Теория Галуа, лекция 5: расширения Галуа

Миша Вербицкий

8 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**.** ■

Алгебраические числа (повторение)

ОПРЕДЕЛЕНИЕ: Поле $\bar{\mathbb{Q}}$ алгебраических чисел есть множество всех элементов $\mathbb{C}$, алгебраичных над $\mathbb{Q}$.

ОПРЕДЕЛЕНИЕ: Алгебраическое замыкание k есть поле $[\bar{k} : k]$, алгебраически замкнутое и алгебраичное над k.

ПРИМЕР: Поле $\bar{\mathbb{Q}}$ является алгебраическим замыканием $\mathbb{Q}$

ТЕОРЕМА: Для любого поля k, **алгебраическое замыкание $[\bar{k} : k]$ существует, и оно единственно с точностью до изоморфизма.**

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. ■

Артиновы кольца (повторение)

ОПРЕДЕЛЕНИЕ: **Артиново кольцо над полем** k, если кольцо, которое конечномерна как векторное пространство над k.

ОПРЕДЕЛЕНИЕ: Артиново кольцо R называется **полупростым**, если в нем нет ненулевых нильпотентов.

ТЕОРЕМА: Пусть A – полупростое артиново кольцо. **Тогда** A **есть прямая сумма полей.**

УТВЕРЖДЕНИЕ: Пусть A и B – кольца над полем k. В силу билинейности произведения, **существует мультипликативная операция** $(A \otimes_k B) \times (A \otimes_k B) \longrightarrow A \otimes_k B$**, переводящая** $a \otimes b, a' \otimes b'$ **в** $aa' \otimes bb'$**.**

ОПРЕДЕЛЕНИЕ: Это кольцо называется **тензорным произведением колец** A **и** B, и обозначается $A \otimes_k B$.

ТЕОРЕМА: В характеристике 0, тензорное произведение полупростых алгебр всегда полупросто.

ПРИМЕР 1: Пусть $P(t)$ – полином над полем k, $[K : k]$ – расширение, а $K_1 = k[t]/P(t)$. Предположим, что $P(t)$ разлагается на линейные множители над K. **Тогда** $K_1 \otimes K \cong K[t]/P(t) = \oplus$

Расширения Галуа

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 $P(t) \in k[t]$ – неприводимый полином степени n, имеющий n попарно различных корней в $K = k[t]/P$. **Тогда $[K : k]$ – расширение Галуа.** В самом деле, $K \otimes_k K = K[t]/(P) = \bigoplus_i K[t]/(t - a_i)$

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

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

Кратные корни и производная

Полезное утверждение, которое будет использоваться дальше:

УТВЕРЖДЕНИЕ: Пусть $P(t)$ – неприводимый полином над полем k характеристики 0. **Тогда $P(t)$ имеет n попарно различных корней** в алгебраическом замыкании $\bar{k}$.

ДОКАЗАТЕЛЬСТВО: В поле $\bar{k}$ полином $P(t)$ разлагается на множители: $P(t) = \prod_i (t - \alpha_i)$. **Если среди корней есть кратные, $P(t)$ имеет общий делитель $Q(t)$ с $P'(t)$,** в $\bar{k}[t]$. Поскольку наличие общих делителей проверяется применением алгоритма Евклида, многочлен $Q(t)$ тоже определен над k. ■

Расширения Галуа и корни

ЛЕММА: Пусть $[K : K_1 : k]$ – цепочка конечных расширений, причем $K \otimes_k K_1 = K^{\oplus^n}$ и $K \otimes_{K_1} K = K^{\oplus^m}$. **Тогда** $K \otimes_k K = K^{\oplus^{nm}}$.

ДОКАЗАТЕЛЬСТВО: Поскольку $K_1 \otimes_{K_1} K = K$, имеем $K \otimes_k K = K \otimes_k K_1 \otimes_{K_1} K = K^{\oplus_n} \otimes_{K_1} K = K^{\oplus^{nm}}$. ■

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.**

Доказательство. Шаг 1: Рассмотрим цепочку расширений $K_0 = k \subset K_1 \subset K_2 \subset ...K_n = K$, полученных из k последовательным добавлением α_i. Каждое из этих расширений имеет вид $K_i = K_{i-1}[t]/P_i$, где $P_i(t)$ – какой-то из делителей $P(t)$ в $K_{i-1}[t]$. **В силу примера 1, каждое из** K_i **удовлетворяет** $K_i \otimes_{K_{i-1}} K = K^{\oplus^{n_i}}$.

