

М. М. ПОСТНИКОВ

ТЕОРИЯ ГАЛУА



ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1963

517.1
Π 63

ОГЛАВЛЕНИЕ

Предисловие	6
I. ОСНОВЫ ТЕОРИИ ГАЛУА	
Г л а в а 1. Элементы теории полей	9
1. Предварительные замечания	9
2. Некоторые важные типы расширений	10
3. Минимальный многочлен. Строение простых алгебраических расширений	13
4. Алгебраичность конечных расширений	15
5. Строение составных алгебраических расширений	16
6. Составные конечные расширения	18
7. Теорема о том, что составное алгебраическое расширение является простым	21
8. Поле алгебраических чисел	23
9. Композит полей	24
Г л а в а 2. Необходимые сведения из теории групп	26
1. Определение группы	26
2. Порядки элементов	28
3. Подгруппы, нормальные делители и факторгруппы	30
4. Гомоморфные отображения	34
Г л а в а 3. Теория Галуа	38
1. Нормальные расширения	38
2. Автоморфизмы полей. Группа Галуа	42
3. Порядок группы Галуа	45
4. Соответствие Галуа	49
5. Теорема о сопряженных элементах	52
6. Группа Галуа нормального под поля	54
7. Группа Галуа композита двух полей	55
II. РЕШЕНИЕ УРАВНЕНИЙ В РАДИКАЛАХ	
Г л а в а 1. Дополнительные сведения из общей теории групп	57
1. Обобщение теоремы о гомоморфизмах	57
2. Нормальные ряды	58
3. Циклические группы	62

4. Разрешимые и абелевы группы	67
5. Группы Z'_n и M_n	70
Г л а в а 2. Уравнения, разрешимые в радикалах	74
1. Простые радикальные расширения	74
2. Циклические расширения	77
3. Радикальные расширения	82
4. Нормальные поля с разрешимой группой Галуа	86
5. Уравнения, разрешимые в радикалах	89
Г л а в а 3. Построение уравнений, неразрешимых в радикалах	91
1. Группа Галуа уравнения как группа подстановок	91
2. Разложение подстановок в произведение циклов	94
3. Четные подстановки. Знакопеременная группа	97
4. Строение знакопеременной и симметрической групп	100
5. Пример уравнения с симметрической группой Галуа	105
6. Обсуждение полученных результатов	109
Г л а в а 4. Неразрешимость в радикалах общего уравнения степени $n \geq 5$	112
1. Поле формальных степенных рядов	112
2. Поле дробностепенных рядов	118
3. Группа Галуа общего уравнения степени n	122
4. Решение уравнений низших степеней	126
III. ДОПОЛНИТЕЛЬНЫЕ ВОПРОСЫ ТЕОРИИ ГАЛУА	
Г л а в а 1. Практическое вычисление групп Галуа уравнений	131
1. Задание групп подстановок степени n многочленами от n неизвестных	131
2. Сопряженные группы подстановок	134
3. Вычисление группы Галуа произвольного многочлена .	136
4. Пример: уравнения, группы Галуа которых содержатся в знакопеременной группе	140
5. Уравнения третьей и четвертой степени	141
Г л а в а 2. Уравнения пятой степени	144
1. Транзитивные группы подстановок	144
2. Транзитивные группы простой степени	145
3. Транзитивные группы пятой степени	146
4. Вычисление группы Галуа неприводимого уравнения пятой степени	149
5. Определяющий многочлен для метациклической группы .	151
6. Случай уравнений в нормальном виде	153
7. Уравнения пятой степени, разрешимые в радикалах . .	155
8. Приведение уравнения пятой степени к нормальному виду	157

Г л а в а 3. Решение уравнений в неприводимых радикалах	160
1. Формулировка основной теоремы	160
2. Сведение основной теоремы к двум частным случаям	161
3. Доказательство теоремы А	163
4. Мультипликативная группа классов по примарному модулю	164
5. Группы Галуа примарных круговых расширений	168
6. Доказательство теоремы В	171
Г л а в а 4. Уравнения деления круга	174
1. Строение полей деления круга простого показателя	174
2. Решение уравнений деления круга	177
3. Прием Гаусса	178
4. Уравнение деления круга на 17 частей	181
Г л а в а 5. Построения циркулем и линейкой	185
1. Основная теорема теории геометрических построений	185
2. Примарные группы	194
3. Пифагоровы расширения	197
4. Некоторые конкретные задачи на построение	199
Задача об удвоении куба (199). Задача о трисекции угла (200). Задача о трех биссектрисах (201). Задача о построении правильного n -угольника. (202). Задача о квадратуре круга (205). Задача о луночках Гиппократа (211).	

ПРЕДИСЛОВИЕ

Эта книга представляет собой переработанный и значительно расширенный вариант книги автора «Основы теории Галуа», выпущенной в свет Физматгизом в 1960 г. При переработке автор стремился сохранить элементарный характер книги, так что от читателя по-прежнему требуется владение лишь основами высшей алгебры в объеме действующей программы первого курса университетов. К сожалению, автор был лишен возможности пополнить книгу упражнениями. Как и в «Основах теории Галуа», задачи, включенные в текст книги, совершенно тривиальны и предназначены исключительно для самоконтроля читателя.

Теория Галуа по-прежнему излагается для полей, принадлежащих некоторому единому «универсальному», алгебраически замкнутому полю характеристики 0 (для определенности — полю комплексных чисел). Это позволяет избежать трудной для начинающего абстрактной теоремы о существовании и единственности (с точностью до изоморфизма) поля разложения данного многочлена. С другой стороны, при таком изложении фактической потери общности не происходит, поскольку любое поле можно, как известно, включить в алгебраически замкнутое.

При первоначальном изучении теории Галуа серьезные трудности часто возникают также в связи с теоремой о продолжении изоморфизма. Поэтому в этой книге теорема о продолжении изоморфизма во всех случаях заменяется, быть может, более кустарными, но зато значительно более доступными соображениями теории симметрических функций.

Теория групп излагается здесь лишь постольку, поскольку это необходимо для теории Галуа и ее применения. Отдельные сведения из теории групп вкраплены в текст в тех местах, где они необходимы. Никакого целостного и более или ме-

нее исчерпывающего изложения даже отдельных глав теории групп в книге не дается. Однако затронутые вопросы теории групп разобраны со всей тщательностью, иногда даже подробнее, чем это обычно принято.

При изложении теории подстановок подробно доказывается теорема о разложении подстановок в произведение независимых циклов, а понятие четности подстановки вводится на основе рассмотрения разложения подстановки в произведение транспозиций. Простота знакопеременной группы доказывается по Редеи.

Задача о решении уравнений в радикалах сначала ставится и решается для произвольных (быть может, приводимых) радикалов. В частности, уравнения деления круга по определению считаются разрешимыми в радикалах. Классическая постановка задачи (о решении уравнений в неприводимых радикалах) рассматривается отдельно и значительно позже. Читатель, желающий познакомиться лишь с основными идеями, на которых основывается применение теории Галуа к задаче о решении уравнений в радикалах, может, таким образом, не вникать в достаточной мере в сложную теорию круговых расширений.

Так как полями коэффициентов общих (т. е. имеющих буквенные коэффициенты) уравнений являются поля рациональных функций, то для обоснования применимости к таким уравнениям результатов теории Галуа, доказанных в книге лишь для подполя универсального поля, нам приходится специально доказывать, что любое поле рациональных функций можно включить в универсальное, т. е. алгебраически замкнутое, поле (именно в поле дробностепенных рядов). Алгебраическую замкнутость поля дробностепенных рядов мы доказываем по Островскому с помощью леммы Гензеля. Это доказательство хотя и не эффективно, но значительно проще конструктивного доказательства, основанного на многоугольнике Ньютона и не раз излагавшегося на русском языке.

В книге большое внимание уделяется задаче практического вычисления групп Галуа уравнений. Эта задача подробно рассмотрена как в общем виде, так и в применении к уравнениям третьей, четвертой и пятой степени. Специальное внимание удалено уравнениям пятой степени. В частности, полностью описаны все уравнения пятой степени, разрешимые в радикалах.

Много места уделено также применением теории Галуа к теории геометрических построений. Хотя основная теорема теории геометрических построений циркулем и линейкой не относится, строго говоря, к теории Галуа, однако мы ее здесь доказываем, обращая особенное внимание на алгебраические тонкости доказательства, обычно оставляемые в тени.

Наряду с общими результатами теории геометрических построений в последней главе книги рассмотрены также и некоторые конкретные построения, и притом не только классические (как задача о трисекции угла и т. п.), но и более свежие (задача о луночках Гиппократа). При рассмотрении задачи о квадратуре круга детально доказана трансцендентность числа π .

Для ссылок на материал первого курса использована книга А. Г. Куроша «Курс высшей алгебры», в дальнейшем именуемая «Курс». При этом страницы указываются по шестому изданию.

В заключение автор хочет горячо поблагодарить С. С. Рышкова и В. Г. Болтянского, прочитавших книгу в рукописи и сделавших много ценных замечаний.

Автор

I. ОСНОВЫ ТЕОРИИ ГАЛУА

ГЛАВА 1 ЭЛЕМЕНТЫ ТЕОРИИ ПОЛЕЙ

1. Предварительные замечания

Полем мы называем непустое множество P комплексных чисел, обладающее следующими свойствами:

- 1) если $a \in P$ и $b \in P$, то $a + b \in P$ и $ab \in P$;
- 2) если $a \in P$, то $-a \in P$ и $a^{-1} \in P$ (при $a \neq 0$).

Полями являются, например, поле рациональных чисел R , поле действительных чисел D и поле комплексных чисел C .

Поле P называется *подполем* поля K , а поле K — *расширением* поля P , если любой элемент поля P принадлежит полю K , т. е. если¹⁾ $P \subset K$. Любое поле (в нашем смысле) является подполем поля комплексных чисел.

Легко видеть, что каждое поле содержит единицу, а следовательно, и все поле рациональных чисел R , т. е. любое поле является расширением поля рациональных чисел. В современной алгебре принято абстрактное определение поля как множества с двумя алгебраическими операциями, удовлетворяющими определенным аксиомам (см. Курс, стр. 276). В отличие от таких «абстрактных» полей, поля в нашем смысле называются *числовыми*. Излагаемую в этой книге теорию можно без большого труда перенести и на случай нечисловых полей. Переход от числовых полей к произвольным влечет в основном лишь чисто технические трудности. Эти трудности связаны с тем, что в нечисловом поле некоторое кратное единицы может оказаться равным нулю, а неприводимый многочлен — обладать кратными корнями.

¹⁾ Обозначение $P \subset K$ не исключает случая, когда P совпадает с K ,

Поля, в которых это затруднение не возникает, называются полями характеристики 0 (см. Курс, стр. 280 и 296). К ним, кроме числовых полей, принадлежат, например, поля рациональных функций. Другая, более существенная трудность, возникающая при переходе от числовых к нечисловым полям, проявляется, в частности, в том, что различные нечисловые поля, вообще говоря, никак не связаны между собой: например, нельзя говорить о сумме элементов двух различных полей. Эту трудность удобнее всего преодолеть, ограничив класс рассматриваемых полей подполями некоторого достаточно широкого «универсального» поля. Именно на этом пути, выбирая за универсальное поле поле комплексных чисел, мы и приходим к числовым полям. В общем случае от универсального поля достаточно потребовать алгебраической замкнутости, т. е. потребовать, чтобы любой многочлен над этим полем разлагался в нем на линейные множители. Легко проверяется, что *вся излагаемая ниже теория остается справедливой без каких-либо изменений, если под полями понимать подполя некоторого алгебраически замкнутого поля характеристики 0.*

Это обстоятельство мы существенно используем в гл. 4, ч. II.

2. Некоторые важные типы расширений

Расширение K поля P называется *конечным*, если в поле K существуют такие элементы $\alpha_1, \dots, \alpha_n$, что любой элемент $\beta \in K$ единственным образом записывается в виде линейной комбинации этих элементов с коэффициентами из поля P :

$$\beta = b_1\alpha_1 + \dots + b_n\alpha_n, \quad b_1, \dots, b_n \in P.$$

Обладающая этим свойством система элементов $\alpha_1, \dots, \alpha_n$ называется *базисом* поля K над полем P .

К понятию конечного расширения можно подойти и с другой стороны, заметив, что любое расширение L поля P можно рассматривать как линейное пространство над полем P . Действительно, элементы поля K можно складывать и умножать на элементы поля P , причем обе операции (сложение и умножение на элементы поля P), очевидно, обладают всеми необходимыми свойствами. С этой точки зрения расширение K тогда и только тогда конечно, когда оно имеет конечную

размерность (как линейное пространство над полем P), а система элементов тогда и только тогда является его базисом (в только что определенном смысле), когда она является его базисом в смысле теории линейных пространств. Так как все базисы конечномерного линейного пространства состоят из одного и того же числа векторов, то, в частности, все базисы поля K над полем P состоят из одного и того же числа элементов. Это число называется *степенью* поля K над полем P и обозначается через $[K : P]$ (с точки зрения теории линейных пространств степень поля K — это его размерность как линейного пространства над полем P).

Задача. Доказать, что степень $[K : P]$ тогда и только тогда равна единице, когда $K = P$.

Пусть P — произвольное поле (числовое) и $\alpha_1, \dots, \alpha_n$ — произвольные числа (т. е. элементы поля C). Рассмотрим всевозможные поля, являющиеся расширениями поля P и содержащие числа $\alpha_1, \dots, \alpha_n$. Такие поля существуют, ибо, например, к их числу принадлежит поле C всех комплексных чисел. Легко видеть, что пересечение всех этих полей также является полем (вообще без труда доказывается, что пересечение любой системы полей само является полем). Это пересечение является, очевидно, минимальным расширением поля P , содержащим числа $\alpha_1, \dots, \alpha_n$ (минимальность означает, что это пересечение является подполем любого другого, содержащего числа $\alpha_1, \dots, \alpha_n$, расширения поля P). Это минимальное расширение обозначается через $P(\alpha_1, \dots, \alpha_n)$ и называется расширением, *порожденным* числами $\alpha_1, \dots, \alpha_n$.

Очевидно, что $P(\alpha_1, \dots, \alpha_n) = P$ тогда и только тогда, когда $\alpha_1, \dots, \alpha_n \in P$.

Задача. Доказать, что поле $P(\alpha_1, \dots, \alpha_n)$ можно определить как совокупность всех чисел, получающихся в результате применения к числам поля P и числам $\alpha_1, \dots, \alpha_n$ всевозможных комбинаций четырех арифметических действий.

Число α называется *алгебраическим над полем P* , если оно является корнем некоторого (не равного тождественно нулю) многочлена с коэффициентами из поля P . Любой элемент поля P , очевидно, алгебраичен над этим полем (если верно и обратное, т. е. если любое алгебраическое над полем P число принадлежит этому полю, то P называется *алгебраически замкнутым* полем; ср. п. 1).

Очевидно, далее, что любое число, алгебраическое над полем P , является алгебраическим числом и над любым расширением поля P . Подчеркнем, что обратное утверждение, вообще говоря, неверно. Например, любое комплексное число является алгебраическим над полем D действительных чисел (ибо оно является корнем квадратного трехчлена с действительными коэффициентами), тогда как существуют числа (даже действительные), не алгебраические над полем R рациональных чисел. В качестве примера неалгебраических над полем R чисел можно указать известные числа e и π , неалгебраичность которых доказывается в полных курсах теории чисел (см. также ниже, ч. III, гл. 4, п. 4).

Расширение K поля P называется *алгебраически порожденным*, если оно порождается некоторой конечной системой алгебраических над полем P чисел, т. е. если существуют такие алгебраические над полем P числа $\alpha_1, \dots, \alpha_s$, что $K = P(\alpha_1, \dots, \alpha_n)$. Если, в частности $s = 1$, то поле $K = P(\alpha_1)$ называется *простым алгебраическим расширением поля P* .

Расширение K поля P называется *составным алгебраическим расширением*, если существует такая цепочка подполяй

$$P = L_0 \subset L_1 \subset \dots \subset L_{s-1} \subset L_s = K,$$

начинающаяся с поля P и кончающаяся полем K , что для любого $i = 1, \dots, s$ поле L_i является простым алгебраическим расширением поля L_{i-1} . Если $L_i = L_{i-1}(\alpha_i)$, $i = 1, \dots, s$, то поле K обозначается через $P(\alpha_1)(\alpha_2) \dots (\alpha_s)$. Подчеркнем, что алгебраичность чисел $\alpha_2, \dots, \alpha_s$ над полем P в этом определении не предполагается.

Наконец, расширение K поля P называется *алгебраическим*, если любой его элемент является числом алгебраическим над полем P .

Таким образом, мы ввели следующие пять типов расширения:

- 1° конечные расширения;
- 2° алгебраически порожденные расширения;
- 3° составные алгебраические расширения;
- 4° простые алгебраические расширения;
- 5° алгебраические расширения.

В этой главе мы изучим соотношения, имеющиеся между этими типами расширений, а также строение расширений каждого из этих типов (кроме, впрочем, последнего).

3. Минимальный многочлен. Строение простых алгебраических расширений

Пусть P — произвольное поле и α — алгебраическое над полем P число. По определению, число α является корнем некоторого отличного от нуля многочлена над полем P (т. е. многочлена с коэффициентами из поля P). Многочлен, имеющий наименьшую степень среди всех многочленов с этим свойством, называется *минимальным многочленом* алгебраического числа α . Этот многочлен неприводим, ибо в противном случае число α было бы корнем хотя бы одного его делителя меньшей степени, что по условию невозможно. Любой многочлен, корнем которого является число α , не взаимно прост с минимальным многочленом и, следовательно, делится на этот многочлен. В частности, неприводимый многочлен с корнем α может отличаться от минимального многочлена лишь постоянным множителем. Другими словами, неприводимый многочлен с корнем α определен однозначно (с точностью до постоянного множителя). Степень n этого многочлена называется *степенью алгебраического числа α над полем P* . Степень n равна единице тогда и только тогда, когда $\alpha \in P$.

Пусть α — алгебраическое над полем P число, $f(x)$ — его минимальный многочлен и n — его степень. Рассмотрим множество K всех чисел β , для каждого из которых существует такой многочлен $g(x)$ над полем P , что $\beta = g(\alpha)$. Очевидно, что

$$K \subset P(\alpha).$$

Докажем, что K является полем. Так как сумма, разность и произведение любых элементов из K , очевидно, снова принадлежат K , то нужно только доказать, что для любого отличного от нуля числа $\beta \in K$ число β^{-1} также принадлежит K .

По определению

$$\beta = g(\alpha),$$

где $g(x)$ — некоторый многочлен над полем P . Поскольку $g(\alpha) \neq 0$, то многочлен $g(x)$ не делится на многочлен $f(x)$ и, следовательно (в силу неприводимости многочлена $f(x)$), многочлены $g(x)$ и $f(x)$ взаимно просты. Поэтому, согласно известной теореме (см. Курс, стр. 141), над полем P существуют такие многочлены $u(x)$ и $v(x)$, что

$$f(x)u(x) + g(x)v(x) = 1.$$

Полагая в этом равенстве $x = \alpha$, мы получим

$$\beta v(\alpha) = 1,$$

т. е. $\beta^{-1} = v(\alpha)$, так что $\beta^{-1} \in K$.

Таким образом, множество K действительно является полем. Так как, по определению, $P \subset K$ и $\alpha \in K$, то K является расширением поля P , содержащим число α . Поэтому в силу минимальности поля $P(\alpha)$

$$P(\alpha) \subset K.$$

Сопоставляя это включение с включением $K \subset P(\alpha)$, мы получаем, что

$$K = P(\alpha).$$

Тем самым мы доказали, что

для любого элемента β поля $P(\alpha)$ найдется такой многочлен $g(x)$ над полем P , что $\beta = g(\alpha)$.

Этот многочлен определен неоднозначно, ибо к нему можно прибавить любой многочлен, делящийся на многочлен $f(x)$. Другими словами, если разность $g(x) - g_1(x)$ делится на многочлен $f(x)$, то $g(\alpha) = g_1(\alpha)$. Обратно, если $g(\alpha) = g_1(\alpha)$, то многочлены $g(x) - g_1(x)$ и $f(x)$ не взаимно просты (ибо они имеют общий корень α) и, следовательно, многочлен $g(x) - g_1(x)$ делится на многочлен $f(x)$. Таким образом,

$$g(\alpha) = g_1(\alpha)$$

тогда и только тогда, когда разность $g(x) - g_1(x)$ делится на многочлен $f(x)$.

В частности, если $r(x)$ — остаток от деления многочлена $g(x)$ на многочлен $f(x)$, то $g(\alpha) = r(\alpha)$. Следовательно, любой элемент поля $P(\alpha)$ можно представить в виде $r(\alpha)$, где степень многочлена $r(x)$ меньше n (т. е. меньше степени многочлена $f(x)$). Другими словами, для любого

элемента $\beta \in P(\alpha)$ существуют такие элементы $b_0, b_1, \dots, b_{n-1} \in P$ (коэффициенты многочлена $r(x)$), что

$$\beta = b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1}. \quad (1)$$

Так как разность $r(x) - r_1(x)$, где $r(x)$ и $r_1(x)$ — многочлены степени, меньшей n , делится на многочлен $f(x)$ степени n только тогда, когда $r(x) = r_1(x)$, то это представление однозначно. Таким образом, любой элемент β поля $P(\alpha)$ однозначно записывается в виде (1). Другими словами,

элементы

$$1, \alpha, \dots, \alpha^{n-1}$$

образуют базис поля $P(\alpha)$ над полем P .

Следовательно,

простое алгебраическое расширение $P(\alpha)$ является конечным расширением и его степень $[P(\alpha) : P]$ равна степени числа α .

Таким образом, класс расширений типа 4° содержится в классе расширений типа 1° .

4. Алгебраичность конечных расширений

Пусть β — произвольный элемент конечного расширения K поля P , и пусть $[K : P] = n$. Так как в n -мерном линейном пространстве любые $n+1$ векторов линейно зависимы, то, в частности, элементы

$$1, \beta, \dots, \beta^n$$

линейно зависимы над полем P , т. е. в P существуют такие числа c_0, c_1, \dots, c_n , среди которых хотя бы одно не равно нулю, что

$$c_0 + c_1\beta + \dots + c_n\beta^n = 0.$$

Это означает, что число β служит корнем многочлена

$$c_0 + c_1x + \dots + c_nx^n$$

и, следовательно, является алгебраическим (над полем P) числом. Тем самым доказано, что

любое конечное расширение алгебраично,

т. е. класс расширений типа 1° содержится в классе расширений типа 5° .

Кроме того, мы получаем, что степень над полем P любого элемента конечного расширения K поля P не превосходит степени n этого расширения.

Пусть теперь $\alpha_1, \dots, \alpha_n$ — базис поля K над полем P . Так как числа $\alpha_1, \dots, \alpha_n$ являются, по доказанному, алгебраическими числами (над P), то порожденное ими расширение $P(\alpha_1, \dots, \alpha_n)$ является алгебраически порожденным расширением. В силу минимальности этого расширения оно содержится в поле K :

$$P(\alpha_1, \dots, \alpha_n) \subset K.$$

С другой стороны, так как из $\alpha_1, \dots, \alpha_n \in P(\alpha_1, \dots, \alpha_n)$ следует, что $b_1\alpha_1 + \dots + b_n\alpha_n \in P(\alpha_1, \dots, \alpha_n)$ для любых чисел $b_1, \dots, b_n \in P$, то любой элемент поля K содержится в поле $P(\alpha_1, \dots, \alpha_n)$, т. е.

$$K \subset P(\alpha_1, \dots, \alpha_n).$$

Следовательно,

$$K = P(\alpha_1, \dots, \alpha_n).$$

Таким образом,

любое конечное расширение является алгебраически порожденным.

Другими словами, класс расширений типа 1° содержится в классе расширений типа 2°.

5. Строение составных алгебраических расширений

Пусть $K = P(\alpha_1) \dots (\alpha_s)$ — составное алгебраическое расширение поля P . Оказывается, что любой элемент поля K выражается в виде многочлена (над P) от $\alpha_1, \alpha_2, \dots, \alpha_s$, т. е. для любого элемента $\beta \in K$ существует над полем P такой многочлен $g(x_1, \dots, x_s)$ от s неизвестных x_1, \dots, x_s , что

$$\beta = g(\alpha_1, \dots, \alpha_s).$$

Мы докажем это утверждение индукцией по s . Если $s = 1$, то $K = P(\alpha_1)$, и, следовательно, в этом случае теорема справедлива (см. п. 3). Предполагая теперь, что теорема уже доказана для поля $L = P(\alpha_1) \dots (\alpha_{s-1})$, рассмотрим произвольный элемент $\beta \in K$. Так как $K = L(\alpha_s)$, то

над полем L существует такой многочлен $h(x)$, что $\beta = h(\alpha_s)$.
Пусть

$$h(x) = \gamma_0 + \gamma_1 x + \dots + \gamma_n x^n, \text{ где } \gamma_0, \gamma_1, \dots, \gamma_n \in L.$$

По предположению индукции для любого $i = 0, 1, \dots, n$ найдется такой многочлен $h_i(x_1, \dots, x_{s-1})$ от $s-1$ неизвестных, что

$$\gamma_i = h_i(\alpha_1, \dots, \alpha_{s-1}).$$

Следовательно, полагая

$$g(x_1, \dots, x_s) = h_0(x_1, \dots, x_{s-1}) + \\ + h_1(x_1, \dots, x_{s-1}) x_s + \dots + h_n(x_1, \dots, x_{s-1}) x_s^n.$$

мы получим, что

$$\beta = g(\alpha_1, \dots, \alpha_s).$$

Тем самым наше утверждение полностью доказано.

Рассмотрим теперь произвольное алгебраически порожденное расширение $P(\alpha_1, \dots, \alpha_s)$ поля P и определим по индукции поле L_0, L_1, \dots, L_s , полагая

$$L_0 = P, \quad L_1 = L_0(\alpha_1), \dots, \quad L_l = L_{l-1}(\alpha_l), \dots, \quad L_s = L_{s-1}(\alpha_s).$$

Так как для любого $l = 1, \dots, s$ число α_l , алгебраическое над полем P , алгебраично и над его расширением L_{l-1} , то поле L_l является простым алгебраическим расширением поля L_{l-1} и, следовательно, поле L_s — составным алгебраическим расширением $P(\alpha_1) \dots (\alpha_s)$ поля P . Поэтому, согласно только что доказанному утверждению, любой элемент поля L_s выражается в виде многочлена (над P) от $\alpha_1, \dots, \alpha_s$ и, следовательно, принадлежит полю $P(\alpha_1, \dots, \alpha_s)$. Иначе говоря,

$$L_s \subset P(\alpha_1, \dots, \alpha_s).$$

С другой стороны, поле L_s содержит все числа $\alpha_1, \dots, \alpha_s$ и, в силу минимальности расширения $P(\alpha_1, \dots, \alpha_s)$,

$$P(\alpha_1, \dots, \alpha_s) \subset L_s.$$

Следовательно,

$$P(\alpha_1, \dots, \alpha_s) = P(\alpha_1) \dots (\alpha_s),$$

ибо $L_s = P(\alpha_1) \dots (\alpha_s)$.

Таким образом,

любое алгебраически порожденное расширение является составным алгебраическим расширением.

Другими словами, класс расширений типа 2° содержится в классе расширений типа 3° .

В частности, тем самым доказано, что

любой элемент алгебраически порожденного расширения $P(\alpha_1, \dots, \alpha_n)$ выражается в виде многочлена над полем P от элементов $\alpha_1, \dots, \alpha_s$.

6. Составные конечные расширения

Пусть L — конечное расширение поля P , K — конечное расширение поля L ,

$$P \subset L \subset K,$$

$\alpha_1, \dots, \alpha_m$ — базис поля L над полем P и β_1, \dots, β_n — базис поля K над полем L . Таким образом,

$$m = [L : P], \quad n = [K : L].$$

Оказывается, что

т_m элементов $\alpha_i\beta_j$, $i = 1, \dots, m$, $j = 1, \dots, n$, образуют базис поля K над полем P .

Другими словами, любой элемент поля K является линейной комбинацией элементов $\alpha_i\beta_j$ с коэффициентами из поля P и элементы $\alpha_i\beta_j$ линейно независимы над полем P .

Действительно, любой элемент β поля K является, по определению, линейной комбинацией элементов β_1, \dots, β_n с коэффициентами из поля L :

$$\beta = \gamma_1\beta_1 + \dots + \gamma_n\beta_n, \quad \text{где } \gamma_1, \dots, \gamma_n \in L,$$

то есть

$$\beta = \sum_{j=1}^n \gamma_j \beta_j. \quad (1)$$

С другой стороны, для каждого $j = 1, \dots, n$ элемент γ_j является линейной комбинацией элементов $\alpha_1, \dots, \alpha_m$ с коэффициентами из поля P :

$$\gamma_j = c_{1j}\alpha_1 + \dots + c_{mj}\alpha_m, \quad \text{где } c_{1j}, \dots, c_{mj} \in P,$$

то есть

$$\gamma_j = \sum_{i=1}^m c_{ij}\alpha_i.$$

Подставляя эти выражения в формулу (1), мы получим, что

$$\beta = \sum_{j=1}^n \sum_{l=1}^m c_{lj} \alpha_l \beta_j.$$

Таким образом, любой элемент поля K является линейной комбинацией элементов вида $\alpha_l \beta_j$, с коэффициентами из поля P .

Предположим теперь, что в поле P существуют такие элементы k_{lj} , что

$$\sum_{j=1}^n \sum_{l=1}^m k_{lj} \alpha_l \beta_j = 0.$$

Для любого $j = 1, \dots, n$ положим

$$\gamma_j = \sum_{l=1}^m k_{lj} \alpha_l.$$

Элементы $\gamma_1, \dots, \gamma_n$ принадлежат полю L и удовлетворяют соотношению

$$\gamma_1 \beta_1 + \dots + \gamma_n \beta_n = 0.$$

Так как элементы β_1, \dots, β_n образуют базис поля K над полем L , то из этого соотношения вытекает, что

$$\gamma_1 = \dots = \gamma_n = 0.$$

Таким образом, для любого $j = 1, \dots, n$

$$\sum_{l=1}^m k_{lj} \alpha_l = 0.$$

Следовательно, поскольку элементы $\alpha_1, \dots, \alpha_m$ образуют базис поля L над полем P , то $k_{lj} = 0$ для всех l и j . Тем самым доказано, что система элементов $\alpha_l \beta_j$ линейно независима.

Из доказанного утверждения вытекает, что поле K является конечным расширением поля P и его степень равна mn , т. е.

$$[K : P] = [K : L][L : P].$$

Эту формулу легко обобщить:

если

$$P = L_0 \subset L_1 \subset \dots \subset L_{t-1} \subset L_t \subset \dots \subset L_s = K,$$

причем для любого $t = 1, \dots, s$ поле L_t является конечным расширением поля L_{t-1} , то поле K будет конечным

расширением поля P и

$$[K : P] = [K : L_{s-1}] \dots [L_s : L_{s-1}] \dots [L_1 : P].$$

Для доказательства достаточно применить индукцию по s .

Эта теорема применима, в частности, к любому составному алгебраическому расширению, ибо, как мы знаем, любое простое алгебраическое расширение является конечным расширением. Таким образом, мы получаем, что

любое составное алгебраическое расширение является конечным расширением.

Другими словами, класс расширений типа 3° содержится в классе расширений типа 1° .

Так как все элементы конечного расширения поля P алгебраичны над полем P , то, в частности, для любого составного алгебраического расширения $P(\alpha_1)(\alpha_2) \dots (\alpha_s)$ элементы $\alpha_1, \alpha_2, \dots, \alpha_s$ алгебраичны над P . Поэтому расширение $P(\alpha_1, \dots, \alpha_s)$ является алгебраически порожденным расширением. Таким образом,

любое составное алгебраическое расширение является алгебраически порожденным расширением.

Другими словами, класс расширений типа 3° содержится в классе расширений типа 2° .

Сопоставляя это замечание с результатами предыдущего пункта, мы видим, что класс составных алгебраических расширений совпадает с классом алгебраически порожденных расширений. При этом, если $K = P(\alpha_1, \dots, \alpha_s)$, то $K = P(\alpha_1) \dots (\alpha_s)$, и наоборот.

Далее, как было доказано в п. 4, класс конечных (т. е. типа 1°) расширений содержится в классе расширений типа 3° , т. е., по доказанному, и в классе расширений типа 2° . Следовательно, класс конечных расширений совпадает с классом составных алгебраических расширений.

Сопоставляя обе эти теоремы, получаем, что

следующие три утверждения равносильны:

- поле K является конечным расширением поля P ;*
- поле K является составным алгебраическим расширением поля P ;*
- поле K является алгебраически порожденным расширением поля P .*

Таким образом, все три термина «конечное», «составное алгебраическое» и «алгебраически порожденное» означают (в применении к расширениям) одно и то же.

Закончим этот пункт некоторыми замечаниями, касающимися подполей конечных расширений.

Пусть K — произвольное конечное расширение поля P , и пусть L — его подполе, содержащее поле P :

$$P \subset L \subset K.$$

Очевидно, что L конечно над P (ибо не может содержать бесконечной линейно независимой над полем P системы элементов), а K конечно над L (ибо любая линейная комбинация над P автоматически является линейной комбинацией над L). Следовательно, мы находимся в условиях применимости доказанной в начале этого пункта теоремы. Поэтому

$$[K:P] = [K:L][L:P].$$

Таким образом,

любое подполе L (содержащее поле P) конечного расширения K поля P является конечным расширением, а его степень $[L:P]$ — делителем степени $[K:P]$ поля K . Соответствующее частное $\frac{[K:P]}{[L:P]}$ равно степени $[K:L]$ поля K над полем L .

Так как простое алгебраическое расширение $P(\alpha)$, порожденное некоторым элементом α конечного расширения K , лежит в K , а его степень равна степени числа α , то

степень (над P) любого элемента конечного расширения K поля P делит степень $[K:P]$ поля K над полем P .

Это — уточнение доказанного в п. 4 неравенства.

Задача. Доказать, что конечное расширение степени n тогда и только тогда является простым алгебраическим расширением, когда в нем существует элемент, имеющий степень n .

7. Теорема о том, что составное алгебраическое расширение является простым

В этом пункте мы докажем следующую теорему.

Любое составное алгебраическое расширение $K = P(\alpha_1) = (\alpha_2) \dots (\alpha_s)$ является простым, т. е. существует такое число θ , что

$$K = P(\theta).$$

Рассмотрим сначала случай $s = 2$, когда $K = P(\alpha_1)(\alpha_2)$. Пусть $f_1(x)$ и $f_2(x)$ — минимальные многочлены (над P) чисел α_1 и α_2 соответственно (как мы знаем, эти числа алгебраичны над P) и пусть

$$\beta_1 = \alpha_1, \beta_2, \dots, \beta_n \quad (1)$$

— корни многочлена $f_1(x)$ и

$$\gamma_1 = \alpha_2, \gamma_2, \dots, \gamma_m \quad (2)$$

— корни многочлена $f_2(x)$. Так как многочлены $f_1(x)$ и $f_2(x)$ неприводимы, то среди корней (1), так же как и среди корней (2), нет одинаковых.

Рассмотрим элементы

$$\frac{\beta_l - \beta_1}{\gamma_1 - \gamma_j}, \quad (3)$$

где $l = 1, 2, \dots, n$, а $j = 2, \dots, m$ (таким образом, $j \neq 1$). Число этих элементов равно $n(m-1)$ и, следовательно, конечно. Поэтому в поле P (даже в поле R рациональных чисел) можно найти число c , не равное ни одному из чисел (3). Положим

$$\theta = \alpha_1 + c\alpha_2 \quad (\text{т. е. } \theta = \beta_1 + c\gamma_1).$$

Так как число c не равно ни одному из чисел (3), то

$$\theta \neq \beta_l + c\gamma_j, \quad (4)$$

ни для каких $l = 1, 2, \dots, n$ и $j = 2, \dots, m$.

Число θ принадлежит полю K и, следовательно, алгебраично. Порожденное им простое алгебраическое расширение $P(\theta)$ содержится в K :

$$P(\theta) \subset K. \quad (5)$$

Рассмотрим многочлен

$$g_1(x) = f_1(\theta - cx).$$

Это — многочлен над полем $P(\theta)$, имеющий общий корень α_2 с многочленом $f_2(x)$ (который также можно считать многочленом над полем $P(\theta)$). Из соотношения (4) вытекает, что никаких других общих корней многочлены $g_1(x)$ и $f_2(x)$ не имеют (ибо если $g_1(\gamma_j) = 0$, то число $\theta - c\gamma_j$ будет корнем многочлена $f_1(x)$, т. е. $\theta - c\gamma_j = \beta_l$ для некоторого l , что по построению возможно только для $l, j = 1$). Следова-

тельно, наибольшим общим делителем этих многочленов является двучлен $x - \alpha_2$. Но, как известно (см. Курс, стр. 289), наибольший общий делитель двух многочленов над некоторым полем (в нашем случае над полем $P(\theta)$) также является многочленом над этим же полем. Поэтому

$$\alpha_2 \in P(\theta)$$

и, следовательно,

$$\alpha_1 = \theta - c\alpha_2 \in P(\theta).$$

В силу минимальности расширения $P(\alpha_1, \alpha_2)$ отсюда вытекает, что

$$P(\alpha_1, \alpha_2) \subset P(\theta).$$

Сопоставляя это включение с включением (5) и учитывая, что $P(\alpha_1, \alpha_2) = P(\alpha_1)(\alpha_2)$, мы получим

$$P(\alpha_1)(\alpha_2) = P(\theta).$$

Таким образом, для $s = 2$ теорема доказана.

Случай любого s сводится к случаю $s = 2$ тривиальным применением метода полной индукции.

Доказанная теорема означает, что к приведенному в предыдущем пункте перечню равносильных свойств расширений мы можем добавить следующее свойство:

г) поле K является простым алгебраическим расширением поля P .

Другими словами,

конечные (т. е. составные алгебраические, т. е. алгебраически порожденные) расширения исчерпываются простыми алгебраическими расширениями.

8. Поле алгебраических чисел

В предыдущих пунктах доказано, что классы расширений типов 1° , 2° , 3° и 4° совпадают. Остается выяснить связи этих расширений с расширениями типа 5° (т. е. с алгебраическими расширениями). Как показано в п. 4, любое конечное расширение алгебраично. Мы сейчас покажем, что обратное неверно, т. е. что класс алгебраических расширений, вообще говоря, существенно шире класса конечных расширений. В дальнейшем этот результат не используется;

он излагается нами лишь для выяснения полной системы соотношений между введенными классами расширений.

Пусть P — произвольное поле. Рассмотрим множество K всех алгебраических над полем P чисел. Пусть $\alpha \in K$ и $\beta \in K$. Тогда расширение $P(\alpha, \beta)$ является алгебраически порожденным и, следовательно, конечным расширением. Поэтому все его элементы, и значит, в частности элементы $\alpha + \beta$, $\alpha\beta$, $-\alpha$ и α^{-1} (если $\alpha \neq 0$), алгебраичны над P , т. е. принадлежат K . Следовательно, множество K является полем. По определению, оно является алгебраическим расширением поля P .

Предположим, что над полем P существуют неприводимые многочлены сколь угодно большой степени (этому условию удовлетворяет, в частности, поле R рациональных чисел; см. Курс, стр. 354). Тогда поле K будет содержать элементы сколь угодно большой степени, и поэтому его степень не может быть конечной, т. е. поле K будет бесконечным расширением.

Таким образом, действительно существуют алгебраические бесконечные расширения (по крайней мере, над полем рациональных чисел).

Задача. Доказать, что поле K всех алгебраических чисел над полем P алгебраически замкнуто.

9. Композит полей

Пусть K_1 и K_2 — произвольные поля. Их *композитом* K называется минимальное поле, содержащее как поле K_1 , так и поле K_2 . Существование поля K следует из того, что его можно определить как пересечение всех полей, содержащих оба поля K_1 и K_2 . Примером композита является расширение $P(\alpha_1, \alpha_2)$, порожденное числами α_1 и α_2 . Это расширение будет композитом расширений $P(\alpha_1)$ и $P(\alpha_2)$.

Простой и пригодный во всех интересных случаях способ построения композита описывается следующей теоремой.

Если поля K_1 и K_2 являются расширениями некоторого поля P , причем существуют такие числа $\theta_1, \dots, \theta_s$, что

$$K_2 = P(\theta_1, \dots, \theta_s),$$

то

$$K = K_1(\theta_1, \dots, \theta_s).$$

Действительно, так как $P \subset K_1$, то поле $K_1(\theta_1, \dots, \theta_s)$ содержит поле $K_2 = P(\theta_1, \dots, \theta_s)$ (и, кроме того, очевидно, поле K_1). Поэтому в силу минимальности композита

$$K \subset K_1(\theta_1, \dots, \theta_s).$$

С другой стороны,

$$K_1(\theta_1, \dots, \theta_s) \subset K,$$

ибо

$$K_1 \subset K \text{ и } \theta_1, \dots, \theta_s \in K.$$

Применим эту теорему к случаю, когда числа $\theta_1, \dots, \theta_s$ алгебраичны над P , т. е. к случаю, когда поле K_2 является алгебраически порожденным (т. е. конечным) расширением поля P .

Алгебраические над полем P числа $\theta_1, \dots, \theta_s$ алгебраичны и над полем K_1 . Поэтому любой элемент поля $K = K_1(\theta_1, \dots, \theta_s)$ выражается в виде многочлена от $\theta_1, \dots, \theta_s$, с коэффициентами из поля K_1 (см. п. 5). Отсюда вытекает, что любой элемент поля K можно представить в виде

$$\alpha_1\beta_1 + \dots + \alpha_r\beta_r, \quad (1)$$

где $\alpha_r, \dots, \alpha_s \in K_1$, $\beta_1, \dots, \beta_r \in K_2$ (именно, β_1, \dots, β_s суть некоторые одночлены от $\theta_1, \dots, \theta_s$). Таким образом,

если хотя бы одно из расширений K_1 , K_2 поля P конечно, то любой элемент их композита K имеет вид (1).

Задача. Доказать, что композит конечных расширений является конечным расширением.

ГЛАВА 2

НЕОБХОДИМЫЕ СВЕДЕНИЯ ИЗ ТЕОРИИ ГРУПП

1. Определение группы

Говорят, что в непустом множестве G определена *алгебраическая операция*, если задано правило, по которому любым двум элементам $a \in G$, $b \in G$ ставится в соответствие некоторый однозначно определенный элемент $c \in G$. Элемент c обычно обозначается через ab , в связи с чем рассматриваемая алгебраическая операция называется *умножением*. Иногда элемент c обозначается через $a + b$, и тогда алгебраическая операція называется *сложением*. Мы, как правило, будем пользоваться первой, *мультипликативной* записью.

Множество G с алгебраической операцией называется группой, если

1) для любых элементов a , b , $c \in G$

$$(ab)c = a(bc);$$

2) существует такой элемент $e \in G$, что

$$ae = ea = a$$

для любого элемента $a \in G$;

3) для любого элемента $a \in G$ существует такой элемент $a^{-1} \in G$, что

$$aa^{-1} = a^{-1}a = e.$$

Условие 1) (закон ассоциативности) позволяет однозначным образом определить произведение любого конечного числа элементов группы, т. е. позволяет доказать независимость произведения любых n элементов от первоначального распределения скобок. Детальное доказательство см. Курс, стр. 272.

В частности, можно говорить о произведении n равных между собой элементов, т. е. ввести понятие о степени a^n элемента a с целым положительным показателем.

Элемент e , предусмотренный условием 2), называется единицей группы и иногда обозначается через 1. Легко видеть, что единица группы определена однозначно, т. е. если элементы e и e' группы G обладают свойством 2), то $e = e'$. Действительно, так как e обладает свойством 2), то $e'e = e'$. Аналогично, $e'e = e$. Следовательно, $e' = e$.

Элемент a^{-1} , предусмотренный условием 3), называется обратным к элементу a . Легко видеть, что для любого элемента a обратный элемент a^{-1} определен однозначно, т. е. если $ab = e$, то $b = a^{-1}$ (действительно, $b = eb = a^{-1}ab = a^{-1}e = a^{-1}$). Кроме того, для любого элемента $a \in G$ и любого целого положительного n

$$(a^n)^{-1} = (a^{-1})^n.$$

(ибо $(a^n)(a^{-1})^n = aa \dots aa^{-1} \dots a^{-1}a^{-1} = e$).

Мы вводим степени элемента a с целыми отрицательными коэффициентами, полагая

$$a^{-n} = (a^n)^{-1} \quad (\text{т. е. } a^{-n} = (a^{-1})^n).$$

Кроме того, полагаем

$$a^0 = e.$$

Легко проверяется, что все обычные правила действий со степенями одного элемента остаются справедливыми в любой группе.

Подчеркнем, что справедливость в группе закона коммутативности ($ab = ba$), вообще говоря, не предполагается. Группы, в которых операция удовлетворяет этому закону, называются коммутативными или абелевыми.

В абелевых группах правила действий над степенями сохраняются и для степеней нескольких элементов. В частности, для любых двух элементов a и b абелевой группы и любого целого n имеет место равенство

$$(ab)^n = a^n b^n.$$

Если операция, заданная в группе, обозначена знаком $+$, т. е. если группа задана в аддитивной записи, то элемент e называется нулем и обозначается обычно символом 0.

Аналогично элемент a^{-1} обозначается в этом случае через — a и называется *противоположным* элементом, а элемент a^n обозначается через na и называется *n-кратным* элементу a . Как правило, аддитивная запись группы используется лишь для абелевых групп.

2. Порядки элементов

Пусть g — произвольный элемент группы G . Рассмотрим всевозможные его степени

$$\dots g^{-2}, g^{-1}, g^0 = e, g^1 = g, g^2, \dots$$

Если все эти степени различны, то элемент g называется элементом *бесконечного порядка*; в противном случае он называется элементом *конечного порядка*.

Пусть g — элемент конечного порядка, т. е. пусть $g^{n_1} = g^{n_2}$ для двух различных целых чисел n_1 и n_2 . Без ограничения общности можно считать, что $n_1 > n_2$, т. е. число $N = n_1 - n_2$ положительно. Так как $g^N = g^{n_1} (g^{n_2})^{-1}$, то $g^N = e$. Таким образом, для любого элемента конечного порядка существуют такие положительные целые числа N , что $g^N = e$. Наименьшее из этих чисел называется *порядком* элемента g .

Заметим, что порядок 1 имеет только единица e группы G .

Пусть n — порядок элемента g , и пусть a — произвольное (не обязательно положительное) целое число. Оказывается, что

порядок элемента g^a равен $n_1 = n/d$, где d — наибольший (положительный) общий делитель чисел n и a .

Действительно, во-первых,

$$(g^a)^{n_1} = (g^n)^{a_1} = e,$$

где $a_1 = a/d$. Во-вторых, если $(g^a)^m = e$, где $m > 0$, то, разделив (с остатком) число am на n , т. е. найдя такие числа q и r , что

$$am = nq + r \text{ и } 0 \leq r < n$$

(легко видеть, что обладающие этими свойствами числа q и r существуют и тогда, когда число am отрицательно), мы

получим, что

$$g^r = g^{am-nq} = \frac{g^{am}}{g^{nq}} = e.$$

Отсюда, ввиду минимальности числа n , вытекает, что $r=0$ и, значит, $am=nq$. Сокращая это равенство на d , мы получим, что

$$a_1m = n_1q.$$

Так как числа a_1 и n_1 взаимно просты, из этого равенства следует (докажите!), что m делится на n_1 , и потому не меньше чем n_1 . Таким образом, n_1 является наименьшим положительным числом среди всех чисел m , для которых $(g^a)^m = e$, т. е. является порядком элемента g^a .

Из доказанного утверждения немедленно вытекает, что

1) если число a делит порядок p элемента g , то порядок элемента g^a равен p/a ;

2) если числа a и p взаимно просты, то порядок элемента g^a равен p ;

3) порядок элемента g^{-1} равен порядку элемента g ;

4) если $g^a = e$, то число a делится на p .

Докажем, например, следствие 4). Равенство $g^a = e$ означает, что порядок элемента g^a равен единице. Поэтому по доказанной теореме число d равно p , т. е. a делится на p .

Задача. Докажите утверждения 1) — 4) непосредственно, т. е. не используя доказанную выше общую теорему.

Если элемент g_1 группы G имеет порядок n_1 , а элемент g_2 — порядок n_2 , то о порядке элемента g_1g_2 в общем случае ничего сказать нельзя (элемент g_1g_2 может даже оказаться элементом бесконечного порядка). Однако,

если группа G абелева, а порядки n_1 и n_2 элементов g_1 и g_2 взаимно просты, то порядок элемента g_1g_2 равен n_1n_2 .

Действительно, во-первых,

$$(g_1g_2)^{n_1n_2} = g_1^{n_1n_2} g_2^{n_1n_2} = e,$$

а во-вторых, если $(g_1g_2)^m = e$, где $m > 0$, то

$$g_1^{mn_2} = g_1^{mn_2} g_2^{mn_2} = (g_1g_2)^{mn_2} = e,$$

и потому mn_2 делится на n_1 . Следовательно, m делится на n_1 (докажите!). Аналогично доказывается, что m делится

на n_2 . Следовательно, m делится и на n_1n_2 . Таким образом, число n_1n_2 действительно является порядком элемента g_1g_2 .

Очевидно, что аналогичное утверждение справедливо и для произведения любого числа элементов (взаимно простых порядков).

3. Подгруппы, нормальные делители и факторгруппы

Непустое подмножество H группы G называется *подгруппой*, если

1) произведение h_1h_2 любых элементов $h_1 \in H$, $h_2 \in H$ принадлежит H ;

2) для любого элемента $h \in H$ обратный элемент h^{-1} принадлежит H .

Задача. Доказать, что подмножество H группы G тогда и только тогда является подгруппой, когда для любых элементов $h_1 \in H$ и $h_2 \in H$ элемент $h_1h_2^{-1}$ принадлежит H .

Очевидно, что любая подгруппа является группой (относительно определенной во всей группе операции).

Задача. Доказать, что пересечение любого числа подгрупп является подгруппой.

Заметим, что подмножество группы G , состоящее из ее единицы e , а также сама группа G являются подгруппами. Эти подгруппы мы будем называть *тривиальными подгруппами*.

Пусть G — произвольная группа и H — некоторая ее подгруппа. Подмножество группы G , состоящее из всех элементов вида hg , где h — произвольный элемент подгруппы H , а g — некоторый фиксированный элемент группы G , называется *смежным классом* элемента g по подгруппе H и обозначается через Hg .

Очевидно, что $g \in Hg$ (ибо $e \in H$).

Пусть g' — произвольный элемент смежного класса Hg . По определению

$$g' = h'g,$$

где h' — некоторый элемент подгруппы H . Рассмотрим смежный класс Hg' элемента g' . Любой элемент этого смежного класса имеет вид hg' , т. е. вид $hh'g$, где $h \in H$. Следовательно, так как $hh' \in H$, то любой элемент смежного класса Hg'

принадлежит смежному классу Hg , т. е.

$$Hg' \subset Hg.$$

С другой стороны, любой элемент $hg \in Hg$ можно представить в виде $h(h')^{-1}h'g = h(h')^{-1}g'$. Так как $h(h')^{-1} \in H$, то, следовательно, $hg \in Hg'$. Таким образом,

$$Hg \subset Hg'.$$

Тем самым доказано, что

$$Hg' = Hg,$$

то есть

смежный класс Hg' любого элемента g' из смежного класса Hg совпадает с классом Hg .

Отсюда следует, что

если два смежных класса пересекаются, то они совпадают.

Действительно, смежный класс Hg элемента g , лежащего в пересечении данных смежных классов, совпадает с каждым из этих классов.

Теперь легко доказать, что

два элемента g_1 и g_2 группы G тогда и только тогда принадлежат одному смежному классу по подгруппе H , когда $g_1g_2^{-1} \in H$.

Действительно, если $g_1g_2^{-1} \in H$, т. е. $g_1g_2^{-1} = h$, где $h \in H$, то $g_1 = hg_2$, т. е. $g_1 \in Hg_2$ и, следовательно, элемент g_1 принадлежит тому же смежному классу Hg_2 , которому принадлежит элемент g_2 . Обратно, если существует такой смежный класс Hg , что $g_1 \in Hg$ и $g_2 \in Hg$, то $Hg_1 = Hg_2$ и, следовательно, $g_1 \in Hg_2$, т. е. $g_1 = hg_2$, где $h \in H$. Поэтому $g_1g_2^{-1} \in H$.

Наконец,

смежный класс Hg тогда и только тогда совпадает с подгруппой H , когда $g \in H$.

Для доказательства достаточно заметить, что подгруппу H можно рассматривать как смежный класс единицы e .

Пусть Hg — произвольный смежный класс по подгруппе H . Определим отображение ω подгруппы H на смежный класс Hg , положив для любого элемента $h \in H$

$$\omega(h) = hg.$$

Очевидно, что это отображение взаимно однозначно (ибо если $h_1g = h_2g$, то, умножая справа на g , мы получим, что $h_1 = h_2$). Таким образом, для любого смежного класса по подгруппе H существует (вообще говоря, не единственное) взаимно однозначное отображение подгруппы H на этот смежный класс. В частности, если подгруппа H конечна (т. е. состоит из конечного числа элементов), то все смежные классы по подгруппе H состоят из одного и того же числа элементов.

Применим этот результат к случаю, когда группа конечна. Пусть n — число элементов группы G . Любая подгруппа H конечной группы G , очевидно, конечна, и число m ее элементов не превышает n . Пусть k — число различных смежных классов по подгруппе H . (Это число конечно в силу конечности группы G .) По доказанному выше, эти классы, во-первых, не пересекаются, а во-вторых, каждый из них состоит из m элементов. Поэтому все эти классы вместе содержат km различных элементов. Следовательно, заметив, что любой элемент g группы G обязательно принадлежит какому-нибудь смежному классу (именно классу Hg), мы видим, что число n всех элементов группы равно km .

Число элементов конечной группы принято называть ее *порядком*. Таким образом, введенное выше число n является порядком группы G , а число m — порядком подгруппы H . Число k смежных классов по подгруппе H называется *индексом* подгруппы H (в группе G). Доказанное выше равенство $n = km$ означает справедливость следующей теоремы.

Порядок конечной группы делится на порядок любой ее подгруппы. Соответствующее частное равно индексу подгруппы.

Эта теорема известна как теорема Лагранжа.

