

# 11 Основы теории Галуа

## 1. Расширения полей и колец

Кольцо  $B$  — **расширение** кольца  $A$ , если  $A \subseteq B$ , т.е.  $A$  — подкольцо кольца  $B$ .

Этот  $\varphi \in B$  **алгебраический** над  $A$ , если  $\exists f(x) \in A[x] : f(\varphi) = 0$ , и **трансцендентный**, над  $A$  в противном случае.

$B$  — **алгебраическое расширение** кольца  $A$ , если каждый элемент кольца  $B$  алгебраический над  $A$ .

Зам. Здесь и далее "Кольцо" = асоц. комм. кольцо с  $1$

$n$ -м  $x_1, \dots, x_n \in B$  алгебр. ЗАБЧ самх, если  
 $\exists f(x_1, \dots, x_n) \in A[x_1, \dots, x_n] : f(x_1, \dots, x_n) = 0$ .

$A[x_1, \dots, x_n] = \{f(x_1, \dots, x_n) \mid f \in A[x_1, \dots, x_n]\}$  —  
покажем, что  $A \subseteq B$  (и расщепление кольца  $A$ ),  
*по теореме* над  $A$  эл-мы  $x_1, \dots, x_n \in B$ ,

$B$  конечно порождено над  $A$ , если  $\exists x_1, \dots, x_n \in B$   
такие, что  $B = A[x_1, \dots, x_n]$ .

Мы знаем, что  $A[x_1, \dots, x_n] \cong A[x_1, \dots, x_n]/I$ ,  
где  $I \trianglelefteq A[x_1, \dots, x_n]$ . В частности, эл-ты  
 $x_1, \dots, x_n$  алг. независимы  $\Leftrightarrow I = 0 \Leftrightarrow$   
 $A[x_1, \dots, x_n] \cong A[x_1, \dots, x_n]$ .

Если  $B$  — целое кольцо (тогда  $A$  тоже),  
то можно взять  $B$  и  $A$  в их полных  
частях  $\mathcal{O}(B) = L$  и  $\mathcal{O}(A) = K$ , т.е.

$$\begin{array}{ccc} A & \subseteq & B \\ \cap & & \cap \\ K & \subseteq & L \end{array} \quad (\text{рис. 1})$$

Если  $u_1, \dots, u_n \in L$  ант. ЗАБ над  $K$ , то  
они ант. ЗАБ и над  $A$  ( $\text{ЗАБ}$  — сд  $f(u_1 - u_i) = 0$   
над  $K$  "преобразуется" в  $\text{ЗАБ}$  — сд  $\tilde{f}(u_i - u_j) = 0$   
над  $A$  "умножением на 3-элемент").

Рассмотрим стандартное расширение полей.  
Всюду далее поле  $L$  — расширение поля  $K$ .

Опр 1 Пусть  $u_1, \dots, u_n \in L$ . Поле, порожденное  
наз  $K$  эл-ми  $u_1, \dots, u_n$ , наз-ся  $Q(K[u_1, \dots, u_n])$   
поле всех отношений эл-тов из  $K[u_1, \dots, u_n]$ .

Обозн:  $K(u_1, \dots, u_n) = Q(K[u_1, \dots, u_n])$  — расширение  
поля  $K$  присоединением эл-тов  $u_1, \dots, u_n$ .

Если  $L = K(u_1, \dots, u_n)$ , то  $L$  порождается наз  $K$   
(как поле) эл-ми  $u_1, \dots, u_n$ .

Расширение  $L$  поля  $K$  наз-ся **простым**, если  
 $L = K(u)$  для некоторого  $u \in L$ .

Расширение  $L$  поля  $K$  наз-ся **конечным**, если  
 $\dim_K L < \infty$ , т.е.  $L$  конечномерно как в.ч.над  $K$ .  
Обозн:  $[L:K] = \dim_K L$  — **степень расширения**

Мы начнем с очевидного, но в некотором смысле универсального примера получаем конечных расширений поля.

Напомним, что фактор-кольцо  $A/I$  — поле  $\Leftrightarrow I$  — макс. идеал.

