Теория Галуа, лекция 4: тензорные произведения полей и композиты

Миша Вербицкий

8 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.

УТВЕРЖДЕНИЕ: Пусть $[K_2 : K_1 : K]$ – расширения полей. **Если** $[K_1 : K]$ **и** $[K_2 : K_1]$ **алгебраичны, то** $[K_2 : K]$ **алгебраично. Если они конечны, то** $[K_2 : K]$ **конечно.**

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**.

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. ■

Нильрадикал и идемпотенты (повторение)

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. Этот идеал называется **нильрадикалом** кольца.

УТВЕРЖДЕНИЕ: Фактор кольца по нильрадикалу не имеет ненулевых нильпотентов.

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)**

Артиновы кольца (продолжение)

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

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

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

Тензорные произведения колец (повторение)

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

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

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: $H^*(X \times Y, k) = H^*(X, k) \otimes_k H^*(Y, k)$ **(формула Кюннета)**

ПРИМЕР: $k[x, y]/(x^n, y^n) = k[x]/(x^n) \otimes_k k[y]/(y^n)$.

Инвариантные билинейные формы

ОПРЕДЕЛЕНИЕ: Пусть R – алгебра над полем k, а g – симметричная билинейная форма на R. Форма g называется **инвариантной**, если $g(x, yz) = g(xy, z)$ для любых x, y, z.

ЗАМЕЧАНИЕ: Если R содержит единицу, то для любой инвариантной формы g, имеем $g(x, y) = h(xy, 1)$, то есть g определяется линейным функционалом.

ПРИМЕР: На кольце $\mathbb{R}[x, y]/(x^{n+1}, y^{n+1}) = H^*(\mathbb{C}P^n \times \mathbb{C}P^n)$ есть функционал $\varepsilon(\sum a_{ij}x^i y^j) := a_{nn}$. **Соответствующая билинейная инвариантная форма $g(x, y) := \varepsilon(xy)$ невырождена (проверьте).** Это форма Пуанкаре на $H^*(\mathbb{C}P^n \times \mathbb{C}P^n)$

ОПРЕДЕЛЕНИЕ: Фробениусова алгебра есть конечномерная алгебра над полем, снабженная невырожденной билинейной инвариантной формой.

УПРАЖНЕНИЕ: Приведите пример артинова кольца, не допускающего такой формы.

Форма следа

УТВЕРЖДЕНИЕ: Пусть $[K:k]$ – расширение полей, а ε – ненулевой k-линейный функционал на K. **Тогда форма $g(x,y):=\varepsilon(xy)$ невырождена.**

ДОКАЗАТЕЛЬСТВО: Пусть $\varepsilon(a)\neq 0$. Тогда $g(x,x^{-1}a)\neq 0$. ■

ОПРЕДЕЛЕНИЕ: **След** линейного оператора есть сумма всех диагональных членов в каком-то матричном представлении.

ОПРЕДЕЛЕНИЕ: Пусть R – артиново кольцо над полем k. Рассмотрим билинейную форму $a,b\longrightarrow \operatorname{tr}(ab)$, где $\operatorname{tr}(ab)$ – след эндоморфизма $L_{ab}\in \operatorname{End}_k R$, $x\stackrel{L_{ab}}{\longrightarrow} abx$. Эта форма называется **формой следа**, и обозначается $\operatorname{tr}_k(ab)$.

ЗАМЕЧАНИЕ: Пусть $[K:k]$ – конечное расширение полей. В силу доказанного выше утверждения, **форма следа $\operatorname{tr}_k(ab)$ невырождена, если tr_k не тождественно равен нулю.**

Форма следа и сепарабельность

ОПРЕДЕЛЕНИЕ: Расширение $[K : k]$ называется **сепарабельным**, если форма следа $\mathrm{tr}_k(ab)$ ненулевая.

ЗАМЕЧАНИЕ: В характеристике 0, любое расширение сепарабельно, ибо $\mathrm{tr}_k(1) = \dim_k K$.

ТЕОРЕМА: Пусть R – артинова алгебра над k с невырожденной формой следа. **Тогда R полупросто.**

ДОКАЗАТЕЛЬСТВО: Поскольку $\mathrm{tr}_k(ab) = 0$ для любого нильпотента a (след нильпотентного оператора равен нулю), **в R нет нильпотентов.**
■

Тензорное произведение полей

ЛЕММА: Пусть R, R' – артиновы кольца над k. Обозначим естественные билинейные формы $a, b \longrightarrow \operatorname{tr}(ab)$ на них через g, g'. Рассмотрим тензорное произведение $R \otimes_k R'$ с естественной структурой артинова кольца. **Тогда форма следа на $R \otimes_k R'$ равна $g \otimes g'$.**

ДОКАЗАТЕЛЬСТВО: Если V, W – векторные пространства над k, μ, ρ – эндоморфизмы V, W, то след $\mu \otimes \rho$ на $V \otimes W$ равен $\operatorname{tr}(\mu)\operatorname{tr}(\rho)$, что ясно из блочного разложение матрицы $\mu \otimes \rho$. **Это дает след для разложимых векторов вида $r \otimes r' \in R \otimes_k R'$, на все остальные оно продолжается по линейности.** ■

СЛЕДСТВИЕ: Если $[K_1 : k]$, $[K_2 : k]$ – сепарабельные расширения, то $K_1 \otimes_k K_2$ **полупросто,** то есть изоморфно прямой сумме полей.

