие формы $g^{(p)}$, что f является p -адически эквивалентной формам $[r] \oplus g^{(p)}$, а в заключении — что существует такая форма g , что f эквивалентна $[r] \oplus g$.

Стало быть, p -адические инварианты искомой формы g должны быть такими же, как у данных форм $g^{(p)}$. Существует ли такая форма g ? Да, существует! Единственное препятствие к ее существованию возникает из глобального соотношения, а оно для g выполнено, поскольку оно выполнено и для f , и для $[r]!$ $\square$

Теорема о четных унимодулярных формах

При $p \geq 3$ всякая целая квадратичная форма с определителем, взаимно простым с p , имеет целую p -адическую диагонализацию

$$f \simeq [a_1, a_2, \dots, a_n],$$

в которой все a_i взаимно просты с p . Стало быть, ее p -сигнатура равна n , а ее p -избыток равен нулю. Следовательно, для унимодулярной формы глобальное соотношение упрощается и принимает вид $e_{-1}(f) + e_2(f) \equiv 0 \pmod{8}$; равносильное условие: сигнатура формы f сравнима с ее нечетностью по модулю 8. Мы сейчас докажем, что у всякой четной унимодулярной квадратичной формы нечетность равна нулю, так что нулю по модулю 8 равна и сигнатура.

Форма указанного вида обязательно представляет число вида $2a$, где a нечетно, и мы можем воспользоваться этим обстоятельством, чтобы по индукции преобразовать форму в прямую сумму форм вида

$$\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \quad (a \text{ и } b \text{ нечетны})$$

над целыми 2-адическими числами. Над $\mathbb{Q}_2$ вписанная форма эквивалентна форме

$$[2a, 2a'], \quad a' = ad,$$

где $d = 4ac - b^2$ — определитель формы, сравнимый с -1 по модулю 4. Следовательно, одно из чисел a или a' сравнимо с 1 или 5 по модулю 8 а другое — с 3 или 7 по модулю 8. Следовательно, нечетность этой формы равна

$$(1 \text{ или } 5 + 4) + (3 + 4 \text{ или } 7),$$

что в любом случае делится на 8.

История четных унимодулярных решеток

Тот замечательный факт, что размерность положительно определенной четной унимодулярной решетки кратна восьми, является частным

случаем доказанного результата. Как мы видели, этот результат вытекает из формулы произведения. С другой стороны, можно показать, что, как и в рациональном случае, глобальное соотношение (являющееся почти немедленным следствием квадратичного закона взаимности) является единственным соотношением между p -адическими структурами для различных p , так что если оно выполнено, то существует квадратичная форма над рациональными числами с заданными p -адическими инвариантами. Этот результат можно уточнить с помощью «формулы массы», которая в некотором смысле дает подсчет числа квадратичных форм с заданными инвариантами.

В 1867 году Г. Дж. С. Смит [43] показал с помощью формулы массы, что существует восьмимерная четная унимодулярная решетка; эта решетка E_8 была в явном виде построена Коркиным и Золотарёвым в 1873 году. С помощью формулы массы можно также показать, что эта решетка единственна. В 1941 году Витт нашел две четные унимодулярные решетки размерности 16 (мы упоминали их в лекции 2). В 1973 году Нимейер показал, что имеется ровно 24 четных унимодулярных решетки в размерности 24, включая небезызвестную решетку Лича.

Теорема о трех квадратах

В следующем параграфе мы докажем знаменитую *теорему Лезжандра о трех квадратах*, датированную 1798 годом: целое положительное число является суммой трех квадратов тогда и только тогда, когда оно не является произведением степени четверки и числа, сравнимого с -1 по модулю 8. В этом параграфе мы покажем, что всякое такое число является суммой трех рациональных квадратов.

Заметим, что форма представляет число над $\mathbb{Q}$ тогда и только тогда, когда она представляет его над каждым из $\mathbb{Q}_p$. Стало быть, n является суммой трех квадратов рациональных чисел тогда и только тогда, когда его можно представить в виде суммы трех квадратов действительных чисел, а также в виде суммы трех квадратов рациональных p -адических чисел для каждого положительного простого числа $p=2, \dots$. Выяснить, существуют ли такие представления, очень просто, поскольку нам необходимо рассмотреть только одно число для каждого p -адического класса по модулю квадратов.

Рассмотрим различные случаи.

$p = -1$: число -1 , конечно, непредставимо, но $+1 = 1^2 + 0^2 + 0^2$ представимо. Стало быть, ненулевое n представимо в виде суммы трех квадратов тогда и только тогда, когда оно положительно.