Вернемся теперь к рассмотрению произвольных (быть может, бесконечных) групп.

Подгруппа H группы G называется *нормальным делителем*, если для любого элемента $h \in H$ и любого элемента $g \in G$ элемент ghg^{-1} принадлежит H . Очевидно, что в абелевой группе любая подгруппа является нормальным делителем.

Задача. Доказать, что пересечение нормальных делителей является нормальным делителем.

Очевидно, что если подгруппа N является нормальным делителем группы G , то она будет нормальным делителем и в любой содержащей подгруппу N подгруппе $H \subset G$. Следует иметь в виду, что обратное, вообще говоря, неверно: если

$$N \subset H \subset G$$

и N есть нормальный делитель в H , то N может и не быть нормальным делителем в G .

Задача. Доказать, что пересечение $N \cap H$ нормального делителя N и произвольной подгруппы H является нормальным делителем в H .

Тривиальные подгруппы (т. е. G и e) являются, очевидно, нормальными делителями. Группа, не имеющая никаких других нормальных делителей, называется *простой*.

Пусть H — произвольный нормальный делитель группы G и пусть Hg_1, Hg_2 — некоторые смежные классы по нормальному делителю H . Произвольно выбрав в классе Hg_1 некоторый элемент h_1g_1 , а в классе Hg_2 — элемент h_2g_2 , рассмотрим произведение $h_1g_1h_2g_2$ этих элементов. Так как

$$h_1g_1h_2g_2 = h_1(g_1h_2g_1^{-1})g_1g_2$$

и, по условию, $g_1h_2g_1^{-1} \in H$, а значит, и $h_1(g_1h_2g_1^{-1}) \in H$, то это произведение лежит в смежном классе Hg_1g_2 и следовательно, его смежный класс совпадает с классом Hg_1g_2 . Таким образом, при любом выборе элементов из данных смежных классов смежный класс их произведения получается один и тот же. Этот однозначно определенный смежный класс называется *произведением* смежных классов Hg_1 и Hg_2 и обозначается через $Hg_1 \cdot Hg_2$. По доказанному

$$Hg_1 \cdot Hg_2 = Hg_1g_2.$$

Тем самым мы определили во множестве всех смежных классов поциальному делителю H некоторую алгебраическую операцию. Легко проверить, что относительно этой операции множество смежных классов является группой (единицей является смежный класс $H = He$, а класс, обратный классу Hg ,

определяется формулой $(Hg)^{-1} = Hg^{-1}$). Эта группа называется *факторгруппой группы G по нормальному делителю H* и обозначается через G/H .

Для конечной группы G факторгруппа G/H конечна и ее порядок равен индексу подгруппы H .

Если $H = e$, то факторгруппа G/H совпадает, очевидно, с группой G , а если $H = G$, то факторгруппа G/H состоит только из одного элемента (единицы).

4. Гомоморфные отображения

Пусть G и G' — произвольные группы. Отображение $\varphi: G \rightarrow G'$ группы G в группу G' называется *гомоморфизмом* (или *гомоморфным отображением*), если оно произведение переводит в произведение, т. е. если для любых элементов g_1, g_2 группы G имеет место равенство

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2).$$

Полагая в этом равенстве $g_1 = g_2 = e$, мы получим, что $\varphi(e) = \varphi(e)\varphi(e)$, откуда следует, что $\varphi(e)$ равно единице группы G' . Далее, полагая $g_1 = g$, $g_2 = g^{-1}$, мы получим, что $\varphi(e) = \varphi(g)\varphi(g^{-1})$, т. е. что $\varphi(g^{-1}) = \varphi(g)^{-1}$. Таким образом, гомоморфизм переводит единицу в единицу и обратный элемент в обратный.

Взаимно однозначное гомоморфное отображение называется *изоморфизмом* (или *изоморфным отображением*). Две группы называются *изоморфными*, если существует хотя бы одно изоморфное отображение одной группы на другую. Изоморфные группы обладают одинаковыми алгебраическими свойствами и в общей теории групп рассматриваются как одинаковые (см. Курс, стр. 282 и 395).

Пусть $\varphi: G \rightarrow G'$ — произвольный гомоморфизм. Очевидно, что для любой подгруппы H группы G совокупность всех элементов группы G' , имеющих вид $\varphi(h)$, где $h \in H$, является подгруппой группы G' . Эта подгруппа называется *образом подгруппы H при гомоморфизме φ* и обозначается обычно через $\varphi(H)$.

В частности, определена подгруппа $\varphi(G)$ — образ группы G при гомоморфизме φ . Эта подгруппа называется также *образом гомоморфизма φ* и обозначается иногда через $\text{Im } \varphi$.

Если $\varphi(G) = G'$, т. е. если для любого элемента $g' \in G'$ существует такой элемент g (вообще говоря, не однозначно определенный), что $\varphi(g) = g'$, то φ называется *эпиморфным отображением* (или просто *эпиморфизмом*) группы G на группу G' .

Особое значение эпиморфизмов определяется тем, что любой гомоморфизм $\varphi: G \rightarrow G'$ можно рассматривать как эпиморфное отображение группы G на подгруппу $\varphi(G)$. Это замечание легко обобщается: для любой подгруппы H группы G гомоморфизм φ можно рассматривать как эпиморфное отображение подгруппы H на подгруппу $\varphi(H)$. Точнее, гомоморфизм φ определяет некоторое эпиморфное отображение $\bar{\varphi}: H \rightarrow \varphi(H)$ (отображения φ и $\bar{\varphi}$ на элементах подгруппы H совпадают и отличаются лишь тем, что φ определено на всей группе G , а $\bar{\varphi}$ — лишь на подгруппе H).

Пусть опять $\varphi: G \rightarrow G'$ — произвольный гомоморфизм, и пусть H и H' — такие нормальные делители групп G и G' соответственно, что $\varphi(H) \subset H'$. Рассмотрим в группе G произвольный смежный класс Hg . Любой элемент hg этого смежного класса при гомоморфизме φ переходит в элемент $\varphi(h)\varphi(g)$, принадлежащий смежному классу $H'\varphi(g)$. Таким образом, все элементы смежного класса Hg переходят в элементы одного и того же смежного класса $H'\varphi(g)$. Обозначим этот однозначно определенный смежный класс через $\bar{\varphi}(Hg)$:

$$\bar{\varphi}(Hg) = H'\varphi(g).$$

Тем самым мы определили некоторое отображение

$$\bar{\varphi}: G/H \rightarrow G'/H'.$$

Это отображение гомоморфно, ибо

$$\begin{aligned} \bar{\varphi}(Hg_1 Hg_2) &= \bar{\varphi}(Hg_1 g_2) = H'\varphi(g_1 g_2) = H'\varphi(g_1)\varphi(g_2) = \\ &= H'\varphi(g_1) H'\varphi(g_2) = \bar{\varphi}(Hg_1) \bar{\varphi}(Hg_2). \end{aligned}$$

Мы будем говорить, что гомоморфизм $\bar{\varphi}$ *индуцирован* гомоморфизмом φ . Подчеркнем, что он определен только тогда, когда

$$\varphi(H) \subset H'.$$

В частном случае, когда нормальный делитель H' состоит только из единицы e' группы G' , мы получаем, что

если $\varphi(H) = e'$, то гомоморфизм $\varphi: G \rightarrow G'$ индуцирует гомоморфизм $\bar{\varphi}: G/H \rightarrow G'$.

Очевидно, что

гомоморфизм, индуцированный эпиморфным отображением, является эпиморфизмом.

Рассмотрим теперь совокупность N всех элементов, переходящих при гомоморфизме $\varphi: G \rightarrow G'$ в единицу e' группы G' . Если $a \in N$, $b \in N$, т. е. $\varphi(a) = e'$, $\varphi(b) = e'$, то $\varphi(ab) = e'e' = e'$, т. е. $ab \in N$. Аналогично, если $a \in N$, то $a^{-1} \in N$. Кроме того, если $a \in N$ и g — любой элемент группы G , то $\varphi(gag^{-1}) = \varphi(g)\varphi(g)^{-1} = e'$, т. е. $gag^{-1} \in N$. Таким образом, N является нормальным делителем группы G . Этот нормальный делитель называется ядром гомоморфизма φ и обозначается через $\text{Кер } \varphi$.

Если $\varphi(a) = \varphi(b)$, то $\varphi(ab^{-1}) = e'$, т. е. $ab^{-1} \in N$. Обратно, если $ab^{-1} \in N$, то $\varphi(a) = \varphi(b)$. Но $ab^{-1} \in N$ тогда и только тогда, когда a и b принадлежат одному смежному классу по подгруппе N . Таким образом,

при гомоморфизме $\varphi: G \rightarrow G'$ элементы группы G тогда и только тогда переходят в один и тот же элемент группы G' , когда они принадлежат одному смежному классу по ядру гомоморфизма φ .

Если $\text{Кер } \varphi = e'$, то гомоморфизм φ называется мономорфизмом. Из только что доказанного утверждения следует, что мономорфизм $\varphi: G \rightarrow G'$ переводит различные элементы группы G в различные элементы группы G' , т. е. является изоморфным отображением группы G на подгруппу $\varphi(G)$ группы G' . В частности, отображение одновременно мономорфное и эпиморфное является изоморфизмом, и обратно.

Так как для любого гомоморфизма $\varphi: G \rightarrow G'$ с ядром N

$$\varphi(N) = e',$$

то гомоморфизм φ индуцирует некоторый гомоморфизм

$$\bar{\varphi}: G/N \rightarrow G'.$$

Гомоморфизм $\bar{\varphi}$ определяется формулой

$$\bar{\varphi}(Ng) = \varphi(g).$$

Если $\bar{\varphi}(Ng) = e'$, т. е. $\varphi(g) = e'$, то $g \in N$ и, следовательно, $Ng = N$. Другими словами, ядро гомоморфизма φ

состоит только из одного смежного класса N — единицы группы G/N , т. е. гомоморфизм φ является мономорфизмом. Таким образом,

любой гомоморфизм $\varphi: G \rightarrow G'$ индуцирует мономорфизм $\bar{\varphi}: G/N \rightarrow G'$, где $N = \text{Кер } \varphi$.

Если гомоморфизм φ является эпиморфизмом, то, как мы знаем, гомоморфизм $\bar{\varphi}$ также будет эпиморфизмом, а значит и изоморфизмом. Таким образом,

любой эпиморфизм $\varphi: G \rightarrow G'$ индуцирует изоморфизм $\bar{\varphi}: G/N \rightarrow G'$, где $N = \text{Кер } \varphi$.

Это утверждение известно как теорема о гомоморфизмах.

Группа G' называется гомоморфным образом группы G , если существует хотя бы одно эпиморфное отображение группы G на группу G' (принято говорить именно «гомоморфный образ», хотя, конечно, более последовательно было бы говорить «эпиморфный образ»). Из доказанного предложения немедленно следует, что *любой гомоморфный образ группы изоморчен некоторой ее факторгруппе*.

Заметим, что обратное утверждение также справедливо: *любая факторгруппа G/N группы G является гомоморфным образом группы G .*

Для доказательства достаточно построить хотя бы одно эпиморфное отображение φ группы G на факторгруппу G/N . Такое отображение можно, например, определить формулой

$$\varphi(g) = Ng.$$

Заметим, что так определенное отображение φ есть не что иное, как отображение, индуцированное тождественным отображением группы G на себя (в общем определении нужно за H принять единичную подгруппу, а за H' нормальный делитель N).

ГЛАВА 3

ТЕОРИЯ ГАЛУА

1. Нормальные расширения

Во всей этой главе предполагается заданным некоторое фиксированное поле P . Мы будем называть это поле *основным полем*. Все другие поля предполагаются расширениями этого основного поля. Подчеркнем, что основное поле можно выбрать совершенно произвольно.

Пусть $f(x)$ — произвольный (вообще говоря, приводимый) многочлен над полем P . Расширение $P(\alpha_1, \dots, \alpha_n)$ поля P , порожденное всеми корнями $\alpha_1, \dots, \alpha_n$ многочлена $f(x)$, называется *полем разложения* этого многочлена (заметим, что это определение отличается от определения, принятого в Курсе, стр. 304, где полем разложения называется любое, не обязательно минимальное расширение поля P , содержащее корни $\alpha_1, \dots, \alpha_n$). Согласно гл. 1, п. 5, любой элемент поля $P(\alpha_1, \dots, \alpha_n)$ выражается в виде многочлена от $\alpha_1, \dots, \alpha_n$ с коэффициентами из поля P .

Конечное расширение K поля P называется *нормальным* расширением, если любой неприводимый над P многочлен, имеющий в K хотя бы один корень, разлагается в K на линейные множители. Другими словами, расширение K поля P нормально, если выполняются следующие два условия:

1) K конечно над P ;

2) если неприводимый над P многочлен имеет в K хотя бы один корень, то K содержит поле разложения этого многочлена.

Нормальные расширения основного поля P мы будем также называть *нормальными полями*.

Два алгебраических (над полем P) числа называются *сопряженными* (над P), если их минимальные многочлены

(над P) совпадают (точнее, отличаются на постоянный множитель). Другими словами, алгебраические числа сопряжены, если они являются корнями одного и того же неприводимого над P многочлена. Понятие сопряженных чисел позволяет следующим образом переформулировать определение нормального расширения: расширение K поля P нормально, если

- 1) K конечно над P ;
- 2) любое число, сопряженное некоторому числу из K , также принадлежит K .

Эта форма определения нормального расширения часто наиболее удобна.

Пусть K — произвольное нормальное расширение поля P . Так как поле K , по определению, конечно над P , то существуют такие элементы $\alpha_1, \dots, \alpha_s \in K$, что

$$K = P(\alpha_1, \dots, \alpha_s).$$

Пусть $f_l(x)$ — минимальный многочлен числа α_l , $l = 1, \dots, s$, над полем P . Так как поле K нормально (т. е. является нормальным расширением поля P), то многочлены $f_l(x)$, имеющие в нем корни, разлагаются в K на линейные множители. Следовательно, в поле K разлагается на линейные множители и произведение

$$f(x) = f_1(x) \cdots f_s(x)$$

многочленов $f_1(x), \dots, f_s(x)$, т. е. поле K содержит поле разложения Q многочлена $f(x)$. С другой стороны, числа $\alpha_1, \dots, \alpha_s$ являются корнями (не всеми!) многочлена $f(x)$, и потому поле K содержится в поле Q . Следовательно, $K = Q$. Таким образом,

любое нормальное поле является полем разложения некоторого многочлена.

Задача. Доказать, что любое нормальное поле является полем разложения неприводимого многочлена.

Оказывается, что нормальными полями исчерпываются все поля разложения, т. е.

любое поле, являющееся полем разложения некоторого многочлена (над полем P), будет нормальным расширением поля P .

Для доказательства этого важного утверждения нам понадобятся некоторые сведения из теории многочленов от n неизвестных, имеющие и самостоятельный интерес.

Пусть

$$a = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

— произвольная подстановка степени n (см. Курс, стр. 30, а также ниже, ч. II, гл. 3, п. 1). Любому многочлену $g(x_1, \dots, x_n)$ от n неизвестных над полем P отнесем с помощью подстановки a многочлен $g_a(x_1, \dots, x_n)$, определив его формулой

$$g_a(x_1, \dots, x_n) = g(x_{i_1}, \dots, x_{i_n}).$$

Очевидно, что

$$g_e = g$$

и

$$(g_a)_b = g_{ab}.$$

Кроме того, равенство $g_a = g$ тогда и только тогда имеет место для любой подстановки a , когда многочлен g является симметрическим многочленом.

Пусть теперь

$$a_1 = e, a_2, \dots, a_{n!}$$

— все подстановки степени n . Рассмотрим многочлены

$$g_{a_1} = g, g_{a_2}, \dots, g_{a_{n!}}, \quad (1)$$

где g — произвольный многочлен от n неизвестных x_1, \dots, x_n . Воздействуя на эти многочлены произвольной подстановкой a степени n , мы получим многочлены

$$g_{a_1 a} = g_a, g_{a_2 a}, \dots, g_{a_{n!} a}. \quad (2)$$

Так как подстановки

$$a_1 a, a_2 a, \dots, a_{n!} a,$$

очевидно, исчерпывают все подстановки степени n (их $n!$, и все они различные), то многочлены (2) с точностью до порядка следования совпадают с многочленами (1). Отсюда вытекает, что любой симметрический многочлен от $g_{a_1}, g_{a_2}, \dots, g_{a_{n!}}$ является симметрическим многочленом и от

x_1, \dots, x_n , т. е. если $F(y_1, \dots, y_{n!})$ — симметрический многочлен от $n!$ переменных $y_1, \dots, y_{n!}$, то подставляя вместо y_i многочлен $g_{\alpha_i}(x_1, \dots, x_n)$, мы получим симметрический многочлен от x_1, \dots, x_n . В частности, все коэффициенты многочлена

$$G(x; x_1, \dots, x_n) = \prod_{i=1}^{n!} (x - g_{\alpha_i}(x_1, \dots, x_n)) \quad (3)$$

(рассматриваемого как многочлен от неизвестного x) являются симметрическими многочленами от x_1, \dots, x_n и, следовательно (см. Курс, стр. 322), выражаются в виде многочленов (с коэффициентами из поля P) от элементарных симметрических многочленов.

Вернемся теперь к доказательству сформулированного выше утверждения.

Пусть K — поле разложения некоторого многочлена $f(x)$ над полем P . Тогда, как уже выше отмечалось, любой элемент β поля K записывается в виде многочлена от корней $\alpha_1, \dots, \alpha_n$ многочлена $f(x)$ (вообще говоря, многими различными способами), т. е. существует такой многочлен $g(x_1, \dots, x_n)$ от n неизвестных x_1, \dots, x_n , что

$$\beta = g(\alpha_1, \dots, \alpha_n).$$

Рассмотрим многочлен

$$\bar{G}(x) = G(x; \alpha_1, \dots, \alpha_n),$$

где $G(x; x_1, \dots, x_n)$ — многочлен (3), построенный для многочлена $g(x_1, \dots, x_n)$. По определению

$$\bar{G}(x) = \prod_{i=1}^{n!} (x - \beta_i),$$

где

$$\beta_i = g_{\alpha_i}(\alpha_1, \dots, \alpha_n) \in K.$$

Согласно сказанному выше, коэффициенты многочлена $\bar{G}(x)$ выражаются в виде многочленов над полем P от элементарных симметрических многочленов от $\alpha_1, \dots, \alpha_n$, т. е. выражаются в виде многочленов от коэффициентов многочлена $f(x)$. Следовательно, $\bar{G}(x)$ является многочленом над полем P .

Минимальный многочлен $h(x)$ числа β (над полем P) имеет с многочленом $\bar{G}(x)$ общий корень $\beta = \beta_1$ и поэтому делит многочлен $\bar{G}(x)$. Следовательно, все корни многочлена $h(x)$, т. е. все числа, сопряженные с числом β , содержатся среди чисел β_1, \dots, β_n и поэтому принадлежат полю K .

Таким образом, мы доказали, что все числа, сопряженные с любым элементом расширения K (как мы знаем, конечного), принадлежат K . Следовательно, поле K нормально.

2. Автоморфизмы полей. Группа Галуа

Взаимно однозначное отображение S некоторого поля K на себя называется *автоморфизмом*, если оно сумму переводит в сумму, а произведение в произведение, т. е. если для любых элементов α, β поля K

$$\begin{aligned} (\alpha + \beta)^S &= \alpha^S + \beta^S, \\ (\alpha\beta)^S &= \alpha^S\beta^S \end{aligned} \tag{1}$$

(элемент, в который при автоморфизме S переходит элемент α , мы обозначаем через α^S).

Подчеркнем, что автоморфизм должен быть взаимно однозначным отображением (преобразованием), т. е., кроме условий (1), он должен удовлетворять также следующим требованиям:

а) для любого элемента $\alpha \in K$ элемент α^S однозначно определен и принадлежит K ;

б) если $\alpha \neq \beta$, то $\alpha^S \neq \beta^S$;

в) для любого элемента $\beta \in K$ существует такой элемент $\alpha \in K$, что $\alpha^S = \beta$.

Из условия б) следует, что предусмотренный условием в) элемент α определен однозначно. Следовательно, обозначая этот элемент через $\beta^{S^{-1}}$:

$$\alpha = \beta^{S^{-1}},$$

мы получим некоторое (очевидно, взаимно однозначное) преобразование S^{-1} (так называемое *обратное* преобразование). Это преобразование однозначно характеризуется тем, что для любого элемента $\alpha \in K$

$$(\alpha^{S^{-1}})^S = \alpha. \tag{2}$$

Оказывается, что преобразование S^{-1} также является автоморфизмом. Действительно, для любых элементов $\alpha \in K$ и $\beta \in K$

$$(\alpha s^{-1} + \beta s^{-1})^s = (\alpha s^{-1})^s + (\beta s^{-1})^s = \alpha + \beta$$

и, следовательно, по определению,

$$(\alpha + \beta)^{s^{-1}} = \alpha^{s^{-1}} + \beta^{s^{-1}}.$$

Аналогично доказывается, что

$$(\alpha\beta)^{s^{-1}} = \alpha^{s^{-1}}\beta^{s^{-1}}.$$

Произведением ST двух автоморфизмов S и T называется преобразование, получающееся в результате последовательного выполнения сначала преобразования S , а затем преобразования T ; для любого элемента $\alpha \in K$ элемент α^{ST} определяется формулой

$$\alpha^{ST} = (\alpha^S)^T.$$

Непосредственно проверяется, что преобразование ST также является автоморфизмом.

Задача. Доказать, что умножение автоморфизмов ассоциативно.

Умножение автоморфизмов, очевидно, обладает единицей — ею служит *тождественный автоморфизм* E , оставляющий все элементы поля K на месте:

$$\alpha^E = \alpha.$$

По определению (см. формулу (2))

$$S^{-1}S = E. \quad (3)$$

Рассмотрим теперь автоморфизм $(S^{-1})^{-1}$, обратный автоморфизму S^{-1} . По определению

$$(S^{-1})^{-1} S^{-1} = E. \quad (4)$$

Умножая это равенство справа на S и пользуясь формулой (3), мы получим, что

$$(S^{-1})^{-1} = S.$$

Подставляя это выражение в формулу (4), получаем

$$SS^{-1} = E.$$

Итак,

$$S^{-1}S = SS^{-1} = E.$$

Таким образом, мы видим, что относительно операции умножения автоморфизмов множество всех автоморфизмов является группой. Эта группа называется *группой автоморфизмов поля K* .

Задача. Доказать, что любой автоморфизм оставляет на месте все рациональные числа (в частности, числа 0 и 1).

Пусть теперь P — некоторое подполе поля K . Автоморфизм S поля K называется *автоморфизмом над полем P* , если он все элементы поля P оставляет на месте, т. е. если для любого элемента $c \in P$

$$c^S = c.$$

Очевидно, что совокупность всех автоморфизмов над полем P является подгруппой группы автоморфизмов поля K . Если поле K является нормальным расширением поля P , то эта подгруппа называется *группой Галуа поля K над полем P* и обозначается символом $G(K, P)$.

Пусть

$$f(x) = c_0 + c_1x + \dots + c_nx^n$$

— произвольный многочлен над полем P , имеющий в K хотя бы один корень α :

$$c_0 + c_1\alpha + \dots + c_n\alpha^n = 0. \quad (5)$$

Применяя к равенству (5) автоморфизм S из группы Галуа $G(K, P)$, мы, как легко видеть, получим, что

$$c_0 + c_1\alpha^S + \dots + c_n(\alpha^S)^n = 0$$

(ибо $c_i^S = c_i$ для любого $i = 0, 1, \dots, n$), т. е. что

$$f(\alpha^S) = 0.$$

Таким образом,

любой автоморфизм из группы Галуа $G(K, P)$ переводит каждый корень произвольного многочлена над полем P снова в корень этого же многочлена.

Отсюда, в частности, следует, что

для любого числа $a \in K$ и любого автоморфизма $S \in G(K, P)$ число a^S сопряжено над полем P с числом a .

Замечание. Если считать известным понятие линейного преобразования и тот факт, что линейное преобразо-

вание конечномерного пространства тогда и только тогда взаимно однозначно, когда оно никакой отличный от нуля вектор не переводит в нулевой вектор (см. Курс, стр. 205), то можно показать, что для случая конечных (и в частности нормальных) расширений в определении понятия автоморфизма поля K над полем P условие взаимной однозначности можно опустить, т. е.

любое отображение S конечного расширения K в себя, обладающее свойствами (1) и оставляющее на месте все элементы поля P , взаимно однозначно, т. е. является автоморфизмом поля K над полем P .

Действительно, если $c \in P$ и $\alpha \in K$, то

$$(c\alpha)^S = c^S \alpha^S = c\alpha^S.$$

Кроме того, для любых элементов α и β поля K

$$(\alpha + \beta)^S = \alpha^S + \beta^S.$$

Это означает, что отображение S представляет собой линейное преобразование поля K , рассматриваемого как линейное (конечномерное) пространство над полем P (см. гл. 1, п. 2). Поэтому, в силу отмеченного выше факта из теории линейных преобразований, для доказательства сформулированного утверждения достаточно показать, что если $\alpha \neq 0$, то и $\alpha^S \neq 0$. Но если $\alpha \neq 0$, то в поле K существует такой элемент β , что $\alpha\beta = 1$ и, следовательно, $\alpha^S\beta^S = 1$. Таким образом, действительно, $\alpha^S \neq 0$.

3. Порядок группы Галуа

Пусть K — произвольное нормальное расширение поля P . Согласно гл. 1, п. 7, расширение K является простым алгебраическим расширением, т. е. в K существует такой элемент θ , что

$$K = P(\theta).$$

Степень n минимального многочлена $f(x)$ элемента θ равна степени $[K : P]$ поля K над полем P . Любой элемент α поля K имеет однозначную запись вида

$$\alpha = c_0 + c_1\theta + \dots + c_{n-1}\theta^{n-1}, \text{ где } c_0, c_1, \dots, c_{n-1} \in P. \quad (1)$$

Как доказано в предыдущем пункте, любой автоморфизм S из группы Галуа $G(K, P)$ переводит корень θ снова в корень

многочлена $f(x)$. Другими словами, каждому автоморфизму $S \in G(K, P)$ соответствует некоторый корень многочлена $f(x)$ (при выбранном корне θ). Изучим это соответствие подробнее.

Пусть θ' — произвольный корень многочлена $f(x)$. Так как поле K нормально и $\theta \in K$, то $\theta' \in K$. Определим преобразование S поля K в себя, положив для любого элемента (1) из этого поля

$$\alpha^S = c_0 + c_1 \theta' + \dots + c_{n-1} \theta'^{n-1}. \quad (2)$$

Так как запись элемента α в виде (1) однозначна, то формула (2) определяет элемент α^S единственным образом.

Определение преобразования S можно, очевидно, сформулировать следующим образом: если

$$\alpha = g(\theta),$$

где $g(x)$ — многочлен над полем P , имеющий степень, меньшую n , то

$$\alpha^S = g(\theta').$$

Рассмотрим теперь над полем P многочлен $g(x)$ произвольной степени, и пусть

$$\alpha = g(\theta).$$

Разделим (с остатком) многочлен $g(x)$ на многочлен $f(x)$:

$$g(x) = f(x)q(x) + r(x). \quad (3)$$

Полагая в этом равенстве $x = \theta$, мы получим, поскольку $f(\theta) = 0$, что

$$\alpha = r(\theta).$$

Так как степень многочлена $r(x)$ меньше n , то отсюда вытекает, что

$$\alpha^S = r(\theta').$$

С другой стороны, полагая в формуле (3) $x = \theta'$, мы получим, что

$$g(\theta') = r(\theta').$$

Следовательно,

$$\alpha^S = g(\theta').$$

Таким образом,

$$g(\theta)^S = g(\theta')$$

независимо от того, какова степень многочлена $g(x)$.

Пусть теперь

$$\alpha_1 = g_1(\theta), \quad \alpha_2 = g_2(\theta)$$

— произвольные элементы поля K . Тогда

$$\alpha_1 + \alpha_2 = g_1(\theta) + g_2(\theta),$$

$$\alpha_1 \alpha_2 = g_1(\theta) g_2(\theta)$$

и, следовательно,

$$(\alpha_1 + \alpha_2)^S = g_1(\theta') + g_2(\theta') = \alpha_1^S + \alpha_2^S,$$

$$(\alpha_1 \alpha_2)^S = g_1(\theta') g_2(\theta') = \alpha_1^S \alpha_2^S.$$

Таким образом, преобразование S сохраняет сумму и произведение, т. е. обладает свойствами (1) п. 2. Кроме того, это преобразование, очевидно, оставляет все элементы поля P на месте. Поэтому (см. замечание к п. 2) преобразование S является автоморфизмом поля K над полем P , т. е. принадлежит группе Галуа $G(K, P)$.

Тот факт, что преобразование S является автоморфизмом, т. е., кроме свойств (1) п. 2, обладает также и свойством взаимной однозначности, можно доказать и не пользуясь замечанием к п. 2. Действительно, рассмотрим поле $P(\theta')$. Так как $\theta' \in K$, то

$$P(\theta') \subset K.$$

С другой стороны, степень поля $P(\theta')$ над полем P равна степени многочлена $f(x)$, т. е. равна степени поля K . Следовательно,

$$P(\theta') = K.$$

Отсюда следует, что наряду с записью (1) любой элемент α поля K имеет однозначную запись вида

$$\alpha = c'_0 + c'_1 \theta' + \dots + c'_{n-1} \theta'^{n-1}, \quad (4)$$

где $c'_0, c'_1, \dots, c'_{n-1} \in P$.

Определим теперь преобразование S' поля K в себя, положив для любого элемента (4) из этого поля

$$\alpha^{S'} = c'_0 + c'_1 \theta + \dots + c'_{n-1} \theta^{n-1}.$$

Так как, очевидно,

$$S'S = SS' = E$$

(т. е. $S' = S^{-1}$), то преобразование S является, как и утверждалось, взаимно однозначным преобразованием поля K на себя (ибо из $\alpha^S = \beta^S$ следует, что $\alpha^{SS'} = \beta^{SS'}$, т. е. что $\alpha = \beta$ и для любого элемента $\alpha \in K$ существует такой элемент β , именно $\beta = \alpha^{S'}$, что $\beta^S = \alpha$), т. е. является автоморфизмом.

Построенный автоморфизм S переводит корень θ в корень θ' :

$$\theta^S = \theta',$$

т. е. этот автоморфизм соответствует корню θ' в указанном выше смысле. Таким образом, доказано, что для любого корня многочлена $f(x)$ существует в группе Галуа $G(K, P)$ автоморфизм, которому этот корень соответствует. Оказывается, что автоморфизм однозначно определяется соответствующим корнем, т. е. если

$$\theta^S = \theta^T,$$

то

$$S = T.$$

Действительно, если $\theta^S = \theta^T$, то $\theta^{ST^{-1}} = \theta$, т. е. автоморфизм ST^{-1} оставляет корень θ на месте и, следовательно, оставляет на месте любое выражение вида

$$c_0 + c_1\theta + \dots + c_{n-1}\theta^{n-1}, \text{ где } c_0, \dots, c_{n-1} \in P,$$

т. е. оставляет на месте любой элемент поля K . Таким образом, $ST^{-1} = E$ и потому $S = T$.

Итак, элементы группы Галуа $G(K, P)$ (т. е. автоморфизмы поля K над полем P) находятся во взаимно однозначном соответствии с корнями многочлена $f(x)$, и, следовательно, их число, т. е. порядок группы $G(K, P)$, равно числу корней многочлена $f(x)$, т. е. равно n (все корни многочлена $f(x)$ различны, так как этот многочлен неприводим). Тем самым мы доказали, что

порядок группы Галуа $G(K, P)$ равен степени поля K над полем P .

4. Соответствие Галуа

Пусть, как и выше, $K = P(\theta)$ — произвольное нормальное расширение основного поля P и $G(K, P)$ — его группа Галуа над полем P .

В этом пункте мы будем рассматривать расширения L поля P , содержащиеся в поле K :

$$P \subset L \subset K.$$

Такие расширения мы будем называть *промежуточными полями*.

Многочлен $f(x)$ над полем P , корнем которого является число θ , можно рассматривать и как многочлен над любым промежуточным полем L . Очевидно, что его полем разложения над L является поле $L(\theta)$ (почему?). Следовательно, поле $L(\theta)$ нормально над полем L . С другой стороны, так как $P \subset L$, то $P(\theta) \subset L(\theta)$, т. е. $K \subset L(\theta)$, а так как $L \subset K$ и $\theta \in K$, то $L(\theta) \subset K$. Следовательно, $K = L(\theta)$. Таким образом,

поле K нормально над любым промежуточным полем L .

Поэтому можно говорить о группе Галуа $G(K, L)$ поля K над полем L . Согласно доказанному в предыдущем пункте, порядок группы $G(K, L)$ равен степени поля K над полем L .

Элементами группы $G(K, L)$ являются, по определению, автоморфизмы поля K , оставляющие на месте любой элемент поля L . Так как $P \subset L$, то эти автоморфизмы оставляют на месте и любой элемент поля P , т. е. являются элементами группы Галуа $G(K, P)$ поля K над полем P . Таким образом,

$$G(K, L) \subset G(K, P),$$

то есть

группа Галуа поля K над полем L является подгруппой группы Галуа поля K над полем P . Ее порядок равен степени $[K : L]$ поля K над полем L .

Пусть теперь H — произвольная подгруппа группы Галуа $G(K, P)$. Очевидно, что совокупность всех элементов поля K , остающихся на месте при любом автоморфизме из подгруппы H , является подполем поля K . Это подполе содержит поле P , т. е. является промежуточным полем. Мы будем обозначать его через $K(H, P)$.

Пусть

$$T_1 = E, T_2, \dots, T_m$$

— все элементы подгруппы H (таким образом, m — порядок подгруппы H). Рассмотрим многочлен

$$h(x) = \prod_{i=1}^m (x - \theta^{T_i}).$$

Его корнями являются числа

$$\theta^{T_1} = \theta, \theta^{T_2}, \dots, \theta^{T_m}. \quad (1)$$

При любом автоморфизме $T \in H$ эти числа переходят в числа

$$\theta^{T_i T} = \theta^T, \theta^{T_2 T}, \dots, \theta^{T_m T}. \quad (2)$$

Но элементы

$$T_1 T = T, T_2 T, \dots, T_m T,$$

очевидно, исчерпывают все элементы подгруппы H (их m и они все различны). Следовательно, числа (2) с точностью до порядка следования совпадают с числами (1). Другими словами, при любом автоморфизме $T \in H$ корни многочлена $h(x)$ лишь переставляются. Поэтому любой симметрический многочлен от этих корней, в частности любой коэффициент многочлена $h(x)$, остается на месте при автоморфизме T и, следовательно (поскольку T — любой автоморфизм из подгруппы H), принадлежит полю $K(G, H)$. Таким образом, многочлен $h(x)$ является многочленом над полем $K(G, H)$. Следовательно, минимальный многочлен элемента θ над полем $K(G, H)$ является делителем многочлена $h(x)$, и поэтому его степень (т. е. степень числа θ над полем $K(G, H)$) меньше или равна m . Но, как мы видели выше, поле K является простым алгебраическим расширением любого промежуточного поля (и значит, в частности, поля $K(G, H)$), порожденным числом θ . Поэтому степень поля K над полем $K(G, H)$ равна степени минимального (над $K(G, H)$) многочлена числа θ , т. е., по доказанному, меньше или равна m .

Рассмотрим теперь группу Галуа $G(K, L)$ поля K над полем $L = K(G, H)$. Согласно п. 3, порядок этой группы равен степени поля K над полем $K(G, H)$ и поэтому меньше или равен m . С другой стороны, группа $G(K, L)$ состоит,

по определению, из всех автоморфизмов поля K , оставляющих на месте элементы поля $L = K(G, H)$ и поэтому содержащих подгруппу H . Следовательно, ее порядок не может быть меньше m .

Отсюда вытекает, что порядок группы $G(K, L)$ равен m и потому она совпадает с подгруппой H . Таким образом,

если $L = K(G, H)$, то $G(K, L) = H$.

Пусть теперь L — произвольное промежуточное поле, и пусть $H = G(K, L)$. Рассмотрим поле $K(G, H)$. Очевидно, что

$$L \subset K(G, H).$$

Согласно гл. 1, п. 6,

$$[K(G, H) : L] = \frac{[K : L]}{[K : K(G, H)]}.$$

С другой стороны, по только что доказанному, степень $[K : K(G, H)]$ поля K над полем $K(G, H)$ равна порядку группы $H = G(K, L)$, т. е. равна степени $[K : L]$ поля K над полем L . Следовательно, $[K(G, H) : L] = 1$, т. е. $L = K(G, H)$. Тем самым доказано, что

если $H = G(K, L)$, то $K(G, H) = L$.

Мы видим, таким образом, что любому промежуточному полю L соответствует некоторая подгруппа группы $G(K, P)$ (именно группа $G(K, L)$), причем для любой подгруппы H группы $G(K, P)$ существует промежуточное поле L (именно поле $K(G, H)$), которому соответствует эта подгруппа, и различным промежуточным полям соответствуют различные подгруппы (потому что, если $G(K, L_1) = G(K, L_2)$, то имеем $L_1 = K(G, G(K, L_1)) = K(G, G(K, L_2)) = L_2$).

Другими словами, мы построили взаимно однозначное соответствие между множеством всех промежуточных полей и множеством всех подгрупп группы Галуа. Это соответствие называется *соответствием Галуа*.

Повторим еще раз, что

в соответствии Галуа промежуточному подполю L нормального поля K соответствует группа Галуа $G(K, L)$ поля K над полем L , а подгруппе H группы $G(K, P)$ — подполе $K(G, H)$, состоящее из всех элементов поля K ,

остающихся на месте при каждом автоморфизме из H . Порядок группы $G(K, L)$ равен степени поля K над полем L , а степень поля K над полем $K(G, H)$ равна порядку группы H .

В частности, всей группе $G(K, P)$ соответствует поле P . Следовательно,

поле P состоит из всех элементов поля K , остающихся на месте при каждом автоморфизме из группы $G(K, P)$.

Единичной подгруппе E , т. е. подгруппе, состоящей только из тождественного автоморфизма E , соответствует, очевидно, все поле K .

Соответствие Галуа позволяет теорию подполяй данного нормального поля в некотором смысле «отобразить» в теорию подгрупп его группы Галуа и тем самым изучить эти подполя теоретико-групповыми методами. Например, из конечности числа подгрупп конечной группы немедленно следует, что число промежуточных подполяй любого нормального поля конечно. Доказать этот факт, не пользуясь соответствием Галуа, довольно затруднительно.

Применяя соответствие Галуа, нужно всегда иметь в виду, что оно «обращает знаки включения», т. е. если подполям L_1 и L_2 поля K соответствуют подгруппы H_1 и H_2 его группы Галуа, то из

$$L_1 \subset L_2 \quad (3)$$

вытекает, что

$$H_1 \supset H_2, \quad (4)$$

и, наоборот, из (4) вытекает (3).

5. Теорема о сопряженных элементах

Пусть α — произвольный элемент нормального поля K . Рассмотрим элементы

$$\alpha^{S_1} = \alpha, \alpha^{S_2}, \dots, \alpha^{S_n}, \quad (1)$$

где

$$S_1 = E, S_2, \dots, S_n$$

— все автоморфизмы из группы Галуа $G(K, P)$ поля K над полем P . При любом автоморфизме S поля K над полем P

числа (1) переходят в числа

$$\alpha^{s_1 s} = \alpha^s, \alpha^{s_2 s}, \dots, \alpha^{s_n s},$$

т. е. подвергаются лишь некоторой перестановке. Поэтому все коэффициенты многочлена

$$g(x) = \prod_{i=1}^n (x - \alpha^{s_i})$$

остаются на месте при любом автоморфизме S , т. е. принадлежат полю P .

Поскольку $\alpha = \alpha^{s_1}$, многочлен $g(x)$ и минимальный многочлен $f(x)$ элемента α имеют общий корень и, следовательно, многочлен $g(x)$ делится на многочлен $f(x)$ (ибо многочлен $f(x)$ неприводим). С другой стороны, мы знаем (см. п. 2), что все числа $\alpha^{s_1}, \dots, \alpha^{s_n}$ (среди этих чисел, вообще говоря, могут быть одинаковые) сопряжены с числом α , т. е. являются корнями многочлена $f(x)$. Таким образом, каждый корень многочлена $g(x)$ является корнем многочлена $f(x)$. Пусть

$$g(x) = p_1(x)^{k_1} p_2(x)^{k_2} \dots p_l(x)^{k_l}$$

— разложение многочлена $g(x)$ в произведение степеней различных неприводимых многочленов (имеющих старшие коэффициенты, равные единице). Так как многочлен $g(x)$ делится на многочлен $f(x)$ и многочлен $f(x)$ неприводим, то многочлен $f(x)$ должен совпадать с одним из многочленов $p_1(x), \dots, p_l(x)$ (мы предполагаем, что старший коэффициент многочлена $f(x)$ равен единице). Пусть для определенности $f(x) = p_1(x)$, так что

$$g(x) = f(x)^{k_1} p_2(x)^{k_2} \dots p_l(x)^{k_l}.$$

Так как все корни многочлена $g(x)$ являются корнями многочлена $f(x)$, а ни один из корней многочлена $p_2(x), \dots, p_l(x)$ не может быть (в силу неприводимости этих многочленов) корнем многочлена $f(x)$, то многочлены $p_2(x), \dots, p_l(x)$ не могут иметь корней, т. е.

$$p_2(x) = \dots = p_l(x) = 1.$$

Таким образом,

$$g(x) = f(x)^{k_1}.$$

Отсюда, в частности, следует, что числа $\alpha^{s_1}, \dots, \alpha^{s_n}$ исчерпывают (вообще говоря, с повторениями) все числа, сопряженные с числом α . Тем самым доказано, что

элементы поля K тогда и только тогда сопряжены (над полем P), когда существует автоморфизм поля K над полем P , переводящий один элемент в другой.

6. Группа Галуа нормального подполя

Пусть промежуточное поле L является нормальным расширением основного поля P . Тогда для любого элемента $\alpha \in L$ и любого автоморфизма $S \in G(K, P)$ элемент α^S также принадлежит полю L (ибо он сопряжен с α ; см. п. 2). Поэтому формула

$$\alpha^{S'} = \alpha^S, \quad \alpha \in L,$$

определяет некоторое преобразование S' поля L в себя. Легко видеть, что преобразование S' является автоморфизмом поля L над полем P , т. е. элементом группы Галуа $G(L, P)$ поля L над полем P . (Автоморфизмы S и S' действуют в поле L одинаково; различие между ними состоит в том, что автоморфизм S определен во всем поле K , а автоморфизм S' — только в поле L .)

Очевидно, что

$$(ST)' = S'T',$$

т. е. что соответствие

$$S \rightarrow S' \tag{1}$$

является гомоморфным отображением группы $G(K, P)$ в группу $G(L, P)$. Ядро этого отображения состоит из автоморфизмов S , оставляющих на месте каждый элемент поля L , т. е. ядром является группа Галуа $G(K, L)$ поля K над полем L . Так как ядро любого гомоморфизма является нормальным делителем, то, следовательно,

подгруппа группы Галуа $G(K, P)$, соответствующая нормальному промежуточному полю L (т. е. группа Галуа $G(K, L)$ поля K над полем L), является нормальным делителем группы $G(K, P)$.

Пусть теперь L — промежуточное поле, соответствующее произвольномуциальному делителю H группы $G(K, P)$, т. е. $L = K(G, H)$. Так как для любого автоморфизма $T \in H$

и любого автоморфизма $S \in G(K, P)$ автоморфизм STS^{-1} принадлежит H , то для любого числа $\alpha \in L$

$$\alpha^{STS^{-1}} = \alpha,$$

то есть

$$\alpha^{ST} = \alpha^S.$$

Так как T — произвольный автоморфизм из H , то отсюда следует, что $\alpha^S \in L$. Таким образом, все элементы, сопряженные каждому элементу $\alpha \in L$, принадлежат L , т. е. L нормально над P . Тем самым доказано, что

подполе $K(G, H)$ нормального поля K , соответствующее нормальному делителю H группы Галуа $G(K, P)$ поля K над полем P является нормальным расширением поля P .

Таким образом,

в соответствии Галуа нормальным подполям соответствуют нормальные делители, и обратно.

Вернемся теперь к рассмотрению гомоморфизма (1). Пусть G' — его образ, т. е. подгруппа группы $G(L, P)$, состоящая из автоморфизмов вида S' . Согласно теореме о гомоморфизмах (см. гл. 2, п. 4), гомоморфизм (1) индуцирует изоморфное отображение факторгруппы $G(K, P)/G(K, L)$ на группу G' . Следовательно, порядок группы G' равен индексу подгруппы $G(K, L)$ в группе $G(K, P)$. Но этот индекс равен (почему?) степени поля L над полем P , т. е. равен порядку группы $G(L, P)$. Таким образом, порядок подгруппы G' равен порядку всей группы $G(L, P)$, откуда следует, что $G' = G(L, P)$. Тем самым доказано, что отображение (1) эпиморфно. Индуцированный им гомоморфизм является, следовательно, изоморфным отображением факторгруппы $G(K, P)/G(K, L)$ на группу $G(L, P)$. Таким образом,

группа Галуа нормального промежуточного поля L над полем P изоморфна факторгруппе группы Галуа поля K над полем P по группе Галуа поля K над полем L .

7. Группа Галуа композита двух полей

Пусть нормальное расширение K поля P является композитом расширений K_1 и K_2 . В группе Галуа $G(K, P)$ подполю K_1 соответствует подгруппа $G(K, K_1)$, а подполю K_2 — подгруппа $G(K, K_2)$. Автоморфизмы из подгруппы $G(K, K_1)$ оставляют на месте все элементы поля K_1 , а авто-

морфизмы из подгруппы $G(K, K_2)$ оставляют на месте все элементы поля K_2 . Следовательно, любой автоморфизм из пересечения $G(K, K_1) \cap G(K, K_2)$ оставляет на месте любой элемент вида

$$\alpha_1\beta_1 + \dots + \alpha_r\beta_r, \quad (1)$$

где $\alpha_1, \dots, \alpha_r \in K_1$, $\beta_1, \dots, \beta_r \in K_2$. Но, согласно гл. 1, п. 9, элементами вида (1) исчерпываются все элементы композита K (результаты гл. 1, п. 9 применимы, так как поля K_1 и K_2 конечны над P). Следовательно, рассматриваемое пересечение содержит только тождественный автоморфизм. Таким образом,

если нормальное расширение K поля P является композитом расширений K_1 и K_2 , то

$$G(K, K_1) \cap G(K, K_2) = E. \quad (2)$$

Задача. Доказать обратное утверждение, т. е. доказать, что если нормальное поле K содержит подполя K_1 и K_2 , удовлетворяющие условию (2), то K является композитом полей K_1 и K_2 .

Предположим теперь, что поле K_1 нормально над полем P . Тогда его группа Галуа $G(K_1, P)$ является гомоморфным образом группы Галуа $G(K, P)$, причем ядром соответствующего эпиморфизма является группа $G(K, K_1)$ (см. п. 6). Из формулы (2) непосредственно следует, что этот эпиморфизм на подгруппе $G(K, K_2)$ является мономорфизмом. Другими словами, группа $G(K, K_2)$ изоморфна некоторой подгруппе группы $G(K_1, P)$. Таким образом,

если нормальное расширение K поля P является композитом нормального расширения K_1 и (вообще говоря, произвольного) расширения K_2 , то группа Галуа $G(K, K_2)$ изоморфна некоторой подгруппе группы $G(K_1, P)$.

II. РЕШЕНИЕ УРАВНЕНИЙ В РАДИКАЛАХ

ГЛАВА 1 ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ ИЗ ОБЩЕЙ ТЕОРИИ ГРУПП

1. Обобщение теоремы о гомоморфизмах

Пусть $\varphi: G \rightarrow G'$ — произвольный гомоморфизм и H' — некоторая подгруппа группы G' . Рассмотрим совокупность H всех элементов группы G , переходящих при гомоморфизме φ в элементы подгруппы H' . Таким образом, $g \in H$ тогда и только тогда, когда $\varphi(g) \in H'$.

Очевидно, что подмножество H является подгруппой группы G . Эта подгруппа обозначается через $\varphi^{-1}(H')$ и называется *полным прообразом* подгруппы H' при гомоморфизме φ . В этой терминологии ядро гомоморфизма φ есть не что иное, как полный прообраз единицы e' группы G' .

Легко видеть, что полный прообраз $H = \varphi^{-1}(H')$ нормального делителя H' группы G' является нормальным делителем группы G (доказать!). Так как $\varphi(H) \subset H'$, то определен индуцированный гомоморфизм

$$\bar{\varphi}: G/H \rightarrow G'/H'.$$

Без труда проверяется (см. ч. I, гл. 2, п. 4, где разобран случай $H' = e'$), что гомоморфизм $\bar{\varphi}$ является мономорфизмом. Таким образом,

для любого гомоморфизма $\varphi: G \rightarrow G'$ и любого нормального делителя $H' \subset G'$ индуцированный гомоморфизм

$$\bar{\varphi}: G/H \rightarrow G'/H',$$

где $H = \varphi^{-1}(H')$, является мономорфизмом; если отображение φ эпиморфно, то отображение φ изоморфно.

Если $H' = e'$, то это предложение сводится к доказанной ранее теореме о гомоморфизмах.

Задача. Доказать, что

1) подгруппа H группы G тогда и только тогда является полным прообразом некоторой подгруппы группы G' при гомоморфизме $\varphi: G \rightarrow G'$, когда

$$\text{Ker } \varphi \subset H;$$

2) если $\text{Ker } \varphi \subset H_1$ и $\text{Ker } \varphi \subset H_2$, то $\varphi(H_1) = \varphi(H_2)$ тогда и только тогда, когда $H_1 = H_2$;

3) если гомоморфизм φ является эпиморфизмом, то $\varphi^{-1}(H'_1) = \varphi^{-1}(H'_2)$ тогда и только тогда, когда $H'_1 = H'_2$.

Вывести отсюда, что эпиморфизм $\varphi: G \rightarrow G'$ определяет некоторое взаимно однозначное соответствие между множеством всех подгрупп группы G' и множеством тех подгрупп группы G , которые содержат ядро эпиморфизма φ .

2. Нормальные ряды

Пусть G — произвольная группа и G_1, G_2 — некоторые ее подгруппы, из которых вторая является погруппой первой:

$$G_1 \supseteq G_2.$$

Цепочка вложенных друг в друга подгрупп

$$G_1 = H_0 \supseteq H_1 \supseteq \dots \supseteq H_{t-1} \supseteq H_t \supseteq \dots \supseteq H_s = G_2, \quad (1)$$

начинающаяся с подгруппы G_1 и кончающаяся подгруппой G_2 , называется *нормальным рядом*, если для любого $i = 1, \dots, s$ подгруппа H_i является нормальным делителем подгруппы H_{i-1} (нормальным делителем по всей группе G подгруппа H_i может и не быть). Соответствующие факторгруппы H_{i-1}/H_i называются *факторами* нормального ряда (1).

Подчеркнем, что мы, вообще говоря, не требуем, чтобы нормальный ряд (1) не содержал повторений: вполне может быть, что для некоторого i подгруппа H_i совпадает с подгруппой H_{i-1} . Конечно, при желании можно из нормальных рядов удалять все повторяющиеся группы.

Особое значение имеют нормальные ряды

$$G = H_0 \supset H_1 \supset \dots \supset H_{t-1} \supset H_t \supset \dots \supset H_s = e, \quad (2)$$

начинающиеся с группы G и кончающиеся единичной подгруппой e . Такие нормальные ряды мы будем называть *нормальными рядами группы G* . Очевидно, что если группа G конечна, то для любого ее нормального ряда (2) все факторы H_{t-1}/H_t также конечны и

$$n = n_1 n_2 \dots n_s, \quad (3)$$

где n — порядок группы G , а n_l , $l = 1, \dots, s$ — порядок группы H_{t-1}/H_t . Обратно, если группа G обладает нормальным рядом с конечными факторами, то сама группа G также конечна и ее порядок n выражается через порядки n_1, \dots, n_s факторов нормального ряда согласно формуле (3).

Пусть теперь $\varphi: G \rightarrow G'$ — произвольный гомоморфизм. Очевидно, что если подгруппа H_2 группы G содержится в подгруппе H_1 :

$$H_1 \supset H_2,$$

то подгруппа $\varphi(H_2)$ группы G' содержит в подгруппе $\varphi(H_1)$:

$$\varphi(H_1) \supset \varphi(H_2).$$

Кроме того, если подгруппа H_2 является нормальным делителем в подгруппе H_1 , то подгруппа $\varphi(H_2)$ является нормальным делителем в подгруппе $\varphi(H_1)$ (доказать!). Следовательно, для любого нормального ряда

$$G_1 = H_0 \supset H_1 \supset \dots \supset H_{t-1} \supset H_t \supset \dots \supset H_s = G_2 \quad (4)$$

цепочка

$$\varphi(G_1) = \varphi(H_0) \supset \varphi(H_1) \supset \dots$$

$$\dots \supset \varphi(H_{t-1}) \supset \varphi(H_t) \supset \dots \supset \varphi(H_s) = \varphi(G_2) \quad (5)$$

является нормальным рядом. Если, в частности, $G_1 = G$ и $G_2 = e$ (т. е. если ряд (4) является нормальным рядом группы G), а отображение φ эпиморфно, то $\varphi(G_1) = G'$ и $\varphi(G_2) = e'$ (т. е. ряд (5) будет нормальным рядом группы G'). Таким образом,

произвольный эпиморфизм $\varphi: G \rightarrow G'$ переводит любой нормальный ряд

$$G = H_0 \supset H_1 \supset \dots \supset H_{t-1} \supset H_t \supset \dots \supset H_s = e \quad (6)$$

группы G в некоторый нормальный ряд

$$G' = \varphi(H_0) \supset \varphi(H_1) \supset \dots$$

$$\dots \supset \varphi(H_{t-1}) \supset \varphi(H_t) \supset \dots \supset \varphi(H_s) = e' \quad (7)$$

группы G' .

Заметим, что для любого $t = 1, \dots, s$ эпиморфизм φ индуцирует некоторый эпиморфизм

$$H_{t-1}/H_t \rightarrow \varphi(H_{t-1})/\varphi(H_t)$$

(ибо условия, при которых определен индуцированный гомоморфизм, очевидно, здесь выполнены). Следовательно,

факторы ряда (7) являются гомоморфными образами факторов ряда (6).

