Теория Галуа, лекция 6: группа Галуа

Миша Вербицкий

15 февраля, 2013

матфак ВШЭ

Расширения полей (повторение)

ОПРЕДЕЛЕНИЕ: Расширение поля k есть поле K, содержащее k.

ОПРЕДЕЛЕНИЕ: Конечное расширение есть расширение $[K : k]$ такое, что K конечномерно как векторное пространство над k. **Степень** конечного расширения есть размерность K как векторного пространства над k.

ОПРЕДЕЛЕНИЕ: Элемент K называется **алгебраическим над** k, если он содержится в конечном расширении $[K' : k]$, то есть мультипликативно порождает поле K'', конечномерное над k. **Алгебраическое расширение** есть такое расширение $[K : k]$, что все элементы K алгебраичны над k.

ТЕОРЕМА: Сумма, произведение, частное алгебраических над k **элементов алгебраично над** k**.** ■

Примитивные расширения (повторение)

УТВЕРЖДЕНИЕ: Пусть $v \in R$ – элемент конечномерной алгебры R над k, а $P(t)$ – его минимальный полином. **Тогда подалгебра $R_v \subset R$, порожденная v, изоморфна $k[t]/(P)$.** ■

ОПРЕДЕЛЕНИЕ: Полином $P(t) \in k[t]$ **неприводим**, если его нельзя разложить на множители положительной степени.

УТВЕРЖДЕНИЕ: Обозначим идеал $k[t]P(t)$, порожденный полиномом $P(t)$, за (P). Полином $P(t)$ **неприводим тогда и только тогда, когда факторкольцо $k[t]/(P)$ является полем.** ■

ОПРЕДЕЛЕНИЕ: Пусть $P(t) \in k[t]$ – неприводимый полином. Поле $k[t]/(P)$ называется **расширение k, полученное добавлением корня $P(t)$**. Расширение $[k[t]/(P) : k]$ называется **примитивным**.

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – конечное расширение. **Тогда K может быть получено из k последовательностью примитивных расширений.** Иначе говоря, существует набор промежуточных расширений $[K = K_n : K_{n-1} : K_{n-2} : ... : K_0 = k]$, таких, что каждое $[K_i : K_{i-1}]$ примитивно. ■

Расширения Галуа (повторение)

ОПРЕДЕЛЕНИЕ: Пусть $[K : k]$ – конечное расширение поля k. Говорят, что $[K : k]$ **расширение Галуа**, если $K \otimes_k K$ изоморфно (как кольцо) прямой сумме нескольких копий K.

ПРИМЕР: Пусть p – простое. Тогда **для любого корня из единицы ζ степени p, $[\mathbb{Q}[\zeta] : \mathbb{Q}]$ – расширение Галуа.** А если p не простое?

ПРИМЕР: Пусть $[k : \mathbb{Q}]$ – расширение степени 2 (т.е. K двумерно как векторное пространство над $\mathbb{Q}$). **Тогда $[k : \mathbb{Q}]$ – расширение Галуа.**

ТЕОРЕМА: Пусть $K \supset K' \supset k$ – цепочка конечных расширений. Предположим, что $[K : k]$ – расширение Галуа. **Тогда $[K : K']$ тоже расширение Галуа.** ■

ТЕОРЕМА: Пусть $P(t) \in k[t]$ – неприводимый полином степени n, имеющий n попарно различных корней $\alpha_1, ..., \alpha_n$ в конечном расширении $[K : k]$. Предположим, что K порождено $\{\alpha_i\}$. **Тогда это расширение Галуа.**

ОПРЕДЕЛЕНИЕ: Пусть $[\overline{k} : k]$ – алгебраическое замыкание k, а $K \subset \overline{k}$ – поле, полученное из k добавлением всех корней $\alpha_i \in \overline{k}$. Тогда K называется **полем разложения $P(t)$.**

Группа Галуа и идемпотенты

ОПРЕДЕЛЕНИЕ: Пусть $[K : k]$ – расширение Галуа. **Группой Галуа** $[K : k]$ называется группа $\mathrm{Aut}_k(K)$ k-линейных автоморфизмов поля K.

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – расширение Галуа. Тогда **существует естественная биекция между следующими множествами.**

(а) Группой Галуа $\mathrm{Aut}_k(K)$

(б) Простые идеалы в $K \otimes_k K$.

(в) Гомоморфизмы $K \otimes_k K \longrightarrow K$,

тождественные на $K = K \otimes_k k \subset K \otimes_k K$.

Доказательство. Шаг 1: Биекция между (б) и (в) строится так: **каждому простому идеалу соответствует проекция** $K \otimes_k K = K^{\bigoplus^n} \longrightarrow K$.