$p = 2$: равенства

$$\begin{aligned} 1 &= 1^2 + 0^2 + 0^2, & 3 &= 1^2 + 1^2 + 1^2, & 5 &= 2^2 + 1^2 + 0^2, \\ 2 &= 1^2 + 1^2 + 0^2, & 6 &= 2^2 + 1^2 + 1^2, & 10 &= 3^2 + 1^2 + 0^2, \\ & & 14 &= 3^2 + 2^2 + 1^2 \end{aligned}$$

покрывают все классы по модулю квадратов, кроме -1 (или 7). Покажем, что -1 действительно не является суммой квадратов трех 2-адических рациональных чисел. В самом деле, в противном случае можно было бы считать, что

$$-d^2 = a^2 + b^2 + c^2,$$

где a , b и c — целые 2-адические числа, хотя бы одно из которых (скажем, a) нечетно (в противном случае можно было бы сократить на два). По модулю 8 получаем сравнение

$$-(0, 1 \text{ или } 4) \equiv 1 + (0, 1 \text{ или } 4) + (0, 1 \text{ или } 4),$$

что невозможно.

$p \geq 3$: как и в лекции 4, пусть $u = r + 1$ — наименьшее положительное число, являющееся квадратичным невычетом по модулю p , и пусть $r \equiv x^2 \pmod{p}$. Тогда классы чисел 1 и u по модулю квадратов представимы суммами *двух* квадратов, а именно

$$r \equiv x^2 + 0^2, \quad u \equiv x^2 + 1^2.$$

Следовательно, всякое число tp , являющееся кратным числа p , есть сумма трех квадратов, поскольку $tp - 1$ лежит в том же классе по модулю квадратов, что r или u , и тем самым является суммой двух квадратов.

Это рассуждение объясняет роль двух условий в теореме Лежандра. (-1) -адическое условие состоит в том, что n должно быть положительным; 2-адическое условие состоит в том, что n не должно быть равно $4^a(8k - 1)$; прочие p -адические условия выполнены всегда.

Представление в виде суммы трех квадратов целых чисел

Покажем, что всякое целое число, являющееся суммой трех квадратов рациональных чисел, является и суммой трех квадратов целых

чисел; в доказательстве мы воспользуемся остроумным методом спуска, опубликованным Обри в 1912 году [1].

Равенство

$$n = x_1^2 + x_2^2 + x_3^2$$

гласит, что $n = (x, x)$, где $x = (x_1, x_2, x_3)$. Пусть теперь не все числа x_i являются целыми; обозначим через m_i целое число, ближайшее к x_i , и пусть $x_i = m_i + r_i$. Тогда имеем $x = m + r$, где $0 < r \cdot r < 1$, и векторы m и dr имеют целые координаты. Следовательно,

$$n = (x, x) = (m, m) + 2(m, r) + (r, r),$$

откуда вытекает, во-первых, что $2(m, r) + (r, r)$ — целое число (обозначим его, скажем, через N), а во-вторых, что (r, r) — правильная дробь со знаменателем d (можно считать, что она равна d'/d , где $0 \leq d' < d$). Это, в свою очередь, показывает, что знаменатель вектора $r/(r, r) = dr/d'$ делит d' .

Теперь подвергнем x отражению в векторе r ! В результате получится новый вектор x' , для которого $(x', x') = (x, x)$, и тем самым новое представление n в виде суммы трех квадратов рациональных чисел. При этом, однако, имеем

$$x' = x - 2 \frac{(x, r)}{(r, r)} r = m + r - 2 \frac{(m, r)}{(r, r)} r - 2r = m - \frac{N}{(r, r)} r,$$

и это вектор, знаменатель которого делит d' .

Стало быть, отправляясь от произвольного представления n в виде суммы квадратов рациональных чисел с общим знаменателем $d > 1$, мы можем получить другое такое представление с общим знаменателем $d' < d$. Продолжая этот процесс, мы придем к представлению n , для которого $d = 1$, то есть к представлению в виде суммы трех квадратов *целых* чисел.

Следствия из теоремы Лежандра

Возможно, самая знаменитая запись в математическом дневнике, который вел молодой Гаусс, датирована 10 июля 1796 года. Вот эта запись:

$$\text{EÜRNKA!} \quad n \text{um} = \Delta + \Delta + \Delta.$$

Видимо, Гаусс доказал одно из утверждений, высказанных Ферма: всякое целое положительное число есть сумма трех треугольных чисел.

Это утверждение легко следует из теоремы Лежандра, говорящей нам, что $8n+3$ является суммой трех квадратов. Поскольку все эти квадраты должны быть нечетными, имеет место равенство

$$8n+3=(2a+1)^2+(2b+1)^2+(2c+1)^2,$$

из которого вытекает, что

$$n = \frac{a(a+1)}{2} + \frac{b(b+1)}{2} + \frac{c(c+1)}{2}.$$

Теорема Лежандра позволяет нам также выяснить, какие числа являются суммами четырех *положительных* квадратов. Заметим для начала, что числа вида $8k+3$ и $8k+6$, будучи суммами трех, но не двух, квадратов, с неизбежностью являются суммами трех положительных квадратов. Умножая на 4, получаем, что то же верно и для чисел $32k+12$ и $32k+24$.

