Ж.П. Серр

Курс арифметики

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
Ж11

Ж.П. Серр
Ж11 Курс арифметики / Ж.П. Серр – М.: Книга по Требованию, 2021. – 184 с.

ISBN 978-5-458-26867-7

Современный университетский учебник повышенного типа по теории чисел. Сжатое, но весьма содержательное изложение ведётся с позиции современной алгебры; развивается теория конечных полей, теория p-адичесих чисел, локальная теория квадратичных форм, начальные сведения из теории L-рядов с теоремой Дирихле о прогрессии, элементы теории модулярных форм. Автор - выдающийся французский математик; вышедшие в русском переводе его книги: "Алгебраические группы и поля классов", "Когомологии Галуа" ("Мир", 1968), "Алгебры Ли и группы Ли" ("Мир", 1969), "Линейные представления конечных групп" ("Мир", 1970) получили высокую оценку советских учёных. Новый труд Ж.-П. Серра, несомненно, будет пользоваться ещё большей популярностью.

ISBN 978-5-458-26867-7

ПРЕДИСЛОВИЕ РЕДАКТОРА ПЕРЕВОДА

Читателя не должно ввести в заблуждение название книги: это курс основ теории чисел, предполагающий известной теорию делимости и элементы теории сравнений целых рациональных чисел, а также требующий владения некоторыми терминами и результатами общей алгебры. Для успешного изучения книги Серра в основном достаточно общего курса алгебры, читающегося студентам наших университетов и педагогических институтов в первые два года обучения. Правда, система алгебраического образования во Франции несколько отличается от нашей, но недостающие сведения читатель может найти, например, в соответствующих выпусках «Элементов математики» Н. Бурбаки и в книге С. Ленга «Алгебра» (конечно, систематическое изучение этих сочинений не предполагается).

Ж.-П. Серр известен не только как один из крупнейших современных математиков, но и как автор многих содержательных и ясно написанных книг (некоторые из них переведены на русский язык). Предлагаемая книга — одно из наиболее удачных произведений этого выдающегося автора. Она составлена из записей двух курсов лекций, читанных автором для студентов второго года обучения Высшей нормальной школы.

Нет нужды останавливаться на содержании книги, ибо оно подробно описано в предисловии автора. По тематике ее можно сравнить с известной книгой З. И. Боревича и И. Р. Шафаревича «Теория чисел». Однако книга Серра значительно отличается от последней как по отбору материала, так — и особенно —

по манере изложения. В то время как книга Боревича — Шафаревича представляет собой монографию, небольшая книга Серра является современным университетским учебником.

Выход в свет русского перевода книги Серра тем более актуален, что сейчас идет активная перестройка университетского математического образования. Традиционный обязательный курс теории чисел в ряде университетов ликвидирован. Бóльшая часть его материала включена в курс высшей алгебры, где кольцо целых чисел играет роль модели, на которой демонстрируются абстрактные алгебраические понятия и конструкции, однако при этом ряд важных результатов теории чисел естественно оказывается опущенным. Книга Серра заполняет появившийся пробел. Ее можно рассматривать как первый спецкурс, обязательный для всех, кто хочет специализироваться по теории чисел и смежным с нею дисциплинам. Конечно, отбор материала для такого курса, предлагаемый автором, очень интересен, но не единственно возможен. Представляется, что материал первых трех глав (конечные поля, p-адические поля, символ Гильберта) должен войти в той или иной мере в любой курс основ теории чисел. Содержание же остальных глав может быть развито и в самостоятельные более специализированные курсы арифметики квадратичных форм, теории L-рядов, теории модулярных форм.

Нет сомнения, что предлагаемую книгу Серра будут с пользой и интересом читать студенты средних и старших курсов университетов и педагогических институтов, специализирующиеся в области алгебры, теории чисел и смежных областях математики. Она будет полезна преподавателям и научным работникам — и знающие материал книги читатели с удовольствием познакомятся с изложением Серра.

А. Малышев

ПРЕДИСЛОВИЕ

Эта книга делится на две части.

Первая часть — чисто алгебраическая. Ее целью является классификация квадратичных форм над полем рациональных чисел (теорема Минковского — Хассе); этой теме посвящена глава IV. Предыдущие три главы содержат различные предварительные сведения: квадратичный закон взаимности, p-адические поля, символы Гильберта. В главе V предыдущие результаты прилагаются к квадратичным формам с целыми коэффициентами и определителем ± 1; такие формы используются в различных вопросах: модулярные функции, дифференциальная топология, конечные группы.

