

4. Сенарабелность и расщепления Гауса

Опр 1 Мн-н $f(x) \in K[x]$ наз-ся **сенарабелным**, если он не имеет кратных корней (в своем поле разложения).

Предл 1 $f(x)$ сенарабелен $\Leftrightarrow (f, f') = 1$, где $f'(x)$ - производная от f (см. опр. 5.3. Чиз [ВЛМ]),
В частности, если f неразл. над K , то f не сенарабелен $\Leftrightarrow f'(x) = 0$ (тождество)

Л. 1 Пусть $f(x) \in K[x]$ неразл. мн-н. Тогда

1) если $\text{char } F = 0$, то f сенарабелен

2) если $\text{char } F = p > 0$, то f не сенарабелен $\Leftrightarrow \exists h \in K[x]$
 $f(x) = h(x^p)$. В частности, если $p \nmid \deg f$, то f сенарабелен.

Л-во: Так $f(x)$ неразл, $\Rightarrow \deg f > 0$. Из $\text{чрезл} \Rightarrow 1$.

Так $\text{Char } F = p$ и $f(x) = \sum_{k=0}^n a_k x^k$. Тогда $f' \equiv 0 \Leftrightarrow$

$$a_k = 0 \quad \forall k \neq 0(p) \Leftrightarrow f(x) = a_0 + a_p x^p + \dots \Leftrightarrow$$

$$f(x) = h(x^p) \text{ где некот. } h \in K[x] \quad \blacksquare$$

Хотя существуют примеры нечувствительных
случаев, в большинстве "разных" случаев все
хорошо!

Опр. 2 Поле K **совершенно**, если каждый неразл.
мн-к из $K[x]$ сепарабелен; и **несовершенно** в
противном случае.

Т. 2 Пусть K -поле. Тогда

а) $\text{char } K = 0 \Rightarrow K$ совершенно.

2) Если $\text{char } F = p > 0$, то F совершенно в себе.

См. лемма 11.3.1: а) F алг. замкн б) F конечно.

Лемма 11.3.2: Пусть F — поле. Тогда из 11.3.1 п.2 а) следует, что

F алг. замкн \Rightarrow каждый многочл. из $F[x]$ имеет корень в F .

Доказательство. В силу утвержд. 11.3.2 (см. АН-73) $\forall a \in F$

$\exists b \in F: b^p = a$. Если $f(x)$ — многочл. в $F[x]$,

$$f(x) = h(x^p) = a_0 + a_1 x^p + \dots + a_m x^{pm} = b_0^p + b_1^p x^p + \dots + b_m^p x^{pm}$$

$$= (b_0 + b_1 x + \dots + b_m x^m)^p, \text{ что противоречит лемме 11.3.1. } \blacksquare$$

Пример Пусть $F = \mathbb{Z}_p(t) = \left\{ \frac{g(t)}{h(t)} \mid h \neq 0, g, h \in \mathbb{Z}_p[t] \right\}$

— простое трансценд. расширение поля \mathbb{Z}_p .

p -и лемма $f(x) = x^p - t \in F[x]$. Очевидно, что $f(x) =$

$$= (x - s)^p, \text{ где } s^p = t, \text{ т.е. } f(x) \text{ имеет корень в } F. \text{ Чтб и требовалось.}$$

Зок-П, что $f(x)$ неразложим над F , имеет степень

$|F(s) : F|$, Если $s^{p-1}, s^{p-2}, \dots, s, 1$ л.н. незав.

над F , то $\exists a_i \in \mathbb{Z}_p(t) : a_0 + a_1 s + \dots + a_{p-1} s^{p-1} = 0$

"Умножая на знаменатель", считаем, что $a_i \in \mathbb{Z}_p[t]$.

Диф-я л.н. зав-ств $(p-1)$ раз имеет $a_{p-1}(p-1)(p-2)\dots 2 \cdot 1 = 0$

над $\mathbb{Z}_p \Rightarrow a_{p-1} = 0$. Аналогично, $a_i = 0 \forall i \Rightarrow$

$\dim |F(s) : F| = p \Rightarrow x^p - t$ неразложим над F .

