Теория Галуа

Напомним, что расширение полей называется *расширением Галуа*, если оно нормально и сепарабельно. *Группой Галуа* расширения $\mathsf{k} \subset K$ называется группа автоморфизмов K, постоянных на k.

Теория Галуа устанавливает соответствие между промежуточными полями в расширении Галуа и подгруппами в группе Галуа этого расширения. Её основное утверждение – следующая

Теорема 1 (основная теорема теории Галуа). *Пусть $\mathsf{k} \subset K$ – конечное расширение Галуа. Тогда между множеством подгрупп в группе Галуа $G = Gal(K, \mathsf{k})$ и множеством промежуточных расширений $\mathsf{k} \subset F \subset K$ есть взаимно обратные биекции:*

$$\begin{tikzcd} \{H \mid H \subset G\} \arrow[r, bend left, "H \mapsto K^H"] & \{F \mid \mathsf{k} \subset F \subset K\}. \arrow[l, bend left, "F \mapsto Gal(K,F)"] \end{tikzcd}$$

А именно, подгруппе $H \subset Gal(K, \mathsf{k})$ отвечает поле инвариантов

$$K^H = \{\alpha \in K \mid \forall \sigma \in H \ \sigma(\alpha) = \alpha\},$$

а подполю F соответствует подгруппа

$$Gal(K, F) = \{\sigma \mid \forall \alpha \in F \ \sigma(\alpha) = \alpha\} \subset G.$$

Заметим, что для любого промежуточного поля $\mathsf{k} \subset F \subset K$ расширение K/F – расширение Галуа. Оно нормально потому, что K есть поле разложения некоторого семейства многочленов из $\mathsf{k}[x]$, а значит, и некоторого семейства многочленов из $F[x]$ (того же самого). Оно сепарабельно, это было доказано на прошлой лекции.

Для доказательства теоремы нам понадобится

Лемма 2. *В обозначениях основной теоремы теории Галуа*

$$|Gal(K, F)| = [K : F] \qquad \text{и} \qquad [K : K^H] = |H|.$$

Доказательство. Первое равенство было доказано на прошлой лекции. Для доказательства второго нам понадобится лемма о примитивном элементе (её мы докажем позже). Она утверждает, что любое конечное сепарабельное расширение полей порождено одним элементом. Пусть K порождено над k (а значит, и над K^H) одним элементом α. Рассмотрим многочлен $f(x) = \prod_{\sigma \in H}(x - \sigma(\alpha))$. Группа H переставляет корни f, поэтому f неподвижен относительно H, т.е. $f \in K^H[x]$. При этом α – корень f, поэтому $[K : K^H] = \deg_{K_H} \alpha \leqslant \deg f = |H|$. С другой стороны, H – подгруппа в группе Галуа $Gal(K, K^H)$, значит $|H| \leqslant |Gal(K, K^H)| = [K : K^H]$ по первому равенству леммы. Получаем, что $|H| = [K : K^H]$. ☐

Доказательство основной теоремы теории Галуа. Во-первых, покажем, что $K^{Gal(K,F)} = F$. Очевидно, что $F \subset F_1 = K^{Gal(K,F)}$ и что $Gal(K, F_1) \supset Gal(K, F)$. Если при этом $F \neq F_1$, то $[K : F] > [K : F_1] = |Gal(K, F_1)| \geqslant |Gal(K, F)| = [K : F]$ – противоречие (здесь мы пользовались первым равенством леммы 2).

Во-вторых, покажем, что $Gal(K, K^H) = H$. Очевидно, что $H \subset H_1 = Gal(K, K^H)$ и что $K^{H_1} \supset K^H$. Если при этом $H \neq H_1$, то $|H| < |H_1| = [K : K^{H_1}] \leqslant [K : K^H] = |H|$ – противоречие (здесь мы пользовались вторым равенством леммы 2). ☐

Основная теорема устанавливает связь между подполями и подгруппами только для расширений Галуа. Если же нужно описать подполя для расширения $\mathsf{k} \subset K$, которое не нормально, то это можно сделать, перейдя к большему расширению Галуа $\mathsf{k} \subset L$, где L содержит K. При этом подполя в K соответствуют тем подгруппам в $Gal(L, \mathsf{k})$, которые содержат $Gal(L, K)$.

