В. И. Арнольд

Динамика, статистика и проективная геометрия полей Галуа

МЦНМО

УДК 511
ББК 22.13
А84

Арнольд В. И.
Динамика, статистика и проективная геометрия полей Галуа
Электронное издание
М.: МЦНМО, 2014
72 с.
ISBN 978-5-4439-2046-7

В этой книге, являющейся записью прочитанной автором 13 ноября 2004 года лекции для школьников Малого мехмата МГУ, рассказано об удивительных недавно открытых связях алгебраической теории полей Галуа с теорией динамических систем, хаоса и статистики с одной стороны и с геометрией проективных структур на множествах из конечного числа точек — с другой.

Бóльшая часть этих новых открытий обнаружена экспериментальным путём, а возникшие при этом гипотезы во многих случаях ещё не доказаны, хотя и их понимание, и их эмпирическая проверка легко доступны школьникам, особенно владеющим компьютером.

Ждут пытливых исследователей и многие теоретические вопросы — например, напрашивающийся вопрос о том, чем выделяется подгруппа проективных перестановок в полной группе всех перестановок конечного множества, каковы специальные геометрические свойства проективных перестановок дюжины точек, отличающие эти перестановки от непроективных.

Подготовлено на основе книги: *В. И. Арнольд*. Динамика, статистика и проективная геометрия полей Галуа. — М.: МЦНМО, 2005.

Издательство Московского центра
непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11. Тел. (499) 241-74-83
http://www.mccme.ru

ISBN 978-5-4439-2046-7

© Арнольд В. И., 2005
© МЦНМО, 2014

ОГЛАВЛЕНИЕ

§ 1. Что такое поле Галуа? 4

§ 2. Как устроены поле Галуа и его таблица 11

§ 3. Хаотичность и случайность чисел таблицы поля Галуа 18

§ 4. Равномерное распределение геометрической прогрессии вдоль конечного одномерного тора 24

§ 5. Адиабатический анализ распределения геометрической прогрессии остатков 36

§ 6. Проективные структуры для полей Галуа 42

§ 7. Вычисление проективных структур на конечных проективных прямых для полей из p^2 элементов 51

Приложение. Кубические таблицы полей 63

§ 1
ЧТО ТАКОЕ ПОЛЕ ГАЛУА?

Поля Галуа — это поля из конечного числа элементов. Они относятся к небольшому набору самых фундаментальных объектов математики, при помощи которых описываются все другие математические структуры и модели.

Всем известный пример подобных фундаментальных объектов — простые числа, $p = 2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots, 997, \ldots$, т. е. целые положительные числа, делящиеся нацело только на два целых числа: на себя и на единицу (которую простым числом не считают).

Первый же естественно-научный вопрос, возникающий при рассмотрении простых чисел, уже довольно труден: *конечно ли количество простых чисел*, или же последовательность простых чисел продолжается неограниченно? Ответ на этот вопрос получен несколько тысячелетий назад: *последовательность простых чисел не ограничена*, *самого большого простого числа нет.*

Это видно, например, из того, что большое число

$$(2 \cdot 3 \cdot 5 \cdot \ldots \cdot p) + 1$$

даёт в остатке единицу при делении на каждое простое число до p включительно, а потому не делится ни на одно из них. Из этого следует, что это большое число имеет простой делитель, больший чем p, а значит, *наибольшего простого числа не может существовать.*

Это замечательное математическое рассуждение оставляет для естествоиспытателя открытым главный вопрос: *насколько часто* встречаются простые числа в натуральном ряду, растут ли интервалы между ними по мере роста чисел? Насколько велико миллионное простое число?

Первым естествоиспытателем, занявшимся этими вопросами, был Лежандр, исследовавший в XVIII веке все простые числа до миллиона и заметивший следующий *закон убывания плотности простых чисел*: среднее расстояние между последовательными простыми числами, близкими к числу n, растёт с ростом n как $\ln n$ (натуральный логарифм, т. е. логарифм при основании $e = 2{,}71828...$). Например, $\ln 10 \approx 2{,}3$, а в районе значения $n = 10$ среднее расстояние между последовательными простыми числами немного больше двух ($7 - 5 = 2$, $11 - 7 = 4$, $13 - 11 = 2$). Поблизости от числа $n = 100$ последовательность простых состоит из чисел 89, 97, 101, 103, так что среднее расстояние между соседями есть $4\frac{2}{3}$, тогда как $\ln 100 = 2 \ln 10 \approx 4{,}6$.

Разумеется, наличие «близнецов» (пар простых чисел с разностью 2) препятствует постоянному росту самого расстояния с ростом чисел, но *среднее* расстояние может расти с n, даже если число пар близнецов и бесконечно (так что существуют сколь угодно большие близнецы — эта знаменитая гипотеза о бесконечности числа пар близнецов, до сих пор не доказанная и не опровергнутая, считается одной из важнейших задач теории чисел).