Опр 3 Пусть L -расширение поля K , $\alpha \in L$

сепарабелен над K , если α - корень непр. сепарабельного м.н.-я. Алгебр. расширение

L поля K **сепарабельно** над K , если все $\alpha \in L$ $\alpha \notin K$ сепарабельны над K .

Предл. 2 Касное алг. расширение соврщ. поля
сепарабельно над ним.

Т. 3 (о примитивном эле) Пусть $L = K(\alpha_1, \alpha_2, \dots, \alpha_t)$ —
кон. алгебр. расширение поля K и n_1, \dots, n_t
(но не обязат. α_1) сепарабельны над K . Тогда
 $\exists \theta \in L : L = K(\theta)$, т.е. L — простое расширение.

Л-во: Для $t=1$ год. — тривиально. Пусть сначала $t=2$.

Т.е. $L = K(\alpha, \beta)$ и β сепарабелен. Пусть $f(x)$ и $g(x)$
— неразл. мн-ки m_1 и m_2 соот-но, и $\alpha = \alpha_1, \alpha_2, \dots, \alpha_t$ — разл.
корни f , $\beta = \beta_1, \dots, \beta_s$ — разл. корни $g(x)$ (в частности,
 $\deg g = s$, т.к. $g(x)$ сепарабелен). Можно считать что
поле K дрсв., иначе L тоже конечно $\Rightarrow L$ простое
(см. Ал-м. 73).

Для $k=2, \dots, s$ $\beta_k \neq \beta_1 \Rightarrow \forall i=1 \dots r \quad \forall k=2 \dots s$ ур-е

$$\alpha_i + x\beta_k = \alpha_1 + x\beta_1 \quad (*)$$

имеет не более одного решения x из K ,

Выберем $c \in K$, отличным от всех корней ур-я из (*).

Положим $\Theta = \alpha_1 + c\beta_1 = \alpha + c\beta$. Тогда $\Theta \in K(\alpha, \beta)$.

Мы ж-ем, что $K(\alpha, \beta) = K(\Theta)$.

Эт-т β явл-ся корнем ур-я $g(x) = 0$ и $f(\Theta - cx) = 0$,
коэф-ты которых лежат в $K(\Theta)$. Поэтому $x = \beta$ имеет
мх $\text{НОЗ} = d(x)$. Замечает, что β_k ур-я $k \neq 2$ не явл-ся корнем
 $f(\Theta - cx)$, т.к. иначе $\Theta - c\beta_k = \alpha_i$ для нек-т. $i=1 \dots r$, что
противоречит выбору c и Θ . Сл-но, $d(x) = (x - \beta)^k$, т.е.
 β — простой корень $g(x) \Rightarrow d(x) = x - \beta$. Но коэф-ты d ,

как код $g(x)$ и $f(\theta \cdot x)$ должны лежать в $K(\theta)$
 $\Rightarrow \beta \in K(\theta) \Rightarrow \alpha = \theta \cdot \beta \in K(\theta) \Rightarrow K(\theta) = L$,

Так как $t \geq 2$ и т-матрица задана для $t-1$, т.е.
 $\exists \eta \in L: K(\alpha_1, \dots, \alpha_{t-1}) = K(\eta)$. Тогда $L = K(\alpha_1, \dots, \alpha_{t-1}, \alpha_t) =$
 $= K(\eta, \alpha_t) = K(\theta)$ по доказанному при $t=2$ \square

Следствие 1 Кантовское кон. сепарабельное расширение
— простое.

Мн-во авт-завис расщ. L над полем K (см. AN-71)
образует группу, кот. мы обозначим $\text{Aut}_K L$.

Следствие 2 Если L — кон. сепарабельное расщ.

над K , то $|\text{Aut}_K L| \leq |L:K|$.

Зам. сепарабельно ст тут можно брать (см. т. 7 из AN-71)

1-во: По т. 3 $L = K(\theta)$ и $|L:K| = \deg m_\theta = n$

Согласно лемме о продолжении автоморфизма (л. 3-вет. 11.1.7, см. АН-71) $| \text{Aut}_K L |$, равное числу способов продолжить тождеств. авт-зм поля K до автоморфизма поля L , равно числу корней m_θ в L , т.е. $\leq n$ \square

Опр 4 Конечное расширение L поля K наз-ся

расширением Галуа, если $| \text{Aut}_K L | = |L:K|$.

