4. Лекция 4

4.1. **Автоморфизмы полей.** Пусть K — поле, F — его подполе. *Автоморфизм* поля K — это изоморфизм $\sigma\colon K \to K$. Говорят, что автоморфизм σ оставляет подполе F неподвижным, если $\sigma\alpha = \alpha$ для любого $\alpha \in F$. Группа автоморфизмов поля K обозначается через $\mathrm{Aut}(K)$, подгруппа автоморфизмов, оставляющих неподвижным подполе F — через $\mathrm{Aut}(K/F)$. Поскольку для любого автоморфизма $\sigma(0) = 0$ и $\sigma(1) = 1$, то σ оставляет неподвижным простое подполе $\mathbb{Q}$ или $\mathbb{F}_p$. Значит, если F — простое подполе, то $\mathrm{Aut}(K/F) = \mathrm{Aut}(K)$.

Докажем, что элементы K, алгебраические над F, при любом автоморфизме переходят в алгебраические элементы той же степени.

Предложение 4.1. *Пусть элемент $\alpha \in K$ алгебраичен над F, и $m_\alpha(x)$ — его минимальный многочлен. Тогда для любого $\sigma \in \mathrm{Aut}(K/F)$ элемент $\sigma\alpha$ — тоже корень $m_\alpha(x)$. Более того, если α — корень многочлена $f(x) \in F[x]$, то $\sigma\alpha$ — тоже корень этого многочлена.*

Доказательство. Пусть $f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$. Применим к этому равенству автоморфизм σ. Учитывая, что $\sigma(a_i) = a_i$, получим, что $a_n(\sigma\alpha)^n + \cdots + a_1\sigma\alpha + a_0 = 0$, что и означает, что $f(\sigma\alpha) = 0$. □

Пример 4.2. Пусть $K = \mathbb{Q}(\sqrt{2})$. Рассмотрим элемент $\sqrt{2}$; его минимальный многочлен — $x^2 - 2$. Это значит, что для всякого автоморфизма $\tau \in \mathrm{Aut}\,\mathbb{Q}(\sqrt{2})$ элемент $\tau(\sqrt{2})$ тоже есть корень этого многочлена, то есть $\sqrt{2}$ или $-\sqrt{2}$. Это полностью описывает автоморфизм τ: в первом случае он оказывается тождественным, а во втором — это *сопряжение*: $\tau(a + b\sqrt{2}) = a - b\sqrt{2}$. Поэтому $\mathrm{Aut}\,\mathbb{Q}(\sqrt{2}) = \mathbb{Z}/2\mathbb{Z}$.

Пример 4.3. Пусть $K = \mathbb{Q}(\sqrt[3]{2})$. Тогда минимальный многочлен элемента $\sqrt[3]{2}$ — это $x^3 - 2$. В поле K нет других элементов, удовлетворяющих уравнению $x^3 - 2 = 0$ (остальные два корня этого многочлена не являются вещественными, а значит, не лежат и в $\mathbb{Q}(\sqrt[3]{2})$. Поэтому любой автоморфизм поля $\mathbb{Q}(\sqrt[3]{2})$ оставляет $\sqrt[3]{2}$ на месте, а значит, является тождественным: $\mathrm{Aut}\,\mathbb{Q}(\sqrt[3]{2}) = \{1\}$.

4.2. **Соответствие между подполями и подгруппами в** $\mathrm{Aut}(K/F)$**.** Пусть E — некоторое "промежуточное" подполе в K: $F \subset E \subset K$. Тогда в $\mathrm{Aut}(K/F)$ можно рассмотреть подгруппу $\mathrm{Aut}(K/E)$ автоморфизмов, оставляющих E неподвижным. Обратно, подгруппе H в $\mathrm{Aut}(K/F)$ можно сопоставить подмножество элементов $K^H \subset K$, состоящее из всех неподвижных относительно H элементов.

