Теория Галуа, лекция 2: расширения полей

Миша Вербицкий

25 января, 2013

матфак ВШЭ

Расширения полей

ОПРЕДЕЛЕНИЕ: Расширение поля k есть поле K, содержащее k. Отношение «быть расширением» обозначается $[K : k]$.

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.

Утверждение 1: Если $[K : K_1]$ и $[K_1 : k]$ – конечные расширения, то $[K : k]$ тоже конечно.

ДОКАЗАТЕЛЬСТВО: Возьмем базис $a_1, ..., a_n$ в K_1 над k, и $b_1, ..., b_m$ в K над K_1. Тогда $k\langle a_1, ..., a_n\rangle = K_1$, что дает

$$K = \bigoplus_{i=1}^{m} K_1 \cdot b_i = \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{n} k \cdot a_j b_i$$

то есть конечномерно. ■

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.

Конечные расширения

ОПРЕДЕЛЕНИЕ: **Делители нуля** в кольце суть такие x, y, что $xy = 0$.

ОПРЕДЕЛЕНИЕ: Если $k \subset K$ – подполе K, а V, W – линейные пространства над K, мы можем рассмотреть V, W как линейные пространства V_k, W_k над k. В такой ситуации, линейное отображение $V_k \to W_k$ называется **k-линейным отображением пространства V в W.**

УТВЕРЖДЕНИЕ: Пусть K – конечномерное пространство над k, снабженное структурой кольца. **Если K не имеет делителей нуля, то это поле.**

Доказательство. Шаг 1: Для любого конечного расширения $[K : k]$, рассмотрим умножение на $x \in K$ как k-линейный эндоморфизм $A_x : K \to K$. Ядра у него нет, потому что K без делителей нуля. **Поскольку размерность ядра равна размерности коядра, A_x сюрьективен.**

Шаг 2: Значит, найдется $y \in A$ такой, что $xy = 1$. ■

СЛЕДСТВИЕ: Пусть $x \in K$ – элемент расширения $[K : k]$, алгебраичный над k. **Тогда кольцо $k[x]$, порожденное x, это поле.** ■

Корни многочленов

ОПРЕДЕЛЕНИЕ: Пусть $P(t) \in K[t]$ – многочлен степени > 0. **Корень** P есть $\alpha \in K$ такое, что $P(\alpha) = 0$.

ТЕОРЕМА: Пусть $[K : k]$ расширение, а $x \in K$. Тогда следующие условия равносильны.
(i) x **– корень многочлена** $P(x) = 0$ над k.
(ii) **алгебраичен.**

ДОКАЗАТЕЛЬСТВО: , Если x алгебраичен, то $k[x]$ конечномерно над k, то есть x^d выражается как линейная комбинация x^{d-1}, x^{d-2}, ... x, 1 с коэффициентами из k. **Значит,** x **корень полинома.**

Наоборот, если x – корень многочлена, то x^d выражается как линейная комбинация x^{d-1}, x^{d-2}, ... x, 1, значит $k[x]$ **конечномерно над** k**;** в силу доказанного выше утверждения, $k[x]$ **конечномерное кольцо без делителей нуля, то есть поле.** ■

Алгебраические числа

ЗАМЕЧАНИЕ: Пусть $[K_1 = k[x] : k]$ конечное расширение, а $[K_2 = K_1[y] : K_1$ – тоже конечное расширение. Значит, **кольцо $k[x,y]$, порожденное x и y, конечномерно.**

СЛЕДСТВИЕ: Пусть $[K : k]$ – конечное расширение, $x_1, ..., x_n \in K$ – алгебраические элементы. Тогда **кольцо $R := k[x_1, x_2, ..., x_n]$, порожденное $x_1, ..., x_n$, является полем,** и расширение $[R : k]$ конечно. ■

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

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

ОПРЕДЕЛЕНИЕ: Поле K **алгебраически замкнуто**, если любой многочлен $P(t) \in k[t]$ имеет корень в K.

Алгебраические числа (продолжение)

ТЕОРЕМА: Поле $\bar{\mathbb{Q}}$ алгебраически замкнуто.

Доказательство. Шаг 1: $\mathbb{C}$ алгебраически замкнуто, значит, **любой многочлен $P(t) \in \bar{\mathbb{Q}}[t]$ над $\bar{Q}$ имеет корень в $\mathbb{C}$.**

Шаг 2: Пусть α – корень многочлена $P(t)$ с коэффициентами в $\bar{\mathbb{Q}}$. Рассмотрим **поле K, порожденное этими коэффициентами.** Поскольку коэффициенты $P(t)$ алгебраичны, расширение $[K : k]$ конечно. Значит, α алгебраичен над K.