Группа Галуа и идемпотенты (продолжение)

УТВЕРЖДЕНИЕ: Пусть $[K:k]$ – расширение Галуа. Тогда **существует естественная биекция между следующими множествами.**

(а) Группой Галуа $\mathrm{Aut}_k(K)$

(б) Простые идеалы в $K \otimes_k K$.

(в) Гомоморфизмы $K \otimes_k K \longrightarrow K$,

тождественные на $K = K \otimes_k k \subset K \otimes_k K$.

Шаг 2: Простые идеалы в $K \otimes_k K = \bigoplus K_e$ соответствуют неразложимым идемпотентам, то есть компонентам разложения. Каждый неразложимый идемпотент e задает проекцию $K \otimes_k K \xrightarrow{\pi} K_e$, переводящую 1 в 1. Рассмотрим гомоморфизмы $L_e, R_e: \ K \longrightarrow K_e$, полученные композицией $L_e: \ K = K \otimes_k k \subset K \otimes_k K \xrightarrow{\pi} K_e$ и $R_e: \ K = k \otimes_k K \subset K \otimes_k K \xrightarrow{\pi} K_e$ Поскольку это поля одинаковой размерности над k, L_e и R_e – изоморфизмы. **Поставим в соответствие идемпотенту e автоморфизм $L_e R_e^{-1} \in \mathrm{Aut}_k(K)$.** Это задает (б) $\Rightarrow$ (а).

Шаг 3: Каждому автоморфизму $\zeta \in \mathrm{Aut}_k(K)$ поставим в соответствие гомоморфизм $v_\zeta: \ K \otimes_k K \longrightarrow K$, переводящий $a \otimes b$ в $a\zeta^{-1}(b)$. Ядро этого гомоморфизма - простой идеал. **Мы получили соответствие (а) $\Rightarrow$ (в) = (б).**

Осталось доказать, что это биекция.

Группа Галуа и идемпотенты (окончание)

УТВЕРЖДЕНИЕ: Пусть $[K:k]$ – расширение Галуа. Тогда **существует естественная биекция между следующими множествами.**

(а) Группой Галуа $\mathrm{Aut}_k(K)$

(б) Простые идеалы в $K \otimes_k K$.

(в) Гомоморфизмы $K \otimes_k K \longrightarrow K$,

тождественные на $K = K \otimes_k k \subset K \otimes_k K$.

Доказательство биективности построенных отображений из (а) в (б) и наоборот.

Шаг 4: Удобнее доказывать биективность соответствия между (а) и (в). Для каждого $\zeta \in \mathrm{Aut}_k(K)$, соответствующий гомоморфизм v_ζ удовлетворяет $v_\zeta(a \otimes 1) = a$, $v_\zeta(1 \otimes a) = \zeta^{-1}(a)$. **Для соответствующего идемпотента получаем $a \otimes 1 \cdot e = 1 \otimes \zeta(a) \cdot e$, то есть $L_e(a) = R_e(\zeta(a))$.** Значит, соответствие (а) $\Rightarrow$ (в) $\Rightarrow$ (а) биективно на $\mathrm{Aut}_k(K)$.

Шаг 5. В обратную сторону: Достаточно убедиться, что идемпотент однозначно восстанавливается по автоморфизму ζ. Если есть два идемпотента e, e' с одинаковым ζ, соответствующие гомоморфизмы в K удовлетворяют $v_e(a \otimes 1) = v_{e'}(a \otimes 1) = a$ и $v_e(1 \otimes a) = v_{e'}(1 \otimes a) = \zeta^{-1}(a)$, **то есть равны на $K \otimes_k K$.** ■

Порядок группы Галуа

СЛЕДСТВИЕ: Порядок группы Галуа равен степени $[K:k]$.

ДОКАЗАТЕЛЬСТВО: $\mathrm{Aut}_k(K)$ находится в биективном соответствии с компонентами $K \otimes_k K$, что дает $|\mathrm{Aut}_k(K)| = \dim_K(K \otimes_k K) = \deg[K:k]$. ■

СЛЕДСТВИЕ: Пусть $[K:k]$ – расширение Галуа. Рассмотрим действие группы Галуа $\mathrm{Aut}_k(K)$ на $K \otimes_k K$ автоморфизмами, $\zeta(a \otimes b) = a \otimes \zeta(b)$. **Это действие транзитивно на компонентах разложения в прямую сумму $K \otimes_k K = \oplus K$.**

ДОКАЗАТЕЛЬСТВО: Достаточно убедиться, что $\mathrm{Aut}_k(K)$ действует транзитивно на простых идеалах в $K \otimes_k K$. Но **каждый такой простой идеал является ядром гомоморфизма $K \otimes_k K \longrightarrow K$ вида $a \otimes b \longrightarrow a\zeta(b)$.** ■

Инварианты группы Галуа

Левое и правое действие K на $K \otimes_k K$ отличается на действие группы Галуа.