Предложение 4.4. *Пусть $H \subset \mathrm{Aut}(K/F)$ — подгруппа. Тогда $K^H = \{\alpha \in K \mid \sigma\alpha = \alpha \quad \forall \sigma \in H\}$ — подполе в K.*

Доказательство. По определению гомоморфизма, подмножество K^H будет замкнуто относительно взятия суммы, произведения и обратного. Значит, это подполе. □

Следующее предложение тоже очевидно:

Предложение 4.5. *Такое соответствие между подполями и подгруппами обращает отношение включения: если $F_1 \subset F_2 \subset K$, то $\mathrm{Aut}(K/F_2) \supset \mathrm{Aut}(K/F_1)$. Обратно, если $H_1 \subset H_2 \subset \mathrm{Aut}(K/F)$, то $K^{H_1} \supset K^{H_2}$.*

Пример 4.3 показывает, что это соответствие не всегда биективно: так, подполю $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ и всему полю $\mathbb{Q}(\sqrt[3]{2})$ соответствует одна и та же (тривиальная) подгруппа автоморфизмов. Получается, что автоморфизмов в $\mathrm{Aut}(K/F)$ "слишком мало" для того, чтобы это соответствие было бы биективным.

Приведем ещё один пример:

Пример 4.6. Пусть теперь $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ — поле разложения многочлена $x^3 - 2$ (напомним, что его корни имеют вид $\zeta^j \sqrt[3]{2}$, где $0 \le j \le 2$, а $\zeta = (-1 + \sqrt{-3})/2$ — первообразный корень из 1 степени 3). Это расширение степени 6. Группа $\mathrm{Aut}(K)$ состоит из шести элементов, реализующих все перестановки трёхэлементного множества корней этого многочлена, т.е. $\mathrm{Aut}(K) \cong S_3$. В K имеется одно подполе, являющееся квадратичным расширением $\mathbb{Q}$ — это $\mathbb{Q}(\sqrt{-3})$, и три расширения $\mathbb{Q}$ степени 3: это $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\zeta\sqrt[3]{2})$ и $\mathbb{Q}(\zeta^2\sqrt[3]{2})$. Подгруппы, отвечающие этим подполям в S_3 — это нормальная подгруппа A_3 (она имеет индекс 2) и три подгруппы индекса 3, порождённые транспозициями и не являющиеся нормальными. Видим, что в данном случае описанное соответствие между подгруппами и подполями биективно, причём степень подполя над $\mathbb{Q}$ равняется индексу отвечающей ему подгруппы в $\mathrm{Aut}(K)$.

Такие "хорошие" расширения полей называются *расширениями Галуа*.

4.3. **Расширения Галуа. Формулировка основной теоремы.** В этом разделе мы анонсируем результаты, которые будут доказаны позже.

Теорема 4.7. *Для произвольного конечного расширения имеется неравенство $|\mathrm{Aut}(K/F)| \le [K : F]$.*

Мы видели в предыдущих примерах, что в "хороших" случаях (скажем, для квадратичного расширения, или в примере 4.6) это неравенство обращается в равенство. Сначала дадим "хорошей" ситуации название:

Определение 4.8. Расширение полей K/F называется *расширением Галуа*, если

$$|\operatorname{Aut}(K/F)| = [K : F].$$

Группа автоморфизмов поля K при этом называется его *группой Галуа* и обозначается через $\operatorname{Gal}(K/F)$.

Биекции между подполями в K и подгруппами в $\operatorname{Aut}(K/F)$, которую мы видели в примерах 4.2 и 4.6, суть частные случаи следующей общей теоремы.

Теорема 4.9 (Основная теорема теории Галуа)**.** *Пусть K/F — расширение Галуа. Тогда имеется биекция между подполями в K, содержащими F, и подгруппами в группе $G = \operatorname{Gal}(K/F)$. При этой биекции подполю E соответствует подгруппа $H = \operatorname{Aut}(K/E) \subset G$, а подгруппе $H \subset G$ — её неподвижное подполе $E = K^H$. Эта биекция обладает следующими свойствами:*

(1) *она обращает включения: $E_1 \subset E_2 \Leftrightarrow H_1 \supset H_2$;*
(2) *степень расширения $[K : E]$ равна порядку группы H, а степень расширения $[E : F]$ — индексу подгруппы $[G : H]$;*
(3) *расширение K/E является расширением Галуа, и $\operatorname{Gal}(K/E) = H$;*
(4) *расширение E/F является расширением Галуа тогда и только тогда, когда H нормальна в G; при этом $\operatorname{Gal}(E/F) = G/H$;*
(5) *Пересечению подполей $E_1 \cap E_2$ соответствует группа $\langle H_1, H_2\rangle \subset G$, а композиту полей E_1E_2 — пересечение групп $H_1 \cap H_2$.*

Доказательству теорем из этого раздела будет посвящена оставшаяся часть этой и значительная часть следующей лекции.

4.4. **Характеры.**

Определение 4.10. *(Мультипликативный) характер* группы G со значениями в поле L — это гомоморфизм $\chi\colon G \to L^*$.

