

Теория Галуа, лекция 7: группы Галуа конечных полей и другие применения основной теоремы

Миша Вербицкий

1 марта, 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 $[K = K_n : K_{n-1} : K_{n-2} : \dots : K_0 = k]$, 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 .

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 $\alpha_1, \dots, \alpha_n$ в конечном расширении $[K : k]$. Предположим, что K порождено $\{\alpha_i\}$. **Тогда это расширение Галуа.**

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

ЗАМЕЧАНИЕ: В характеристике 0, поля разложения суть поля Галуа (в характеристике p , не обязательно)

УТВЕРЖДЕНИЕ: Если $[K : k]$ – конечное расширение, $\text{char } k = 0$, то существует расширение $[K_1 : K]$ такое, что $[K_1 : k]$ – расширение Галуа.

Группа Галуа (повторение)

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

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

- (а) Группой Галуа $\text{Aut}_k(K)$
- (б) Простые идеалы в $K \otimes_k K$.

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

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

Основная теорема теории Галуа (повторение)

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

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

ЗАМЕЧАНИЕ: (осталось с прошлой лекции)

Пусть группа G действует на векторном пространстве V .

Тогда $(V \otimes_k V)^{G \times G} = V^G \otimes_k V^G$. **Докажите это!**

ТЕОРЕМА: (Основная теорема теории Галуа)

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

Теорема о примитивном элементе

ТЕОРЕМА: (теорема Артина о примитивном элементе)

Пусть $[K : k]$ – конечное расширение, причем K бесконечно, и выполнено одно из условий: (1) $\text{char } k = 0$ (2) $[K : k]$ – расширение Галуа. **Тогда $[K : k]$ примитивно**, то есть порождено одним элементом $x \in K$.

Доказательство. Шаг 1: Заменяем $[K : k]$ на расширение Галуа $[K_1 : k]$, содержащее K . В силу основной теоремы теории Галуа, **существует не более чем конечное число промежуточных полей $K \supseteq K' \supseteq k$** . Обозначим за Z объединение всех этих подполей.

Шаг 2: Элемент x примитивен тогда и только тогда, когда $x \notin Z$. Значит, **теорема о примитивном элементе вытекает из следующей леммы.**

ЛЕММА: Пусть V – векторное пространство над бесконечным полем, а Z – конечное объединение подпространств $W_i \subsetneq V$, $i = 1, \dots, N$. **Тогда $V \setminus Z$ непусто.**

УПРАЖНЕНИЕ: Докажите это самостоятельно!

Теорема о примитивном элементе (окончание)

ЛЕММА: Пусть V – векторное пространство над бесконечным полем k , а Z – конечное объединение подпространств $W_i \subsetneq V$, $i = 1, \dots, N$. **Тогда $V \setminus Z$ непусто.**

Доказательство. Шаг 1: Без ограничения общности, можно считать все W_i гиперплоскостями, которые пересекаются трансверсально. Применяв индукцию по размерности V , **найдем точку $w \in W_0$, которая не принадлежит объединению $\bigcup_{j \neq 0} W_j$.**

Шаг 2: Рассмотрим гиперплоскость V' , трансверсальную W_0 , и проходящую через w . Эта гиперплоскость **не содержится ни в одном из W_i , $i > 0$, так как она содержит w .**

Шаг 3: Применяв индукцию по размерности V , лемму можно считать доказанной для любого V' с $\dim V' < \dim V$. Применяем ее к V' из шага 2, с гиперплоскостями $W'_i := V' \cap W_i$, и найдем точку на V' , которая не содержится ни в одном из W_i . ■

■

Конечные поля

Сведения о конечных полях: Порядок конечного поля равен p^n , где p — его характеристика. На любом поле k характеристики p задан **гомоморфизм Фробениуса**, $Fr : k \rightarrow k, x \rightarrow x^p$. В любое поле характеристики p естественно вложено конечное поле \mathbb{F}_p из p элементов.