Теорема. *Целые положительные числа, не представимые в виде суммы четырех положительных квадратов, суть в точности*

$$1, 3, 5, 9, 11, 17, 29, 41, 2 \times 4^m, 6 \times 4^m, 14 \times 4^m.$$

Доказательство. Покажем для начала, что всякое число, большее 49 и не кратное восьми, является суммой четырех положительных квадратов; для этого мы будем вычитать из данного числа квадрат с тем, чтобы разность стала числом, про которое выше доказана представимость в виде суммы трех положительных квадратов. Это делается так:

из $8k+2$ вычесть 2^2	— получится $8k+6$;
из $8k+3$ вычесть 4^2	— получится $8k+3$;
из $8k+4$ вычесть 1^2	— получится $8k+3$;
из $8k+6$ вычесть 4^2	— получится $8k+6$;
из $8k+7$ вычесть 2^2	— получится $8k+3$;
из $8k+1$ вычесть $1^2, 3^2, 5^2$ или 7^2	— получится $32k+24$;
из $8k+5$ вычесть $1^2, 3^2, 5^2$ или 7^2	— получится $32k+12$.

Для завершения доказательства надо перебрать числа, не превосходящие 49, и убедиться, что $8k$ является суммой трех положительных квадратов тогда и только тогда, когда такой суммой является $2k$. [Если один, два или три квадрата нечетны, то число имеет вид $4k+1$, $4k+2$ или $4k+3$, а если все четыре квадрата нечетны, то оно имеет вид $8k+4$. Следовательно, все квадраты должны быть четны.] $\square$

Аналогичными методами доказывается, что различные положительно определенные формы от четырех переменных универсальны,

т. е. представляют все целые положительные числа. Таковы, например, формы

$$x^2 + y^2 + z^2 + mt^2,$$

где $m = 1, 2, 3, 4, 5, 6, 7$. Теорема о трех квадратах показывает, что если такая форма не представляет некоторое целое число, то наименьшее из непредставляемых ей целых чисел должно иметь вид $8k + 7$. Однако же, вычитая mt^2 , где t в указанных семи случаях равно 1, 1, 2, 1, 1, 1, 2 соответственно, мы получим числа вида $8k + 6, 8k + 5, 8k + 3, 8k + 2, 8k + 1, 8k + 3$, которые уже представимы в виде $x^2 + y^2 + z^2$.

Теорема о пятнадцати

Уильям Шнеебергер (William Schneeberger) и я доказали недавно с использованием этих идей замечательную теорему. Именно, оказывается, что если положительно определенная квадратичная форма (от произвольного числа переменных) с целочисленной матрицей представляет каждое из чисел

$$1, 2, 3, 5, 6, 7, 10, 14, 15,$$

то она представляет всякое целое положительное число. Чтобы вывести, например, из этой теоремы теорему Лагранжа о четырех квадратах, достаточно убедиться, что каждое из выписанных целых чисел есть сумма не более чем четырех квадратов:

$$\begin{aligned} 1 &= 1^2, & 2 &= 1^2 + 1^2, & 3 &= 1^2 + 1^2 + 1^2, & 5 &= 2^2 + 1^2, \\ 6 &= 2^2 + 1^2 + 1^2, & 7 &= 2^2 + 1^2 + 1^2 + 1^2, & 10 &= 3^2 + 1^2, \\ 14 &= 3^2 + 2^2 + 1^2, & 15 &= 3^2 + 2^2 + 1^2 + 1^2. \end{aligned}$$

Вот теорема Лагранжа и доказана!

Заинтересованный читатель может вывести из этой теоремы еще какое-нибудь утверждение того же типа: например, всякое целое положительное число можно записать в виде $a^2 + 2b^2 + 5c^2 + 5d^2 + 15e^2$.

Теорема о пятнадцати доказывается рассуждением, аналогичным вышеприведенному, но вместо суммы трех квадратов рассматриваются другие формы g ; эти формы строятся следующим образом. Если f представляет девять выписанных выше чисел, то в ее решетке должны содержаться векторы с нормами 1, 2, 3, 5, ... Подрешетка, порожденная этими векторами, может принадлежать только к конечному числу видов, и почти во всех случаях можно найти трехмерную

подрешетку, для которой соответствующая форма g является единственным элементом своего рода. Стало быть, мы знаем, какие числа представляются формой g , а отсюда можно вывести, что всякое число представляется формой f .

Ни одна знакоопределенная тернарная форма не является универсальной

Простое рассуждение показывает, что, напротив, всякая знакоопределенная тернарная форма должна не представлять бесконечно много целых чисел (даже над $\mathbb{Q}$). В самом деле, если тернарная форма f с определителем d представляет число, лежащее в классе элементов $\mathbb{Q}_p$ по модулю квадратов, содержащем $-d$, то она должна быть p -адически эквивалентна форме $[-d, a, b]$, где «факторформа» имеет определитель -1 ; стало быть, над $\mathbb{Q}_p$ форма f должна быть изотропной формой $[-d, 1, -1]$.

Однако же положительно определенная форма не представляет -1 и тем самым не является p -адически изотропной при $p = -1$. Ввиду глобального соотношения должно существовать еще одно p , для которого эта форма не является p -адически изотропной, так что она не может представлять все p -адические числа (для данного p), лежащие в классе $-d$ по модулю квадратов!

