содержащим E. Если $\sigma_1, \ldots, \sigma_n$ — все различные вложения E в $\overline{E}$, то расширение

$$K = (\sigma_1 E)(\sigma_2 E) \ldots (\sigma_n E),$$

композит всех этих вложений, является нормальным расширением k. Действительно, любое его вложение, скажем τ, мы можем применить к каждому расширению $\sigma_i E$; тогда $(\tau\sigma_1, \ldots, \tau\sigma_n)$ будет перестановкой совокупности $(\sigma_1, \ldots, \sigma_n)$ и, следовательно, τ отображает K в себя. Всякое нормальное расширение поля k, содержащее E, должно содержать $\sigma_i E$ для каждого i, и, таким образом, *наименьшее нормальное расширение поля k, содержащее E, в точности равно композиту*

$$(\sigma_1 E) \ldots (\sigma_n E).$$

Если E сепарабельно над k, то из теоремы 9 с помощью индукции заключаем, что наименьшее нормальное расширение поля k, содержащее E, также сепарабельно над k.

Аналогичные результаты будут справедливы и для бесконечного алгебраического расширения E поля k, если взять бесконечный композит. Что касается терминологии, то если E — алгебраическое расширение поля k и σ — произвольное вложение E в $\overline{k}$ над k, то мы называем поле σE сопряженным с E в $\overline{k}$. Мы можем сказать, что *наименьшее нормальное расширение поля k, содержащее E, есть композит всех сопряженных с E подполей в $\overline{E}$.*

Пусть α — алгебраический элемент над k. Если $\sigma_1, \ldots, \sigma_n$ — различные вложения поля $k(\alpha)$ в $\overline{k}$ над k, то мы называем элементы $\sigma_1\alpha, \ldots, \sigma_r\alpha$ *сопряженными* с α в $\overline{k}$. Этими элементами являются попросту различные корни неприводимого многочлена над k, соответствующего элементу α. Наименьшее нормальное расширение поля k, содержащее один из этих сопряженных элементов, совпадает с $k(\sigma_1\alpha, \ldots, \sigma_r\alpha)$.

§ 5. Конечные поля

Мы получили достаточно общих теорем для того, чтобы описать строение конечных полей. Это интересно само по себе, а также дает примеры к общей теории.

Пусть F — конечное поле из q элементов. Как мы уже отмечали раньше, имеется гомоморфизм

$$\mathbf{Z} \to F,$$

переводящий 1 в 1, ядро которого не может быть 0, и, следовательно, является главным идеалом, порожденным простым числом p, по-

скольку $\mathbf{Z}/p\mathbf{Z}$ вкладывается в F, а F не имеет делителей 0. Таким образом, F имеет характеристику p и содержит поле, изоморфное $\mathbf{Z}/p\mathbf{Z}$.

Заметим, что поле $\mathbf{Z}/p\mathbf{Z}$ не имеет других автоморфизмов, кроме тождественного. Действительно, любой автоморфизм должен отображать 1 в 1 и, следовательно, оставляет каждый элемент на месте, так как 1 аддитивно порождает $\mathbf{Z}/p\mathbf{Z}$. Будем отождествлять $\mathbf{Z}/p\mathbf{Z}$ с его образом в F. Тогда F есть векторное пространство над $\mathbf{Z}/p\mathbf{Z}$, причем это векторное пространство должно быть конечномерным, поскольку F конечно. Пусть его размерность будет n, и пусть $\omega_1, \ldots, \omega_n$ — базис для F над $\mathbf{Z}/p\mathbf{Z}$. Всякий элемент из F имеет единственное представление в виде

$$a_1\omega_1 + \ldots + a_n\omega_n,$$

где $a_i \in \mathbf{Z}/p\mathbf{Z}$. Следовательно, $q = p^n$.

Мультипликативная группа F^* поля F имеет порядок $q - 1$. Всякий элемент $\alpha \in F^*$ удовлетворяет уравнению $X^{q-1} = 1$. Следовательно, всякий элемент из F удовлетворяет уравнению

$$f(X) = X^q - X = 0.$$

Это означает, что многочлен $f(X)$ имеет q различных корней в F, а именно все элементы из F. Следовательно, f разлагается в F на множители степени 1, а именно

$$X^q - X = \prod_{\alpha \in F} (X - \alpha).$$

В частности, F есть поле разложения для f. Но поле разложения однозначно определено с точностью до изоморфизма. Следовательно, если конечное поле порядка p^n существует, то оно однозначно определено с точностью до изоморфизма как поле разложения многочлена $X^{p^n} - X$ над $\mathbf{Z}/p\mathbf{Z}$.

Для краткости будем обозначать $\mathbf{Z}/p\mathbf{Z}$ также через $\mathbf{F}_p$. Пусть n — целое число $\geqslant 1$. Рассмотрим поле разложения многочлена

$$X^{p^n} - X = f(X)$$

в алгебраическом замыкании $\bar{\mathbf{F}}_p$. Мы утверждаем, что это поле разложения совпадает с множеством корней многочлена $f(X)$ в $\bar{\mathbf{F}}_p$. Действительно, пусть α, β — корни. Тогда

$$(\alpha + \beta)^{p^n} - (\alpha + \beta) = \alpha^{p^n} + \beta^{p^n} - \alpha - \beta = 0,$$

откуда $\alpha + \beta$ — корень. Точно так же

$$(\alpha\beta)^{p^n} - \alpha\beta = \alpha^{p^n}\beta^{p^n} - \alpha\beta = \alpha\beta - \alpha\beta = 0$$

и, значит, $\alpha\beta$ — корень. Отметим, что 0, 1 — корни $f(X)$. Если $\beta \neq 0$, то

$$(\beta^{-1})^{p^n} - \beta^{-1} = (\beta^{p^n})^{-1} - \beta^{-1} = 0,$$

так что β^{-1} — корень. Наконец,

$$(-\beta)^{p^n} - (-\beta) = (-1)^{p^n}\beta^{p^n} + \beta.$$

Если p нечетно, то $(-1)^{p^n} = -1$, и мы видим, что $-\beta$ — корень. Если p четно, то $-1 = 1$ (в $\mathbf{Z}/2\mathbf{Z}$) и, следовательно, $-\beta = \beta$ — корень. Это доказывает наше утверждение.