В этом случае группа $\text{Aut}_K L$ наз-ся группой Галуа этого расширения. Обозн: $\text{Gal}(L/K) = \text{Aut}_K L$.

Опр 5 Алгебраическое расщ. L поля K наз-ся **нор-**
мальным, если каждый неразр. мн-н из $K[x]$
распадается над L на линейные множители.


Предл 3 кон. алг. расщ. L поля K нормальное \Leftrightarrow
 L - поле разложения кон. семейства $\{f_i \mid i \in I\}$
мн-нов из $K[x]$, т.е. получено присоединением
всех корней этих мн-нов.

Упр 1 Д-ть предл. 3 Указание: Все сводится к
случаю, когда L - поле разложения одного мн-на.

Т. 4 Пусть L - кон. старейшее норм. расщ.-
ение поля K . Тогда L - расщепление Галуа.

1-во: В силу сепарабельности $L = K(\Theta)$ гл. некот.

$\Theta \in K$. В силу нормальности L -поле разложения $h = m_\Theta$, т.е. все корни h лежат в L .

По лемме о продолжении изм-зма $|\text{Aut}_K L| = \deg h = [L:K]$. 

Зам. Группа Галуа, конечно, не зависит от выбора примитивного эл-та Θ расширения L над K .
Более того, для её определения достаточно не обязательно искать этот элемент, можно р-ть $L = K(\alpha_1 \dots \alpha_s)$ — как конечное расширение нормальн-эп-го из эт.п.

Опр 6 Пусть $L = K(\alpha_1, \dots, \alpha_n)$ — поле разложения
 мн-ка $f(x) \in K[x]$, не имеющего кратных корней,
 с мн-вом корней $\alpha_1, \dots, \alpha_n$. Группой Галуа уравнения
 $f(x) = 0$ (или мн-ка $f(x)$) наз-ся группа $\text{Gal}(L/K)$.

Предл 4 Пусть в обозн. Опр 6 $\Sigma = \{\alpha_1, \dots, \alpha_n\}$ и $G =$
 $= \text{Gal}(L/K)$. Тогда G точно действует на Σ ,
 т.е. задан инволютивный пом-зм σ из G в $\text{Sym}(\Sigma)$,
 где которого $\alpha_i^\sigma = \alpha_{i^\sigma}$.

Д-во: Из леммы о продолжении пом-змов \Rightarrow
 Корни переходят в корни пог-ся с-вами σ из G .
 Тот факт, что это пом-зм вытекает из Опр. 5.

При этом, если $\alpha^G = \begin{pmatrix} \alpha_1 & \dots & \alpha_n \\ \alpha_1' & \dots & \alpha_n' \end{pmatrix}$, то $\left(\frac{h(\alpha_1 - \dots - \alpha_n)}{g(\alpha_1 - \dots - \alpha_n)} \right)^x =$
 $= \left(\frac{h(\alpha_1' - \dots - \alpha_n')}{g(\alpha_1' - \dots - \alpha_n')} \right)$ потому что г. н.с.г. и с.г.с. корни
 соответствуют г. н.с.г.с. абс. 3-м расширениям \square

Мы будем часто отождествлять G с G^G .

Пример Если $L = K(\sqrt{d})$ — кв.др. расширение
 (через $K \neq 2$), где $d \in K \setminus K^2$, то L -расширение
 $\text{Gal}(L/K) = \langle \varphi \rangle$, где $\varphi: a + b\sqrt{d} \mapsto a - b\sqrt{d}$
 — абс. 3-м порядка 2. Это можно проверить как
 перестановку корней \sqrt{d} и $-\sqrt{d}$ ур-я $x^2 + d = 0$.

Упр 2 $f(x)$ непр. над $K \Leftrightarrow$ группа Галуа

транзитивна

Упр 3 Найдите группу Галуа ур-я $x^3 + px + q$ в 3-м

Вспомогательная p и q (Указ. Если $f(x)$ неразл. рас-
смотрим $D = -4p^2 - 27q^3 = \prod_{i < j} (\alpha_i - \alpha_j)^2$,

Упр 4 Какие группы Галуа поля Галуа $GF(p^n)$

a) над $GF(p)$

б) над $GF(p^m)$, где $m | n$.