5. Лекция 5

В этой лекции мы докажем основную теорему теории Галуа. Для этого сначала выведем несколько следствий из теоремы 4.14.

5.1. **Три следствия из теоремы 4.14.**

Следствие 5.1. *Пусть K/F — конечное расширение. Тогда* $|\operatorname{Aut}(K/F)| \leq [K : F]$.

Доказательство. Пусть F_1 — неподвижное поле группы $\operatorname{Aut}(K/F)$. Тогда $F_1 \supset F$. По теореме 4.14 $|\operatorname{Aut}(K/F)| = [K : F_1] = [K : F]/[F_1 : F] \leq [K : F]$. □

Следствие 5.2. *Пусть G — конечная группа автоморфизмов поля K, и $F = K^G$. Тогда всякий автоморфизм поля K, оставляющий F на месте, содержится в G, т.е.* $\operatorname{Aut}(K/F) = G$. *В частности, отсюда вытекает, что K/F — расширение Галуа.*

Доказательство. По условию, подполе F неподвижно относительно G, то есть $G \subset \operatorname{Aut}(K/F)$, следовательно, $|G| \leq |\operatorname{Aut}(K/F)|$. Но по теореме 4.14 имеем равенство $|G| = [K : F]$, а по предыдущему следствию $|\operatorname{Aut}(K/F)| \leq [K : F]$. Получаем цепочку неравенств:

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

Значит, они все являются равенствами, откуда и следует требуемое утверждение. □

Следствие 5.3. *Пусть* $G_1, G_2 \subset \operatorname{Aut}(K)$. *Если $G_1 \neq G_2$, то $K^{G_1} \neq K^{G_2}$.*

Доказательство. Пусть $F_1 = K^{G_1}$, $F_2 = K^{G_2}$. Если $F_1 = F_2$, то поле F_1 неподвижно относительно G_2, и поэтому $G_2 \subset G_1$. Аналогично получаем, что $G_1 \subset G_2$. Поэтому $G_1 = G_2$. □

5.2. **Нормальные сепарабельные расширения.**

Предложение 5.4. *Пусть $f(x) \in F[x]$ — многочлен без кратных сомножителей, E — его поле разложения. Тогда E является расширением Галуа тогда и только тогда, когда $f(x)$ сепарабелен.*

Доказательство. Напомним (это теорема 2.15), что для любого изоморфизма $\varphi\colon F \to F'$ существует продолжающий его изоморфизм полей разложения многочленов f и $\varphi(f)$, обозначавшийся через $\sigma\colon E \to E'$.

Покажем по индукции по степени расширения $[E : F]$, что таких гомоморфизмов σ, продолжающих φ, не более чем $[E : F]$, причем равенство достигается тогда и только тогда, когда $f(x)$ сепарабелен.

База индукции очевидна: если $[E : F] = 1$, то $E = F$, и $\sigma = \varphi$.

Если $[E : F] > 1$, то у $f(x)$ существует неприводимый сомножитель $p(x)$. Пусть α — корень $p(x)$. Если σ — продолжение φ, то пусть $\tau = \sigma|_{F(\alpha)} \colon F(\alpha) \to E'$. Гомоморфизм τ однозначно задаётся своим действием на α. Ясно, что $\beta = \tau\alpha$ — корень многочлена $p'(x) = \varphi(p(x))$. Поэтому число способов продолжить φ до $\tau \colon F(\alpha) \to F'(\beta)$ не превосходит $\deg p(x) = [F(\alpha) : F]$, причем равняется ему, если $p(x)$ сепарабелен. Теперь можно применить предположение индукции к продолжению гомоморфизма $\tau \colon F(\alpha) \to F'(\beta)$ до гомоморфизма $\sigma \colon E \to E'$. Число этих продолжений, согласно предположению индукции, не превосходит $[E : F(\alpha)]$.

Для завершения доказательства осталось заметить, что $[E : F] = [E : F(\alpha)][F(\alpha) : F]$. Поэтому число продолжений φ до σ, т.е. элементов $\mathrm{Aut}(E/F)$, равняется $[E : F]$ в точности тогда, когда $f(x)$ сепарабелен. □

Следствие 5.5. *Нормальное сепарабельное расширение является расширением Галуа.*

Оказывается, верно и обратное утверждение. Удобно сформулировать его вместе с предыдущим предложением, в форме "тогда и только тогда".