Т. 1 Пусть  $h \in K[x]$  неразложим,  $\deg h = n$ .

Тогда  $L = K[x]/(h)$  — конечное простое алгебр. расширение поля  $K$ , причем  $\dim_K L = n$ .

Д-во: 1)  $h$  неразл  $\Rightarrow (h)$  — макс. идеал  $\Rightarrow$   
 $\Rightarrow L$  — поле.

2)  $K[x] - \text{PID} \Rightarrow \forall u \in L : \exists a_0, \dots, a_{n-1} \in K :  
u = a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + (h) \Rightarrow$  см. классы:

$$u_0 = 1 + (h), u_1 = x + (h), \dots, u_{n-1} = x^{u_1} + (h) - \text{дальше}$$

б.н.  $L$  над  $K \Rightarrow \dim_K L = n$ , т.е.  $L$ -кон.расширение.

3)  $\forall u \in L \exists f \in K[x]: u = f(u_1)$ , где  $u_1 = x + (h) \in L$ ,  
т.е.  $L = K[u_1] = K(u)$  — простое расширение

4) т.к.  $h(u_1) = 0$ , то  $L$ -алгебр.расширение  $\square$

Если ж-т  $u \in L$  алгебр.над  $K$ , то  $\exists$  нераз-  
м-н  $h \in K[x]: K[u] \simeq K[x]/(h)$ . Мин-н

$h = m_u$  — **минимальный полином** для  $u$ , а

$\deg m_u$  — **степень** алгебр.анчиского ж-та  $u$ .

Т. 2 Элемент  $u \in L$  алгебраич. над  $K \Leftrightarrow$   
 $K[u]$  — к.м. б.н. над  $K$ . В этом случае  $K[u] = K(u)$  —

- поле и  $|K(u):K|$  равна степени  $n$  над  $K$ .

Л-во:  $\Leftrightarrow \dim_K K[u] < \infty \Rightarrow \exists n \in \mathbb{N}$ :

$u^n$  лев. вып-ся через  $1, u, \dots, u^{n-1}$  над  $K \Rightarrow$   
 $u$  алгебраичен над  $K$ ,


$\Rightarrow$ ) Рас-м лев-зм  $\varphi: K[x] \rightarrow L, f(x) \mapsto f(u)$ .

$\text{Im } \varphi = K[u]$ , а  $\text{Ker } \varphi = (m_u)$ . - идеал, порожд.

лев. лев-зом  $m_u$  эн-га  $u$  и  $\deg m_u = n$ .

Сл-но,  $K[u] \cong K[x]/(m_u)$ . Лев-и  $m_u$

выразл. над  $K$ , сл-но по т-1  $K[u]$ -поле

и  $\dim_K K[u] = n$ . В частности,  $K(u) = K[u]$  

(последнее рав-во, феномен ушлого некий управ-ств  
в знаменателе")

Следствие Кансово конечное расширение поля  
явл-ся алгебраическим.

Примеры 1) Пусть  $a \in K$  не квадрат, т.е.  $\nexists b \in K: b^2 = a$ .

Поле  $L = K[\sqrt{a}] = K(\sqrt{a})$ , полученное присоединением  
к  $K$  корня мн-ка  $x^2 = a$  явл-ся **квадратичным**  
расширением поля  $K$ , т.е.  $[L:K] = 2$ . В частности,  
 $\mathbb{C} = \mathbb{R}[\sqrt{-1}]$ .

2) Пусть  $p$ -простое. Мн-к  $\Phi_{p-1}(x) = x^{p-1} + \dots + x + 1$  нераз-  
ложим над  $\mathbb{Q}$  (пример 3.6.2 из [Вук])  $\Rightarrow \varepsilon_p = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p}$   
комп. корень  $p$ -ой ст. из 1 — это корень  $\Phi_{p-1}(x) \Rightarrow$   
 $\mathbb{Q}[\varepsilon_p]$  — поле и  $[\mathbb{Q}[\varepsilon_p]: \mathbb{Q}] = p-1$ ,  $\mathbb{Q}[\varepsilon_p]$  наз-ся  
**круговым полем или полем деления круга**.



