Часть 1. Сепарабельная степень

Лемма 1.1. *Если K/F — алгебраическое расширение, а $\sigma : F \to L$ — гомоморфизм в алгебраически замкнутое поле, то количество гомоморфизмов $\tau : K \to L$, продолжающих σ, не зависит от σ.*

Доказательство: пусть $\sigma' : F \to L'$ — другой гомоморфизм. Пусть $\overline{F}$ и $\overline{F}'$— алгебраические замыкания F в L и L' соответственно. Выберем изоморфизм $\rho : \overline{F} \to \overline{F}'$ над F. Тогда $\tau \mapsto \rho \circ \tau$ искомая биекция. □

Определение 1.2. Пусть K'/K — конечное расширение и $\sigma : K \to L$ — гомоморфизм в алгебраически замкнутое поле. Определим сепарабельную степень $[K' : K]_s$ как количество различных гомоморфизмов $K' \to L$, продолжающих σ.

Лемма 1.3. *Сепарабельная степень мультипликативна в башнях: если $K \subset K' \subset K''$ — конечные расширения полей, то $[K'' : K]_s = [K'' : K']_s [K' : K]_s$.*

Доказательство: Пусть $K \subset K' \subset K''$ — конечные расширения, L — алгебраически замкнутое поле и $\rho : K \to L$ — гомоморфизм. Пусть $\sigma_1, \ldots, \sigma_n$, $n = [K' : K]_s$ — набор различных гомоморфизмов $K' \to L$, продолжающих ρ. Пусть далее $\tau_{i1}, \ldots, \tau_{im}$, $m = [K'' : K']_s$ — набор различных гомоморфизмов $K'' \to L$, продолжающих σ_i. Покажем, что τ_{ij} различны. Действительно, если $\tau_{ij} = \tau_{kl}$, то $\sigma_i = \tau_{ij|K'} = \tau_{kl|K'} = \sigma_k$, значит $i = k$, но тогда $j = l$. Пусть теперь $\tau : K'' \to L$ — произвольный гомоморфизм, продолжающий ρ. Тогда $\tau_{|K'}$ — тоже продолжает ρ, следовательно $\tau_{|K'} = \sigma_i$ для некоторого i и, значит, $\tau = \tau_{ij}$ для некоторого j. Таким образом, мы показали, что существует ровно mn гомоморфизмов $K'' \to L$, продолжающих ρ, и тем самым доказали мультипликативность сепарабельной степени. □

Лемма 1.4. *Для любого конечного расширения K'/K имеем $[K' : K]_s \leqslant [K' : K]$.*

Доказательство: поскольку как степень, так и сепарабельная степень мультипликативны в башнях, то достаточно показать, что $[K(\alpha) : K]_s \leqslant [K(\alpha) : K]$. Но мы уже знаем, что $[K(\alpha) : K]_s$ равно количеству различных корней многочлена $\mathrm{Irr}_\alpha^K(x)$ в поле $\overline{K}$, в то время как $[K(\alpha) : K]$ равно степени этого многочлена. □

Следствие 1.5. *Пусть $K \subset K' \subset K''$ — башня конечных расширения полей. Тогда*
$[K'' : K]_s = [K'' : K] \iff [K'' : K']_s = [K'' : K']$ *и* $[K' : K]_s = [K' : K]$.

Часть 2. Сепарабельные расширения

Определение 2.1. Неприводимый многочлен $f(x) \in K[x]$ называется сепарабельным, если $f(x)$ не имеет кратных корней в $\overline{K}$.

Лемма 2.2. *Неприводимый многочлен $f(x) \in K[x]$ не сепарабелен $\iff \mathrm{char}\, K = p > 0$ и $f(x) = g(x^{p^n})$, где $g(x) \in K[x]$ — неприводимый сепарабельный многочлен.*

Доказательство: если $f(x)$ имеет кратные корни в $\overline{K}$, то НОД$(f(x), f'(x)) \neq 1$. Но $f(x)$ — неприводим, значит[1] НОД$(f(x), f'(x)) = f(x)$, значит $f'(x) = 0$. Отсюда следует, что $\mathrm{char}\, K = p > 0$ и $f(x) = f_1(x^p)$, где $f_1(x) \in K[x]$. Ясно, что $f_1(x)$ неприводим, поэтому по индукции $f_1(x) = g(x^{p^{\mu'}})$, где $g(x)$ неприводим и сепарабелен. Значит $f(x) = g(x^{p^{\mu'+1}})$. □

Определение 2.3. Пусть L/K — расширение полей. Элемент $\alpha \in L$ называется сепарабельным над K, если многочлен $\mathrm{Irr}_\alpha^K(x)$ — сепарабелен. Алгебраическое расширение L/K называется сепарабельным, если любой элемент поля L сепарабелен над K.

