

5. Основная теорема теории Галуа и её приложения

Пусть поле L - расщ. поля K и $|L:K| = n$.

Опр 1 Пусть $H \leq \text{Aut}_K L$ и $L \supseteq P \supseteq K$. Положим

$$P^H = \{ \alpha \in P \mid \alpha^h = \alpha \ \forall h \in H \}$$

$$H_P = \{ h \in H \mid \alpha^h = \alpha \ \forall \alpha \in P \}$$

Предп 1 а) P^H - нормальное поле P , содержащее K ;

б) $H_P \leq H$. Упр 1 $\Delta \rightarrow \Pi$ предп 1.

Основная т.ма Галуа говорит о соответствии между подгруппами $\text{Aut}_K L$ и нормальными полями L , содержащими K .
В случае, когда L - расщ. Галуа. По началу мы не будем этого предполагать.

Т. 1 Пусть L - сепарабельное расширение по полю K ,
 $H \leq \text{Aut}_K L$. Тогда $L^H = K \Leftrightarrow |H| = n (= |L:K|)$.

Кроме того, \forall полей $P, Q: K \leq P \leq Q \leq L$,
каждый n -ом-3м $\varphi: P \rightarrow L$ над K продолжается
до n -ом-3м $\psi: Q \rightarrow L$ ровно $\dim_P Q$ способами.

Л-во: \Leftarrow) Согласно вып 1, $H \leq \text{Aut}_{L^H} L \Rightarrow$

$|H| \leq |L: L^H| \leq |L: K| = n$. Поэтому если

$|H| = n$, то $|L: L^H| = |L: K| \Rightarrow K = L^H$.

\Rightarrow) Пусть $L^H = K$. $\forall \alpha \in L$ пусть $\alpha^H = \{\alpha_1, \dots, \alpha_m\}$.

H -орбита n -ра α . Тогда $f(x) = \prod_{i=1}^m (x - \alpha_i) \in L^H[x] = K[x]$ —
— мин. мн-н α над K .
(Т-ма о сирм. мн-н α !)

По построению $f(x)$ разл. на мин. мн-ли над L ,
 Т.к. исходное сепарабельно, то расширение Q над P
 тоже. По теореме о примитивном элементе (т. 11.4.3.
 см. фрейл AN-74) $Q = P(\alpha)$ — простое расширение
 пусть $h \in P[x]$ — минимальный мн-л для α над P .
 Тогда в кольце $P[x]$ $h \mid f$, где f — мин. мн-л для
 α над K . Сл-но, $h^\varphi \mid f$ в кольце $P^\varphi[x]$
 (φ — гом-зм из условия т-мы!) \Rightarrow раскл. на разл.
 мин. мн-ли в $L[x]$, по лемме о продолжении
 гом-зпа (AN-71), φ продолжается до φ поля
 $\deg h^\varphi = \deg h = [Q:P]$ по свойствам. Применяя это
 к $P=K$ и $Q=L$ имеем $|Aut_K L| = n$.

Осталось доказать, что $L^H = K \Rightarrow H = \text{Aut}_K L$.

Пусть $g \in \text{Aut}_K L$. Тогда $\forall \alpha \in L$ αg будет корнем мин. мн-на $f(x) \in K[x]$ (ср. выше). С-но,
 $\exists h \in H : \alpha g = \alpha h$.

Если поле L конечно, то взяв $\alpha \in L$ так, что $L^* = \langle \alpha \rangle$ имеем $\alpha g = \alpha h \quad \forall \alpha \in L \Rightarrow h = g \Rightarrow H = \text{Aut}_K L$.

Если поле L бесконечно, то $\forall h \in H$ рассмотрим $L_h = \{ \alpha \in L : \alpha g = \alpha h \}$ — подгр-па в L . Из доказательства $\Rightarrow L = \bigcup_{h \in H} L_h$. Поэтому достаточно показать, что $\exists h \in H : L = L_h$. Это вытекает из след. леммы:

Лемма Конечное в.п. над беск. полем не может
быть изоморфно конечным числом собствен. подгр-в.