ЛЕММА: Пусть $[K : k]$ – расширение Галуа, а $K \otimes_k K = \bigoplus_{\zeta \in \mathrm{Aut}_k(K)} K_\zeta$ – разложение $K \otimes_k K$ в компоненты, пронумерованные элементами группы Галуа. Обозначим через μ_l левое действие K^* на $K \otimes_k K$, а за μ_r правое действие. **Тогда** $\mu_l(a)e_\zeta = \mu_r(\zeta(a))e_\zeta$.

ДОКАЗАТЕЛЬСТВО: K_ζ отождествляется с образом гомоморфизма $K \otimes_k K \longrightarrow K$, переводящего $v_1 \otimes v_2$ в $v_1\zeta(v_2)$. Каждое $a \in K$ действует на соответствующей компоненте $K_\zeta \subset K \otimes_k K$ по формуле $\mu_l(a)(v_1 \otimes v_2) = av_1\zeta(v_2)$ и $\mu_r(a)(v_1 \otimes v_2) = v_1\zeta(av_2) = \zeta(a)v_1\zeta(v_2)$. ■

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – расширение Галуа, а $a \in K$ – элемент, инвариантный относительно $\mathrm{Aut}_k(K)$. **Тогда** $a \in k \subset K$.

ДОКАЗАТЕЛЬСТВО: Поскольку $\mu_l(a) = \mu_r(a)$ на $K \otimes_k K$, имеем $a \otimes_k 1 = 1 \otimes_k a$, что влечет $a \in K$. ■

Основная теорема теории Галуа

ТЕОРЕМА: (Основная теорема теории Галуа)
Пусть $[K:k]$ – расширение Галуа. Тогда соответствия **стрелки** $G' \longrightarrow K^{G'}$ **и** $K' \longrightarrow \operatorname{Aut}_{K'} K \subset G$ **устанавливают биекцию между множеством подгрупп** $G' \subset \operatorname{Aut}_k(K)$ **и множеством промежуточных подполей** $K \supset K' \supset k$**.**

Доказательство. Шаг 1: Для любого промежуточного подполя $K \supset K' \supset k$, расширение $[K:K']$ есть расширение Галуа. В силу предыдущего утверждения, $K^{G'} = K'$, где $G' = \operatorname{Aut}_{K'} K \subset G$. Получаем, что **соответствие (подполя)** $\Rightarrow$ **(подгруппы)** $\Rightarrow$ **(подполя) биективно.**

Шаг 2: Осталось убедиться, что две подгруппы $G_1, G_2 \subset G$ не могут удовлетворять $K' := K^{G_1} = K^{G_2}$. Без ограничения общности можно считать, что $G_1 = \operatorname{Aut}_{K'} K$, а $G_2 \subsetneq G_1$. **Поэтому все следует из такой леммы.**

ЛЕММА: Пусть $[K:k]$ – расширение Галуа, а $G' \subsetneq \operatorname{Aut}_k K$ есть нетривиальная подгруппа группы Галуа. **Тогда** $K^{G'} \neq k$**.**

Доказательство см. следующий слайд.

Основная теорема теории Галуа (окончание)

ЗАМЕЧАНИЕ: Пусть группа G действует на векторном пространстве V. **Тогда** $(V \otimes_k V)^{G\times G} = V^G \otimes_k V^G$. **Докажите это!**

ЛЕММА: Пусть $[K : k]$ – расширение Галуа, а $G' \subsetneq \operatorname{Aut}_k K$ есть нетривиальная подгруппа группы Галуа. **Тогда** $K^{G'} \neq k$.

Доказательство. Шаг 1: Поскольку $K^{G'} = k$, имеем $(K \otimes_k K)^{G'\times G'} = k$.

Шаг 2: Пусть $\zeta \in G$, а $a \otimes b \xrightarrow{v_\zeta} a\zeta(b)$ – соответствующий гомоморфизм $K \otimes_k K \longrightarrow K$. Для любого $\chi \times \chi' \in G \times G$, $\chi \times \chi'(v_\zeta)$ переводит $a \otimes b$ в $\chi(a)\chi'\zeta(b)$, то есть имеет то же самое ядро, что у $v_{\chi'\zeta\chi^{-1}}$. Значит, $G \times G$ **переводит идемпотент** e_ζ **в** $e_{\chi'\zeta\chi^{-1}}$.

Шаг 3: Получаем, что действие G' **на** $K \otimes_k K$ **сохраняет нетривиальный идемпотент** $\sum_{g\in G'} e_g$, что противоречит утверждению шага 1. ■