Вторая часть (главы VI и VII) использует «аналитические» средства (голоморфные функции). В главе VI дается доказательство теоремы Дирихле об арифметической прогрессии; кстати, эта теорема используется в одном узловом пункте первой части (п. 2.2 гл. III). Глава VII посвящена модулярным формам, в частности, тэта-функциям; здесь вновь появляются некоторые квадратичные формы главы V.

Эти две части соответствуют курсу, прочитанному в 1962 и 1964 гг. студентам второго года обучения Высшей нормальной школы. Предварительная редакция курса, размноженного на ротаторе, принадлежит Сансу (главы I—IV) и Рами и Руже (главы VI—VII). Она была существенно использована мною; я приношу благодарность этим авторам.

Часть первая

АЛГЕБРАИЧЕСКИЕ МЕТОДЫ

Глава I

КОНЕЧНЫЕ ПОЛЯ

Всякое поле, рассматриваемое в дальнейшем, предполагается коммутативным.

§ 1. Общие положения

1.1. *Простые поля. Конечные поля*

Пересечение подполей данного поля K является наименьшим его подполем; оно содержит канонический образ кольца $\mathbf{Z}$, изоморфный $\mathbf{Z}$ или $\mathbf{Z}/p\mathbf{Z}$, где p — некоторое простое число. Следовательно, это подполе будет изоморфно или полю рациональных чисел $\mathbf{Q}$, или полю $\mathbf{Z}/p\mathbf{Z}$.

Определение 1. *Поля* $\mathbf{Q}$ *и* $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, *где* p *— простое число, будем называть простыми полями; характеристикой поля* K *называем число* $\operatorname{caract}(K) = 0$ *или* p *в зависимости от того, является* K *расширением поля* $\mathbf{Q}$ *или поля* $\mathbf{F}_p$.

Поэтому если $\operatorname{caract}(K) = p \neq 0$, то p — наименьшее целое число $n > 0$ такое, что $n \cdot 1 = 0$.

Лемма. *Если* $\operatorname{caract}(K) = p$, *то* $\sigma\colon x \longmapsto x^p$ *есть изоморфное отображение* K *на его подполе*[1]) K^p.

[1]) Здесь через K^p автор обозначает совокупность p-х степеней поля K. Аналогичное значение имеют $\mathbf{F}_q^{*2}$ (§ 3) и $\mathbf{Q}_p^{*2}$ (§ 3 гл. II). Обычно же через K^n обозначается прямое произведение n экземпляров множества K (§ 2 этой главы; § 2 гл. II и т. д.). — *Прим. ред.*

Действительно, $\sigma(xy) = \sigma(x)\,\sigma(y)$. Далее, если $1 \leqslant k < p$, то биномиальный коэффициент $\binom{p}{k}$ сравним с $0 \pmod p$; поэтому

$$\sigma(x+y) = \sigma(x) + \sigma(y),$$

так что σ — гомоморфизм. Наконец, очевидно, что σ — инъективное отображение.

Теорема 1. i) *Характеристика конечного поля* K *есть простое число* $p \neq 0$; *если* $f = [K : \mathbf{F}_p]$, *то число элементов* K *равно* p^f.

ii) *Пусть* p — *простое число и* $q = p^f$ — *степень* p ($f \geqslant 1$). *Пусть* Ω — *некоторое алгебраически замкнутое поле характеристики* p. *Тогда существует единственное подполе* $\mathbf{F}_q$ *поля* Ω, *состоящее из* q *элементов*; $\mathbf{F}_q$ *есть множество корней полинома* $X^q - X$.

iii) *Любое конечное поле, состоящее из* $q = p^f$ *элементов, изоморфно полю* $\mathbf{F}_q$.

Так как K — конечное поле, то оно не может содержать поля $\mathbf{Q}$; поэтому его характеристика есть простое число p. Если f — степень расширения $K/\mathbf{F}_p$, то ясно, что $\operatorname{card}(K) = p^f$, что доказывает i).