1.30: Лемма 10.6.1 из [ВЧН] \square

Тут теперь L -расширение Галуа поля K ,
т.е. порядок $G = \text{Gal}(L/K) = \text{Aut}_K L$ равен
 $n = |L:K|$, тут $K \leq P \leq L$ и $H \leq G$, и в соот.
с опр 1: $L^H = \{ \alpha \in L : \alpha^h = \alpha \ \forall h \in H \}$ и
 $G_P = \{ g \in G : \alpha^g = \alpha \ \forall \alpha \in P \}$.

Т. 2 (Основная теорема теории Галуа)

От-я $P \mapsto G_P$ и $H \mapsto L^H$ взаимно обратны, т.е.
 $L^{G_P} = P$ и $G_{L^H} = H$ (*)

и, таким образом, устанавливает в.з. соотнош.
соответствие между лн-вами подполей поля L ,
содержащихся K , и подгруппами G . В частности,

$$|G_P| = |L:P| \text{ и } |L:L^H| = |H| \quad (**)$$

При этом подполям P , являющимся расширениями
Галуа поля K , соответствуют нормальные под-
группы H группы G , и наоборот.

Л-во: В силу т. 1 число $|G_P|$, равное числу
автоморфизмов поля L , по ис. к P , равно
числу способов продолжить тождеств. вложение
 $\varphi: P \rightarrow L$ до автоморфизма $L \rightarrow L$, а значит
равно $|L:P| \Rightarrow |G_P| = |L:P|$.

Пологая $L^H = K$ в Т. 1, имеем $|L: L^H| = |H|$,
и (***) полностью доказано.

Из опр-я \underline{G}_P вытекает $P \leq \underline{G}_P$. Применяя
(**), выводим $|L: P| = |\underline{G}_P| = |L: \underline{G}_P| \Rightarrow P = \underline{G}_P$.
Аналогично, $H \leq \underline{G}_H$ и $|H| = |L: L^H| = |\underline{G}_H| \Rightarrow H = \underline{G}_H$.

Слова из Т. 1 все авт-зми поля P над K
проходятся до авт-зми поля $L \Rightarrow P$ -расши-
рение Галуа поля $K \Leftrightarrow$ все n -н пр. G , переводя-
щие P в себя, инд. на нем ровно $|P: K|$ раз. авт-зми

Но $|P: K| = \frac{|L: K|}{|L: P|} = |\underline{G}: \underline{G}_P|$. Поэтому P -расшир.

Галуа поля $K \Leftrightarrow$ все n -н пр. G переводят P в себя.

Т.к. $P = L^H$, где $H = \underline{G}_P$, то $P^g = L^{H^g}$. Поэтому

$$P^g = P \Leftrightarrow H^g = H, \text{ т.е. } H \trianglelefteq G \quad \blacksquare$$

Следствие Если $K \leq P_1 \leq P_2 \leq L$, то

$$G = G_K \geq G_{P_1} \geq G_{P_2} \geq G_L = 1. \text{ И наоборот,}$$

$$\text{если } 1 \leq H_1 \leq H_2 \leq G, \text{ то } L = L^1 \geq L^{H_1} \geq L^{H_2} \geq L^G = K.$$

Зам. Соотв. к Лемме обращения Вейля!

Пример Пусть φ - абт-зм Φ -пространства поля Галуа \mathbb{F}_{p^n} .

Тогда $G = \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}) = \langle \varphi \rangle_n$ - цикл. группа
 порядка n . Если $H \leq G$, то $H = \langle \varphi^m \rangle_{n/m}$ - цикл.
 подгруппа порядка n/m . L^H - это минимальное поле
 абт-зма $\varphi^m \Rightarrow |L : L^H| = m \Rightarrow L^H \cong \mathbb{F}_{p^m}$.

Упр 2 Описать решетку нормировки \mathbb{Q} и найти базу
 для \mathbb{Q} -м-н $f(x)$, а затем решетку нормировки, лежащих
 над \mathbb{Q} полей разложения $f(x)$ и \mathbb{Q} , если
 а) $f(x) = x^3 - 2$ б) $f(x) = x^4 - 2$ в) $f(x) = x^p - 2$ а
 p — простое.

