Теория Галуа, лекция 3: тензорные произведения полей

Миша Вербицкий

1 февраля, 2013

матфак ВШЭ

Расширения полей (повторение)

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.

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.

Алгебраические числа (повторение)

ТЕОРЕМА: 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.

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

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 $\sum_{i=0}^\infty 2^{-2^i}$.

Минимальные полиномы (повторение)

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

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

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 $k[t]/(P)$.** ■

Неприводимые полиномы (повторение)

ТЕОРЕМА: Кольцо полиномов $k[t]$ **факториально** (с однозначным разложением на множители). ■

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. ■

Тензорные произведения колец (повторение)

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**

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

ПРИМЕР: $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C} \oplus \mathbb{C}$.

ПРИМЕР: Пусть $\mathbb{R}(t)$ – поле рациональных функций с коэффициентами из $\mathbb{R}$. Тогда $\mathbb{R}(t) \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}(t)$.

ЗАМЕЧАНИЕ: Как будет доказано на следующей лекции, **тензорное произведение полей есть «почти всегда» прямая сумма полей.**

Бесконечное тензорное произведение

Я сейчас буду определять **"бесконечное тензорное произведение"** для бесконечного набора колец $R_\alpha \supset k$, проиндексированных набором индексов $\alpha \in \mathfrak{S}$.

Пусть $S \subset \mathfrak{S}$ – конечное подмножество, а $R_S := \bigotimes_{\alpha \in S} R_\alpha$ – произведение (над k) всех колец, входящих в S.

ЛЕММА: Пусть $S \subset S'$ – подмножество, а $\zeta = x_1 \otimes_k x_2 \otimes ... \in R_S$ какой-то моном, а $\zeta' := x_1 \otimes_k x_2 \otimes ... \otimes 1 \otimes 1 \in R_{S'}$ соответствующий моном в $R_{S'}$, дополненный единицами. Рассмотрим отображение $R_S \xrightarrow{\varphi(S,S')} R_{S'}$, переводящее ζ в ζ'. **Тогда φ индуцирует вложение колец.** ■

ОПРЕДЕЛЕНИЕ: Бесконечное тензорное произведение $\bigoplus_{\alpha \in \mathfrak{S}} R_\alpha$ есть объединение R_S для всех конечных подмножеств $S \subset \mathfrak{S}$ по вложениям $\varphi(S, S')$.

Конструкция алгебраического замыкания

Пусть $\mathfrak{S}$ – множество всех конечных расширений $[K_\alpha : k]$, проиндексированных $\alpha \in \mathfrak{S}$, а $R_\mathfrak{S} := \bigotimes_{\alpha\in\mathfrak{S}} K_\alpha$ – произведение (над k) всех полей, входящих в S.

ТЕОРЕМА: Пусть$\mathfrak{I}$ – максимальный идеал, а $K := R_\mathfrak{S}/\mathfrak{I}$ – 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: Каждый элемент $R_\mathfrak{S}$ происходит из конечного произведения, то есть представлен в виде $\zeta \in R_S \hookrightarrow R_\mathfrak{S}$, где R_S – алгебра, которая конечномерна над k. Поскольку ζ лежит в конечномерной алгебре, у ζ есть минимальный полином $P(t)$, с коэффициентами из k. **Значит, все элементы K алгебраичны.**

Шаг 2: Для любого неприводимого полинома $P(t)$, соответствующее поле $K_P := k[t]/(P)$ содержит корень $P(t)$. Поскольку $R_\mathfrak{S}$ содержит K_P, существует $\zeta \in R_\mathfrak{S}$ такой, что $P(\zeta) = 0$

Шаг 3: Образ ζ в K является корнем $P(t)$. ■

Конструкция алгебраического замыкания (продолжение)

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.**

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. Шаг 1: 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 $k^{(n+1)}$.

Конструкция алгебраического замыкания (окончание)

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.**

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. ■

Идеалы в кольцах (повторение)

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.

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

ОПРЕДЕЛЕНИЕ: Элемент $r \in R$ в кольце R называется **нильпотентным**, если $r^k = 0$, для какого-то $k \in \mathbb{N}$.

ЗАМЕЧАНИЕ: Множество всех нильпотентов в кольце образует идеал **(проверьте это).** Этот идеал называется **нильрадикалом** кольца.

УПРАЖНЕНИЕ: Докажите, что **фактор кольца по нильрадикалу не имеет ненулевых нильпотентов.**

Артиновы кольца

ОПРЕДЕЛЕНИЕ: Кольцо над полем (ассоциативное, коммутативное, но не обязательно с единицей) будем называть **коммутативной алгеброй**.