Теорема о трех квадратах хорошо иллюстрирует эту ситуацию: форма $[1, 1, 1]$ не представляет -1 не только (-1) -адически, но и 2-адически! В третьей лекции мы видели, что малая мафусаилова форма

$$x^2 + 2y^2 + yz + 4z^2$$

не представляет число 31. Теперь мы видим, что коль скоро она не представляет (-1) -адический класс своего определителя $-31/4$ (т. е. отрицательные числа), она также должна не представлять бесконечно много целых положительных чисел, лежащих в 31-адическом классе числа $-31/4$ по модулю квадратов.

Библиография

Наряду со статьями (иногда весьма давними), на которые мы ссылаемся в тексте, мы включили в библиографию некоторые учебники для дальнейшего чтения.

Во-первых, за подробностями и гораздо более полной библиографией можно обращаться к книге энциклопедического характера [7], а также к серии статей [9]–[14].

Далее, при изучении классической теории бинарных квадратичных форм бесспорно стоит полистать основополагающую работу [20]. Из учебников см. [5], [6] (продвинутый учебник, написанный на вполне элементарном языке), [17] (особенно теорему о спинорном роде), [18] (изложение работ Гаусса), [25] (довольно абстрактное изложение), [23] (вполне элементарный), [33], [36], [37], [42] (прекрасное элементарное изложение теорем Минковского–Хассе и Дирихле, а также p -адических чисел) и [49], а также библиографии в этих книгах.

- [1] L. Aubry. Solution de quelques questions d'analyse indéterminée // Sphinx-Œdipe. — 1912. — V. 7. — P. 81–84.
- [2] P. Buser, J. Conway, P. Doyle, K.-D. Semmler. Some planar isospectral domains // Internat. Math. Res. Notices. — 1994. — № 9. — 391ff., approx. 9 pp. (electronic).
- [3] M. Berger, P. Cauduchon, E. Mazet. Spectre d'une variété riemannienne. — Springer-Verlag, 1971. — (Lect. Notes Math., V. 194).
- [4] H. Blichfeldt. The minimum values of positive quadratic forms in six, seven, and eight variables // Math. Z. — 1935. — V. 39. — P. 1–15.
- [5] D. A. Buell. Binary Quadratic Forms: Classical Theory and Modern Computations. — Springer-Verlag, 1989.
- [6] J. W. S. Cassels. Rational Quadratic Forms. — Academic Press, 1978. — Русский перевод: Дж. Касселс. Рациональные квадратичные формы. — М.: Мир, 1982.
- [7] J. H. Conway, N. J. A. Sloane. Sphere Packings, Lattices, and Groups. — Springer-Verlag, 1986; 2nd ed. — 1992. — Русский перевод: Дж. Конвей, Н. Слоэн. Упаковки шаров, решетки и группы: В 2 т. — М.: Мир, 1990.

- [8] J. H. Conway, N. J. A. Sloane. Four-dimensional lattices with the same theta series // *Duke Math. J.* — 1992. — V. 66. — P. 93–96.
- [9] J. H. Conway, N. J. A. Sloane. Low-dimensional lattices I: Quadratic forms of small determinant // *Proc. Roy. Soc. Lond., Ser. A.* — 1988. — V. 418. — P. 17–41.
- [10] J. H. Conway, N. J. A. Sloane. Low-dimensional lattices II: Subgroups of $GL_n(\mathbb{Z})$ // *Proc. Roy. Soc. Lond., Ser. A.* — 1988. — V. 419. — P. 29–68.
- [11] J. H. Conway, N. J. A. Sloane. Low-dimensional lattices III: Perfect forms // *Proc. Roy. Soc. Lond., Ser. A.* — 1988. — V. 418. — P. 43–80.
- [12] J. H. Conway, N. J. A. Sloane. Low-dimensional lattices IV: The mass formula // *Proc. Roy. Soc. Lond., Ser. A.* — 1989. — V. 419. — P. 259–286.
- [13] J. H. Conway, N. J. A. Sloane. Low-dimensional lattices V: Integral coordinates for integral lattices // *Proc. Roy. Soc. Lond., Ser. A.* — 1989. — V. 426. — P. 211–232.
- [14] J. H. Conway, N. J. A. Sloane. Low-dimensional lattices VI: Voronoi reduction of three-dimensional lattices // *Proc. Roy. Soc. Lond., Ser. A.* — 1991. — V. 436. — P. 55–68.
- [15] Б. Н. Делоне. Sur la partition régulière de l'espace à 4 dimensions // *Изв. Акад. Наук СССР, отдел физ.-мат. наук.* — 1929. — Т. 7. — С. 79–110, 147–164.
- [16] A. Earnest, G. Nipp. On the theta series of positive definite ternary quadratic forms // *C. R. Math. Rep. Acad. Sci. Canad.* — 1991. — V. 13, № 1. — P. 33–38.
- [17] M. Eichler. Quadratische Formen und Orthogonale Gruppen. // *Grundl. der Math. Wiss., V. 63.* — Springer-Verlag, 1952; 2nd ed. — 1974.
- [18] D. Flath. Introduction to Number Theory. — John Wiley and Sons, 1989.
- [19] S. Gallot, D. Hulin, J. Lafontaine. Riemannian Geometry. — Springer-Verlag, 1987; 2nd ed. — 1990.
- [20] C. F. Gauss. Disquisitiones Arithmeticae. — Leipzig: Fleischer, 1801. — English transl.: Yale Univ. Press, reprinted: Springer-Verlag, 1986.
- [21] C. F. Gauss. Besprechung des Buchs von L. A. Seeber, "Untersuchung über die Eigenschaften der positiven ternären quadratischen Formen usw." // *Göttingen Gelehrte Anzeigen.* — Jul. 9,