Шаг 3: Расширение $[K : \mathbb{Q}]$ конечно и $[K[\alpha] : K]$ тоже конечно. **В силу «Утверждения 1» со 2-й страницы, $[K[\alpha] : \mathbb{Q}]$ – конечное расширение.** ■

ЗАМЕЧАНИЕ: Коль скоро $\bar{\mathbb{Q}}$ счетно **(проверьте это!)** а $\mathbb{C}$ несчетно, в $\mathbb{C}$ существуют неалгебраические числа. Они называются **трансцендентными**.

Трансцендентными являются числа e, π, e^α для любого алгебраического $\alpha \neq 0$, e^π, $2^{\sqrt{2}}$, $\ln(\alpha)$ для любого алгебраического $\alpha \neq 1$, и число Фредгольма $\sum_{i=0}^{\infty} 2^{-2^i}$.

Алгоритм Евклида

ЗАМЕЧАНИЕ: В дальнейшем, все полиномы предполагаются по умолчанию **положительной степени.**

ТЕОРЕМА: (Алгоритм Евклида)
Пусть $P(t), Q(t) \in k[t]$ – полиномы над полем k. **Тогда существует полином $V(t)$, делящий $P(t)$ и $Q(t)$, который можно можно выразить как линейную комбинацию P и Q** над $k[t]$. ■

УПРАЖНЕНИЕ: Докажите эту теорему.

ОПРЕДЕЛЕНИЕ: Наибольший общий делитель P и Q есть полином наибольшей степени, который делит P и Q.

ЗАМЕЧАНИЕ: Наибольший общий делитель $P(t)$ и $Q(t)$ пропорционален $V(t)$, построенному выше. Действительно, **любой делитель $P(t)$ и $Q(t)$ обязан делить их линейную комбинацию** $V(t) = A(t)P(t) + B(t)Q(t)$.

СЛЕДСТВИЕ: Кольцо полиномов $k[t]$ **факториально** (обладает однозначным разложением на простые множители).

Неприводимые полиномы

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 $k[t]/(P)$ не имеет делителей нуля.**

Доказательство. Шаг 1: Произведение полиномов, взаимно простых с $P(t)$, снова взаимно просто с $P(t)$, в силу факториальности.

Шаг 2: Поэтому, если полином $P(t)$ неприводим, то любой полином $Q(t)$ **либо делится на $P(t)$, либо взаимно прост с ним.** Значит $k[t]/(P)$ не имеет делителей нуля.

Шаг 3: Наоборот, если $k[t]/(P)$ не имеет делителей нуля, то произведение полиномов, которые не делятся на $P(t)$, тоже не делится на $P(t)$. ■

Минимальный полином

УТВЕРЖДЕНИЕ: Пусть v – элемент конечномерной алгебры R над k. Рассмотрим подпространство R, порожденное $1, v, v^2, v^3, \dots$ (для всех степеней v). Пусть оно n-мерно. **Тогда $P(v) = 0$ для некоторого полинома $P = t^n + a_{n-1}t^{n-1} + \dots$ с коэффициентами из k. Более того, этот полином единственный**.

Доказательство. Шаг 1: Существование нетривиального полинома P степени $d \leqslant n$, удовлетворяющего $P(v) = 0$, **сразу следует из наличия линейных соотношений между $1, v, v^2, v^3, \dots$.** (если таких соотношений нет, R должно быть как минимум $n+1$-мерно).

Шаг 2: $\deg P \leqslant n$, потому что $v^d, v^{d+1}, \dots$ **выражаются через $1, v, v^2, v^3, \dots, v^{d-1}$.** Мы получили, что $\deg P = n$

Шаг 3: Если таких полиномов 2, то **они равны, либо их разность $Q(t)$ – полином степени $< n$, удовлетворяющий $Q(v) = 0$.** Это доказывает единственность. ■

Минимальный полином (продолжение)

ОПРЕДЕЛЕНИЕ: Пусть v – элемент конечномерной алгебры R над k, а $P(t) == t^n + a_{n-1}t^{n-1} + \dots$ полином минимальной степени с коэффициентами из k, удовлетворяющий $P(v) = 0$. Этот полином называется **минимальный полином** $v \in R$.

ЗАМЕЧАНИЕ: Минимальный полином линейного оператора определяется точно также.

Утверждение 2: 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 $k[t]/(P)$.**

ДОКАЗАТЕЛЬСТВО: Определим гомоморфизм $k[t]/(P) \to R_v$, переводящий t в v. Он по построению сюръективен. Поскольку $\dim R_v = \deg P$, размерность этих колец одинаковая. ■

Примитивные расширения

Пусть $P(t) \in k[t]$ – неприводимый полином. **Поскольку $k[t]/(P)$ конечномерно над k и не имеет делителей нуля, это поле.** А поскольку $P(t) = 0$ имеет решение t в $k[t]/(P)$, $P(t)$ имеет корень в этом поле.