К сожалению, наблюдения Лежандра не были признаны математиками за научное достижение, так как он «ничего не доказал, а только рассмотрел миллионы примеров» (и обобщил полученные в этих примерах эмпирические статистические данные), вовсе не умея строго перейти к пределу при неограниченном возрастании числа n.

Колмогоров не раз говорил мне о своих исследованиях гидродинамической турбулентности: «Не ищите там теорем, их нет, я ничего не умею выводить из исходных для этой теории уравнений Навье—Стокса. Мои результаты об их решениях *не доказаны*, *а верны* — что гораздо важнее всех доказательств».

Первым оценил достижение Лежандра русский математик Чебышёв. Прежде всего он доказал, что если изучаемое среднее расстояние между близкими к n простыми числами и не ведёт себя асимптотически как $\ln n$, то оно всё же в среднем отличается от такого выражения *не более чем в конечное число раз*, т. е. заключено между $c_1 \ln n$ и $c_2 \ln n$ (с явно найденным постоянными, $c_1 < c_2$).

Позже он доказал больше: если колебания между указанными границами «затухают» при увеличении числа n, так что устанавливается асимптотика $c \ln n$ среднего расстояния между близкими к n простыми числами, то *постоянная c может быть только единицей*.

Это ещё не *доказывает* асимптотики Лежандра, так как не исключает возможности вечно продолжающихся колебаний между $c_1 \ln n$ и $c_2 \ln n$ без установления предельного режима $c \ln n$.

Но не прошло и ста лет после открытия Лежандра, как два знаменитых математика, француз Адамар и бельгиец Валле Пуссен, доказали затухание этих колебаний, т. е. *существование* предельной асимптотики $c \ln n$.

С тех пор считается, что Адамар и Валле Пуссен сделали великое открытие — обнаружили статистический закон распределения больших простых чисел.

С моей точки зрения приписывать это открытие Адамару и Валле Пуссену — сильная несправедливость. Ведь эти (действительно замечательные) математики доказали только *существование* некоторого (равного неизвестному им c) предела. И открытие естественно-научного факта (пропорционального в среднем величине $\ln n$ роста расстояния между

последовательными простыми числами), и вычисление предела c (равного на самом деле 1) — и то и другое сделано не ими, а Лежандром и Чебышёвым, которым и принадлежит на самом деле великое открытие, описанное выше.

В предлагаемых лекциях для школьников я буду следовать скорее Лежандру, чем Адамару: я расскажу об экспериментальных числовых наблюдениях, которые подсказывают новые (поразительные) законы природы, но которые далеко не сразу превращаются в теоремы. Я думаю, что в некоторых случаях доказательств придётся ждать сотню-другую лет (как это произошло и с законом распределения простых чисел), хотя сами открытия новых законов могут быть доступны школьникам (не обязательно владеющим компьютерной техникой, которая всё же может помочь в экспериментальном поиске эмпирических законов, хотя я её и избегал, когда искал те факты, о которых пойдёт речь ниже).

Наряду с простыми числами, другой яркий пример фундаментальных математических объектов — *правильные многогранники* (называемые также «платоновыми телами», так как их открыл не Платон), рис. 1.1. Их пять: тетраэдр, октаэдр, куб, икосаэдр (имеющий 20 треугольных граней, на что указывает греческое числительное «икос») и додекаэдр (имеющий «додека» = 12 пятиугольных граней и использованный Кеплером для описания «четвертым законом Кеплера» распределения радиусов планетных орбит Солнечной системы).

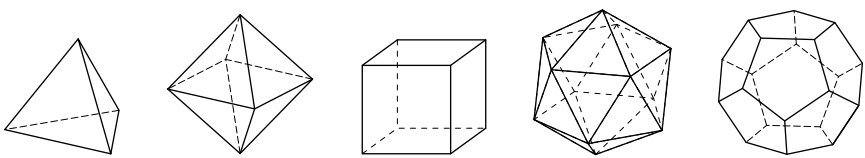

Рис. 1.1. Правильные многогранники

Правильные многогранники неожиданно оказались ответственными за на вид никак не связанную с ними область физики — теорию *оптических каустик*, доставляющую объяснение радуги (с её угловым радиусом 42°, рис. 1.2) с одной стороны и, например, теорию скапливания галактик в крупномасштабной структуре Вселенной — с другой.

Колмогоров говорил, что особенную красоту математическим теориям придаёт именно обнаруживаемое ими *сходство между на вид совершенно разными явлениями природы* (например, сходство между теориями электрического и магнитного полей, доставляемое уравнениями Максвелла).