Опр 2 Это 2 расширения поля K **известная-**
есть в радикалах (соот. в квадратичных радикалах)
 если 2 впр-ся через n -н поля K при помощи
 арифм. операций и извлечения корней (соотв.
 квадратичных корней). Иными словами, $\exists S \subseteq \mathbb{N} : \alpha \in K_S$
 (**) $K = K_0 \leq K_1 \leq \dots \leq K_{S-1} \leq K_S$, где $K_i = K_{i-1}(\alpha_i)$
 и $\alpha_i^{n_i} \in K_{i-1}$ для $n_i \in \mathbb{N}$ (соот. $\alpha_i^2 \in K_{i-1}$), $i = 1 \dots S$.

Предл 2 Если $f(x)$ неразл. в $K[x]$ и хотя бы один его корень представл. в радикалах (кв. рад) над K , то и остальные его корни обл. этим св-вом.

Д-во: Т.к. $f(x)$ неразл., то гл. м.д.н. его корней α и β найдётся авт-зм $\varphi \in \text{Aut}_K L$ (L -поле разл. f): $\alpha^\varphi = \beta$. Тогда φ -из-зм над K поля $K(\alpha)$ в $K(\beta)$, поэтому β обл. тем же св-м, что и α . \square

Опр 3 Авт. уравнение $f(x) = 0$, где $f \in K[x]$, **разрешимо в радикалах** (в кв. рад. радикалах) над K , если каждый его корень обл. этим св-вом, экв-но, поле разл. $f(x) \subseteq$ поле, получ. чисел. корней (***).

Т.3 Пусть f нераз. мн-к над полем K , $\text{char } K \neq 2$,
 и L — его поле разложения над K . Тогда $f(x) = 0$ раз-
 решимо в кв. радикалах над $K \Leftrightarrow |L:K| = 2^n$ ($n \in \mathbb{N}$).
 Д-во: \Rightarrow) Пусть $f(x) = 0$ разр. в кв. радикалах, т. е.
 существует цепочка расширений $(\times \times \times)$: $L \subseteq K_s$,
 где $|K_i:K_{i-1}| = 2$, $i = 1 \dots s$. Имеем $|L:K| \mid |K_s:K| = 2^s$
 \Leftarrow) Пусть $|L:K| = 2^n$. Тогда $\forall \alpha \in L$ $\deg m_\alpha = 2^t$, т. к.
 $m_\alpha \mid |L:K|$. По лемме 11.4.1 (из АН-74) L separabelно
 над K . По пред. 11.4.3 оно нормально и, сл-но,
 по т. 11.4.4 $\Rightarrow L$ — расширение Галуа над K .
 Поэтому группа $G = \text{Gal}(L/K)$ определена и

$|G| = 2^n$. Т.к. G — 2-группа, то G разрешима (по
 т. 10.3.5, см. АН-63). Значит, по л. Жоржиса-Белзаре
 она разр. композиционным рядом (т. 10.4.3, см. АН-64),
 $G = G_0 \geq G_1 \geq \dots \geq G_s = 1$ и $|G_i/G_{i+1}| = 2, i = 0 \dots s-1$.
 Положим $K_i = G_i$, в силу сим. т.м. Галуа имеем
 $K = K_0 \leq K_1 \leq \dots \leq K_s = L$, где $|K_i : K_{i+1}| = 2, i = 0 \dots s-1$.
 Т.к. $|K(\alpha) : K| = 2$ значит, что $\exists a \in K : \alpha^2 = a$, то
 $f(x)$ разрешима в абстр. радикалах \square

Оказывается, что задача о построении отрезка
 с помощью циркуля и линейки может быть

связана к проблеме представления числа $\alpha \in \mathbb{R}$ в кв. радиклах над $K = \mathbb{Q}(a_1 \dots a_k)$, где $a_i \in \mathbb{R}$.

В частности, если α трансцендентно над K , то задача, очевидно, неразрешима. Например, Франсуа число π означает неразрешимость "кв. деления круга".

Пример задачи "удвоения куба" сводится к построению отрезка длины $\sqrt[3]{2}$. Т.к. $x^3 - 2$ непр. над \mathbb{Q} и гл. его поля разл. L вт-ся $|L:\mathbb{Q}| = 6 \neq 2^n$, то и эта задача неразрешима.