Теорема 5.6. *Расширение K/F является расширением Галуа тогда и только тогда, когда K является полем разложения некоторого сепарабельного многочлена над F. Более того, каждый неприводимый многочлен с коэффициентами из F, имеющий корни в K, сепарабелен, и все его корни лежат в K.*

Доказательство. Часть "тогда" – это предложение 5.4.

Докажем часть "только тогда". Сначала покажем, что если K/F — расширение Галуа, то каждый неприводимый многочлен $p(x) \in F[x]$ с корнем в K раскладывается над K на линейные множители. Пусть $G = \mathrm{Gal}(K/F)$

Пускай $\alpha \in K$ — корень $p(x)$; рассмотрим орбиту этого корня под действием группы Галуа: $G\alpha = \{\alpha_1, \dots, \alpha_r\}$ (все элементы последнего множества различны). Ясно, что каждый элемент $\tau \in G$ как-то переставляет эти элементы. У многочлена $f(x) = (x - \alpha_1)\dots(x - \alpha_r)$ коэффициенты (элементарные симметрические многочлены от $\alpha_1, \dots, \alpha_r$) инвариантны относительно G, поэтому они принадлежат полю F.

Поскольку $p(x)$ неприводим и имеет α корнем, то $p(x)$ — минимальный многочлен для α над полем F. Но α также является корнем многочлена $f(x) \in F[x]$. Поэтому $p(x)|f(x)$ в $F[x]$. Но, с другой стороны, все числа $\alpha_1, \dots, \alpha_r$ — корни $p(x)$, поэтому $f(x)|p(x)$. Значит, $p(x) = f(x)$. Поэтому $p(x)$ сепарабелен, и все его корни лежат в K.

Далее, пусть K/F — расширение Галуа, и $\omega_1, \dots, \omega_n$ — базис поля K над F. Пусть $p_i(x)$ — минимальный многочлен элемента ω_i. По доказанному выше, он сепарабелен, и все его корни лежат в K. Возьмём произведение этих многочленов: $f(x) = p_1(x) \dots p_n(x)$. Пусть многочлен $g(x)$ получается из $f(x)$ вычёркиванием всех кратных множителей (т.е. это делитель $f(x)$ максимальной степени, свободный от квадратов). Многочлен $g(x)$ сепарабелен, его поле разложения содержит $\omega_1, \dots, \omega_n$, то есть содержит K. С другой стороны, все корни этого многочлена лежат в K. Поэтому K и есть его поле разложения. $\square$

Определение 5.7. Пусть K/F — расширение Галуа, $\sigma \in \mathrm{Gal}(K/F)$, $\alpha \in K$. Элементы α и $\sigma\alpha$ называют *сопряжёнными.* Если $E \subset K$, то $\sigma(E)$ — *сопряжённое к E подполе.*

В доказательстве предыдущей теоремы мы показали, что в расширении Галуа все корни неприводимого многочлена являются сопряжёнными (т.е. группа Галуа действует на корнях транзитивно).

Итак, у нас имеются четыре равносильных описания расширения Галуа. Расширение Галуа K/F — это:

(1) поле разложения сепарабельного многочлена с коэффициентами в F;
(2) расширение, в котором $K^{\mathrm{Aut}(K/F)}$ есть в точности F (т.е. не больше);
(3) расширение, для которого $|\mathrm{Aut}(K/F) = [K : F]$ (исходное определение);
(4) нормальное сепарабельное расширение.