Далее, если Ω — алгебраически замкнутое поле характеристики p, то по предыдущей лемме отображение $x \mapsto x^q$ (где $q = p^f$, $f \geqslant 1$) является автоморфизмом; действительно, оно является f-й степенью автоморфизма σ: $x \mapsto x^p$ (заметим, что σ сюръективно в силу алгебраической замкнутости Ω). Элементы x поля Ω, инвариантные относительно отображения $x \mapsto x^q$, образуют некоторое подполе $\mathbf{F}_q$ поля Ω. Это x поле состоит из q элементов. Действительно, производная $X^q - X$, равная

$$qX^{q-1} - 1 = p \cdot p^{f-1}X^{q-1} - 1 = -1,$$

не обращается в нуль; поэтому (в силу алгебраической замкнутости Ω) полином $X^q - X$ имеет q различных корней; таким образом, $\operatorname{card}(\mathbf{F}_q) = q$. Обратно, если K есть подполе поля Ω, состоящее из q элементов, то мультипликативная группа K^* ненулевых

элементов поля K состоит из $q-1$ элемента; поэтому $x^{q-1}=1$, если $x \in K^*$; итак, $x^q - x = 0$, если $x \in K$. Отсюда следует, что K содержится в $\mathbf{F}_q$; так как

$$\mathrm{card}\,(K) = \mathrm{card}\,(\mathbf{F}_q),$$

то $K = \mathbf{F}_q$, что заканчивает доказательство ii).

Наконец, утверждение iii) следует из ii), если учесть, что всякое поле из p^f элементов может быть вложено в поле Ω, ибо Ω алгебраически замкнуто.

1.2. *Мультипликативная группа конечного поля*

Пусть p — простое число, f — целое число $\geqslant 1$, $q = p^f$.

Теорема 2. *Мультипликативная группа $\mathbf{F}_q^*$ конечного поля $\mathbf{F}_q$ является циклической группой порядка $q-1$.*

Доказательство. Пусть d — целое число $\geqslant 1$; вспомним обозначение $\varphi(d)$ для *функции Эйлера* — числа целых чисел x, удовлетворяющих условию $1 \leqslant x \leqslant d$ и *взаимно простых с d* (иначе говоря, чисел x, образы которых в факторгруппе $\mathbf{Z}/d\mathbf{Z}$ являются образующими этой группы).

Ясно, что число образующих циклической группы порядка d равно $\varphi(d)$.

Лемма 1. *Если n — целое число $\geqslant 1$, то*

$$n = \sum_{d \mid n} \varphi(d).$$

(Напоминаем, что $d \mid n$ обозначает, что n *делится на* d.)

Если d — делитель числа n, то пусть C_d — единственная подгруппа факторгруппы $\mathbf{Z}/n\mathbf{Z}$, имеющая порядок d; пусть Φ_d — множество образующих группы C_d. Так как каждый элемент группы $\mathbf{Z}/n\mathbf{Z}$ порождает одну из подгрупп C_d, то $\mathbf{Z}/n\mathbf{Z}$ есть объединение непересекающихся множеств Φ_d, так что

$$n = \mathrm{card}\,(\mathbf{Z}/n\mathbf{Z}) = \sum_{d \mid n} \mathrm{card}(\Phi_d) = \sum_{d \mid n} \varphi(d).$$

Лемма 2. *Пусть* H — *группа конечного порядка* n. *Предположим, что для каждого делителя* d *числа* n *множество всех* $x \in H$, *таких, что* $x^d = 1$, *имеет самое большее* d *элементов. Тогда* H — *циклическая группа.*

Пусть d — делитель числа n. Если существует элемент $x \in H$ порядка d, то подгруппа $(x) = \{1, x, \ldots, x^{d-1}\}$, порожденная элементом x, является циклической группой порядка d; поэтому, по предположению, каждый элемент $y \in H$, такой, что $y^d = 1$, принадлежит (x). В частности, элементы группы H порядка d (и только они) являются образующими подгруппы (x), так что их число равно $\varphi(d)$. Итак, число элементов группы H порядка d равно 0 или $\varphi(d)$. Если хотя бы одному из d отвечало значение 0, то из формулы леммы 1 следовало бы, что число элементов H меньше n; а это противоречит предположению. В частности, существует элемент $x \in H$ порядка n, и H совпадает с циклической группой (x).

Теорема 2 следует из леммы 2, если положить $H = \mathbf{F}_q^*$, $n = q - 1$; действительно, очевидно, что уравнение $x^d = 1$, будучи степени d, имеет не более d решений в F_q.

Замечание. Приведенное выше доказательство позволяет доказать и более общее утверждение: всякая конечная подгруппа мультипликативной группы любого поля является циклической.

§ 2. Уравнения над конечным полем

Пусть q — степень простого числа p, и пусть K — поле, состоящее из q элементов.