Пусть опять $\varphi: G \rightarrow G'$ — произвольный гомоморфизм. Очевидно, что если подгруппа H'_2 группы G' содержится в подгруппе H'_1 :

$$H'_1 \supset H'_2,$$

то подгруппа $\varphi^{-1}(H'_2)$ группы G содержится в подгруппе $\varphi^{-1}(H'_1)$:

$$\varphi^{-1}(H'_1) \supset \varphi^{-1}(H'_2).$$

Кроме того, если подгруппа H'_2 является нормальным делителем в подгруппе H'_1 , то подгруппа $\varphi^{-1}(H'_2)$ является нормальным делителем в подгруппе $\varphi^{-1}(H'_1)$. Следовательно, для любого нормального ряда

$$G'_1 = H'_0 \supset H'_1 \supset \dots \supset H'_{t-1} \supset H'_t \supset \dots \supset H'_s = G'_2 \quad (8)$$

цепочка

$$\varphi^{-1}(G'_1) = \varphi^{-1}(H'_0) \supset \varphi^{-1}(H'_1) \supset \dots$$

$$\dots \supset \varphi^{-1}(H'_{t-1}) \supset \varphi^{-1}(H'_t) \supset \dots \supset \varphi^{-1}(H'_s) = \varphi^{-1}(G'_2) \quad (9)$$

также является нормальным рядом. Если, в частности, $G'_1 = G'$ и $G'_2 = e'$ (т. е. если ряд (8) является нормальным рядом группы G'), а отображение φ мономорфно, то $\varphi^{-1}(G'_1) = G$ и $\varphi^{-1}(G'_2) = e$ (т. е. ряд (9) является нормальным рядом группы G). Таким образом,

при каждом мономорфизме $\varphi: G \rightarrow G'$ любому нормальному ряду

$$G' = H'_0 \supset H'_1 \supset \dots \supset H'_{t-1} \supset H'_t \supset \dots \supset H'_s = e' \quad (10)$$

группы G' соответствует некоторый нормальный ряд $G = \varphi^{-1}(H'_0) \supset \varphi^{-1}(H'_1) \supset \dots \supset \varphi^{-1}(H'_{t-1}) \supset \varphi^{-1}(H'_t) \supset \dots \supset \varphi^{-1}(H_s) = e$

$$\dots \supset \varphi^{-1}(H'_{t-1}) \supset \varphi^{-1}(H'_t) \supset \dots \supset \varphi^{-1}(H_s) = e \quad (11)$$

группы G .

Заметим, что для любого $t = 1, \dots, s$ мономорфизм φ индуцирует некоторый мономорфизм

$$\varphi^{-1}(H'_{t-1})/\varphi^{-1}(H'_t) \rightarrow H'_{t-1}/H'_t.$$

Следовательно,

факторы ряда (11) изоморфны подгруппам факторов ряда (10).

Пусть теперь G — произвольная группа и

$$G = H_0 \supset H_1 \supset \dots \supset H_{t-1} \supset H_t \supset \dots \supset H_s = e \quad (12)$$

— некоторый ее нормальный ряд. Предположим, что для любого $t = 1, \dots, s$ в соответствующей факторгруппе H_{t-1}/H_t задан нормальный ряд

$$H_{t-1}/H_t = K_{t0} \supset K_{t1} \supset \dots \supset K_{tj-1} \supset K_{tj} \supset \dots \supset K_{tu_t} = e. \quad (13)$$

Рассмотрим естественный эпиморфизм

$$\varphi_t: H_{t-1} \rightarrow H_{t-1}/H_t$$

(определенный формулой $\varphi_t(h) = H_t h$). При этом эпиморфизме ряду (13) соответствует нормальный ряд

$$H_{t-1} = \varphi_t^{-1}(K_{t0}) \supset \varphi_t^{-1}(K_{t1}) \supset \dots \supset \varphi_t^{-1}(K_{tj-1}) \supset \varphi_t^{-1}(K_{tj}) \supset \dots \supset \varphi_t^{-1}(K_{tu_t}) = H_t. \quad (14)$$

Вставив для каждого $t = 1, \dots, s$ между членами H_{t-1} и H_t ряда (12) ряд (14), мы, очевидно, снова получим нормальный ряд группы G . Этот нормальный ряд называется *уплотнением ряда (12) с помощью рядов (13)*.

Любой фактор этого ряда имеет вид

$$\varphi_i^{-1}(K_{ij-1})/\varphi_i^{-1}(K_{ij})$$

и потому, согласно обобщенной теореме о гомоморфизмах (см. п. 1), изоморфен факторгруппе

$$K_{ij-1}/K_{ij}.$$

Таким образом,

факторы уплотненного ряда изоморфны факторам уплотняющих рядов (13).

Так как любая непростая группа обладает нетривиальными (т. е. содержащими нетривиальные подгруппы) нормальными рядами, то любой нормальный ряд, имеющий хотя бы один непростой фактор, обладает нетривиальными (т. е. не сводящимися к повторениям) уплотнениями. Наоборот, если все факторы нормального ряда являются простыми группами, то все уплотнения этого нормального ряда сводятся к повторениям.

В заключение обратим внимание на определенный параллелизм между доказанными в этом пункте теоремами, относящимися к эпиморфизмам, и теоремами, относящимися к мономорфизмам. Весьма глубокие основания этого параллелизма мы здесь выяснить не можем.

3. Циклические группы

Группа G называется *циклической*, если все ее элементы являются степенями одного и того же элемента g_0 . Этот элемент g_0 называется *образующей* циклической группы G . Любая циклическая группа, очевидно, абелева.

Циклической группой является, например, группа целых чисел по сложению. Эту группу мы будем обозначать символом Z . Ее образующей является число 1 (а также число -1). Циклической группой является также группа, состоящая только из одного элемента (единицы).

В произвольной группе G степени g^n любого элемента g составляют циклическую подгруппу с образующей g . Порядок этой подгруппы, очевидно, совпадает с порядком элемента g . Отсюда в силу теоремы Лагранжа (см. стр. 32) следует, что *порядок любого элемента группы делит*

порядок группы (заметим, что все элементы конечной группы являются элементами конечного порядка). Поэтому

для любого элемента g конечной группы порядка n имеет место равенство

$$g^n = e.$$

Это простое замечание часто бывает полезно.

Заметим, далее, что

конечная группа G порядка n тогда и только тогда является циклической группой, когда она обладает элементом порядка n . Этот элемент является образующей.

Действительно, если группа G циклическая и g_0 — ее образующая, то порядок элемента g_0 равен n . Обратно, если группа G обладает элементом порядка n , то среди степеней этого элемента имеется n различных, и поэтому эти степени исчерпывают всю группу G .

Мы видим, таким образом, что циклическая группа может иметь несколько различных образующих (именно, любой элемент порядка n является образующей).

Задача. Доказать, что любая группа простого порядка является циклической группой.

Задача. Доказать, что циклическая группа порядка n имеет ровно $\phi(n)$ образующих, где $\phi(n)$ — число положительных чисел, меньших n и взаимно простых с n .

Наряду с порядком любой конечной группе можно отнести число \bar{n} — наименьшее общее кратное порядков всех ее элементов.

Задача. Доказать, что для любой конечной группы G число \bar{n} делит порядок группы.

Очевидно, что для циклической группы число \bar{n} совпадает с порядком. Обратное, вообще говоря, не верно. Тем не менее имеет место следующее утверждение, характеризующее циклические группы в классе конечных абелевых групп:

конечная абелева группа G , для которой число \bar{n} равно ее порядку n , является циклической группой.

Действительно, пусть

$$m_1, m_2, \dots, m_{n-1} \quad (1)$$

— порядки всевозможных отличных от единицы элементов конечной абелевой группы G порядка n , и пусть \bar{n} — их наименьшее общее кратное. Разложим число \bar{n} в произведение степеней различных простых чисел:

$$\bar{n} = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}.$$

Пусть $l = 1, 2, \dots, s$. Поскольку число \bar{n} является, по определению, наименьшим общим кратным чисел (1), среди этих чисел существует хотя бы одно число, делящееся точно на $p_l^{a_l}$, т. е. имеющее вид $b p_l^{a_l}$, где b взаимно просто с $p_l^{a_l}$. Пусть это число является порядком элемента g . Тогда элемент g^b имеет порядок $p_l^{a_l}$ (см. следствие 1) на стр. 29). Таким образом, для любого $l = 1, 2, \dots, s$ в группе G существует хотя бы один элемент порядка $p_l^{a_l}$. Выбрав для каждого $l = 1, 2, \dots, s$ один такой элемент, рассмотрим их произведение. Согласно утверждению, доказанному на стр. 29—30, порядок этого произведения равен произведению порядков $p_l^{a_l}$, т. е. равен числу \bar{n} . Поскольку последнее число по условию равно n , тем самым доказано, что в группе G существует элемент порядка n . Следовательно, эта группа является циклической группой.

Пусть теперь G — произвольная циклическая группа с образующей g_0 и H — некоторая ее подгруппа. Так как любой элемент подгруппы H является элементом группы G , то его можно представить в виде g_0^d , где d — некоторое положительное или отрицательное целое число (вообще говоря, определенное неоднозначно). Рассмотрим множество всех *положительных* чисел d , для которых элемент g_0^d принадлежит подгруппе H . Так как это множество непусто (почему?), то в нем существует наименьшее число d_0 . Оказывается, что любой элемент h подгруппы H является степенью элемента $g_0^{d_0}$. Действительно, по определению, существует такое число d , что $h = g_0^d$ (число d может быть и отрицательным). Разделим (с остатком) число d на число d_0 :

$$d = d_0 q + r, \quad 0 \leq r < d_0.$$

Так как $g_0^r = g_0^d (g_0^{d_0})^{-q} \in H$, то в силу минимальности числа d_0 остаток r должен быть равен нулю. Таким образом,

$d = d_0 q$ и $h = (g_0^{d_0})^q$. Тем самым доказано, что элемент $g_0^{d_0}$ является образующей группы H , т. е. что группа H цикличесна. Итак,

любая подгруппа циклической группы является циклической группой.

Задача. Доказать, что число d_0 равно индексу подгруппы H и, следовательно, делит порядок группы G (если группа G конечна).

Заметим еще, что

для любого делителя m порядка n конечной циклической группы G в группе G существует одна и только одна подгруппа H порядка m (а именно подгруппа с образующей $g_0^{n/m}$).

Отсюда вытекает, что

если конечная циклическая группа проста, то ее порядок является простым числом (или единицей).

Отметим наконец, что

любая факторгруппа G/H (и, следовательно, любой гомоморфный образ) циклической группы G является циклической группой.

Для доказательства достаточно заметить, что образующей группы G/H служит смежный класс Hg_0 , содержащий образующую g_0 группы G .

В частности, любая факторгруппа группы целых чисел Z является циклической группой. Изучим эти циклические группы более подробно.

Так как группа Z абелева, то любая ее подгруппа H является нормальным делителем. С другой стороны, согласно доказанному выше, подгруппа H является циклической группой. Так как факторгруппы по тривиальным подгруппам нам известны, то мы можем считать подгруппу H нетривиальной. Пусть число n является образующей подгруппы H . Мы можем считать это число положительным (почему?) и, следовательно, большим единицы.

Подгруппа H состоит, очевидно, из всех целых чисел, делящихся на n . Поэтому два числа тогда и только тогда принадлежат одному смежному классу по подгруппе H , когда их разность делится на n , т. е. когда они сравнимы по модулю n (см. Курс, стр. 277). Таким образом, смежные классы по подгруппе H суть не что иное, как классы чисел,

сравнимых между собой по модулю n . Другими словами, факторгруппа группы Z по подгруппе H является группой (по сложению) классов чисел, сравнимых между собой по модулю n . Мы будем эту группу обозначать через Z_n . Ее образующей является класс, содержащий число 1.

Оказывается, что

любая циклическая группа $G \neq e$ изоморфна либо группе Z (если она бесконечна), либо одной из групп Z_n (если ее порядок конечен).

Действительно, пусть g_0 — образующая группы G . Определим отображение φ группы Z в группу G , полагая

$$\varphi(a) = g_0^a, \quad a \in Z.$$

Из правил действий над степенями следует, что для любых чисел $a, b \in Z$ имеет место равенство

$$\varphi(a+b) = \varphi(a)\varphi(b),$$

т. е. отображение φ гомоморфно. Его образ $\varphi(Z)$ состоит из всех элементов группы G , являющихся степенями элемента g_0 , т. е. совпадает с группой G . Таким образом, группа G является гомоморфным образом группы Z и, следовательно, изоморфна некоторой ее факторгруппе, т. е. либо самой группе Z , либо одной из групп Z_n (мы предполагаем, что группа G не состоит только из единицы). Какой из групп Z_n изоморфна группа G , однозначно определяется тем, что изоморфные группы должны иметь одинаковый порядок.

Тем самым строение циклических групп полностью описано.

Важный пример циклических групп получается на основании следующих соображений.

Пусть n — произвольное целое положительное число. Как известно (см. Курс, стр. 127), существует точно n различных корней

$$\epsilon_0 = 1, \epsilon_1, \dots, \epsilon_{n-1}$$

степени n из единицы:

$$\epsilon_l^n = 1, \quad l = 0, 1, \dots, n - 1.$$

Произведение любых двух корней степени n из единицы и число, обратное к корню степени n из единицы, очевидно,

также являются корнями степени n из единицы. Следовательно, совокупность всех корней степени n из единицы является группой порядка n .

Известно (см. Курс, стр. 129), что любой корень степени n из единицы является степенью так называемого *первообразного корня*. Следовательно, группа всех корней степени n из единицы является циклической группой порядка n . Ее образующими служат первообразные корни и только они.

Задача. Построить изоморфное отображение группы корней степени n из единицы на группу Z_n .

4. Разрешимые и абелевы группы

Нормальный ряд

$$G = H_0 \supset H_1 \supset \dots \supset H_{l-1} \supset H_l \supset \dots \supset H_s = e \quad (1)$$

группы G называется *разрешимым рядом*, если для любого $i = 1, \dots, s$ факторгруппа H_{i-1}/H_i является циклической группой. Конечная группа, обладающая хотя бы одним разрешимым рядом, называется *разрешимой*; группа, не имеющая разрешимых рядов, называется *неразрешимой*. Примером разрешимой группы может, очевидно, служить любая конечная циклическая группа (разрешимый ряд состоит из группы G и единичной подгруппы e). Неразрешимой группой является, например, любая простая группа, если только она не является циклической (т. е. если ее порядок не является простым числом). Примеры таких групп будут построены ниже в главе 2.

Очевидно, что любое уплотнение разрешимого ряда также является разрешимым рядом (ибо как подгруппы, так и факторгруппы циклических групп являются циклическими группами). С другой стороны, любой нормальный ряд конечной группы может быть уплотнен до ряда с простыми факторами. Следовательно,

любая разрешимая группа обладает нормальным рядом, факторами которого служат циклические группы простых порядков (являющиеся делителями порядка группы).

Как мы знаем, любой эпиморфизм $\phi: G \rightarrow G'$ переводит нормальный ряд (1) группы G в некоторый нормальный ряд

группы G' , факторы которого являются гомоморфными образами факторов ряда (1). Так как гомоморфный образ циклической группы является циклической группой, то, следовательно, любой эпиморфизм $\varphi: G \rightarrow G'$ переводит разрешимый ряд группы G в разрешимый ряд группы G' . Таким образом,

любой гомоморфный образ разрешимой группы является разрешимой группой.

Пусть H — произвольная подгруппа разрешимой группы G . Определим отображение φ группы H в группу G , полагая

$$\varphi(h) = h, \quad h \in H$$

(отображение φ есть тождественное отображение группы H , рассматриваемое как отображение в большую группу G). Отображение φ является, очевидно, мономорфизмом. Следовательно, нормальному ряду (1) группы G в подгруппе H соответствует некоторый нормальный ряд (составленный из подгрупп $\varphi^{-1}(H_i) = H_i \cap H$), факторы которого изоморфны подгруппам факторов ряда (1). Так как любая подгруппа циклической группы является циклической группой, то отсюда следует, что

любая подгруппа разрешимой группы является разрешимой группой.

Из изложенного доказательства вытекает, что если разрешимая группа обладает разрешимым рядом длины s (т. е. рядом, состоящим из $s - 1$ членов), то и любая ее подгруппа также обладает разрешимым рядом длины s (напомним, что мы допускаем разрешимые ряды с повторениями).

Из доказанных двух теорем непосредственно вытекает, что

все факторы любого нормального ряда разрешимой группы являются разрешимыми группами.

Оказывается, что верно и обратное утверждение:

группа G , обладающая нормальным рядом с разрешимыми факторами, является разрешимой группой.

Действительно, пусть

$$G = H_0 \supset H_1 \supset \dots \supset H_{t-1} \supset H_t \supset \dots \supset H_s = e \quad (1)$$

— нормальный ряд группы G с разрешимыми факторами H_{t-1}/H_t . По определению, факторгруппа H_{t-1}/H_t для любого $t = 1, \dots, s$ обладает некоторым разрешимым рядом

$$H_{t-1}/H_t = K_{t0} \supset K_{t1} \supset \dots \supset K_{tj-1} \supset K_{tj} \supset \dots \supset K_{tl_t} = e'. \quad (2)$$

Уплотним ряд (1) с помощью рядов (2). Как мы знаем, факторы уплотненного ряда изоморфны факторам ряда (2) и, следовательно, являются циклическими группами. Другими словами, уплотненный ряд разрешим. Таким образом, группа G обладает разрешимым рядом, т. е. является разрешимой группой.

Частным случаем доказанной теоремы является следующее утверждение:

если группа G обладает разрешимым нормальным делителем H , факторгруппа G/H по которому разрешима, то и сама группа G также разрешима.

Действительно, условие, наложенное на группу G , означает, что она обладает нормальным рядом

$$G \supset H \supset e$$

с разрешимыми факторами. Следовательно, по только что доказанной теореме группа G разрешима.

Это предложение позволяет доказать следующее утверждение, существенно расширяющее запас известных нам примеров разрешимых групп:

любая конечная абелева группа G разрешима.

Доказательство мы проведем индукцией по порядку n группы G . Если $n = 1$, то группа G состоит только из единицы e и, следовательно, разрешима. Предположим, что уже доказана разрешимость любой конечной абелевой группы, имеющей порядок меньший, чем n , и рассмотрим произвольную абелеву группу G порядка n .

Пусть g — произвольный отличный от единицы элемент группы G . Так как $g \neq e$, то циклическая подгруппа H группы G с образующей g имеет порядок, больший единицы, и следовательно, порядок факторгруппы G/H меньше n (факторгруппу строить можно, ибо в абелевой группе любая подгруппа является нормальным делителем). Так как любая факторгруппа абелевой группы является абелевой группой (доказать!), то, следовательно, по предположению индукции, группа G/H разрешима. Таким образом, в группе G имеется разрешимый (даже циклический) нормальный делитель H , факторгруппа G/H по которому разрешима. Следовательно, по доказанной выше теореме группа G разрешима.

5. Группы Z'_n и M_n

Пусть n — произвольное целое положительное число. Рассмотрим множество Z'_n всех классов чисел, сравнимых между собой по модулю n . Класс, содержащий число a , мы будем обозначать через $[a]$ (в Курсе, стр. 227, этот класс обозначался через C_a). В множестве Z'_n , кроме сложения (относительно которого оно является, как мы знаем, циклической группой), можно определить также и умножение. Как и сложение, умножение классов сравнимых между собой чисел определяется по представителям:

$$[a][b] = [ab].$$

Это умножение, очевидно, коммутативно и ассоциативно. Кроме того, оно обладает единицей (именно единицей этого умножения служит класс $[1]$, содержащий число 1). Однако относительно этого умножения множество Z'_n группой не является, потому что, например, нулевой класс $[0]$ (состоящий из чисел, делящихся на n) не имеет обратного. Выясним, какие классы имеют обратные.

Пусть $[a]$ — произвольный класс по модулю n , для которого существует обратный класс, т. е. такой класс $[b]$, что

$$[a][b] = [1].$$

Тогда число $ab - 1$ делится на n , т. е. существует такое целое число k , что

$$ab + kn = 1.$$

Очевидно, что это равенство возможно только тогда, когда числа a и b взаимно просты с числом n . Таким образом, если для класса $[a]$ существует обратный класс, то число a взаимно просто с числом n .

Оказывается верно и обратное, так что
класс $[a]$ тогда и только тогда имеет обратный,
когда число a взаимно просто с числом n .

Докажем предварительно следующую лемму.

Лемма. Для любых целых чисел a и b существуют такие целые числа u и v , что

$$au + bv = d,$$

где d — наибольший общий делитель чисел a и b .

Для доказательства мы рассмотрим все числа, которые можно представить в виде

$$ax + by,$$

где x и y — произвольные целые числа (положительные или отрицательные). Пусть d — наименьшее из всех *положительных* чисел такого вида:

$$d = au + bv. \quad (1)$$

Разделим (с остатком) число a на число d :

$$a = dq + r, \quad 0 \leq r < d. \quad (2)$$

Из формул (1) и (2) вытекает, что

$$r = a(1 - qu) + b(-qv).$$

Отсюда в силу минимальности числа d следует, что $r = 0$, т. е. что a делится на d . Аналогично доказывается, что b делится на d . С другой стороны, ясно, что любой общий делитель чисел a и b делит число d . Следовательно, d является наибольшим общим делителем чисел a и b . Лемма полностью доказана.

Согласно этой лемме, если число a взаимно просто с числом n , то существуют такие целые числа u и v , что

$$au + nv = 1.$$

Переходя в этом равенстве к классам и учитывая, что $[nv] = [0]$, мы получим, что

$$[a][u] = [1].$$

Таким образом, класс $[u]$ обратен к классу $[a]$. Тем самым сформулированная выше теорема полностью доказана.

Из этой теоремы немедленно вытекает, что совокупность всех классов по модулю n , состоящих из взаимно простых с n чисел, является группой относительно умножения (очевидно, абелевой). Эта группа обозначается через Z'_n и называется *мультипликативной группой классов по модулю n* . Ее порядок равен числу $\varphi(n)$ всех положительных чисел, меньших n и взаимно простых с n .

Можно показать, что если, например, число n делится на два нечетных простых числа, то группа Z'_n не циклична.

Этот факт нам не понадобится, и мы его оставим без доказательства. Случай $n = p^a$ мы изучим позже (ч. III, гл. 3, п. 4).

Рассмотрим теперь множество всех пар вида (a, b) , где a и b — целые числа, причем число a взаимно просто с числом n . Разобьем это множество на классы, относя к одному классу пары (a, b) и (a_1, b_1) тогда и только тогда, когда число a сравнимо с числом a_1 по модулю n , а число b сравнимо с числом b_1 по модулю n . Класс, содержащий пару (a, b) , мы будем обозначать через $[a, b]$, а множество всех классов — через M_n .

Определим в множестве M_n алгебраическую операцию («умножение»), положив

$$[a, b][c, d] = [ac, bc + d].$$

Без труда проверяется, что эта формула действительно определяет в множестве M_n однозначную операцию, т. е. если $[a, b] = [a_1, b_1]$ и $[c, d] = [c_1, d_1]$, то $[ac, bc + d] = [a_1c_1, b_1c_1 + d_1]$.

Легко видеть, что относительно так определенного умножения множество M_n является группой. Единицей этой группы служит класс $[1, 0]$, а обратный элемент определяется формулой

$$[a, b]^{-1} = [\bar{a}, \bar{ab}],$$

где \bar{a} — такое число, что

$$[a][\bar{a}] = [1] \quad (\text{в группе } Z'_n).$$

Группа M_n как легко видеть, неabelева (если $n > 2$). Например,

$$[1, 2][a, 0] = [a, 2a],$$

$$[a, 0][1, 2] = [a, 2].$$

Задача. Доказать, что порядок группы M_n равен $n\varphi(n)$.

Непосредственно из определения группы M_n вытекает, что отображение $\Phi: M_n \rightarrow Z'_n$, определенное (как легко видеть, однозначно) формулой

$$\Phi[a, b] = [a],$$

является гомоморфизмом. Это отображение, очевидно, эпиморфно, и потому группа Z'_n изоморфна факторгруппе M_n/N_n группы M_n по ядру N_n отображения Φ .

Ядро N_n состоит, очевидно, из элементов вида $[1, b]$. Так как

$$[1, b][1, b_1] = [1, b + b_1],$$

то, сопоставив классу $[1, b]$ класс $[b]$, мы получим изоморфное отображение группы N_n на группу Z_n . Следовательно, ядро N_n является циклическим нормальным делителем группы M_n . Факторгруппа группы M_n по ядру N_n изоморфна, как мы видели, группе Z'_n и потому является абелевой и, следовательно, разрешимой группой. Таким образом, группа M_n обладает разрешимым (даже циклическим) нормальным делителем, факторгруппа по которому разрешима (даже абелева). Следовательно, группа M_n также разрешима.

ГЛАВА 2

УРАВНЕНИЯ, РАЗРЕШИМЫЕ В РАДИКАЛАХ

1. Простые радикальные расширения

Простым радикальным расширением поля P называется поле разложения K двучленного уравнения вида

$$x^n - a = 0, \quad \text{где } a \in P, \quad a \neq 0. \quad (1)$$

Как известно (см. Курс, стр. 128), все корни уравнения (1) получаются из одного умножением на корни степени n из единицы. Но любой корень степени n из единицы является степенью первообразного корня. Таким образом, если θ — произвольный корень уравнения (1), а ζ — некоторый первообразный корень степени n из единицы, то числа

$$\theta = \theta\zeta^0, \theta\zeta, \dots, \theta\zeta^{n-1} \quad (2)$$

исчерпывают все корни уравнения (1). Следовательно, поле $P(\zeta, \theta)$ содержит все корни уравнения (1), и потому

$$K \subset P(\zeta, \theta).$$

С другой стороны, поле K содержит числа θ и $\theta\zeta$ и потому содержит числа θ и $\zeta = \theta\zeta/\theta$. Следовательно,

$$P(\zeta, \theta) \subset K.$$

Таким образом,

$$K = P(\zeta, \theta).$$

Может случиться, что поле P уже содержит корень ζ . В этом случае простое радикальное расширение K имеет вид $P(\theta)$. Другой крайний случай возникает тогда, когда $a = 1$. В этом случае в качестве корня θ мы можем принять число 1, откуда следует, что $K = P(\zeta)$. (Заметим, что уравнение (1) неприводимым не предполагается.)

Являясь полем разложения, поле $K = P(\zeta, \theta)$ нормально, и поэтому мы можем говорить о его группе Галуа $G(K, P)$.

Пусть S — произвольный автоморфизм из группы Галуа $G(K, P)$. Так как число ζ является корнем многочлена $x^n - 1$, то число ζ^S также будет корнем этого многочлена (см. ч. I, гл. 3, п. 2). Следовательно, найдется такое число a , что

$$\zeta^S = \zeta^a. \quad (3)$$

Если бы число ζ^a было корнем многочлена $x^m - 1$, где $m < n$, то и число $\zeta = (\zeta^a)^{S^{-1}}$ также было бы корнем многочлена $x^m - 1$, т. е. было бы корнем из единицы степени $m < n$. Но это невозможно, так как по условию число ζ является первообразным корнем степени n из единицы. Следовательно, число ζ^a не может быть корнем из единицы степени m , меньшей n , т. е. является первообразным корнем степени n . Поэтому число a взаимно просто с числом n (см. Курс, стр. 129).

Далее, так как число θ является корнем уравнения (1), то и число θ^S также будет корнем уравнения (1), т. е. найдется такое число b , что

$$\theta^S = \zeta^b \theta. \quad (4)$$

Таким образом, каждому автоморфизму $S \in G(K, P)$ соответствует пара чисел a и b , причем число a взаимно просто с числом n . Это соответствие не однозначно, ибо, например, пара (a_1, b_1) , где числа a_1 и b_1 отличаются от чисел a и b на число, кратное n , также соответствует тому же автоморфизму S . Разберем этот вопрос подробнее.

Пусть пары (a, b) и (a_1, b_1) соответствуют одному и тому же автоморфизму S , т. е. пусть

$$\zeta^S = \zeta^a, \quad \zeta^S = \zeta^{a_1},$$

$$\theta^S = \zeta^b \theta, \quad \theta^S = \zeta^{b_1} \theta.$$

Тогда

$$\zeta^a = \zeta^{a_1}, \quad \zeta^b = \zeta^{b_1},$$

то есть

$$\zeta^{a-a_1} = 1, \quad \zeta^{b-b_1} = 1.$$

Так как ζ — первообразный корень степени n из единицы, то эти равенства возможны тогда и только тогда, когда

разности $a - a_1$ и $b - b_1$ делятся на n , т. е. когда числа a и b сравнимы по модулю n соответственно с числами a_1 и b_1 . Другими словами, пары (a, b) и (a_1, b_1) тогда и только тогда соответствуют одному и тому же автоморфизму $S \in G(K, P)$, когда эти пары принадлежат одному классу в смысле гл. 1, п. 5, т. е. определяют один и тот же элемент $[a, b]$ группы M_n . Таким образом, если мы каждому автоморфизму S из группы Галуа $G(K, P)$ отнесем элемент $[a, b]$ группы M_n , где числа a и b определяются из формул (3) и (4), то мы получим однозначное отображение группы $G(K, P)$ в группу M_n . Мы будем обозначать это отображение буквой φ :

$$\varphi(S) = [a, b].$$

Оказывается, что отображение φ гомоморфно. Действительно, если $\varphi(S) = [a, b]$ и $\varphi(T) = [c, d]$, т. е. если

$$\zeta^S = \zeta^a, \quad \theta^S = \zeta^b \theta,$$

$$\zeta^T = \zeta^c, \quad \theta^T = \zeta^d \theta,$$

то

$$\zeta^{ST} = (\zeta^a)^T = (\zeta^T)^a = \zeta^{ac},$$

$$\theta^{ST} = (\zeta^b \theta)^T = (\zeta^T)^b \theta^T = \zeta^{bc} \zeta^d \theta = \zeta^{bc+d} \theta.$$

Таким образом,

$$\varphi(ST) = [ac, bc + d],$$

то есть

$$\varphi(ST) = \varphi(S)\varphi(T).$$

Найдем ядро гомоморфизма φ . Если автоморфизм $S \in G(K, P)$ принадлежит ядру гомоморфизма φ , то

$$\zeta^S = \zeta, \quad \theta^S = \theta,$$

т. е. автоморфизм S оставляет на месте элементы ζ и θ . Следовательно, автоморфизм S оставляет на месте и любой многочлен (с коэффициентами из P) от элементов ζ и θ . Поэтому, поскольку любой элемент поля $K = P(\zeta, \theta)$ выражается в виде многочлена от ζ и θ , автоморфизм S оставляет на месте любой элемент поля K , т. е. $S = E$. Таким образом, ядро гомоморфизма φ состоит только из тождественного автоморфизма E , т. е. φ является мономорфизмом. Другими словами, φ осуществляет изоморфное отображение

группы $G(K, P)$ на некоторую подгруппу группы M_n . Так как группа M_n (а потому и любая ее подгруппа) разрешима, то отсюда вытекает, что

группа Галуа простого радикального расширения является разрешимой группой.

Если $\zeta \in P$, т. е. если $K = P(\theta)$, то образ мономорфизма φ содержится, очевидно, в подгруппе N_n группы M_n , состоящей из элементов вида $[1, b]$. Так как эта подгруппа изоморфна группе Z_n , то отсюда следует, что

если $\zeta \in P$, то группа Галуа простого радикального расширения $K = P(\theta)$ является циклической группой, порядок которой делит число n .

В «противоположном» случае, когда $a = 1$, т. е. когда $K = P(\zeta)$ и $\theta = 1$, образ мономорфизма φ содержится в подгруппе группы M_n , состоящей из всех элементов вида $[a, 0]$. Так как эта подгруппа изоморфна, очевидно, группе Z'_n , то отсюда следует, что

группа Галуа простого радикального расширения $K = P(\zeta)$ поля P , где ζ — первообразный корень степени n из единицы, изоморфна некоторой подгруппе группы Z'_n и потому абелева.

2. Циклические расширения

Нормальное расширение K поля P называется *циклическим расширением*, если его группа Галуа $G(K, P)$ является циклической группой. Примером циклического расширения может служить простое радикальное расширение, определяемое двучленным уравнением степени n , при условии, что основное поле P содержит первообразный корень степени n из единицы (см. п. 1). Степень m этого расширения, вообще говоря, меньше n . Равенство $m = n$ имеет место тогда и только тогда, когда уравнение (1) из п. 1, определяющее данное простое радикальное расширение, неприводимо.

Целью этого пункта является доказательство следующего «обратного» утверждения.

Если поле P содержит первообразный корень степени n из единицы, то любое его циклическое расширение K степени n является простым радикальным расширением, которое определяется неприводимым двучленным уравнением степени n .

Доказательству этого утверждения мы предпошлем несколько предварительных замечаний.

Пусть ζ — первообразный корень степени n из единицы, а S — некоторая образующая группы $G(K, P)$ (эта группа, по предположению, циклична, т. е. ее элементы исчерпываются степенями $S^0 = E, S^1, \dots, S^{n-1}$). Любому элементу α поля K отнесем элемент

$$(\zeta^t, \alpha) = \alpha + \zeta^t \alpha^S + \zeta^{2t} \alpha^{S^2} + \dots + \zeta^{(n-1)t} \alpha^{S^{n-1}},$$

т. е. элемент

$$(\zeta^t, \alpha) = \sum_{k=0}^{n-1} \zeta^{kt} \alpha^{S^k},$$

где t — некоторое целое число. Элемент (ζ^t, α) мы будем называть *резольвентой Лагранжа* элемента α , соответствующей числу t .

В первую очередь мы рассмотрим резольвенту

$$(\zeta, \alpha) = \alpha + \zeta \alpha^S + \zeta^2 \alpha^{S^2} + \dots + \zeta^{n-1} \alpha^{S^{n-1}},$$

соответствующую числу 1.

Так как $\alpha \in K$, то $P(\alpha) \subset K$. Следовательно, в соответствии Галуа полю $P(\alpha)$ отвечает некоторая подгруппа H группы $G(K, P)$ (именно, $H = G(K, P(\alpha))$). Являясь подгруппой циклической группы, группа H циклична. За ее образующую можно принять элемент S^d , где d — индекс подгруппы H . Так как $S^d \in H = G(K, P(\alpha))$, то $\alpha^{S^d} = \alpha$ и, следовательно, $\alpha^{S^{ld+j}} = \alpha^{S^j}$ для любых l и j . Поэтому, обозначая через $m = n/d$ порядок подгруппы H , мы получим, что

$$\begin{aligned} (\zeta, \alpha) &= \sum_{k=0}^{n-1} \zeta^k \alpha^{S^k} = \sum_{l=0}^{m-1} \sum_{j=0}^{d-1} \zeta^{ld+j} \alpha^{S^{ld+j}} = \\ &= \sum_{l=0}^{m-1} \sum_{j=0}^{d-1} \zeta^{ld+j} \alpha^{S^j} = \sum_{j=0}^{d-1} \zeta^j \alpha^{S^j} \sum_{l=0}^{m-1} \zeta^{ld}. \end{aligned}$$

Но если $d \neq n$, то $\zeta^d \neq 1$, и потому

$$\sum_{l=0}^{m-1} \zeta^{ld} = 1 + \zeta^d + \dots + \zeta^{(m-1)d} = \frac{1 - \zeta^{md}}{1 - \zeta^d} = \frac{1 - \zeta^n}{1 - \zeta^d} = 0,$$

ибо $\zeta^n = 1$. Таким образом, если $d \neq n$, то $(\zeta, \alpha) = 0$. Следовательно, если $(\zeta, \alpha) \neq 0$, то $d = n$. С другой стороны, равенство $d = n$ означает, что $H = E$, т. е. что $P(\alpha) = K$. Тем самым доказано, что

если $(\zeta, \alpha) \neq 0$, то $P(\alpha) = K$.

В связи с этим утверждением естественно возникает вопрос о существовании таких элементов $\alpha \in K$, что $(\zeta, \alpha) \neq 0$. (Следует иметь в виду, что из $P(\alpha) = K$ еще не вытекает, что $(\zeta, \alpha) \neq 0$.) Для ответа на этот вопрос мы воспользуемся теоремой, доказанной в ч. I, гл. 1, п. 7. Согласно этой теореме в поле K существует такой элемент θ , что

$$K = P(\theta).$$

Так как $[K : P] = n$, то θ является корнем неприводимого уравнения степени n . Мы покажем, что *хотя бы одна из резольвент*

$$(\zeta, \theta), (\zeta, \theta^2), \dots, (\zeta, \theta^{n-1}) \quad (1)$$

отлична от нуля.

Действительно, если все резольвенты (1) равны нулю, т. е. если

$$\begin{aligned} \theta + \zeta\theta^s + \dots + \zeta^{n-1}\theta^{s^{n-1}} &= 0, \\ \theta^2 + \zeta(\theta^2)^s + \dots + \zeta^{n-1}(\theta^2)^{s^{n-1}} &= 0, \\ \dots &\dots \dots \dots \dots \dots \dots \dots \\ \theta^{n-1} + \zeta(\theta^{n-1})^s + \dots + \zeta^{n-1}(\theta^{n-1})^{s^{n-1}} &= 0, \end{aligned}$$

то, поскольку

$$(\zeta, 1) = 1 + \zeta + \dots + \zeta^{n-1} = 0,$$

определитель

$$\left| \begin{array}{cccc} 1 & 1 & \dots & 1 \\ \theta & \theta^s & \dots & \theta^{s^{n-1}} \\ \theta^2 & (\theta^2)^s & \dots & (\theta^2)^{s^{n-1}} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ \theta^{n-1} & (\theta^{n-1})^s & \dots & (\theta^{n-1})^{s^{n-1}} \end{array} \right|$$

равен нулю (его столбцы линейно зависимы). С другой стороны, так как отображение S является автоморфизмом, то

$$(\theta^i)^{S^j} = (\theta^{S^j})^i \text{ для любых } i \text{ и } j.$$

Следовательно, написанный выше определитель можно переписать в следующем виде:

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ \theta & \theta^S & \dots & \theta^{S^{n-1}} \\ \theta^2 & (\theta^S)^2 & \dots & (\theta^{S^{n-1}})^2 \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ \theta^{n-1} & (\theta^S)^{n-1} & \dots & (\theta^{S^{n-1}})^{n-1} \end{vmatrix}. \quad (2)$$

Полученный определитель представляет собой определитель Вандермонда элементов $\theta, \theta^S, \dots, \theta^{S^{n-1}}$ (см. Курс, стр. 50). Как известно, он равен произведению всевозможных разностей этих элементов. Но мы знаем, что среди этих элементов нет одинаковых (ибо если $\theta^{S^i} = \theta^{S^j}$, то $S^i = S^j$; см. ч. I, гл. 3, п. 3). Поэтому определитель (2) отличен от нуля. Однако выше было показано, что он равен нулю. Полученное противоречие доказывает, что все резольвенты (1) не могут быть одновременно равны нулю.

Таким образом,

в поле K существует такой элемент α , что $(\zeta, \alpha) \neq 0$.

Рассмотрим теперь для элемента α с $(\zeta, \alpha) \neq 0$ резольвенту (ζ^t, α) , соответствующую произвольному целому числу t . Применяя к резольвенте

$$(\zeta^t, \alpha) = \alpha + \zeta^t \alpha^S + \zeta^{2t} \alpha^{S^2} + \dots + \zeta^{(n-1)t} \alpha^{S^{n-1}}$$

автоморфизм S и учитывая, что $\zeta^S = \zeta$ (ибо $\zeta \in P$), мы получим, что

$$(\zeta^t, \alpha)^S = \alpha^S + \zeta^t \alpha^{S^2} + \dots + \zeta^{(n-2)t} \alpha^{S^{n-1}} + \zeta^{(n-1)t} \alpha$$

(ибо $S^n = E$), т. е.

$$(\zeta^t, \alpha)^S = \zeta^{-t} (\zeta^t, \alpha) \quad (3)$$

(ибо $\zeta^{n-1} = \zeta^{-1}$). В частности,

$$(\zeta, \alpha)^S = \zeta^{-1} (\zeta, \alpha).$$

Возводя это равенство в t -ю степень и учитывая, что S является автоморфизмом, мы получим, что

$$((\zeta, \alpha)^t)^S = \zeta^{-t} (\zeta, \alpha)^t. \quad (4)$$

Разделив равенство (3) на равенство (4) (напомним, что по условию $(\zeta, \alpha) \neq 0$), мы получим, что

$$\left(\frac{(\zeta^t, \alpha)}{(\zeta, \alpha)^t} \right)^S = \frac{(\zeta^t, \alpha)}{(\zeta, \alpha)^t},$$

т. е. автоморфизм S оставляет на месте число

$$c_t = \frac{(\zeta^t, \alpha)}{(\zeta, \alpha)^t}.$$

Ясно, что любая степень автоморфизма S также оставляет число c_t на месте. Другими словами, любой элемент группы $G(K, P)$ (т. е. любой автоморфизм поля K над полем P) оставляет число c_t на месте (ибо вся группа $G(K, P)$ исчерпывается, по определению, степенями автоморфизма S), и следовательно, $c_t \in P$ (см. ч. I, гл. 3, п. 4). Тем самым доказано, что для любого t в поле P существует такой элемент c_t , что

$$(\zeta^t, \alpha) = c_t (\zeta, \alpha)^t.$$

Следовательно, все элементы (ζ^t, α) принадлежат полю $P(\beta)$, где $\beta = (\zeta, \alpha)$.

Найдем теперь сумму всех резольвент Лагранжа (ζ^t, α) для $t = 0, 1, \dots, n-1$. Имеем

$$\sum_{t=0}^{n-1} (\zeta^t, \alpha) = \sum_{t=0}^{n-1} \sum_{k=0}^{n-1} \zeta^{kt} \alpha^{S^k} = \sum_{k=0}^{n-1} \alpha^{S^k} \sum_{t=0}^{n-1} \zeta^{kt}. \quad (5)$$

Но если $\zeta^k \neq 1$, т. е. если $k \neq 0$, то

$$\sum_{t=0}^{n-1} \zeta^{kt} = \frac{\zeta^{kn} - 1}{\zeta^k - 1} = 0,$$

ибо $\zeta^n = 1$. Таким образом, в сумме (3) отличны от нуля только члены, соответствующие $k = 0$, т. е.

$$\sum_{t=0}^{n-1} (\zeta^t, \alpha) = n\alpha.$$

Поскольку $(\zeta^t, \alpha) \in P(\beta)$, из этой формулы следует, что $\alpha \in P(\beta)$, так что $P(\alpha) \subset P(\beta)$, т. е.

$$K \subset P(\beta),$$

ибо $K = P(\alpha)$.

Так как, с другой стороны, $P(\beta) \subset K$ (ибо $\beta \in K$), то

$$K = P(\beta).$$

Наконец, полагая в формуле (4) $t = n$ и учитывая, что $\zeta^n = 1$, мы получим, что

$$(\beta^n)^s = \beta^n,$$

откуда следует (см. выше аналогичные рассуждения для чисел c_t), что $\beta^n \in P$. Таким образом, полагая $c = \beta^n$, мы видим, что число β является корнем двучленного неприводимого (почему?) уравнения

$$x^n - c = 0, \text{ где } c \in P.$$

Тем самым доказано, что поле K является простым радикальным расширением, определяемым неприводимым двучленным уравнением, т. е. доказано сформулированное в начале этого пункта утверждение.

Строение циклических расширений в общем случае (когда основное поле P не содержит нужных корней из единицы) будет изучено в п. 4.

3. Радикальные расширения

Расширение K основного поля P называется *радикальным расширением*, если существует такая цепочка

$$P = L_0 \subset L_1 \subset \dots \subset L_{l-1} \subset L_l \subset \dots \subset L_s = K \quad (1)$$

вложенных друг в друга подполя K , начинающаяся с поля P и кончающаяся полем K , что для любого $l = 1, \dots, s$ поле L_l является простым радикальным расширением поля L_{l-1} . Цепочка (1) называется при этом *ради-*

кальным рядом. Подчеркнем, что радикальное расширение может обладать многими различными радикальными рядами.

Несмотря на то, что в радикальном ряду (1) каждое поле L_i является нормальным расширением поля L_{i-1} , все поле может не быть нормальным расширением поля P . Это связано с тем, что, вообще говоря, нормальное расширение нормального расширения не является нормальным расширением основного поля.

Условие, необходимое и достаточное для того, чтобы нормальное расширение нормального расширения было нормальным расширением основного поля, указывается следующей леммой.

Лемма. *Пусть P — произвольное поле, L — его нормальное расширение и K — нормальное расширение поля L . Оказывается, что поле K тогда и только тогда является нормальным расширением поля P , когда над полем P существует многочлен, полем разложения которого над полем L является поле K .*

Действительно, если поле K нормально над полем P , то существует такой многочлен $f(x)$ с коэффициентами из поля P , что

$$K = P(\alpha_1, \dots, \alpha_n),$$

где $\alpha_1, \dots, \alpha_n$ — все корни многочлена $f(x)$. Тогда

$$K \subset L(\alpha_1, \dots, \alpha_n)$$

(ибо $P \subset L$), а с другой стороны,

$$L(\alpha_1, \dots, \alpha_n) \subset K$$

(ибо $L \subset K$ и $\alpha_1, \dots, \alpha_n \in K$). Следовательно,

$$K = L(\alpha_1, \dots, \alpha_n),$$

т. е. K является полем разложения многочлена $f(x)$ над полем L .

(Заметим, что нормальность поля L мы в этом рассуждении не использовали.)

Обратно, пусть

$$K = L(\alpha_1, \dots, \alpha_n),$$

где $\alpha_1, \dots, \alpha_n$ — все корни некоторого многочлена $f(x)$ над полем P . Так как поле L , по условию, нормально над P ,

то существует такой многочлен $g(x)$ с коэффициентами из поля P , что

$$L = P(\beta_1, \dots, \beta_m),$$

где β_1, \dots, β_m — все корни многочлена $g(x)$. Тогда

$$K = P(\beta_1, \dots, \beta_m, \alpha_1, \dots, \alpha_n). \quad (2)$$

Так как числа $\beta_1, \dots, \beta_m, \alpha_1, \dots, \alpha_n$ исчерпывают все корни многочлена $g(x)f(x)$, то равенство (2) означает, что поле K является полем разложения многочлена $g(x)f(x)$ с коэффициентами из поля P и, следовательно, является нормальным расширением поля P . Тем самым лемма полностью доказана.

Мы будем называть поле K *нормальным радикальным расширением* поля P , если оно является нормальным и одновременно радикальным расширением этого поля. Связь нормальных радикальных расширений с произвольными радикальными расширениями описывается следующей теоремой.

Любое радикальное расширение K поля P содержится в некотором нормальном радикальном расширении \bar{K} .

Мы докажем эту теорему индукцией по длине s радикального ряда (1), которым обладает радикальное расширение K . Если $s=1$, то K является простым радикальным, а потому и нормальным расширением поля P . Поэтому в этом случае за поле \bar{K} можно принять само поле K .

Предполагая теперь, что теорема уже доказана для всех радикальных расширений, обладающих радикальными рядами длины $s-1$, рассмотрим радикальное расширение K с радикальным рядом (1) длины s . Так как поле $L = L_{s-1}$ является радикальным расширением поля P с радикальным рядом длины $s-1$, то, по предположению индукции, существует нормальное радикальное расширение \bar{L} , содержащее поле L :

$$L \subset \bar{L}.$$

По условию поле $K = L_s$ является простым радикальным расширением поля $L = L_{s-1}$, т. е.

$$K = L(\zeta, \theta),$$

где ζ — первообразный корень из единицы некоторой степени n , а θ — произвольный корень уравнения

$$x^n - \beta = 0, \text{ где } \beta \in L.$$

Рассмотрим минимальный многочлен $g(x)$ числа β над полем P . Так как поле \bar{L} нормально и $\beta \in L \subset \bar{L}$, то \bar{L} содержит все корни $\beta_1 = \beta, \beta_2, \dots, \beta_r$ многочлена $g(x)$. Для любого $i = 1, \dots, r$ рассмотрим уравнение

$$x^n - \beta_i = 0.$$

Пусть α_i — произвольный корень этого уравнения (для $i = 1$ положим $\alpha_1 = \theta$), и пусть

$$\bar{K} = \bar{L}(\zeta, \alpha_1, \dots, \alpha_r).$$

Так как $\alpha_1 = \theta$, то поле \bar{K} содержит поле K :

$$K \subset \bar{K}.$$

Далее, над полем \bar{L} поле \bar{K} обладает радикальным рядом

$$\bar{L} = \bar{L}_0 \subset \bar{L}_1 \subset \dots \subset \bar{L}_{t-1} \subset \bar{L}_t \subset \dots \subset \bar{L}_r = \bar{K}, \quad (3)$$

где

$$\bar{L}_t = \bar{L}_{t-1}(\zeta, \alpha_t), \quad t = 1, \dots, r$$

(при $t > 1$ можно даже считать, что $\bar{L}_t = \bar{L}_{t-1}(\alpha_t)$, ибо $\zeta \in \bar{L}_1 \subset \bar{L}_{t-1}$). По условию поле \bar{L} является радикальным расширением поля P , т. е. обладает радикальным рядом, начинающимся с поля P и кончающимся полем \bar{L} . Продолжая этот ряд рядом (3), мы, очевидно, получим радикальный ряд поля \bar{K} , начинающийся с поля P . Тем самым доказано, что поле \bar{K} является радикальным расширением поля P .

Наконец, рассмотрим многочлен $G(x) = g(x^n)$. Коэффициенты этого многочлена принадлежат полю P . Так как

$$G(x) = (x^n - \beta_1) \dots (x^n - \beta_r),$$

то числа $\alpha_1, \dots, \alpha_r$ являются корнями многочлена $G(x)$. Все остальные корни этого многочлена получаются из корней $\alpha_1, \dots, \alpha_r$ умножением на корни из единицы степени n , т. е. умножением на степени первообразного корня ζ . Поэтому поле \bar{K} содержит все корни многочлена $G(x)$, т. е. содержит его поле разложения Q над полем \bar{L} . С другой стороны, $\bar{L} \subset Q$ и $\alpha_1, \dots, \alpha_r \in Q$, так что $\bar{K} = \bar{L}(\alpha_1, \dots, \alpha_r) \subset Q$. Следовательно, $\bar{K} = Q$, т. е. \bar{K} является полем разложения над полем \bar{L} многочлена $G(x)$. Поскольку поле \bar{L} является

нормальным расширением поля P , а многочлен $G(x)$ является многочленом над полем P , то отсюда, согласно лемме, следует, что поле \bar{K} нормально над полем P .

Таким образом, мы нашли поле \bar{K} , содержащее поле K и являющееся нормальным радикальным расширением поля P . Тем самым сформулированная выше теорема полностью доказана.

4. Нормальные поля с разрешимой группой Галуа

Пусть K — произвольное нормальное радикальное расширение поля P . В его группе Галуа $G(K, P)$ радикальному ряду

$$P = L_0 \subset L_1 \subset \dots \subset L_{t-1} \subset L_t \subset \dots \subset L_s = K$$

соответствует ряд подгрупп

$$G(K, P) = H_0 \supset H_1 \supset \dots \supset H_{t-1} \supset H_t \supset \dots \supset H_s = E, \quad (1)$$

где

$$H_t = G(K, L_t), \quad t = 1, \dots, s.$$

Для любого $t = 1, \dots, s$ рассмотрим тройку полей

$$L_{t-1} \subset L_t \subset K.$$

Так как поле L_t является нормальным расширением поля L_{t-1} , то группа $H_t = G(K, L_t)$ будет нормальным делителем группы $H_{t-1} = G(K, L_{t-1})$. Таким образом, ряд (1) является нормальным рядом.

Далее, факторгруппа H_{t-1}/H_t изоморфна группе Галуа $G(L_t, L_{t-1})$ поля L_t над полем L_{t-1} , которая, как мы знаем, разрешима (ибо поле L_t есть простое радикальное расширение поля L_{t-1}). Таким образом, ряд (1) является нормальным рядом с разрешимыми факторами. Существование такого ряда обеспечивает, как мы знаем (см. гл. 1, п. 4), разрешимость группы $G(K, P)$. Таким образом,

группа Галуа любого нормального радикального расширения разрешима.

Пусть теперь Q — произвольное нормальное подполе поля K (как всегда предполагается, что Q содержит основное поле P). Тогда группа Галуа $G(Q, P)$ поля Q над полем P изоморфна, как мы знаем, некоторой факторгруппе группы

$G(K, P)$. Так как любая факторгруппа разрешимой группы является разрешимой группой, то, следовательно,

группа Галуа любого нормального под поля произвольного нормального радикального расширения является разрешимой группой.

Оказывается, что верно и обратное:

любое нормальное поле, имеющее разрешимую группу Галуа, является под полем некоторого нормального радикального расширения.

Другими словами, нормальными под полями нормальных радикальных расширений исчерпываются все нормальные поля с разрешимой группой Галуа.

Мы докажем это утверждение сначала для циклических полей, т. е. для нормальных полей, имеющих циклическую группу Галуа.

Пусть Q — нормальное расширение поля P степени m с циклической группой Галуа $G(Q, P)$.

Рассмотрим поле

$$K = Q(\epsilon),$$

где ϵ — первообразный корень из единицы степени m . Легко видеть, что поле K нормально над полем P (доказать!). Так как поле K является композитом нормальных полей $P(\epsilon)$ и Q , то, согласно теореме ч. I, гл. 3, п. 7, группа Галуа $G(K, P(\epsilon))$ изоморфна некоторой подгруппе группы Галуа $G(Q, P)$. Так как группа $G(Q, P)$ по условию циклическа, а любая подгруппа циклической группы является циклической группой, то, следовательно, группа $G(K, P(\epsilon))$ является циклической группой. Ее порядок $n = [K : P(\epsilon)]$ делит число m , и потому первообразный корень ζ из единицы степени n является степенью корня ϵ , т. е. принадлежит полю $P(\epsilon)$:

$$\zeta \in P(\epsilon).$$

Таким образом, поле K является циклическим расширением степени n поля $P(\epsilon)$, содержащим первообразный корень степени n из единицы. Поэтому, согласно теореме п. 2, поле K является простым радикальным расширением поля $P(\epsilon)$. Поскольку последнее является простым радикальным расширением поля P , тем самым доказано, что поле K представляет собой (по построению, нормальное) радикальное расширение поля P . Итак, доказано, что любое цикли-

ческое расширение Q поля P содержится в некотором нормальном радикальном расширении.