Производная многочлена $f(X)$ равна

$$f'(X) = p^n X^{p^n-1} - 1 = -1.$$

Следовательно, у $f(X)$ нет кратных корней, и, значит, он имеет p^n различных корней в $\mathbf{F}_p$. Таким образом, его поле разложения содержит ровно p^n элементов. Суммируем наши результаты.

Теорема 10. *Для всякого простого числа p и всякого целого числа $n \geqslant 1$ существует поле порядка p^n, обозначаемое символом $\mathbf{F}_{p^n}$, однозначно определенное как подполе в алгебраическом замыкании $\overline{\mathbf{F}}_p$. Это поле разложения многочлена*

$$X^{p^n} - X,$$

и его элементы — корни этого многочлена. Всякое конечное поле изоморфно одному и только одному из полей $\mathbf{F}_{p^n}$.

Мы обычно полагаем $p^n = q$ и пишем $\mathbf{F}_q$ вместо $\mathbf{F}_{p^n}$.

Следствие. *Пусть $\mathbf{F}_q$ — конечное поле и m — целое число $\geqslant 1$. В данном алгебраическом замыкании $\overline{\mathbf{F}}_q$ существует одно и только одно расширение поля $\mathbf{F}_q$ степени m, и этим расширением является поле $\mathbf{F}_{q^m}$.*

Доказательство. Пусть $q = p^n$. Тогда $q^m = p^{mn}$. Поле разложения многочлена $X^{q^m} - X$ есть в точности $\mathbf{F}_{p^{mn}}$ и имеет степень mn над $\mathbf{Z}/p\mathbf{Z}$. Так как $\mathbf{F}_q$ имеет степень n над $\mathbf{Z}/p\mathbf{Z}$, то F_{q^n} имеет степень m над $\mathbf{F}_q$. Обратно, любое расширение степени m над $\mathbf{F}_q$ имеет степень mn над $\mathbf{F}_p$ и, следовательно, должно совпадать с $F_{p^{mn}}$. Это доказывает наше следствие.

Теорема 11. *Мультипликативная группа конечного поля — циклическая.*

Доказательство. Это уже было доказано в гл. V, § 4, теорема 6.

Опишем все автоморфизмы конечного поля.

Пусть $q = p^n$ и $\mathbf{F}_q$ — конечное поле из q элементов. Рассмотрим отображение Фробениуса

$$\varphi\colon \mathbf{F}_q \to \mathbf{F}_q,$$

такое, что $\varphi(x) = x^p$. Очевидно, φ — гомоморфизм и его ядро равно 0, поскольку $\mathbf{F}_q$ — поле. Следовательно, φ инъективно. Так как F_q конечно, то отсюда вытекает, что φ сюръективно и что, следовательно, φ — изоморфизм. Отметим, что он оставляет $\mathbf{F}_p$ неподвижным.

Теорема 12. *Группа автоморфизмов поля $\mathbf{F}_q$ является циклической группой порядка n с образующей φ.*

Доказательство. Пусть G — группа, порожденная φ. Заметим, что $\varphi^n = \mathrm{id}$, поскольку $\varphi^n(x) = x^{p^n} = x$ для всех $x \in \mathbf{F}_q$. Следовательно, n — показатель для φ. Пусть d — период φ, так что $d \geqslant 1$. Имеем $\varphi^d(x) = x^{p^d}$ для всех $x \in \mathbf{F}_q$. Следовательно, всякий элемент $x \in \mathbf{F}_q$ является корнем уравнения

$$X^{p^d} - X = 0.$$

Это уравнение имеет самое большее p^d корней. Следовательно, $d \geqslant n$, откуда $d = n$.

Остается доказать, что G совпадает с группой всех автоморфизмов поля $\mathbf{F}_q$. Любой автоморфизм поля $\mathbf{F}_q$ должен оставлять $\mathbf{F}_p$ на месте, т. е. являться автоморфизмом $\mathbf{F}_q$ над $\mathbf{F}_p$. В силу теоремы 6 из § 4 число таких автоморфизмов $\leqslant n$. Следовательно, $\mathbf{F}_q$ не может иметь никаких других автоморфизмов, кроме тех, что содержатся в G.

Теорема 13. *Пусть m, n — целые числа $\geqslant 1$. Поле $\mathbf{F}_{p^n}$ содержится в $\mathbf{F}_{p^m}$ тогда и только тогда, когда m делится на n. Если это так, то положим $q = p^n$ и $m = nd$. Тогда $\mathbf{F}_{p^m}$ нормально и сепарабельно над $\mathbf{F}_q$ и группа автоморфизмов поля $\mathbf{F}_{p^m}$ над $\mathbf{F}_q$ есть циклическая группа, порожденная отображением φ^n.*

Доказательство. Все утверждения теоремы являются тривиальными следствиями уже доказанного выше, и их проверка предоставляется читателю.

§ 6. Примитивные элементы

Теорема 14. *Пусть E — конечное расширение поля k. Элемент $\alpha \in E$, для которого $E = k(\alpha)$, существует тогда и только тогда, когда имеется лишь конечное число промежуточных по-*