ДОКАЗАТЕЛЬСТВО: Потому что форма следа невырождена. ■

ЗАМЕЧАНИЕ: В частности, **в характеристике 0 произведение конечных расширений поля k есть всегда прямая сумма полей.**

Тензорные произведения полей: примеры

УТВЕРЖДЕНИЕ: Пусть $P(t)$ – полином над полем k, $[K:k]$ – расширение, а $K_1 = k[t]/P(t)$. **Тогда** $K_1 \otimes K \cong K[t]/P(t)$**.** ■

УТВЕРЖДЕНИЕ: 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** $K_1 \otimes K \cong K[t]/P(t) = \oplus$

ДОКАЗАТЕЛЬСТВО: Пусть $P = (t-a_1)(t-a_2)...(t-a_n)$. **По китайской теореме об остатках, отображение** $K[t]/(P) \longrightarrow \oplus_i K[t]/(t-a_i) = K$ **сюрьективно,** и по соображениям размерности, это изоморфизм. ■

УПРАЖНЕНИЕ: Пусть $P(t) \in \mathbb{Q}[t]$ – многочлен, у которого есть ровно r вещественных корней и ровно $2s$ комплексных, но не вещественных, причем все корни разные. **Докажите, что** $(\mathbb{Q}[t]/P) \otimes_{\mathbb{Q}} \mathbb{R} = \oplus_s \mathbb{C} \oplus \oplus_r \mathbb{R}$**.**

ЗАДАЧА: Докажите, что $[K:k]$ **несепарабельно тогда и только тогда, когда** $K \otimes_k K$ **содержит нильпотенты.**

Композит расширений

ОПРЕДЕЛЕНИЕ: Пусть K_1, K_2 – расширения k, причем $[K_1 : k]$ конечное. Обозначим за $\mathfrak{n}$ нильрадикал произведения $K_1 \otimes_k K_2$, и пусть $R = K_1 \otimes_k K_2/\mathfrak{n}$. Поскольку R конечномерно над K_2 и без нильпотентов, это прямая сумма полей. Каждое из этих полей называется **композитом** K_1 и K_2.

УТВЕРЖДЕНИЕ: K_1 и K_2 канонически вложено в любой их композит.

ДОКАЗАТЕЛЬСТВО: $K_1 \otimes_k 1 \subset K_1 \otimes_k K_2$ есть подполе, содержащее 1, и проекция $K_1 \otimes_k 1$ переводит 1 в 1, значит, не равна нулю. С другой стороны, ненулевой гомоморфизм из поля куда угодно есть вложение. ■

УТВЕРЖДЕНИЕ: Для каждого поля, допускающего k-линейный гомоморфизм $K_1 \xrightarrow{\mu_1} L$, $K_2 \xrightarrow{\mu_2} L$, **естественное отображение** $K_1 \otimes_k K_2 \xrightarrow{\mu_1 \otimes \mu_2} L$ **инъективно на каком-то из композитов** $K \subset K_1 \otimes_k K_2$**.**

ДОКАЗАТЕЛЬСТВО: Гомоморфизм из поля куда угодно инъективен либо равен нулю. С другой стороны, ограничение $\mu_1 \otimes \mu_2$ на $K_1 \otimes_k 1 \subset K_1 \otimes_k K_2$ равно μ_1, значит ненулевое. ■

Универсальное свойство композита

ТЕОРЕМА: (Универсальное свойство композита) Пусть K_1, K_2 – расширения k, причем одно из них конечное, а L – расширение k, снабженное k-линейными гомоморфизмами $K_1 \stackrel{\varphi}{\longrightarrow} L$, $K_2 \stackrel{\psi}{\longrightarrow} L$. Предположим, что L порождено образами φ и ψ. **Тогда L это композит K_1 и K_2.**

ДОКАЗАТЕЛЬСТВО: В силу предыдущего утверждения, существует инъективное отображение $K \longrightarrow L$, где K есть какой-то композит K_1 и K_2. **Поскольку L порожден образами K_1 и K_2, это отображение сюръективно.** ■

УТВЕРЖДЕНИЕ: Пусть $K = k[t]/P(t)$ – расширение, полученное добавлением корня неприводимого многочлена $P(t)$, а $P(t) = P_1(t)P_2(t)...P_n(t)$ – неприводимое разложение $P(t)$ над полем $K' \supset k$. **Тогда композиты K и K' суть все поля вида $K'[t]/P_i(t)$.**

ДОКАЗАТЕЛЬСТВО: Следует из того, что
$K \otimes_k K' = k[t]/(P) \otimes_k K = K[t]/(P) = \oplus_{i=1}^n K[t]/(P_i)$. ■

УПРАЖНЕНИЕ: Докажите последнее из этих равенств, используя китайскую теорему об остатках.

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 непростое?

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