Т.3 Если  $M$  - кон. расщ. поля  $K$ , а  $L$  - кон. расщ. поля  $M$ ,  
то  $L$  - кон. расщ. поля  $K$  и  $|L:K| = |L:M| |M:K|$ ,

Δ-во: Если  $e_i, i=1..m$ , и  $f_j, j=1..n$ , - базисы  
соотв. расширений, то  $e_i f_j$  - базис расщ.  $L$  над  $K$   $\square$

Упр 1 Проверьте последнее утверждение в Δ-во Т.3.

Т.4 Если  $L = K(u_1, \dots, u_n)$  и все  $u_1, \dots, u_n$   
алгебраичны над  $K$ , то  $L$  - кон. расщ. поля  $K$ .

Δ-во:  $K(u_1, \dots, u_n) = K(u_1, \dots, u_{n-1})(u_n)$ . Индук-  
цией по  $n$  можно считать, что  $M = K(u_1, \dots, u_{n-1})$  - кон.  
расщ. поля  $K$ . Так  $u_n$  алгебр. над  $K$ , то  $u_n$  - алг. над  $M$   
по Т.2  $\Rightarrow |M(u_n):M| < \infty$ . По Т.3  $L$  - кон. расщ. поля  $K$   $\square$

Поле  $K$  **алгебраически замкнуто** в своем расшире-  
нии  $L$ , если любой эл-т  $\alpha \in L$  алгебр. над  $K$   
лежит в  $K$ .

Т. 5 Пусть  $L$ -расшир. поля  $K$  и  $\overline{K} = \{ \alpha \in L \mid \alpha \text{ алг. над } K \}$   
Тогда  $\overline{K}$  - поле, алг. замкнутое в  $L$  (оно наз-ся  
**алгебр. замыканием** поля  $K$  в поле  $L$ ).

Л-во: см л-во т. 9.5.3 из [Вик]  $\square$

Пример Поле всех алгебр. чисел  $\overline{\mathbb{Q}}$  - это алг.  
замыкание поля  $\mathbb{Q}$  в поле  $\mathbb{C}$ .

Упр 2 а) Поле  $\overline{\mathbb{Q}}$  алгебр. замк. (в абсолютном смысле  
как и поле  $\mathbb{C}$ ) б) Каждое кон. расшир. поля  $\overline{\mathbb{Q}}$   
наз-ся **полем алг. чисел** и изоморфно полному в  $\overline{\mathbb{Q}}$ .


Гомоморфизмы расширений поля  $K$ , то называется **гомоморфизмами над  $K$** .

Два расширения  $L$  и  $L'$  поля  $K$  **изоморфны над  $K$**  (эквивалентны как  $K$ -расширения), если  $\exists$  из-зм  $\varphi: L \rightarrow L'$  над  $K$ , т.е. такой, что  $\varphi|_K = \text{id}_K$ .

Т. 6. Пусть  $L = K(u)$  и  $L' = K'(u')$  — простые расширения поля  $K$ . Тогда  $L$  и  $L'$  изом. над  $K \Leftrightarrow$  либо  $u$  и  $u'$  трансцендентны над  $K$ , либо  $u$  и  $u'$  — корни одного и того же неразл. мн-на из  $K[x]$

Д-во: Если  $u$  трансцен., то  $f(u) \neq 0 \forall f \in K[x] \Rightarrow K(u) \simeq K(x) = \mathbb{Q}(K[x])$  — поле рац. ф-ций над  $K$ .

В частности  $|K(u) : K| = \infty$  и  $K(u) \simeq K(u') \Leftrightarrow u'$  тоже трансцендентен.

