§ 6. Циклические расширения

Напомним, что конечное расширение называется циклическим, если оно является расширением Галуа и его группа Галуа циклическая.

Теорема 90 Гильберта. *Пусть K/k — циклическое расширение с группой Галуа G. Пусть σ — образующая группы G и $\beta \in K$. Норма $N_k^K(\beta) = N(\beta)$ равна 1 в том и только в том случае, когда существует элемент $\alpha \neq 0$ в K, такой, что $\beta = \alpha/\sigma\alpha$.*

Доказательство. Предположим, что такой элемент α существует. Беря норму от β, получаем $N(\alpha)/N(\sigma\alpha)$. Но норма — это произведение по всем автоморфизмам из G. Применение σ лишь переставляет эти автоморфизмы. Следовательно, норма равна 1.

Будет удобно использовать экспоненциальные обозначения. Если $\tau, \tau' \in G$ и $\xi \in K$, то пишем

$$\xi^{\tau+\tau'} = \xi^{\tau}\xi^{\tau'}.$$

В силу теоремы Артина о характерах отображение

$$\mathrm{id} + \beta\sigma + \beta^{1+\sigma}\sigma^2 + \ldots + \beta^{1+\sigma+\ldots+\sigma^{n-2}}\sigma^{n-1}$$

не равно тождественно нулю. Следовательно, существует $\theta \in K$, для которого элемент

$$\alpha = \theta + \beta\theta^{\sigma} + \beta^{1+\sigma}\theta^{\sigma^2} + \ldots + \beta^{1+\sigma+\ldots+\sigma^{n-2}}\theta^{\sigma^{n-1}}$$

не равен нулю. Если воспользоваться тем фактом, что $N(\beta) = 1$ и что, следовательно, при применении σ к последнему члену суммы мы получим $\beta^{-1}\theta$, то становится очевидным, что $\beta\alpha^{\sigma} = \alpha$. Чтобы завершить доказательство, разделим на α^{σ}.

Теорема 10. *Пусть k — поле, n — целое число > 0, взаимно простое с характеристикой поля k, причем в k имеется примитивный корень n-й степени из единицы.*

(а) *Если K — циклическое расширение степени n, то существует элемент $\alpha \in K$, такой, что $K = k(\alpha)$ и α удовлетворяет уравнению $X^n - a = 0$ для некоторого $a \in k$.*

(б) *Обратно, пусть $a \in k$ и α — некоторый корень многочлена $X^n - a$. Тогда $k(\alpha)$ — циклическое расширение над k степени d, $d \mid n$ и α^d — элемент из k.*

Доказательство. Пусть ζ — примитивный корень n-й степени из единицы в k, K/k — циклическое расширение с группой G и σ — образующая G. Имеем $N(\zeta^{-1}) = (\zeta^{-1})^n = 1$. В силу теоремы 90 Гильберта существует элемент $\alpha \in K$, такой, что $\sigma\alpha = \zeta\alpha$. Поскольку

ζ лежит в k, то $\sigma^i\alpha = \zeta^i\alpha$ для $i = 1, \ldots, n$. Следовательно, элементы $\zeta^i\alpha$ составляют n различных сопряженных с α над k, откуда вытекает, что $[k(\alpha) : k]$ не меньше, чем n. Так как $[K : k] = n$, то $K = k(\alpha)$. Кроме того,

$$\sigma(\alpha^n) = \sigma(\alpha)^n = (\zeta\alpha)^n = \alpha^n.$$

Неподвижный относительно σ элемент α^n будет неподвижен относительно всякой степени σ и, следовательно, неподвижен относительно G. Поэтому α^n лежит в k и мы полагаем $a = \alpha^n$. Это доказывает первую часть теоремы.

Обратно, пусть $a \in k$ и α — корень многочлена $X^n - a$. Тогда $\zeta^i\alpha$ для всякого $i = 1, \ldots, n$ также является корнем этого многочлена и, следовательно, все его корни лежат в поле $k(\alpha)$, которое тем самым нормально над k. При этом все корни различны, так что $k(\alpha)$ является расширением Галуа над k. Пусть G — его группа Галуа.

Если σ — автоморфизм расширения $k(\alpha)/k$, то $\sigma\alpha$ также будет корнем многочлена $X^n - a$. Следовательно, $\sigma\alpha = \omega_\sigma\alpha$, где ω_σ — некоторый корень n-й степени из единицы, не обязательно примитивный. Отображение $\sigma \mapsto \omega_\sigma$ является, очевидно, гомоморфизмом G в группу корней n-й степени из единицы, причем инъективным. Так как всякая подгруппа циклической группы циклическая, то мы заключаем, что G — циклическая группа, скажем, порядка d и $d \mid n$. Образ G есть циклическая группа порядка d. Если σ — образующая G, то ω_σ — примитивный корень d-й степени из единицы. Далее получаем

$$\sigma(\alpha^d) = (\sigma\alpha)^d = (\omega_\sigma\alpha)^d = \alpha^d.$$

Следовательно, элемент α^d неподвижен относительно G. Это элемент из k, и наша теорема доказана.

Теперь мы переходим к аналогу теоремы 90 Гильберта в характеристике p для циклического расширения степени p.

Теорема 90 Гильберта (аддитивная форма). *Пусть k — поле, K/k — циклическое расширение степени n с группой G и σ — образующая G. Пусть $\beta \in K$. След $\mathrm{Tr}_k^K(\beta)$ равен 0 в том и только в том случае, когда существует элемент $\alpha \in K$, такой, что $\beta = \alpha - \sigma\alpha$.*

Доказательство. Если такой элемент α существует, то след будет 0, поскольку след равен сумме, взятой по всем элементам G, а применение σ лишь переставляют эти элементы.