Лемма 3. *Пусть $\mathsf{k} \subset K$ – конечное сепарабельное расширение. Тогда существует такое расширение $K \subset L$, что L/k – конечное расширение Галуа.*

Доказательство. Можно считать, что K вложено в $\bar{\mathsf{k}}$. Пусть K порождено над k элементами $\alpha_1, \ldots, \alpha_n$, а $f_i \in \mathsf{k}[x]$ – минимальные многочлены для α_i. Пусть $L \subset \bar{\mathsf{k}}$ – поле разложения семейства многочленов f_i, т.е. поле, порождённое всеми корнями всех f_i. Тогда L/k конечно (так как порождено конечным числом корней), нормально (так как это поле разложения семейства многочленов) и сепарабельно (так как все элементы α_i, а значит и все многочлены f_i и все корни всех f_i сепарабельны над k). Т.е. поле L – искомое. $\square$

Лемма 4. *Пусть $\mathsf{k} \subset K$ – конечное сепарабельное расширение. Тогда существует лишь конечное число промежуточных полей $\mathsf{k} \subset F \subset K$.*

Доказательство. Согласно предыдущей лемме, можно, расширив K, считать, что $\mathsf{k} \subset K$ – конечное расширение Галуа. В таком случае утверждение следует из основной теоремы теории Галуа и из того, что в группе Галуа $Gal(K, \mathsf{k})$ лишь конечное число подгрупп. $\square$

Лемма 5 (о примитивном элементе). *Пусть $\mathsf{k} \subset K$ – конечное сепарабельное расширение. Тогда K порождено над k одним элементом.*

Доказательство. Рассмотрим два случая: k конечно и k бесконечно.

В первом случае K также конечно и в качестве порождающего элемента можно взять образующий группы K^* (как известно, она циклическая).

Во втором случае предположим противное – для любого элемента $\alpha \in K$ порождённое им поле $\mathsf{k}[\alpha]$ отлично от K. Тогда получится, что собственные подпространства $\mathsf{k}[\alpha]$ конечномерного над k векторного пространства K полностью его покрывают. При этом этих подпространств по лемме 4 конечное число. Несложно убедиться, что в случае бесконечного поля k такого не бывает. $\square$

Нужно заметить: логически замкнутого круга в проведённых рассуждениях нет. При доказательстве леммы 4 использовалась лишь та часть основной теоремы теории Галуа, где утверждается, что разным подполям отвечают разные подгруппы. Но при доказательстве этой части теоремы (т.е. того, что $F = K^{Gal(K,F)}$) мы не пользовались леммой о примитивном элементе, а использовали лишь известное ранее равенство $|Gal(K, F)| = [K : F]$.

Соответствие Галуа обладает замечательными свойствами, которые собраны ниже. Оно позволяет переводить утверждения о полях на язык групп и наоборот.

Определение 6. *Композитом* двух подполей F_1, F_2 некоторого поля K называется подполе, порождённое F_1 и F_2. Обозначение: F_1F_2.

Предложение 7. *Пусть* $\mathsf{k} \subset K$ *– конечное расширение Галуа,* $G = Gal(K, \mathsf{k})$. *Буквами* F *и* H *мы будем обозначать соответствующие друг другу подполя в* K *и подгруппы в* G. *Тогда*

1. $[K : F] = |H|$,
2. $F_1 \subset F_2 \Leftrightarrow H_2 \subset H_1$,
3. F_1F_2 *соответствует* $H_1 \cap H_2$, $F_1 \cap F_2$ *соответствует* H_1H_2,
4. *расширение* F/k *нормально титтк подгруппа* $H \subset G$ *нормальна. При этом* $Gal(F, \mathsf{k}) = G/H$.

Доказательство. 1 было доказано на прошлой лекции, 2 очевидно.