Если  $\pi$  алгебр. над  $K$ , то идеал  $(m_\pi)$  определен однозначно неразл. лев-пол  $m_\pi$  на-та  $\pi$ . Поэтому отображение  $\varphi: K[x]/(m_\pi) \rightarrow K(\pi)$ ,  $\sum_{i=0}^{n-1} a_i x^i + (m_\pi) \mapsto \sum_{i=0}^{n-1} a_i \pi^i$ , изоморфизм (см. т. 1), причем в числ 0-ст.  $a_0 + (m_\pi) \xrightarrow{\varphi} a_0 \in K \leq L$ . Очевидно, что  $m_\pi$ -лев-пол. лев-пол  $\pi$  и  $\pi$  в  $K[x]/(m_\pi)$ . Поэтому  $L(\pi) \cong L(\pi') \Leftrightarrow L(\pi') \cong K[x]/(m_\pi) \Leftrightarrow (m_\pi) = (m_{\pi'})$  

Пр 2 Рассечение  $L$  поля  $K$  наз-ся **полем разло-  
мения** лев-пол  $f \in K[x]$ , если  $f$  разлагается в  $L[x]$  на линейные лев-пол  $\pi$  и  $L$  порожд. над  $K$  ево корнями.

Теорема 7 Поле разложения мн-н  $f \in K[x]$  существует и единственно (точность до изоморфизма  $K$ ).

о продолжении гомоморфизма

Лемма Пусть  $P(\alpha)$  — расширение поля  $P$ ,  $h = m_\alpha \in P[x]$  — мин. мн-н  $\alpha$  над  $P$ . Пусть  $\varphi: P \rightarrow F$  — гом-зм поля  $P$  в поле  $F$ . Тогда гом-зм  $\varphi$  продолжается до гом-зма  $\psi: P(\alpha) \rightarrow F$  ровно столько способами, сколько разл. корней в  $F$  имеет мн-н  $h^\varphi$  — образ  $h$  в  $F[x]$ .

Д-во: Если  $\psi$  существует, то задается  $\psi$ -ом:

$$(a_0 + a_1 \alpha + \dots + a_m \alpha^m)^\psi = a_0^\varphi + a_1^\varphi \beta + \dots + a_m^\varphi \beta^m, \text{ где } \beta = \alpha^\varphi \in F(x)$$

Гл-венная (\*) к ф-л-е  $h(\alpha) = 0$ , имеет  $h^\varphi(\beta) = 0$ .


Обратно, если  $\beta \in F$  и  $h^\varphi(\beta) = 0$ , то ф-л-а (\*) корректно задает гом-зм  $\psi: P(\alpha) \rightarrow F$ .

Лемма 1. Теорема 1: Р-м поле-ть расширения

$$K = K_0 \subset K_1 \subset \dots \subset K_{s-1} \subset K_s = L$$

В которой  $K_i$  получается из  $K_{i-1}$  присоединением корня мн-ля  $f_i$  мн-ля  $f$  степени  $> 1$  и неразл. над  $K_{i-1}$ . Ясно, что этот процесс не может быть бесконечным. Пусть  $L = K_s$  - последний член этой послед-сти. По построению  $L$ -поле разложения мн-ля  $f$ .

Пусть  $\tilde{L}$  - еще одно поле разложения. Построим по-з-му  $\varphi_i: K_i \rightarrow \tilde{L}$ ,  $i = 0, 1, \dots, s$  так, чтобы  $\varphi_0 = \text{id}_K$  и  $\varphi_i|_{K_{i-1}} = \varphi_{i-1}$ . Согласно лемме,  $i$ -й шаг возможен, если  $\tilde{f}_i = f_i^{\varphi_{i-1}}$  имеет корень в  $\tilde{L}$ . Мн-я  $f_i | f$  в  $K_{i-1}[x] \Rightarrow \tilde{f}_i | f$  в  $\tilde{L}[x]$ , но  $f$  раскл.

на мн. мн-м в  $\tilde{L}[x] \Rightarrow \tilde{f}_i$  имеет корень в  $\tilde{L}$ .  
Поэтому  $\varphi_i$  сну-ют  $\forall i=0, \dots, s$ . Последний из  
мнх  $\varphi = \varphi_s: L \rightarrow \tilde{L}$  явл-ся изоморфизмом, т.к.  
из сур-я поля разл. вытекает, что оно мультипли-  
кативное поле с зад. свойствами. 

Упр 3 Постройте поля разл. мнх  $M$  и  $L$  над  $\mathbb{Q}$   
мн-ков  $x^3 - 1$  и  $x^3 - 2$  соот-но; убедитесь, что  
 $|M: \mathbb{Q}| = 2$  и  $|L: \mathbb{Q}| = 6$ .