- 1831 = Werke, Bd II, 1876, 188–196.
- [22] A. Hurwitz. Über die Reduktion der binären und ternären quadratischen Formen // Math. Ann. — 1894. — V. 45, P. 85–117 = Werke, Bd II, 157–190.
- [23] B. W. Jones. The Arithmetic Theory of Quadratic Forms. — John Wiley and Sons, 1950. — (Carus Math. Monographs, V. 10).
- [24] M. Kac. Can one hear the shape of a drum? // Am. Math. Monthly. — 1966. — V. 73, № 4, part II. — P. 1–23.
- [25] Y. Kitaoka. The Arithmetic of Quadratic Forms. — Cambridge Univ. Press, 1993. — (Cambridge Tracts in Math., V. 106).
- [26] Y. Kitaoka. Positive definite quadratic forms with the same representation numbers // Arch. Math. — 1977. — V. 28. — P. 495–497.
- [27] M. Kneser. Lineare Relationen zwischen Darstellungszahlen quadratischer Formen // Math. Ann. — 1967. — V. 168. — P. 31–39.
- [28] A. Korkine, G. Zolotareff. Sur les formes quadratiques positives quaternaires // Math. Ann. — 1872. — V. 5. — P. 581–583.
- [29] A. Korkine, G. Zolotareff. Sur les formes quadratiques // Math. Ann. — 1872. — V. 6. — P. 366–389.
- [30] A. Korkine, G. Zolotareff. Sur les formes quadratiques positives, // Math. Ann. — 1877. — V. 11. — P. 242–292.
- [31] J. L. Lagrange. Démonstration d'un théorème d'Arithmétique // Nouv. Mém. Acad. Roy. Soc. de Berlin. — 1770 (1772). — P. 123–133 [Œuvres, V. 3, P. 189–201].
- [32] A. M. Legendre. Essai sur la théorie des nombres. — Paris, chez Duprat, 1798.
- [33] G. B. Matthews. Theory of Numbers. — 1896 = Chelsea, 1961.
- [34] J. Milnor, D. Husemoller. Symmetric Bilinear Forms. — Springer-Verlag, 1973. — (Ergebnisse der Math., V. 73). — Русский перевод: Милнор Дж., Хьюзмоллер Д. Симметрические билинейные формы. — М.: Наука, 1986.
- [35] L. J. Mordell. Observation on the minimum of a positive definite quadratic forms on eight variables // J. Lond. Math. Soc. — 1944. — P. 3–6.
- [36] O. T. O'Meara. Introduction to Quadratic Forms. — Springer-Verlag, 1963; 2nd printing — 1971. — (Grundle. der Math. Wiss., V. 117).
- [37] W. Scharlau. Quadratic and Hermitian Forms. — Springer-Verlag, 1985. — (Grundle. der Math. Wiss., V. 270).
- [38] A. Schiemann. Ein Beispiel positiv definite quadratischer Formen der Dimension 4 mit gleichen Darstellungszahlen // Arch.

- Math. — 1990. — V. 54. — P. 372–375.
- [39] A. Schiemann. Ternäre positiv definite quadratischer Formen mit gleichen Darstellungszahlen. — Dissertation, Bonn, 1993.
- [40] A. Scholz. Einführung in die Zahlentheorie. // Sammlung Göschen Bd. 1131, W. de Gruyter & Co., 1939.
- [41] E. Selling. Über die binären und ternären quadratischen Formen // J. reine angew. Math. — 1874. — V. 77. — P. 143–229.
- [42] J. P. Serre. Cours d'Arithmétique. — Paris, Presses Universitaires de France, 1970. — Русский перевод: Серр Ж. - П. Курс арифметики. М.: Мир, 1972.
- [43] H. J. S. Smith. On the orders and genera of ternary quadratic forms // Phil. Trans. Roy. Soc. Lond. — 1867. — V. 157. — P. 255–298 = Coll. Math. Papers. — V. I. — P. 455–509.
- [44] H. J. S. Smith. On the orders and genera of quadratic forms containing more than three indeterminates // Proc. Roy. Soc. — 1867. — V. 16. — P. 197–208 = Coll. Math. Papers. — V. I. — P. 510–523.
- [45] М. И. Штогрин. Правильные разбиения Дирихле–Вороного для второй триклинной группы. // Труды мат. инст. им. Стеклова. — 1973. — V. 123.
- [46] I. Stewart, D. Tall. Algebraic Number Theory. — 2nd ed. — Chapman and Hall, 1987.
- [47] Н. М. Ветчинкин. Единственность классов положительных квадратичных форм, на которых значения констант Эрмита достигаются при $6 \leq n \leq 8$ // Труды мат. инст. им. Стеклова. — 1980. — V. 152. — P. 37–95.
- [48] G. F. Voronoï. Nouvelles applications des paramètres continus à la théorie des formes quadratiques // J. reine angew. Math. I. Sur quelques propriétés des formes quadratiques positives parfaites. — 1908. — V. 133. — P. 97–178; II.1. Recherches sur les paralléloèdres primitifs. — 1908. — V. 134. — P. 198–287; II.2 Domaines de formes quadratiques correspondant aux différents types de paralléloèdres primitifs. — 1909. — V. 136. — P. 67–181.
- [49] G. L. Watson. Integral Quadratic Forms. — Cambridge Univ. Press, 1960. — (Cambridge Tracts in Math and Math. Phys., V. 57).
- [50] E. Witt. Eine Identität zwischen Modulformen zweiten Grades // Abh. Math. Sem. Univ. Hamb. — 1941. — V. 14. — P. 323–337.