Шаг 2: Применив индукцию, будем считать, что $K_{i-1} \otimes_k K = K^{\oplus^{m_i}}$. Поскольку $K_i \otimes_{K_{i-1}} K = K^{\oplus^{n_i}}$ в силу леммы выше, получаем

$$K_i \otimes_k K = (K_i \otimes_{K_{i-1}} K_{i-1}) \otimes_k K =$$
$$K_i \otimes_{K_{i-1}} (K_{i-1} \otimes_k K) = K_i \otimes_{K_{i-1}} K^{\oplus^{m_i}} = K^{\oplus^{m_i n_i}}.$$

Цепочки расширений Галуа

УТВЕРЖДЕНИЕ: Пусть $[K : k]$ – расширение Галуа, а $[K : K_1 : k]$ – цепочка расширений. **Тогда $[K : K_1]$ – тоже расширение Галуа.**

ДОКАЗАТЕЛЬСТВО: Из определения тензорного произведения, получаем K-линейную сюрьекцию $K \otimes_k K \longrightarrow K \otimes_{K_1} K$. Поскольку $K \otimes_k K = K^{\oplus^n}$, а $K \otimes_{K_1} K$ – его фактор по идеалу, $K \otimes_{K_1} K = K^{\oplus^{n'}}$. ■

Поля разложения

ОПРЕДЕЛЕНИЕ: Пусть $P \in k[t]$ – полином степени n без кратных корней над полем k характеристики 0. Положим $K_1 = k$, и рассмотрим последовательность расширений, $K_l \supset K_{l-1} \supset \cdots \supset K_1$, полученных индуктивно следующим образом. Пусть K_j построено. Разложим P на неприводимые сомножители $P = \prod P_i$ в K_j. Если все P_i линейны, мы закончили. В противном случае, пусть P_0 – неприводимый сомножитель P степени > 1. Возьмем $K_{j+1} = K_j[t]/P_0$. **Этот процесс заканчивается через конечное число шагов**, **(докажите это!)** и в результате мы получаем поле $[K : k]$. Это поле называется **полем разложения** (splitting field) многочлена P.

ЗАМЕЧАНИЕ: Несколько слайдов назад было доказано, что **поле разложения является полем Галуа.**

УТВЕРЖДЕНИЕ: 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 изоморфно полю разложения $P(t)$.** ■

СЛЕДСТВИЕ: Поле разложения многочлена определено однозначно. ■

Группа Галуа

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

ЗАМЕЧАНИЕ: K^* действует на $K \otimes_k K$ умножениями справа (**правое действие**) и слева (**левое**). Зафиксируем раз и навсегда левое действие, и будем рассматривать $K \otimes_k K$ как векторное пространство над K с левым действием 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 $K \otimes_k K \longrightarrow K$, линейные относительно левого действия K.

Доказательство см. следующий слайд.

Группа Галуа (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 $K \otimes_k K \longrightarrow K$, линейные относительно левого действия K.

ДОКАЗАТЕЛЬСТВО: Биекция между (б) и (в) строится так: **каждому простому идеалу соответствует проекция** $K \otimes_k K = K^{\oplus^n} \longrightarrow K$, а из K-линейности получаем, что такое отображение однозначно задается своим идеалом.

Ограничивая K-линейный гомоморфизм $\mu: K \otimes_k K \longrightarrow K$ на $K = k \otimes K \subset K \otimes K$, получаем k-линейный гомоморфизм $\mu|_{k \otimes_k K}: K \longrightarrow K$. Это задает отображение из (в) в (а).

Для каждого элемента группы Галуа $\nu \in \mathrm{Aut}_k(K)$, определим гомоморфизм $K \otimes_k K \longrightarrow K$ по формуле $v_1 \otimes v_2 \longrightarrow v_1 \nu(v_2)$. Это задает обратную биекцию из (а) в (в). ■

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

ДОКАЗАТЕЛЬСТВО: Каждое $a \in K$ действует на соответствующей компоненте $K_\nu \subset K \otimes_k K$ по формуле $\mu_l(a)(v_1 \otimes v_2) = av_1\nu(v_2)$ и $\mu_r(a)(v_1 \otimes v_2) = v_1\nu(av_2) = \nu(a)v_1\nu(v_2)$. ■

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

ЛЕММА: Пусть $[K:k]$ – расширение Галуа, а K' – промежуточное поле, $K \supset K' \supset k$. **Тогда $K' = K^{G'}$, где $G' \subset \mathrm{Aut}_{K'}(K)$ – группа K'-линейных автоморфизмов K, а $K^{G'}$ обозначает множество G'-инвариантов.**

ДОКАЗАТЕЛЬСТВО: $[K:K']$ – расширение Галуа, а $G' = \mathrm{Aut}_{K'}(K)$ значит, $K^{G'} = K'$. ■

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

ДОКАЗАТЕЛЬСТВО: Из предыдущей леммы, получаем, что $G' = \mathrm{Aut}_{K'}(K)$ однозначно задает $K' = K^{G'}$. ■