Перейдем теперь к общему случаю. Пусть Q — нормальное расширение поля P , имеющее разрешимую группу Галуа $G(Q, P)$, и пусть

$$G(Q, P) = H_0 \supset H_1 \supset \dots \supset H_{l-1} \supset H_l \supset \dots \supset H_s = E \quad (2)$$

— произвольный разрешимый ряд группы $G(Q, P)$. Если $s = 1$, то группа $G(Q, P)$ циклична и, следовательно, согласно доказанному выше, поле Q содержится в некотором нормальном радикальном расширении поля P . Предполагая теперь, что теорема уже доказана для нормальных полей, имеющих разрешимую группу Галуа с разрешимым рядом длины $s - 1$, рассмотрим нормальное поле Q , имеющее разрешимую группу Галуа с разрешимым рядом (2) длины s . В этом поле подгруппе H_1 группы Галуа соответствует некоторое подполе

$$L = K(G, H_1).$$

Поле L нормально над полем P , и его группа Галуа $G(L, P)$ изоморфна факторгруппе $G(Q, P)/H_1$, т. е. является циклической группой. Следовательно, согласно уже доказанному, поле L содержится в некотором нормальном радикальном расширении \bar{L} поля P . Рассмотрим композит \bar{Q} полей Q и \bar{L} . Как мы знаем (см. ч. I, гл. 3; п. 7), группа Галуа $G(\bar{Q}, \bar{L})$ композита \bar{Q} над полем \bar{L} изоморфна некоторой подгруппе группы Галуа $G(Q, L)$ поля Q над полем L (за основное поле мы принимаем здесь поле L). Но $G(Q, L) = H_1$ и, следовательно, группа $G(Q, \bar{L})$, а потому и любая ее подгруппа (см. гл. 1, п. 4), обладает разрешимым рядом длины $s - 1$. Поэтому, по предположению индукции, поле \bar{Q} , а значит и поле Q , содержится в некотором нормальном радикальном расширении K поля \bar{L} . Так как поле \bar{L} является по построению радикальным расширением поля P , то поле K будет радикальным расширением поля P . Далее, как мы знаем, радикальное расширение K содержится в некотором нормальном радикальном расширении \bar{K} (быть может, совпадающем с K).

Таким образом, мы нашли нормальное радикальное расширение \bar{K} поля P , содержащее данное нормальное расширение Q с разрешимой группой Галуа. Тем самым сформулированная выше теорема полностью доказана.

5. Уравнения, разрешимые в радикалах

Говорят, что корень θ уравнения

$$f(x) = 0 \quad (1)$$

над полем P выражается в радикалах, если существует радикальное расширение поля P , содержащее корень θ , т. е. если вычисление корня θ сводится к четырем арифметическим действиям и решению цепи двучленных уравнений. Если все корни уравнения (1) выражаются в радикалах, то говорят, что это уравнение *решается в радикалах*.

Оказывается, что

если хотя бы один корень неприводимого уравнения выражается в радикалах, то уравнение решается в радикалах.

Действительно, пусть корень θ уравнения (1) принадлежит радикальному расширению K поля P . Как мы знаем, радикальное расширение K можно расширить до некоторого нормального радикального расширения \bar{K} . Так как нормальному полю \bar{K} принадлежит один корень неприводимого уравнения (1), то ему должны принадлежать и все остальные корни. Таким образом, каждый корень уравнения (1) лежит в радикальном расширении \bar{K} , т. е. выражается в радикалах.

Нормальное радикальное расширение \bar{K} , содержащее все корни уравнения (1), содержит и его поле разложения. Следовательно, если неприводимое уравнение решается в радикалах, то его поле разложения содержитя в некотором нормальном радикальном расширении поля P . Очевидно и обратное, если поле разложения уравнения (1) содержитя в нормальном радикальном расширении, то уравнение (1) разрешимо в радикалах. Но, как мы видели в предыдущем пункте, нормальное поле тогда и только тогда содержитя в некотором нормальном радикальном расширении, когда его группа Галуа разрешима. Следовательно,

неприводимое уравнение тогда и только тогда разрешимо в радикалах, когда группа Галуа его поля разложения разрешима.

Принято группу Галуа поля разложения некоторого уравнения называть *группой Галуа этого уравнения*. В этой

терминологии доказанная теорема звучит следующим образом:

неприводимое уравнение тогда и только тогда разрешимо в радикалах, когда его группа Галуа разрешима.

Задача. Доказать эту теорему для приводимых уравнений. (Указание: предварительно доказать, что композит радикальных расширений является радикальным расширением.)

Подчеркнем, что доказанные в этой главе теоремы позволяют для любого уравнения с разрешимой группой Галуа эффективно построить радикальное расширение, содержащее его корни, т. е. эффективно выразить его корни через радикалы. (Пример такого построения см. ниже, гл. 4, п. 4.)

ГЛАВА 3

ПОСТРОЕНИЕ УРАВНЕНИЙ, НЕРАЗРЕШИМЫХ В РАДИКАЛАХ

1. Группа Галуа уравнения как группа подстановок

Напомним (см. Курс, стр. 30), что *подстановкой* называется взаимно однозначное отображение некоторого конечного множества M на себя. Число n элементов этого множества называется *степенью* подстановки. Так как природа элементов множества M не играет в дальнейшем никакой роли, то мы можем считать, что множество M состоит из чисел $1, 2, \dots, n$.

Если при данной подстановке a число j переходит в число t_j , то подстановку обозначают символом

$$a = \begin{pmatrix} 1 & 2 & \dots & n \\ t_1 & t_2 & \dots & t_n \end{pmatrix}.$$

В этой записи числа $1, 2, \dots, n$ можно произвольным образом переставлять (соответственно переставляя числа t_1, t_2, \dots, t_n): если j_1, j_2, \dots, j_n — произвольная перестановка чисел $1, 2, \dots, n$, то символ

$$\begin{pmatrix} j_1 & j_2 & \dots & j_n \\ t_{j_1} & t_{j_2} & \dots & t_{j_n} \end{pmatrix}$$

обозначает ту же подстановку a .

Результат последовательного выполнения двух подстановок a и b (одной и той же степени) также, очевидно, является подстановкой. Эта подстановка называется *произведением* подстановок a и b и обозначается через ab . Подчеркнем, что подстановка ab получается при выполнении сначала

подстановки a , а затем подстановки b . Это замечание существенно, так как при $n > 2$ умножение подстановок некоммутативно.

Легко видеть, что умножение подстановок ассоциативно (см. Курс, стр. 34). При умножении любой подстановки a на тождественную подстановку

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

подстановка a не меняется:

$$ea = ae = a.$$

Кроме того, произведение (в любом порядке) подстановки

$$a = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

на подстановку

$$a^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix} \quad (1)$$

является тождественной подстановкой

$$a^{-1}a = aa^{-1} = e.$$

Все сказанное означает, что совокупность S_n всех подстановок степени n является группой.

Единицей этой группы служит подстановка e , а подстановка, обратная некоторой подстановке a , определяется формулой (1).

Группа S_n называется симметрической группой n -й степени. Ее порядок равен $n!$.

Подгруппы симметрической группы S_n называются группами подстановок степени n . Другими словами, группой подстановок (степени n) называется группа, элементами которой являются подстановки одной и той же степени n , а операцией — умножение подстановок.

После этих предварительных замечаний вернемся к группам Галуа уравнений.

Пусть $f(x)$ — произвольный многочлен над основным полем P . Как мы уже говорили, группой Галуа многочлена $f(x)$

(или уравнения $f(x) = 0$) называется группой Галуа $G(Q, P)$ его поля разложения Q , т. е. поля

$$Q = P(\alpha_1, \dots, \alpha_n),$$

где $\alpha_1, \dots, \alpha_n$ — все корни многочлена $f(x)$ (пронумерованные в некотором определенном порядке). Мы будем предполагать, что многочлен $f(x)$ не имеет кратных корней (что, очевидно, не уменьшает общности). Как мы знаем (см. ч. I, гл. 3, п. 2), для любого автоморфизма $S \in G(Q, P)$ и любого корня α_i многочлена $f(x)$ число α_i^S также является корнем этого многочлена, т. е. существует такой индекс k_i , что

$$\alpha_i^S = \alpha_{k_i}.$$

Так как автоморфизм S является взаимно однозначным отображением, а все корни $\alpha_1, \dots, \alpha_n$ различны, то $k_i \neq k_j$, если $i \neq j$. Следовательно, символ

$$\begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$$

является символом некоторой подстановки a степени n . Чтобы подчеркнуть зависимость подстановки a от автоморфизма, мы будем обозначать эту подстановку через $\varphi(S)$. Таким образом, φ будет некоторым отображением группы $G(Q, P)$ в симметрическую группу S_n . Очевидно, что для любых двух автоморфизмов $S, T \in G(Q, P)$ имеет место равенство

$$\varphi(ST) = \varphi(S)\varphi(T),$$

т. е. отображение φ является гомоморфизмом. Ядро этого гомоморфизма состоит из автоморфизмов, оставляющих на месте каждый из корней $\alpha_1, \dots, \alpha_n$. Но если автоморфизм поля Q над полем P оставляет на месте все корни $\alpha_1, \dots, \alpha_n$, то он оставляет на месте и любой элемент, выражющийся в виде многочлена (с коэффициентами из поля P) от $\alpha_1, \dots, \alpha_n$, т. е. оставляет на месте любой элемент поля $Q = P(\alpha_1, \dots, \alpha_n)$. Следовательно, ядро гомоморфизма φ состоит только из тождественного автоморфизма E , т. е. φ является мономорфизмом. Другими словами, φ осуществляет изоморфное отображение группы Галуа $G(Q, P)$ на некоторую группу подстановок. Таким образом, группу Галуа

любого уравнения (не имеющего кратных корней) можно рассматривать как группу подстановок. Степень этой группы подстановок равна степени уравнения.

Заметим, что мономорфизм φ (а потому и его образ $\text{Im } \varphi$) существенно зависит от нумерации корней многочлена $f(x)$. Поэтому, рассматривая группу Галуа некоторого многочлена как группу подстановок, мы не должны менять первоначально введенной нумерации корней.

§ 2. Разложение подстановок в произведение циклов

Пусть

$$a = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix}$$

— произвольная подстановка степени n . Если для некоторого i число k_i отлично от i , то говорят, что подстановка a действительно *перемещает* число i ; в противном случае говорят, что подстановка a оставляет число i на месте.

Рассмотрим циклическую подгруппу группы S_n , состоящую из степеней подстановки a . Если m — порядок этой подгруппы, то она состоит из подстановок

$$a^0 = e, \quad a, \quad a^2, \quad \dots, \quad a^{m-1},$$

причем все эти подстановки различны. Пусть i_0 — произвольное действительно перемещаемое подстановкой a число. Обозначим через i_k число, в которое переводит число i_0 подстановка a^k . Очевидно, что подстановка a переводит число i_k в число i_{k+1} . Если бы оказалось, что $i_k = i_{k+1}$, то, применив к этому равенству подстановку a^{-k} , мы получили бы, что $i_0 = i_1$, т. е. что подстановка a оставляет, вопреки предположению, число i_0 на месте. Следовательно, все числа i_0, i_1, \dots действительно перемещаются подстановкой a . Среди этих чисел имеется не более m различных, ибо i_m , очевидно, равно i_0 . Если числами

$$i_0, \quad i_1, \quad \dots, \quad i_{m-1}$$

исчерпываются все числа, действительно перемещаемые подстановкой a , то подстановка a называется *циклом* и обозначается символом $(i_0 i_1 \dots i_{m-1})$.

В этом случае все числа i_0, i_1, \dots, i_{m-1} различны.

Действительно, если, например, $l_k = l_{k+l}$, где $0 \leq k + l \leq m - 1$, $l > 0$, $k \geq 0$, то, применяя к этому равенству подстановку a^{-k} , мы получили бы, что $l_0 = l_l$, т. е. что подстановка a^l оставляет число l_0 на месте. Но для любого q подстановка a^{-q} переводит число l_q в число l_0 , подстановка a^l оставляет число l_0 на месте и подстановка a^q переводит число l_0 в число l_q . Следовательно, подстановка $a^l = a^{-q}a^l a^q$ оставляет на месте любое число l_q , т. е., согласно условию, любое число, действительно перемещаемое подстановкой a . С другой стороны, любое число, оставляемое подстановкой a на месте, подстановка a^l также оставляет на месте. Следовательно, подстановка a^l оставляет на месте все числа, т. е. $a^l = e$, что невозможно, ибо $l < m$.

Заметим, что для любой системы l_0, l_1, \dots, l_{m-1} различных чисел существует цикл (очевидно, единственный), переводящий число l_0 в число l_1 , число l_1 в число l_2, \dots , число l_{m-2} в число l_{m-1} и, наконец, число l_{m-1} в число l_0 . Этот цикл представляется символом

$$(l_0 \dots l_{m-1}) = \begin{pmatrix} l_0 & l_1 & \dots & l_{m-1} & j_1 & \dots & j_{n-m} \\ l_1 & l_2 & \dots & l_0 & j_1 & \dots & j_{n-m} \end{pmatrix},$$

где j_1, \dots, j_{n-m} — все числа из ряда 1, 2, ..., n , отличные от чисел l_0, \dots, l_{m-1} .

Заметим еще, что запись цикла в виде $(l_0 l_1 \dots l_{m-1})$ неоднозначна. Именно

$$(l_0 l_1 \dots l_{m-1}) = (l_1 \dots l_{m-1} l_0) = \dots = (l_{m-1} l_0 l_1 \dots l_{m-2}),$$

т. е. запись цикла можно начинать с любого действительно перемещаемого им числа. С точностью до преобразований такого рода запись цикла, как легко видеть, однозначна.

Количество m чисел, действительно перемещаемых циклом a , называется его *длиной*. Из сказанного выше ясно, что *длина цикла равна его порядку*.

Наименьшая возможная длина цикла равна двум. Циклы длины два называются *транспозициями*. Транспозиция (lj) переводит число l в число j , число j — в число l и оставляет все остальные числа на месте.

Задача. Доказать, что подстановка, действительно перемещающая только два числа, является транспозицией.

Любой цикл длины m является произведением $m - 1$ транспозиций.

Действительно,

$$(l_0 l_1 l_2 \dots l_{m-1}) = (l_0 l_1) (l_0 l_2) \dots (l_0 l_{m-1}).$$

Два цикла называются *независимыми*, если они не имеют общих действительно перемещаемых чисел. Очевидно, что при перемножении независимых циклов порядок множителей не играет никакой роли (т. е. независимые циклы, как говорят, *перестановочны*).

Оказывается, что

любая не тождественная подстановка является произведением независимых циклов.

Мы докажем это утверждение индукцией по числу s действительно перемещаемых чисел. С этой целью заметим, во-первых, что число s не может быть равно единице. Действительно, если подстановка a переводит число i в число $j \neq i$, то число j она не может оставлять на месте, так как в противном случае два различных числа i и j переводились бы подстановкой a в одно и то же число j . Поэтому $s \geq 2$. Если $s = 2$, то подстановка является транспозицией, и следовательно, теорема для нее справедлива. Тем самым начальный этап индукции обоснован.

Предположим теперь, что теорема уже доказана для всех подстановок, действительно перемещающих менее s чисел, и рассмотрим произвольную подстановку a , действительно перемещающую s чисел. Пусть l_0 — одно из чисел, действительно перемещаемых подстановкой a . Применяя к этому числу изложенное выше построение (т. е. воздействуя на него степенями подстановки a), мы получим числа $l_0, l_1, \dots, l_k, \dots$, действительно перемещаемые подстановкой a (см. выше). Пусть l_q — первое из этих чисел с положительным номером, совпадающее с числом l_0 . Такое число существует, так как, например, число l_m , где m — порядок подстановки a , равно числу l_0 . Докажем, что числа l_0, l_1, \dots, l_{q-1} все различны. Действительно, если, например, $l_q = l_{q+p}$, то, применяя к этому равенству подстановку a^{-1} , мы получим $l_0 = l_p$, что в силу минимальности числа q невозможно.

Поскольку числа l_0, l_1, \dots, l_{q-1} все различны (и $q > 1$, ибо $l_0 \neq l_1$; см. выше), то мы можем составить цикл $(l_0 l_1 \dots$

$\dots l_{q-1}$). Подстановка $a(l_0 l_1 \dots l_{q-1})^{-1}$ оставляет на месте все числа, которые оставляются на месте подстановкой a , а кроме того и все числа l_0, \dots, l_{q-1} . Таким образом, она действительно перемещает не более $s - q$ чисел и, следовательно, по предположению индукции, разлагается в произведение независимых циклов. Для завершения доказательства остается заметить, что эти циклы независимы и с циклом $(l_0 l_1 \dots l_{q-1})$.

Так как каждый цикл разлагается на транспозиции, то из доказанной теоремы следует, что

любая подстановка разлагается в произведение транспозиций (уже, вообще говоря, не независимых).

Числа, входящие в независимые циклы, на которые разложена некоторая подстановка, суть числа, действительно перемещаемые этой подстановкой. Каждый цикл разложения состоит из тех чисел, которые перемещаются друг в друга степенями данной подстановки. Таким образом, количество и строение независимых циклов, на которые разлагается подстановка, однозначно определяются этой подстановкой. Другими словами,

разложение подстановки в произведение независимых циклов однозначно (с точностью до порядка множителей).

3. Четные подстановки. Знакопеременная группа

Как мы видели выше, любая подстановка разлагается в произведение транспозиций. Вообще говоря, одну и ту же подстановку можно представить в виде произведения транспозиций многими различными способами. Например, очевидно, что

$$(j\ k)(l\ k) = (l\ j)(j\ k), \text{ если } l \neq j, \quad (1)$$

$$(l\ j)(l\ k) = (l\ k)(j\ k), \text{ если } j \neq k \quad (2)$$

(формулы (1) и (2) выражают, как легко видеть, один и тот же факт, но в различных обозначениях).

Лемма. Если произведение нескольких транспозиций равно тождественной подстановке, то число этих транспозиций четно.

Мы докажем эту лемму индукцией по числу s различных чисел, входящих в записи данных транспозиций. Наименьшее

возможное значение числа s равно, очевидно, двум. Если $s = 2$, то рассматриваемое произведение является степенью некоторой транспозиции и поэтому равно тождественной подстановке только тогда, когда показатель степени четен (ибо любая транспозиция имеет порядок 2). Таким образом, в случае $s = 2$ лемма доказана.

Предполагая теперь, что лемма уже доказана для любого произведения транспозиций, записи которых содержат менее s различных чисел, рассмотрим некоторое, равное тождественной подстановке произведение транспозиций

$$(l_1 l_2) (l_3 l_4) \dots (l_{2q-1} l_{2q}) = e, \quad (3)$$

в записи которых входит ровно s различных чисел. Пусть l — одно из этих чисел. Пользуясь соотношением (1) и тем, что независимые транспозиции перестановочны, мы можем «переместить вперед» все транспозиции, в запись которых входит число l , т. е. перейти от произведения (3) к равному произведению вида

$$(l j_1) \dots (l j_p) (k_1 k_2) \dots (k_{2r-1} k_{2r}), \quad (4)$$

в котором все числа k_1, k_2, \dots, k_{2r} отличны от числа l . Если $p > 1$, то, пользуясь соотношением (2) или соотношением

$$(l j) (l j) = e, \quad (5)$$

мы можем от произведения (4) перейти к произведению такого же вида, но с меньшим p . В результате ряда таких преобразований мы либо полностью уничтожим все транспозиции, в записи которых входит число l , либо получим произведение, содержащее только одну такую транспозицию:

$$(l j_1) (l_1 l_2) \dots (l_{2t-1} l_{2t}).$$

Но это произведение переводит, очевидно, число j_1 в число l и потому не может быть тождественной подстановкой. Следовательно, последний случай невозможен. Таким образом, в результате наших преобразований мы получим равное тождественной подстановке произведение транспозиций, записи которых не содержат числа l . Никаких новых чисел записи этих подстановок, очевидно, не содержат. Следовательно, согласно предположению индукции, в это произведение входит четное число транспозиций. Остается заметить,

что при описанных преобразованиях число транспозиций либо не меняется (когда мы пользуемся соотношениями (1), (2)), либо уменьшается на две единицы (когда мы пользуемся соотношением (5)). Поэтому исходное произведение (3) также состоит из четного числа транспозиций. Тем самым лемма полностью доказана.

Пусть теперь некоторая подстановка a двумя способами разложена в произведение транспозиций:

$$a = (l_1 l_2) \dots (l_{2p-1} l_{2p}),$$

$$a = (j_1 j_2) \dots (j_{2q-1} j_{2q})$$

(первое разложение содержит p транспозиций, а второе q). Тогда

$$(l_1 l_2) \dots (l_{2p-1} l_{2p})(j_{2q} j_{2q-1}) \dots (j_2 j_1) = aa^{-1} = e,$$

и, следовательно, по доказанной лемме, число $p+q$ четно.

Таким образом, числа p и q либо одновременно четны, либо одновременно нечетны. Другими словами,

при всех разложениях подстановки в произведение транспозиций четность числа этих транспозиций будет одна и та же.

Подстановка называется *четной*, если она разлагается в произведение четного числа транспозиций, и *нечетной* — в противном случае. Согласно доказанной теореме, четность подстановки не зависит от выбора ее разложения в произведение транспозиций.

Любая транспозиция, или вообще любой цикл четной длины, является нечетной подстановкой, а любой цикл нечетной длины, в частности любой цикл длины 3, является четной подстановкой. Тождественная подстановка, очевидно, четна.

Если

$$a = (l_1 l_2)(l_3 l_4) \dots (l_{s-1} l_s)$$

— разложение подстановки a в произведение транспозиций, то

$$a^{-1} = (l_s l_{s-1}) \dots (l_4 l_3)(l_2 l_1),$$

откуда следует, что

подстановка, обратная четной подстановке, четна, обратная нечетной — нечетна.

Далее, если

$$a = (l_1 l_2) \dots (l_{s-1} l_s),$$

$$b = (j_1 j_2) \dots (j_{t-1} j_t),$$

то

$$ab = (l_1 l_2) \dots (l_{s-1} l_s) (j_1 j_2) \dots (j_{t-1} j_t).$$

Поэтому

произведение двух четных или двух нечетных подстановок является четной подстановкой; произведение четной и нечетной подстановок является нечетной подстановкой.

Отсюда следует, что совокупность всех четных подстановок (данной степени n) является подгруппой симметрической группы S_n . Эта подгруппа обозначается через A_n и называется *знакопеременной группой степени n* .

Так как для любой четной подстановки a и произвольной подстановки b произведение bab^{-1} является четной подстановкой, то знакопеременная группа A_n является нормальным делителем симметрической группы S_n . Так как для любых двух нечетных подстановок a и b подстановка ab^{-1} четна, т. е. принадлежит группе A_n , то все нечетные подстановки образуют один смежный класс по подгруппе A_n . Следовательно, факторгруппа S_n/A_n состоит только из двух элементов, т. е. имеет порядок 2. Поэтому

порядок группы A_n , т. е. число четных подстановок степени n , равен $\frac{1}{2} n!$

4. Строение знакопеременной и симметрической групп

Изучим строение группы A_n при различных значениях n .

Для $n = 2$ знакопеременная группа состоит только из тождественной подстановки e .

Для $n = 3$ знакопеременная группа имеет порядок $\frac{1}{2} 3! = 3$ и, следовательно, циклична. В качестве ее образующей можно принять любую четную подстановку (например, цикл $(1, 2, 3)$).

Для $n = 4$ знакопеременная группа имеет порядок $\frac{1}{2} 4! = 12$ и состоит из следующих элементов:

 e

$$\begin{aligned} t_1 &= (1\ 2)(3\ 4), \quad t_2 = (1\ 3)(2\ 4), \quad t_3 = (1\ 4)(2\ 3), \\ s_1 &= (1\ 2\ 3), \quad s_2 = (1\ 2\ 4), \quad s_3 = (1\ 3\ 2), \quad s_4 = (1\ 3\ 4), \\ s_5 &= (1\ 4\ 2), \quad s_6 = (1\ 4\ 3), \quad s_7 = (2\ 3\ 4), \quad s_8 = (2\ 4\ 3). \end{aligned}$$

Легко проверяется, что

$$\begin{aligned} t_1^2 &= t_2^2 = t_3^2 = e, \quad t_2 t_1 = t_1 t_2 = t_3, \\ t_3 t_1 &= t_1 t_3 = t_2, \quad t_3 t_2 = t_2 t_3 = t_1. \end{aligned}$$

Следовательно, подстановки e , t_1 , t_2 , t_3 образуют подгруппу группы A_4 . Эта подгруппа называется *клейновской группой* и обозначается B_4 . Группа B_4 абелева и имеет порядок 4.

Далее легко проверить, что

$$\begin{aligned} s_1 t_1 s_1^{-1} &= t_2, & s_1 t_2 s_1^{-1} &= t_3, & s_1 t_3 s_1^{-1} &= t_1, \\ s_2 t_1 s_2^{-1} &= t_3, & s_2 t_2 s_2^{-1} &= t_1, & s_2 t_3 s_2^{-1} &= t_2, \\ s_3 t_1 s_3^{-1} &= t_3, & s_3 t_2 s_3^{-1} &= t_1, & s_3 t_3 s_3^{-1} &= t_2, \\ s_4 t_1 s_4^{-1} &= t_2, & s_4 t_2 s_4^{-1} &= t_3, & s_4 t_3 s_4^{-1} &= t_1, \\ s_5 t_1 s_5^{-1} &= t_2, & s_5 t_2 s_5^{-1} &= t_3, & s_5 t_3 s_5^{-1} &= t_1, \\ s_6 t_1 s_6^{-1} &= t_3, & s_6 t_2 s_6^{-1} &= t_1, & s_6 t_3 s_6^{-1} &= t_2, \\ s_7 t_1 s_7^{-1} &= t_3, & s_7 t_2 s_7^{-1} &= t_1, & s_7 t_3 s_7^{-1} &= t_2, \\ s_8 t_1 s_8^{-1} &= t_2, & s_8 t_2 s_8^{-1} &= t_3, & s_8 t_3 s_8^{-1} &= t_1. \end{aligned}$$

Следовательно, группа B_4 является нормальным делителем группы A_4 . Соответствующая факторгруппа A_4/B имеет порядок 3 и поэтому является циклической группой.

Так как группа B_4 абелева, то любая ее подгруппа, например циклическая подгруппа C_4 второго порядка, состоящая из тождественной подстановки e и подстановки t_1 , является нормальным делителем (группы B_4 , но не всей группы A_4). Порядок факторгруппы B_4/C_4 равен двум, и следовательно, эта факторгруппа является циклической группой.

Таким образом, цепочка подгрупп

$$A_4 \supset B_4 \supset C_4 \supset e$$

является разрешимым рядом группы A_4 . Тем самым доказано, что группа A_4 разрешима.

Группы A_2 и A_3 также, очевидно, разрешимы. Таким образом,

для $n \leq 4$ группа A_n разрешима.

Рассмотрим теперь случай $n \geq 5$. Пусть N — произвольный нормальный делитель группы A_n , отличный от e . Поскольку $N \neq e$, то в N существует хотя бы одна подстановка $t \neq e$. Разложение подстановки t в произведение независимых циклов может иметь одну из следующих четырех форм:

- 1) $t = (l_0 l_1 l_2 l_3 \dots) (\dots) \dots$ (имеется цикл длины ≥ 4);
- 2) $t = (l_0 l_1 l_2) (l_3 l_4 \dots) (\dots) \dots$ (имеется цикл длины 3 и еще другие циклы);
- 3) $t = (l_0 l_1 l_2)$ (подстановка t является циклом длины 3);
- 4) $t = (l_0 l_1) (l_2 l_3) (\dots) \dots$ (подстановка t разлагается в произведение независимых транспозиций)

(подстановка t четна и поэтому не может быть транспозицией; многоточия обозначают некоторые числа или циклы, которые могут и отсутствовать). Так как N является нормальным делителем, то для любой четной подстановки r подстановка rtr^{-1} , а следовательно, и подстановка $rtr^{-1}t^{-1}$ принадлежат N . В зависимости от того, какую из указанных выше форм имеет подстановка t , мы выберем подстановку r следующим образом:

- 1) $r = (l_1 \ l_2 \ l_3);$
- 2) $r = (l_1 \ l_2 \ l_4);$
- 3) $r = (l_1 \ l_2 \ l_3);$
- 4) $r = (l_1 \ l_2 \ l_3).$

Сосчитав в каждом из четырех случаев подстановку $s = rtr^{-1}t^{-1}$, мы получим, что

- 1) $s = (l_0 \ l_2 \ l_3);$
- 2) $s = (l_0 \ l_3 \ l_1 \ l_2 \ l_4);$
- 3) $s = (l_0 \ l_3) (l_1 \ l_2);$
- 4) $s = (l_0 \ l_2) (l_1 \ l_3).$

Таким образом, если в нормальном делителе N существует подстановка t вида 1), то существует и подстановка вида 3). Если же существует подстановка вида 2), то существует подстановка вида 1) и, следовательно, по только что сказанному, подстановка вида 3). Наконец, если существует подстановка вида 3) или 4), то существует подстановка, являющаяся произведением точно двух независимых транспозиций. Таким образом, в N обязательно существует подстановка, являющаяся произведением точно двух независимых транспозиций. Пусть это будет подстановка $(j_1 j_2)(j_3 j_4)$.

Пусть теперь $(k_1 k_2)(k_3 k_4)$ — произвольная подстановка, являющаяся произведением двух независимых транспозиций. Рассмотрим подстановку

$$a = \begin{pmatrix} k_1 & k_2 & k_3 & k_4 & \dots \\ j_1 & j_2 & j_3 & j_4 & \dots \end{pmatrix},$$

где на месте точек стоят произвольные числа (конечно, в верхней строчке эти числа отличны от чисел k_1, k_2, k_3, k_4 , а в нижней — от чисел j_1, j_2, j_3, j_4). Легко видеть, что

$$a(j_1 j_2)(j_3 j_4)a^{-1} = (k_1 k_2)(k_3 k_4).$$

Кроме того, обозначая для упрощения формул подстановку $a(j_1 j_2)$ через b , мы получим, что

$$\begin{aligned} b(j_1 j_2)(j_3 j_4)b^{-1} &= a(j_1 j_2)(j_1 j_2)(j_3 j_4)(j_1 j_2)a^{-1} = \\ &= a(j_1 j_2)(j_3 j_4)a^{-1}, \end{aligned}$$

то есть, что

$$b(j_1 j_2)(j_2 j_4)b^{-1} = (k_1 k_2)(k_3 k_4).$$

Подстановки a и b , отличаясь транспозицией, имеют различную четность, т. е. одна из них четна, а другая нечетна. Обозначим четную из подстановок a и b через c , т. е. положим $c = a$, если подстановка a четна, и $c = b$, если подстановка b четна. По доказанному

$$c(j_1 j_2)(j_3 j_4)c^{-1} = (k_1 k_2)(k_3 k_4).$$

Так как $(j_1 j_2)(j_3 j_4) \in N$, $c \in A_n$, а N является, по условию, нормальным делителем в A_n , то отсюда вытекает, что $(k_1 k_2)(k_3 k_4) \in N$. Таким образом, мы доказали, что нормаль-

ный делитель N содержит все подстановки, являющиеся произведениями двух независимых транспозиций.

Рассмотрим теперь подстановку, являющуюся произведением двух зависимых транспозиций. Такая подстановка имеет вид $(j_1 j_2)(j_1 j_3)$. Так как по условию $n \geq 5$, то существуют два различных числа l_1 и l_2 , не превосходящих n и отличных от чисел j_1 , j_2 и j_3 . Подстановки $(j_1 j_2)(l_1 l_2)$ и $(l_1 l_2)(j_1 j_3)$, являясь произведениями двух независимых транспозиций, по доказанному принадлежат нормальному делителю N . Но

$$(j_1 j_2)(l_1 l_2) \cdot (l_1 l_2)(j_1 j_3) = (j_1 j_2)(j_1 j_3)$$

и, следовательно, подстановка $(j_1 j_2)(j_1 j_3)$ также принадлежит N . Таким образом,циальному делителю N принадлежит любая подстановка, являющаяся произведением двух произвольных транспозиций, а следовательно, и любая подстановка, являющаяся произведением произвольного четного числа транспозиций, т. е. любая четная подстановка. Поэтому нормальный делитель N содержит все четные подстановки, т. е. $N = A_n$.

Таким образом, если $N \neq e$, то $N = A_n$. Другими словами, группа A_n не имеет никаких нормальных делителей, кроме тривиальных, т. е. является простой группой. Итак, мы доказали, что

для $n \geq 5$ знакопеременная группа A_n проста и, следовательно, неразрешима (ибо простые разрешимые группы исчерпываются циклическими группами простого порядка).

Заметим, что для $n = 2$ и $n = 3$ группа A_n , очевидно, также проста.

Из доказанных результатов относительно группы A_n немедленно вытекает, что

для $n \leq 4$ симметрическая группа S_n разрешима (ибо она обладает следующим разрешимым рядом:

$$S_2 \supset e, \text{ если } n = 2,$$

$$S_3 \supset A_3 \supset e, \text{ если } n = 3,$$

$$S_4 \supset A_4 \supset B_4 \supset C_4 \supset e, \text{ если } n = 4),$$

а для $n \geq 5$ группа S_n неразрешима (ибо она содержит неразрешимую группу A_n).

5. Пример уравнения с симметрической группой Галуа

Группа G подстановок степени n называется *транзитивной*, если для любых двух чисел i, j (конечно, предполагается, что $1 \leq i, j \leq n$) в группе G существует хотя бы одна подстановка, переводящая число i в число j . Значение транзитивных групп для теории Галуа объясняется следующей теоремой.

Группа Галуа неприводимого многочлена транзитивна.

Для доказательства достаточно заметить, что если многочлен $f(x)$ неприводим, то все его корни $\alpha_1, \dots, \alpha_n$ сопряжены между собой, и поэтому для любой пары корней α_i, α_j в поле $Q = P(\alpha_1, \dots, \alpha_n)$ существует автоморфизм (над P), переводящий корень α_i в корень α_j (см. ч. I, гл. 3, п. 5).

Задача. Доказать, что многочлен, имеющий транзитивную группу Галуа, неприводим.

Не имея в виду изучить любые транзитивные группы, мы ограничимся рассмотрением групп, содержащих хотя бы одну транспозицию.

Пусть транзитивная группа G содержит транспозицию $(i_1 i_2)$. Кроме этой транспозиции, группа G может содержать и другие транспозиции вида $(i_1 j)$. Пусть

$$(i_1 i_2), (i_1 i_3), \dots, (i_1 i_m)$$

— все транспозиции вида $(i_1 j)$, содержащиеся в группе G . Тогда группа G не содержит ни одной транспозиции вида

$$(j i_q), \quad q = 1, 2, \dots, m,$$

для которой число j отлично от чисел i_1, i_2, \dots, i_m (транспозиции вида $(i_p i_q)$, где $1 \leq p, q \leq m$, группа G содержит, ибо $(i_p i_q) = (i_1 i_p)(i_1 i_q)(i_1 i_p)$). Действительно, для $q = 1$ это очевидно, а для $q > 1$ из соотношений $(j i_p) \in G$ и $(i_1 j) = (i_1 i_q)(j i_q)(i_1 i_q)$ вытекает, что, вопреки условию, $(i_1 j) \in G$.

Если теперь $m < n$, т. е. если существует число $j \leq n$, отличное от чисел i_1, \dots, i_m , то, поскольку группа G транзитивна, в ней существует хотя бы одна подстановка a ,

переводящая число i_1 в число j . Пусть

$$a = \begin{pmatrix} i_1 & i_2 & \dots & i_m & \dots \\ j_1 & j_2 & \dots & j_m & \dots \end{pmatrix},$$

где

$$j_1 = j.$$

Из доказанного выше следует, что ни одно из чисел j_1, \dots, j_m не равно ни одному из чисел i_1, i_2, \dots, i_m , ибо подстановка $a(i_1 i_q) a^{-1} = (j_1 j_q) = (j j_q)$ принадлежит группе G . Следовательно, $2m \leq n$.

Если $2m < n$, то существует число $k \leq n$, отличное как от чисел i_1, \dots, i_m , так и от чисел j_1, \dots, j_m . В силу транзитивности группы G в ней существует хотя бы одна подстановка b , переводящая число i_1 в число k . Пусть

$$b = \begin{pmatrix} i_1 & i_2 & \dots & i_m & \dots \\ k_1 & k_2 & \dots & k_m & \dots \end{pmatrix},$$

где

$$k_1 = k.$$

Как и выше, доказывается, что ни одно из чисел k_1, \dots, k_m не равно ни одному из чисел i_1, \dots, i_m . Кроме того, оказывается, что ни одно из чисел k_1, \dots, k_m не равно ни одному из чисел j_1, \dots, j_m . Действительно, если, например, $k_p = j_q$, то группа G содержит транспозицию

$$ab^{-1}(i_1 i_p)ba^{-1} = (k' i_q),$$

где k' — число, переводящееся подстановкой a в число k , что невозможно, ибо число k' , очевидно, отлично от чисел i_1, \dots, i_q . Следовательно, $3m \leq n$.

Если $3m < n$, то аналогичным построением мы можем найти m чисел i_1, \dots, i_m , отличных от всех ранее найденных, и тем самым доказать, что $4m \leq n$. Процесс построения новых чисел остановится лишь тогда, когда мы исчерпаем все n чисел $1, 2, \dots, n$. Но так как на каждом шаге мы добавляем ровно m чисел, то такое исчерпание возможно лишь тогда, когда m делит n . С другой стороны, процесс должен обязательно остановиться, ибо число n конечно. Тем самым мы доказали, что **число m делит число n** (степень группы G).

Так как $m \geq 2$, то отсюда следует, что в случае, когда n — простое число, число m должно совпадать с n . Таким образом, в этом случае числа ℓ_1, \dots, ℓ_m исчерпывают все числа $1, 2, \dots, n$, и потому группа G содержит любую транспозицию (ℓj) (ибо $(\ell j) = (\ell_1 \ell)(\ell_1 j)(\ell_1 \ell)$). Следовательно, $G = S_n$, потому что каждая подстановка разлагается в произведение транспозиций. Тем самым доказано, что

транзитивная группа простой степени, содержащая транспозицию, совпадает со всей симметрической группой.

Применим эту теорему к задаче отыскания группы Галуа неприводимого многочлена $f(x)$ простой степени n . Предположим, что все корни многочлена $f(x)$ действительны, кроме двух. Пусть, например, α_1, α_2 — не действительные корни многочлена $f(x)$, а $\alpha_3, \dots, \alpha_n$ — его действительные корни. Предположим далее, что основное поле P состоит только из действительных чисел (например, является полем R рациональных чисел). Тогда корни α_1 и α_2 являются, как известно, комплексно сопряженными числами

$$\alpha_2 = \bar{\alpha}_1.$$

Любой элемент α поля $Q = P(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n)$ выражается в виде многочлена (с коэффициентами из P) от $\alpha_1, \alpha_2, \dots, \alpha_n$:

$$\alpha = g(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n).$$

Так как все коэффициенты этого многочлена являются по условию действительными числами, то

$$\bar{\alpha} = g(\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3, \dots, \bar{\alpha}_n),$$

то есть

$$\bar{\alpha} = g(\alpha_2, \alpha_1, \alpha_3, \dots, \alpha_n)$$

(напомним, что корни $\alpha_3, \dots, \alpha_n$ по условию являются действительными числами), и следовательно, $\bar{\alpha} \in Q$. Поэтому, полагая

$$\alpha^S = \bar{\alpha},$$

мы получим некоторое отображение S поля Q в себя. Из элементарных свойств операции $\alpha \rightarrow \bar{\alpha}$ (см. Курс, стр. 122) легко следует, что отображение S является автоморфизмом поля Q над полем P , т. е. $S \in G(Q, P)$. Подстановка, соот-

всему соответствующая автоморфизму S , является очевидно, транспозицией (1 2). Таким образом, группа Галуа многочлена $f(x)$ (рассматриваемая как группа подстановок) является транзитивной (ибо многочлен $f(x)$ неприводим) группой простой степени n , содержащей транспозицию (1 2). Поэтому эта группа совпадает со всей группой S_n . Таким образом, доказана следующая теорема.

Если

- 1) поле R состоит только из действительных чисел;
- 2) многочлен $f(x)$ неприводим над полем R ;
- 3) степень n многочлена $f(x)$ является простым числом;
- 4) многочлен $f(x)$ имеет точно два не действительных корня,

то группой Галуа многочлена $f(x)$ является симметрическая группа S_n .

Примером многочлена над полем R рациональных чисел, который удовлетворяет условиям этой теоремы, служит многочлен

$$x^5 + px + p,$$

где p — произвольное простое число. Неприводимость этого многочлена следует из критерия Эйзенштейна (см. Курс, стр. 353). Ряд Штурма для него имеет вид

$$x^5 + px + p, \quad 4x^4 + p, \quad 3px + 4, \quad 1,$$

и следовательно, согласно теореме Штурма, многочлен $x^5 + px + p$ имеет три действительных корня. Таким образом, этот многочлен удовлетворяет условиям теоремы. Значит, его группой Галуа является группа S_5 . Так как последняя группа неразрешима, то уравнение

$$x^5 + px + p = 0$$

неразрешимо в радикалах. Таким образом,

над полем рациональных чисел существуют неразрешимые в радикалах уравнения пятой степени.

Так как если все уравнения некоторой степени n разрешимы в радикалах, то разрешимы в радикалах и все уравнения любой меньшей степени (почему?), то тем самым доказано, что

над полем рациональных чисел существуют неразрешимые в радикалах уравнения любой степени, большей или равной пяти.

Для построения таких уравнений достаточно многочлен $x^5 + px + p$ умножить на произвольный многочлен соответствующей степени.

6. Обсуждение полученных результатов

Изложенные в конце предыдущего пункта соображения позволяют привести лишь отдельные примеры неразрешимых в радикалах уравнений над полем рациональных чисел. При этом для степеней, больших пяти, получаются обязательно приводимые уравнения. Таким образом, вопрос о существовании неразрешимых в радикалах неприводимых уравнений степеней, больших пяти, остается для нас пока открытым. Кроме того, остается открытым вопрос о существовании неразрешимых в радикалах уравнений (хотя бы приводимых) над полями P , отличными от поля рациональных чисел. Для каждого конкретного поля P (по крайней мере, если оно состоит только из действительных чисел) примеры таких уравнений можно пытаться построить, пользуясь теоремой, доказанной в предыдущем пункте (при этом, конечно, нужно предполагать, что поле P не слишком велико, так как, например, над полем действительных чисел любое уравнение разрешимо в радикалах, ибо любой многочлен разлагается на линейные и квадратичные множители). Основная трудность здесь состоит в доказательстве неприводимости. Так как для произвольных полей не существует никаких критериев неприводимости, то на этом пути нельзя надеяться получить никаких общих результатов.

Ввиду этих затруднений целесообразно вопрос о разрешимости в радикалах любого уравнения данной степени n над данным полем P поставить несколько в иной плоскости, заменив его вопросом о разрешимости в радикалах общего уравнения степени n над полем P . При этом под общим уравнением степени n над полем P мы понимаем уравнение

$$x^n + a_1 x^{n-1} + \dots + a_n = 0, \quad (1)$$

где a_1, \dots, a_n — независимые переменные, которые мы мыслим пробегающими независимо друг от друга все элементы

поля P . На этом пути в первую очередь нужно определить, что значит выражение «уравнение (1) разрешимо в радикалах», так как определение разрешимости в радикалах, которым мы пользовались выше (для уравнений с числовыми коэффициентами) в этом случае неприменимо.

Первое, естественно возникающее определение разрешимости в радикалах общего уравнения (1) можно сформулировать следующим образом: уравнение (1) разрешимо в радикалах над полем P , если существует такая формула:

$$R(a_1, a_2, \dots, a_n), \quad (2)$$

содержащая, кроме знаков арифметических действий, только знаки $\sqrt[k]{-}$, что при любом выборе значений $a_1^0, a_2^0, \dots, a_n^0 \in P$ коэффициентов уравнения (1) число $R(a_1^0, a_2^0, \dots, a_n^0)$ является корнем уравнения (уже числового!):

$$x^n + a_1^0 x^{n-1} + \dots + a_n^0 = 0.$$

(Ввиду многозначности операции $\sqrt[k]{-}$ нужно при этом оговорить, какие имеются в виду значения корней $\sqrt[k]{-}$). В формулу (2) могут, конечно, входить и некоторые постоянные числа. Естественно при этом требовать, чтобы эти числа принадлежали полю P .

При этом понимании разрешимости в радикалах общего уравнения легко видеть, что если общее уравнение степени n разрешимо в радикалах над полем P , то и любое (числовое) уравнение над полем P разрешимо в радикалах (в нашем прежнем смысле). Отсюда, в частности, следует, что

над полем рациональных чисел общее уравнение степени $n \geq 5$ неразрешимо в радикалах.

Изложенное определение разрешимости в радикалах общего уравнения имеет тот недостаток, что оно совершенно формально и, по существу, никак не связано с общими понятиями теории Галуа. Поэтому, оставаясь на этой точке зрения, мы не в состоянии применить развитую выше теорию к решению вопроса о разрешимости в радикалах общего уравнения над произвольным полем.

Более содержательная точка зрения состоит в рассмотрении общего уравнения (1) над полем $P(a_1, a_2, \dots, a_n)$ всех рациональных дробей от переменных a_1, \dots, a_n (имеющих

коэффициенты в поле P). Как было сказано в ч. I, гл. 1, п. 1, вся развитая выше теория применима не только к числовым полям, но и к любым подполям некоторого алгебраически замкнутого поля (характеристики 0). Поэтому, если мы, рассматривая уравнение (1) над полем $P(a_1, a_2, \dots, a_n)$, хотим применить к нему теорию Галуа, мы должны доказать, что поле $P(a_1, a_2, \dots, a_n)$ содержится в некотором алгебраически замкнутом поле. Если это будет доказано, то понятие разрешимости в радикалах, так же как и найденный выше критерий разрешимости, будет автоматически применимо к общему уравнению (1). Следовательно, определив группу Галуа этого уравнения, мы немедленно решим вопрос о его разрешимости в радикалах. Детальному проведению этих соображений будет посвящена следующая глава.

ГЛАВА 4

НЕРАЗРЕШИМОСТЬ В РАДИКАЛАХ ОБЩЕГО УРАВНЕНИЯ СТЕПЕНИ $n \geq 5$

1. Поле формальных степенных рядов

Пусть P — произвольное поле характеристики 0 (например, числовое). *Формальным степенным рядом над полем P от переменной x* называется выражение вида

$$a_{-m}x^{-m} + a_{-m+1}x^{-m+1} + \dots + a_{-1}x^{-1} + \\ + a_0 + a_1x + \dots + a_kx^k + \dots, \quad (1)$$

где $a_{-m}, a_{-m+1}, \dots, a_0, a_1, \dots, a_k, \dots$ — произвольные элементы поля P . Подчеркнем, что ряд (1) мы рассматриваем чисто формально, не накладывая никаких ограничений на сходимость (к тому же для произвольного (не числового) поля P говорить о сходимости ряда (1) не имеет смысла).

Среди коэффициентов $a_{-m}, \dots, a_0, \dots, a_k, \dots$ ряда (1) могут быть равные нулю. Мы будем считать, что при удалении (а значит, и при прибавлении) членов, имеющих нулевые коэффициенты, ряд (1) не меняется.

Степенные ряды можно складывать и перемножать точно так же, как и многочлены. Легко проверяется, что относительно сложения и умножения совокупность $P\langle x \rangle$ всех формальных степенных рядов над полем P от переменной x является кольцом. Оказывается, что

кольцо $P\langle x \rangle$ является полем,
т. е. для любого отличного от нуля степенного ряда f существует такой степенной ряд g , что $fg = 1$.

Действительно, любой отличный от нуля степенной ряд можно записать в следующем виде:

$$f = x^n(a_0 + a_1x + \dots + a_kx^k + \dots),$$

где n — некоторое целое число (положительное, отрицательное или нуль), а $a_0 \neq 0$. Определим числа $b_0, b_1, \dots, b_k, \dots$ из уравнений

$$\begin{aligned} a_0 b_0 &= 1, \\ a_0 b_1 + a_1 b_0 &= 0, \\ a_0 b_2 + a_1 b_1 + a_2 b_0 &= 0, \\ \dots &\dots \dots \dots \dots \\ a_0 b_k + a_1 b_{k-1} + \dots + a_k b_0 &= 0. \end{aligned}$$

Так как $a_0 \neq 0$, то эти уравнения последовательно позволяют однозначно определить числа $b_0, b_1, \dots, b_k, \dots$. Положив теперь

$$g = x^{-n}(b_0 + b_1 x + \dots + b_k x^k + \dots),$$

мы, очевидно, получим, что

$$fg = 1.$$

Тем самым наше утверждение полностью доказано.

Любой многочлен $a_0 + a_1 x + \dots + a_p x^p$ мы можем (добавляя члены с нулевыми коэффициентами) рассматривать как степенной ряд. Следовательно, кольцо $P[x]$ всех многочленов над полем P от переменной x является подкольцом кольца $P(x)$. Но так как кольцо $P(x)$ является полем, то вместе с любыми многочленами оно содержит также и все их отношения, т. е. все дробно-рациональные функции (рациональные дроби) от переменной x с коэффициентами из поля P (этот факт является алгебраическим эквивалентом того известного обстоятельства, что любая рациональная дробь разлагается в степенной ряд). Таким образом,

поле $P(x)$ всех рациональных дробей является подполем поля $P(x)$.

Пусть

$$F(z) = z^n + f_1 z^{n-1} + \dots + f_n$$

— произвольный многочлен над полем $P(x)$ (со старшим коэффициентом, равным единице). Коэффициентами f_1, \dots, f_n этого многочлена являются степенные ряды над полем P от переменной x . Мы будем предполагать, что эти коэффициенты не содержат членов с отрицательными степенями переменной x , т. е. что

$$f_i = a_{i0} + a_{i1} x + \dots + a_{ik} x^k + \dots$$

Рассмотрим многочлен (над полем P)

$$F_0(z) = z^n + a_{10}z^{n-1} + \dots + a_{n0}$$

(этот многочлен получается из многочлена $F(z)$ подстановкой $x = 0$). Оказывается, что

если многочлен $F_0(z)$ над полем P разлагается на произведение двух взаимно простых многочленов

$$F_0(z) = G_0(z) H_0(z),$$

то над полем $P(x)$ существуют такие многочлены $G(x)$ и $H(z)$, что

$$F(z) = G(z)H(z),$$

причем при подстановке $x = 0$ многочлен $G(z)$ переходит в многочлен $G_0(z)$, а многочлен $H(z)$ — в многочлен $H_0(z)$.

Для доказательства мы запишем многочлен $F(z)$ в виде формального ряда

$$F(z) = F_0(z) + F_1(z)x + \dots + F_k(z)x^k + \dots,$$

где

$$F_k(z) = a_{1k}z^{n-1} + \dots + a_{nk}, \quad k = 1, 2, \dots,$$

и рассмотрим систему уравнений

$$G_0(z)H_1(z) + G_1(z)H_0(z) = F_1(z),$$

$$G_0(z)H_2(z) + G_1(z)H_1(z) + G_2(z)H_0(z) = F_2(z),$$

• (2)

$$G_0(z)H_k(z)+G_1(z)H_{k-1}(z)+\dots+G_k(z)H_0(z)=F_k(z),$$

относительно неизвестных многочленов

$$G_1(z), G_2(z), \dots, G_k(z), \dots \quad (3)$$

$$H_1(z), H_2(z), \dots, H_k(z), \dots \quad (4)$$

Докажем, что всегда существуют такие многочлены (3), (4), что, во-первых, они удовлетворяют системе (2), а во-вторых, степень каждого многочлена (3) меньше степени p многочлена $G_0(z)$, а степень каждого много-

члена (4) меньше степени q многочлена $H_0(z)$. Полагая с этой целью

$$B_1(z) = F_1(z),$$

$$B_2(z) = F_2(z) - G_1(z) H_1(z),$$

$$\begin{aligned} B_k(z) &= F_k(z) - G_1(z) H_{k-1}(z) - G_2(z) H_{k-2}(z) - \dots \\ &\quad \dots - G_{k-1}(z) H_1(z), \end{aligned}$$

мы перепишем уравнения (2) в следующем виде:

$$G_0(z) H_1(z) + G_1(z) H_0(z) = B_1(z),$$

$$G_0(z) H_2(z) + G_2(z) H_0(z) = B_2(z),$$

$$\dots \dots \dots \dots \dots$$

$$G_0(z) H_k(z) + G_k(z) H_0(z) = B_k(z),$$

$$\dots \dots \dots \dots \dots$$

Предположим теперь, что для некоторого k уже найдены многочлены $G_1(z), \dots, G_{k-1}(z), H_1(z), \dots, H_{k-1}(z)$, удовлетворяющие перечисленным выше условиям. Тогда многочлен $B_k(z)$ мы можем рассматривать как известный нам многочлен. Степень этого многочлена, очевидно, меньше чем $n = p + q$.

Так как многочлены $G_0(z)$ и $H_0(z)$ взаимно просты, то существуют такие многочлены $\bar{H}_k(z)$ и $\bar{G}_k(z)$, что

$$G_0(z) \bar{H}_k(z) + \bar{G}_k(z) H_0(z) = 1$$

(см. Курс, стр. 141). Пусть $H_k(z)$ — остаток от деления многочлена $\bar{H}_k(z) B_k(z)$ на многочлен $H_0(z)$:

$$\bar{H}_k(z) B_k(z) = H_0(z) \Phi_k(z) + H_k(z).$$

Тогда

$$\begin{aligned} G_0(z) H_k(z) &= G_0(z) \bar{H}_k(z) B_k(z) - G_0(z) H_0(z) \Phi_k(z) = \\ &= (1 - \bar{G}_k(z) H_0(z)) B_k(z) - G_0(z) H_0(z) \Phi_k(z), \end{aligned}$$

т. е.

$$G_0(z) H_k(z) + G_k(z) H_0(z) = B_k(z),$$

где

$$G_k(z) = \bar{G}_k(z) B_k(z) + G_0(z) \Phi_k(z).$$

По построению, степень многочлена $H_k(z)$ меньше q и потому степень многочлена $G_k(z)H_0(z) = B_k(z) - G_0(z)H_k(z)$ меньше $n = p + q$. Следовательно, степень многочлена $G_k(z)$ меньше $p = n - q$.