ОПРЕДЕЛЕНИЕ: Пусть дана коммутативная алгебра R с единицей над полем k. Говорят, что R **артиново кольцо над полем** k, если R конечномерна как векторное пространство.

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

ОПРЕДЕЛЕНИЕ: Пусть $R_1, \ldots, R_n$ – алгебры над полем. Возьмем прямую сумму $\oplus R_i$, с естественным (почленным) умножением и сложением. Получившаяся алгебра называется **прямой суммой** R_i, обозначается $\oplus R_i$.

Сейчас я буду доказывать такую теорему.

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

Конечномерные алгебры над полем и идемпотенты

ОПРЕДЕЛЕНИЕ: Пусть $v \in R$ – такой элемент алгебры R, что $v^2 = v$. Тогда v называется **идемпотентом**.

ЗАМЕЧАНИЕ: Произведение идемпотентов - идемпотент. Если e – идемпотент, то $1 - e$ – тоже идемпотент.

СЛЕДСТВИЕ: Для идемпотента e, произведение $e(1 - e)$ равно нулю. Поэтому **каждый идемпотент $e \in A$ задает разложение A в прямую сумму:** $A = eA + (1 - e)A$ **(проверьте это)**

Конечномерные алгебры над полем и идемпотенты (продолжение)

УТВЕРЖДЕНИЕ: Пусть A – коммутативная алгебра, в которой нет нильпотентов и конечномерная над полем. **Тогда A содержит идемпотент.**

Доказательство. Шаг 1: Поскольку A конечномерно, любая убывающая цепочка идеалов обрывается. Значит, **есть идеал $I \subset A$, который не содержит ненулевых идеалов.** Дальше мы будем рассматривать этот идеал как подалгебру в A (без единицы).

Шаг 2: Поскольку в A нет нильпотентов, $z^2 \neq 0$. А поскольку I минимальный, для любого ненулевого $z \in I$, имеем $zI = I$.

Шаг 3: Му доказали, что умножение на любой $z \in I$ не имеет ядра в I. Следовательно, **все элементы I обратимы,** как эндоморфизмы I.

Шаг 4: Поскольку I конечномерно, элементы $z, z^2, z^3, ... \in \operatorname{End} I$ линейно зависимы, что дает выражение вида $P(z) = 0$. Если у этого полинома нет свободного члена, разделим на z, пользуясь тем, что у z нет ядра. Получим соотношение $\operatorname{Id}_I = az + bz^2 + cz^3 + ...$ в кольце эндоморфизмов I.

Шаг 5: Элемент $U := az + bz^2 + cz^3 + ...$ удовлетворяет $Ux = x$ для любого $x \in I$, **поэтому является идемпотентом.** ■

Структурная теорема для полупростых артиновых алгебр

ЗАМЕЧАНИЕ: Аргумент шага 5 доказывает следующее утверждение. Пусть I – коммутативная алгебра без делителей нуля, конечномерная над полем. **Тогда I содержит единицу, т.е. является полем.**

СЛЕДСТВИЕ: Пусть A есть кольцо, конечномерное над полем, и без нильпотентов. **Тогда A есть прямая сумма полей.**

Доказательство. Шаг 1: Пусть $I \subset A$ – нетривиальный идеал. В силу доказанного утверждения, I содержит ненулевой идемпотент a.

Тогда a и $a-1$ – идемпотенты, произведение которых равно нулю, а сумма равна 1. **Это дает $A = aA \oplus (1-a)A$, где aA и $(1-a)A$ – подалгебры с единицей.** Воспользовавшись индукцией по $\dim A$, можно считать, что aA и $(1-a)A$ – прямые суммы полей. ■

В следующей лекции я буду применять эти знания к тензорным произведениям полей.

Структурная теорема для полупростых артиновых алгебр: единственность разложения

ЛЕММА: Пусть A есть прямая сумма полей, $A = \bigoplus_i k_i$. **Тогда разложение $A = \bigoplus_i k_i$ определено однозначно** с точностью до перестановки слагаемых.

ДОКАЗАТЕЛЬСТВО: Если $A = \bigoplus_i k_i = \bigoplus_i k_i'$, каждое из полей k_i разложится в прямую сумму, $k_i = \bigoplus_j k_i \cap k_j'$. Поскольку поле не имеет нетривиальных разложений такого вида, **получаем, что $k_i = k_j'$ для какого-то индекса j.** ■