Упр 3 Является разрешимой "задача отрисовки угла"?
а) $\alpha = 45^\circ$ б) $\alpha = 60^\circ$ в) В общем случае?

Т. 4' (король d-бот-мн ателорх) Тона C ан. замкн,

1-во: мы уже знаем, что

(1) $f(x) \in \mathbb{R}[x]$ и $\deg f$ нечетно, то $\exists \alpha \in \mathbb{R} : f(\alpha) = 0$

(2) $\forall \alpha \in \mathbb{C} \exists \beta \in \mathbb{C} : \alpha = \beta^2$ — в поле \mathbb{C} возм.
извлечение кв. корня

Из (1) \Rightarrow в любом \mathbb{R} нет корня расщ. нечетной степени (имеет $\exists \alpha : \deg m_\alpha$ нечетна и > 1 , что невозможно)

Аналог, если \mathbb{C} не алг. замкн., то $\exists f(x) \in \mathbb{R}[x]$ неразр. над $\mathbb{C} : \deg f > 1$ (см. § 5.5 из [ВЛМ]).

Тогда L — поле разра $f(x)$ над \mathbb{R} и $G = \text{Gal}(L/\mathbb{R})$
(L — норм. как поле разра. и следовательно, га что $L = \mathbb{C}$).

Тогда. Снова $\exists H \in \text{Syl}_2(G)$, P -м поле $K = \mathbb{Z}^H$,
 Так. $|K : \mathbb{R}| = \frac{|L : \mathbb{R}|}{|L : K|} = \frac{|G|}{|H|}$ - нечетное число, то

$K = \mathbb{R} \Rightarrow |G| = |H| \Rightarrow G$ - 2-группа. По т. 3
 поле L получено из поля \mathbb{R} некотор. присоедине-
 нием кв. радикалов, но тогда из (2) $\Rightarrow L = \mathbb{R}_{\text{ин}} \mathbb{C}$,
 $\Rightarrow f(x)$ имеет корни в \mathbb{C} \square

Ост. результат Э. Галуа (1830) таков:

т. 5 Пусть f неразл. мн-к над полем K и пусть
 хар-ки n и L -его поле разложения над K . Ч-е
 $f(x) = 0$ разрешимо в радикалах над $K \Leftrightarrow$
 $G = \text{Gal}(L/K)$ разрешима.

Док-зо: (отдельно)

По **общему уравнению** (многочлену) n -ой степени подматсся ур-е

$$f(x) = x^n + a_n x^{n-1} + \dots + a_{n-1} x + a_n,$$

Коэф-ты которого a_1, \dots, a_n рассматриваются как эл-ты поля $K = k(a_1, \dots, a_n)$ разг. функ-ей от n незав. переменных над некоторым полем k .

Пусть L - поле разложения f над K и $x_1, \dots, x_n \in L$ его корни. По ф-лам Виета $a_k = (-1)^k \sigma_k$, где σ_k - k -й элем. сим. мн-н от x_1, \dots, x_n . Сл-но, $L = K(x_1, \dots, x_n) = k(x_1, \dots, x_n)$. Поскольку $K \leq L$ и степень

Трансцендентно сои K над k (не алгебры)
 $\text{tr. deg } K = \text{tr. deg } k(a_1, \dots, a_n) = n$, со и
 $\text{tr. deg } L = n$, т.е. x_1, \dots, x_n алгебр. незав.
 над k . В частности, x_1, \dots, x_n различны, т.е.
 f сепарабелен и L -расширение Галуа над K .
 Любая перестановка корней x_1, \dots, x_n опре-
 авт-зм поля L , т.е. элемент σ из K (т.е. σ_k
 не меняется при перестановке). Сл-но, $\text{Gal}(L/K) \cong S_n$.

Следствие 1 Общее ур-е $f(x) = 0$ степени n
 разрешимо в радикалах $\Leftrightarrow n \leq 4$.

Д-во: $\text{Gal}(L/K) \cong S_n$ и S_n -разр $\Leftrightarrow n \leq 4$ \square .

Следствие 2 $k(x_1, \dots, x_n)^{S_n} = k(\sigma_1, \dots, \sigma_n)$ — озн-ия о
 симм. мн-ств.