Заметим, что многочлены $G_k(z)$ и $H_k(z)$ определяются единственным образом. Действительно, если

$$G_0(z)H_k(z) + G_k(z)H_0(z) = B_k(z)$$

и

$$G_0(z)H'_k(z) + G'_k(z)H_0(z) = B_k(z),$$

где степени многочленов $G_k(z)$ и $G'_k(z)$ меньше p , а степени многочленов $H_k(z)$ и $H'_k(z)$ меньше q , то

$$G_0(z)(H_k(z) - H'_k(z)) = (G'_k(z) - G_k(z))H_0(z),$$

откуда следует (в силу взаимной простоты многочленов $G_0(z)$ и $H_0(z)$), что разность $H_k(z) - H'_k(z)$ делится на многочлен $H_0(z)$. Поскольку степень многочлена $H_k(z) - H'_k(z)$ по условию меньше степени q многочлена $H_0(z)$, это возможно только тогда, когда $H_k(z) - H'_k(z) = 0$, т. е. когда $H_k(z) = H'_k(z)$. Аналогично $G_k(z) = G'_k(z)$.

Предположение о том, что уже найдены многочлены $G_1(z), \dots, G_{k-1}(z), H_1(z), \dots, H_{k-1}(z)$, нам было нужно только для того, чтобы рассматривать многочлен $B_k(z)$ как известный. Так как многочлен $B_1(z)$ нам известен с самого начала (он равен многочлену $F_1(z)$), то все изложенные рассуждения применимы и к случаю $k = 1$. Таким образом, начиная с $k = 1$, мы можем последовательно (и притом единственным образом) определить все многочлены (3) и (4). Положим теперь

$$\left. \begin{aligned} G(z) &= G_0(z) + G_1(z)x + \dots + G_k(z)x^k + \dots, \\ H(z) &= H_0(z) + H_1(z)x + \dots + H_k(z)x^k + \dots \end{aligned} \right\} \quad (5)$$

Собирая вместе члены, содержащие одинаковые степени переменной z , мы видим, что $G(z)$ и $H(z)$ являются многочленами над полем $P(x)$ (степеней p и q соответственно). С другой стороны, перемножая (формально) их выражения (5) и пользуясь соотношениями (2), мы, очевидно, получим, что

$$G(z)H(z) = F(z).$$

Тем самым сформулированная выше теорема полностью доказана.

В дальнейшем нам понадобится следующее утверждение, легко вытекающее из доказанной теоремы:

если поле P алгебраически замкнуто, то многочлен

$$F(z) = z^n + f_1 z^{n-1} + \dots + f_n$$

степени $n > 1$ над полем $P\langle x \rangle$, имеющий старший коэффициент, равный единице, приводим, когда выполнены следующие условия:

1) все его коэффициенты f_1, \dots, f_n не содержат членов с отрицательными степенями переменной x ;

2) хотя бы один коэффициент f_1, \dots, f_n имеет свободный член, т. е. содержит член с нулевой степенью переменной x ;

3) хотя бы один коэффициент f_1, \dots, f_n не имеет свободного члена, т. е. начинается с члена, имеющего положительную степень относительно x .

Действительно, в силу условия 1) для многочлена $F(z)$ определен многочлен $F_0(z)$ (над полем P), получающийся из многочлена $F(x)$ подстановкой $x=0$. В силу условия 2) многочлен $F_0(z)$, кроме члена z^n , имеет еще по крайней мере один член с отличным от нуля коэффициентом. Поэтому в поле P существует хотя бы один отличный от нуля корень a многочлена $F_0(z)$ (напомним, что поле P предполагается алгебраически замкнутым). Пусть $G_0(z) = (z - a)^p$ — наивысшая степень двучлена $z - a$, на которую делится многочлен $F_0(z)$. Таким образом,

$$F_0(z) = G_0(z) H_0(z), \quad (6)$$

где многочлен $H_0(z)$ взаимно прост с многочленом $G_0(z)$. Это разложение не тривиально, т. е. степень p многочлена $G_0(z)$ не равна n . Действительно, если $p = n$, то $F_0(z) = (z - a)^n$ и, следовательно, все коэффициенты многочлена $F_0(z)$ отличны от нуля (напомним, что поле P мы предполагаем полем характеристики 0), что противоречит условию 3). Согласно доказанной выше теореме, разложение (6) определяет некоторое разложение $F(z) = G(z) H(z)$ многочлена $F(z)$. Тем самым приводимость многочлена $F(z)$ доказана (ибо степень многочлена $G(z)$ равна p и, следовательно, меньше n).

2. Поле дробностепенных рядов

Пусть, как и выше, P — произвольное поле характеристики 0. Дробностепенным рядом над полем P от переменной x называется выражение вида

$$a_0 x^{\frac{n_0}{n}} + a_1 x^{\frac{n_1}{n}} + \dots + a_k x^{\frac{n_k}{n}} + \dots, \quad (1)$$

где n — произвольное целое положительное число, $n_0, n_1, \dots, n_k, \dots$ — возрастающие целые числа

$$n_0 < n_1 < \dots < n_k < \dots$$

(среди них могут быть и отрицательные, но только в конечном числе), а $a_0, a_1, \dots, a_k, \dots$ — некоторые элементы поля P . Если $n = 1$, то дробностепенной ряд есть не что иное, как формальный степенной ряд в смысле п. 1. Так же как и для степенных рядов, мы не считаем различными дробностепенные ряды, отличающиеся членами с нулевыми коэффициентами. Дробностепенные ряды можно складывать и перемножать по тем же правилам, как и формальные степенные ряды, причем, как легко видеть, относительно операций сложения и умножения совокупность $P\{x\}$ всех дробностепенных рядов над полем P от переменной x является кольцом. Оказывается, что

кольцо $P\{x\}$ является полем.

Для доказательства достаточно заметить, что любой дробностепенной ряд

$$f = a_0 x^{\frac{n_0}{n}} + \dots + a_k x^{\frac{n_k}{n}} + \dots$$

можно рассматривать как формальный степенной ряд от переменной

$$\xi = x^{\frac{1}{n}}.$$

Так как кольцо $P\langle\xi\rangle$ формальных степенных рядов от переменной ξ является полем, то для ряда f , рассматриваемого как степенной ряд от ξ , существует (конечно, если $f \neq 0$) такой степенной ряд g от ξ , что $fg = 1$. Заменяя в ряде g переменную ξ обратно на $x^{\frac{1}{n}}$, мы получим (уже дробностепенной) ряд от x , для которого $fg = 1$.

Основное свойство поля $P\{x\}$ описывается следующей теоремой:

Если поле P алгебраически замкнуто, то и поле $P\{x\}$ также алгебраически замкнуто.

Другими словами, любой многочлен $F(z)$ над полем $P\{x\}$ разлагается на линейные множители.

Для доказательства этого утверждения, очевидно, достаточно доказать, что любой многочлен

$$F(z) = z^n + f_1 z^{n-1} + \dots + f_n$$

над полем $P\{x\}$ степени $n > 1$ приводим. Имея это в виду, заметим, что без ограничения общности мы можем предполагать, что в многочлене $F(z)$ коэффициент f_1 при z^{n-1} равен нулю. Действительно, если $f_1 \neq 0$, то, введя новое неизвестное

$$y = z + \frac{f_1}{n},$$

мы, как легко видеть, получим многочлен с равным нулю коэффициентом f_1 . С другой стороны, при такой замене неприводимый многочлен остается неприводимым, а приводимый — приводимым.

Если все коэффициенты f_i многочлена $F(z)$ равны нулю, т. е. если $F(z) = z^n$, то многочлен $F(z)$ приводим, так что в этом случае теорема верна. Таким образом, мы можем предполагать, что среди коэффициентов f_i есть отличные от нуля. Пусть разложение отличного от нуля коэффициента f_i в дробностепенной ряд от переменной x начинается с члена $a_i x^{r_i}$, где $a_i \neq 0$, а r_i — некоторое рациональное число (которое может быть и отрицательным). Пусть r — наименьшее из чисел $\frac{r_i}{i}$. Тогда для любого i (для которого $f_i \neq 0$)

$$r_i \geqslant i r,$$

причем равенство достигается хотя бы для одного i .

Произведем теперь замену неизвестного, положив

$$z = yx^r.$$

Тогда, как легко видеть,

$$F(z) = x^{nr} G(y),$$

где

$$G(y) = y^n + g_2 y^{n-2} + \dots + g_n$$

($g_1 = 0$, ибо мы предполагаем, что $f_1 = 0$), причем для любого i

$$g_i = f_i x^{-ir}.$$

Следовательно, разложение отличного от нуля коэффициента g_i начинается с члена

$$a_i x^{r_i - ir}$$

(т. е. члена неотрицательной степени), причем хотя бы для одного i разложение коэффициента g_i имеет свободный член.

Пусть теперь m — наименьший общий знаменатель всех показателей, с которыми переменная x входит в ряды g_2, \dots, g_n . Тогда эти ряды можно рассматривать как формальны

е степенные ряды от переменной $\xi = x^{\frac{1}{m}}$, а следовательно, многочлен $G(y)$ — как многочлен над полем $P(\xi)$. Очевидно, что этот многочлен (рассматриваемый над полем $P(\xi)$) удовлетворяет всем условиям доказанного в конце предыдущего пункта предложения (условие 3) для него выполнено потому, что $g_1 = 0$). Следовательно, над полем $P(\xi)$ этот многочлен приводим, т. е. представляется в виде произведения некоторых многочленов над полем $P(\xi)$, имеющих положительные степени, отличные от n . Полагая в коэффи-

циентах этих многочленов $\xi = x^{\frac{1}{m}}$, мы, очевидно, получим разложение многочлена $G(y)$ в произведение многочленов над полем $P(x)$: Тем самым доказано, что многочлен $G(y)$ приводим. Для завершения доказательства остается заметить, что из приводимости многочлена $G(y)$ немедленно вытекает и приводимость многочлена $F(z)$. Тем самым алгебраическая замкнутость поля $P(x)$ полностью доказана.

Наряду с дробностепенными рядами от одного неизвестного x можно определить дробностепенные ряды от нескольких неизвестных x_1, \dots, x_n . Совокупность $P(x_1, \dots, x_n)$ всех дробностепенных рядов над полем P от неизвестных x_1, \dots, x_n проще всего определить по индукции:

$$P(x_1, \dots, x_n) = P(x_1, \dots, x_{n-1}) \{x_n\},$$

т. е. определить $P(x_1, \dots, x_n)$ как поле дробностепенных

рядов над полем $P\{x_1, \dots, x_{n-1}\}$ от переменной x_n . Легко можно дать прямое (хотя и несколько громоздкое) определение поля $P\{x_1, \dots, x_n\}$. Например, элементами поля $P\{x_1, x_2\}$, т. е. дробностепенными рядами от двух неизвестных x_1 и x_2 , являются выражения вида

$$\sum_{i=0}^{\infty} \sum_{j=0}^{\infty} a_{ij} x_1^{\frac{n_i}{m}} x_2^{\frac{m_j}{m}}, \quad n_0 < n_1 < \dots; \quad m_0 < m_1 < \dots$$

Сложение и умножение таких рядов определяются по очевидным правилам.

Если поле P алгебраически замкнуто, то, как мы знаем, алгебраически замкнуто и поле $P\{x_1\}$, а потому и поле $P\{x_1, x_2\}$ (как поле дробностепенных рядов над алгебраически замкнутым полем $P\{x_1\}$). По аналогичным соображениям алгебраически замкнуто поле $P\{x_1, x_2, x_3\}$ и вообще любое поле $P\{x_1, \dots, x_n\}$. Таким образом,

если поле P алгебраически замкнуто, то поле $P\{x_1, \dots, x_n\}$ также алгебраически замкнуто.

В частности,

поле $C\{x_1, \dots, x_n\}$ дробностепенных рядов от n переменных с комплексными коэффициентами алгебраически замкнуто.

Как мы видели выше, поле рациональных дробей $P(x)$ от переменной x над полем P является подполем поля $P\langle x \rangle$ формальных степенных рядов. С другой стороны, поскольку любой степенной ряд является также и дробностепенным рядом, то $P\langle x \rangle \subset P\{x\}$. Таким образом,

$$P(x) \subset P\{x\}.$$

Отсюда по индукции легко следует, что вообще для любого n

$$P(x_1, \dots, x_n) \subset P\{x_1, \dots, x_n\}.$$

Следовательно, в частности,

для любого числового поля P поле рациональных дробей $P(x_1, \dots, x_n)$ содержится в алгебраически замкнутом поле $C\{x_1, \dots, x_n\}$.

Тем самым мы обосновали возможность применения теории Галуа к уравнениям над полями рациональных дробей (с числовыми коэффициентами) и, в частности, к общему уравнению степени n (см. гл. 3, п. 6).

3. Группа Галуа общего уравнения степени n

Напомним, что под *общим уравнением степени n* мы понимаем уравнение вида

$$x^n + a_1 x^{n-1} + \dots + a_n = 0, \quad (1)$$

где a_1, \dots, a_n — независимые переменные. Это уравнение мы рассматриваем как уравнение над полем $\bar{P} = P(a_1, \dots, a_n)$ рациональных дробей от переменных a_1, \dots, a_n с коэффициентами из некоторого числового поля P . Поскольку поле $P(a_1, \dots, a_n)$ содержится в алгебраически замкнутом поле $C\{a_1, \dots, a_n\}$, то, как мы уже неоднократно отмечали, к уравнению (1) применимы все понятия и методы теории Галуа.

В частности, мы можем говорить о его поле разложения (над полем \bar{P}):

$$Q = \bar{P}(t_1, \dots, t_n),$$

где t_1, \dots, t_n — корни уравнения (1), т. е. некоторые дробностепенные ряды из поля $C\{a_1, \dots, a_n\}$. В этом поле содержится, в частности, поле $P(t_1, \dots, t_n)$:

$$P(t_1, \dots, t_n) \subset Q.$$

Но ввиду известных формул Вьета коэффициенты a_1, \dots, a_n уравнения (1) рационально выражаются через его корни и поэтому принадлежат полю $P(t_1, \dots, t_n)$. Следовательно,

$$\bar{P} \subset P(t_1, \dots, t_n),$$

и потому

$$\bar{P}(t_1, \dots, t_n) \subset P(t_1, \dots, t_n).$$

Таким образом,

$$Q = P(t_1, \dots, t_n).$$

Отсюда следует, что любой элемент поля Q выражается в виде рациональной дроби от элементов t_1, \dots, t_n с коэффициентами из поля P . Действительно, совокупность всех рациональных дробей от элементов t_1, \dots, t_n с коэффициентами из поля P является, очевидно, подполем поля Q .

содержащим поле P и элементы t_1, \dots, t_n . Поэтому в силу минимальности поля $P(t_1, \dots, t_n)$ это множество совпадает со всем полем $P(t_1, \dots, t_n) = Q$.

Оказывается, что

любой элемент поля Q единственным образом выражается в виде рациональной дроби с коэффициентами из поля P .

Действительно, если

$$\frac{f_1(t_1, \dots, t_n)}{g_1(t_1, \dots, t_n)} = \frac{f_2(t_1, \dots, t_n)}{g_2(t_1, \dots, t_n)},$$

то

$$g_2(t_1, \dots, t_n) f_1(t_1, \dots, t_n) - g_1(t_1, \dots, t_n) f_2(t_1, \dots, t_n) = 0.$$

Но если дроби $\frac{f_1}{g_1}$ и $\frac{f_2}{g_2}$ различны, то многочлен $g_2 f_1 - g_1 f_2$ отличен от нуля (т. е. имеет отличные от нуля коэффициенты). Поэтому если хотя бы один элемент поля Q двумя разными способами выражается в виде рациональной дроби от t_1, \dots, t_n , то над полем P существует такой отличный от нуля многочлен f от n неизвестных x_1, x_2, \dots, x_n , что

$$f(t_1, \dots, t_n) = 0.$$

Рассмотрим для этого многочлена f все многочлены вида f_a (см. ч. I, гл. 3, п. 1), где

$$a = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

— произвольная подстановка степени n . По определению

$$f_a(x_1, x_2, \dots, x_n) = f(x_{i_1}, x_{i_2}, \dots, x_{i_n}).$$

Все многочлены f_a отличны от нуля, и следовательно, их произведение $F(x_1, x_2, \dots, x_n)$ также отлично от нуля. Но, как мы знаем (см. ч. I, гл. 3, п. 1), это произведение является симметрическим многочленом. Следовательно, по основной теореме о симметрических многочленах (см. Курс, стр. 322) многочлен $F(x_1, x_2, \dots, x_n)$ выражается в виде некоторого отличного от нуля многочлена (с коэффициен-

тами из поля P) от элементарных симметрических многочленов от x_1, \dots, x_n . Но при $x_i = t_i$ последние многочлены с точностью до знаков совпадают с коэффициентами a_1, \dots, a_n уравнения (1). Следовательно, над полем P существует такой отличный от нуля многочлен g , что

$$g(a_1, \dots, a_n) = F(t_1, \dots, t_n).$$

С другой стороны, элемент $F(t_1, \dots, t_n)$ поля Q является произведением всех элементов вида $f_a(t_1, \dots, t_n)$, где $a \in S_n$. Так как среди сомножителей этого произведения содержится равный нулю элемент $f(t_1, \dots, t_n) = f_e(t_1, \dots, t_n)$, то

$$F(t_1, \dots, t_n) = 0.$$

Следовательно, мы нашли над полем P такой отличный от нуля многочлен g , что

$$g(a_1, \dots, a_n) = 0.$$

Но это невозможно, ибо по условию коэффициенты a_1, \dots, a_n являются независимыми переменными и никакой отличный от нуля многочлен над полем P от них не равен нулю.

Полученное противоречие доказывает, что представление любого элемента поля Q в виде рациональной дроби от t_1, \dots, t_n однозначно.

Заметим, что из доказанного утверждения следует, что *все корни t_1, \dots, t_n различны*. Действительно, если, например, $t_1 = t_2$, то существует такой отличный от нуля многочлен f от n неизвестных x_1, \dots, x_n (именно многочлен $f(x_1, \dots, x_n) = x_1 - x_2$), что $f(t_1, \dots, t_n) = 0$. Таким образом,

общее уравнение (1) не имеет кратных корней.

Рассмотрим теперь группу Галуа $G(Q, \bar{P})$ поля Q над полем \bar{P} , т. е. группу Галуа уравнения (1). (Заметим, что поле Q конечно над полем \bar{P} (ибо оно является полем разложения некоторого многочлена) и бесконечно над полем P (ибо оно содержит элементы a_1, \dots, a_n , не удовлетворяющие никакому уравнению); поэтому говорить о группе Галуа поля Q над полем P нельзя.)

Так как уравнение (1) не имеет кратных корней, то можно группу Галуа $G(Q, \bar{P})$ рассматривать как группу подстановок (см. гл. 3, п. 1). Более точно: существует естественное мономорфное отображение группы Галуа $G(Q, \bar{P})$ в симметрическую группу S_n . Подстановка

$$a = \begin{pmatrix} 1 & 2 & \dots & n \\ t_1 & t_2 & \dots & t_n \end{pmatrix},$$

соответствующая при этом мономорфизму автоморфизму $S \in G(Q, \bar{P})$, определяется из соотношений

$$t_k^S = t_{i_k}.$$

Следовательно, если подстановка a соответствует автоморфизму S , то для любого элемента

$$\frac{f(t_1, \dots, t_n)}{g(t_1, \dots, t_n)} \quad (2)$$

поля Q имеет место равенство

$$\left(\frac{f(t_1, \dots, t_n)}{g(t_1, \dots, t_n)} \right)^S = \frac{f_a(t_1, \dots, t_n)}{g_a(t_1, \dots, t_n)}. \quad (3)$$

Докажем теперь, что рассматриваемый мономорфизм одновременно является и эпиморфизмом (а значит, и изоморфизмом), т. е. что любая подстановка a получается из некоторого автоморфизма $S \in G(Q, \bar{P})$.

С этой целью любой подстановке $a \in S_n$ отнесем некоторое преобразование S поля Q , определив его формулой (3). Так как любой элемент поля Q единственным образом записывается в виде (2), то формула (3) действительно определяет некоторое однозначное преобразование поля Q . Легко видеть, что преобразование S взаимно однозначно (именно обратное преобразование тем же способом строится с помощью подстановки a^{-1}) и сохраняет операции сложения и умножения, т. е. является автоморфизмом поля S . Наконец, если элемент (2) принадлежит полю \bar{P} , т. е. выражается через a_1, \dots, a_n , то многочлены f и g являются симметрическими многочленами, и потому $f_a = f$, $g_a = g$, т. е. автоморфизм S оставляет элемент (2) на месте. Таким образом, S является автоморфизмом поля Q над полем \bar{P} , т. е. $S \in G(Q, \bar{P})$. Остается заметить, что соответствующая автоморфизму S подстановка совпадает, очевидно, с подстановкой a .

Тем самым доказано, что группа Галуа $G(Q, P)$ изоморфна симметрической группе S_n , т. е.

группа Галуа общего уравнения степени n над произвольным полем P изоморфна симметрической группе S_n степени n .

Следовательно,

общее уравнение степени n при $n \geq 5$ неразрешимо в радикалах (каково бы ни было поле P).

Напротив,

если $n \leq 4$, то общее уравнение степени n в радикалах разрешимо.

Последний результат общеизвестен (см. Курс, стр. 233—240), однако небезинтересно вывести известные формулы решения уравнений степени $n \leq 4$ из общих соображений теории Галуа.

4. Решение уравнений низших степеней

Рассмотрим сначала квадратное уравнение

$$x^2 + a_1x + a_2 = 0. \quad (1)$$

Пусть t_1, t_2 — его корни и $Q = \bar{C}(t_1, t_2)$ — его поле разложения над полем $\bar{C} = C(a_1, a_2)$ (так как основное поле P не играет никакой роли, то мы принимаем за него поле C комплексных чисел). Группой Галуа уравнения (1) является симметрическая группа S_2 . Так как эта группа является циклической группой второго порядка и, следовательно, не имеет никаких подгрупп, то и поле Q не имеет никаких промежуточных подполей. Поэтому, например, поле $\bar{C}(t_1)$ совпадает с полем Q :

$$Q = \bar{C}(t_1).$$

Единственный не тождественный автоморфизм S поля Q над полем \bar{C} переводит корень t_1 в корень t_2 :

$$t_1^S = t_2$$

(ибо в противном случае $S = E$).

Согласно общей теории, мы должны составить резольвенты Лагранжа. Так как первообразным корнем из единицы

степени 2 является число -1 , то резольвенты Лагранжа имеют в нашем случае вид

$$\begin{aligned}(-1, t_1) &= t_1 - t_2, \\(1, t_1) &= t_1 + t_2.\end{aligned}$$

Обозначим резольвенту $(-1, t_1)$ буквой θ :

$$\theta = t_1 - t_2.$$

Другая резольвента является элементарным симметрическим многочленом

$$t_1 + t_2 = -a_1.$$

Из равенств $t_1 + t_2 = -a_1$ и $t_1 - t_2 = \theta$ вытекает, что

$$2t_1 = -a_1 + \theta, \quad 2t_2 = -a_1 - \theta$$

(что также согласуется с общей теорией; см. гл. 2, п. 2), т. е. что

$$t_{1,2} = \frac{-a_1 \pm \theta}{2}.$$

Далее,

$$\theta^2 = t_1^2 + t_2^2 - 2t_1 t_2 = a_2^2 - 4a_1$$

и, следовательно,

$$\theta = \sqrt{a_2^2 - 4a_1}.$$

Таким образом, мы действительно получили известные формулы решения квадратного уравнения.

Рассмотрим теперь кубическое уравнение

$$y^3 + a_1 y^2 + a_2 y + a_3 = 0.$$

Полагая

$$x = y + \frac{a_1}{3},$$

мы приведем его к виду

$$x^3 + px + q = 0, \tag{2}$$

где

$$p = -\frac{a_1^2}{3} + a_2, \quad q = \frac{2a_1^3}{27} - \frac{a_2 a_1}{3} + a_3.$$

(Это преобразование не вызывается существом дела и производится только для упрощения дальнейших выкладок.)

Пусть t_1, t_2, t_3 — корни уравнения (2) и, следовательно, $Q = \bar{C}(t_1, t_2, t_3)$, где $\bar{C} = C(p, q)$ — его поле разложения. Как мы знаем, группа Галуа S_3 этого уравнения обладает разрешимым рядом

$$S_3 \supset A_3 \supset e.$$

Пусть L — промежуточное поле

$$\bar{C} \subset L \subset Q,$$

соответствующее подгруппе A_3 . Тогда группой Галуа $G(Q, L)$ поля Q над полем L является группа A_3 . Эта группа циклическая, третьего порядка и ее образующей является, например, подстановка $(1\ 2\ 3)$. Пусть S — автоморфизм, соответствующий этой подстановке:

$$t_1^S = t_2, \quad t_2^S = t_3, \quad t_3^S = t_1.$$

Так как $t_1^S \neq t_1$, то $t_1 \notin L$. Следовательно, поле $L(t_1)$ должно совпадать со всем полем Q :

$$Q = L(t_1)$$

(почему?). В соответствии с общей теорией мы должны рассмотреть резольвенты Лагранжа

$$(p, t_1) = t_1 + pt_1^S + p^2t_1^{S^2} = t_1 + pt_2 + p^2t_3,$$

$$(p^2, t_1) = t_1 + p^2t_1^S + p^4t_1^{S^2} = t_1 + p^2t_2 + p^4t_3,$$

$$(p^3, t_1) = t_1 + p^3t_1^S + p^6t_1^{S^2} = t_1 + p^3t_2 + p^6t_3,$$

где

$$p = \frac{-1 + \sqrt{-3}}{2}$$

— первообразный корень третьей степени из единицы. Так как $p^2 = \bar{p}$ и $p^3 = 1$, то

$$(p, t_1) = t_1 + pt_2 + \bar{p}t_3,$$

$$(p^2, t_1) = t_1 + \bar{p}t_2 + pt_3,$$

$$(p^3, t_1) = t_1 + t_2 + t_3 = 0.$$

Складывая все три резольвенты, мы получим

$$3t_1 = (p, t_1) + (p^2, t_1). \quad (3)$$

(третью резольвенту мы не пишем, так как она равна нулю). Этот результат также согласуется с общей теорией.

Согласно общей теории, третья степень резольвенты (ρ, t_1) должна принадлежать полю L . Но

$$\begin{aligned} (\rho, t_1)^3 &= t_1^3 + t_2^3 + t_3^3 + 3\rho(t_1^2t_2 + t_2^2t_3 + t_3^2t_1) + \\ &\quad + 3\bar{\rho}(t_1t_2^2 + t_2t_3^2 + t_3t_1^2) + 6t_1t_2t_3 = \\ &= t_1^3 + t_2^3 + t_3^3 - \frac{3}{2}(t_1^2t_2 + t_2^2t_3 + t_3^2t_1 + t_1t_2^2 + t_2t_3^2 + t_3t_1^2) + \\ &\quad + 6t_1t_2t_3 + \frac{3\sqrt{-3}}{2}(t_1^2t_2 + t_2^2t_3 + t_3^2t_1 - t_1t_2^2 - t_2t_3^2 - t_3t_1^2). \end{aligned}$$

Выражая симметрические многочлены через элементарные (и учитывая, что $t_1 + t_2 + t_3 = 0$, $t_1t_2 + t_1t_3 + t_2t_3 = p$, $t_1t_2t_3 = -q$), мы получим

$$\begin{aligned} t_1^3 + t_2^3 + t_3^3 &= -3q, \\ t_1^2t_2 + t_2^2t_3 + t_3^2t_1 + t_1t_2^2 + t_2t_3^2 + t_3t_1^2 &= 3q, \\ t_1t_2t_3 &= -q. \end{aligned}$$

Далее, легко видеть, что

$$t_1^2t_2 + t_2^2t_3 + t_3^2t_1 - t_1t_2^2 - t_2t_3^2 - t_3t_1^2 = \theta,$$

где

$$\theta = (t_1 - t_2)(t_1 - t_3)(t_2 - t_3).$$

Таким образом,

$$(\rho, t_1)^3 = -\frac{27}{2}q + \frac{3\sqrt{-3}}{2}\theta. \quad (4)$$

Мы видим, что действительно $(\rho, t_1)^3 \in L$, ибо $\theta^3 = \theta$, и потому $\theta \in L$.

Аналогично вычисляется, что

$$(\rho^2, t_1)^3 = -\frac{27}{2}q - \frac{3\sqrt{-3}}{2}\theta. \quad (5)$$

Найдем теперь θ . Любая транспозиция переводит θ в $-\theta$, а любая четная подстановка оставляет θ на месте. Поэтому с θ сопряжено только число $-\theta$ и, следовательно, $\theta^2 \in \bar{C}$. Действительно, простое вычисление показывает, что

$$\theta^2 = -4p^3 - 27q^2. \quad (6)$$

Сопоставляя формулы (3), (4), (5) и (6), находим окончательно следующую формулу решения кубического уравнения:

$$t_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

т. е. известную формулу Кардано.

Уравнения четвертой степени рассматриваются аналогично. Проведение соответствующих рассуждений предоставляется читателю.

III. ДОПОЛНИТЕЛЬНЫЕ ВОПРОСЫ ТЕОРИИ ГАЛУА

ГЛАВА I

ПРАКТИЧЕСКОЕ ВЫЧИСЛЕНИЕ ГРУПП ГАЛУА УРАВНЕНИЙ

1. Задание групп подстановок степени n многочленами от n неизвестных

Пусть $g(x_1, \dots, x_n)$ — произвольный многочлен (с коэффициентами из основного поля P) от n переменных x_1, \dots, x_n , и пусть

$$a = \begin{pmatrix} 1 & 2 & \dots & n \\ l_1 & l_2 & \dots & l_n \end{pmatrix}$$

— произвольная подстановка степени n . Воздействуя на неизвестные x_1, \dots, x_n подстановкой a , мы получим из многочлена $g(x_1, \dots, x_n)$ многочлен

$$g_a(x_1, \dots, x_n) = g(x_{l_1}, \dots, x_{l_n})$$

(см. ч. I, гл. 3, п. 1). Мы будем говорить, что многочлен $g(x_1, \dots, x_n)$ принадлежит подстановке a , если многочлен $g_a(x_1, \dots, x_n)$ совпадает с многочленом $g(x_1, \dots, x_n)$.

Любой многочлен принадлежит тождественной подстановке e . Многочлен, принадлежащий всем подстановкам степени n , является симметрическим многочленом.

Пусть теперь G — произвольная группа подстановок степени n . Мы будем говорить, что многочлен $g(x_1, \dots, x_n)$ принадлежит группе G , если он принадлежит (в смысле предыдущего определения) любой подстановке из группы G . Ясно, что, если многочлен $g(x_1, \dots, x_n)$ принадлежит группе G , то он принадлежит и любой подгруппе H этой группы. Мы будем говорить, что многочлен $g(x_1, \dots, x_n)$ точно принадлежит группе G , если он не принадлежит никакой большей группе.

Легко видеть, что любой многочлен $g(x_1, \dots, x_n)$ от n неизвестных точно принадлежит одной (и только одной) группе G подстановок степени n . Эта группа состоит из всех подстановок $a \in S_n$, для которых $g_a = g$.

Покажем теперь, что

многочлен $g(x_1, \dots, x_n)$ тогда и только тогда точно принадлежит группе G , когда для любых двух подстановок a и b степени n из равенства $g_a = g_b$ вытекает включение $ab^{-1} \in G$, и обратно, из включения $ab^{-1} \in G$ вытекает равенство $g_a = g_b$.

Действительно, если $g_a = g_b$, то $g_{ab^{-1}} = g_e = g$, и потому для многочлена g , точно принадлежащего группе G , равенство $g_a = g_b$ имеет место тогда и только тогда, когда $ab^{-1} \in G$. Обратно, если равенство $g_a = g_b$ имеет место тогда и только тогда, когда $ab^{-1} \in G$, то, полагая $b = e$, мы получим, что равенство $g_a = g (= g_e)$ имеет место тогда и только тогда, когда $a \in G$, т. е. получим, что многочлен g точно принадлежит группе G .

Будем говорить, что подстановки

$$a_1 = e, a_2, \dots, a_m \quad (1)$$

составляют полную систему представителей смежных классов симметрической группы S_n по ее подгруппе G , если все смежные классы

$$G = Ga_1, Ga_2, \dots, Ga_m$$

различны и любой смежный класс Ga группы S_n по подгруппе G среди них содержится. Таким образом, число m равно индексу группы G в группе S_n .

Из доказанной выше теоремы немедленно вытекает, что многочлен $g(x_1, \dots, x_n)$ тогда и только тогда точно принадлежит группе G , когда для любой полной системы (1) представителей смежных классов группы S_n по подгруппе G все многочлены

$$g = g_{a_1}, g_{a_2}, \dots, g_{a_m}$$

поларно различны и любой многочлен вида g_a среди них содержится.

Покажем теперь, что

для произвольной группы G подстановок степени n существует (над любым полем P) многочлен $g(x_1, \dots, x_n)$, точно принадлежащий этой группе.

С этой целью мы рассмотрим многочлен

$$h(x_1, \dots, x_n) = c_1x_1 + c_2x_2 + \dots + c_nx_n,$$

где c_1, c_2, \dots, c_n — произвольные попарно различные элементы поля P . Ясно, что для любой нетождественной подстановки a степени n многочлен h_a отличен от многочлена h . Другими словами, многочлен h точно принадлежит единичной подгруппе $e \subset S_n$.

Пусть теперь

$$b_1 = e, b_2, \dots, b_s$$

— все подстановки группы G . Рассмотрим многочлен $\varphi(t, x_1, \dots, x_n)$ от $n+1$ неизвестных t, x_1, \dots, x_n , определенный формулой

$$\varphi(t, x_1, \dots, x_n) = (t - h_{b_1})(t - h_{b_2}) \dots (t - h_{b_s}).$$

Этот многочлен можно рассматривать либо как многочлен над полем P от $n+1$ неизвестных t, x_1, \dots, x_n , либо как многочлен от n неизвестных x_1, \dots, x_n над полем $P(t)$ рациональных функций от t (с коэффициентами из поля P), либо, наконец, как многочлен от одного неизвестного t над полем $P(x_1, \dots, x_n)$ рациональных функций от неизвестных x_1, \dots, x_n (с коэффициентами из поля P).

Рассматривая его как многочлен над полем $P(t)$, мы можем воздействовать на него подстановками a степени n , получая многочлены $\varphi_a(t, x_1, \dots, x_n)$. Рассматривая его как многочлен от t над полем $P(x_1, \dots, x_n)$, мы можем говорить о его корнях. Ясно, что этими корнями служат многочлены $h = h_{b_1}, h_{b_2}, \dots, h_{b_s}$. В этом же смысле корнями многочлена $\varphi_a(t, x_1, \dots, x_n)$ являются многочлены $h_a = h_{b_1a}, h_{b_2a}, \dots, h_{b_sa}$.

Так как набор многочленов h_{b_1}, \dots, h_{b_s} тогда и только тогда совпадает (с точностью до порядка) с набором $h_{b_1a}, \dots, h_{b_sa}$, когда $a \in G$, то $\varphi_a = \varphi$ тогда и только тогда, когда $a \in G$. Другими словами, многочлен φ (рассматриваемый как многочлен от x_1, \dots, x_n над полем $P(t)$) точно принадлежит группе G .

Пусть теперь

$$a_1 = e, a_2, \dots, a_m$$

— произвольная полная система представителей смежных классов группы S_n по ее подгруппе G . Тогда все многочлены

$$\varphi_{a_1}(t, x_1, \dots, x_n), \varphi_{a_2}(t, x_1, \dots, x_n), \dots, \varphi_{a_m}(t, x_1, \dots, x_n)$$

попарно различны и любой многочлен вида $\varphi_a(t, x_1, \dots, x_n)$ равен одному из этих многочленов. Поскольку поле P бесконечно (оно содержит все рациональные числа), в нем можно найти такое число t_0 , что многочлены

$$\varphi_{a_1}(t_0, x_1, \dots, x_n), \varphi_{a_2}(t_0, x_1, \dots, x_n), \dots, \varphi_{a_m}(t_0, x_1, \dots, x_n)$$

над полем P от неизвестных x_1, \dots, x_n будут все попарно различны (число t_0 следует взять отличным от корней каждого из многочленов $\varphi_{a_i}(t, x_1, \dots, x_n) - \varphi_{a_j}(t, x_1, \dots, x_n)$, рассматриваемых как многочлены от t над полем $P(x_1, \dots, x_n)$). Таким образом, многочлен

$$g(x_1, \dots, x_n) = \varphi(t_0, x_1, \dots, x_n)$$

(над полем P) будет обладать тем свойством, что равенство $g_a = g_b$ имеет место тогда и только тогда, когда для многочлена φ (над полем $P(t)$) имеет место равенство $\varphi_a = \varphi_b$. Отсюда следует, что поскольку многочлен φ точно принадлежит группе G , многочлен g также обладает этим свойством.

Теорема полностью доказана.

Так как многочлен, точно принадлежащий группе, однозначно эту группу определяет, а, согласно только что доказанной теореме, такой многочлен существует для любой группы подстановок, то мы можем задавать группы подстановок, выписывая многочлены, точно им принадлежащие.

2. Сопряженные группы подстановок

Легко видеть, что для любой группы G подстановок степени n и любой подстановки a той же степени n совокупность $a^{-1}Ga$ всех подстановок вида $a^{-1}ba$, где b — произвольная подстановка группы G , представляет собой группу,

изоморфную группе G (изоморфизм осуществляется соответствием $b \rightarrow a^{-1}ba$). Эта группа называется группой подстановок, *сопряженной* группе G (посредством подстановки a).

Очевидно, что множество всех групп подстановок степени n распадается на непересекающиеся классы, обладающие тем свойством, что две группы тогда и только тогда принадлежат одному классу, когда они сопряжены. Эти классы называются *классами сопряженных групп*. Класс, содержащий группу G , мы будем обозначать символом $[G]$.

Легко видеть, что

если многочлен $g(x_1, \dots, x_n)$ точно принадлежит группе G , то многочлен $g_a(x_1, \dots, x_n)$, где $a \in S_n$, точно принадлежит сопряженной группе $a^{-1}Ga$.

Действительно, равенство $(g_a)_b = g_a$, т. е. равенство $g_{ab} = g_a$, имеет место тогда и только тогда, когда $aba^{-1} \in G$, т. е. когда $b \in a^{-1}Ga$.

Отсюда вытекает, что все группы класса $[G]$ задаются многочленами

$$g = g_{a_1}, g_{a_2}, \dots, g_{a_m}, \quad (1)$$

где

$$a_1 = e, a_2, \dots, a_m$$

— произвольная полная система представителей смежных классов группы S_n по ее подгруппе G . (Заметим, что разные многочлены из системы (1) вполне могут принадлежать одной и той же группе класса $[G]$.)

Вместо многочленов (1) для задания групп класса $[G]$ можно воспользоваться одним многочленом $G(z)$ над полем $P(x_1, \dots, x_n)$ от некоторого нового неизвестного z , а именно многочленом

$$G(z) = (z - g_{a_1})(z - g_{a_2}) \dots (z - g_{a_m}).$$

Мы будем называть многочлен $G(z)$ определяющим многочленом класса $[G]$.

Подчеркнем, что он зависит от выбора многочлена $g(x_1, \dots, x_n)$.

Легко видеть, что

все коэффициенты определяющего многочлена $G(z)$ являются симметрическими многочленами от неизвестных x_1, \dots, x_n .

Задача. Докажите это утверждение.

3. Вычисление группы Галуа произвольного многочлена

Пусть

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$$

— произвольный многочлен над полем P без кратных корней. Раз и навсегда занумеровав его корни

$$\alpha_1, \dots, \alpha_n$$

в некотором определенном порядке, будем рассматривать его группу Галуа как группу подстановок степени n .

Пусть теперь G — произвольная группа подстановок степени n и пусть $G(z)$ — определяющий многочлен класса $[G]$. Подставив в коэффициенты многочлена $G(z)$ вместо неизвестных x_1, \dots, x_n числа $\alpha_1, \dots, \alpha_n$, мы получим некоторый многочлен $g(z)$ уже с числовыми коэффициентами. Поскольку коэффициенты многочлена $G(z)$ являются симметрическими многочленами от неизвестных x_1, \dots, x_n , все коэффициенты многочлена $g(z)$ принадлежат полю P .

Легко видеть, что

если группа Галуа многочлена $f(x)$ содержится в группе G , то хотя бы один корень многочлена $g(z)$ принадлежит полю P .

Действительно, корнями многочлена $g(z)$ являются элементы

$$\beta_1 = g_{a_1}(\alpha_1, \dots, \alpha_n), \beta_2 = g_{a_2}(\alpha_1, \dots, \alpha_n), \dots, \beta_m = g_{a_m}(\alpha_1, \dots, \alpha_n)$$

поля $K = P(\alpha_1, \dots, \alpha_n)$, где $g(x_1, \dots, x_n)$ — точно принадлежащий группе G многочлен от неизвестных x_1, \dots, x_n , по которому был построен определяющий многочлен $G(z)$, а $a_1 = e, a_2, \dots, a_m$ — полная система представителей смежных классов группы S_n по ее подгруппе G . Если группа Галуа многочлена $f(x)$ содержится в группе G , то любая ее подстановка a не меняет многочлена g , т. е. $g_a = g$. Пусть S — автоморфизм поля K над полем P , которому соответствует подстановка a . Тогда

$$\beta_1^S = g(\alpha_1, \dots, \alpha_n)^S = g_a(\alpha_1, \dots, \alpha_n) = g(\alpha_1, \dots, \alpha_n) = \beta_1.$$

Поскольку S представляет собой произвольный автоморфизм поля K над полем P , отсюда вытекает (см. ч. I, гл. 3, п. 4), что элемент β_1 принадлежит основному полю P .

Обратное утверждение справедливо в следующей форме:
если многочлен $g(z)$ не имеет кратных корней и хотя бы один его корень принадлежит полю P , то группа Галуа многочлена $f(x)$ содержится в некоторой группе, сопряженной группе G .

Действительно, пусть a — произвольная подстановка группы Галуа многочлена $f(x)$, и пусть S — соответствующий автоморфизм поля $K = P(\alpha_1, \dots, \alpha_n)$ над полем P . По условию, хотя бы один корень многочлена $g(z)$ содержится в поле P . Пусть это будет корень $\beta_i = g_{a_i}(\alpha_1, \dots, \alpha_n)$. Так как $\beta_i \in P$, то $\beta_i^S = \beta_i$. С другой стороны,

$$\beta_i^S = g_{a_i a}(\alpha_1, \dots, \alpha_n) = g_{a_j}(\alpha_1, \dots, \alpha_n) = \beta_j,$$

где a_j — представитель смежного класса, содержащего подстановку $a_i a$ (таким образом, $a_i a = b a_j$, где $b \in G$). Поскольку многочлен $g(z)$ не имеет по условию кратных корней, отсюда следует, что $\beta_i = \beta_j$, т. е. что $i = j$. Таким образом, $a_i a = b a_i$, где $b \in G$, т. е. $a \in a_i^{-1} G a_i$. Так как это верно для любой подстановки a группы Галуа, то и вся группа Галуа многочлена $f(x)$ содержится в группе $a_i^{-1} G a_i$. Теорема доказана.

Доказанные теоремы дают удобный практический способ определения класса сопряженных групп, которому принадлежит группа Галуа любого многочлена, т. е. вычисления этой группы «с точностью до изоморфизма». Правда, для его проведения требуется уметь определять, имеет ли данное уравнение над полем P хотя бы один корень, содержащийся в этом поле, что для случая произвольного поля представляет собой сложную задачу, не имеющую пока общего решения. Однако на практике основным полем P является, как правило, поле R рациональных чисел, для которого эта задача имеет простое и эффективное решение (см. Курс, стр. 355—358).

Другое затруднение связано с тем, что многочлен $g(z)$ может иметь кратные корни, и потому доказанный выше критерий будет неприменим. На практике в этом случае целесообразнее всего произвести дополнительное исследование, пользуясь теми или иными частными соображениями. Однако с теоретической точки зрения это затруднение преодолевается легко. Именно, оказывается, что

для любой группы G и любого многочлена $f(x)$ над полем P без кратных корней всегда существует такой многочлен $g(x_1, \dots, x_n)$, точно принадлежащий группе G , что соответствующий многочлен $g(z)$ не имеет кратных корней.

Для доказательства этого утверждения, очевидно, достаточно доказать, что

существует такой многочлен $g(x_1, \dots, x_n)$, точно принадлежащий группе G , что для любых подстановок a и b степени n равенство $g_a(\alpha_1, \dots, \alpha_n) = g_b(\alpha_1, \dots, \alpha_n)$, где $\alpha_1, \dots, \alpha_n$ — корни многочлена $f(x)$, имеет место тогда и только тогда, когда многочлены $g_a(x_1, \dots, x_n)$ и $g_b(x_1, \dots, x_n)$ совпадают, т. е. когда $ab^{-1} \in G$.

С этой целью мы докажем следующее вспомогательное предложение:

в поле P существуют такие числа c_1, \dots, c_n , что для любого $k = 1, 2, \dots, n$ многочлен

$$h^{(k)}(x_1, \dots, x_n) = c_1 x_1 + c_2 x_2 + \dots + c_k x_k$$

обладает следующим свойством:

если подстановки a и b степени n по-разному перемещают хотя бы одно из чисел $1, 2, \dots, k$, то

$$h_a^{(k)}(\alpha_1, \dots, \alpha_n) \neq h_b^{(k)}(\alpha_1, \dots, \alpha_n).$$

Доказательство мы проведем индукцией по числу k . Для $k = 1$ предложение очевидно (поскольку все корни $\alpha_1, \dots, \alpha_n$ различны, за c_1 можно взять любое отличное от нуля число поля P). Пусть это предложение уже доказано для $k - 1$, т. е. пусть найден многочлен $h^{(k-1)}(x_1, \dots, x_n)$, обладающий требуемым свойством. Поскольку поле P содержит бесконечно много элементов (например, все рациональные числа), в нем найдется число c_k , отличное от всех чисел вида

$$\frac{h_a^{(k-1)}(\alpha_1, \dots, \alpha_n) - h_b^{(k-1)}(\alpha_1, \dots, \alpha_n)}{\alpha_{l_k} - \alpha_{j_k}},$$

где a и b — произвольные подстановки степени n , перемещающие число k в различные числа l_k и j_k . Очевидно, что многочлен

$$h^{(k)}(x_1, \dots, x_n) = h^{(k-1)}(x_1, \dots, x_n) + c_k x_k$$

обладает всеми требуемыми свойствами. Предложение доказано.

Рассмотрим, в частности, многочлен

$$h(x_1, \dots, x_n) = h^{(n)}(x_1, \dots, x_n) = c_1 x_1 + c_2 x_2 + \dots + c_n x_n.$$

По доказанному он обладает следующим свойством:

если подстановки a и b степени n различны, то

$$h_a(\alpha_1, \dots, \alpha_n) \neq h_b(\alpha_1, \dots, \alpha_n).$$

Положим этот многочлен в основу определения нужного нам многочлена $g(x_1, \dots, x_n)$ (см. п. 1), т. е. рассмотрим многочлен

$$\varphi(t, x_1, \dots, x_n) = (t - h_{b_1})(t - h_{b_2}) \dots (t - h_{b_s}),$$

где $b_1 = e, b_2, \dots, b_s$ — все подстановки группы G . Легко видеть, что

для любых двух подстановок a и b степени n многочлены $\varphi_a(t, x_1, \dots, x_n)$ и $\varphi_b(t, x_1, \dots, x_n)$ (рассматриваемые как многочлены над полем $P(t)$) тогда и только тогда совпадают, когда совпадают многочлены $\varphi_a(t, \alpha_1, \dots, \alpha_n)$ и $\varphi_b(t, \alpha_1, \dots, \alpha_n)$ от t над полем $K = P(\alpha_1, \dots, \alpha_n)$.

Действительно, если $\varphi_a(t, x_1, \dots, x_n) = \varphi_b(t, x_1, \dots, x_n)$, то $\varphi_a(t, \alpha_1, \dots, \alpha_n) = \varphi_b(t, \alpha_1, \dots, \alpha_n)$. Обратно, пусть $\varphi_a(t, \alpha_1, \dots, \alpha_n) = \varphi_b(t, \alpha_1, \dots, \alpha_n)$. Корнями многочлена $\varphi_a(t, \alpha_1, \dots, \alpha_n)$ являются числа $h_{b_1}a(\alpha_1, \dots, \alpha_n), \dots, h_{b_s}a(\alpha_1, \dots, \alpha_n)$, а корнями многочлена $\varphi_b(t, \alpha_1, \dots, \alpha_n)$ — числа $h_{b_1}b(\alpha_1, \dots, \alpha_n), \dots, h_{b_s}b(\alpha_1, \dots, \alpha_n)$. Поскольку у равных многочленов корни могут отличаться только порядком следования, среди чисел $h_{b_1}b(\alpha_1, \dots, \alpha_n), \dots, h_{b_s}b(\alpha_1, \dots, \alpha_n)$ содержится, скажем, число $h_a(\alpha_1, \dots, \alpha_n) = h_{b_1}a(\alpha_1, \dots, \alpha_n)$. Другими словами, в группе G существует такой элемент b_t , что $h_a(\alpha_1, \dots, \alpha_n) = h_{b_t}b(\alpha_1, \dots, \alpha_n)$. Следовательно, $a = b_t b$, т. е. $ab^{-1} \in G$, и потому $\varphi_a(t, x_1, \dots, x_n) = \varphi_b(t, x_1, \dots, x_n)$ (ибо многочлен $\varphi(t, x_1, \dots, x_n)$ принадлежит группе G ; см. п. 1).

Пусть теперь

$$\varphi_{a_1}(t, \alpha_1, \dots, \alpha_n), \varphi_{a_2}(t, \alpha_1, \dots, \alpha_n), \dots, \varphi_{a_m}(t, \alpha_1, \dots, \alpha_n)$$

— такие попарно различные многочлены вида $\varphi_{\alpha}(t, \alpha_1, \dots, \alpha_n)$, что любой многочлен этого вида равен одному из них. Поскольку поле P бесконечно, в нем существует такой элемент t_0 , что все числа

$\varphi_{\alpha_1}(t_0, \alpha_1, \dots, \alpha_n), \varphi_{\alpha_2}(t_0, \alpha_1, \dots, \alpha_n), \dots, \varphi_{\alpha_m}(t_0, \alpha_1, \dots, \alpha_n)$ попарно различны. Пусть

$$g(x_1, \dots, x_n) = \varphi(t_0, x_1, \dots, x_n).$$

Ясно, что многочлен $g(x_1, \dots, x_n)$ обладает всеми требуемыми свойствами.

4. Пример: уравнения, группы Галуа которых содержатся в знакопеременной группе

Применим изложенный выше общий метод к разысканию уравнений без кратных корней, группа Галуа которых содержится в знакопеременной группе A_n . Для этого, в первую очередь, следует отыскать многочлен $g(x_1, \dots, x_n)$, точно принадлежащий группе A_n . Простейший такой многочлен описывается в следующей теореме.

Знакопеременной группе A_n точно принадлежит многочлен

$$\begin{aligned} \Delta(x_1, \dots, x_n) = & (x_2 - x_1)(x_3 - x_1) \dots (x_n - x_1) \times \\ & \times (x_3 - x_2) \dots (x_n - x_2) \times \\ & \dots \dots \dots \dots \dots \times (x_n - x_{n-1}) \end{aligned}$$

(так называемый определитель Вандермонда для неизвестных x_1, \dots, x_n ; см. Курс. стр. 50).

Действительно, под воздействием четных подстановок этот многочлен, очевидно, не меняется, а под воздействием нечетных меняет знак.

Соответствующий определяющий многочлен $G(z)$ класса $[A_n]$ (заметим кстати, что этот класс содержит только группу A_n) имеет, следовательно, вид

$$z^2 - D(x_1, \dots, x_n),$$

где $D(x_1, \dots, x_n) = \Delta^2(x_1, \dots, x_n)$.

Таким образом, для того чтобы решить, содержится ли группа Галуа некоторого многочлена $f(x)$ с корнями $\alpha_1, \dots, \alpha_n$ в знакопеременной группе A_n , мы должны рассмотреть многочлен

$$g(z) = z^2 - D(\alpha_1, \dots, \alpha_n).$$

Число $D(\alpha_1, \dots, \alpha_n)$ (содержащееся в основном поле P) представляет собой не что иное, как *дискриминант* многочлена $f(x)$ (см. Курс., стр. 343). Это число отлично от нуля (ибо многочлен $f(x)$ не имеет по условию кратных корней), и поэтому корни $\Delta(\alpha_1, \dots, \alpha_n)$ и $-\Delta(\alpha_1, \dots, \alpha_n)$ многочлена $g(z)$ различны. Отсюда ввиду общей теоремы, доказанной в п. 3, вытекает следующий результат:

группа Галуа многочлена $f(x)$ тогда и только тогда содержится в знакопеременной группе, когда $\Delta(\alpha_1, \dots, \alpha_n) \in P$, т. е. когда дискриминант многочлена $f(x)$ является квадратом некоторого элемента поля P .

5. Уравнения третьей и четвертой степени

Применим теперь изложенную выше теорию к задаче вычисления группы Галуа многочленов третьей и четвертой степени. Для простоты мы ограничимся случаем, когда данный многочлен неприводим. Тогда его группа Галуа транзитивна (см. ч. II, гл. 3, п. 5). Но легко видеть, что единственными транзитивными группами подстановок третьей степени являются симметрическая группа S_3 и знакопеременная группа A_3 (доказать!). Следовательно,

группой Галуа неприводимого уравнения третьей степени является либо симметрическая группа S_3 (циклическая группа шестого порядка), либо знакопеременная группа A_3 (циклическая группа третьего порядка); в первом случае дискриминант уравнения не является точным квадратом некоторого элемента основного поля, а во втором является таким квадратом.

Что же касается группы S_4 , то можно показать (сделайте это!), что любая ее нетривиальная транзитивная подгруппа либо совпадает с группой A_4 , либо совпадает с клейновской группой B_4 (см. стр. 101), либо сопряжена с группой B_4' восьмого

порядка, состоящей из подстановок

$$\begin{aligned} e, t_1, t_2, t_3, \\ s, t_1s, t_2s, t_3s, \end{aligned}$$

где e, t_1, t_2, t_3 — подстановки группы B_4 , а s — транспозиция (1 2). При этом класс $[B'_4]$ состоит из трех групп (перечислите эти группы), пересечение которых совпадает с группой B_4 .