5.3. **Доказательство основной теоремы теории Галуа.** Напомним формулировку основной теоремы (мы её уже приводили в предыдущей лекции):

Теорема 5.8 (Основная теорема теории Галуа)**.** *Пусть K/F — расширение Галуа. Тогда имеется биекция между подполями в K, содержащими F, и подгруппами в группе $G = \mathrm{Gal}(K/F)$. При этой биекции подполю E соответствует подгруппа $H = \mathrm{Aut}(K/E) \subset G$, 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 $\mathrm{Gal}(K/E) = H$;*
(4) *расширение E/F является расширением Галуа тогда и только тогда, когда H нормальна в G; при этом $\mathrm{Gal}(E/F) = G/H$;*
(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 $H_1 \cap H_2$.*

Доказательство. Во-первых, по каждой подгруппе $H \subset G = \mathrm{Gal}(K/F)$ можно построить подполе $E = K^H \subset K$. Согласно следствию 5.3, это соответствие инъективно: разным группам отвечают разные подполя.

Далее, если K — поле разложения сепарабельного многочлена $f(x) \in F[x]$, то $f(x)$ можно рассматривать как элемент кольца $E[x]$ для любого поля $E \supset F$. Поэтому K также будет полем разложения многочлена $f(x)$ как многочлена с коэффициентами в E. Поэтому K/E всегда будет расширением Галуа (описание (1) из предыдущего пункта). Стало быть, E есть неподвижное поле группы $\mathrm{Aut}(K/E) \subset G$. Поэтому *любое* подполе в K, содержащее F, есть неподвижное поле для некоторой подгруппы $H \subset G$. Значит, соответствие Галуа — биекция.

Обращение включений (часть (1) теоремы) очевидно.

Далее, если $E = K^H$ — неподвижное поле подгруппы H, то $[K : E] = |H|$ (т.к. K/E — расширение Галуа), а $[K : F] = |G|$ (по той же причине), поэтому $[E : F] = [G : H]$. Отсюда получается (2).

(3) получается из следствия 5.2.

Пусть $E = K^H$ — неподвижное поле подгруппы H. Всякий автоморфизм $\sigma \in G$, ограниченный на E, определяет вложение $\sigma|_E \colon E \to \sigma(E) \subset K$. Обратно, пусть $\tau \colon E \tilde{\to} \tau E \subset \overline{F}$ — вложение E в алгебраическое замыкание поля F, содержащее K. Тогда $\tau(E) \subset K$. Действительно, если $\alpha \in E$ отвечает минимальный многочлен $m_{\alpha,F}(x) \in F[x]$, то элемент $\tau\alpha$ тоже является корнем этого многочлена, и по теореме 5.6 поле K содержит все эти корни. Поэтому K является полем разложения некоторого многочлена $f(x)$ над E, а также полем разложения многочлена $\tau f(x) = f(x)$. Согласно теореме о продолжении гомоморфизма, существует такой автоморфизм $\sigma \colon K \to K$ поля K, который продолжает изоморфизм $\tau \colon E \to \tau(E)$.

Если ограничения автоморфизмов σ и σ' на одно и то же вложение E совпадают, это значит, что $\sigma^{-1}\sigma' = 1$. Поэтому $\sigma^{-1}\sigma' \in H$, или, что то же самое, $\sigma' \in \sigma H$. Поэтому различные автоморфизмы поля K, оставляющие E неподвижным, взаимно однозначно отвечают смежным классам σH. Поэтому

$$|\,\mathrm{Emb}(E/F)| = [G : H] = [E : F],$$

где $\mathrm{Emb}(E/F)$ — множество *вложений* E в K, оставляющих F неподвижным.

Расширение E/F является расширением Галуа тогда и только тогда, когда $|\,\mathrm{Aut}(E/F) = [E : F]$. Это значит, что всякое вложение E в K есть *автоморфизм* поля E, то есть $\sigma(E) = E$ для любого $\sigma \in G$.

Если $\sigma \in G$, то подгруппа в G, оставляющая на месте подполе $\sigma(E)$, есть $\sigma H \sigma^{-1}$, то есть $\sigma(E) = K^{\sigma H \sigma^{-1}}$. Наоборот, если

$\sigma H \sigma^{-1} = H$, то $\sigma(E) = E$. Поэтому H нормальна тогда и только тогда, когда E/F есть расширение Галуа, и в этом случае $\mathrm{Gal}(E/F) = G/H$.

Упражнение 5.9. Докажите самостоятельно часть (5) теоремы.

□