2.1. *Суммы степеней*

Лемма. *Пусть* u — *целое число* $\geqslant 0$. *Сумма*

$$S(X^u) = \sum_{x \in K} x^u$$

равна -1, *если* $u \geqslant 1$ *и* $(q-1) \mid u$; *в противном случае эта сумма равна* 0.

(Условимся, что если $u=0$, то $x^u=1$ *даже при* $x=0$.)

Если $u=0$, то каждый член этой суммы равен 1, так что $S(X^u)=q\cdot 1=0$, ибо поле K имеет характеристику p.

Если $u\geqslant 1$ и u делится на $q-1$, то $0^u=0$ и $x^u=1$ для $x\neq 0$; поэтому $S(X^u)=(q-1)\cdot 1=-1$.

Наконец, если $u\geqslant 1$ и u не делится на $q-1$, то, поскольку K^* — циклическая группа порядка $q-1$ (теорема 2), найдется $y\in K^*$, такое, что $y^u\neq 1$. Так как

$$S(X^u)=\sum_{x\in K^*}x^u=\sum_{x\in K^*}y^u x^u=y^u S(X^u),$$

то $(1-y^u)\,S(X^u)=0$, откуда следует, что $S(X^u)=0$.

(*Вариант*. Использовать то обстоятельство, что при $d\geqslant 2$ сумма корней d-й степени из единицы равна нулю.)

2.2. *Теорема Шевалле*

Теорема 3 (Шевалле — Варнинг). *Пусть*

$$f_\alpha\in K[X_1,\ \ldots,\ X_n]$$

— полиномы от n переменных, причем $\sum\deg(f_\alpha)<n$, *и пусть* V *— множество их общих нулей на* K^n. *Тогда*

$$\operatorname{card}(V)\equiv 0\pmod p.$$

Положим $P=\prod_\alpha\left(1-f_\alpha^{q-1}\right)$. Пусть $x\in K^n$; если $x\in V$, то все $f_\alpha(x)$ равны нулю и потому $P(x)=1$; если $x\notin V$, то хотя бы один из $f_\alpha(x)$ не равен нулю, так что $f_\alpha^{q-1}(x)=1$, а потому $P(x)=0$. Таким образом, P *— характеристическая функция* множества V. Если для произвольного полинома f

$$S(f)=\sum_{x\in K^n}f(x),$$

то

$$\operatorname{card}(V)\equiv S(P)\pmod p,$$

и остается проверить, что $S(P)=0$.

Действительно, из предположения $\sum \deg(f_\alpha) < n$ вытекает неравенство

$$\deg(P) < n(q-1);$$

поэтому P есть линейная комбинация одночленов

$$X^u = X_1^{u_1} \dots X_n^{u_n},$$

причем $\sum u_i < n(q-1)$. Достаточно доказать, что для такого одночлена X^u имеет место равенство $S(X^u) = 0$. Но это следует из леммы, ибо $u_i < q-1$ хотя бы для одного i. Ч. т. д.

Следствие 1. *Если* $\sum \deg(f_\alpha) < n$ *и полиномы* f_α *не имеют свободных членов, то эти полиномы имеют общий нетривиальный нуль.*

Действительно, если бы V свелось к {0}, то $\mathrm{card}(V) = 1$ и $\mathrm{card}(V)$ не делилось бы на p.

Особенно интересны приложения следствия 1, когда формы f_α *однородны*; в частности

Следствие 2. *Всякая квадратичная форма от трех и более переменных над* K *имеет нетривиальный нуль.*

(На геометрическом языке: всякий конус над конечным полем имеет рациональную точку.)

§ 3. Квадратичный закон взаимности

3.1. *Квадраты поля* $\mathbf{F}_q$

Пусть q — степень простого числа p.

Теорема 4. a) *Если* $p = 2$, *то каждый элемент поля* $\mathbf{F}_q$ *является квадратом.*

b) *Если* $p \neq 2$, *то квадраты группы* $\mathbf{F}_q^*$ *образуют ее подгруппу индекса* 2; *эта подгруппа есть ядро гомоморфизма* $x \longmapsto x^{(q-1)/2}$; *значения* $x^{(q-1)/2}$ *в алгебраическом замыкании* Ω *поля* $\mathbf{F}_q$ *суть* $\{\pm 1\}$.

(В других терминах: последовательность

$$1 \to \mathbf{F}_q^{*2} \to \mathbf{F}_q^* \to \{\pm 1\} \to 1$$

является точной.)