Характер можно (и нужно) рассматривать как L-значную функцию на группе G.

Замечание 4.11. В курсе теории представлений мы уже встречались с более общим понятием характера: мы рассматривали следы всевозможных конечномерных (а не только одномерных) представлений. Однако характеры у нас были только комплекснозначные, и работа с ними существенно использовала специфику поля $\mathbb{C}$. Оказывается, что некоторые утверждения — например, теорема о линейной независимости характеров — верны и для произвольного поля.

Теорема 4.12. *Попарно различные характеры $\chi_1, \ldots, \chi_n$ линейно независимы как функции на G.*

Доказательство. Предположим противное: пусть имеется нулевая линейная комбинация характеров, т.е. при всех $g \in G$

$$a_1\chi_1(g) + \cdots + a_n\chi_n(g) = 0.$$

Будем считать, что n минимально (т.е. всякая линейная комбинация $n-1$ характера уже будет нетривиальной).

Поскольку характеры χ_1 и χ_n различны, найдётся такой элемент h, что $\chi_1(h) \neq \chi_n(h)$. Домножим предыдущее равенство на $\chi_n(h)$:

$$a_1\chi_n(h)\chi_1(g) + \cdots + a_n\chi_n(h)\chi_n(g) = 0. \qquad (*)$$

С другой стороны, для любого g

$$a_1\chi_1(hg) + \cdots + a_n\chi_n(hg) = 0,$$

то есть, в силу мультипликативности характеров,

$$a_1\chi_1(h)\chi_1(g) + \cdots + a_n\chi_n(h)\chi_n(g) = 0.$$

Вычтем из этого равенства $(*)$:

$$a_1[\chi_1(h) - \chi_n(h)]\chi_1(g) + \cdots + a_{n-1}[\chi_{n-1}(h) - \chi_n(h)]\chi_{n-1}(g) = 0.$$

Мы получили нетривиальную (т.к. $\chi_1(h) - \chi_n(h) \neq 0$) линейную комбинацию из $n-1$ характера, тождественно равную нулю. Противоречие. □

Пусть $\sigma\colon K \to L$ — гомоморфизм полей (ненулевой, а следовательно, инъективный). Тогда $\sigma\colon K^* \to L^*$ — характер. Обратно, каждый характер однозначно задаёт гомоморфизм: σ нужно доопределить только в нуле, а $\sigma(0) = 0$. Получается

Следствие 4.13. *Пусть $\sigma_1, \ldots, \sigma_n$ — различные вложения $K \to L$. Тогда они линейно независимы как L-значные функции на K.*

4.5. **Порядок группы автоморфизмов поля равен степени расширения поля над ее неподвижным подполем.** В этом разделе мы докажем следующую теорему.

Теорема 4.14. *Пусть $G = \{\sigma_1 = 1, \ldots, \sigma_n\}$ — некоторая группа автоморфизмов поля K, и пусть $F = K^G$ — неподвижное подполе этой группы. Тогда $[K : F] = n = |G|$.*

Доказательство. Сначала покажем, что $n \leq [K : F]$. Предположим противное: $n > [K : F] = m$, и пусть $\omega_1, \ldots, \omega_m$ — базис K как векторного пространства над F. Рассмотрим систему уравнений

$$\begin{aligned} \sigma_1(\omega_1)x_1 + \cdots + \sigma_n(\omega_1)x_n &= 0; \\ &\cdots \\ \sigma_1(\omega_m)x_1 + \cdots + \sigma_n(\omega_m)x_n &= 0. \end{aligned}$$

Это система из m уравнений с $n > m$ неизвестными. Значит, у неё есть нетривиальное решение $\beta_1, \ldots, \beta_n$, где $\beta_i \in K$.

Пусть $a_1, \ldots, a_m$ — произвольные элементы поля F. Тогда $\sigma_i(a_j) = a_j$. Учитывая это, домножим i-е уравнение на a_i и получим:

$$\begin{aligned} \sigma_1(a_1\omega_1)\beta_1 + \cdots + \sigma_n(a_1\omega_1)\beta_n &= 0; \\ &\cdots \\ \sigma_1(a_m\omega_m)\beta_1 + \cdots + \sigma_n(a_m\omega_m)\beta_n &= 0. \end{aligned}$$

Сложив все уравнения, получим, что

$$\sigma_1(a_1\omega_1 + \cdots + a_m\omega_m)\beta_1 + \cdots + \sigma_n(a_1\omega_1 + \cdots + a_m\omega_m)\beta_n = 0.$$

Линейная комбинация в скобках может при подходящем выборе a_i равняться любому элементу из K, т.к. ω_i — базис. Значит, для любого $\alpha \in K$

$$\sigma_1(\alpha)\beta_1 + \cdots + \sigma_n(\alpha)\beta_n = 0.$$

Получаем, что σ_i линейно зависимы, что противоречит следствию 4.13.

