

предполагать, что $E = k(a, \beta)$, где a, β сепарабельны над k . Пусть $\sigma_1, \dots, \sigma_n$ — различные вложения поля $k(a, \beta)$ в \bar{k} над k . Положим

$$P(X) = \prod_{i \neq j} (\sigma_i a + X \sigma_i \beta - \sigma_j a - X \sigma_j \beta).$$

Очевидно, $P(X)$ — ненулевой многочлен и, следовательно, существует элемент $c \in k$, для которого $P(c) \neq 0$. Тогда элементы $\sigma_i(a + c\beta)$ ($i = 1, \dots, n$) все различны, а потому $k(a + c\beta)$ имеет над k степень не меньше n . Но $n = [k(a, \beta) : k]$ и, следовательно, $k(a, \beta) = k(a + c\beta)$, что и требовалось доказать.

Если $E = k(a)$, то мы будем говорить, что a — *примитивный элемент* поля E (над k).

§ 7. Чисто несепарабельные расширения

Этот параграф имеет чисто технический характер и может быть опущен почти без ущерба для понимания остальной части книги.

Мы всюду предполагаем, что k — поле характеристики $p > 0$.

Элемент a , алгебраический над k , называется *чисто несепарабельным* над k , если существует целое число $n \geq 0$, такое, что a^{p^n} лежит в k .

Пусть E — алгебраическое расширение поля k . Мы утверждаем, что следующие условия эквивалентны:

Ч. Нес. 1. $[E : k]_s = 1$.

Ч. Нес. 2. Всякий элемент a из E чисто несепарабелен над k .

Ч. Нес. 3. Неприводимое уравнение для всякого элемента $a \in E$ над k имеет вид $X^{p^n} - a = 0$ при некоторых $n \geq 0$ и $a \in k$.

Ч. Нес. 4. Существует такое множество образующих $\{a_i\}_{i \in I}$ поля E над k , что каждый элемент a_i чисто несепарабелен над k .

Чтобы доказать эту эквивалентность, допустим, что выполняется Ч. Нес. 1. В силу теоремы 6 заключаем, что $[k(a) : k]_s = 1$. Пусть $f(X) = \text{Irr}(a, k, X)$. Тогда f имеет только один корень, поскольку

$$[k(a) : k]_s$$

равна числу различных корней многочлена $f(X)$. Положим $m = [k(a) : k]$. Тогда $\deg f = m$ и разложение f над $k(a)$ имеет вид $f(X) = (X - a)^m$. Но $m = p^nr$, где r — целое число, взаимно-простое с p . Поэтому

$$f(X) = (X^{p^n} - a^{p^n})^r = X^{p^nr} - r a^{p^n} X^{p^n(r-1)} + \text{младшие члены}.$$

Так как коэффициенты многочлена $f(X)$ лежат в k , то

$$r a^{p^n}$$

лежит в k , и так как $r \neq 0$ (в k), то a^{p^n} лежит в k . Пусть $a = a^{p^n}$. Тогда a есть корень многочлена $X^{p^n} - a$, делящегося на $f(X)$. Отсюда вытекает, что $f(X) = X^{p^n} - a$.

По существу то же самое рассуждение, что и предыдущее, показывает, что Ч. Нес. 2 влечет Ч. Нес. 3. То, что третье условие влечет четвертое, тривиально.

Наконец, предположим, что выполняется Ч. Нес. 4. Пусть E — расширение, порожденное чисто несепарабельными элементами a_i ($i \in I$). Любое вложение поля E над k отображает a_i в корень многочлена

$$f_i(X) = \text{Irr}(a_i, k, X).$$

Но $f_i(X)$ делит некоторый многочлен $X^{p^n} - a$, имеющий только один (кратный) корень. Следовательно, любое вложение поля E над k тождественно на каждом a_i , а потому тождественно на E и мы заключаем, что $[E : k]_s = 1$, что и требовалось доказать.

Расширение, удовлетворяющее четырем предыдущим условиям, будет называться *чисто несепарабельным*.

Предложение 10. *Чисто несепарабельные расширения образуют отмеченный класс расширений.*

Доказательство. Утверждение о башне вытекает из теоремы 6, а свойство подъема — из условия Ч. Нес. 4.

Предложение 11. *Пусть E — алгебраическое расширение поля k , и пусть E_0 — композит всех подполей F поля E , таких, что $F \subset k$ и F сепарабельно над k . Тогда E_0 сепарабельно над k , а E чисто несепарабельно над E_0 .*

Доказательство. Поскольку сепарабельные расширения образуют отмеченный класс, то, как мы знаем, E_0 сепарабельно над k . Фактически E_0 состоит из всех элементов E , сепарабельных над k . В силу предложения 9 для заданного элемента $\alpha \in E$, существует такая степень p , скажем p^n , что α^{p^n} сепарабелен над k . Следовательно, E чисто несепарабельно над E_0 , что и требовалось показать.

Следствие 1. *Если алгебраическое расширение E поля k одновременно и сепарабельно, и чисто несепарабельно, то $E = k$.*

Доказательство. Очевидно.