Следствие 2.4. *Если $\mathrm{char}\, K = 0$, то всякое алгебраическое расширение поля K сепарабельно.*

[1] если $f(x), g(x) \in K[x]$ и $h(x) = \text{НОД}_{\overline{K}[x]}(f(x), g(x))$, то $h(x) \in K[x]$. Докажите это!

Пусть теперь $\operatorname{char} K = p > 0$.

Лемма 2.5. *Элемент α сепарабелен над K $\iff$ найдется многочлен $f(x) \in K[x]$, такой что $f(\alpha) = 0$ и $f(x)$ не имеет кратных корней в $\overline{K}$.*

Доказательство: $\Longrightarrow$) Очевидно. $\Longleftarrow$) Ясно, что $\operatorname{Irr}_\alpha^K(x)$ делит $f(x)$, поэтому если $f(x)$ не имеет кратных корней, то и $\operatorname{Irr}_\alpha^K(x)$ не имеет кратных корней в поле $\overline{K}$. $\square$

Лемма 2.6. *Если башня полей сепарабельна, то каждый ее этаж сепарабелен.*

Доказательство: пусть $K \subset K' \subset K''$ и K''/K сепарабельно. Все элементы в K'', а значит и в K'сепарабельны над K. С другой стороны, $\forall \alpha \in K''$ многочлен $\operatorname{Irr}_\alpha^K(x) \in K[x] \subset K'[x]$ сепарабелен, значит по лемме 2.5 элемент α сепарабелен и над K'. $\square$

Лемма 2.7. *Пусть α — алгебраический элемент над полем K, $f(x) = \operatorname{Irr}_\alpha^K(x)$ и $f(x) = g(x^{p^\mu})$, где $g(x)$ — неприводимый и сепарабельный. Тогда α^{p^μ} сепарабелен над K и $[K(\alpha) : K]_s = \deg g(x)$. В частности, $[K(\alpha) : K] = p^\mu [K(\alpha) : K]_s$.*

Доказательство: Пусть $g(x) = \prod_{i=1}^m (x - \beta_i)$, $\beta_i \in \overline{K}$, причем $\beta_i \neq \beta_j$ при $i \neq j$. Заметим, что для каждого β_i найдется единственный $\alpha_i \in \overline{K}$, т.ч. $\alpha_i^{p^\mu} = \beta_i$ ($\alpha_i^{p^\mu} = {\alpha'_i}^{p^\mu} \Longrightarrow 0 = \alpha_i^{p^\mu} - {\alpha'_i}^{p^\mu} = (\alpha_i - \alpha'_i)^{p^\mu} \Longrightarrow \alpha_i = \alpha'_i$). Тогда $f(x) = g(x^{p^\mu}) = \prod_{i=1}^m (x^{p^\mu} - \alpha_i^{p^\mu}) = \prod_{i=1}^m (x - \alpha_i)^{p^\mu}$, поэтому $[K(\alpha) : K]_s = m = \deg g(x)$. Кроме того, $[K(\alpha) : K] = \deg f(x) = p^\mu \deg g(x) = p^\mu [K(\alpha) : K]_s$. Наконец, α^{p^μ} сепарабелен так как является корнем сепарабельного многочлена $g(x)$. $\square$

Следствие 2.8. *Элемент α сепарабелен $\iff$ $[K(\alpha) : K]_s = [K(\alpha) : K]$.*

Теорема 2.9. *Конечное расширение K'/K сепарабельно $\iff$ $[K' : K]_s = [K' : K]$.*

Доказательство: пусть K'/K сепарабельно. Возьмем $\alpha \in K' \setminus K$ и рассмотрим башню $K \subset K(\alpha) \subset K'$. По лемме 2.6 каждый этаж сепарабелен. Далее, в силу 2.8 имеем $[K(\alpha) : K]_s = [K(\alpha) : K]$, кроме того, по индукции имеем $[K' : K(\alpha)]_s = [K' : K(\alpha)]$, значит $[K' : K]_s = [K' : K]$ в силу мультипликативности степеней. Обратно, предположим, что $[K' : K]_s = [K' : K]$ и возьмем произвольный $\alpha \in K'$. По следствию 1.5 имеем $[K(\alpha) : K]_s = [K(\alpha) : K]$, значит в силу 2.8 элемент α сепарабелен. $\square$