Предметный указатель

- 2-адический антиквадрат 92
 - символ 101, 102
 - —, инвариантность 107
- 2-адическое гауссово среднее 107
- 2-сигнатура 92
- A_n (решетка) 55
- D_n (решетка) 55
- E_7 (решетка) 56
- E_8 (решетка) 56
- $GL_2(\mathbb{Z})$ 35
- p -адическая рациональная эквивалентность 93
- p -адические сигнатуры 91, 111
 - —, инвариантность 111
 - числа 93, 111, 113, 115
 - — рациональные 88, 93, 113
- p -адический антиквадрат 92
 - символ 101
 - —, инвариантность 106
 - —, связь с родами 103
 - —, слышимость 53, 106
- p -адическое гауссово среднее 104
 - — —, инвариантность 105
- p -избыток 94, 126
- p -члены 96
- $PGL_2(\mathbb{Z})$ 37
- $PSL_2(\mathbb{Z})$ 32, 40
- $SL_2(\mathbb{Z})$ 35
- $\mathbb{Z}$ -модуль 10
- Алгебра Ли типа E_8 41
- Алгоритм, решающий проблему представления 31
 - , решающий проблему эквивалентности 31
- Альберс Д. (Albers Donald) 5
- Амбиговые формы 115
- Антиквадрат 2-адический 92
- Антиквадрат p -адический 92
- Аполлония теорема 15
- Арифметическая прогрессия 15
- Базис 9, 12
 - , приведенный по Минковскому 80
- Барабан 38
 - , его форма 38, 47
- Барановский Е. П. 87
- Бинарные формы над $\mathbb{Q}_p$ 113
- Блихфельд Г. Ф. (Blichfeldt H. F.) 79
- Бузер П. (Buser P.) 38, 48
- Вебб Д. (Webb David) 38
- Вектор Вороного 21, 63
 - — в нестрогом смысле 65
 - — в строгом смысле 64
- Верхняя полуплоскость 32
- Ветчинкин Н. М. 79
- Виртуальные конормы 76
 - конормы 74
- Витт Э. (Witt Ernst) 41, 57
- Вольперт С. (Wolpert Scott) 38
- Конормы 21, 62, 66, 69
 - виртуальные 76
 - , выражение через конормы 70
 - для трехмерных решеток 69
 - несобственные 66
 - собственные 69
- Вороной Г. Ф. 20, 63, 76
- Гаусс К. Ф. (Gauss C. F.) 8, 79, 115, 131
- Гауссово среднее 51, 53
 - — 2-адическое 107
 - — p -адическое 104
 - — диагональной формы 53