Следствие 2. *Пусть расширение K нормально над k , и пусть K_0 — его максимальное сепарабельное подрасширение. Тогда K_0 также нормально над k .*

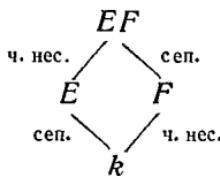
Доказательство. Пусть σ — вложение K_0 в \bar{K} над k . Продолжим σ до вложения поля K . Тогда σ будет автоморфизмом K .

Кроме того, поле σK_0 сепарабельно над k , следовательно, оно содержится в K_0 , поскольку K_0 — максимальное сепарабельное подполе. Значит, $\sigma K_0 = K_0$, что и утверждалось.

Следствие 3. Пусть E, F — два конечных расширения поля k , причем E/k сепарабельно, а F/k чисто несепарабельно. Предположим, что E, F — подполя некоторого общего поля. Тогда

$$\begin{aligned}[EF : F] &= [E : k] = [EF : k]_s, \\ [EF : E] &= [F : k] = [EF : k]_i.\end{aligned}$$

Доказательство. Картина имеет следующий вид:



Доказательство состоит в тривиальном жонглировании индексами с использованием следствий предложения 9. Мы предоставляем его читателю.

Следствие 4. Обозначим через E^p поле всех элементов вида x^p , $x \in E$. Пусть E — конечное расширение поля k . Если $E^p k = E$, то E сепарабельно над k . Если E сепарабельно над k , то $E^{pn} k = E$ для всех $n \geq 1$.

Доказательство. Пусть E_0 — максимальное сепарабельное подполе в E . Допустим, что $E^p k = E$. Положим $E = k(a_1, \dots, a_n)$. Так как E чисто несепарабельно над E_0 , то существует такое m , что $a_i^p \in E_0$ для всех $i = 1, \dots, n$. Следовательно, $E^p \subset E_0$. Но $E^p k = E$, так что $E = E_0$ сепарабельно над k . Обратно, предположим, что E сепарабельно над k . Но E чисто несепарабельно над $E^p k$. Так как E в то же время сепарабельно над $E^p k$, то заключаем, что $E = E^p k$. Итерируя, получаем $E = E^{pn} k$ для $n \geq 1$, что и требовалось доказать.

Предложение 11 показывает, что любое алгебраическое расширение может быть разложено в башню, состоящую из максимального сепарабельного подрасширения и чисто несепарабельного этажа над ним. Обычно бывает нельзя обратить порядок в этой башне. Однако имеется важный случай, когда это может быть сделано.

Предложение 12. Пусть K — нормальное расширение поля k , G — его группа автоморфизмов над k и K^G — неподвижное поле группы G . Тогда K^G чисто несепарабельно над k и K

сепарабельно над K^G . Если K_0 — максимальное сепарабельное подрасширение K , то $K = K^G K_0$ и $K_0 \cap K^G = k$.

Доказательство. Пусть $a \in K^G$ и τ — произвольное вложение поля $k(a)$ над k в \bar{K} . Продолжим τ до вложения поля K ; будем обозначать это продолжение по-прежнему через τ . Тогда τ — автоморфизм поля K , поскольку K нормально над k . По определению $\tau a = a$ и, следовательно, τ тождественно на $k(a)$. Поэтому $[k(a) : k]_s = 1$ и элемент a чисто несепарабелен. Таким образом, K^G чисто несепарабельно над k . Пересечение K_0 и K^G одновременно и сепарабельно, и чисто несепарабельно над k , и, следовательно, равно k .

Чтобы доказать сепарабельность K над K^G , предположим сначала, что K конечно над k и что, следовательно, группа G конечна в силу теоремы 6. Пусть $a \in K$, и пусть $\sigma_1, \dots, \sigma_r$ — максимальное подмножество элементов из G , такое, что элементы

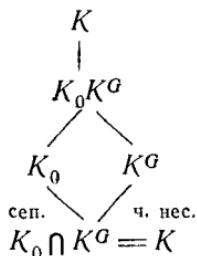
$$\sigma_1 a, \dots, \sigma_r a$$

различны. Тогда некоторое σ_i тождественно на a и a есть корень многочлена

$$f(X) = \prod_{i=1}^r (X - \sigma_i a).$$

Заметим, что $f^\tau = f$ для любого $\tau \in G$, поскольку τ переставляет корни. Мы видим, что f сепарабелен и что его коэффициенты лежат в неподвижном поле K^G . Поэтому a сепарабелен над K^G . Редукция бесконечного случая к конечному основывается на том наблюдении, что всякий элемент $a \in K$ содержится в некотором конечном нормальном подрасширении в K . Детали мы предоставляем читателю.

Теперь имеем следующую диаграмму:



В силу предложения 11 K чисто несепарабельно над K_0 и, следовательно, чисто несепарабельно над $K_0 K^G$. С другой стороны, K сепарабельно над K^G и, следовательно, сепарабельно над $K_0 K^G$. Таким образом, $K = K_0 K^G$, что и доказывает наше предложение.