Изомисл. теперь выразу, как некоторые  
из наших рез-тов о расширениях полей могут  
быть обобщены на расширения Гётефовых полей.

Далее возьм  $B$  - расширение поля  $A$ .

Опр 3 Элемент  $u \in B$  наз-ся **целым** (целым алгебраическим) над  $A$ , если  $\exists h \in A[x]$  со свод. коэф-том  $1: h(u) = 0$ .  
Очевидно, что а)  $u \in A$  цел над  $A$ ; б) если  $u \in B$  алгебр. над  $A$ , то  $\exists$  ненул.  $a \in A: au$  целым над  $A$ .

Кольцо  $B$  наз-ся **целым** над  $A$  (**целым расширением** кольца  $A$ ), если все его эл-ты целы над  $A$ .

Зам Если  $A$  — поле, то целым = алгебраическим.

Опр 4 Расширение  $B$  кольца  $A$  **конечно**, если  $B$  — к.п.  $A$ -модуль.

След. теорема 8-11 — аналог лем 2-5. Для  $u \in \Delta$ -ВА надо заметить слово "базис" на св. порожд. модуля и т.ч. о базисе в 7-м § 9.4.1 (см. АН-54).



Т. 8  $\exists n \in \mathbb{N}$  и  $\chi \in B$  цел. из  $A \Leftrightarrow A[\chi]$  - к.п.  $A$ -модель

След. Кон. расщ. нётерова кольца - целое

Т. 9  $|A:C| = |A:B|/|B:C|$ , где  $A \supseteq B \supseteq C$ .

Т. 10 Если  $B$  нормал. из  $A$  конечным числом  
целых  $\exists n$ -тов, то  $B$ -конечное расщ. кольца  $A$ .

Зам. Кон. нор. (и тем более конечное) расщ. нётерова  
кольца снова нётерово.

Т. 11 Пусть  $B$ -расширение нётерова кольца  $A$ . Совокупность

$\bar{A}$  всех  $\exists n$ -тов кольца  $B$ , целых из  $A$ , явл-ся  
подкольцом, **целое замыкание** в  $B$  (т.е. если  $\chi \in B$   
цел из  $\bar{A}$ , то он лежит в  $\bar{A}$  и, значит, явл-ся целым из  $A$ ).

Кольцо  $\overline{A}$  наз-ся **целым замыканием**  $A$  в  $B$ .

Пример  $\overline{\mathbb{Z}}$  - все целые алгебр. числа - по-прежнему в поле  $\overline{\mathbb{Q}}$  всех алг. чисел. При этом  $\mathbb{Q}(\overline{\mathbb{Z}}) = \overline{\mathbb{Q}}$ .

Т.12 Пусть  $A$  - целостное целостное в своем поле отношений  $K$  Гёте-Рова кольцо,  $L$  - кон. расщ. поля  $K$  и  $B$  - целое замыкание  $A$  в  $L$ . Предп. что  $\text{char } K = 0$ . Тогда  $B$  - кон. расширение кольца  $A$ , (см. рис 1).  $A$  - во: см. д-во Т. 9.5.12 из [Вин],

Пример  $\mathbb{Q} \leq K \leq \overline{\mathbb{Q}}$  и  $\mathbb{Z}/K$  - целое зам.  $\mathbb{Z}$  в  $K$  (наз-ся **кольцо целых чисел** поля  $K$ ). Из Т.12  $\Rightarrow \mathbb{Z}$  - к.и. ад. зр. и не имеет кручения  $\Rightarrow \mathbb{Z}_K \cong \underbrace{\mathbb{Z} \otimes A}_{\text{наз-ся}} A \otimes \mathbb{Z}$ . Т.к.  $\forall u \in K \exists a \in K$ :  $au \in \mathbb{Z}$ , то  $\text{rk } \mathbb{Z}_K = \dim_{\mathbb{Q}} K$ . **наз-ся** (см. также зам 2 и 3 из § 9.5 [Вин])