Теперь докажем неравенство в обратную сторону: $n \geq [K : F]$. Заметим, что мы пока не пользовались тем фактом, что G — это группа, а не произвольный набор автоморфизмов.

Итак, допустим, что $n < [K : F]$. Поэтому в K можно выбрать $n+1$ линейно независимый над F элемент $\alpha_1, \ldots, \alpha_{n+1} \in K$. Снова составим систему:

$$\begin{aligned} \sigma_1(\alpha_1)x_1 + \cdots + \sigma_1(\alpha_{n+1})x_{n+1} &= 0; \\ &\cdots \\ \sigma_n(\alpha_1)x_1 + \cdots + \sigma_n(\alpha n + 1)x_{n+1} &= 0. \end{aligned}$$

Она имеет нетривиальное решение $\beta_1, \ldots, \beta_{n+1} \in K$. Среди всех нетривиальных решений системы выберем такое, у которого количество отличных от нуля компонент (обозначим его через r) минимально.

Заметим, что среди β_i есть элементы не из F: действительно, поскольку $\sigma_1 = 1$, то $\sigma_1\alpha_i = \alpha_i$, и если бы все β_i были из F, то из первого уравнения следовала бы линейная зависимость α_i над F. Будем считать, что $\beta_1 \neq F$. Далее, будем считать, что первые r чисел $\beta_1, \ldots, \beta_r$ отличны от 0. Кроме того, домножив их все на подходящее число, можно сделать $\beta_r = 1$. Тогда система примет вид

$$\begin{aligned} \sigma_1(\alpha_1)\beta_1 + \cdots + \sigma_1(\alpha_{r-1})\beta_{r-1} + \sigma_1(\alpha_r) &= 0; \\ &\cdots \\ \sigma_n(\alpha_1)\beta_1 + \cdots + \sigma_n(\alpha_{r-1})\beta_{r-1} + \sigma_n(\alpha_r) &= 0, \end{aligned}$$

или, что то же самое,

$$\sigma_i(\alpha_1)\beta_1 + \cdots + \sigma_i(\alpha_{r-1})\beta_{r-1} + \sigma_i(\alpha_r) = 0. \qquad (**)$$

Существует такой автоморфизм $\tilde{\sigma}$, что $\tilde{\sigma}\beta_1 \neq \beta_1$. Применив $\tilde{\sigma}$ к $(**)$, получим систему уравнений вида

$$\tilde{\sigma}\sigma_i(\alpha_1)\tilde{\sigma}(\beta_1) + \cdots + \tilde{\sigma}\sigma_i(\alpha_{r-1})\tilde{\sigma}(\beta_{r-1}) + \tilde{\sigma}\sigma_i(\alpha_r) = 0.$$

Мы подействовали на G левым сдвигом на $\tilde{\sigma}$. Поэтому множества $\{\sigma_1, \ldots, \sigma_n\}$ и $\{\tilde{\sigma}\sigma_1, \ldots, \tilde{\sigma}\sigma_n\}$ совпадают. Значит, последнюю систему уравнений можно переписать (поменяв порядок уравнений) как

$$\sigma_i(\alpha_1)\tilde{\sigma}(\beta_1) + \cdots + \sigma_i(\alpha_{r-1})\tilde{\sigma}(\beta_{r-1}) + \sigma_i(\alpha_r) = 0.$$

Вычтя из неё $(**)$, получим систему

$$\sigma_i(\alpha_1)[\tilde{\sigma}(\beta_1) - \beta_1] + \cdots + \sigma_i(\alpha_{r-1})[\tilde{\sigma}(\beta_{r-1}) - \beta_{r-1}] = 0.$$

Мы получили нетривиальное решение исходной системы (поскольку $\tilde{\sigma}(\beta_1) \neq \beta_1$), у которого имеется не более $r-1$ ненулевой компоненты. Это противоречит минимальности r.

Значит, $|G| = [K : F]$. Теорема доказана.

□