Мы видим, что всякое нормальное расширение распадается в композит чисто несепарабельного и сепарабельного расширений. В следующей главе мы определим расширение Галуа как нормальное сепарабельное расширение. Тогда K_0 будет расширением Галуа над k и нормальное расширение распадается на расширение Галуа и чисто несепарабельное расширение. Группа G называется группой Галуа расширения K/k .

Поле k называется *совершенным*, если $k^p = k$. (Всякое поле характеристики нуль также называется совершенным.)

Следствие. Если поле k совершенно, то любое его алгебраическое расширение сепарабельно. Всякое алгебраическое расширение поля k совершенно.

Доказательство. Всякое конечное алгебраическое расширение содержится в нормальном расширении, поэтому наши утверждения непосредственно следуют из предложения 12.

УПРАЖНЕНИЯ

1. Пусть k — конечное поле из q элементов, $f(X) \in k[X]$ — неприводимый многочлен. Показать, что $f(X)$ делит многочлен $X^{q^n} - X$ тогда и только тогда, когда степень f делит n .

2. Показать, что

$$X^{q^n} - X = \prod_{d|n} \prod_{f_d \text{ непр.}} f_d(X),$$

где второе произведение берется по всем неприводимым многочленам степени d со старшим коэффициентом 1. Подсчитав степени, показать, что

$$q^n = \sum_{d|n} d\psi(d),$$

где $\psi(d)$ — число неприводимых многочленов степени d . С помощью элементарной теории чисел получить двойственное равенство

$$n\psi(n) = \sum_{d|n} \mu(d) q^{n/d}.$$

(μ — функция Мёбиуса, см. стр. 236.)

3. Пусть k — поле характеристики p , и пусть t, u алгебраически независимы над k . Доказать следующие утверждения:

(i) $k(t, u)$ имеет степень p^2 над $k(t^p, u^p)$.

(ii) Между $k(t, u)$ и $k(t^p, u^p)$ существует бесконечно много расширений.

4. Пусть E — конечное расширение поля k характеристики $p > 0$, и пусть $p' = [E:k]_p$. Допустим, что не существует степени p^s с $s < r$, для которой $E^{p^s}k$ сепарабельно над k (т. е. такой, что a^{p^s} сепарабелен над k для всякого a из E). Показать, что E может быть порождено одним элементом над k . [Указание: предположить сначала, что E чисто несепарабельно.]

5. Пусть k — поле, $f(X)$ — неприводимый многочлен из $k[X]$ и K — конечное нормальное расширение над k . Показать, что если g, h — неприводимые множители $f(X)$ в $K[X]$, то существует автоморфизм σ поля K над k , для которого $g = h^\sigma$. Привести пример, показывающий, что это утверждение неверно, если K не нормально над k .

6. Пусть x_1, \dots, x_n алгебраически независимы над полем k , а u алгебраичен над $k(x) = k(x_1, \dots, x_n)$. Пусть $P(X_{n+1})$ — неприводимый многочлен элемента u над $k(x)$ и $\varphi(x)$ — наименьшее общее кратное знаменателей коэффициентов многочлена P . Тогда коэффициенты многочлена $\varphi(x)P$ являются элементами из $k[x]$. Показать, что

$$f(X_1, \dots, X_{n+1}) = \varphi(X_1, \dots, X_n) P(X_{n+1})$$

неприводим над k как многочлен от $n+1$ переменной. Обратно, пусть $f(X_1, \dots, X_{n+1})$ — неприводимый многочлен над k и x_1, \dots, x_n алгебраически независимы над k . Показать, что

$$f(x_1, \dots, x_n, X_{n+1})$$

неприводим над $k(x_1, \dots, x_n)$.

Если f — многочлен от n переменных и $(b) = (b_1, \dots, b_n)$ такой набор из n элементов, что $f(b) = 0$, то мы говорим, что (b) — нуль многочлена f . Мы говорим, что нуль (b) нетривиален, если не все координаты b_i равны 0.

7. Пусть $f(X_1, \dots, X_n)$ — однородный многочлен степени 2 (соответственно 3) над полем k . Показать, что если f имеет нетривиальный нуль в некотором расширении нечетной степени (соответственно, степени 2) над k , то f имеет нетривиальный нуль в k .

8. Пусть $f(X, Y)$ — неприводимый многочлен от двух переменных над полем k , и пусть t трансцендентно над k , причем существуют взаимно простые целые числа m, n и элементы $a, b \in k$, $ab \neq 0$, такие, что $f(at^n, bt^m) = 0$. Показать, что после возможной замены X или Y на обратную величину и с точностью до постоянного множителя многочлен f имеет вид

$$X^m Y^n - c$$

с некоторым $c \in k$.

Ответ к следующему упражнению неизвестен.

9. (А р т и н) Пусть f — однородный многочлен степени d от n переменных с рациональными коэффициентами. Показать, что если $n > d$, то существуют корень из единицы ζ и элементы $x_1, \dots, x_n \in \mathbb{Q}[\zeta]$, не все равные нулю, такие, что $f(x_1, \dots, x_n) = 0$.