Группе B'_4 точно принадлежит многочлен $g(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4$. Соответствующий многочлен $G(z)$ (см. п. 2) имеет, как легко видеть, вид

$$z^3 - \sigma_2 z^2 + (\sigma_1 \sigma_3 - 4\sigma_4) z - \sigma_4 (\sigma_1^2 - 4\sigma_2) - \sigma_3^2,$$

где $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ — элементарные симметрические функции переменных x_1, x_2, x_3, x_4 .

Пусть теперь

$$f(x) = x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4$$

— произвольный многочлен четвертой степени без кратных корней над полем P . Согласно сказанному в п. 3, для решения вопроса о том, не является ли его группа Галуа подгруппой группы B'_4 (или группы, сопряженной с группой B'_4), мы должны составить многочлен

$$g(z) = z^3 - a_2 z^2 + (a_1 a_3 - 4a_4) z - a_4 (a_1^2 - 4a_2) - a_3^2. \quad (1)$$

Корнями этого многочлена являются числа

$$\alpha_1 \alpha_2 + \alpha_3 \alpha_4, \alpha_1 \alpha_3 + \alpha_2 \alpha_4, \alpha_1 \alpha_4 + \alpha_2 \alpha_3, \quad (2)$$

где $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ — корни многочлена $f(x)$. Легко видеть, что корни (2) все различны. Действительно, если, например, $\alpha_1 \alpha_2 + \alpha_3 \alpha_4 = \alpha_1 \alpha_3 + \alpha_2 \alpha_4$, то $\alpha_1(\alpha_2 - \alpha_3) = \alpha_4(\alpha_2 - \alpha_3)$, откуда $\alpha_2 = \alpha_3$ или $\alpha_1 = \alpha_4$, что противоречит предположению об отсутствии у многочлена $f(x)$ кратных корней. Таким образом, многочлен (1) не имеет кратных корней, и потому

группа Галуа многочлена $f(x)$ тогда и только тогда содержитя в группе B'_4 (или в группе, сопряженной группе B'_4), когда многочлен (1) имеет корень в поле P .

В частности,

если многочлен $f(x)$ неприводим, то многочлен (1) тогда и только тогда имеет корень в поле P , когда группа Галуа многочлена $f(x)$ либо сопряжена с группой B'_4 , либо совпадает с группой B_4 .

Поскольку $B_4 = B'_4 \cap A_4$,

последний случай имеет место тогда и только тогда, когда дискриминант многочлена $f(x)$ является точным квадратом некоторого элемента поля P .

Задача. Докажите, что группа Галуа многочлена $f(x)$ тогда и только тогда содержитя в группе B_4 , когда все три корня уравнения (1) принадлежат полю P .

Резюмируя все сказанное, мы получаем следующее правило для вычисления группы Галуа неприводимого многочлена четвертой степени:

если дискриминант многочлена $f(x)$ не является точным квадратом и многочлен (1) не имеет в поле P корней, то группой Галуа многочлена $f(x)$ является группа S_4 ;

если дискриминант многочлена $f(x)$ является точным квадратом, но многочлен (1) не имеет в поле P корней, то группой Галуа многочлена $f(x)$ является группа A_4 ;

если дискриминант многочлена $f(x)$ не является точным квадратом, но многочлен (1) имеет в поле P хотя бы один корень, то группа Галуа многочлена $f(x)$ сопряжена группе B'_4 ;

наконец, если дискриминант многочлена $f(x)$ является точным квадратом и все корни многочлена (1) принадлежат полю P (впрочем, достаточно требовать, чтобы только один корень принадлежал полю P), то группой Галуа многочлена $f(x)$ является группа B_4 .

Аналогичные результаты можно получить и для уравнений любой высшей степени. В следующей главе мы рассмотрим с этой точки зрения уравнения пятой степени.

ГЛАВА 2

УРАВНЕНИЯ ПЯТОЙ СТЕПЕНИ

1. Транзитивные группы подстановок

Начнем с доказательства следующей общей теоремы:
Порядок транзитивной группы подстановок степени n делится на n .

Действительно, пусть G — произвольная транзитивная группа подстановок степени n . Разобьем группу G на непересекающиеся классы, относя в один класс все подстановки, одинаково воздействующие на число 1. В силу транзитивности группы число этих классов равно n . Пусть H — класс, состоящий из подстановок группы G , оставляющих на месте число 1. Очевидно, что этот класс является подгруппой группы G . Две подстановки $g_1, g_2 \in G$ тогда и только тогда принадлежат одному классу, когда $g_1 g_2^{-1} \in H$, т. е. когда подстановки g_1, g_2 принадлежат одному смежному классу группы G по подгруппе H . Другими словами, рассматриваемые классы совпадают со смежными классами по подгруппе H . Следовательно, индекс подгруппы H равен n . Поскольку группа G обладает подгруппой индекса n , ее порядок делится на n . Теорема доказана.

Простейшими транзитивными группами являются циклические группы. Очевидно, что

циклическая группа подстановок степени n тогда и только тогда транзитивна, когда ее образующей служит цикл длины n .

В частности, порядок такой группы равен $n!$

Легко видеть, что

число всех циклов длины n равно $(n - 1)!$.

Действительно, любой цикл длины n единственным образом записывается в виде $(1 \ l_2 \ l_3 \dots \ l_n)$, где $l_2 \ l_3 \dots \ l_n$ — некоторая перестановка чисел $2, 3, \dots, n$,

Поскольку циклическая группа порядка n содержит $\varphi(n)$ образующих (см. стр. 63), отсюда вытекает, что

число всех циклических транзитивных групп подстановок степени n равно $\frac{(n-1)!}{\varphi(n)}$.

В частности, при $n=5$ это число равно шести.

2. Транзитивные группы простой степени

Ясно, что группа подстановок, содержащая цикл длины n , транзитивна. Оказывается, что если число n является простым числом p , то верно и обратное, т. е.

любая транзитивная группа подстановок простой степени p содержит цикл длины p .

Действительно, пусть G — произвольная транзитивная группа подстановок степени p . Разобьем множество всех циклов длины p , не принадлежащих группе G , на классы, относя циклы a_1 и a_2 к одному классу, если в группе G существует такой элемент b , что $a_2 = b^{-1}a_1b$. Класс, содержащий цикл a , мы будем обозначать символом C_a . Легко видеть, что для любых двух циклов a_1 и a_2 длины p , не принадлежащих группе G , соответствующие классы C_{a_1} и C_{a_2} либо совпадают, либо не пересекаются.

Задача. Докажите последнее утверждение.

Пусть теперь $a = (l_1 \dots l_p)$ — произвольный цикл длины p , не принадлежащий группе G , и пусть b — произвольный элемент группы G . Ясно, что если

$$b = \begin{pmatrix} l_1 & l_2 & \dots & l_p \\ j_1 & j_2 & \dots & j_p \end{pmatrix}, \quad (1)$$

то

$$b^{-1}ab = (j_1 j_2 \dots j_p),$$

т. е. подстановка $b^{-1}ab$ также является циклом длины p . Кроме того, поскольку $b(b^{-1}ab)b^{-1} = a$, цикл $b^{-1}ab$ не принадлежит группе G . Следовательно, формула

$$\varphi(b) = b^{-1}ab$$

определяет некоторое отображение φ группы G на класс C_a . Оказывается, что это отображение взаимно однозначно, т. е. из равенства $\varphi(b_1) = \varphi(b_2)$ следует равенство $b_1 = b_2$.

Действительно, если $\varphi(b_1) = \varphi(b_2)$, т. е. $b_1^{-1}ab_1 = b_2^{-1}ab_2$, то $(b_1b_2^{-1})^{-1}a(b_1b_2^{-1}) = a$, т. е. $b^{-1}ab = a$, где $b = b_1b_2^{-1}$. Таким образом, если подстановка b имеет вид (1), то $a = (j_1 j_2 \dots j_p)$, откуда немедленно следует (почему?), что $b = a^k$, где k — такое число, что $j_1 = i_{k+1}$. Если $k > 0$, то существуют такие числа u и v , что $ku + pv = 1$ (число k взаимно просто с p , потому что оно меньше p). Тогда $a = a^{ku+pv} = a^{ku} = b^u$ и, следовательно, вопреки предположению, $a \in G$. Поэтому $k = 0$, т. е. $b = e$ и $b_1 = b_2$.

Таким образом, все классы C_a состоят из одного и того же числа элементов, равного порядку группы G . Поэтому число всех циклов длины p , не принадлежащих группе G , делится на порядок группы G и, следовательно (см. п. 1) делится на число p . С другой стороны, согласно доказанному в предыдущем пункте, число всех циклов длины p равно $(p - 1)!$ и поэтому на p не делится. Следовательно, группа G непременно содержит циклы длины p . Теорема доказана.

Каждый цикл длины p , содержащийся в группе G , определяет циклическую подгруппу, состоящую из $p - 1$ циклов длины p (и тождественной подстановки). Поскольку эти циклические подгруппы пересекаются только по тождественной подстановке (почему?), общее число циклов, содержащихся в группе G , равно $(p - 1)x$, где x — число циклических подгрупп порядка p группы G . Следовательно, обозначая через py число циклов длины p , не принадлежащих группе G , мы получаем уравнение

$$(p - 1)x + py = (p - 1)!.$$

Из этого уравнения вытекает, что

$$x = (p - 2)! - pz, \quad (2)$$

где z — произвольное неотрицательное число, меньшее чем $\frac{(p - 2)!}{p}$.

3. Транзитивные группы пятой степени

При $p = 5$ число z в формуле (2) предыдущего пункта может принимать лишь значения 0 и 1. В соответствии с этим мы получаем, что $x = 1$ или 6, т. е,

транзитивная группа пятой степени содержит либо только одну циклическую группу пятого порядка либо все шесть таких групп.

Если транзитивная группа G подстановок пятой степени содержит все шесть циклических групп пятого порядка, то ввиду тождеств

$$(l \ j)(k \ l) = (l \ k \ j \ m \ l)(l \ k \ j \ l \ m),$$

$$(l \ j)(l \ k) = (l \ k \ m \ l \ j)(l \ k \ j \ l \ m)$$

группа G содержит произведения любых двух транспозиций и потому содержит любую четную подстановку. Следовательно, в этом случае группа G является либо знакопеременной группой A_5 , либо симметрической группой S_5 .

Пусть теперь группа G содержит только одну циклическую группу пятого порядка, и пусть s — образующая этой группы. Для определенности мы будем считать, что

$$s = (1 \ 2 \ 3 \ 4 \ 5).$$

Любой другой вид цикла s сводится к этому посредством соответствующей перенумеровки переставляемых символов 1, 2, 3, 4, 5.

Циклическую группу с образующей $s = (1 \ 2 \ 3 \ 4 \ 5)$ мы будем обозначать символом C_5 . Ее порядок равен пяти.

Рассмотрим теперь наряду с циклом s еще подстановку

$$r = (2 \ 5)(3 \ 4).$$

Легко видеть, что

$$r^2 = e, \quad rs = s^4r.$$

Поэтому подстановки

$$e, \quad s, \quad s^2, \quad s^3, \quad s^4,$$

$$r, \quad sr, \quad s^2r, \quad s^3r, \quad s^4r$$

образуют группу. Эта группа называется *полуметациклической группой*. Мы будем обозначать ее символом B_5 . Ее порядок равен десяти. Она содержит циклическую группу C_5 в качестве нормального делителя (докажите!), причем факторгруппа B_5/C_5 является группой второго порядка и поэтому циклична. Следовательно, группа B_5 разрешима.

Рассмотрим далее подстановку

$$t = (2 \ 3 \ 5 \ 4).$$

Легко видеть, что

$$t^4 = e, \quad ts = s^3t.$$

Поэтому подстановки

$$\begin{aligned} &e, \quad s, \quad s^2, \quad s^3, \quad s^4, \\ &t, \quad st, \quad s^2t, \quad s^3t, \quad s^4t, \\ &t^2, \quad st^2, \quad s^2t^2, \quad s^3t^2, \quad s^4t^2, \\ &t^3, \quad st^3, \quad s^2t^3, \quad s^3t^3, \quad s^4t^3 \end{aligned}$$

образуют группу. Эта группа называется *метациклической группой*. Мы будем обозначать ее символом B'_5 . Ее порядок равен двадцати. Поскольку, как легко видеть, $t^2 = r$, группа B'_5 содержит полуметациклическую группу B_5 в качестве нормального делителя индекса 2. Поэтому

группа B'_5 разрешима.

Заметим кстати, что

$$A_5 \cap B'_5 = B_5.$$

Задача. Докажите, что группа B'_5 изоморфна группе M_5 (см. ч. II, гл. 1, п. 5).

Оказывается, что

группами C_5 , B_5 , B'_5 исчерпываются (при выбранной нумерации переставляемых символов) все транзитивные группы подстановок пятой степени, содержащие только одну циклическую группу пятого порядка.

Действительно, пусть a — произвольная подстановка транзитивной группы G , содержащей только одну циклическую группу пятого порядка (а именно: при выбранной нумерации переставляемых символов группу C_5). Если эта подстановка переводит число 1 в число k , то подстановка $b = as^{-k}$ оставляет число 1 на месте. Пусть

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & l_2 & l_3 & l_4 & l_5 \end{pmatrix}.$$

Тогда

$$b^{-1}sb = (1 \ l_2 \ l_3 \ l_4 \ l_5).$$

Так как любой цикл длины 5, содержащийся в группе G , является по условию степенью цикла s , то отсюда следует, что

$$b^{-1}sb = s^k, \quad k = 1, 2, 3, 4.$$

Поскольку

$$s = (1\ 2\ 3\ 4\ 5), \quad s^3 = (1\ 4\ 2\ 5\ 3),$$

$$s^2 = (1\ 3\ 5\ 2\ 4), \quad s^4 = (1\ 5\ 4\ 3\ 2),$$

отсюда вытекает, что подстановка b совпадает с одной из следующих четырех подстановок:

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}, t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix}, t^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}, r = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$$

(ибо запись цикла в виде $(1\ l_2\ l_3\ l_4\ l_5)$ однозначна), и поэтому принадлежит группе B'_5 . Следовательно, группе B'_5 принадлежит и подстановка a . Тем самым доказано, что группа G содержится в группе B'_5 . Для завершения доказательства остается заметить, что единственными подгруппами группы B'_5 , содержащими группу C_5 , являются группы C_5 , B_5 и B'_5 .

Теорема доказана.

4. Вычисление группы Галуа неприводимого уравнения пятой степени

Пусть $f(x)$ — произвольный неприводимый (над основным полем P) многочлен пятой степени. Поскольку группа Галуа неприводимого многочлена транзитивна, эта группа должна совпадать (при соответствующей нумерации корней многочлена) с одной из пяти групп C_5 , B_5 , B'_5 , A_5 и S_5 , перечисленных в предыдущем пункте. Согласно сказанному в предыдущей главе, для того чтобы определить эту группу, следует для каждой из групп C_5 , B_5 , B'_5 и A_5 рассмотреть некоторый точно принадлежащий этой группе многочлен $g(x_1, \dots, x_5)$, составить по этому многочлену многочлен $G(z)$ над полем $P(x_1, \dots, x_5)$, подставить в коэффициенты многочлена $G(z)$ вместо неизвестных x_1, \dots, x_5 корни многочлена $f(x)$, выразить эти коэффициенты через коэффициенты многочлена $f(x)$ и определить, имеет ли полученный многочлен $g(z)$ хотя бы один корень в поле P . Если такой корень

существует и если многочлен $g(z)$ не имеет кратных корней, то группа Галуа многочлена $f(x)$ содержится в соответствующей группе C_5 , B_5 , B'_5 (или в некоторой сопряженной группе).

Степень многочлена $g(z)$, равная индексу соответствующей группы в группе S_5 , указана в следующей таблице:

C_5	24
B_5	12
B'_5	6
A_5	2

Для составления этого многочлена можно воспользоваться следующими многочленами, точно принадлежащими соответствующим группам (здесь ϵ — первообразный корень пятой степени из единицы):

$$C_5: (x_1 + \epsilon x_2 + \epsilon^2 x_3 + \epsilon^3 x_4 + \epsilon^4 x_5)^5,$$

$$B_5: x_1 x_2 + x_2 x_3 + x_3 x_4 + x_4 x_5 + x_5 x_1,$$

$$B'_5: (x_1 x_2 + x_2 x_3 + x_3 x_4 + x_4 x_5 + x_5 x_1 - x_1 x_3 - x_3 x_5 - x_5 x_2 - x_2 x_4 - x_4 x_1)^2,$$

$$A_5: \Delta(x_1, x_2, x_3, x_4, x_5) \quad (\text{см. гл. 1, п. 4}).$$

В общем случае коэффициенты соответствующих многочленов $g(z)$ (конечно, кроме многочлена, соответствующего группе A_5) весьма сложно выражаются через коэффициенты многочлена $f(x)$, и мы их вычислять не будем. Однако с принципиальной стороны это вычисление не представляет никаких трудностей и требует лишь определенного терпения. Во всяком случае, для каждого конкретного уравнения (с числовыми коэффициентами) это вычисление всегда можно провести до конца в конечное число чисто механических действий. На практике следует в первую очередь найти дискриминант D многочлена $f(x)$. Если он не является полным квадратом, то группа Галуа многочлена либо совпадает с симметрической группой S_5 , либо сопряжена с метациклической группой B'_5 . В противном случае группа Галуа сопряжена с одной из трех групп C_5 , B_5 , A_5 . Полезно также иметь в виду, что если многочлен $g(z)$, соответствующий

группе C_5 , имеет корень в поле P (и не имеет кратных корней), то группа Галуа данного многочлена сопряжена с группой C_5 (ибо эта группа не имеет транзитивных подгрупп).

5. Определяющий многочлен для метациклической группы

Рассмотрим подробнее многочлен $G(z)$ для метациклической группы B'_5 . За исходный многочлен g , точно принадлежащий группе B'_5 , мы примем указанный в предыдущем пункте многочлен h^2 , где

$$h = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 - x_1x_3 - \\ - x_3x_5 - x_5x_2 - x_2x_4 - x_4x_1.$$

Легко проверяется, что подстановки

$$s_1 = e, \quad s_2 = (1\ 2\ 3), \quad s_3 = (2\ 3\ 4), \quad s_4 = (3\ 4\ 5), \\ s_5 = (1\ 4\ 5), \quad s_6 = (1\ 2\ 5)$$

образуют полную систему представителей смежных классов группы S_5 по ее подгруппе B'_5 . Следовательно,

$$G(z) = (z - h^2)(z - h_{s_2}^2)(z - h_{s_3}^2)(z - h_{s_4}^2)(z - h_{s_5}^2)(z - h_{s_6}^2).$$

Положим

$$H(z) = (z - h)(z - h_{s_2})(z - h_{s_3})(z - h_{s_4})(z - h_{s_5})(z - h_{s_6}).$$

Ясно, что

$$G(z^2) = H(z)H(-z).$$

Таким образом, достаточно вычислить лишь многочлен $H(z)$. Пусть

$$H(z) = z^6 + b_1z^5 + b_2z^4 + b_3z^3 + b_4z^2 + b_5z + b_6.$$

Без труда проверяется, что многочлен h точно принадлежит полуметациклической группе B_5 , причем под воздействием подстановок из группы B'_5 , не принадлежащих группе B_5 , этот многочлен лишь меняет знак. Следовательно, для любой подстановки $a \in S_5$ многочлен h_a совпадает с одним из многочленов h_{s_l} или $-h_{s_l}$, причем первый случай имеет место, когда подстановка a четна, а второй — когда она нечетна. Отсюда вытекает, что коэффициенты b_2, b_4, b_6

многочлена $H(z)$, являющиеся симметрическими функциями многочленов h_{s_l} четной степени, не меняются под воздействием произвольной подстановки $a \in S_5$, т. е. являются симметрическими многочленами от x_1, x_2, x_3, x_4, x_5 . Напротив, коэффициенты b_1, b_3, b_5 , являющиеся симметрическими функциями многочленов h_{s_l} нечетной степени, не меняются лишь под воздействием четных подстановок и меняют свой знак под воздействием нечетных подстановок.

Но легко видеть, что любой, обладающий этим свойством многочлен $b(x_1, \dots, x_5)$ делится на определитель Вандермонда $\Delta = \Delta(x_1, \dots, x_5)$. Для доказательства следует рассмотреть многочлен $b(x_1, \dots, x_5)$ как многочлен от x_1 над полем $P(x_2, \dots, x_5)$. Очевидно, что величины x_2, \dots, x_5 являются его корнями, т. е. при подстановке в многочлен $b(x_1, \dots, x_5)$ вместо неизвестной x_1 любой из неизвестных x_2, \dots, x_5 этот многочлен обращается в нуль. Действительно, например, многочлен $b(x_2, x_2, \dots, x_5)$ под воздействием транспозиции (12) с одной стороны не меняется, а с другой — меняет знак. Поэтому он равен нулю. Следовательно, многочлен $b(x_1, \dots, x_5)$ делится на разности $x_1 - x_2, \dots, x_1 - x_5$ (теорема Безу). По аналогичным соображениям он делится и на все другие разности вида $x_i - x_j$, а потому делится и на их произведение Δ . Соответствующее частное b/Δ является, очевидно, симметрическим многочленом от x_1, \dots, x_5 .

Таким образом, мы видим, что многочлен $H(z)$ имеет следующий вид:

$$H(z) = z^6 + b_2 z^4 + b_4 z^2 + b_6 + \Delta (c_1 z^5 + c_3 z^3 + c_5 z),$$

где $b_2, b_4, b_6, c_1, c_3, c_5$ — некоторые симметрические многочлены от x_1, \dots, x_5 .

Оценим теперь степени многочленов c_1, c_3, c_5 . Многочлены h_{s_l} являются квадратичными формами от неизвестных x_1, \dots, x_5 . Поэтому коэффициенты b_l являются однородными многочленами степени $2l$ от x_1, \dots, x_n . В частности, многочлены $b_1 = \Delta c_1, b_3 = \Delta c_3, b_5 = \Delta c_5$ имеют соответственно степени 2, 6 и 10. Но многочлен Δ имеет степень 10. Поэтому

$$c_1 = 0, c_2 = 0, c_5 = \text{const},$$

Тем самым доказано, что

многочлен $H(z)$ имеет следующий вид:

$$H(z) = z^6 + b_2 z^4 + b_4 z^2 + b_6 + \Delta c z,$$

где b_2, b_4, b_6 — однородные симметрические многочлены от x_1, \dots, x_5 степеней 4, 8 и 12 соответственно, Δ — определитель Вандермонда и c — постоянное число (элемент поля P).

Отсюда вытекает, что

многочлен $G(z)$ имеет вид

$$G(z) = (z^3 + b_2 z^2 + b_4 z + b_6)^2 - Dc^2 z,$$

где b_2, b_4, b_6 и c имеют прежние значения, а D — квадрат определителя Δ .

6. Случай уравнений в нормальном виде

Мы будем говорить, что многочлен $f(x)$ пятой степени имеет *нормальный вид*, если

$$f(x) = x^5 + ux + v, \quad (1)$$

где u, v — элементы основного поля P . Ниже (см. п. 8) мы покажем, что любой многочлен пятой степени можно привести к такому виду, а в этом пункте мы вычислим для таких многочленов многочлен $g(z)$, получающийся из найденного в предыдущем пункте многочлена $G(z)$ подстановкой вместо неизвестных x_1, \dots, x_5 корней $\alpha_1, \dots, \alpha_5$ многочлена (1).

Мы имеем

$$g(z) = (z^3 + b_2 z^2 + b_4 z + b_6)^2 - Dc^2 z,$$

где D — дискриминант многочлена (1), c — некоторое число, не зависящее от u и v , а b_2, b_4, b_6 — симметрические многочлены от корней $\alpha_1, \dots, \alpha_5$ степеней 4, 8 и 12 соответственно. Согласно общей теории симметрических многочленов, многочлены b_2, b_4, b_6 должны выражаться через элементарные симметрические многочлены u и v . Но многочлен u имеет степень 4, а многочлен v — степень 5. Поэтому

$$b_2 = c_2 u, \quad b_4 = c_4 u^2, \quad b_6 = c_6 u^3,$$

где c_2, c_3, c_4 — некоторые постоянные (не зависящие от u и v). Таким образом,

$$g(z) = (z^3 + c_2uz^2 + c_4u^2z + c_6u^3)^2 - Dc^2z.$$

(Заметим, что коэффициент v в выражение многочлена $g(z)$ явно не входит.)

Для того чтобы найти постоянные числа c_2, c_4, c_6 и c , мы рассмотрим многочлен

$$x^5 - x \quad (u = -1, v = 0).$$

Для этого многочлена

$$\alpha_1 = 0, \quad \alpha_2 = 1, \quad \alpha_3 = -1, \quad \alpha_4 = -1, \quad \alpha_5 = 1.$$

Следовательно,

$$\begin{aligned} \Delta(\alpha_1, \dots, \alpha_5) &= \\ &= (1-0)(-1-0)(-1-0)(1-0)(-1-1)(-1-1) \times \\ &\quad \times (1-1)(-1+1)(1+1)(1+1) = \\ &= -2^2 \cdot 1(1+1)^2(1-1)^2 = -16, \end{aligned}$$

то есть

$$D = -256.$$

Таким образом, в рассматриваемом случае

$$g(z) = (z^3 - c_2z^2 + c_4z - c_6)^2 + 256c^2z,$$

то есть

$$\begin{aligned} g(z) &= z^6 - 2c_2z^5 + (c_2^2 + 2c_4)z^4 - 2(c_2c_4 + c_6)z^3 + \\ &\quad + (c_4^2 + 2c_2c_6)z^2 - (2c_4c_6 - 256c^2)z + c_6^2. \end{aligned}$$

С другой стороны, легко видеть, что

$$\begin{aligned} h(\alpha_1, \dots, \alpha_5) &= -2, \quad h_{s_4}(\alpha_1, \dots, \alpha_5) = -2, \\ h_{s_2}(\alpha_1, \dots, \alpha_5) &= -2, \quad h_{s_5}(\alpha_1, \dots, \alpha_5) = -2, \\ h_{s_1}(\alpha_1, \dots, \alpha_5) &= 2 + 4t, \quad h_{s_6}(\alpha_1, \dots, \alpha_5) = -2 + 4t. \end{aligned}$$

Поэтому

$$\begin{aligned} g(z) &= (z + 4)^4(z + 12 - 16t)(z + 12 + 16t) = z^6 + 40z^5 + \\ &\quad + 880z^4 + 8960z^3 + 44800z^2 + 108544z + 102400. \end{aligned}$$

Приравнивая коэффициенты, мы легко получим, что

$$c_2 = 20, \quad c_4 = 240, \quad c_6 = 320, \quad c = 32.$$

Таким образом, мы окончательно получаем, что

$$g(z) = (z^3 - 20uz^2 + 240u^2z + 320u^3)^2 - 1024Dz.$$

Здесь удобно ввести новое неизвестное

$$y = \frac{z}{4}.$$

Для этого неизвестного мы получим (после сокращения на 1024) многочлен

$$(y^3 - 5uy^2 + 15u^2y + 5u^3)^2 - Dy. \quad (2)$$

Таким образом,

если многочлен (2) не имеет кратных корней, то группа Галуа многочлена (1) тогда и только тогда сопряжена некоторой подгруппе метациклической группы B'_5 , когда хотя бы один корень многочлена (2) принадлежит полю P .

Заметим, что это утверждение справедливо и для приводимых многочленов (1).

7. Уравнения пятой степени, разрешимые в радикалах

Результаты предыдущего пункта позволяют, в частности, полностью описать все уравнения пятой степени (имеющие нормальный вид), которые можно решить в радикалах. Действительно, если уравнение

$$x^5 + ux + v = 0 \quad (1)$$

приводимо, то оно сводится к уравнениям меньших степеней и потому решается в радикалах. Если же уравнение (1) не-приводимо, то его группа Галуа либо содержит группу A_5 (и поэтому неразрешима), либо сопряжена некоторой подгруппе метациклической группы (и поэтому разрешима). Кроме того, оказывается, что

если многочлен

$$(y^3 - 5uy^2 + 15u^2y + 5u^3)^2 - Dy \quad (2)$$

имеет кратный корень, то уравнение (1) решается в радикалах.

Действительно, пусть многочлен (2) имеет кратный корень y_0 . Тогда

$$(y_0^3 - 5uy_0^2 + 15u^2y_0 + 5u^3)^2 - Dy_0 = 0, \quad (3)$$

$$2(y_0^3 - 5uy_0^2 + 15u^2y_0 + 5u^3)(3y_0^2 - 10uy_0 + 15u^2) - D = 0. \quad (4)$$

Следовательно,

$$(y_0^3 - 5uy_0^2 + 15u^2y_0 + 5u^3)^2 - 2(y_0^3 - 5uy_0^2 + 15u^2y_0 + 5u^3)(3y_0^2 - 10uy_0 + 15u^2)y_0 = 0. \quad (5)$$

Если $D = 0$, то уравнение (1) имеет кратные корни, приводимо и решается в радикалах. Пусть $D \neq 0$. Тогда ввиду равенства (4)

$$y_0^3 - 5uy_0^2 + 15u^2y_0 + 5u^3 \neq 0.$$

Следовательно, после сокращения мы получим из уравнения (5) уравнение

$$5y_0^3 - 15uy_0^2 + 15u^2y_0 - 5u^3 = 0,$$

из которого следует, что

$$y_0 = u.$$

Подставляя это значение y_0 в равенство (3), мы получим, что

$$Du = 256u^6.$$

Но легко сосчитать, что для уравнения (1)

$$D = 256u^5 + 3125v^4. \quad (6)$$

Следовательно,

$$3125v^4u = 0,$$

т. е. либо $u = 0$, либо $v = 0$. В обоих случаях уравнение (1) разрешимо в радикалах.

Задача. Доказать формулу (6).

Из всего сказанного вытекает следующее окончательное утверждение.

Уравнение (1) тогда и только тогда решается в радикалах, когда оно либо приводимо, либо хотя бы один корень многочлена (2) принадлежит основному полю P .

Это утверждение справедливо для любых уравнений (1), даже имеющих кратные корни.

Пользуясь формулой (6), многочлен (2) можно переписать в следующем виде:

$$(y - u)^4(y^2 - 6uy + 25u^2) - 3125v^4y.$$

Пусть этот многочлен имеет корень $y_0 \in P$. Полагая

$$u = \frac{y_0}{\lambda}, \quad v = u\mu,$$

где λ, μ — некоторые параметры, мы получим, что

$$(u\lambda - u)^4(u^2\lambda^2 - 6u^2\lambda + 25u^2) - 3125u^5\lambda\mu^4 = 0.$$

Отсюда

$$u = \frac{3125\lambda\mu^4}{(\lambda - 1)^4(\lambda^2 - 6\lambda + 25)}, \quad v = \frac{3125\lambda\mu^5}{(\lambda - 1)^4(\lambda^2 - 6\lambda + 25)}. \quad (7)$$

Таким образом,

уравнение (1) тогда и только тогда решается в радикалах, когда оно либо приводимо, либо его коэффициенты u и v имеют вид (7), где λ и μ — некоторые элементы основного поля P .

8. Приведение уравнения пятой степени к нормальному виду

Покажем в заключение, что любое уравнение

$$a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0 \quad (1)$$

пятой степени может быть приведено к нормальному виду.

С этой целью мы введем новое неизвестное y , полагая

$$y = c_0 + c_1x + c_2x^2 + c_3x^3 + c_4x^4, \quad (2)$$

где c_0, \dots, c_4 — некоторые, пока неопределенные параметры. Для того чтобы составить уравнение, которому удовлетворяет неизвестная y , следует исключить из уравнений (1) и (2) неизвестную x . Согласно общей теории исключения (см. Курс, стр. 340), для этого нужно составить результат многочленов

$$\begin{aligned} &a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5, \\ &c_4x^4 + c_3x^3 + c_2x^2 + c_1x + (c_0 - y) \end{aligned}$$

и приравнять его нулю. В результате мы получим уравнение

$$\begin{vmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & 0 & 0 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & 0 & 0 \\ 0 & 0 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & 0 \\ 0 & 0 & 0 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \\ c_4 & c_3 & c_2 & c_1 & c_0 - y & 0 & 0 & 0 & 0 \\ 0 & c_4 & c_3 & c_2 & c_1 & c_0 - y & 0 & 0 & 0 \\ 0 & 0 & c_4 & c_3 & c_2 & c_1 & c_0 - y & 0 & 0 \\ 0 & 0 & 0 & c_4 & c_3 & c_2 & c_1 & c_0 - y & 0 \\ 0 & 0 & 0 & 0 & c_4 & c_3 & c_2 & c_1 & c_0 - y \end{vmatrix} = 0.$$

Раскрывая этот определитель, мы получим, что уравнение для y имеет вид

$$y^5 + C_1 y^4 + C_2 y^3 + C_3 y^2 + C_4 y + C_5 = 0,$$

где C_1, \dots, C_5 — некоторые однородные многочлены от параметров c_0, \dots, c_4 . Коэффициенты этих многочленов являются многочленами от коэффициентов a_0, \dots, a_5 исходного уравнения (1) и поэтому принадлежат основному полю P .

Легко видеть, что степень многочлена C_l , $l = 1, \dots, 5$, равна l .

Выберем теперь параметры c_0, \dots, c_4 так, чтобы удовлетворялись уравнения

$$C_1 = 0, \quad C_2 = 0, \quad C_3 = 0,$$

т. е. чтобы уравнение для y имело нормальный вид

$$y^5 + C_4 y + C_5 = 0. \quad (3)$$

Первое уравнение $C_1 = 0$ линейно. Получив из него выражение, скажем, параметра c_0 через параметры c_1, c_2, c_3, c_4 , внесем его в остальные два уравнения. В результате мы получим некоторые уравнения

$$C'_2 = 0, \quad C'_3 = 0$$

второй и третьей степени относительно параметров c_1, c_2, c_3, c_4 .

Выражение C'_2 представляет собой квадратичную форму от переменных c_1, c_2, c_3, c_4 . Согласно теории приведения квадратичных форм (см. Курс, стр. 175), эту форму можно

представить в следующем виде:

$$C'_2 = z_1^2 + z_2^2 + z_3^2 + z_4^2,$$

где z_1, \dots, z_4 — некоторые линейные формы (возможно, равные нулю) от неизвестных c_1, \dots, c_4 . Коэффициенты этих линейных форм, вообще говоря, принадлежат не полю P , а некоторому большему полю, порожденному над полем P корнями квадратными из элементов поля P . Потребовав, чтобы удовлетворялись линейные уравнения

$$z_1 = lz_2, \quad z_3 = lz_4 \quad (l = \sqrt{-1}), \quad (4)$$

мы автоматически удовлетворим и квадратному уравнению $C'_2 = 0$.

Решив уравнения (4), скажем, относительно неизвестных c_1, c_2 и, подставив получающиеся выражения в уравнение $C'_3 = 0$, мы получим для параметров c_3 и c_4 некоторое однородное уравнение третьей степени

$$C''_3 = 0.$$

Выбирая произвольно параметр c_3 , например полагая $c_3 = 1$, мы получим отсюда для параметра c_4 кубическое уравнение. Решив его, мы найдем параметр c_4 , а потому и все остальные параметры c_0, c_1, c_2, c_3 .

Тем самым показано, что

преобразование (2) любое уравнение (1) можно привести к нормальному виду (3).

Получающееся уравнение (3) будет уравнением уже не над полем P , а над некоторым большим полем Q , порожденным над полем P корнями квадратных и кубических уравнений. Поскольку квадратные и кубические уравнения разрешимы в радикалах, уравнение (1) тогда и только тогда разрешимо в радикалах над полем P , когда над полем Q разрешимо в радикалах уравнение (3). Поскольку на вопрос о разрешимости в радикалах уравнения (3) мы отвечать умеем, отсюда следует, что

для любого уравнения пятой степени (1) мы можем эффективно ответить на вопрос, разрешимо оно в радикалах или нет.

ГЛАВА 3

РЕШЕНИЕ УРАВНЕНИЙ В НЕПРИВОДИМЫХ РАДИКАЛАХ

1. Формулировка основной теоремы

Тот факт, что корень θ некоторого уравнения выражается в радикалах, означает, что он может быть получен в результате решения цепи двучленных уравнений вида

$$x^{n_1} - a_1 = 0, \quad x^{n_2} - a_2 = 0, \dots, \quad x^{n_s} - a_s = 0,$$

где число a_1 принадлежит основному полю P , число a_2 — полю $P_1 = P(\sqrt[n_1]{a_1})$, число a_3 — полю $P_2 = P_1(\sqrt[n_2]{a_2})$ и т. д. Таких «разрешающих» цепей двучленных уравнений может существовать, вообще говоря, много. Интересен вопрос: существует ли разрешающая цепь, состоящая из *неприводимых* уравнений? В случае, когда такая цепь существует, мы будем говорить, что корень θ выражается в *неприводимых радикалах*.

На первый взгляд кажется, что класс уравнений, корни которых выражаются в неприводимых радикалах, значительно уже класса уравнений, корни которых выражаются в любых радикалах. Действительно, разрешающие цепи двучленных уравнений, построенные согласно методам, изложенным в ч. II, гл. 2, обязательно содержат приводимые уравнения вида

$$x^n - 1 = 0,$$

корнями которых служат корни из единицы (этих уравнений не будет только в том случае, когда основное поле P содержит все нужные корни из единицы), и как обойтись без этих уравнений, априори совершенно не ясно. Тем не менее оказывается, что

если корень некоторого уравнения выражается в радикалах, то он выражается и в неприводимых радикалах.

Эта важная теорема позволяет оценить «сложность» любого разрешимого в радикалах уравнения. Именно за меру сложности можно принять набор степеней неприводимых радикалов, через которые выражается корень данного уравнения. (Вопрос о том, в какой мере этот набор степеней определяется данным уравнением, мы здесь не рассматриваем.)

Доказательству сформулированной теоремы будет посвящена вся эта глава. Мы проведем его в рамках теории полей, и потому в первую очередь нам нужно сформулировать эту теорему на языке теории полей.

Расширение K основного поля P мы будем называть *неприводимо-радикальным расширением*, если существует такая цепочка

$$P = L_0 \subset L_1 \subset \dots \subset L_{l-1} \subset L_l \subset \dots \subset L_s = K$$

вложенных друг в друга подполя поля K , начинающаяся с поля P и кончающаяся полем K , что для любого $l = 1, \dots, s$

$$L_l = L_{l-1}(\theta_l),$$

где θ_l — корень некоторого неприводимого (над полем L_{l-1}) уравнения вида

$$x^{n_l} - a_l = 0, \quad a_l \in L_{l-1}.$$

Интересующую нас теорему мы можем теперь сформулировать в следующем виде (в котором мы и будем ее доказывать):

любое радикальное расширение содержится в некотором неприводимо-радикальном расширении.

Задача. Доказать, что имеет место следующее «обратное» утверждение: любое неприводимо-радикальное расширение содержится в некотором радикальном расширении.

2. Сведение основной теоремы к двум частным случаям

В этом пункте мы покажем, что для доказательства сформулированной в конце предыдущего пункта основной теоремы этой главы достаточно доказать следующие ее частные случаи.

Теорема А. Если поле P содержит все корни из единицы степени n , то любое его простое радикальное расширение, определяемое двучленным уравнением степени n , является неприводимо-радикальным расширением.

Теорема В. Любое расширение вида $P(\zeta)$, где ζ — произвольный корень из единицы, содержится в некотором неприводимо-радикальном расширении.

В первую очередь мы рассмотрим случай, когда рассматриваемое радикальное расширение K поля P является простым радикальным расширением, т. е. имеет вид $P(\zeta, \theta)$, где θ — корень двучленного уравнения

$$x^n - a = 0, \quad a \in P, \quad (1)$$

а ζ — первообразный корень из единицы степени n . Согласно теореме В, существует такое неприводимо-радикальное расширение L поля P , что $P(\zeta) \subset L$. Пусть

$$\bar{K} = L(\theta).$$

Поле \bar{K} является простым радикальным расширением поля L , определяемым уравнением (1) степени n , причем поле L содержит, по построению, первообразный корень из единицы ζ степени n . Поэтому, согласно теореме А, поле \bar{K} является неприводимо-радикальным расширением поля L .

Заметим теперь, что из определения неприводимо-радикального расширения непосредственно вытекает следующая

Лемма. Если поле Q является неприводимо-радикальным расширением некоторого поля, которое в свою очередь представляет собой неприводимо-радикальное расширение поля P , то поле Q является неприводимо-радикальным расширением и поля P .

Согласно этой лемме, построенное выше поле \bar{K} является неприводимо-радикальным расширением поля P . Тем самым в рассматриваемом частном случае наша основная теорема доказана, ибо поле \bar{K} содержит, очевидно, поле K .

Пусть теперь K — произвольное радикальное расширение поля P , и пусть

$$P = L_0 \subset L_1 \subset \dots \subset L_{s-1} \subset L_s = K$$

— некоторый его радикальный ряд. Проведем индукцию по числу s . Для $s=1$ теорема уже доказана. Пусть она уже

доказана для числа $s = 1$, т. е. пусть уже доказано, что расширение L_{s-1} содержится в некотором неприводимо-радикальном расширении \bar{L} поля P . Рассмотрим композит Q полей \bar{L} и K . Легко видеть, что поле Q является простым радикальным расширением поля \bar{L} (доказать!) и потому, согласно доказанному выше, содержится в некотором неприводимо-радикальном расширении \bar{K} поля \bar{L} . Согласно лемме, поле \bar{K} представляет собой неприводимо-радикальное расширение поля P и, очевидно, содержит поле K . Тем самым теорема полностью доказана.

3. Доказательство теоремы А

Таким образом, нам осталось лишь доказать теоремы А и В. В первую очередь мы докажем теорему А, как более простую.

Пусть рассматриваемое простое радикальное расширение K поля P определяется двучленным уравнением

$$x^n - a = 0, \quad a \in P, \quad (1)$$

т. е. пусть

$$K = P(\theta),$$

где θ — произвольный корень уравнения (1). (Напомним, что поле P содержит по условию все корни из единицы степени n , т. е. содержит первообразный корень ζ степени n). Пусть, далее, $f(x)$ — минимальный многочлен числа θ над полем P , и пусть m — его степень, т. е. степень $[K : P]$ поля K над полем P . Поскольку многочлен $f(x)$ неприводим и имеет общий корень θ с многочленом $x^n - a$, он делит этот многочлен и потому имеет вид

$$f(x) = (x - \theta)(x - \zeta^{a_1}\theta) \dots (x - \zeta^{a_{m-1}}\theta),$$

где a_1, \dots, a_{m-1} — некоторые целые числа. Раскрывая в этом выражении скобки и обозначая свободный член многочлена $f(x)$ через $(-1)^m \beta$, мы получим, что

$$\beta = \zeta^a \theta^m,$$

где $a = a_1 + \dots + a_{m-1}$. Возведя это равенство в степень n и учитывая, что $\zeta^n = 1$, $\theta^n = a$, мы получим, что

$$\beta^n = a^n.$$

Пусть теперь α — наибольший общий делитель чисел n и m . Тогда, как мы знаем (см. лемму на стр. 70), существуют такие числа u и v , что

$$nu + mv = d.$$

Следовательно,

$$\alpha^d = (\alpha^u)^n (\alpha^m)^v = (\alpha^u \beta^v)^n,$$

то есть

$$\alpha = \epsilon (\alpha^u \beta^v)^{n_1},$$

где $n_1 = n/d$, а ϵ — некоторый корень из единицы степени d . Поскольку корень ϵ можно представить в виде ζ^{cn_1} , где c — некоторое целое число, отсюда вытекает, что многочлен $x^n - \alpha = (x^d)^{n_1} - \gamma^{n_1}$, где $\gamma = \zeta^c \alpha^u \beta^v \in P$ делится на многочлен $x^d - \gamma$. Поскольку за θ принят произвольный корень уравнения (1), можно считать, что θ является корнем как раз многочлена $x^d - \gamma$. Поскольку $d \leq m$, отсюда следует, что $f(x) = x^d - \gamma$, т. е. что $d = m$ и многочлен $x^m - \gamma$ неприводим. Таким образом, поле K порождается над полем P корнем θ неприводимого двучленного уравнения

$$x^m - \gamma = 0, \quad \gamma \in P,$$

т. е. представляет собой неприводимо-радикальное расширение. Тем самым теорема А полностью доказана.

Замечание. Теорему А можно доказать и значительно быстрее, если использовать теорию циклических расширений.

Действительно, как мы знаем (см. ч. II, гл. 2, п. 1), группа Галуа поля K над полем P является циклической группой, причем ее порядок m делит число n . Так как поле P содержит первообразный корень из единицы степени m (почему?), то в силу основной теоремы о циклических расширениях (ч. II, гл. 2, п. 2) поле K определяется над полем P неприводимым двучленным уравнением, т. е. поле K , как и утверждается в теореме А, является неприводимо-радикальным расширением поля P .

4. Мультипликативная группа классов по примарному модулю

Для доказательства теоремы В мы должны предварительно изучить строение мультипликативной группы Z'_n классов по модулю n . Этому изучению и будет посвящен этот пункт.

При этом мы ограничимся единственным нужным нам случаем, когда число p *примарно*, т. е. имеет вид p^a , где p — некоторое простое число.

В первую очередь мы рассмотрим случай, когда простое число p нечетно (т. е. не равно двум).

Если простое число p нечетно, то для любого $a \geq 1$ группа Z'_{p^a} циклична.

Пусть сначала $a = 1$. Поскольку любое положительное число, меньшее p , взаимно просто с p , группа Z'_p состоит из всех классов по модулю p за исключением нулевого, т. е. имеет порядок $p - 1$. Так как множество Z'_p всех (включая и нулевой) классов по модулю p является абелевой группой по сложению, а его подмножество Z'_p — абелевой группой по умножению, причем закон дистрибутивности, очевидно, выполнен, то множество Z'_p представляет собой (абстрактное) поле (см. Курс, стр. 278).

Пусть теперь m — наименьшее общее кратное порядков всех элементов группы Z'_p . Тогда для любого элемента $z \in Z'_p$ имеет место равенство $z^m = [1]$. Другими словами, уравнение $z^m = [1]$ над полем Z_p имеет в этом поле $p - 1$ корень. Поэтому его степень m не меньше $p - 1$. (Теорема о том, что степень уравнения не меньше числа его корней, справедлива над любым полем; см. Курс, стр. 289). С другой стороны, число m не может быть больше порядка $p - 1$ группы Z'_p . Следовательно, оно равно этому порядку. Поэтому группа Z'_p циклична (см. стр. 63).

Образующие $[g]$ группы Z'_p принято называть *первообразными классами*, а принадлежащие им числа g — *первообразными корнями* (по модулю p). Заметим, что согласно этому определению, вместе с числом g первообразным корнем по модулю p является также и число $g + p$.

Пусть теперь $a > 1$. Легко видеть, что порядок $\varphi(p^a)$ группы Z'_{p^a} равен

$$p^{a-1}(p - 1) = p^a - p^{a-1},$$

ибо среди всех неотрицательных целых чисел, меньших p^a , не взаимно прости с p^a лишь числа, делящиеся на p , а таких чисел ровно p^{a-1} (все они имеют вид pu , где $0 \leq u < p^{a-1}$).

Рассмотрим произвольный первообразный корень g по модулю p . Так как $[g]^{p-1} = [1]$, то

$$g^{p-1} = 1 + pu, \quad (1)$$

где u — некоторое целое число. Без потери общности можно считать, что число u не делится на p , ибо в противном случае число g можно заменить числом $g + p$. Действительно, из равенства

$$(g + p)^{p-1} = g^{p-1} + (p - 1)g^{p-2}p + \\ + \frac{(p-1)(p-2)}{2}g^{p-3}p^2 + \dots = 1 + p(u - g^{p-2} + pt),$$

где t — некоторое целое число, вытекает, что если u делится на p , то

$$(g + p)^{p-1} = 1 + pv,$$

где $v = u - g^{p-2} + pt$ на p уже не делится.

Рассмотрим теперь класс $[g]_{p^a}$ числа g по модулю p^a . Пусть порядок этого класса равен n . Тогда имеет место равенство $[g]_p^n = [1]_{p^a}$, т. е. равенство

$$g^n = 1 + p^a v, \quad (2)$$

где v — некоторое целое число. Следовательно, между классами по модулю p имеет место аналогичное равенство $[g]^n = [1]$, из которого немедленно следует, что число n делится на порядок $p - 1$ группы Z'_p (ибо класс $[g]$ является образующей этой группы). С другой стороны, число n делит (см. стр. 63) порядок $p^{a-1}(p - 1)$ группы Z'_{p^a} . Следовательно,

$$n = p^r(p - 1), \quad \text{где } 0 \leq r \leq a - 1.$$

Возводя равенство (1) в степень p^r , мы получим отсюда, что

$$g^n = (1 + pu)^{p^r} = 1 + p^r pu + \frac{p^r(p^r - 1)}{2}(pu)^2 + \dots = \\ = 1 + p^{r+1}(u + pt),$$

где t — некоторое целое число. Сопоставив это равенство с равенством (2), мы получим, что

$$p^a v = p^{r+1}(u + pt).$$

Так как число $u + pt$ не делится на p (ибо на p не делится число u), то это равенство возможно лишь при $a = r + 1$.

Следовательно, $n = p^{a-1}(p-1) = \varphi(p^a)$. Таким образом, мы нашли в группе Z'_{p^a} элемент, порядок которого равен порядку группы. Как мы знаем (см. стр. 63), отсюда следует, что группа Z'_{p^a} циклическа.

Пусть теперь $p = 2$. Очевидно, что группа Z'_2 состоит только из одного элемента (класса [1]) и потому является циклической группой. Группа Z'_4 содержит два элемента и, следовательно, также является циклической группой. Оказывается, что этими двумя группами исчерпываются все циклические группы вида Z'_{2^a} . Именно, как мы сейчас покажем,

группа Z'_{2^a} при $a \geq 3$ не циклическа.

Поскольку порядок $\varphi(2^a)$ группы Z'_{2^a} равен 2^{a-1} (числу нечетных чисел, меньших чем 2^a), для доказательства этого утверждения достаточно показать, что

порядок любого элемента группы Z'_{2^a} при $a \geq 3$ не превосходит числа 2^{a-2} .

Но это очевидно, ибо для любого нечетного числа $c = 1 + 2t$ и любого целого числа $k \geq 1$ имеет место равенство

$$c^{2^k} = 1 + 2^{k+2}t_k, \quad (3)$$

где t_k — некоторое целое число. Действительно, для $k = 1$ равенство (3) справедливо (причем $t_1 = t + t^2$), а если оно справедливо для $k - 1$, то оно справедливо и для k (причем $t_k = t_{k-1} + 2^k t_{k-1}^2$). Следовательно, при $a \geq 3$ число $c^{2^{a-2}}$ сравнимо с единицей по модулю 2^a .

Оценка 2^{a-2} точная, т. е. в группе Z'_{2^a} на самом деле существуют элементы порядка 2^{a-2} . Таким элементом является, например, класс числа 5. Действительно, легко видеть, что для любого целого числа $k \geq 0$ имеет место равенство

$$5^{2^k} = 1 + 2^{k+2} + 2^{k+3}s_k,$$

где s_k — некоторое целое число ($s_0 = 0$ и $s_k = 2^{k-1} + (1 + 2^{k+2})s_{k-1}$), так что число $5^{2^{a-3}}$ сравнимо по модулю 2^a с числом $1 + 2^{a-1}$, и потому

$$[5]_{2^a}^{2^{a-3}} \neq [1]_{2^a}.$$

Таким образом, порядок класса $[5]_{2^a}$ равен 2^{a-2} .

168 гл. 3. РЕШЕНИЕ УРАВНЕНИЙ В НЕПРИВОДИМЫХ РАДИКАЛАХ

Класс $[5]_{2^a}$ мы будем в дальнейшем обозначать символом x_{2^a} или просто x . Циклическую подгруппу порядка 2^{a-2} группы Z'_{2^a} , порожденную элементом x_{2^a} , мы будем обозначать символом X_{2^a} . Она состоит из элементов

$$e = [1], \quad x, \quad x^2, \dots, \quad x^{2^{a-2}-1}. \quad (4)$$

Рассмотрим теперь класс $[-1]_{2^a}$ числа -1 по модулю 2^a . В дальнейшем этот класс мы будем обозначать символом y_{2^a} или просто y . Ясно, что $y^2 = e$. Оказывается, что класс y не принадлежит подгруппе X_{2^a} . Действительно, если бы, например, $y = x^t$, где $1 \leq t \leq 2^{a-2} - 1$, то число $5^t + 1$ делилось бы на 2^a и потому делилось бы на 4, что, как легко видеть, невозможно (почему?).

Отсюда вытекает, что, кроме элементов (4), группа Z'_{2^a} содержит также элементы

$$y = ey, \quad xy, \quad x^2y, \dots, \quad x^{2^{a-2}-1}y, \quad (5)$$

причем все эти элементы отличны друг от друга и от элементов (4).

Поскольку элементов (4) и (5) вместе ровно 2^{a-1} , они исчерпывают собой все элементы группы Z'_{2^a} .

5. Группы Галуа примарных круговых расширений

Поля вида $P(\zeta)$, где ζ — некоторый корень из единицы, мы будем называть *круговыми расширениями* поля P . Это название связано с тем, что корни из единицы степени n определяют разбиение окружности на n равных частей.

Показателем кругового расширения $P(\zeta)$ мы будем называть такое число n , что корень ζ является первообразным корнем из единицы степени n . Если число n примарно, т. е. имеет вид p^a , где p — простое число, то круговое расширение мы будем называть *примарным*.

Как мы знаем (см. ч. II, гл. 1, п. 1), группа Галуа $G(P(\zeta), P)$ кругового расширения $P(\zeta)$ с показателем n изоморфна некоторой подгруппе мультипликативной группы Z'_n классов по модулю n . Для $n = p^a$ отсюда и из результатов предыдущего пункта немедленно вытекает, что

при p нечетном (а также при $p = 2$ и $a \leq 2$) группа Галуа $G(P(\zeta), P)$ примарного кругового расширения $P(\zeta)$ с показателем p^a является циклической группой, порядок которой делит число $p^{a-1}(p-1)$.