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.

Доказательство. Шаг 1: Возьмем $\alpha \in K$, и пусть $K_1 = k[\alpha]$ – кольцо, порожденное α. Тогда $[K_1 : K_0]$ **примитивно, в силу Утверждения 2.**

Шаг 2: Если $K_1 \neq K$, повторим эту процедуру, получив примитивное расширение $[K_2 : K_1]$ и так далее. На каждом шаге размерность K_i над k увеличивается, но она не может быть больше $\dim_k K$, поэтому **этот процесс остановится, когда $K_n = K$.** ■

Идеалы в кольце

ЗАМЕЧАНИЕ: Все кольца в дальнейшем предполагаются коммутативные, с единицей, и $1 \neq 0$. Все гомоморфизмы сохраняют 1. Все идеалы в кольце R по умолчанию предполагаются **нетривиальными**, то есть не равными R. Кольцо, содержащее поле k, называется **коммутативной k-алгеброй**, или **кольцом над k**.

ОПРЕДЕЛЕНИЕ: **Максимальный идеал** в кольце есть идеал, который не содержится ни в каком большем.

УПРАЖНЕНИЕ: Докажите, что **идеал $I \subset R$ максимален тогда и только тогда, когда R/I – поле.**

ТЕОРЕМА: Каждый идеал I в кольце **содержится в максимальном идеале.** ■

УПРАЖНЕНИЕ: Докажите это.

Тензорные произведения колец

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

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

ПРИМЕР: Пусть $k[t_1, t_2, ..., t_p]$, $k[u_1, u_2, ..., u_q]$ – кольца полиномов. **Тогда**

$$k[t_1, t_2, ..., t_p] \otimes_k k[u_1, u_2, ..., u_q] \cong k[t_1, t_2, ..., t_p, u_1, u_2, ..., u_q].$$

УТВЕРЖДЕНИЕ: Пусть $R = k[u_1, u_2, ..., u_d]$ кольцо полиномов от какого-то набора переменных, а $F_i \in k[u_i]$ – полином положительной степени. Рассмотрим идеал $I \subset R$, порожденный $F_i(u_i)$. **Тогда** $R/I = \otimes_{i=1}^{d} \Big(k[u_i]/(F_i) \Big)$.

Доказательство. Шаг 1: Положим $R' := k[u_1, u_2, ..., u_{d-1}]$, и пусть идеал I' порожден $F_1(u_1), ..., F_{d-1}(u_{d-1})$. **Воспользовавшись индукцией, получим** $R'/I' = \otimes_{i=1}^{d-1} \Big(k[u_i]/(F_i) \Big)$.

Тензорные произведения колец (продолжение)

ЛЕММА: Пусть $R = k[u_1, u_2, ..., u_d]$ кольцо полиномов от какого-то набора переменных, а $F_i \in k[u_i]$, $i = 1, ..., d$ – полиномы положительной степени. Рассмотрим идеал $I \subset R$, порожденный $F_i(u_i)$. **Тогда**

$$R/I = \bigotimes_{i=1}^{d} \Big(k[u_i]/(F_i) \Big).$$

Доказательство. Шаг 1: Положим $R' := k[u_1, u_2, ..., u_{d-1}]$, и пусть идеал I' порожден $F_1(u_1), ..., F_{d-1}(u_{d-1})$. **Воспользовавшись индукцией, получим** $R'/I' = \otimes_{i=1}^{d-1} \Big(k[u_i]/(F_i) \Big)$.

Шаг 2: $R = R' \otimes_k k[u_d]/(F_d(u_d))$, ибо **по модулю I' идеал I главный и порожден $(F_d(u_d))$.**

Шаг 3: Искомый изоморфизм получается из объединения утверждений шага 1 и шага 2. ■

СЛЕДСТВИЕ: Кольцо R/I, определенное в этом утверждении, ненулевое.

Тензорные произведения колец (окончание)

ЛЕММА: Пусть $R = k[u_1, u_2, ...,]$ кольцо полиномов от какого-то набора переменных, не обязательно конечного, а $F_i \in k[u_i]$, $i = 1, 2, ...$ – полиномы положительной степени. Рассмотрим идеал I, порожденный $F_i(u_i)$. **Тогда I – собственный идеал, то есть не содержит 1.**

Доказательство. Шаг 1: Если I содержит 1, то существует конечное линейное выражение вида $1 = \sum_{l=1}^{k} A_l F_{i_l}(u_{i_l})$, где $A_l \in k[u_1, u_2, ...,]$. Рассмотрим конечно-порожденное подкольцо $R' = k[u_1, u_2, ..., u_d]$, в которое входят все переменные, встречающиеся в полиномах A_l, и все u_{i_l}. **Из $1 = \sum_{l=1}^{k} A_l F_{i_l}(u_{i_l})$ следует, что $1 \in I \cap R'$.**