- Гауссово среднее
модифицированное 103
— — прямой суммы 53
Гексаромбический додекаэдр 78
Гензель К. (Hensel K.) 111
Геометрия Лобачевского 33
Гиллман Л. (Gillman Leonard) 5
Гильбертов символ норменного
вычета 99
Гильбертово произведение 99
— — полное 99
Глобальное соотношение 94, 111,
116
— —, доказательство 126
Гордон Каролина (Gordon
Caroline) 38, 47
Группа изометрий 28, 31
- Давидовф Джулиана (Davidoff
Juliana) 6
Дамба 29
Двойственная решетка 51
— факторгруппа 52, 55
Делоне Б. Н. 76, 83
Дерево 17, 27
Диагонализация 89
Диофантовы приближения 35
— уравнения 28, 30
Дискриминант 10
Древесное свойство топокарты
17
Дроби Фарея 32, 34, 35, 37
- Единица Минковского 98
— — сопряженная 98
- Жорданово разложение 101
Жордановы компоненты 101
- Задача Дирихле 38
— —, граничные условия 49
Задача Неймана 50
Задача эквивалентности 31
Зеллинг Э. (Selling E.) 21, 63, 76
- Знакоопределенные тернарные
формы, неуниверсальность 134
Золотарёв Е. И. 79, 120, 129
Зона Бриллюэна 63
- Изокубическая решетка 44, 109
Изоспектральность по Дирихле
50
Изоспектральные коды 43
— многообразия 47
— области 47–50
— решетки 39, 41–43
— —, 12- и 8-мерные примеры 43
— —, 16-мерные примеры 42
— —, бесконечное семейство
пятимерных примеров 45
— —, отсутствие двумерных
примеров 47
— —, отсутствие трехмерных
примеров 47
— —, первая шимановская пара
46
— —, пример Милнора 40
— —, шестимерные примеры 43
— —, шимановские
четырёхмерные примеры 45
— торы 41
Изотропные формы 114
Инварианты Минковского–Хассе
98–99
— тривиальные 94
— целых форм 99
- Кац Марк (Kac Mark) 38, 47
Квадратичные формы 8
— —, гауссово среднее 51
— —, запись в базисе 16
— —, классификация 54
— —, прямая сумма 52
Квадратичный закон взаимности
120
— — —, для символа Якоби 124
Китаока Ё. (Kitaoka Y.) 43

Классификация квадратичных форм 23, 54
— — — неопределенных 62
— — — целых бинарных 31
Классы по модулю квадратов 113
— p -адические 114
Клеевой вектор 55
Кнезер М. (Kneser M.) 42, 54
Колодец 19
— двойной 23, 66
— для положительно определенных форм 18
— простой 21
Конормы 21, 62, 66, 70, 76, 83
— виртуальные 74
—, выражение вонорм через конормы 70
— для трехмерных решеток 70
— для четырехмерных решеток 83
—, связь с параметрами Зеллинга 76, 83
—, связь с характеристиками 66, 70
— характеров 70
Коркин А. Н. 79, 129
Круги Форда 33
Кубическая решетка 42, 109
Кубичность, неслышимость 44
—, слышимость 44, 60
Лагранж Ж.-Л. (Lagrange J.-L.) 133
Лапласиан 38
Лежандр А.-М. (Legendre A.-M.) 8, 115, 129
Лемма Витта о решетках корней 58
— о возрастании 17
— о замене 96
— о колодце 19
Линейный символ Якоби 125
Лич Дж. (Leech John) 57, 129
Малая мафусаилова форма 81

Матрица 10, 11
—, восстановление по топокарте 16
Матричная целочисленность 10
Медианта 34
Милнор Дж. (Milnor John) 38
Минимальная норма 79
Модулярная группа 40
— форма 40
Морделл Л. (Mordell L. J.) 79
Неопределенные формы 24, 62
— —, классификация 62
— —, представляющие нуль 29
Неполное гильбертово произведение 99
Неравенство треугольника 20
Неслышимость кубичности 44
— рода в старших размерностях 109
Несобственные вонормы 66
Нестрогий базис 12
— вектор 12
— супербазис 12
Несущественный знаменатель 117
Нечетность 92
Нимейер Х.-Ф. (Niemeier H.-V.) 57
Нимейеровские решетки 57
Норма вектора 15
Нормы Вороного см. вонормы
Область 14
— Вороного 62, 63, 76–79
— — двумерной решетки 76
— — для 4- и 5-мерных решеток 82
— —, пять видов 76
— — с 62 гранями 87
— —, содержащая начало координат 63
— — трехмерной решетки 76

- Область Дирихле 63
 Обри Л. (Aubry L.) 131
 Озеро 24
 — и река 29
 Определитель 10, 11, 51
 —, слышимость 51
 Орицикл 37
 Ортогональная группа 117
- Параметры Зеллинга** 21, 63, 76, 83
 — —, связь с конормами 76, 83
 Периодическая река 26
 Периодичность символа Якоби 123
 Плоскость Лобачевского 37
 — Фано 68
 Правило арифметической прогрессии 15
 — движения знаков 103
 — слияния нечетностей 102
 Приведение по Минковскому 80
 Примитивные решетки 87
 Примитивный вектор 12
 — — на топокарте 14
 Пространство вонорм 67
 — конорм 67
 Прямая сумма 52
 — —, гауссово среднее 53
 Прямоугольный параллелепипед 78
- Рациональная эквивалентность** 88
 Рациональные квадратичные формы 88
 — — — заданными инвариантами 114
 Река 24, 25
 —, единственность 26
 — между двумя озерами 29
 — нулевой длины 29
 — периодическая 26
- Река, участки 24
 Решетка 9, 38
 — A_n 55
 — D_n 55
 — E_7 56
 — E_8 56
 —, ее двойственная факторгруппа 52, 55
 — изокубическая 44
 — Лича 57, 129
 Решетки 16-мерные 41
 — изоспектральные 41, 42
 — корней 55, 58
 — неграфовые 86
 — нийееровские 24-мерные 57
 — примитивные 87
 —, склеивание 56
 —, соответствующие упаковкам сфер 79
 — четные унимодулярные 41
 — — —, история 128
 — четырехмерные графовые 84
 Риманово многообразие 38, 39
 Род 62, 103
 —, неслышимость в старших размерностях 109
 —, связь с p -адическими символами 103
 —, слышимость в размерности 4 108, 109
 Ромбическая упаковка 41
 Ромбодекаэдр 78
 Рышков С. С. 87
 Ряд Фарея 34
- Связность топокарты** 18, 21
 Серр Ж.-П. (Serge J.-P.) 115
 Сигнатура 2-сигнатура 92
 — p -адическая 91
 — по Сильвестру 91
 Сильвестр Дж. (Sylwester J. J.) 91
 Символ 107