Докажем 3: $Gal(K, F_1F_2) = H_1 \cap H_2$ и $K^{H_1H_2} = F_1 \cap F_2$. Действительно, автоморфизм $\sigma \in G$ сохраняет $F_1F_2 \Leftrightarrow \sigma$ сохраняет F_1 и $F_2 \Leftrightarrow \sigma \in H_1 \cap H_2$. Аналогично, $\alpha \in K$ сохраняется подгруппой $H_1H_2 \Leftrightarrow \alpha$ сохраняется H_1 и сохраняется $H_2 \Leftrightarrow \alpha \in F_1 \cap F_2$.

Докажем 4. Пусть $\sigma \in G$, тогда подгруппа $\sigma H \sigma^{-1}$ соответствует полю $\sigma(F)$. Действительно, если $\tau \in H, \alpha \in F$, то $\sigma\tau\sigma^{-1}(\sigma(\alpha)) = \sigma\tau(\alpha) = \sigma(\alpha)$, так как $\alpha \in F = K^H$. Поэтому $\sigma\tau\sigma^{-1} \in Gal(K, \sigma(F))$, и значит $\sigma H \sigma^{-1} \subset Gal(K, \sigma(F))$. Обратно, если $\rho \in Gal(K, \sigma(F)), \alpha \in F$, то $(\sigma^{-1}\rho\sigma)(\alpha) = \sigma^{-1}(\rho(\sigma(\alpha))) = \sigma^{-1}\sigma(\alpha) = \alpha$ так как ρ сохраняет $\sigma(\alpha)$. Значит, $\sigma^{-1}\rho\sigma \in Gal(K, F) = H$ и $\rho \in \sigma H \sigma^{-1}$, поэтому $Gal(K, \sigma(F)) \subset \sigma H \sigma^{-1}$.

По определению, подгруппа $H \subset G$ нормальна титтк $\sigma H \sigma^{-1} = H$ для всех $\sigma \in G$, это равносильно тому, что $\sigma(F) = F$ при всех $\sigma \in Gal(K, \mathsf{k})$. Так как K/k нормально, это и означает нормальность расширения F/k: все автоморфизмы K/k продолжаются до автоморфизма $\bar{\mathsf{k}}$ над k и все автоморфизмы $\bar{\mathsf{k}}$ над k сохраняют K.

Если F/k нормально, то имеется гомоморфизм ограничения $Gal(K, \mathsf{k}) \to Gal(F, \mathsf{k})$. Он сюръективен, так как любой автоморфизм F над k продолжается до автоморфизма $\bar{\mathsf{k}}$ над k, который сохраняет K. Ядро этого гомоморфизма – подгруппа $Gal(K, F) \subset Gal(K, \mathsf{k})$, получаем $Gal(F, \mathsf{k}) = Gal(K, \mathsf{k})/Gal(K, F)$. □

Определение 8. *Группой Галуа* многочлена $f \in \mathsf{k}[x]$ называется группа Галуа расширения K/k, где K – поле разложения f.

Поле разложения многочлена f над k порождено его корнями $\alpha_1, \ldots, \alpha_n$. Группа Галуа $G = Gal(K, \mathsf{k})$ переставляет эти корни, поэтому $G \subset S_n$. Исторически это первый пример группы Галуа (и вообще группы). Как мы увидим на следующей лекции, решение уравнения $f(x) = 0$ по сути сводится к вычислению группы Галуа f, однако это нетривиальная задача.

Пример 9. Рассмотрим многочлен $f(x) = x^4 - 2 \in \mathbb{Q}[x]$, пусть K – его поле разложения, через $\sqrt[4]{2}$ будем обозначать положительный вещественный корень. Очевидно, $K = \mathbb{Q}[\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}] = \mathbb{Q}[i, \sqrt[4]{2}]$, причём $i \notin \mathbb{Q}[\sqrt[4]{2}]$, поэтому

$$[K : \mathbb{Q}] = \left[\mathbb{Q}[i, \sqrt[4]{2}] : \mathbb{Q}[\sqrt[4]{2}]\right] \cdot \left[\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}\right] = 2 \cdot 4 = 8.$$