Поле порядка p^n обозначается \mathbb{F}_{p^n} . В устаревшей литературе эти поля называются "полями Галуа".

УТВЕРЖДЕНИЕ: Все элементы \mathbb{F}_{p^n} удовлетворяют уравнению $x^{p^n} - x = 0$.

ДОКАЗАТЕЛЬСТВО: Группа обратимых элементов $\mathbb{F}_{p^n}^*$ имеет порядок $p^n - 1$, и по теореме Лагранжа, все ее элементы удовлетворяют $x^{p^n-1} = 1$. ■

СЛЕДСТВИЕ: \mathbb{F}_{p^n} есть поле разложения многочлена $x^{p^n-1} - 1$ над \mathbb{F}_p . Поэтому все поля из p^n элементов изоморфны.

Конечные поля и примитивные корни

УТВЕРЖДЕНИЕ: Группа $\mathbb{F}_{p^n}^*$ – циклическая.

Доказательство. Шаг 1: Пусть $p^n - 1 = \prod p_i^{\alpha_i}$ – разложение $p^n - 1$ на простые множители. По теореме о классификации абелевых групп, $G := \mathbb{F}_{p^n}^*$ есть произведение абелевых групп G_{p_i} порядка $p_i^{\alpha_i}$. G **циклическая** \Leftrightarrow **все G_i циклические** (китайская теорема об остатках).

Шаг 2: Значит, если G не циклическая, то **порядок каждого элемента в $\mathbb{F}_{p^n}^*$ делит $m := \prod p_i^{\alpha_i - k_i}$** , где какой-то из k_i больше 0.

Шаг 3: В этом случае, **все элементы $\mathbb{F}_{p^n}^*$ являются корнями многочлена $x^m = 1$, что противоречит теореме Безу.** ■

ОПРЕДЕЛЕНИЕ: $\alpha \in \mathbb{F}_{p^n}^*$ называется **примитивным корнем** (или первообразным корнем), если его порядок равен $p^n - 1$.

ЗАМЕЧАНИЕ: Нахождение примитивных корней есть **важная народно-хозяйственная задача**. К примеру, первая современная криптосистема с открытым ключом (Diffie-Hellman key exchange, 1976) использовала вычислительную трудность нахождения "конечного логарифма", то есть числа $b := \log_\varepsilon(a) \bmod p$ такого, что $\varepsilon^b = a$, где ε первообразный корень, а a какой-то остаток.

Группа Галуа для конечного поля

ТЕОРЕМА: Любое расширение конечных полей есть расширение Галуа.

Доказательство. Шаг 1: Поскольку k содержит \mathbb{F}_p , достаточно доказать, что $[K : \mathbb{F}_p]$ расширение Галуа, где $K = \mathbb{F}_{p^n}$.

Шаг 2: Возьмем первообразный корень $\varepsilon \in \mathbb{F}_{p^n}^*$. Тогда $K = \mathbb{F}_p[\varepsilon]$, но ε является корнем многочлена $P(t) = t^{p^n-1} - 1$, который разлагается на множители в K . Значит, $K \otimes_{\mathbb{F}_p} K = K[t]/(P) = \bigoplus K$. ■

ТЕОРЕМА: Группа Галуа $[\mathbb{F}_{p^n} : \mathbb{F}_p]$ **это циклическая группа, порожденная гомоморфизмом Фробениуса Fr .**

Доказательство. Шаг 1: Поскольку порядок группы Галуа равен степени расширения (то есть n), **достаточно убедиться, что порядок Fr равен n .**

Шаг 2: Любой элемент $z \in \mathbb{F}_{p^n}$ удовлетворяет $z^{p^n} = z$, то есть $\text{Fr}^n = 1$. Если $\text{Fr}^k = 1$ для $k < n$, мы получим, что $z^{p^k} = z$ **имеет p^n решений в \mathbb{F}_{p^n} , что невозможно по теореме Безу.** ■