Обратно, предположим, что $\mathrm{Tr}(\beta) = 0$. Существует элемент $\theta \in K$, для которого $\mathrm{Tr}(\theta) \neq 0$. Положим

$$\alpha = \frac{1}{\mathrm{Tr}(\theta)}\left[\beta\theta^\sigma + (\beta + \sigma\beta)\theta^{\sigma^2} + \ldots + (\beta + \sigma\beta + \ldots + \sigma^{n-2}\beta)\theta^{\sigma^{n-1}}\right].$$

Отсюда сразу вытекает, что $\beta = \alpha - \sigma\alpha$.

Теорема 11 (Артин — Шрейер). *Пусть k — поле характеристики p.*

(а) *Если K — циклическое расширение над k степени p, то существует элемент $\alpha \in K$, такой, что $K = k(\alpha)$, причем α удовлетворяет уравнению $X^p - X - a = 0$ для некоторого $a \in k$.*

(б) *Обратно, для данного элемента $a \in k$ многочлен $f(X) = X^p - X - a$ либо имеет корень в k, и тогда все его корни лежат в k, либо неприводим. В последнем случае, если α — некоторый его корень, то $k(\alpha)$ — циклическое расширение степени p над k.*

Доказательство. Пусть K/k — циклическое расширение степени p. Тогда $\mathrm{Tr}_k^K(-1) = 0$ (это просто результат сложения -1 с собой p раз). Пусть σ — образующая группы Галуа. В силу аддитивной формы теоремы 90 Гильберта имеется элемент $\alpha \in K$, для которого $\sigma\alpha - \alpha = 1$, или, что то же самое, $\sigma\alpha = \alpha + 1$. Следовательно, $\sigma^i\alpha = \alpha + i$ для всех целых чисел $i = 1, \ldots, p$ и α имеет p различных сопряженных, так что $[k(\alpha) : k] \geqslant p$. Отсюда вытекает, что $K = k(\alpha)$. Заметим, что

$$\sigma(\alpha^p - \alpha) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha.$$

Следовательно, элемент $\alpha^p - \alpha$, неподвижный относительно σ, будет неподвижен относительно степеней σ, а потому и относительно G. Таким образом, он лежит в неподвижном поле k. Полагая $a = \alpha^p - \alpha$, видим, что наше первое утверждение доказано.

Обратно, пусть $a \in k$. Если α — корень многочлена $X^p - X - a$, то $\alpha + i$ при $i = 1, \ldots, p$ также служит его корнем. Таким образом, $f(X)$ имеет p различных корней. Если один корень лежит в k, то и все корни лежат в k. Допустим, что ни один из корней не лежит в k. Мы утверждаем, что многочлен неприводим. Предположим, что

$$f(X) = g(X)\,h(X),$$

где $g, h \in k[X]$ и $1 \leqslant \deg g < p$. Так как

$$f(X) = \prod_{i=1}^{p} (X - \alpha - i),$$

то $g(X)$ совпадает с произведением по некоторым целым числам i. Пусть $d = \deg g$. Коэффициент при X^{d-1} будет суммой членов $-(\alpha + i)$, взятой точно по d целым числам i. Следовательно, он равен $-d\alpha + j$, где j — некоторое целое число. Но $d \neq 0$ в k и, значит, α лежит в k, поскольку коэффициенты g лежат в k — противоречие. Таким образом, $f(X)$ неприводим. Все его корни лежат в поле $k(\alpha)$, которое по этой причине нормально над k. Так как $f(X)$ не имеет кратных корней, то $k(\alpha)$ будет расширением Галуа

над k. Имеется автоморфизм σ поля $k(\alpha)$ над k, такой, что $\sigma\alpha = \alpha + 1$ (поскольку $\alpha + 1$ также корень). Степени σ^i автоморфизма σ дают $\sigma^i(\alpha) = \alpha + i$ для $i = 1, \ldots, p$ и поэтому все различны. Следовательно, группа Галуа состоит из этих степеней, а потому является циклической, что и доказывает теорему.

§ 7. Разрешимые и радикальные расширения

Конечное расширение E/k (которое мы для удобства будем предполагать сепарабельным) называется *разрешимым*, если группа Галуа наименьшего расширения Галуа K над k, содержащего E, является разрешимой группой. Это эквивалентно тому, что существует разрешимое расширение Галуа L поля k, такое, что $k \subset E \subset L$. Действительно, имеем $k \subset E \subset K \subset L$ и $G(K/k)$ есть гомоморфный образ группы $G(L/k)$.

Предложение 2. *Разрешимые расширения образуют отмеченный класс расширений.*

Доказательство. Пусть E/k разрешимо и F — поле, содержащее k, причем E, F — подполя некоторого алгебраически замкнутого поля. Пусть K — разрешимое расширение Галуа над k и $E \subset K$. Тогда KF будет расширением Галуа над F и $G(KF/F)$ — подгруппой в $G(K/k)$ в силу теоремы 4 из § 1. Следовательно, EF/F разрешимо. Ясно, что подрасширение разрешимого расширения разрешимо. Пусть $E \supset F \supset k$ — башня с разрешимыми расширениями E/F и F/k. Пусть K — конечное разрешимое расширение Галуа поля k, содержащее F. Как мы только что видели, EK/K разрешимо. Пусть L — разрешимое расширение Галуа поля K, содержащее EK. Если σ — произвольное вложение L над k в заданное алгебраическое замыкание, то $\sigma K = K$ и, следовательно, σL — разрешимое расширение поля K. Пусть M — композит всех расширений σL для всех вложений σ поля L над k. Тогда M — расширение Галуа над k, а следовательно, и над K. Группа Галуа поля M над K является подгруппой произведения $\prod_{\sigma} G(\sigma L/K)$,