Корни 4-й степени из 2 лежат в вершинах квадрата в $\mathbb{C}$. Очевидно, $G = Gal(K, \mathbb{Q})$ состоит из тех перестановок, которые переводят пары противоположных вершин в пары противоположных, т.е. соответствуют движениям квадрата, причём все движения реализуются: $G \cong D_4$. Пусть $\sigma\colon K \to K$ – комплексное сопряжение, а $\tau\colon K \to K$ – автоморфизм такой, что $\tau(\sqrt[4]{2}) = i\sqrt[4]{2}, \tau(i) = i$. Тогда σ и τ отвечают симметрии относительно вещественной оси и повороту на 90°.

Ниже изображена структура подгрупп в D_4 и соответствующая ей структура подполей в $\mathbb{Q}[i, \sqrt[4]{2}]$:

$$
\begin{tikzcd}
 & & D_4 \arrow[dll, dash] \arrow[d, dash] \arrow[drr, dash] & & \\
\{1,\tau^2,\sigma,\sigma\tau^2\} \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \{1,\tau,\tau^2,\tau^3\} \arrow[d, dash] & & \{1,\tau^2,\sigma\tau,\sigma\tau^3\} \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \\
\{1,\sigma\} \arrow[drr, dash] & \{1,\sigma\tau^2\} \arrow[dr, dash] & \{1,\tau^2\} \arrow[d, dash] & \{1,\sigma\tau\} \arrow[dl, dash] & \{1,\sigma\tau^3\} \arrow[dll, dash] \\
 & & \{1\}, & &
\end{tikzcd}
$$

$$
\begin{tikzcd}
 & & \mathbb{Q} \arrow[dll, dash] \arrow[d, dash] \arrow[drr, dash] & & \\
\mathbb{Q}[\sqrt{2}] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \mathbb{Q}[i] \arrow[d, dash] & & \mathbb{Q}[i\sqrt{2}] \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \\
\mathbb{Q}[\sqrt[4]{2}] \arrow[drr, dash] & \mathbb{Q}[i\sqrt[4]{2}] \arrow[dr, dash] & \mathbb{Q}[i,\sqrt{2}] \arrow[d, dash] & \mathbb{Q}[(1-i)\sqrt[4]{2}] \arrow[dl, dash] & \mathbb{Q}[(1+i)\sqrt[4]{2}] \arrow[dll, dash] \\
 & & \mathbb{Q}[i,\sqrt[4]{2}]. & &
\end{tikzcd}
$$

Пример 10. Приведём пример группы Галуа многочлена, равной S_n.

Пусть $K = \mathbb{C}(x_1, \dots, x_n)$ – поле рациональных функций от n переменных. Пусть $\mathsf{k} = \mathbb{C}(x_1, \dots, x_n)^{S_n} \subset K$ – подполе, состоящее из симметричных функций, т.е. таких, которые не меняются при любой перестановке переменных. Рассмотрим многочлен

$$f(x) = \prod(x - x_i).$$

Очевидно, f не изменяется при всех перестановках переменных, поэтому $f \in \mathsf{k}[x]$. Поле K – поле разложения многочлена f, так как оно порождено его корнями x_i и многочлен f раскладывается в $K[x]$ на линейные множители. Ясно, что группа Галуа $Gal(K, \mathsf{k}) = S_n$ состоит из всех перестановок переменных (т.е. корней f).

Пусть

$$
\begin{aligned}
\sigma_1 &= x_1 + x_2 + \ldots + x_n, \\
\sigma_2 &= x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n, \\
\sigma_3 &= x_1x_2x_3 + \ldots, \\
&\ldots \\
\sigma_n &= x_1x_2\ldots x_n
\end{aligned}
$$

– элементарные симметрические многочлены. По теореме Виета, коэффициенты многочлена $f = \prod(x - x_i)$ – это элементарные симметрические многочлены с точностью до знака, а именно $f(x) = x^n - \sigma_1x^{n-1} + \sigma_2x^{n-2} + \ldots + (-1)^n\sigma_n$.