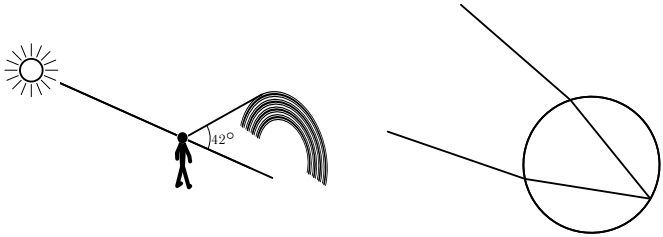

Рис. 1.2. Происхождение радуги

В отличие от описанных выше примеров, поля Галуа пока ещё не нашли физических (или иных естественно-научных) приложений. Я верю, что эти приложения со временем будут найдены, и хотел бы приблизить это время своим геометрическим изложением теории полей Галуа (в духе описания естественно-научных объектов, скорее чем в стиле алгебраически-аксиоматических сверхабстрактных исследований, господствующем в этой алгебраической теории).

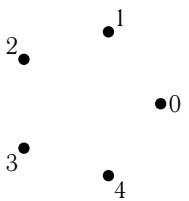

Рис. 1.3. Конечная окружность: поле Галуа $\mathbb{Z}_5$

Простейшим примером поля Галуа является *поле вычетов по модулю простого числа* p (т. е. остатков от деления на p)

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z},$$

рис. 1.3. Например, при $p = 2$ получаем поле двух элементов

$$\mathbb{Z}_2 = \{0, 1\},$$

с обычной арифметикой Митрофанушки:

$$0+0=0, \quad 0+1=1+0=1, \quad 1+1=0,$$
$$0\cdot 0=0\cdot 1=1\cdot 0=0, \quad 1\cdot 1=1.$$

Эта «бинарная» арифметика лежит в основе действующих в двоичной системе компьютеров, так что простейшее поле Галуа имеет массу приложений:

$$(\text{поле } \mathbb{Z}_2) \Rightarrow (\text{компьютеры}).$$

Общее понятие поля совершенно аналогично: две операции (сложения и умножения) удовлетворяют обычным условиям коммутативности, ассоциативности, дистрибутивности, и вдобавок в поле можно делить на любой отличный от 0 элемент.

Остатки от деления на 3 образуют поле $\mathbb{Z}_3$ из трёх элементов (в котором $\frac{1}{2}=2$, так как $2\cdot 2=1$ для остатков от деления на 3).

Напротив, остатки от деления на 4 поля не образуют, так как элемент 2 не имеет обратного (остаток $2x$ принимает значения 0 и 2, но не равен 1 ни при каком остатке x).

Оказывается, всё же существует поле из четырёх элементов (операции в котором отличны от сложения и умножения остатков). Найти операции в этом поле — интересная и полезная (хотя и не трудная) школьная задача.

Конечные поля называются *полями Галуа* потому, что он открыл их следующие 2 замечательные свойства.

1. Число элементов конечного поля — не любое натуральное число, а число вида p^n, где p — простое число (притом любое), а n — натуральное число (тоже любое).

Таким образом, существуют поля из

$$2,\ 3,\ 4,\ 5,\ 7,\ 8,\ 9,\ 11,\ 13,\ 16,\ 17,\ 19,\ 23,\ 25,\ 27$$

элементов, но нет полей с числами элементов

$$6,\ 10,\ 12,\ 14,\ 15,\ 18,\ 20,\ 21,\ 22,\ 24,\ 26.$$

2. Поле из p^n элементов определяется своим числом элементов однозначно (с точностью до изоморфизма).

Например, компьютер, использующий поле $\mathbb{Z}_2$ в Москве, и другой компьютер, работающий в Петербурге, могут использовать разные копии этого поля. Скажем, в Петербурге элементы поля $\mathbb{Z}_2$ можно было бы обозначить буквами α и β, а операции определить таблицей

$$\alpha+\alpha=\beta+\beta=\beta,\quad \alpha+\beta=\beta+\alpha=\alpha,$$
$$\alpha\cdot\alpha=\alpha,\quad \alpha\cdot\beta=\beta\cdot\alpha=\beta\cdot\beta=\beta.$$

Но заданное этой таблицей поле изоморфно обычному московскому полю вычетов (отличаясь от него только обозначениями, $\alpha\sim 1$, $\beta\sim 0$).

§ 2
КАК УСТРОЕНЫ ПОЛЕ ГАЛУА И ЕГО ТАБЛИЦА

Умножение в поле Галуа с n элементами 0 и $\{A^k\}$, $1 \leqslant k \leqslant n-1$, сводится просто к сложению «логарифмов» (показателей k) по модулю $n-1$ (остатков от деления k на $n-1$):

$$0 \cdot A^k = 0, \quad A^k \cdot A^l = A^{k+l}$$

(если $k+l > n-1$, то можно, не меняя остатка при делении на $n-1$, заменить эту сумму на $k+l-(n-1)$), чтобы сделать показатель степени меньшим, чем n).

