

над $\mathbf{C}(t)$ и группа Галуа которого есть G . На языке накрытий это означает, что H принадлежит некоторому конечному накрытию поверхности $S - \{P_1, \dots, P_{n+1}\}$.

§ 3. Корни из единицы

Пусть k — поле. Под *корнем из единицы* (в k) мы будем понимать всякий элемент $\zeta \in k$, такой, что $\zeta^n = 1$ для некоторого $n \geq 1$. Если характеристика поля k равна p , то уравнение

$$X^{p^m} = 1$$

имеет только один корень, а именно 1, и, следовательно, нет никаких корней p^m -й степени из единицы, кроме 1.

Пусть n — целое число > 1 , взаимно простое с характеристикой поля k . Многочлен

$$X^n - 1$$

сепарабелен, поскольку его производная nX^{n-1} обращается в нуль лишь при $X = 0$ и, значит, не имеет с $X^n - 1$ общих корней. Следовательно, в \bar{k} многочлен $X^n - 1$ имеет n различных корней, являющихся корнями из единицы. Они, очевидно, образуют группу, а, как мы знаем, всякая конечная мультиплекативная группа в поле циклическая (гл. V, теорема 6). Таким образом, группа корней n -й степени из единицы циклическая. Образующие этой группы называются *примитивными*, или *первообразными*, корнями n -й степени из единицы.

Пусть U_n обозначает группу всех корней n -й степени из единицы в \bar{k} и m , n — взаимно простые целые числа; тогда

$$U_{mn} \approx U_m \times U_n.$$

Это следует из того, что U_m , U_n не могут иметь общих элементов, кроме 1, и, значит, $U_m U_n$ содержит ровно mn элементов, каждый из которых есть корень mn -й степени из единицы. Следовательно, $U_m U_n = U_{mn}$ (откуда и получается разложение в прямое произведение).

Теорема 6. Для всякого примитивного корня n -й степени из единицы ζ

$$[\mathbf{Q}(\zeta) : \mathbf{Q}] = \varphi(n).$$

Доказательство. Пусть $f(X)$ — неприводимый многочлен элемента ζ над \mathbf{Q} . Тогда $f(X)$ делит многочлен $X^n - 1$, скажем $X^n - 1 = f(X)h(X)$, где f , h оба имеют старший коэффициент 1. В силу леммы Гаусса f , h имеют целые коэффициенты. Ниже мы покажем, что если p — простое число, не делящее n , то ζ^p также будет корнем многочлена f . Поскольку ζ^p — тоже примитивный корень n -й степени из единицы и поскольку любой примитивный ко-

рень n -й степени из единицы может быть получен последовательным возведением ζ в простые степени с показателями, не делящими n , то отсюда будет следовать, что все примитивные корни n -й степени из единицы являются корнями многочлена f , который поэтому имеет степень $\geq \varphi(n)$, и, значит, его степень равна точно $\varphi(n)$.

Предположим, что ζ^p не является корнем f . Тогда ζ^p — корень многочлена h , а сам ζ — корень $h(X^p)$. Следовательно, $f(X)$ делит $h(X^p)$, и мы можем написать

$$h(X^p) = f(X)g(X).$$

Так как f имеет целые коэффициенты и старший коэффициент 1, то и g имеет целые коэффициенты. Поскольку $a^p \equiv a \pmod{p}$ для любого целого числа a , то заключаем, что

$$h(X^p) \equiv h(X)^p \pmod{p}$$

и, следовательно,

$$h(X)^p \equiv f(X)g(X) \pmod{p}.$$

В частности, обозначив через \bar{f} и \bar{h} многочлены над $\mathbb{Z}/p\mathbb{Z}$, получающиеся соответственно из f и h при редукции по модулю p , мы видим, что \bar{f} и \bar{h} не являются взаимно простыми, т. е. имеют общий множитель. Но $X^n - 1 = \bar{f}(X)\bar{h}(X)$ и, следовательно, $X^n - 1$ имеет кратные корни. Но это, как сразу видно из рассмотрения производной, невозможно, и наша теорема доказана.

Следствие. Если n, m — взаимно простые целые числа ≥ 1 , то

$$\mathbf{Q}(\zeta_n) \cap \mathbf{Q}(\zeta_m) = \mathbf{Q}.$$

Доказательство. Заметим, что ζ_n и ζ_m содержатся оба в $\mathbf{Q}(\zeta_{mn})$, поскольку ζ_{mn}^n — примитивный корень m -й степени из единицы. Кроме того, $\zeta_m\zeta_n$ — примитивный корень степени mn из единицы. Следовательно,

$$\mathbf{Q}(\zeta_n)\mathbf{Q}(\zeta_m) = \mathbf{Q}(\zeta_{mn}).$$

Наше утверждение вытекает из мультипликативности $\varphi(mn) = \varphi(m)\varphi(n)$.