Как известно, любой симметрический многочлен от n переменных является многочленом от $\sigma_1, \ldots, \sigma_n$. При помощи теории Галуа можно легко доказать немного более слабое утверждение: любая симметрическая рациональная функция от n переменных является рациональной функцией от $\sigma_1, \ldots, \sigma_n$, т.е. $\mathbb{C}(\sigma_1, \ldots, \sigma_n) = \mathbb{C}(x_1, \ldots, x_n)^{S_n}$. Действительно, $f(x) \in \mathbb{C}(\sigma_1, \ldots, \sigma_n)[x]$ и аналогично рассуждениям, проведённым выше, проверяется, что K – поле разложения многочлена f над $\mathbb{C}(\sigma_1, \ldots, \sigma_n)$ и $Gal(K, \mathbb{C}(\sigma_1, \ldots, \sigma_n)) = S_n = Gal(K, \mathbb{C}(x_1, \ldots, x_n)^{S_n})$. По основной теореме теории Галуа, применённой к $K/\mathbb{C}(\sigma_1, \ldots, \sigma_n)$, получаем, что $\mathbb{C}(\sigma_1, \ldots, \sigma_n) = \mathbb{C}(x_1, \ldots, x_n)^{S_n}$.

Как мы видели на прошлой лекции, если число α можно построить при помощи циркуля, линейки и единичного отрезка, то оно лежит в некотором расширении $\mathbb{Q}$, степень которого есть $2^n, n \in \mathbb{N}$. Верно и обратное: если $\alpha \in K$, где $K/\mathbb{Q}$ – расширение Галуа степени 2^n, то α можно построить циркулем и линейкой.

На языке полей это значит следующее: для любого расширения Галуа $K/\mathbb{Q}$ степени 2^n найдётся последовательность полей

$$\mathbb{Q} = K_0 \subset K_1 \subset \ldots \subset K_n = K$$

(такая последовательность называется *фильтрацией*), где K_i получено из K_{i-1} присоединением квадратного корня или, что то же самое, где $[K_i : K_{i-1}] = 2$. При помощи теории Галуа это утверждение переводится на язык групп: для любой группы G порядка 2^n найдётся фильтрация подгруппами

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$$

такая, что $[G_i : G_{i-1}] = 2$. Этот факт будет доказан ниже.

Определение 11. Группа порядка p^n, где p – простое, называется *p-группой.*

Определение 12. *Центром* группы G называется множество $Z(G)$ её элементов, коммутирующих со всеми элементами: $Z(G) = \{s \in G \mid \forall g \in G \; sg = gs\}$. Очевидно, что центр – нормальная подгруппа.

Лемма 13. *Центр p-группы не равен $\{e\}$.*

Доказательство. Рассмотрим действие группы G на себе сопряжениями. Тогда $Z(G)$ – в точности множество неподвижных точек. Порядок любой орбиты этого действия есть индекс стабилизатора любого элемента орбиты, т.е. является степенью p. Значит, группа G разбивается в объединение орбит, содержащих кратное p число элементов, и центра (состоящего из одноточечных орбит). Поэтому число элементов центра кратно p и, стало быть, больше 1. □

Предложение 14. *Для любой p-группы G найдётся фильтрация*

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$$

такая, что $[G_i : G_{i-1}] = p$.

Доказательство. По индукции по $|G|$. База: $|G| = p$, здесь нечего доказывать. Для совершения шага индукции возьмём в G нетривиальную нормальную подгруппу H. Если G абелева, то выбрать такую H несложно, используя классификацию, если G не абелева, то можно взять её центр. По индукции, существуют фильтрации

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_k = H$$

и

$$\{e\} = G'_0 \subset G'_1 \subset \ldots \subset G'_{n-k} = G/H.$$

Тогда в качестве фильтрации для G можно взять

$$\{e\} = G_0 \subset G_1 \subset \ldots \subset G_k = H \subset p^{-1}(G'_1) \subset p^{-1}(G'_2) \subset \ldots \subset p^{-1}(G'_{n-k}) = G,$$

где $p\colon G \to G/H$ – гомоморфизм факторизации. $\square$