- Символ Лежандра 99, 120
— Якоби 102, 120
— —, взаимность 124
— —, линейная версия 125
— —, периодичность 123
Склеивание решеток 54, 56, 58, 60
Слоун Нил (Sloane Neil) 43
Слышимость 39, 51, 88
— p -адических символов 53
— p -размерностей 53
— для двумерных решеток 47
— для трехмерных решеток 47
— кубичности 44
— определителя 51
— рода в размерности 4 108, 109
— тэта-функции 51
Смит Г. (H. J. S. Smith) 129
Собственная функция 49
Собственное значение 38
Собственные вонормы 66, 69
Собственный характер 66
Сопряженная единица Минковского 98
Спиновая норма 118
— эквивалентность 118
Спиновое ядро 118
Спинорный род 62, 118
Стрелки на топокарте 15
Строгий базис 12
— вектор 12
— superbазис 12
Сунада Т. (Sunada Toshikazu) 38
Супербазис 12
— нестрогий 12
— нестрого тупоугольный 66
— строгий 12
— строго тупоугольный 66
— тупоугольный 63, 70
Существенные простые числа 117
Теорема Аполлония 15
Теорема Витта о сокращении 95
— Дирихле 115
— Лагранжа о четырех квадратах 133
— Минковского–Хассе 93
— —, доказательство 94–98
— о трех квадратах 115, 129
— — —, доказательство 129–131
— Уотсона 118
— Эйхлера о классификации 62, 119
Тетракод 45
Тетрарешетка 45
Тождество Аполлония 95
Топокарта 13–16
—, древесное свойство 17
— малой мафусаиловой формы 81
—, независимость общего вида от коэффициентов формы 15
—, ориентация ребер 15
—, связность 18, 21
—, связь с матричной записью 16
Торы 39
— изоспектральные 41
Трехмерные решетки 69
Тупоугольный superbазис 63, 70
— — в размерности 3 72
Тэта-константы 41
Тэта-функция 39, 51
— для двумерной решетки 47
—, слышимость 51
Уотсон Дж. Л. (Watson G. L.) 118
Усеченный октаэдр 77
Усиленный принцип Минковского–Хассе 127
Факторгруппа $L/2L$ 64
Факторпространство 39
Форма p -адическая единичная 101

- Форма амбиговая 115
— барабана 38, 47, 50
— изотропная 114
— малая мафусаилова 81
— не представляющая нуль 24
— неопределенная 24
— отрицательно определенная 19
— — полуопределенная 19
— положительно определенная 18
— — полуопределенная 18
— полуопределенная 28, 29
— представляющая нуль 29
— приведенная по Минковскому 80
— решетки 38, 40, 42, 44, 46, 47
— с дамбой 29
— типа $0 \pm$ 29
— типа I 102
— типа II 102
— типов $0, 0+, 0-, 0 \pm$ 24
— универсальность 132
— целая 26
Формула Зеллинга 20, 21
— произведения 94
— Якоби 51
Фунг Ф. (Fung Francis) 6
Фундаментальная область 32
- Характеры 66
—, их конормы 70
—, связь с конормами 66
— собственные 66
Хедрик Э. Р. (Hedrick Earle Raymond) 4
- Целая квадратичная форма 8, 10
Целое p -адическое число 111
Целочисленная эквивалентность 11
Целочисленность 10
Целые бинарные квадратичные формы, классификация 31
— формы, инварианты 88, 99
— — с заданными инвариантами 116
- Четные унимодулярные решетки 41, 54
— — — 24-мерные 58
— — —, история 128
— — формы 128
Четырехмерные графовые решетки 84
- Шестиугольная решетка 39
Шиман А. (Schiemann A.) 45
Шнеебергер В. (Schneeberger William) 133
Шольц А. (Scholz A.) 124
Штогрин М. И. 83
- Эйхлер М. (Eichler M.) 118
Эквивалентность p -адическая
рациональная 93
— рациональная 89
— с несущественным знаменателем 117
Энгель П. (Engel Peter) 87
- Якоби К. (Jacobi C. G.) 42

Книга, написанная известным американским математиком, содержит нестандартное изложение различных аспектов теории целочисленных и рациональных квадратичных форм, включая теорему Минковского – Хассе. И студенты старших курсов, и аспиранты, и научные работники найдут в книге много необычного и интересного; всем этим читателям книга адресована.

ISBN 978-5-94057-268-8



9 785940 572688 >