Остаётся определить операцию сложения. Обозначая элемент A^k поля значком k, мы приходим к следующей «*тропической*» *операции* «$*$» над этими «логарифмами» элементов поля:

$$A^k + A^l = A^{k*l}.$$

[Недавно возникший термин «*тропическая*» (т. е. экзотическая) математика используется всякий раз, когда «уровень» алгебраических операций понижается так, что умножение становится сложением, а сложение переходит в «тропическое сложение» низшего уровня, относительно которого обычное сложение столь же дистрибутивно, как дистрибутивно обычное умножение по отношению к обычному сложению: $x(y+z) = xy + xz$, $x + (y * z) = (x+y) * (x+z)$.

Примером такого тропического сложения является операция «взятие максимума», $x * y = \max(x, y)$ для вещественных чисел.

Эту тропическую операцию можно было бы получить из обычного сложения логарифмированием, соединённым с квантово-механическим «коротковолновым предельным переходом» при стремлении к нулю длины волны h: определение

$$\frac{x *_h y}{h} = \ln(e^{x/h} + e^{y/h})$$

задаёт тропическую операцию $*_h$, которая переходит в $\max(x, y)$ при $h \to 0$.

Хотя всё сказанное очевидно, из него следует нетривиальный «тропический» вывод: заменяя умножения сложениями и сложения максимумами, можно преобразовать многие формулы и теоремы анализа (вроде теории рядов Фурье) в (неочевидные) «тропические» факты теории линейного программирования и выпуклого анализа.]

Рассмотрим для простоты случай поля F из $z = p^2$ элементов. Оно содержит «скалярные» элементы $1, 2 = 1+1, \ldots$ Поскольку поле конечно,

одна из сумм повторится. Значит, некоторая сумма m слагаемых 1 (являющаяся разностью повторившейся суммы и её повторения) есть нуль, $m = 1 + \ldots + 1 = 0$. Пусть m — наименьший нулевой скаляр.

Докажем, что $m = p$. Действительно, объявим любой элемент x эквивалентным любому элементу $x + 1 + \ldots + 1$ (с числом единиц $\leqslant m$). Классы эквивалентности состоят, каждый, из m элементов и попарно не пересекаются, поэтому число скаляров m является делителем числа p^2 элементов поля. Следовательно, m есть либо p, либо p^2.

Второй случай невозможен. Действительно, рассмотрим скалярный элемент $x = 1 + \ldots + 1$ с p слагаемыми. Он не имеет в поле из p^2 элементов обратного элемента, поскольку никакое целое число pq не может дать при делении на p^2 в остатке 1. Значит, $x = 0$, так что число скаляров $m = p$.

Рассмотрим элемент 1 и примитивный элемент A нашего поля. Повторяя каждое из них слагаемым не более p раз, мы получим p^2 сумм $uA + v1$. Все эти суммы — различные элементы нашего поля (иначе мы получили бы в нём $A = -(v/u)1$, поэтому все элементы поля были бы скалярными суммами единиц, что невозможно, так как таких сумм, как мы выше доказали, всего p, а не p^2). Итак, *поле из p^2 элементов состоит в точности из всех линейных комбинаций*

$$F = \{uA + v1\} \quad \text{с коэффициентами} \quad u \in \mathbb{Z}_p,\ v \in \mathbb{Z}_p.$$

В этом смысле мы можем расположить все элементы поля в квадрате размера $p \times p$ (или, лучше, в «конечном торе» $\mathbb{Z}_p^2$, являющемся плоскостью над полем $\mathbb{Z}_p$, рис. 2.1).

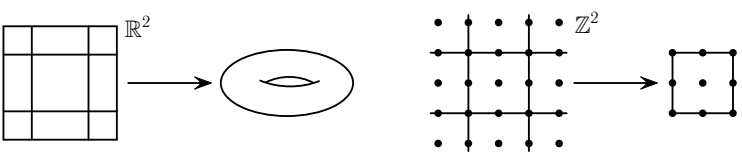

Рис. 2.1. Непрерывный тор и конечный тор из четырех точек

Мы получили, таким образом, заполнение $z = p^2$ клеточек этого конечного тора p^2 символами — «логарифмами» $\{\infty; 1, \ldots, z-1\}$ (где символ k, который можно считать остатком от деления на $z-1$, изображает элемент A^k поля F, а символ ∞ изображает ноль этого поля)[1].

[1] Школьники — слушатели лекции предложили мне считать логарифмом нуля *минус* бесконечность, но я не согласен на это, так как не уверен, что $A > 1$ в F.