Предположим, что $n = p$ — простое число (не имеющее ничего общего с характеристикой). Тогда

$$X^p - 1 = (X - 1)(X^{p-1} + \dots + 1).$$

Любой примитивный корень p -й степени из единицы является корнем второго множителя в правой части этого равенства. Так как

имеется ровно $p - 1$ примитивных корней p -й степени из единицы, то мы заключаем, что ими исчерпываются все корни многочлена

$$X^{p-1} + \dots + 1.$$

Мы видели в гл. V, что этот многочлен может быть преобразован в многочлен Эйзенштейна над полем рациональных чисел. Это дает другое доказательство того факта, что $[\mathbf{Q}(\zeta_p) : \mathbf{Q}] = p - 1$.

Пусть k — произвольное поле, n — целое число, взаимно простое с его характеристикой, $\zeta = \zeta_n$ — примитивный корень n -й степени из единицы в k и σ — вложение $k(\zeta)$ в \bar{k} над k . Тогда

$$(\sigma\zeta)^n = \sigma(\zeta^n) = 1,$$

так что $\sigma\zeta$ также есть корень n -й степени из единицы. Следовательно, $\sigma\zeta = \zeta^i$ для некоторого целого $i = i(\sigma)$, однозначно определенного по модулю n . Значит, σ отображает $k(\zeta)$ в себя и, таким образом, $k(\zeta)$ нормально над k . Если τ — другой автоморфизм поля $k(\zeta)$ над k , то

$$\sigma\tau\zeta = \zeta^{i(\sigma)i(\tau)}.$$

Так как σ и τ — автоморфизмы, то $i(\sigma)$ и $i(\tau)$ взаимно прости с n (иначе $\sigma\zeta$ имел бы период, меньший n). Таким образом, мы получаем гомоморфизм группы Галуа G поля $k(\zeta)$ над k в мультиликативную группу $(\mathbf{Z}/n\mathbf{Z})^*$ целых чисел по модулю n , взаимно простых с n . Этот гомоморфизм, очевидно, инъективен, поскольку $i(\sigma)$ однозначно определяется по модулю n автоморфизмом σ , а действие σ на $k(\zeta)$ определяется действием этого автоморфизма на ζ . Мы заключаем, что $k(\zeta)$ абелово над k .

Пусть φ — функция Эйлера. Как мы знаем, порядок группы $(\mathbf{Z}/n\mathbf{Z})^*$ равен $\varphi(n)$. Следовательно, степень $[k(\zeta) : k]$ делит $\varphi(n)$.

Исследуем более подробно разложение на множители многочлена $X^n - 1$; для простоты предположим, что характеристика равна 0.

Имеем

$$X^n - 1 = \prod_{\omega} (X - \omega),$$

где произведение берется по всем корням n -й степени из единицы. Соберем вместе все члены, соответствующие тем корням из единицы, которые имеют одинаковый период. Пусть

$$f_d(X) = \prod_{\text{период } \omega=d} (X - \omega).$$

Тогда

$$X^n - 1 = \prod_{d|n} f_d(X).$$

Мы видим, что $f_1(X) = X - 1$ и что

$$f_n(X) = \frac{X^n - 1}{\prod_{\substack{d|n \\ d < n}} f_d(X)}.$$

Следовательно, мы можем вычислять $f_n(X)$ рекуррентно, и видно, что $f_n(X)$ является многочленом из $\mathbf{Q}[X]$, поскольку мы последовательно делим друг на друга многочлены, имеющие коэффициенты в \mathbf{Q} . У всех наших многочленов старший коэффициент равен 1, так что в действительности $f_n(X)$ имеет целочисленные коэффициенты в силу теоремы 2 из гл. V, § 4. Таким образом, наша конструкция по существу универсальна и годна для любого поля (характеристика которого не делит n).

Мы называем $f_n(X)$ *n-м круговым многочленом*, или многочленом деления круга на n равных частей.

Корнями f_n являются в точности примитивные корни n -й степени из единицы, и, следовательно,

$$\deg f_n = \varphi(n).$$

В силу теоремы 6 мы заключаем, что f_n неприводим над \mathbf{Q} и, значит,

$$f_n(X) = \text{Irr}(\zeta_n, \mathbf{Q}, X).$$

Доказательства следующих рекуррентных формул мы предоставляем читателю в качестве упражнений

1. Если p — простое число, то

$$f_p(X) = X^{p-1} + X^{p-2} + \dots + 1$$

и для любого целого $r \geq 1$

$$f_{p^r}(X) = f_p(X^{p^{r-1}}).$$

2. Пусть $n = p_1^{r_1} \cdots p_s^{r_s}$ — положительное целое число, разложенное на простые множители. Тогда

$$f_n(X) = f_{p_1 \cdots p_s} \left(X^{p_1^{r_1}-1} \cdots p_s^{r_s-1} \right).$$

3. Если n нечетно, то $f_{2n}(X) = f_n(-X)$.