Пусть теперь $p = 2$ и $a \geq 3$. Рассмотрим подгруппу H группы Z_{2^a} , которой изоморфна группа Галуа $G(P(\zeta), P)$. Возможны следующие три случая:

1) подгруппа H не содержит элементов вида $x^k y$;

2) подгруппа H содержит элементы вида $x^k y$ и не содержит отличных от e элементов вида x^k ;

3) подгруппа H содержит элементы обоих видов.

В случае 1) подгруппа H содержится в подгруппе X_{2^a} и потому является циклической группой, порядок которой делит число 2^{a-2} .

Если подгруппа H содержит элемент $x^k y$, то она содержит и элемент $x^{2k} = (x^k y)^2$ (напомним, что $y^2 = e$). Поэтому в случае 2) число k либо равно нулю, либо равно 2^{a-3} . Обоих элементов y и $x^{2^{a-3}}y$ подгруппа H содержать не может, так как их произведение равно $x^{2^{a-3}}$. Таким образом, либо $H = \{e, y\}$, либо $H = \{e, x^{2^{a-3}}y\}$, так что в случае 2) подгруппа H также является циклической группой (порядка 2, делящего число 2^{a-2}).

В случае 3) мы рассмотрим пересечение $H_0 = H \cap X_{2^a}$, т. е. совокупность всех элементов вида x^k , содержащихся в подгруппе H . Это пересечение, являясь подгруппой группы X_{2^a} , представляет собой циклическую группу. Пусть x' — ее образующая. Число r , являясь индексом подгруппы H_0 в группе X_{2^a} , делит порядок 2^{a-2} группы X_{2^a} , т. е. имеет вид 2^t , где $0 \leq t \leq a-3$. По условию подгруппа H , кроме степеней элемента x' , содержит также некоторые элементы вида $x^k y$. Рассмотрим следующие два случая:

3^a) ни для одного элемента $x^k y \in H$ показатель k не делится на r ;

3^b) хотя бы для одного элемента $x^k y \in H$ показатель k делится на r .

В случае 3^a) любой элемент $x^k y \in H$ мы можем (разделив с остатком число k на число r) представить в виде произ-

введения $(x^r)^l \cdot x^{k_0}y$, где $k_0 < r$. Так как $x^r \in H$, то $x^{k_0}y \in H$. С другой стороны, если $x^{k_0}y \in H$ и $k_0 < r$, то, поскольку $x^{2k_0} = (x^{k_0}y)^2 \in H_0$, число $2k_0$ должно делиться на r , что возможно лишь при $k_0 = r/2$ (заметим, что в рассматриваемом случае $r > 1$). Итак, любой элемент $x^ky \in H$ имеет вид $(x^r)^l \cdot x^{\frac{r}{2}}y$. Но это выражение равно $\left(x^{\frac{r}{2}}y\right)^{2l+1}$, ибо $\left(x^{\frac{r}{2}}y\right)^2 = x^r$. Кроме того, любой элемент вида $(x^r)^l$ равен $\left(x^{\frac{r}{2}}y\right)^{2l}$. Таким образом, мы видим, что любой элемент подгруппы H является степенью элемента $x^{\frac{r}{2}}y$, т. е. подгруппа H является циклической подгруппой с образующей $x^{\frac{r}{2}}y$. Порядок подгруппы H равен, очевидно, $2 \cdot 2^{a-2-t} = 2^{a-1-t}$ и, следовательно, делит число 2^{a-2} (ибо $t > 0$).

Наконец, в случае 3^{б)} подгруппа H содержит, очевидно, элемент y и потому состоит из элементов подгруппы H_0 и их произведений на элемент y . Эта группа уже нециклическая. Она содержит циклическую подгруппу H_0 порядка 2^{a-2-t} , факторгруппа по которой является группой второго порядка.

Возвращаясь к группе Галуа поля $P(\zeta)$, мы окончательно получаем:

при $p=2$ и $a \geq 3$ группа Галуа $G(P(\zeta), P)$ либо является циклической группой, порядок которой делит число 2^{a-2} , либо, являясь нециклической группой, содержит циклическую подгруппу, порядок которой делит число 2^{a-2} , причем соответствующая факторгруппа является группой второго порядка.

Как случай нечетного p , так и случай $p=2$ можно объединить в следующей общей теореме:

в поле $P(\zeta)$ с показателем p^a существует такое промежуточное подполе P' , что

1) группа Галуа $G(P(\zeta), P')$ поля $P(\zeta)$ над полем P' является циклической группой, порядок которой делит число $p^{a-1}(p-1)$;

2) степень поля P' над полем P либо равна единице (т. е. $P' = P$), либо равна двум.

Степень поля P' над полем P тогда и только тогда равна двум, когда группа $G(P(\zeta), P)$ не циклическа (и, значит,

$p = 2$ и $a \geq 3$). В этом случае поле P' определяется как подполе поля $P(\zeta)$, соответствующее указанной в предыдущей теореме циклической подгруппе группы $G(P(\zeta), P)$.

Пусть S — образующая этой подгруппы. Поскольку при мономорфизме $\phi: G(P(\zeta), P) \rightarrow Z_2^{2a}$ (см. ч. II, гл. 2, п. 1), эта образующая переходит в элемент x' , т. е. в класс $[5']_{2a}$, ее действие на элементе ζ определяется формулой

$$\zeta^S = \zeta^{5'}.$$

Аналогично действие автоморфизма T , соответствующего элементу y , определяется формулой

$$\zeta^T = \zeta^{-1}.$$

Так как $5' = 4t + 1$, где t — некоторое целое число, то из этих формул вытекает, что

$$\begin{aligned} (\zeta^{2a-2})^S &= \zeta^{2a-2 \cdot 5'} = \zeta^{2a-2 \cdot 4t \cdot 2a-2} = \zeta^{2at} \cdot \zeta^{2a-2} = \zeta^{2a-2}, \\ (\zeta^{2a-2})^T &= \zeta^{-2a-2} = \zeta^{2a-2a-2} = \zeta^{2a-2(4-1)} = \zeta^3 \cdot \zeta^{2a-2}. \end{aligned}$$

С другой стороны, так как

$$(\zeta^{2a-2})^4 = \zeta^{2a} = 1,$$

то $\zeta^{2a-2} = \pm i$, где $i = \sqrt{-1}$. Таким образом, мы видим, что $i \in P(\zeta)$, причем

$$i^S = i, \quad i^T = \zeta^3 \cdot i.$$

Из первого равенства следует, что $i \notin P'$, а из второго, что $i \notin P$ (ибо $\zeta^3 \neq 1$). Таким образом, во-первых, поле $P(i)$ содержится в поле P' , а во-вторых, степень поля $P(i)$ над полем P равна двум. Это возможно только тогда, когда $P' = P(i)$. Таким образом,

если $P' \neq P$, то $P' = P(i)$.

6. Доказательство теоремы В

Теперь мы уже в состоянии доказать теорему В. Ее доказательство мы проведем индукцией по показателю n кругового расширения $P(\zeta)$.

Если $n = 1$ (а также если $n = 2$) поле $P(\zeta)$ совпадает с полем P , так что в этом случае теорема В тривиальным

образом справедлива (за неприводимо-радикальное расширение K , содержащее данное круговое расширение $P(\zeta)$, можно принять само поле P).

Предположим теперь, что теорема В уже доказана для всех круговых расширений с показателями, меньшими n (каково бы ни было поле P), и докажем ее для расширения $P(\zeta)$ с показателем n . Будем различать следующие два случая:

(I) число n делится по крайней мере на два различных простых числа;

(II) число n имеет вид p^a , где p — простое число.

Случай (I). В этом случае число n можно представить (вообще говоря, многими способами) в виде произведения $n_1 n_2$ двух взаимно простых чисел n_1 и n_2 , каждое из которых меньше n . Пусть ζ_1 и ζ_2 — первообразные корни из единицы степеней n_1 и n_2 соответственно. Так как $\zeta_1 \in P(\zeta)$ и $\zeta_2 \in P(\zeta)$, то $P(\zeta_1, \zeta_2) \subset P(\zeta)$. Оказывается, что имеет место и обратное включение $P(\zeta) \subset P(\zeta_1, \zeta_2)$, так что

$$P(\zeta) = P(\zeta_1, \zeta_2). \quad (1)$$

Для доказательства этого включения достаточно показать (почему?), что произведение $\zeta_1 \zeta_2$ представляет собой первообразный корень из единицы степени n , т. е. что из равенства $(\zeta_1 \zeta_2)^m = 1$ вытекает, что m делится на n . Но если $(\zeta_1 \zeta_2)^m = 1$, то $\zeta_1^m = \zeta_2^{-m} = 1$, ибо, согласно лемме, доказанной на стр. 70—71, для взаимно простых чисел n_1 и n_2 существуют такие числа u и v , что $n_1 u + n_2 v = 1$, и потому

$$\zeta_1^m = \zeta_1^{m(n_1 u + n_2 v)} = (\zeta_1^{n_1})^{mu} \cdot (\zeta_1^{n_2})^{n_2 v} = (\zeta_2^{-m})^{n_2 v} = (\zeta_2^{n_2})^{-mv} = 1.$$

Поскольку корень ζ_1 является по условию первообразным корнем из единицы степени n_1 , из равенства $\zeta_1^m = 1$ вытекает, что m делится на n_1 . Аналогично, из равенства $\zeta_2^{-m} = 1$ вытекает, что m делится на n_2 . Поэтому m делится и на $n_1 n_2$ (ибо $m = m n_1 u + m n_2 v$). Тем самым равенство (1) полностью доказано.

Поскольку показатель n_1 расширения $P(\zeta_1)$ меньше n , поле $P(\zeta_1)$ содержится, по предположению индукции, в некотором неприводимо-радикальном расширении K_1 поля P . Рассмотрим поле $K_1(\zeta_2)$. Это — круговое расширение поля K_1 с показателем n_2 , меньшим n . Поэтому, снова по предпо-

ложению индукции, поле $K_1(\zeta_2)$ содержится в неприводимо-радикальном расширении K поля K_1 . Для завершения доказательства теоремы остается теперь заметить, что поле $P(\zeta) = P(\zeta_1, \zeta_2)$ содержится в поле K и что это последнее поле является неприводимо-радикальным расширением поля P (см. лемму из п. 2).

Случай (II). Пусть теперь $n = p^a$. Наряду с полем $P(\zeta)$ рассмотрим поле $P(\eta)$, где η — первообразный корень из единицы степени $p^{a-1}(p - 1)$. Так как $p^{a-1}(p - 1) < p^a$, то, по предположению индукции, поле $P(\eta)$ содержится в некотором неприводимо-радикальном расширении K_1 поля P . Пусть $K = K_1(\zeta)$. Как мы знаем (см. п. 5), в поле K содержится такое подполе $K'_1 \subset K_1$, что группа Галуа $G(K, K'_1)$ является циклической группой, порядок которой делит число $p^{a-1}(p - 1)$. Другими словами, поле K является циклическим расширением поля K'_1 . Поскольку поле K'_1 содержит, по построению, первообразный корень из единицы степени $p^{a-1}(p - 1)$, а потому и первообразный корень из единицы степени, равной степени поля K , над полем K'_1 , к этому циклическому расширению применима теорема, доказанная в ч. II, гл. 2, п. 2, согласно которой поле K является неприводимо-радикальным расширением поля K'_1 . Так как поле K'_1 либо совпадает с полем K_1 , либо имеет вид $K_1(l)$ (см. п. 5), и потому является неприводимо-радикальным расширением поля K_1 , то поле K представляет собой неприводимо-радикальное расширение поля K_1 , а следовательно, и поля P . Для завершения доказательства остается заметить, что $P(\zeta) \subset K$.

Тем самым теорема В, а значит и основная теорема, сформулированная в п. 1, полностью доказана,

ГЛАВА 4

УРАВНЕНИЯ ДЕЛЕНИЯ КРУГА

1. Строение полей деления круга простого показателя

В предыдущей главе было в определенной мере изучено (в процессе доказательства теоремы В) строение произвольных круговых расширений. В этой главе мы углубим и конкретизируем эти результаты для случая *поля деления круга*, т. е. круговых расширений поля R рациональных чисел, в предположении, что показатель расширения является простым нечетным (случай $p = 2$ неинтересен) числом p .

Многочлен, корнями которого являются первообразные корни из единицы некоторой степени p (и только эти корни), называется *многочленом деления круга* на p частей. Поскольку при p простом все отличные от единицы корни степени p из единицы являются первообразными корнями, многочлен деления круга на p частей имеет вид

$$x^{p-1} + x^{p-2} + \dots + x + 1 \quad (1)$$

и потому является многочленом над полем R . Известно (см. Курс, стр. 354), что этот многочлен *неприводим* (над полем R) (по существу, это единственное место, где мы используем тот факт, что основным полем является поле R).

Полем разложения многочлена (1) является поле деления круга $R(\zeta)$, где ζ — произвольный первообразный (т. е. отличный от единицы) корень степени p из единицы. Поскольку многочлен (1) неприводим, степень $[R(\zeta) : R]$ поля $R(\zeta)$ над полем R равна $p - 1$ (степени многочлена (1)).

Рассмотрим теперь элементы

$$\zeta, \zeta^2, \dots, \zeta^{p-1} \quad (2)$$

поля $R(\zeta)$. Все эти элементы являются первообразными корнями степени p из единицы (и любой первообразный корень степени p из единицы среди них содержится).

Легко видеть, что

элементы (2) составляют базис поля $R(\zeta)$ над полем R .

Действительно, их число равно степени $p - 1$ поля $R(\zeta)$ над полем R и они линейно независимы (ибо любая нетривиальная линейная комбинация между ними после сокращения на ζ превращается в уравнение для ζ степени, меньшей чем $p - 1$, а такого уравнения в силу неприводимости многочлена (1) существовать не может).

Из результатов предыдущей главы мы знаем, что группа Галуа $G = G(R(\zeta), R)$ поля $R(\zeta)$ над полем R циклическа, а из сказанного выше о степени поля $R(\zeta)$ следует, что ее порядок равен $p - 1$. Пусть S — произвольная (раз навсегда фиксированная) образующая этой группы. Тогда

$$\zeta^S = \zeta^g,$$

где g — некоторый первообразный корень по модулю p .

Для любого $t = 0, \pm 1, \pm 2, \dots$ мы положим

$$\zeta_t = \zeta^{S^t}, \text{ т. е. } \zeta_t = \zeta^{g^t}.$$

Таким образом, $\zeta_0 = \zeta$ и

$$\zeta_t^S = \zeta_{t+1}. \quad (3)$$

Поскольку $S^n = E$ тогда и только тогда, когда n делится на $p - 1$, равенство $\zeta_t = \zeta_j$ имеет место тогда и только тогда, когда числа t и j сравнимы по модулю $p - 1$ (следует иметь в виду, что из равенства $\zeta^{S^n} = \zeta$ вытекает равенство $S^n = E$). Таким образом, среди чисел ζ_t имеется ровно $p - 1$ различных.

За эти числа можно принять, например, числа

$$\zeta_0 = \zeta, \zeta_1, \zeta_2, \dots, \zeta_{p-2}. \quad (4)$$

Поскольку все числа ζ_t являются первообразными корнями, из единицы степени p числа (4) лишь порядком следования отличаются от чисел (2). Таким образом,

элементы (4) составляют базис поля $R(\zeta)$ над полем R .

Как мы знаем, любая подгруппа группы G является циклической подгруппой с образующей вида S^e , где $e —$

некоторый делитель числа $p - 1$. Обратно, для любого делителя e числа $p - 1$ элемент S^e является образующей некоторой подгруппы. Пусть R_e — подполе поля $R(\zeta)$, соответствующее этой подгруппе. Таким образом, $R_1 = R$ и $R_{p-1} = R(\zeta)$. Степень $[R(\zeta) : R_e]$ поля $R(\zeta)$ над полем R_e равна $f = \frac{p-1}{e}$, а степень $[R_e : R]$ поля R_e над полем R равна e . Элемент α поля $R(\zeta)$ тогда и только тогда принадлежит полю R_e , когда $\alpha^{S^e} = \alpha$.

Заметим теперь, что для любого делителя e числа $p - 1$ все первообразные корни (4) степени p из единицы можно распределить в e групп

$$\begin{aligned} & \zeta_0, \quad \zeta_e, \quad \dots, \quad \zeta_{(f-1)e}, \\ & \zeta_1, \quad \zeta_{e+1}, \quad \dots, \quad \zeta_{(f-1)e+1}, \\ & \dots \dots \dots \dots \dots \\ & \zeta_{e-1}, \quad \zeta_{2e-1}, \quad \dots, \quad \zeta_{fe-1} \end{aligned}$$

по $f = \frac{p-1}{e}$ корней в каждой группе, таким образом, что автоморфизм S^e переводит каждый корень в соседний корень той же группы (корнем соседним с последним корнем $\zeta_{(f-1)e+1}$ группы номера l мы считаем ее первый корень ζ_l).

Пусть

$$\begin{aligned} \eta_l^{(e)} &= \sum_{j=0}^{f-1} \zeta_{je+l} = \zeta_l + \zeta_{e+l} + \dots + \zeta_{(f-1)e+l}, \\ l &= 0, 1, \dots, e-1, \end{aligned} \quad (5)$$

— сумма всех корней, принадлежащих l -й группе. Из сказанного выше непосредственно следует, что элементы $\eta_l = \eta_l^{(e)}$ — они называются f -членными гауссовыми периодами, — не меняются под воздействием автоморфизма S^e :

$$\eta_l^{S^e} = \eta_l, \quad l = 0, 1, \dots, e-1.$$

Следовательно, $\eta_l \in R_e$. Так как число периодов η_l равно степени e поля R_e над полем R и они линейно независимы над полем R (почему?), то

периоды η_l составляют базис поля R_e над полем R .

Пусть $\eta = \eta_0$. Так как $\eta \in R_e$, то $R(\eta) \subset R_e$. Пусть m — степень поля $R(\eta)$ над полем R , т. е. степень непри-

водимого над полем R многочлена $f(x)$ с корнем η . Так как $R(\eta) \subset R_e$, то $m \leq e$. С другой стороны, легко видеть, что

$$\eta_l = \eta^{s^l}, \quad l = 0, 1, \dots, e-1,$$

откуда следует, что все периоды η_l являются корнями многочлена $f(x)$. Таким образом, многочлен $f(x)$ имеет, по крайней мере, e различных корней, и потому $m \geq e$. Следовательно, $m = e$ и

$$R_e = R(\eta).$$

Отсюда, в частности, вытекает, что

любой период η_l выражается в виде многочлена (с рациональными коэффициентами) от периода η .

2. Решение уравнений деления круга

В этом пункте мы применим результаты п. 1 к задаче «решения» уравнения деления круга на p частей, т. е. к задаче приведения этого уравнения к цепи возможно более простых уравнений.

Задача. Доказать, что $R_{e'} \subset R_e$ тогда и только тогда, когда e делится на e' и что степень $[R_e : R_{e'}]$ поля R_e над полем $R_{e'}$ равна e/e' .

Пусть

$$p - 1 = q_1 q_2 \dots q_s$$

— разложение числа $p - 1$ в произведение (не обязательно различных) простых чисел q_1, q_2, \dots, q_s . Полагая

$$R_{(0)} = R, \quad R_{(l)} = R_{q_1 \dots q_l}, \quad l = 1, \dots, s,$$

мы получим в поле $R(\zeta)$ цепочку последовательно вложенных друг в друга подполей

$$R = R_{(0)} \subset R_{(1)} \subset \dots \subset R_{(s-1)} \subset R_{(s)} = R(\zeta)$$

обладающую тем свойством, что каждое подполе этой цепочки (кроме поля $R_{(0)}$) имеет над предшествующим подполем простую степень (именно поле $R_{(l)}$, $l = 1, \dots, s$ имеет над полем $R_{(l-1)}$ степень q_l). Другими словами, полагая $R_{(l)} = R_{(l-1)}(\alpha_l)$, мы получим, что

$$R(\zeta) = R(\alpha_1, \alpha_2, \dots, \alpha_s),$$

причем для любого $l = 1, \dots, s$ число a_l является корнем некоторого неприводимого уравнения простой степени q_l над полем $R_{(l-1)} = R(\alpha_1, \dots, \alpha_{l-1})$. На языке теории уравнений это означает, что

решение уравнения деления круга на r частей сводится к решению уравнений простых степеней q_1, q_2, \dots, q_s .

Назовем простое число p *числом Ферма*, если число $p - 1$ является степенью двойки, т. е. имеет вид 2^n (легко видеть, что это возможно лишь тогда, когда показатель n также является степенью двойки). Из только что доказанного утверждения немедленно вытекает, что

если простое число p является числом Ферма, то решение уравнения деления круга на r частей сводится к решению квадратных уравнений.

Задача. Доказать обратное утверждение.

Замечание. Из теории геометрических построений (см. ниже гл. 4, п. 1) известно, что корень некоторого уравнения тогда и только тогда можно построить циркулем и линейкой, когда решение этого уравнения сводится к цепи квадратных уравнений. Следовательно, имеет место следующая теорема (впервые доказанная Гауссом).

Правильный p -угольник, где p — некоторое простое число, тогда и только тогда можно построить циркулем и линейкой, когда число p является числом Ферма.

Числами Ферма являются, например, числа

$$3, 5, 17, 257, 65531.$$

Существуют ли другие числа Ферма, до сих пор неизвестно.

3. Прием Гаусса

Если бы теоремой предыдущего пункта исчерпывалось все, что можно сказать о решении уравнений деления круга, это совершенно не оправдывало бы труд, затраченный нами в п. 1 на изучение строения поля $R(\zeta)$ и его подполей, ибо легко видеть, что *решение любого уравнения с разрешимой группой Галуа сводится к решению уравнений простых степеней* (так как любая разрешимая группа обладает разрешимым рядом с факторами простых порядков).

В этом пункте мы дополним эту теорему принадлежащим Гауссу изящным приемом построения «разрещающих» уравнений простых степеней или, более общо, уравнений, определяющих произвольное подполе R_e поля $\mathbb{R}(\zeta)$ над полями вида $R_{e'}$, где e' — некоторый делитель числа e (не обязательно отличающийся от числа e лишь на один простой множитель).

Так как $R_e = R(\eta)$, где

$$\eta = \eta_0^{(e)} = \zeta + \zeta_e + \dots + \zeta_{(f-1)e},$$

то $R_e = R_{e'}(\eta)$, и наша задача сводится к тому, чтобы найти неприводимый над полем $R_{e'}$ многочлен с корнем η (т. е. минимальный многочлен числа η над полем $R_{e'}$). С этой целью мы рассмотрим периоды

$$\eta = \eta_0, \eta_{e'}, \eta_{2e'}, \dots, \eta_{(h-1)e'} = \eta_{e-e'}, \quad (1)$$

где $h = e/e'$. Поскольку, как легко видеть,

$$(\eta_{ke'})^{se'} = \eta_{(k+1)e'}, \quad k = 0, 1, \dots, h-1$$

(условно считаем, что $\eta_e = \eta_0$), элементарные симметрические функции от периодов (5) не меняются под воздействием автоморфизма $S^{e'}$, т. е. принадлежат полю $R_{e'}$. Другими словами, многочлен

$$f(x) = (x - \eta)(x - \eta_{e'}) \cdots (x - \eta_{(h-1)e'})$$

представляет собой многочлен над полем $R_{e'}$. Так как его степень равна $h = [R_e : R_{e'}]$, то этот многочлен и является искомым минимальным многочленом числа η над полем $R_{e'}$.

Коэффициент этого многочлена при x^{h-1} лишь знаком отличается от величины

$$\begin{aligned} \eta + \eta_{e'} + \eta_{2e'} + \dots + \eta_{(h-1)e'} &= \sum_{k=0}^{h-1} \eta_{ke'} = \\ &= \sum_{k=0}^{h-1} \sum_{l=0}^{f-1} \zeta_{ke'+le} = \sum_{l=0}^{f-1} \sum_{k=0}^{h-1} \zeta_{e'(k+hl)} = \sum_{j=0}^{f'-1} \zeta_{e'j} \end{aligned}$$

$$\left(\text{где } f' = \frac{p-1}{e'} \right),$$

т. е. от f' -членного гауссова периода $\eta^{(e')} = \eta_0^{(e')}$, соответствующего числу e' . Остальные коэффициенты можно

вычислить на основе формул Вьета, опираясь на следующее утверждение, непосредственно вытекающее из того факта, что периоды $\eta_0, \eta_1, \dots, \eta_{e-1}$ образуют базис поля R_e над полем R .

Произведение $\eta_i \eta_j$ любых двух f -членных гауссовых периодов является целочисленной линейной комбинацией периодов $\eta_0, \eta_1, \dots, \eta_{e-1}$.

Для практического нахождения этой линейной комбинации Гаусс предложил записывать произведение $\eta_i \eta_j$ периодов

$$\eta_i = \zeta_i + \zeta_{i+e} + \dots + \zeta_{i+(f-1)e},$$

в следующем виде, собирая вместе произведения членов, «отстоящих друг от друга на одном расстоянии» (и считая при этом, что после последнего члена каждого периода снова следует его первый член):

Легко видеть, что под воздействием автоморфизма S^e каждый член $\zeta_{i+ke}\zeta_{j+le}$ произведения $\eta_i\eta_j$ переходит в следующий член $\zeta_{i+(k+1)e}\zeta_{j+(l+1)e}$ той же скобки (считаем, что за последним членом скобки следует ее первый член). С другой стороны, являясь произведением корней из единицы степени p , член $\zeta_{i+ke}\zeta_{j+le}$ также представляет собой корень из единицы либо первообразный, либо равный единице. Таким образом, каждая скобка либо состоит из единиц (и потому равна f), либо представляет собой сумму первообразных корней из единицы степени p , последовательно переходящих друг в друга под воздействием автоморфизма S^e , т. е. является одним из периодов $\eta_0, \eta_1, \dots, \eta_{e-1}$. Чтобы найти номер этого периода, достаточно вычислить один член скобки (скажем, первый) и посмотреть, в какой период он входит.

Что же касается скобки, состоящей из единиц, то она равна

$$-f\eta_0 - f\eta_1 - \dots - f\eta_{e-1}.$$

Действительно, сумма $\eta_0 + \eta_1 + \dots + \eta_{e-1}$ равна сумме $\zeta_0 + \zeta_1 + \dots + \zeta_{p-2}$ всех первообразных корней из единицы степени p и потому равна -1 (взятому с обратным знаком коэффициенту при x^{p-2} в уравнении деления круга).

Тем самым мы действительно представили произведение $\eta_i \eta_j$ в виде линейной комбинации периодов $\eta_0, \eta_1, \dots, \eta_{e-1}$.

4. Уравнение деления круга на 17 частей

Для иллюстрации изложенной выше общей теории рассмотрим случай $p = 17$.

Для числа 17 за первообразный корень g можно принять, например, число 6. Тогда

$$\begin{array}{llll} \zeta_0 = \zeta, & \zeta_4 = \zeta^4, & \zeta_8 = \zeta^{16}, & \zeta_{12} = \zeta^{13}, \\ \zeta_1 = \zeta^6, & \zeta_5 = \zeta^7, & \zeta_9 = \zeta^{11}, & \zeta_{13} = \zeta^{10}, \\ \zeta_2 = \zeta^2, & \zeta_6 = \zeta^8, & \zeta_{10} = \zeta^{15}, & \zeta_{14} = \zeta^9, \\ \zeta_3 = \zeta^{12}, & \zeta_7 = \zeta^{14}, & \zeta_{11} = \zeta^5, & \zeta_{15} = \zeta^3. \end{array}$$

Поскольку $p - 1 = 16$, за первое число e мы должны принять число 2. Соответствующие восьмичленные периоды имеют вид

$$\begin{aligned} \eta^{(2)} &= \zeta + \zeta^2 + \zeta^4 + \zeta^8 + \zeta^{16} + \zeta^{15} + \zeta^{13} + \zeta^9, \\ \eta_1^{(2)} &= \zeta^6 + \zeta^{12} + \zeta^7 + \zeta^{14} + \zeta^{11} + \zeta^5 + \zeta^{10} + \zeta^3. \end{aligned}$$

Скобки, на которые разбивается произведение $\eta^{(2)} \eta_1^{(2)}$, начинаются соответственно с членов

$$\begin{array}{ll} \zeta \zeta^6 = \zeta^7 \quad (\text{из периода } \eta_1^{(2)}), & \zeta \zeta^{11} = \zeta^{12} \quad (\text{из периода } \eta_1^{(2)}), \\ \zeta \zeta^{12} = \zeta^{13} \quad (\text{из периода } \eta^{(2)}), & \zeta \zeta^5 = \zeta^6 \quad (\text{из периода } \eta_1^{(2)}), \\ \zeta \zeta^7 = \zeta^8 \quad (\text{из периода } \eta^{(2)}), & \zeta \zeta^{10} = \zeta^{11} \quad (\text{из периода } \eta_1^{(2)}), \\ \zeta \zeta^{14} = \zeta^{15} \quad (\text{из периода } \eta^{(2)}), & \zeta \zeta^3 = \zeta^4 \quad (\text{из периода } \eta_1^{(2)}). \end{array}$$

Следовательно, $\eta^{(2)} \eta_1^{(2)} = 4\eta^{(2)} + 4\eta_1^{(2)}$, т. е.

$$\eta^{(2)} \eta_1^{(2)} = -4,$$

ибо

$$\eta^{(2)} + \eta_1^{(2)} = -1.$$

Таким образом, период $\eta^{(2)}$ (вместе с периодом $\eta_1^{(2)}$) является корнем квадратного уравнения

$$x^2 + x - 4 = 0,$$

то есть

$$\eta^{(2)} = \frac{-1 \pm \sqrt{17}}{2}. \quad (1)$$

Далее, мы должны взять $e = 4$. Соответствующие четырехчленные периоды имеют вид

$$\begin{aligned} \eta^{(4)} &= \zeta + \zeta^4 + \zeta^{16} + \zeta^{13}, & \eta_2^{(4)} &= \zeta^2 + \zeta^8 + \zeta^{15} + \zeta^9, \\ \eta_1^{(4)} &= \zeta^6 + \zeta^7 + \zeta^{11} + \zeta^{10}, & \eta_3^{(4)} &= \zeta^{12} + \zeta^{14} + \zeta^5 + \zeta^3. \end{aligned}$$

Из них нам нужны лишь периоды $\eta^{(4)}$ и $\eta_2^{(4)}$ (так как $e' = 2$).

Согласно общей теории,

$$\eta^{(4)} + \eta_2^{(4)} = \eta^{(2)}.$$

Что же касается произведения $\eta^{(4)}\eta_2^{(4)}$, то скобки, на которые оно разбивается, начинаются соответственно с членов

$$\begin{aligned} \zeta\zeta^2 &= \zeta^3 \text{ (из периода } \eta_3^{(4)}), & \zeta\zeta^{15} &= \zeta^{16} \text{ (из периода } \eta^{(4)}), \\ \zeta\zeta^8 &= \zeta^9 \text{ (из периода } \eta_2^{(4)}), & \zeta\zeta^9 &= \zeta^{10} \text{ (из периода } \eta_1^{(4)}). \end{aligned}$$

Таким образом,

$$\eta^{(4)}\eta_2^{(4)} = \eta_3^{(4)} + \eta_2^{(4)} + \eta^{(4)} + \eta_1^{(4)} = -1.$$

Следовательно, период $\eta^{(2)}$ является корнем уравнения

$$x^2 - \eta^{(2)}x - 1 = 0,$$

то есть

$$\eta^{(2)} = \frac{\eta^{(2)} \pm \sqrt{(\eta^{(2)})^2 + 4}}{2}. \quad (2)$$

Далее, мы должны взять $e = 8$. Соответствующие двухчленные периоды имеют вид

$$\begin{aligned} \eta^{(8)} &= \zeta + \zeta^{16}, & \eta_4^{(8)} &= \zeta^4 + \zeta^{13}, \\ \eta_1^{(8)} &= \zeta^6 + \zeta^{11}, & \eta_5^{(8)} &= \zeta^7 + \zeta^{10}, \\ \eta_2^{(8)} &= \zeta^2 + \zeta^{15}, & \eta_6^{(8)} &= \zeta^8 + \zeta^9, \\ \eta_3^{(8)} &= \zeta^{12} + \zeta^5, & \eta_7^{(8)} &= \zeta^{14} + \zeta^3. \end{aligned}$$

Из них нам нужны только периоды $\eta^{(8)}$ и $\eta_4^{(8)}$.

Согласно общей теории,

$$\eta^{(8)} + \eta_4^{(8)} = \eta^{(4)}.$$

Что же касается произведения $\eta^{(8)}\eta_4^{(8)}$, то, как и выше, находим, что

$$\eta^{(8)}\eta_4^{(8)} = \eta_3^{(8)} + \eta_7^{(8)} = \eta_3^{(4)}.$$

Согласно доказанному в п. 1, период $\eta_3^{(4)}$ выражается через период $\eta^{(4)}$. Чтобы найти это выражение, составим произведение $\eta^{(4)}\eta_3^{(4)}$. Имеем

$$\begin{aligned} \eta^{(4)}\eta_3^{(4)} &= \eta^{(4)} + \eta_2^{(4)} + \eta_1^{(4)} + \eta^{(4)} = \\ &= (\eta^{(4)} + \eta_1^{(4)} + \eta_2^{(4)} + \eta_3^{(4)}) + \eta^{(4)} - \eta_3^{(4)} = -1 + \eta^{(4)} - \eta_3^{(4)}. \end{aligned}$$

Следовательно,

$$\eta_3^{(4)} = \frac{\eta^{(4)} - 1}{\eta^{(4)} + 1}.$$

Таким образом, период $\eta^{(8)}$ является корнем уравнения

$$x^2 - \eta^{(4)}x + \frac{\eta^{(4)} - 1}{\eta^{(4)} + 1} = 0,$$

то есть

$$\eta^{(8)} = \frac{\eta^{(4)} \pm \sqrt{(\eta^{(4)})^2 - 4 \frac{\eta^{(4)} - 1}{\eta^{(4)} + 1}}}{2}. \quad (3)$$

Наконец, поскольку

$$\eta^{(8)} = \zeta + \zeta^{16}$$

и

$$\zeta^{16} = \zeta^{17} = 1,$$

то корень ζ (т. е., если хотите, одночленный период $\eta^{(16)}$) является корнем уравнения

$$x^2 - \eta^{(8)}x + 1 = 0,$$

то есть

$$\zeta = \frac{\eta^{(8)} \pm \sqrt{(\eta^{(8)})^2 - 4}}{2}. \quad (4)$$

Задача. Показать, что во всех формулах (1), (2), (3), (4) перед корнем следует брать знак плюс.

Подставляя выражение (1) для $\eta^{(2)}$ в формулу (2), затем получившееся выражение для $\eta^{(4)}$ в формулу (3) и, наконец, получившееся выражение для $\eta^{(8)}$ в формулу (4), мы получим окончательное выражение для ζ , содержащее, кроме арифметических действий, лишь операцию извлечения квадратного корня. Впрочем, для геометрических надобностей достаточно знать число $\eta^{(8)}$ (представляющее собой, как легко видеть, удвоенную апофему правильного 17-угольника), так что последнюю подстановку (приводящую к мнимостям) можно и не делать. В результате мы получим (после некоторых упрощений) для апофемы $\eta^{(8)}/2$ следующее выражение:

$$\frac{\eta^{(8)}}{2} = \frac{-1 + \sqrt{17} + \sqrt{2}\sqrt{17 - \sqrt{17}} + \sqrt{2}\sqrt{3 + \sqrt{17}}\sqrt{2\sqrt{17} - \sqrt{2}\sqrt{17 - \sqrt{17}}}}{16}.$$

Задача. Исследовать случай $p = 13$ (должны получиться два квадратных уравнения и одно уравнение третьей степени) и случай $p = 19$ (одно квадратное уравнение и два уравнения третьей степени).

ГЛАВА 5

ПОСТРОЕНИЯ ЦИРКУЛЕМ И ЛИНЕЙКОЙ

1. Основная теорема теории геометрических построений

Известно, что любая элементарно-геометрическая фигура определяется (с точностью до положения) длинами некоторых отрезков. Например, окружность определяется ее радиусом, угол — его линией косинуса (в круге единичного радиуса) и т. п. Следовательно, любая задача на построение сводится к задаче построения по некоторым числам (длинам данных отрезков) новых чисел (длин искомых отрезков). В связи с этим естественно возникает задача описания всех чисел, являющихся длинами отрезков, которые можно получить из данных отрезков геометрическими построениями с помощью тех или иных чертежных средств. Мы ограничимся здесь классической постановкой этой задачи, когда за основные чертежные средства принимаются циркуль переменного раствора и односторонняя линейка без делений.

Пусть $1, \alpha, \beta, \dots$ — длины данных отрезков (поскольку выбор единицы длины находится всецело в нашем распоряжении, мы можем считать, что один из данных отрезков имеет длину 1). Мы скажем, что положительное действительное число ξ может быть *построено* (исходя из данных чисел $1, \alpha, \beta, \dots$), если, отправляясь от отрезков длин $1, \alpha, \beta, \dots$, можно с помощью только циркуля и линейки построить отрезок длины ξ .

Замечание. Строго говоря, для придания этому определению точного смысла, нам необходимо предварительно детально описать, что мы понимаем под выражением «построить отрезок с помощью циркуля и линейки». Мы этого делать не будем, поскольку, с одной стороны, такое описание можно найти в любом курсе теории геометрических

построений, а с другой стороны, оно нам, по существу, не нужно. Для наших целей вполне достаточно наивного «школьного» представления о значении этого выражения. Читатель, знакомый с современным, формальным, определением понятия «построить отрезок циркулем и линейкой», без труда сможет сам изложить все дальнейшее в том же формальном стиле.

Как известно, циркулем и линейкой можно, в частности, построить 1) сумму двух или нескольких отрезков, 2) разность двух отрезков, 3) отрезок четвертый пропорциональный к трем данным отрезкам (этот отрезок выражается формулой ab/c , где a , b и c — данные отрезки), 4) отрезок средний пропорциональный к двум данным отрезкам (этот отрезок выражается формулой \sqrt{ab} , где a и b — данные отрезки). Отсюда вытекает, что следующие действия над числами можно осуществить с помощью циркуля и линейки:

- 1) действие сложения,
- 2) действие вычитания (для случая, когда уменьшаемое больше вычитаемого),
- 3) действие умножения (сводится к построению отрезка четвертого пропорционального к отрезкам a , b и 1),
- 4) действие деления (сводится к построению отрезка четвертого пропорционального к отрезкам a , 1 и c),
- 5) действие извлечения квадратного корня (арифметического) из положительного числа (сводится к построению отрезка среднего пропорционального к отрезкам a и 1).

Мы будем называть эти действия *примитивными*. Положительное число ξ мы будем называть *примитивным*, если его можно получить из чисел 1, α , β , ..., применяя (любое конечное число раз) примитивные действия. Оказывается, что примитивными действиями, по существу, исчерпываются все действия над положительными числами, которые можно осуществить циркулем и линейкой. Именно, имеет место следующая основная теорема.

Число ξ тогда и только тогда можно построить (исходя из чисел 1, α , β , ...), когда это число примитивно.

Достаточность этого условия немедленно следует из всего сказанного выше. Поэтому мы должны доказать лишь его необходимость.

Для этого нам удобно несколько расширить список примитивных действий. Рассмотрим следующие действия (над не обязательно положительными числами):

- 1) сложение,
- 2) вычитание (производимое без всяких ограничений),
- 3) умножение,
- 4) деление,
- 5) извлечение квадратного корня (арифметического) из положительного числа.

Мы будем называть эти действия *пифагоровыми* (таким образом, пифагоровы действия отличаются от примитивных лишь тем, что вычитание производится без всяких ограничений).

Запас чисел, которые можно получить из чисел $1, \alpha, \beta, \dots$ пифагоровыми действиями (будем впредь называть эти числа *пифагоровыми*), безусловно больше запаса чисел, которые можно получить из тех же чисел $1, \alpha, \beta, \dots$ примитивными действиями (т. е. запаса примитивных чисел). Например, все примитивные числа положительны (напомним, что исходные числа $1, \alpha, \beta, \dots$ по условию положительны), тогда как среди пифагоровых чисел имеются и отрицательные. Однако оказывается, что

любое пифагорово положительное число примитивно, так что в области положительных чисел пифагоровы действия не дают ничего нового (по сравнению с примитивными).

Для доказательства этого утверждения мы должны более внимательно исследовать строение пифагоровых чисел. Каждое пифагорово число γ получается из исходных чисел $1, \alpha, \beta, \dots$ в результате применения некоторого набора пифагоровых действий. Пусть n — наименьшее число пифагоровых действий, необходимых для получения числа γ . Это число мы будем называть *рангом* пифагорова числа γ . Ранг, равный нулю, имеют исходные числа $1, \alpha, \beta, \dots$ и только они. Число 0 имеет ранг, равный единице (ибо $0 = 1 - 1$). Числа $-1, -\alpha, -\beta, \dots$, противоположные исходным числам $1, \alpha, \beta, \dots$, имеют ранг, не больший двух (ибо, например, $-1 = 0 - 1 = (1 - 1) - 1$). Вообще, если число γ имеет ранг n , то ранг числа $-\gamma$ не превосходит $n + 2$. Однако ранг числа $-\gamma$ может быть и меньше $n + 2$. Например,

если пифагорово число γ ранга n отрицательно, то ранг числа $-\gamma$ (т. е. числа $|\gamma|$) не превосходит n .

Мы докажем это утверждение индукцией по рангу n числа γ . Если $n = 0$, то число γ не может быть отрицательным, так что в этом случае рассматриваемое утверждение справедливо (потому что бессодержательно). Пусть оно уже доказано для всех чисел ранга, меньшего чем n . Любое число γ ранга n выражается через некоторые числа γ_1 и γ_2 меньших рангов по одной из следующих формул:

- a) $\gamma = \gamma_1 + \gamma_2,$
 - б) $\gamma = \gamma_1 - \gamma_2,$
 - в) $\gamma = \gamma_1\gamma_2,$
 - г) $\gamma = \frac{\gamma_1}{\gamma_2},$
 - д) $\gamma = \sqrt{\gamma_1}.$
- (1)

причем для отрицательного γ случай д) невозможен, а в каждом из остальных четырех случаев числа γ_1 и γ_2 можно выбрать так, чтобы их ранги n_1 и n_2 были связаны с рангом n числа γ соотношением

$$n = n_1 + n_2 + 1.$$

Задача. Докажите это утверждение.

Очевидно, что число $-\gamma = |\gamma|$ выражается через числа $|\gamma_1|$ и $|\gamma_2|$ по тем же формулам (однако, например, формула а) может перейти в формулу б) и наоборот). Следовательно, ранг m числа $-\gamma$ не превосходит числа $m_1 + m_2 + 1$, где m_1 , m_2 — ранги чисел $|\gamma_1|$, $|\gamma_2|$ соответственно. Заметим, что ранг m вполне может быть меньше суммы $m_1 + m_2 + 1$. Если число γ_1 положительно, то $\gamma_1 = |\gamma_1|$, и потому $m_1 = n_1$. Если же оно отрицательно, то, по предположению индукции, $m_1 \leq n_1$. Таким образом, во всех случаях $m_1 \leq n_1$. Аналогично $m_2 \leq n_2$, и потому $m \leq m_1 + m_2 + 1 \leq n_1 + n_2 + 1 = n$. Тем самым высказанное утверждение полностью доказано.

Докажем теперь сформулированное выше утверждение о примитивности положительных пифагоровых чисел. Для чисел нулевого ранга оно, очевидно, справедливо. Пусть это утверждение уже доказано для всех положительных пифагоровых чисел ранга, меньшего чем n . Любое положи-

тельное пифагорово число γ принадлежит к одному из пяти типов (1). Если оно принадлежит типу д), т. е. имеет вид $\sqrt{\gamma_1}$, то число γ_1 также положительно. Кроме того, его ранг равен $n - 1$, и потому, по предположению индукции, число γ_1 примитивно. Следовательно, число γ также примитивно. Если число γ принадлежит типу в), или типу г), т. е. имеет вид $\gamma_1\gamma_2$ или γ_1/γ_2 , то либо оба числа γ_1 и γ_2 положительны (и потому, по предположению индукции, примитивны), либо оба они отрицательны, и тогда $\gamma = (-\gamma_1)(-\gamma_2)$ (или соответственно $\gamma = -\gamma_1/-\gamma_2$). Но, согласно доказанному выше утверждению, ранги чисел $-\gamma_1 = |\gamma_1|$ и $-\gamma_2 = |\gamma_2|$ не превосходят соответственно рангов n_1 и n_2 чисел γ_1 и γ_2 . Следовательно, по предположению индукции, числа $-\gamma_1$ и $-\gamma_2$ примитивны. Таким образом, число γ получается из примитивных чисел действиями умножения или деления, и потому само является примитивным числом. Случай, когда число γ принадлежит типу а) или типу б), рассматривается аналогично.

В силу доказанного предложения мы можем теперь сформулировать нашу основную теорему в следующем виде:

число ξ тогда и только тогда может быть построено, когда оно пифагорово.

Как уже упоминалось, достаточность условия этой теоремы очевидна (если, конечно, знать, что положительные пифагоровы числа совпадают с примитивными), так что мы должны доказать лишь его необходимость, т. е. должны доказать, что если число ξ может быть построено, то оно пифагорово.

С этой целью мы выберем на рассматриваемой плоскости (в которой производятся все построения) некоторую декартову систему координат. Будем называть точку плоскости *пифагоровой точкой*, если обе ее координаты являются пифагоровыми числами. Данные отрезки (длин 1, a , b , ...) мы отложим на положительной оси абсцисс так, чтобы левым концом каждого отрезка служило начало координат. Тогда их правые концы будут являться пифагоровыми точками. С другой стороны, ясно, что если концы некоторого отрезка являются пифагоровыми точками, то его длина выражается пифагоровым числом. Кроме того, задача построения отрезка равносильна задаче построения его концов. Поэтому для

доказательства того, что если число ξ может быть построено, то оно пифагорово, достаточно доказать, что

каждая точка, получающаяся из пифагоровых точек геометрическими построениями с помощью циркуля и линейки, сама является пифагоровой точкой.

Оказывается, что аналогичное утверждение имеет место и для других элементарно-геометрических образов (прямых и окружностей). Назовем прямую или окружность *пифагоровой*, если все коэффициенты ее канонического уравнения (т. е. уравнения $y = kx + b$ или $x = a$ для прямой и уравнения $(x - a)^2 + (y - b)^2 = r^2$ для окружности) являются пифагоровыми числами. Тогда имеет место следующее общее предложение:

каждая точка, прямая или окружность, получающаяся из пифагоровых точек в результате некоторого построения циркулем и линейкой, пифагорова.

На первый взгляд кажется, что это утверждение заведомо ложно (впрочем, строго говоря, это действительно так). Дело в том, что, как правило, любое построение содержит некоторый элемент произвола (например, берутся произвольные точки, проводятся окружности произвольного радиуса и т. п.), и, конечно, этот произвол может повлечь появление не пифагоровых образов. Однако мы можем ограничить этот произвол и выбирать «произвольные» образы лишь среди пифагоровых. При этом условии высказанное возражение автоматически отпадает.

Однако здесь появляется другая трудность. В некоторых построениях свобода в выборе «произвольных» образов часто ограничена дополнительными условиями (выбираемая точка должна лежать внутри некоторой фигуры, радиус окружности должен быть не меньше некоторого числа и т. п.) и априори неясно, можно ли совместить эти условия с условием пифагоровости. По этому поводу можно заметить следующее. Во-первых, в любом построении достаточно произвольно выбирать лишь точки (ибо выбор, например, произвольной прямой сводится к выбору двух любых ее точек). Во-вторых, любое условие на выбор точки, могущее возникнуть при элементарно-геометрическом построении, требует, чтобы точка либо принадлежала некоторой уже построенной фигуре, либо лежала вне некоторой другой такой фигуры, наконец, удовлетворяла обоим этим условиям. Поэтому, если мы

предположим, что наше утверждение справедливо для построений, не содержащих произвола, то в построении, содержащем произвол, нам придется выбирать точку на некоторой пифагоровой (т. е. состоящей из пифагоровых точек, прямых и окружностей) фигуре, возможно, вне некоторой другой (но также пифагоровой) фигуры. Однако, поскольку среди чисел $1, \alpha, \beta, \dots$ содержится число 1, среди пифагоровых чисел содержатся все рациональные числа, и потому пифагоровы точки расположены на плоскости «всюду плотно». Поэтому вне любой фигуры пифагорову точку найти всегда можно. Далее, легко видеть, что пересечение двух пифагоровых прямых или окружностей (пересекающихся в конечном числе точек) состоит из пифагоровых точек (ибо координаты этих точек получаются из коэффициентов пересекающихся прямых или окружностей в результате решения линейных или квадратных уравнений). Поэтому, для того чтобы найти на некоторой пифагоровой фигуре пифагорову точку, достаточно найти пифагорову прямую, имеющую с этой фигурой хотя бы одну общую точку. Ясно, что такая прямая всегда существует (даже в классе прямых с рациональными коэффициентами). Более того, таких прямых настолько много, что всегда можно найти прямую, пересекающую данную фигуру в точке, не лежащей на любой другой фигуре. Таким образом, при любом построении выбор «произвольных» точек всегда можно осуществить в классе пифагоровых точек.

Отсюда следует, что наше предложение можно доказывать лишь для построений, не содержащих произвола. Но любое такое построение сводится к ряду построений:

1) общих точек (если они существуют) двух уже построенных прямых или окружностей;

2) прямой, проходящей через две уже построенные точки;

3) окружности с центром в построенной точке и радиусом, равным расстоянию между двумя построенными точками.

Как мы уже видели, построения 1) пифагоровы образы переводят в пифагоровы. Аналогичным свойством обладают, очевидно, и построения 2) и 3) (ибо, например, коэффициенты уравнения прямой, проходящей через две точки, рационально выражаются через координаты этих точек). Следовательно, при любом сколь угодно сложном построении мы, исходя из пифагоровых точек, будем получать лишь

пифагоровы точки, прямые и окружности. Наше утверждение (а вместе с ним и основная теорема) полностью доказано.

Полученное необходимое и достаточное условие возможности построения отрезка имеет дело, по существу, лишь с положительными числами и потому плохо приспособлено для анализа средствами алгебры. Чтобы преодолеть этот недостаток, мы будем говорить, что действительное число ξ (положительное, отрицательное или равное нулю) может быть построено (исходя из положительных чисел 1, α , β , ...), если оно либо равно нулю, либо число $|\xi|$ может быть построено в ранее определенном смысле. Оказывается, что при таком определении

основная теорема (в том виде, как она сформулирована на стр. 189) сохраняет силу и для любых действительных чисел ξ .

Действительно, при $\xi = 0$ это утверждение тривиально, при $\xi > 0$ оно совпадает с основной теоремой, а при $\xi < 0$ непосредственно вытекает из этой теоремы в силу того, что число $-\xi$ может быть построено (является пифагоровым числом) одновременно с числом ξ .

Эта формулировка основной теоремы с алгебраической точки зрения уже более удовлетворительна, однако она не включает комплексные числа. Имея в виду перенести ее и на этот случай, мы будем говорить, что комплексное число $\xi = \xi_1 + i\xi_2$ может быть построено (исходя из чисел 1, α , β , ...), если могут быть построены (в смысле предыдущего определения) действительные числа ξ_1 и ξ_2 . Ясно, что для действительных чисел это определение совпадает с предыдущим.

Далее, мы скажем, что комплексное число *пифагорово* (по отношению к числам 1, α , β , ...), если оно может быть получено из этих чисел с помощью четырех арифметических действий и операции извлечения квадратного корня. Здесь уже неясно, что для действительных чисел это определение совпадает с принятым ранее. Однако это так. Более того, имеет место следующее общее предложение:

комплексное число $\xi = \xi_1 + i\xi_2$ тогда и только тогда является пифагоровым числом, когда пифагоровыми числами (в ранее принятом смысле) являются действительные числа ξ_1 и ξ_2 .

Достаточность этого условия очевидна (ибо число $t = \sqrt{-1}$ пифагорово). Что же касается необходимости, то она непосредственно вытекает из того факта, что извлечение квадратного корня из любых комплексных чисел сводится к арифметическим действиям и извлечению квадратных корней из положительных чисел (см. Курс, стр. 124—125).

Из этого предложения немедленно вытекает, что *основная теорема (как она сформулирована на стр. 189) имеет место и для комплексных чисел.*

Для применения методов теории Галуа удобно сформулировать основную теорему в терминах теории полей.

Пусть P — поле, порожденное над полем R рациональных чисел числами α, β, \dots . Поскольку среди исходных чисел $1, \alpha, \beta, \dots$ содержится число 1, все элементы поля P являются пифагоровыми числами.

Расширение K поля P мы будем называть *пифагоровым*, если

$$K = P(\alpha_1, \alpha_2, \dots, \alpha_s),$$

где числа $\alpha_1, \alpha_2, \dots, \alpha_s$ обладают тем свойством, что для любого $i = 1, 2, \dots, s$ число $\beta_i = \alpha_i^2$ принадлежит полю $P(\alpha_1, \dots, \alpha_{i-1})$ (при $i=1$ полю P).

Ясно, что

число ξ тогда и только тогда является пифагоровым числом, когда оно принадлежит некоторому пифагоровому расширению поля P .

Таким образом, мы приходим к следующей формулировке основной теоремы, которую будем рассматривать как окончательную:

число ξ тогда и только тогда может быть построено (исходя из чисел 1, α, β, \dots), когда оно содержится в некотором пифагоровом расширении поля $P = R(\alpha, \beta, \dots)$.

Замечание. Основную теорему часто формулируют в следующем виде:

число ξ тогда и только тогда может быть построено (исходя из чисел 1, α, β, \dots), когда решение неприводимого уравнения (над полем $P = R(\alpha, \beta, \dots)$) с корнем ξ сводится к решению цепи квадратных уравнений, т. е., как говорят, число ξ выражается в квадратных радикалах (через элементы поля P).

Очевидно, что эта формулировка равносильна нашей.

Доказанная основная теорема хотя и чрезвычайно интересна с теоретической точки зрения, может приобрести практический интерес лишь после того, как будут найдены достаточно простые признаки пифагоровости расширений. Один такой признак, вполне исчерпывающий с практической точки зрения проблему, мы докажем в п. 3. Предварительно в п. 2 мы изложим необходимые для этого сведения из общей теории групп.

2. Примарные группы

Пусть G — произвольная группа. Ее элемент z называется *центральным*, если он перестановочен с любым элементом группы G , т. е. если для любого элемента $g \in G$ имеет место равенство

$$gz = zg.$$

В абелевых группах (и только в них) все элементы центральны. В произвольной группе единица e всегда центральна.