Шаг 2: В силу предыдущей леммы, $R'/I \cap R' \neq 0$, но это противоречит тому, что $1 \in I \cap R'$. ■

Конструкция алгебраического замыкания

Пусть $\mathfrak{S}$ – множество всех полиномов положительной степени $F_\alpha \in k[t]$ над полем k, $R_{\mathfrak{S}} = k[u_1, u_2, ...,]$ кольцо полиномов, проиндексированное $\alpha \in \mathfrak{S}$, а $F_\alpha(u_\alpha)$ – соответствующие полиномы. Пусть $I \subset R$ – идеал, порожденный всеми $F_\alpha(u_\alpha)$, а $\mathfrak{I}$ – максимальный идеал, содержащий I.

ТЕОРЕМА: Пусть $K := R_{\mathfrak{S}}/\mathfrak{I}$ – поле, полученное как фактор $R_{\mathfrak{S}}$ по $\mathfrak{I}$. **Тогда $[K : k]$ алгебраично, а любой полином $P(t) \in k[t]$ положительной степени имеет корень в K.**

Доказательство. Шаг 1: Я буду обозначать элементы K, полученные из $u_\alpha \in R$, той же буквой. Пусть $F_\alpha(t) \in k[t]$ – какой-то полином. Поскольку $F_\alpha(u_\alpha) = 0$ в R/I, $F_\alpha(t)$ имеет корень в K.

Шаг 2: Любой u_α является корнем полинома $F_\alpha(t)$, то есть алгебраичен над k. Но все элементы K выражаются через полиномы от u_α. ■

СЛЕДСТВИЕ: Для каждого поля k **существует алгебраическое расширение $[k' : k]$ такое, что все многочлены $P(t) \in k[t]$ положительной степени имеют корни в K.**

ВОПРОС: А почему из этого не следует сразу что $[k' : k]$ – алгебраическое замыкание k?

Конструкция алгебраического замыкания (продолжение)

Напомню, что **алгебраическое замыкание** поля k есть алгебраическое расширение $[\bar{k} : k]$, которое алгебраически замкнуто.

ТЕОРЕМА: Пусть k – поле. **Тогда существует алгебраическое замыкание** $[\bar{k} : k]$**.**

ДОКАЗАТЕЛЬСТВО: Мы можем построить расширение $[k' : k]$ такое, что все полиномы над k имеют корни в k'. Нам нужно, чтобы все полиномы над k' имели корни в k; это верно, но не вполне очевидно. Вместо этого мы рассмотрим цепочку расширений $k \subset k' \subset k'' \subset ...$, и **положим** $\bar{k} := k \cup k' \cup k'' \cup ....$

Шаг 2: Возьмем полином $P(t) \in \bar{k}$. Каждый из его коэффициентов лежит в одном из полей $k^{(i)}$, их конечное число, что дает $P(t) \in k^{(n)}[t]$. Тогда $P(t)$ имеет корень в $k^{(n+1)}$.

Шаг 3: Осталось убедиться, что $\bar{k}$ алгебраично над k. Каждый элемент $x \in \bar{k}$ лежит в каком-то $k^{(n)}$, значит, **достаточно доказать, что** $[k^{(n)} : k]$ **алгебраично.**

Конструкция алгебраического замыкания (окончание)

Шаг 3: Осталось убедиться, что $\overline{k}$ алгебраично над k. Каждый элемент $x \in \overline{k}$ лежит в каком-то $k^{(n)}$, значит, **достаточно доказать, что** $[k^{(n)} : k]$ **алгебраично.**

Шаг 4: Имеем конечную цепочку расширений $[k^{(n)} : k^{(n-1)} : ... : k]$, и каждое последовательное расширение алгебраично. Поэтому **алгебраичность** $[k^{(n)} : k]$ **вытекает из следующей леммы.**

ЛЕММА: Пусть $K_2 \supset K_1 \supset K_0$ – расширения полей, причем $[K_i : K_{i-1}]$ алгебраично. **Тогда** $[K_2 : K_0]$ **алгебраично.**

ДОКАЗАТЕЛЬСТВО: Каждый $x \in K_2$ является корнем многочлена $P(t) \in K_1[t]$. Возьмем поле $[K_1' : K_0]$, содержащее все коэффициенты $P(t)$. Оно конечно над K_0, потому что порождено конечным числом алгебраических элементов. **Получаем цепочку конечных расширений** $[K_1'[x] : K_1' : K_0]$**,** то есть $[K_1'[x] : K_0]$ конечно (Утверждение 1). ■