Следствие 2.10. *Расширение $K(\alpha_1, \dots, \alpha_n)/K$ сепарабельно $\iff$ $\alpha_1, \dots, \alpha_n$ — сепарабельны над K.*

Доказательство: $\Longrightarrow$) По определению. $\Longleftarrow$) На каждом этаже башни $K \subset K(\alpha_1) \subset \cdots \subset K(\alpha_1, \dots, \alpha_n)$ сепарабельная степень равна степени, поэтому $[K(\alpha_1, \dots, \alpha_n) : K]_s = [K(\alpha_1, \dots, \alpha_n) : K]$ в силу мультипликативности, следовательно по теореме 2.9 расширение $K(\alpha_1, \dots, \alpha_n)/K$ сепарабельно. $\square$

Следствие 2.11. *Башня полей сепарабельна $\iff$ каждый ее этаж сепарабелен.*

Доказательство: $\Longrightarrow$) Уже доказано. $\Longleftarrow$) Действительно, пусть $K \subset K' \subset K''$ — башня и $\alpha \in K''$. Пусть $\operatorname{Irr}_\alpha^{K'}(x) = x^n + a_1 x^{n-1} + \dots + a_0$. Тогда α сепарабелен над $K(a_1, \dots, a_n) \subset K'$, а $K(a_1, \dots, a_n)$ сепарабельно над K. Значит $[K(a_1, \dots, a_n, \alpha) : K]_s = [K(a_1, \dots, a_n, \alpha) : K]$, следовательно α сепарабелен над K. $\square$

Часть 3. Чисто несепарабельные расширения

Лемма 3.1. *Если L/K конечно, то $[L : K]_s$ делит $[L : K]$.*

Доказательство: в силу мультипликативности все следует из леммы 2.8. $\square$

Число $[L : K]_i := [L : K]/[L : K]_s$ называется степенью несепарабельности расширения L/K.

Лемма 3.2. *Если $\operatorname{char} K = 0$, то $[L : K]_i = 1$, а если $\operatorname{char} K = p$, то $[L : K]_i = p^\mu$ для некоторого μ.*

Доказательство: в силу мультипликативности все следует из леммы 2.8. $\square$

Определение 3.3. Элемент α называется чисто несепарабельным над K, если $\alpha^{p^\mu} \in K$. Расширение L/K называется чисто несепарабельным, если всякий $\alpha \in L$ чисто несепарабелен над K.

Лемма 3.4. *Элемент α чисто несепарабелен над K $\iff \operatorname{Irr}_\alpha^K(x) = x^{p^\mu} - a$, $a \in K$.*

Доказательство: если $\operatorname{Irr}_\alpha^K(x) = x^{p^\mu} - a$, то $\alpha^{p^\mu} = a \in K$, поэтому α чисто несепарабелен над K. С другой стороны, если $\mu > 0$ — минимальное число, такое что $\alpha^{p^\mu} \in K$, то $f(x) = (x-\alpha)^{p^\mu} = x^{p^\mu} - \alpha^{p^\mu} \in K[x]$, поэтому $\operatorname{Irr}_\alpha^K(x)$ делит $f(x)$, следовательн $\operatorname{Irr}_\alpha^K(x) = (x-\alpha)^n$, $n \leqslant \mu$. Наконец, если $n = mp^{\mu'}$, НОД$(m,p) = 1$, то $(x-\alpha)^n = \left((x-\alpha)^{p^{\mu'}}\right)^m = (x^{p^{\mu'}} - \alpha^{p^{\mu'}})^m = x^n - m\alpha^{p^{\mu'}} x^{(m-1)p^{\mu'}} + \ldots$, поэтому $\alpha^{p^{\mu'}} \in K$, значит (в силу минимальности μ) имеем $\mu' = \mu$, $m = 1$ и $\operatorname{Irr}_\alpha^K(x) = (x-\alpha)^{p^\mu} = x^{p^\mu} - \alpha^{p^\mu}$. $\square$