Совокупность Z всех центральных элементов группы G называется ее *центром*. Легко видеть, что центр любой группы является ее (очевидно, абелевым) нормальным делителем (возможно состоящим лишь из единицы e). Действительно, во-первых, он непуст (содержит единицу e), во-вторых, является подгруппой (если $z_1 \in Z$ и $z_2 \in Z$, то для любого элемента $g \in G$ имеет место равенство $(z_1 z_2^{-1})g = z_1(z_2^{-1}g) = (z_2^{-1}g)z_1 = (g^{-1}z_2)^{-1}z_1 = (z_2 g^{-1})^{-1}z_1 = g(z_2^{-1}z_1) = g(z_1 z_2^{-1})$, т. е. $z_1 z_2^{-1} \in Z$), в-третьих, для любого элемента $g \in G$ из включения $z \in Z$ вытекает включение $gzg^{-1} \in Z$ (ибо $gzg^{-1} = zgg^{-1} = z$).

Элемент g_1 группы G называется *сопряженным* элементу g , если существует такой элемент $h \in G$, что $g_1 = h^{-1}gh$. Совокупность всех элементов группы G , сопряженных некоторому элементу $g \in G$, называется *классом сопряженных элементов* (определенным элементом g) и обозначается символом $[g]$.

Каждый класс $[g]$ содержит элемент g (ибо $g = e^{-1}ge$); любой элемент g_1 класса $[g]$ определяет тот же класс, т. е.

$[g_1] = [g]$ (действительно, по условию $g_1 = h^{-1}gh$, и если $g' \in [g_1]$, т. е. $g' = (h')^{-1}g_1h'$, то $g' = (h'h)^{-1}g(h'h)$, т. е. $g' \in [g]$, а если $g' \notin [g]$, т. е. $g' = (h')^{-1}gh'$, то $g' = ((h')^{-1}h)^{-1}g_1((h')^{-1}h)$, т. е. $g' \in [g_1]$), так что любые два класса либо совпадают, либо не пересекаются. Таким образом,

группа G распадается на непересекающиеся классы сопряженных элементов.

Понятие класса сопряженных элементов тесно связано с понятием нормального делителя. Именно, подгруппа H группы G тогда и только тогда является нормальным делителем этой группы, когда для любого элемента $g \in H$ весь класс $[g]$ содержится в H . Другими словами, нормальные делители можно определить как подгруппы, состоящие из нескольких полных классов сопряженных элементов.

Класс $[g]$ вполне может состоять лишь из одного элемента. Очевидно, что это имеет место тогда и только тогда, когда элемент g централен.

Рассмотрим теперь совокупность Z_g всех элементов группы G , перестановочных с элементом $g \in G$, т. е. совокупность всех таких элементов $z \in G$, что

$$zg = gz.$$

Эта совокупность непуста (ибо содержит все степени элемента g) и является подгруппой группы G (докажите!). Она называется централизатором элемента g в группе G . Очевидно, что

элемент g тогда и только тогда централен, когда его централизатор Z_g совпадает со всей группой G .

Каждому элементу g_1 класса $[g]$ сопоставим смежный класс $\chi(g_1)$ группы G по централизатору Z_g , положив $\chi(g_1) = Z_g h$, где h — такой элемент группы G , что $g_1 = h^{-1}gh$.

Легко видеть, что это определение законно, т. е. смежный класс $\chi(g_1)$ не зависит от выбора элемента h . Действительно, если $h^{-1}gh = (h')^{-1}gh'$, то $(h(h')^{-1})g = g(h(h')^{-1})$, т. е. $h(h')^{-1} \in Z_g$ и потому $Z_g h = Z_g h'$.

Далее, легко видеть, что если $\chi(g_1) = \chi(g_2)$, где $g_1, g_2 \in [g]$, то $g_1 = g_2$. Действительно, пусть $g_1 = h_1^{-1}gh_1$, и

$g_2 = h_2^{-1}gh_2$. Тогда равенство $\chi(g_1) = \chi(g_2)$ означает, что $h_1 = zh_2$, где $z \in Z_g$. Поэтому $g_1 = h_2^{-1}z^{-1}gh_2 = h_2^{-1}gh_2 = g_2$.

Наконец, очевидно, что любой смежный класс $Z_g h$ группы G по подгруппе Z_g имеет вид $\chi(g_1)$, где $g_1 \in [g]$ (за элемент g_1 можно принять элемент $h^{-1}gh$).

Таким образом, отображение χ осуществляет взаимно-однозначное соответствие между классом $[g]$ и множеством всех смежных классов группы G по централизатору Z_g . Следовательно, (предполагается, конечно, что класс $[g]$ состоит из конечного числа элементов)

число элементов, содержащихся в классе $[g]$, равно индексу централизатора Z_g .

Для конечной группы отсюда и из теоремы Лагранжа вытекает, что

число элементов, содержащихся в любом классе сопряженных элементов конечной группы G делит порядок этой группы.

Применим эти общие теоремы (относящиеся к произвольным группам) к так называемым *примарным* (по некоторому простому числу p) группам, которые определяются как конечные группы, порядок которых имеет вид p^n , где $n \geq 0$.

В первую очередь мы докажем, что

любая примарная группа G содержит отличные от единицы центральные элементы.

Действительно, как мы знаем, группа G распадается на непересекающиеся классы сопряженных элементов. Пусть k_1, k_2, \dots, k_s — числа элементов этих классов. Тогда сумма $k_1 + k_2 + \dots + k_s$ равна порядку p^n группы G :

$$k_1 + k_2 + \dots + k_s = p^n. \quad (1)$$

Все числа k_i делят порядок p^n , т. е. $k_i = p^{n_i}$, где $n_i \geq 0$, причем хотя бы одно из этих чисел равно единице (так как существует класс — именно класс, определяемый единицей в группе G , — состоящий только из одного элемента). Отсюда и из равенства (1) вытекает, что по крайней мере p чисел k_i равны единице, т. е. что существует по крайней мере p центральных элементов. Теорема доказана.

Докажем теперь, что

любая примарная группа G разрешима.

Пусть p^n — порядок группы G . Проведем доказательство индукцией по числу n . Для $n = 0$ (а также для $n = 1$) теорема очевидна. Предполагая, что теорема уже доказана для всех примарных групп порядка p^k , где $k < n$, рассмотрим центр Z группы G . По только что доказанному порядок центра Z отличен от единицы, т. е. имеет вид p^m , где $m > 0$. Поэтому порядок p^{n-m} факторгруппы G/Z меньше p^n , и следовательно, по предположению индукции, эта факторгруппа разрешима. Таким образом, группа G обладает разрешимым (даже абелевым) нормальным делителем Z , факторгруппа по которому разрешима. Следовательно (см. ч. II, гл. 1, п. 4), сама группа G также разрешима.

• 3. Пифагоровы расширения

Ясно, что если $\alpha^2 \in P$ и $\alpha \notin P$, то степень $[P(\alpha) : P]$ поля $P(\alpha)$ над полем P равна двум. Отсюда непосредственно вытекает, что

степень $[K : P]$ любого пифагорова расширения K поля P является степенью двойки, т. е. имеет вид 2^n .

Оказывается, что для нормальных расширений имеет место и обратное утверждение, т. е.

нормальное расширение K поля P тогда и только тогда пифагорово, когда его степень $[K : P]$ является степенью двойки.

Действительно, если степень нормального расширения K является степенью двойки, то его группа Галуа $G = G(K, P)$ примарна (по числу 2) и потому разрешима, т. е. обладает разрешимым рядом

$$G = H_0 \supset H_1 \supset \dots \supset H_{l-1} \supset H_l \supset \dots \supset H_n = e,$$

все факторы H_{l-1}/H_l , которого являются простыми циклическими группами порядков, делящих порядок группы G (см. ч. II, гл. 1, п. 4), т. е. — в рассматриваемом случае — циклическими группами второго порядка. Пусть

$$P = L_0 \subset L_1 \subset \dots \subset L_{l-1} \subset L_l \subset \dots \subset L_n = K$$

— соответствующая цепочка подполя поля K . Так как $[L_l : L_{l-1}] = 2$, то $L_l = L_{l-1}(\alpha_l)$, где α_l — корень некоторого квадратного уравнения над полем L_{l-1} . Поскольку любое квадратное уравнение сводится к уравнению вида $x^2 - a = 0$,

можно без потери общности считать, что $\alpha_l^2 \in L_{l-1}$. Таким образом, $K = P(\alpha_1, \dots, \alpha_n)$, причем для любого $l = 1, \dots, n$ число α_l^2 принадлежит полю $P(\alpha_1, \dots, \alpha_{l-1})$ (при $l=1$ полю P). Другими словами, расширение K пифагорово.

Из доказанного предложения немедленно вытекает, что *любое нормальное подполе нормального пифагорова расширения само является пифагоровым расширением*.

Действительно, его степень является степенью двойки.

Далее, оказывается, что

любое пифагорово расширение K содержится в некотором нормальном пифагоровом расширении \bar{K} .

Действительно, пусть $[K : P] = 2^n$. Проведем индукцию по числу n . Если $n=0$, то $K=P$, и теорема, очевидно, справедлива (за поле \bar{K} можно принять само поле $K=P$). Пусть теорема уже доказана для полей степени 2^{n-1} . По определению, любое пифагорово расширение K степени 2^n имеет вид $L(\alpha)$, где L — пифагорово расширение степени 2^{n-1} , а α — такое число, что $\alpha^2 \in L$. По предположению индукции, поле L содержится в некотором нормальном пифагоровом расширении \bar{L} . Рассмотрим минимальный многочлен $f(x)$ числа α^2 над полем P . Поскольку $\alpha^2 \in L \subset \bar{L}$ и поскольку поле \bar{L} нормально, многочлен $f(x)$ разлагается над полем \bar{L} на линейные множители:

$$f(x) = (x - \beta_1)(x - \beta_2) \dots (x - \beta_m),$$

где $\beta_1 = \alpha^2$, $\beta_2, \dots, \beta_m \in \bar{L}$. Пусть $g(x) = f(x^2)$ (так что $g(\alpha) = 0$), и пусть \bar{K} — поле разложения многочлена $g(x)$ над полем \bar{L} (так что $\alpha \in \bar{K}$). Согласно лемме, доказанной на стр. 83, поле \bar{K} является нормальным расширением поля P . Кроме того, так как $\alpha \in \bar{K}$ и $L \subset \bar{L} \subset \bar{K}$, то $K = L(\alpha) \subset \bar{K}$. Наконец, очевидно, что

$$\bar{K} = \bar{L}(\gamma_1, \dots, \gamma_m),$$

где $\gamma_1, \dots, \gamma_m$ — такие числа, что $\gamma_i^2 = \beta_i$, $i = 1, \dots, m$. Поскольку $\gamma_i^2 \in \bar{L}$, и потому $\gamma_i^2 \in \bar{L}(\gamma_1, \dots, \gamma_{i-1})$, поле \bar{K} является пифагоровым расширением поля \bar{L} , а значит, и поля P (ибо пифагорово расширение пифагорова расширения

само, очевидно, является пифагоровым расширением основного поля). Тем самым теорема полностью доказана.

Полученные результаты о пифагоровых расширениях позволяют доказать следующий, очень удобный на практике критерий пифагоровости числа:

корень ξ неприводимого (над полем P) многочлена $f(x)$ тогда и только тогда является пифагоровым числом (т. е. может быть построен циркулем и линейкой), когда степень поля расширения многочлена $f(x)$ является степенью двойки.

Действительно, если число ξ пифагорово, то оно содержится в некотором пифагоровом расширении K поля P и потому в некотором нормальном пифагоровом расширении \bar{K} . Поскольку поле разложения многочлена $f(x)$ нормально, отсюда вытекает, что оно содержится в поле \bar{K} , и потому его степень является степенью двойки.

Обратно, если степень поля разложения многочлена $f(x)$ является степенью двойки, то оно пифагорово (потому что нормально), так что число ξ содержится в пифагоровом расширении поля P и потому является пифагоровым числом.

Отметим в заключение следующий простой необходимый (но не достаточный!) признак пифагоровости, немедленно вытекающий из доказанной теоремы:

если число ξ пифагорово, то его степень над полем P (т. е. степень его минимального многочлена $f(x)$) является степенью двойки.

Действительно, степень любого алгебраического числа делит степень поля разложения его минимального многочлена.

4. Некоторые конкретные задачи на построение

Применим полученные общие результаты к некоторым классическим задачам на построение.

Задача об удвоении куба формулируется следующим образом: построить куб (т. е. его сторону), объем которого вдвое больше объема данного куба. В этом случае нам задан только один отрезок (сторона данного куба). Принимая его за единичный, мы получаем, во-первых, что основным полем P является поле R рациональных чисел, а во-вторых, что искомая сторона ξ удвоенного куба удовлетворяет

уравнению

$$x^3 - 2 = 0.$$

Поскольку это уравнение неприводимо над полем R (так как оно не имеет рациональных корней), степень числа ξ равна трем. Поэтому это число не пифагорово, т. е. не может быть построено циркулем и линейкой. Таким образом, *удвоение куба с помощью циркуля и линейки невыполнимо*.

Задача о трисекции угла формулируется следующим образом: разделить данный угол φ на три равные части. В этой задаче даны два отрезка (например, гипотенуза и прилежащий катет прямоугольного треугольника с углом φ). Принимая гипотенузу за единичный отрезок, мы получаем, что основным полем P является в этом случае поле $R(\alpha)$, где $\alpha = \cos \varphi$. За искомый отрезок мы примем линию косинуса угла $\frac{\varphi}{3}$. Таким образом, задача сводится к построению числа $\xi = \cos \frac{\varphi}{3}$. Поскольку $4\cos^3 \frac{\varphi}{3} - 3\cos \frac{\varphi}{3} = \cos \varphi$, это число удовлетворяет уравнению

$$4x^3 - 3x - \alpha = 0.$$

Если это уравнение неприводимо над полем $R(\alpha)$, то число ξ имеет степень 3 и потому не пифагорово, т. е. его построение невозможно. Так будет, например, при $\varphi = 60^\circ$, когда $\alpha = \frac{1}{2}$. Действительно, уравнение

$$8x^3 - 6x - 1 = 0$$

неприводимо над полем $R = R\left(\frac{1}{2}\right)$ (в противном случае оно обладало бы рациональным корнем, что, как легко видеть, невозможно). Таким образом, не существует никакого построения, осуществляющего деление угла в 60° на три равные части (т. е. построение угла в 20°). Тем более *не существует никакого единого построения, осуществляющего деление на три равные части произвольного угла*.

Это не мешает, конечно, существованию специальных построений для некоторых отдельных углов (для которых многочлен $4x^3 - 3x - \alpha$ приводим). Так, например, при $\alpha = 0$ (т. е. при $\varphi = 90^\circ$) или при $\alpha = -\frac{\sqrt{2}}{2}$ (т. е. при

$\varphi = 135^\circ$) этот многочлен приводим (над полями R и $R(\sqrt{2})$ соответственно). В первом случае он имеет корень $\frac{\sqrt{3}}{2} = \cos 30^\circ$, а во втором — корень $\frac{\sqrt{2}}{2} = \cos 45^\circ$.

Задача о трех биссектрисах формулируется следующим образом: построить треугольник, если даны его три биссектрисы. Пусть A, B, C — углы искомого треугольника, а $\beta_a, \beta_b, \beta_c$ — данные биссектрисы. Очевидно, что достаточно построить углы A, B и C . Из элементарной геометрии известно, что биссектрисы треугольника следующим образом выражаются через его углы и периметр $2p$:

$$\begin{aligned}\beta_a &= \frac{2p \sin \frac{B}{2} \sin \frac{C}{2}}{\cos \frac{A}{2} \cos \frac{B-C}{2}}, & \beta_b &= \frac{2p \sin \frac{C}{2} \sin \frac{B}{2}}{\cos \frac{B}{2} \cos \frac{C-A}{2}}, \\ \beta_c &= \frac{2p \sin \frac{A}{2} \sin \frac{B}{2}}{\cos \frac{C}{2} \cos \frac{A-B}{2}}.\end{aligned}$$

Следовательно,

$$\frac{\beta_a}{\beta_b} = \frac{\sin \frac{B}{2} \cos \frac{B}{2} \cos \frac{C-A}{2}}{\sin \frac{A}{2} \cos \frac{A}{2} \cos \frac{B-C}{2}}, \quad \frac{\beta_b}{\beta_c} = \frac{\sin \frac{C}{2} \cos \frac{C}{2} \cos \frac{A-B}{2}}{\sin \frac{B}{2} \cos \frac{B}{2} \cos \frac{C-A}{2}}.$$

Эти равенства представляют собой два уравнения, из которых и следует найти неизвестные углы A, B и C (двух уравнений достаточно, так как среди углов треугольника только два независимых).

Предположим для упрощения выкладок, что $\beta_b = \beta_c$. Тогда из второго уравнения легко выводится (сделайте это!), что $B = C$, т. е. искомый треугольник равнобедренный. Но для равнобедренного треугольника $A + 2B = \pi$ и потому

$$\sin \frac{A}{2} = \cos B, \quad \cos \frac{A}{2} = \sin B, \quad \cos \frac{C-A}{2} = \sin \frac{3B}{2}.$$

Кроме того,

$$\cos \frac{B-C}{2} = 1.$$

Поэтому первое уравнение приобретает следующий вид:

$$\frac{\sin \frac{3B}{2}}{2 \cos B} = k,$$

где $k = \frac{\beta_a}{\beta_b}$. Выражая по известным формулам $\sin \frac{3B}{2}$ и $\cos B$ через $\sin \frac{B}{2}$, мы получим отсюда, что величина $\sin \frac{B}{2}$ является корнем уравнения

$$4x^3 - 4kx^2 - 3x + 2k = 0.$$

Поскольку существуют значения k , для которых это уравнение неприводимо (например, в силу критерия Эйзенштейна оно неприводимо при $k = 3$), *построение треугольника по трем биссектрисам циркулем и линейкой невозможно* (даже при дополнительном предположении $\beta_b = \beta_c$).

Задача о построении правильного n -угольника сводится к построению первообразного корня из единицы степени n . Поскольку в этой задаче задается лишь один отрезок (например, радиус описанного круга), основным полем является поле R рациональных чисел.

Заметим в первую очередь, что многочлен $f_n(x)$ деления круга на n частей (т. е. многочлен, корнями которого являются все первообразные корни из единицы степени n и только эти корни) мы можем найти, отыскивая наибольшие общие делители многочленов $x^n - 1$ и $x^m - 1$, где m про-бегает все собственные (т. е. отличные от n) делители числа n , и освобождая от них многочлен $x^n - 1$. Действительно, корень степени n из единицы тогда и только тогда является первообразным корнем, когда он не служит корнем ни одного многочлена $x^m - 1$.

Отсюда немедленно вытекает, что

для любого n многочлен деления круга на n частей является многочленом над полем R (т. е. имеет рациональные коэффициенты).

Степень этого многочлена равна числу всех первообразных корней из единицы степени n , т. е. равна числу $\varphi(n)$ чисел меньших n и взаимно простых с n .

Как мы знаем, если число n простое, то многочлен $f_n(x)$ неприводим (см. гл. 2, п. 1). Оказывается, что это верно

и для любого n . Однако, поскольку доказательство этого факта в общем виде довольно сложно, мы его доказывать не будем, а ограничимся доказательством следующего более частного утверждения:

для любого примарного (т. е. имеющего вид p^a , где p — простое число) числа n многочлен деления круга на n частей неприводим (над полем R).

Действительно, так как все делители числа p^a имеют вид p^b и так как при $c < b$ многочлен $x^{p^b} - 1$ делится на многочлен $x^{p^c} - 1$, то

$$\begin{aligned} f_{p^a}(x) &= \frac{x^{p^a} - 1}{x^{p^{a-1}} - 1} = \\ &= x^{p^{a-1}(p-1)} + x^{p^{a-1}(p-2)} + \dots + x^{p^{a-1}} + 1. \end{aligned}$$

Применяя метод доказательства «от противного», мы предположим, что этот многочлен приводим. Тогда его можно представить в виде произведения $g(x)h(x)$ двух многочленов меньших степеней с целыми коэффициентами (см. Курс, стр. 352). Так как

$$g(1)h(1) = f_{p^a}(1) = p,$$

то одно из (целых) чисел $g(1)$ и $h(1)$ равно ± 1 , а другое равно $\pm p$. Пусть для определенности $g(1) = \pm 1$.

Рассмотрим произвольный первообразный корень ζ степени p^a из единицы, являющийся корнем многочлена $g(x)$. Поскольку все первообразные корни из единицы являются степенями любого из них, для каждого первообразного корня ζ' существует такое число m (взаимно простое с p^a , т. е. не делящееся на p), что $\zeta = (\zeta')^m$. Следовательно, число ζ' является корнем многочлена $g(x^m)$. Отсюда вытекает, что все первообразные корни из единицы степени p^a являются корнями многочлена $F(x)$, представляющего собой произведение всевозможных многочленов вида $g(x^m)$. Поэтому многочлен $F(x)$ делится на многочлен $f_{p^a}(x)$, т. е.

$$F(x) = f_{p^a}(x)\varphi(x),$$

где $\varphi(x)$ — некоторый многочлен с целыми (почему?) коэффициентами. Следовательно,

$$F(1) = f_{p^a}(1)\varphi(1),$$

т. е. число $F(1)$ делится на число $f_{p^a}(1) = p$. Но это невозможно, так как очевидно, что $F(1) = \pm 1$. Полученное противоречие доказывает, что многочлен $f_{p^a}(x)$ неприводим.

Замечание. Неприводимость многочлена $f_{p^a}(x)$ можно также легко доказать, производя замену $x = y + 1$ и используя критерий Эйзенштейна.

Таким образом, первообразные корни из единицы степени p^a являются корнями неприводимого многочлена степени $\varphi(p^a) = p^{a-1}(p - 1)$. Следовательно,

если построение правильного p^a -угольника, где p — простое число, а $a \geq 1$, циркулем и линейкой возможно, то число $p^{a-1}(p - 1)$ должно быть степенью двойки, т. е. либо $p = 2$, либо $a = 1$ и число p является простым числом Ферма.

Так как любой правильный 2^a -угольник, очевидно, можно построить циркулем и линейкой, то, вспоминая результаты гл. 3, мы получаем отсюда, что

построение правильного p^a -угольника циркулем и линейкой возможно тогда и только тогда, когда либо $p = 2$, либо $a = 1$ и число p является простым числом Ферма.

Заметим теперь, что

если числа n_1 и n_2 взаимно просты, то построение правильного n_1n_2 -угольника возможно тогда и только тогда, когда возможно построение правильного n_1 -угольника и правильного n_2 -угольника.

Действительно, построение правильного n -угольника равносильно построению угла $2\pi/n$. Но если мы можем построить угол $\alpha = 2\pi/n_1n_2$, то мы можем построить как угол $n_2\alpha = 2\pi/n_1$, так и угол $n_1\alpha = 2\pi/n_2$. Обратно, если мы можем построить углы $\alpha_1 = 2\pi/n_1$ и $\alpha_2 = 2\pi/n_2$, то мы можем построить любой угол вида $u\alpha_1 + v\alpha_2$, где u и v — произвольные целые числа. Принимая за u и v решения уравнения $n_1u + n_2v = 1$ (эти решения существуют в силу взаимной простоты чисел n_1 и n_2 ; см. лемму на стр. 70—71), мы видим, что угол $u\alpha_1 + v\alpha_2 = 2\pi\left(\frac{u}{n_1} + \frac{v}{n_2}\right) = 2\pi/n_1n_2$ мы также можем построить.

Отсюда и из только что доказанной теоремы вытекает следующий окончательный результат:

построение правильного n -угольника циркулем и линейкой возможно тогда и только тогда, когда число n

имеет вид

$$2^a p_1 p_2 \dots p_s,$$

где p_1, p_2, \dots, p_s — различные числа Ферма.

Задача о квадратуре круга формулируется следующим образом: построить квадрат равновеликий данному кругу. Поскольку в задаче задан только один отрезок (радиус круга), основным полем является поле R рациональных чисел. Принимая радиус данного круга за единицу, мы видим, что задача сводится к построению отрезка $\sqrt{\pi}$, т. е. к построению отрезка π . Мы докажем, что это невозможно, т. е. что квадратуру круга невозможно осуществить циркулем и линейкой. Другими словами, мы докажем, что число π не пифагорово. На самом деле, мы докажем даже большее, а именно что

число π не является корнем никакого многочлена с рациональными коэффициентами,

т. е. не является алгебраическим над полем R числом. (Такие числа называются трансцендентными.)

Пусть

$$g(x) = c_0 + c_1 x + \dots + c_N x^N$$

— произвольный многочлен. Положим

$$G(x) = g(x) + g'(x) + g''(x) + \dots + g^{(N)}(x).$$

Оказывается, что

существуют такие функции

$$q_0 = q_0(x), \quad q_1 = q_1(x), \dots, \quad q_N = q_N(x)$$

переменного x , не зависящие от многочлена $g(x)$, что для любого x имеет место соотношение

$$G(0) e^x = G(x) + Q(x), \quad (1)$$

где

$$Q(x) = \sum_{r=0}^N c_r q_r x^{r+1} = c_0 q_0 x + \dots + c_N q_N x^{N+1},$$

причем

$$|q_r(x)| \leq e^{|x|}$$

для всех x и всех $r = 0, 1, \dots, N$.

Ясно, что соотношение (1) линейно относительно многочлена $g(x)$, т. е. если оно справедливо для многочленов $g_1(x)$ и $g_2(x)$, то оно справедливо и для любого многочлена вида

$a_1g_1(x) + a_2g_2(x)$. Поэтому его достаточно доказать лишь для многочлена вида x^r . Но в этом случае оно принимает вид

$$r!e^x = (x^r + rx^{r-1} + r(r-1)x^{r-2} + \dots + r!) + q_r x^{r+1},$$

т. е. вид

$$e^x = 1 + \frac{x}{1!} + \dots + \frac{x^{r-2}}{(r-2)!} + \frac{x^{r-1}}{(r-1)!} + \frac{x^r}{r!} + q_r \frac{x^{r+1}}{r!}.$$

Поскольку, как известно из элементарного курса анализа,

$$e^x - \left(1 + \frac{x}{1!} + \dots + \frac{x^r}{r!}\right) = \frac{x^{r+1}}{(r+1)!} + \frac{x^{r+2}}{(r+2)!} + \dots,$$

за функцию $q_r(x)$ мы должны принять функцию

$$q_r(x) = \frac{1}{r+1} \left(1 + \frac{x}{r+2} + \dots + \frac{(r+1)!}{(r+k+1)!} x^k + \dots\right).$$

Так как

$$\frac{(r+1)!}{(r+k+1)!} \leq \frac{1}{k!},$$

то ряд в правой части этой формулы абсолютно сходится для всех x и определяет функцию, модуль которой не больше чем $e^{|x|}$. Поэтому $|q_r(x)| \leq \frac{1}{r+1} e^{|x|} \leq e^{|x|}$. Тем самым соотношение (1) полностью доказано.

Пусть теперь

$$f(x) = a_0 + a_1x + \dots + a_n x^n$$

— произвольный многочлен степени n с целыми коэффициентами и свободным членом a_0 , отличным от нуля. Рассмотрим многочлен

$$g(x) = a_n^{np-1} \frac{x^{p-1}}{(p-1)!} f^p(x),$$

где p — некоторое простое число, и соответствующий многочлен

$$G(x) = g(x) + g'(x) + \dots + g^{(N)}(x),$$

где $N = np + p - 1$ — степень многочлена $g(x)$.

Многочлен $g(x)$ мы можем записать в следующем виде:

$$g(x) = \frac{b_0 x^{p-1} + b_1 x^p + \dots + b_{np} x^N}{(p-1)!},$$

где b_0, b_1, \dots, b_{np} — целые числа, причем $b_0 = a_0^p a_n^{np-1}$. Таким образом, в рассматриваемом случае $c_k = 0$, если $k < p - 1$, и $c_k = \frac{b_{p-k-1}}{(p-1)!}$, если $k \geq p - 1$. Отсюда вытекает, что

$$g^{(r)}(0) = \begin{cases} 0 & \text{если } r < p - 1, \\ \frac{r!}{(p-1)!} b_{r-p-1} & \text{если } r \geq p - 1, \end{cases}$$

то есть

$$\begin{aligned} G(0) = a_0^p a_n^{np-1} + pb_1 + p(p+1)b_2 + \dots + \\ + p(p+1)\dots(np+p-1)b_{np}. \end{aligned}$$

Следовательно,

число $G(0)$ целое; если число p не делит коэффициенты a_0 и a_n (например, если $p > |a_0|$ и $p > |a_n|$), то число $G(0)$ не делится на p .

Рассмотрим теперь произвольный корень α многочлена $f(x)$. Используя тождественное соотношение $x = (x - \alpha) + \alpha$, мы можем многочлен $g(x)$ записать в следующем виде:

$$g(x) = \frac{\beta_0 (x - \alpha)^p + \beta_1 (x - \alpha)^{p+1} + \dots + \beta_{np-1} (x - \alpha)^N}{(p-1)!},$$

где $\beta_0, \dots, \beta_{np-1}$ — некоторые многочлены от α степеней, не больших чем $np - 1$ с целыми коэффициентами, делящимися на a_n^{np-1} . Отсюда вытекает, что

$$g^r(\alpha) = \begin{cases} 0 & \text{если } r < p, \\ \frac{r}{(p-1)!} \beta_{r-p} & \text{если } r \geq p, \end{cases}$$

то есть

$$\begin{aligned} G(\alpha) = p\beta_0 + p(p+1)\beta_1 + \dots + \\ + p(p+1)\dots(np+p-1)\beta_{np-1}. \end{aligned}$$

Следовательно,

число $G(\alpha)$ является многочленом от α степени, не большей чем $np - 1$ с целыми коэффициентами; все коэффициенты этого многочлена делятся на число a_n^{np-1} .

Пусть теперь

$$\alpha_1, \alpha_2, \dots, \alpha_n$$

— все корни многочлена $f(x)$. Так как $a_0 \neq 0$, то они все отличны от нуля. Рассмотрим число

$$A = G(\alpha_1) + G(\alpha_2) + \dots + G(\alpha_n).$$

Это число является симметрическим многочленом от $\alpha_1, \dots, \alpha_n$ общей степени, не большей чем $pr - 1$, с целыми коэффициентами, делящимися на ra_n^{pr-1} . Следовательно (см. Курс, стр. 328), оно является многочленом общей степени, не большей чем $pr - 1$, с целыми коэффициентами, делящимися на ra_n^{pr-1} , от элементарных симметрических функций корней $\alpha_1, \dots, \alpha_n$, т. е. от приведенных коэффициентов $\frac{a_0}{a_n}, \frac{a_1}{a_n}, \dots, \frac{a_{n-1}}{a_n}$ многочлена $f(x)$. Значит, это число является многочленом с целыми коэффициентами, делящимися на p , от целых чисел a_0, a_1, \dots, a_{n-1} . Поэтому

число A является целым числом, делящимся на p .

Рассмотрим далее функцию $Q(x)$, соответствующую многочлену $g(x)$ (см. выше соотношение (1)). Пусть M — наибольшее значение абсолютных величин коэффициентов многочлена $f(x)$. Ясно, что абсолютные величины коэффициентов многочлена $f^p(x)$ не превосходят числа $(n+1)^p M^p$ (каждый коэффициент является суммой не более чем $(n+1)^p$ произведений p коэффициентов многочлена $f(x)$). Следовательно, абсолютные величины коэффициентов c_r многочлена $g(x)$ не превосходят числа $\frac{(n+1)^p M^p}{(p-1)!}$. Поэтому, если $|x| > 1$, то

$$|Q(x)| \leq \sum_{r=0}^N |c_r| \cdot |q_r| \cdot |x|^{r+1} \leq \frac{(n+1)^p M^p}{(p-1)!} e^{|x|} |x| \times \\ \times \frac{|x|^{N+1} - 1}{|x| - 1} \leq \frac{(n+1)^p M^p}{(p-1)!} \frac{e^{|x|} |x|}{|x| - 1} |x|^{np+p} = K \frac{L^p}{(p-1)!},$$

где $K = \frac{e^{|x|} |x|}{|x| - 1}$ и $L = (n+1)M|x|^{n+1}$. Аналогично, если $|x| < 1$, то

$$|Q(x)| \leq K \frac{L^p}{(p-1)!}.$$

где $K = \frac{e^{|x|} |x|}{1 - |x|}$ и $L = (n + 1)M$. Наконец, если $|x| = 1$, то

$$|Q(x)| \leq K \frac{L^p p}{(p-1)!},$$

где $K = (n + 1)e^{|x|}$ и $L = (n + 1)M$.

Как известно из курса анализа,

$$\lim_{p \rightarrow \infty} \frac{L^p}{(p-1)!} = \lim_{p \rightarrow \infty} \frac{L^p p}{(p-1)!} = 0.$$

Следовательно,

для любого $\epsilon > 0$ и любого x существует такое число $P(\epsilon, x)$, что

$$|Q(x)| < \epsilon \quad \text{при } p > P(\epsilon, x).$$

В частности, существует такое число P , что для любого $i = 1, \dots, n$

$$|Q(\alpha_i)| < \frac{1}{n} \quad \text{при } p > P.$$

Следовательно,

$$|Q(\alpha_1)| + |Q(\alpha_2)| + \dots + |Q(\alpha_n)| < 1 \quad \text{при } p > P.$$

Рассмотрим теперь число

$$B = e^{a_1} + e^{a_2} + \dots + e^{a_n}.$$

Подставляя в соотношение (1) вместо x числа $\alpha_1, \dots, \alpha_n$ и складывая получившиеся равенства, мы получим, что

$$G(0)B = A + \gamma,$$

где $\gamma = Q(\alpha_1) + \dots + Q(\alpha_n)$. Другими словами,

$$\gamma = G(0)B - A.$$

Предположим, что число B целое, и выберем простое число p (которое пока было вполне произвольным) большим каждого из чисел $|a_0|, |a_n|, |B|$ и P . Тогда целое число $G(0)B$ не будет делиться на p и потому не будет равно числу A (которое, как мы знаем, на p делится). Следовательно, целое число $G(0)B - A$ будет отлично от нуля. Но это невозможно, так как оно равно числу γ , абсолютная

величина $|\gamma|$ которого при $p > P$ меньше единицы (ибо $|\gamma| \leq |Q(\alpha_1)| + \dots + |Q(\alpha_n)|$). Полученное противоречие доказывает следующую теорему.

Если отличные от нуля числа $\alpha_1, \dots, \alpha_n$ являются корнями уравнения

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$$

с целыми коэффициентами, то число

$$e^{\alpha_1} + e^{\alpha_2} + \dots + e^{\alpha_n}$$

не может быть целым.

Из этой теоремы трансцендентность числа π следует уже весьма просто. Предположим, что число π алгебраично. Тогда число πl также алгебраично. Пусть

$$\beta_1 = \pi l, \beta_2, \dots, \beta_m$$

— все числа, сопряженные с числом πl . Так как $e^{\pi l} = -1$, то произведение

$$(e^{\beta_1} + 1)(e^{\beta_2} + 1) \dots (e^{\beta_m} + 1)$$

равно нулю. Следовательно, раскрывая скобки, мы получим, что

$$0 = 1 + \sum_k e^{\beta_k} + \sum_{k, l} e^{\beta_k + \beta_l} + \dots + e^{\beta_1 + \beta_2 + \dots + \beta_m}.$$

Обозначая отличные от нуля показатели $\beta_k, \beta_k + \beta_l, \dots, \beta_1 + \dots + \beta_m$ через $\alpha_1, \alpha_2, \dots, \alpha_n$, мы можем переписать это равенство в следующем виде:

$$e^{\alpha_1} + e^{\alpha_2} + \dots + e^{\alpha_n} = B,$$

где B — некоторое целое число. Таким образом, для того чтобы прийти к противоречию с доказанной выше теоремой, достаточно показать, что все числа $\alpha_1, \alpha_2, \dots, \alpha_n$ являются корнями иекоторого многочлена с целыми коэффициентами, не имеющего никаких других корней, т. е. что любое число, сопряженное с одним из чисел $\alpha_1, \alpha_2, \dots, \alpha_n$ также содержится среди этих чисел. Но это почти очевидно. Действительно, пусть α — любое из чисел $\alpha_1, \dots, \alpha_n$. По условию оно является суммой k чисел вида β_1, \dots, β_m . Рассмотрим все числа $\gamma_1 = \alpha, \gamma_2, \dots, \gamma_s$, которые можно представить

в виде суммы k чисел вида β_1, \dots, β_m . Ясно, что многочлен

$$f(x) = (x - \gamma_1)(x - \gamma_2) \cdots (x - \gamma_s)$$

имеет рациональные коэффициенты (ибо эти коэффициенты являются симметрическими многочленами от чисел β_1, \dots, β_m). Поскольку среди корней многочлена $f(x)$ содержится число $\gamma_1 = a$, любое число, ему сопряженное, также должно быть корнем этого многочлена, т. е. должно быть суммой k чисел вида β_1, \dots, β_m , и потому оно должно совпадать с одним из чисел a_1, \dots, a_n .

Тем самым трансцендентность числа π полностью доказана.

Аналогичным методом может быть доказано следующее общее утверждение:

числа θ и $\sin \theta$ тогда и только тогда одновременно являются алгебраическими числами, когда $\theta = 0$.

Доказательство этого утверждения мы опустим.

Задача о луночках Гиппократа формулируется следующим образом: найти все луночки, т. е. фигуры, ограниченные двумя дугами окружностей, которые можно построить циркулем и линейкой и для которых можно построить (также циркулем и линейкой) равновеликий квадрат (такие луночки называются *квадрируемыми*). Каждая луночка задается длиной общей хорды, стягивающей дуги, ограничивающие луночку, и центральными углами 2α и 2β , измеряющими эти дуги (считаем для определенности, что $\alpha > \beta$). Мы будем рассматривать лишь луночки, для которых углы α и β *соизмеримы*, т. е. для которых существует такой угол θ , что $\alpha = m\theta$ и $\beta = n\theta$, где m и n взаимно простые целые (положительные) числа (причем $m > n$). В этом предположении построение луночки сводится к построению угла θ .

Рассмотрим некоторую квадрируемую луночку с углами α и β . Без ограничения общности мы можем считать, что длина общей хорды, стягивающей дуги, ограничивающие луночку, равна единице. Тогда нетрудно видеть, что площадь S луночки выражается формулой

$$S = \frac{\alpha}{\sin^2 \alpha} - \frac{\beta}{\sin^2 \beta} + \frac{\operatorname{ctg} \beta}{4} - \frac{\operatorname{ctg} \alpha}{4},$$

если дуги, ограничивающие луночку, расположены по одну сторону от хорды (вогнуто-выпуклая луночка), и формулой

$$S = \frac{\alpha}{\sin^2 \alpha} + \frac{\beta}{\sin^2 \beta} + \frac{\operatorname{ctg} \beta}{4} + \frac{\operatorname{ctg} \alpha}{4}, \quad (1)$$

в противном случае (выпуклая луночка). Рассмотрим сначала второй случай. Так как по условию $\alpha = m\theta$ и $\beta = n\theta$, то из формулы (1) вытекает, что

$$\theta = \frac{\left(s - \frac{\operatorname{ctg} n\theta}{4} - \frac{\operatorname{ctg} m\theta}{4}\right) \sin^2 m\theta \sin^2 n\theta}{m \sin^2 n\theta + n \sin^2 m\theta}.$$

Для квадрируемой луночки это число алгебраично. Таким образом, оба числа θ и $\sin \theta$ одновременно алгебраичны, что, как мы знаем, возможно лишь при $\theta = 0$. Следовательно, *квадрируемых выпуклых луночек не существует.*

Аналогичное рассуждение показывает, что *квадрируемая вогнуто-выпуклая луночка, определяемая углами $\alpha = m\theta$ и $\beta = n\theta$, может существовать лишь тогда, когда*

$$n \sin^2 m\theta - m \sin^2 n\theta = 0. \quad (2)$$

Таким образом,

задача построения квадрируемых луночек (с соизмеримыми углами α и β) сводится к задаче построения угла θ , удовлетворяющего уравнению (2).

Заменив в уравнении (2) величины $\sin m\theta$ и $\sin n\theta$ их выражениями через $\cos \theta$, мы получим для $\cos \theta$ некоторое алгебраическое уравнение, которое мы и должны исследовать. Луночка с углами $m\theta$ и $n\theta$ тогда и только тогда может быть построена циркулем и линейкой, когда это уравнение обладает действительным решением, абсолютная величина которого не превосходит единицы и вычисление которого сводится к решению цепи квадратных уравнений.

Впрочем, с вычислительной точки зрения удобнее рассматривать не число $\cos \theta$, а число $\xi = \cos 2\theta + i \sin 2\theta$. Это изменение, конечно, никакого принципиального значения не имеет (ибо число ξ может быть построено тогда и только тогда, когда может быть построено число $\cos \theta$). Поскольку

$$\sin k\theta = \frac{(\xi^k - 1)^2}{4\xi^k}, \quad k = m, n,$$

уравнение для величины ξ имеет вид

$$n(x^m - 1)^2 - mx^{m-n}(x^n - 1)^2 = 0, \quad (3)$$

Таким образом, мы пришли к следующей чисто алгебраической задаче:

при каких взаимно простых целых положительных числах t и n (удовлетворяющих условию $t > n$) решение уравнения (3) сводится к решению квадратных уравнений?

Найдя все уравнения (3), сводящиеся к квадратным уравнениям, мы затем уже легко отберем среди них уравнения, которым соответствуют «действительные» луночки, т. е. уравнения, обладающие корнем ξ , модуль которого равен единице.

Можно доказать, что

если число t составное, то, за исключением случая $t = 9$, $n = 1$, решение уравнения (3) нельзя свести к решению квадратных уравнений.

Доказательство этого утверждения выходит за рамки этой книги, и мы его опустим.

Пусть теперь число t простое. Оказывается, что

если решение уравнения (3) при простом $t = p$ сводится к решению квадратных уравнений, то число p либо равно двум, либо является простым числом Ферма.

Для доказательства мы произведем в уравнении (3) замену $x = y + 1$. В результате мы получим уравнение

$$n \left(\frac{(y+1)^p - 1}{y} \right)^2 = p(y+1)^{p-n} \left(\frac{(y+1)^n - 1}{n} \right)^2,$$

т. е. уравнение

$$n(y^{p-1} + C_p^1 y^{p-2} + C_p^2 y^{p-3} + \dots + C_p^{p-1})^2 - p(y+1)^{p-n}(y^{n-1} + C_n^1 y^{n-2} + \dots + C_n^{n-1})^2 = 0. \quad (4)$$

Раскрыв скобки, мы получим уравнение вида

$$ny^{2(p-1)} + a_1 y^{2p-3} + \dots + a_{2p-3} y + a_{2p-2} = 0,$$

где a_1, \dots, a_{2p-2} — некоторые целые числа.

Заметим теперь, что

если $k \neq 0$, p , то биноминальный коэффициент C_p^k делится на p .

Действительно,

$$C_p^k = \frac{p(p-1)\dots(p-k+1)}{1\cdot 2 \dots k},$$

и простое число p в числителе не может сократиться (ибо все множители знаменателя меньше p).

Отсюда вытекает, что уравнение (4) мы можем переписать в следующем виде:

$$n(y^{p-1} + pf_1(y))^2 + pf_2(y) = 0,$$

где $f_1(y)$ и $f_2(y)$ — некоторые многочлены с целыми коэффициентами, а следовательно, и в следующем виде:

$$ny^{2(p-1)} + pf(y) = 0, \quad (5)$$

где $f(y)$ — некоторый многочлен с целыми коэффициентами. Это означает, что в уравнении (5) все коэффициенты a_1, \dots, a_{2p-2} делятся на p . Поскольку старший коэффициент n на p не делится, а свободный член a_{2p-2} (равный, очевидно, $np^2 - pn = pn(p - p)$) не делится на p^2 , уравнение (5) удовлетворяет условиям критерия Эйзенштейна и потому неприводимо (над полем R). Следовательно, его решение может сводиться к решению квадратных уравнений только тогда, когда его степень $2(p - 1)$ является степенью двойки, т. е. когда число p либо равно двум, либо является простым числом Ферма. Теорема доказана.

Оказывается, что утверждаемое этой теоремой необходимое условие достаточным не является. Именно можно показать, что

если $p > 5$, то решение уравнения (3) (при $m = p$) нельзя свести к решению квадратных уравнений.

Доказательство этого утверждения мы также опустим.

Таким образом, нам остается разобрать лишь случаи $m = 2$, $m = 3$ и $m = 5$, а также случай $m = 9$ и $n = 1$.

Пусть $m = 2$. Тогда $n = 1$, и уравнение (3) (после сокращения на $(x - 1)^2$) приобретает вид

$$x^2 + 1 = 0.$$

Следовательно, в этом случае $2\theta = 90^\circ$, и мы получаем, что луночка с углами $2\alpha = 180^\circ$ и $2\beta = 90^\circ$ квадрируема. Это — известная луночка Гиппократа.

Пусть теперь $m = 3$. Тогда $n = 1$ или $n = 2$. В первом случае уравнение (3) (после сокращения на $(x - 1)^2$) имеет вид

$$(x^2 + x + 1)^2 - 3x^2 = 0.$$

Оно имеет два действительных корня (нам не интересных) и комплексные корни

$$\frac{\sqrt{3}-1}{2} \pm \sqrt{-\frac{\sqrt{3}}{2}}.$$

Следовательно, $\cos 2\theta = \frac{\sqrt{3}-1}{2}$, откуда $2\theta \approx 68^\circ, 5$. Таким образом,

луночка с углами $\arccos \frac{\sqrt{3}-1}{2} \approx 68^\circ, 5$ и $3 \arccos \frac{\sqrt{3}-1}{2} \approx 205^\circ, 6$ *квадрируема.*

При $n=2$ мы получаем уравнение

$$2(x^2 + x + 1)^2 - 3x(x+1)^2 = 0.$$

Полагая $x = y^2$, мы получим уравнение, разлагающееся в поле $R(\sqrt{2}, \sqrt{3})$ на два возвратных уравнения четвертой степени, и потому сводящееся к квадратным уравнениям.

Производя вычисления, мы получим, что $\cos 2\theta = \frac{\sqrt{33}-1}{8}$, т. е. что $2\theta \approx 53^\circ, 6$. Таким образом,

луночка с углами $2 \arccos \frac{\sqrt{33}-1}{8} \approx 107^\circ, 2$ и $3 \arccos \frac{\sqrt{33}-1}{8} \approx 160^\circ, 9$ *квадрируема.*

Эти две луночки также были построены Гиппократом.

Пусть, наконец, $m=5$. Тогда $n=1, 2, 3$ или 4 . При $n=1$ мы получаем уравнение

$$(x^4 + x^3 + x^2 + x + 1)^2 - 5x^4 = 0,$$

которое распадается на два возвратных уравнения четвертой степени

$$x^4 + x^3 + (1 \pm \sqrt{5})x^2 + x + 1 = 0$$

и потому сводится к квадратным уравнениям. В этом случае $\cos 2\theta = \frac{\sqrt{5+4\sqrt{5}}-1}{4}$, откуда $2\theta \approx 46^\circ, 9$. Таким образом,

луночка с углами $\arccos \frac{\sqrt{5+4\sqrt{5}}-1}{4} \approx 46^\circ, 9$ и

$5 \arccos \frac{\sqrt{5+4\sqrt{5}}-1}{4} \approx 234^\circ, 4$ *квадрируема,*

Эта луночка была найдена в 1840 г. Клаузеном.
При $n = 2$ мы получаем уравнение

$$2(x^4 + x^3 + x^2 + x + 1)^2 - 5x^3(x + 1)^2 = 0.$$

Полагая $x = y^2$, мы сведем это уравнение к двум возвратным уравнениям восьмой степени

$$y^8 + y^6 + y^4 + y^2 + 1 \pm \sqrt{\frac{5}{2}} y^3(y^2 + 1) = 0.$$

Решая эти уравнения известным методом (подстановкой $y + \frac{1}{y} = z$), мы получим уравнения четвертой степени

$$z^4 - 3z^2 \pm \sqrt{\frac{5}{2}} z + 1 = 0. \quad (6)$$

Решая последние уравнения методом Феррари (см. Курс, стр. 239), мы получим для вспомогательного неизвестного u (в Курсе это неизвестное обозначалось символом α) кубическое уравнение

$$16u^3 - 24u^2 + 20u - 5 = 0. \quad (7)$$

Так как это уравнение, как легко видеть, неприводимо (не имеет рациональных корней), то его решение нельзя свести к решению квадратных уравнений. Следовательно, исходное уравнение также нельзя свести к квадратным уравнениям (ибо корни уравнения (7) рационально выражаются через корни уравнения (6)). Таким образом,

при $m = 5$ и $n = 2$ квадрируемой луночки не существует.

При $n = 3$ мы получаем уравнение

$$3(x^4 + x^3 + x^2 + x + 1)^2 - 5x^2(x^2 + x + 1)^2 = 0.$$

Оно распадается (в поле $R(\sqrt{3}, \sqrt{5})$) на два возвратных уравнения четвертой степени, и потому его решение сводится к решению квадратных уравнений. Произведя вычисления, мы легко получим, что $\cos 2\theta = t$, где

$$t = \frac{\sqrt{\frac{5}{3}} - 1 + \sqrt{\frac{20}{3} + \sqrt{\frac{20}{3}}}}{4},$$

откуда $2\theta \approx 33^\circ,6$. Таким образом,

луночка с углами $3 \arccos t \approx 100^\circ, 8$ и $5 \arccos t \approx 168^\circ, 0$ квадрируема.

Эта луночка также была найдена Клаузеном.

При $n = 4$ мы получаем уравнение

$$4(x^4 + x^3 + x^2 + x + 1)^2 - 5x(x^3 + x^2 + x + 1)^2 = 0.$$

Так же, как в случае $n = 2$, легко показать, что решение этого уравнения нельзя свести к решению квадратных уравнений. Таким образом,

при $m = 5$ и $n = 4$ квадрируемой луночки не существует.

Рассмотрим, наконец, последний возможный случай: $m = 9$ и $n = 1$. В этом случае мы получаем приводимое уравнение

$$(x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)^2 - 9x^8 = 0,$$

распадающееся на два возвратных уравнения

$$\left. \begin{array}{l} x^8 + x^7 + x^6 + x^5 - 2x^4 + x^3 + x^2 + x + 1 = 0, \\ x^8 + x^7 + x^6 + x^5 + 4x^4 + x^3 + x^2 + x + 1 = 0. \end{array} \right\} \quad (8)$$

После замены $x + \frac{1}{x} = y$ мы получим уравнения четвертой степени

$$\begin{aligned} y^4 + y^3 - 3y^2 - 2y - 2 &= 0, \\ y^4 + y^3 - 3y^2 - 2y - 4 &= 0. \end{aligned}$$

Решение первого уравнения не сводится к решению квадратных уравнений, потому что кубическое уравнение, получаемое по методу Феррари, неприводимо. Что же касается второго уравнения, то в поле $R(i\sqrt{3})$ оно распадается на два квадратных уравнения

$$\left. \begin{array}{l} y^2 + \eta y - 2 = 0, \\ y^2 + \bar{\eta}y - 2 = 0, \end{array} \right\} \quad (9)$$

где $\eta = \frac{1+i\sqrt{3}}{2}$, и потому его решение сводится к решению квадратных уравнений. Таким образом,

при $m = 9$ и $n = 1$ решение уравнения (3) (точнее, одного из его неприводимых множителей восьмой степени) сводится к решению квадратных уравнений,

Попытаемся теперь найти соответствующую луночку. Легко видеть, что у уравнения (9) нет действительных корней. Следовательно, для любого интересующего нас корня ξ уравнения (3) (т. е. для любого корня второго из уравнений (8)) величина $\xi + \frac{1}{\xi}$ не действительна. Однако если бы этому корню соответствовала луночка с углом θ , то, поскольку $\xi = \cos 2\theta + i \sin 2\theta$, величина $\xi + \frac{1}{\xi} = 2 \cos 2\theta$ была бы действительной. Полученное противоречие показывает, что

при $m=9$ и $n=1$ квадрируемой луночки не существует.

Окончательный результат произведенного исследования можно сформулировать в виде следующей теоремы.

Квадрируемые луночки существуют лишь в следующих пяти случаях:

$$\begin{aligned} m &= 2, \quad m = 3, \quad m = 3, \quad m = 5, \quad m = 5 \\ n &= 1, \quad n = 1, \quad n = 2, \quad n = 1, \quad n = 3. \end{aligned}$$

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
«ФИЗМАТГИЗ»

Москва, В-71, Ленинский проспект, 15

ГОТОВЯТСЯ К ИЗДАНИЮ:

Бурбаки Н., Алгебра, выпуск 1, Алгебраическая структура линейной и полилинейной алгебры.

Гельфоид А. О. и Линник Ю. В., Элементарные методы в аналитической теории чисел.

Глушков В. М., Синтез цифровых автоматов.

Годунов С. К. и Рябенский В. С., Введение в теорию разностных схем.

Гутер Р. С. и Овчинский Б. В., Элементы численного анализа и математической обработки результатов опыта.

Проблемы кибернетики, выпуск 8, под редакцией А. А. Ляпунова.

Соминский И. С., Алгебра (дополнительный курс).

Хинчин А. Я., Работы по математической теории масштабного обслуживания.

Михаил Михайлович Постников

Теория Галуа

М., Физматгиз, 1963 г., 220 стр.

Редактор А. П. Баева

Технический редактор И. Ш. Аксельрод

Корректор О. А. Сигал

Сдано в набор 27/VI 1962 г. Подписано к
печати 1/II 1963 г. Бумага 84 × 108^{1/32}. Физ.
печ. л. 6,875. Условн. печ. л. 11,28.
Уч.-изд. л. 9,86. Тираж 11 500 экз. Т-10915.
Цена книги 64 коп. Заказ № 160.

Государственное издательство
физико-математической литературы.
Москва, В-71, Ленинский проспект, 15.

Ленинградский Совет народного хозяйства.
Управление целлюлозно-бумажной и полиграфической промышленности. Отпечатано
в типографии № 1 «Печатный Двор»
им. А. М. Горького. Ленинград, Гатчинская,
26 с матриц типографии № 2
им. Ев. Соколовой. Ленинград, Измайловский пр., 29.