4. Если p — простое число, не делящее n , то

$$f_{pn}(X) = \frac{f_n(X^p)}{f_n(X)}$$

5. Имеем

$$f_n(X) = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)}.$$

Как обычно, μ — это функция Мёбиуса:

$$\mu(n) = \begin{cases} 0, & \text{если } n \text{ делится на } p^2 \text{ для некоторого простого } p; \\ (-1)^r, & \text{если } n = p_1 \dots p_r \text{ — произведение различных простых чисел;} \\ 1, & \text{если } n = 1. \end{cases}$$

В качестве упражнения покажите, что

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{при } n = 1, \\ 0 & \text{при } n > 1. \end{cases}$$

Если ζ — корень n -й степени из единицы и $\zeta \neq 1$, то

$$\frac{1 - \zeta^n}{1 - \zeta} = 1 + \zeta + \dots + \zeta^{n-1} = 0.$$

Это замечание тривиально, но полезно.

Пусть \mathbf{F}_q — конечное поле из q элементов, где q есть некоторая степень простого числа $p \neq 2$. Тогда \mathbf{F}_q^* содержит $q - 1$ элементов и является циклической группой. Следовательно, индекс

$$(\mathbf{F}_q^* : \mathbf{F}_q^{*2}) = 2.$$

Для целого числа $v \not\equiv 0 \pmod{p}$ положим

$$\left(\frac{v}{p} \right) = \begin{cases} 1, & \text{если } v \equiv x^2 \pmod{p}, \\ -1, & \text{если } v \not\equiv x^2 \pmod{p}. \end{cases}$$

Эта функция, известная под названием *квадратичного символа* (или *символа Лежандра*), зависит только от класса вычетов $v \pmod{p}$.

Из нашего предыдущего замечания мы видим, что имеется ровно столько же квадратичных вычетов, сколько и невычетов по модулю p .

Пусть ζ — примитивный корень p -й степени из единицы и

$$S = \sum_v \left(\frac{v}{p} \right) \zeta^v,$$

где сумма берется по всем ненулевым классам вычетов по модулю p . Тогда

$$S^2 = \left(\frac{-1}{p} \right) p.$$

Всякое квадратичное расширение поля \mathbf{Q} содержится в некотором расширении, получающемся присоединением к \mathbf{Q} корня из единицы.

Доказательство. Последнее утверждение следует непосредственно из явного выражения $\pm p$ как квадрата в $\mathbf{Q}(\zeta)$, поскольку квадратный корень из любого целого числа содержится в поле, порожденном присоединением квадратных корней из простых множи-

телей, входящих в его разложение, а также $\sqrt{-1}$. Кроме того, для простого числа 2 имеет место соотношение $(1+i)^2=2i$. Докажем утверждение, касающееся S^2 . Имеем

$$S^2 = \sum_{v, \mu} \left(\frac{v}{p}\right) \left(\frac{\mu}{p}\right) \zeta^{v+\mu} = \sum_{v, \mu} \left(\frac{v\mu}{p}\right) \zeta^{v+\mu}.$$

Когда v пробегает все ненулевые классы вычетов, то же самое происходит с $v\mu$ при любом фиксированном μ и, следовательно, замена v на $v\mu$ дает

$$\begin{aligned} S^2 &= \sum_{v, \mu} \left(\frac{v\mu^2}{p}\right) \zeta^{\mu(v+1)} = \sum_{v, \mu} \left(\frac{v}{p}\right) \zeta^{\mu(v+1)} = \\ &= \sum_{\mu} \left(\frac{-1}{p}\right) \zeta^0 + \sum_{v \neq -1} \left(\frac{v}{p}\right) \sum_{\mu} \zeta^{\mu(v+1)}. \end{aligned}$$

Но $1 + \zeta + \dots + \zeta^{p-1} = 0$, так что сумма по μ , стоящая справа, равна -1 . Следовательно,

$$S^2 = \left(\frac{-1}{p}\right)(p-1) + (-1) \sum_{v \neq -1} \left(\frac{v}{p}\right) = p \left(\frac{-1}{p}\right) - \sum_v \left(\frac{v}{p}\right) = p \left(\frac{-1}{p}\right),$$

что и требовалось установить.

Мы видим, что $\mathbf{Q}(\sqrt{p})$ содержится в $\mathbf{Q}(\zeta, \sqrt{-1})$ или $\mathbf{Q}(\zeta)$ в зависимости от знака квадратичного символа для -1 . Расширение поля называется *круговым*, если оно содержится в поле, полученном присоединением корней из единицы. Выше мы показали, что квадратичные расширения поля \mathbf{Q} являются круговыми. Теорема Кронекера утверждает, что всякое абелево расширение поля \mathbf{Q} является круговым, но ее доказательство требует техники, которая не может быть изложена в этой книге.

§ 4. Линейная независимость характеров

Пусть G — моноид и K — поле. Под *характером* G в K мы (в этой главе) будем понимать гомоморфизм

$$\chi: G \rightarrow K^*$$

монида G в мультиликативную группу поля K . *Тривиальный* характер — это гомоморфизм, принимающий постоянное значение 1. Функции $f_i: G \rightarrow K$ называются *линейно независимыми* над K , если из любого соотношения вида

$$a_1 f_1 + \dots + a_n f_n = 0$$

с $a_i \in K$ следует, что все $a_i = 0$.