Следствие 3.5. *Расширение L/K чисто несепарабельно $\iff \forall \alpha \in L$ имеем $\operatorname{Irr}_\alpha^K(x) = x^{p^\mu} - a$.*

Лемма 3.6. *Конечное расширение L/K чисто несепарабельно $\iff [L:K]_s = 1$.*

Доказательство: Пусть L/K чисто несепарабельно. Вследствии мультипликативности можно считать, что $L = K(\alpha)$. Тогда, в силу леммы 3.4 имеем $\operatorname{Irr}_\alpha^K(x) = x^{p^\mu} - a$, поэтому по лемме 2.8 имеем $[K(\alpha):K]_s = 1$. Обратно, если $[L:K]_s = 1$, то $\forall \alpha \in L$ в силу мультипликативности имеем $[K(\alpha):K]_s = 1$, поэтому по лемме 2.8 имеем $\operatorname{Irr}_\alpha^K(x) = x^{p^\mu} - a$, следовательно по лемме 3.4 элемент α чисто несепарабелен над K. $\square$

Следствие 3.7. *Башня расширений чисто несепарабельна $\iff$ каждый ее этаж чисто несепарабелен.*

Часть 4. Сепарабельное замыкание

Лемма 4.1. *Пусть L/K — расширение. Множество элементов $\alpha \in L$, сепарабельных над K образует подполе $L^{\mathrm{sep}} \subset L$, сепарабельное над K.*

Доказательство: если $\alpha, \beta \in L^{\mathrm{sep}}$, то $K(\alpha,\beta)/K$ сепарабельно по 2.10, следовательно $\alpha+\beta, \alpha\beta, \dots \in L^{\mathrm{sep}}$. $\square$

Поле L^{sep} называется сепарабельным замыканием поля K в L.

Лемма 4.2. *Расширение L^{sep}/K сепарабельно, а L/L^{sep} чисто несепарабельно.*

Доказательство: первое утверждение очевидно. Докажем второе. Пусть $\alpha \in L$. По лемме 2.7 существует μ, такое что α^{p^μ} сепарабелен над K. Поэтому $\alpha^{p^\mu} \in L^{\mathrm{sep}}$, значит α чисто несепарабелен над L^{sep}. $\square$

Замечание 4.3. Таким образом, всякое расширение представляется в виде башни, нижний этаж которой сепарабелен, а верхний — чисто несепарабелен.

Теорема 4.4. *Пусть L/K — нормальное расширение, $G = \operatorname{Aut}(L/K)$. Тогда $L^G := \{\, x \in L \mid Gx = x \,\}$ — подполе в L, причем L/L^G — сепарабельно, а L^G/K — чисто несепарабельно.*

Доказательство: Пусть $\alpha \in L$. Ясно, что орбита $G\alpha \subset L$ конечна. Пусть $G\alpha = \{\, \alpha_1, \dots, \alpha_n \,\}$. Рассмотрим многочлен $p(x) = \prod_{i=1}^n (x-\alpha_i)$. Легко видеть, что $Gp(x) = p(x)$, поэтому $p(x) \in L^G[x]$. Кроме того, по построению $p(\alpha) = 0$ и $p(x)$ не имеет кратных корней. Значит α сепарабелен над L^G. Пусть теперь $\alpha \in L^G$. Пусть $\sigma : K(\alpha) \to \overline{K}$ — произвольный гомоморфизм. Продолжим σ до гомоморфизма $\tau : L \to \overline{K}$ над K. Тогда $\tau \in G$, так как L/K нормально, значит $\alpha^\sigma = \alpha^\tau = \alpha$, так как $\alpha \in L^G$. Но тогда $\sigma = \mathrm{Id}$, значит $[K(\alpha):K]_s = 1$, значит α чисто несепарабелен над K. $\square$

Определение 4.5. Поле K называется совершенным, если $\operatorname{char} K = 0$ или $K^p = K$, где $p = \operatorname{char} K$.

Следствие 4.6. *Любое алгебраическое расширение совершенного поля сепарабельно.*

Доказательство: если $\alpha^{p^\mu} = a \in K$, то $\alpha = \sqrt[p^\mu]{a} \in K$, значит K не имеет нетривиальных чисто несепарабельных расширений. Пусть теперь L/K — произвольное расширение. Пусть L'/K — нормальное расширение, такое что $L \subset L'$. Тогда по теореме 4.4 расширение L'/K сепарабельно, но тогда и L/K сепарабельно. $\square$