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

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

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

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

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

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

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

$$\chi\colon\ G\to K^*$$

моноида G в мультипликативную группу поля K. *Тривиальный* характер — это гомоморфизм, принимающий постоянное значение 1. Функции $f_i\colon G\to K$ называются *линейно независимыми* над K, если из любого соотношения вида

$$a_1f_1+\ldots+a_nf_n=0$$

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

Теорема 7 (Артин) *Пусть* $\chi_1, \ldots, \chi_n$ — *различные характеры* G *в* K *Тогда они линейно независимы над* K

Доказательство Один характер, очевидно, линейно независим. Предположим, что имеется соотношение

$$a_1\chi_1 + \ldots + a_n\chi_n = 0,$$

где коэффициенты $a_i \in K$ не все равны 0 Возьмем такое соотношение с наименьшим возможным n. Тогда $n \geqslant 2$ и ни один a_i не равен 0 Так как χ_1, χ_2 различны, то существует элемент $z \in G$, такой, что $\chi_1(z) \neq \chi_2(z)$. Для всех $x \in G$ имеем

$$a_1\chi_1(xz) + \ldots + a_n\chi_n(xz) = 0,$$

и так как χ_i — характеры, то

$$a_1\chi_1(z)\chi_1 + \ldots + a_n\chi_n(z)\chi_n = 0$$

Разделим на $\chi_1(z)$ и вычтем из нашего первого соотношения Член $a_1\chi_1$ сократится, и мы получим соотношение

$$\left(a_2 - a_2\frac{\chi_2(z)}{\chi_1(z)}\right)\chi_2 + \ldots = 0$$

Первый коэффициент в этом соотношении отличен от 0, и оно имеет меньшую длину, чем первоначальное соотношение — противоречие.

В качестве приложения теоремы Артина можно рассмотреть случай, когда K — конечное нормальное расширение поля k, а характеры — различные автоморфизмы $\sigma_1, \ldots, \sigma_n$ поля K над k, рассматриваемые как гомоморфизмы группы K^* в K^*. Этот частный случай был исследован уже Дедекиндом, который, однако, сформулировал теорему несколько иным образом, рассматривая определитель, составленный из $\sigma_i\omega_j$, где $\{\omega_j\}$ — подходящее множество элементов из K, и доказывая более сложным путем тот факт, что этот определитель отличен от 0 Формулировка, данная выше, и весьма элегантное доказательство теоремы принадлежат Артину

В качестве другого приложения имеем

Следствие. *Пусть* $\alpha_1, \ldots, \alpha_n$ — *различные ненулевые элементы поля* K *Если* $a_1, \ldots, a_n$ — *элементы из* K, *такие, что для всех целых* ν

$$a_1\alpha_1^\nu + \ldots + a_n\alpha_n^\nu = 0,$$

то $a_i = 0$ *для всех* i

Доказательство Применяем теорему к различным гомоморфизмам

$$\nu \longmapsto \alpha_i^\nu$$

группы $\mathbf{Z}$ в K^*.

Другое интересное приложение будет дано в упражнениях (относительные инварианты).