

## **ЛЕКЦИЯ 15**

**ПОЛЯ: ОПРЕДЕЛЕНИЕ И ПРИМЕРЫ**

**ХАРАКТЕРИСТИКА ПОЛЯ**

**РАСШИРЕНИЯ ПОЛЕЙ**

**ПОЛЕ РАЗЛОЖЕНИЯ МНОГОЧЛЕНА**

## ПРИМЕРЫ ПОЛЕЙ

ПРИМЕР 1. Числовые поля  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  являются основными примерами полей для нас.

ПРИМЕР 2. Для каждого простого числа  $p$  мы имеем поле вычетов  $\mathbb{Z}_p$  из  $p$  элементов.

ПРИМЕР 3. Поля из 4, 8, 9, 27 элементов легко строятся как

$$\mathbb{Z}_2[x]/(x^2 + x + 1), \quad \mathbb{Z}_2[x]/(x^3 + x + 1), \quad \mathbb{Z}_3[x]/(x^2 + 1), \\ \mathbb{Z}_3[x]/(x^3 + x^2 + x - 1).$$

ПРИМЕР 4. Для любого натурального числа  $n$ , свободного от квадратов, существует поле  $\mathbb{Q}[\sqrt{n}]$ , которое получается как

$$\mathbb{Q}[x]/(x^2 - n).$$

ПРИМЕР 5. Для любого поля  $\mathbb{F}$  можно рассмотреть поле  $\mathbb{F}(x)$  рациональных дробей над  $\mathbb{F}$ . Оно состоит из дробей

$$\frac{f(x)}{g(x)}, \quad f(x), g(x) \in \mathbb{F}[x], \quad g(x) \neq 0.$$

## ХАРАКТЕРИСТИКА ПОЛЯ

В поле всегда есть единица, не равная нулю. В аддитивной группе поля единица порождает циклическую подгруппу  $\langle 1 \rangle = \{1, 1 + 1, 1 + 1 + 1, \dots\}$ . Если данная группа конечна и содержит  $n$  элементов, то говорят, что характеристика поля равна  $n$ . Если циклическая группа  $\langle 1 \rangle$  бесконечна, то говорят, что характеристика поля - нулевая.

**ЗАМЕЧАНИЕ 1.** Если у поля  $\mathbb{F}$  характеристика равна  $n > 0$ , то  $n$  — простое число.

Действительно, если  $n = mk$ , то в поле  $\mathbb{F}$  сумма  $m$  единиц (не равная нулю), умноженная на сумму  $k$  единиц (не равную нулю) равна нулю. Значит, в поле имеются делители нуля, что невозможно. Таким образом, положительная характеристика всегда является простым числом.

Если единица в поле имеет порядок  $p$  или бесконечный порядок, то такой же порядок имеет и любой ненулевой элемент:

$$a + a + \dots + a + a = a \cdot 1 + a \cdot 1 + \dots + a \cdot 1 = a(1 + 1 + \dots + 1).$$

**ЛЕММА 1.** Если поле  $\mathbb{F}$  имеет характеристику 0, то в него естественно вложено подполе  $\mathbb{Q}$  рациональных чисел. Если поле  $\mathbb{F}$  имеет характеристику  $p$ , то в него естественно вложено подполе  $\mathbb{Z}_p$ .

*Доказательство.* Действительно, пусть характеристика поля  $\mathbb{F}$  равна нулю. Тогда целые числа можно вложить в поле  $\mathbb{F}$  следующим образом: если  $n > 0$ , то  $n = 1 + 1 + \dots + 1$  (сумма  $n$  единиц), отображаем ее в сумму того же числа единиц; ноль отображаем в ноль, а противоположное к  $n$  — в противоположное к его образу.

Такое отображение, очевидно, будет гомоморфизмом. Если бы какой-то ненулевой элемент принадлежал ядру этого гомоморфизма, то сумма конечного числа единиц была бы равно нулю в поле  $\mathbb{F}$ , что невозможно. Значит, это вложение.

Таким образом, можно считать, что целые числа лежат в поле  $\mathbb{F}$ . Рациональные числа тогда лежат в нем как отношения целых к натуральным.

Если у поля  $\mathbb{F}$  характеристика равна  $p$ , то то же самое отображение имеет ядро — все целые числа, кратные  $p$ . Таким образом, образ  $\mathbb{Z}$  — это  $\mathbb{Z}_p$ , которое является полем.  $\square$

**ЛЕММА 2.** *Конечное поле может содержать только  $p^n$  элементов, где  $p$  — простое,  $n$  — натуральное число.*

*Доказательство.* Любое поле является линейным пространством над своим подполем (прямая проверка). В конечном поле характеристики  $p$  (ясно, что конечное поле не может иметь характеристику ноль) содержится подполе  $\mathbb{Z}_p$ . Также ясно, что конечное поле конечномерно. Пусть его размерность над  $\mathbb{Z}_p$  равна  $n$ . Тогда в нем ровно  $p^n$  элементов.  $\square$

**УПРАЖНЕНИЕ 1.** Существует ли бесконечное поле положительной характеристики?

**ЛЕММА 3.** *Если поле  $\mathbb{F}$  характеристики  $p$  конечно, то отображение  $x \mapsto x^p$  является его автоморфизмом.*

*Доказательство.* Действительно, это отображение, очевидно, мультипликативно. Оно аддитивно, так как

$$(x + y)^p = x^p + C_p^1 x^{p-1} y + C_p^2 x^{p-2} y^2 + \dots + C_p^{p-1} x y^{p-1} + y^p,$$

а так как  $C_p^i$  для  $i = 1, \dots, p-1$  делится на  $p$ , то эта сумма равна  $x^p + y^p$  в поле  $\mathbb{F}$ .

Отображение инъективно, так как из  $x^p = y^p$  следует  $x^p - y^p = 0 \implies (x - y)^p = 0 \implies x - y = 0$ .

Благодаря конечности поля оно оказывается биективным.  $\square$

## РАСШИРЕНИЯ ПОЛЕЙ

ОПРЕДЕЛЕНИЕ 1. Поле  $L$  называется *расширением* поля  $K$ , если  $K$  является подполем в  $L$ . Расширение  $L$  поля  $K$  называется *конечным*, если  $\dim_K L < \infty$ . Число  $\dim_K L < \infty$  в этом случае называется *степенью* расширения  $L$ .

Элемент  $x \in L$  называется *алгебраическим* над  $K$ , если он удовлетворяет некоторому нетривиальному алгебраическому уравнению с коэффициентами из  $K$ , и *трансцендентным* в противном случае. Расширение  $L$  поля  $K$  называется *алгебраическим*, если всякий его элемент алгебраичен над  $K$ .

ТЕОРЕМА 1. *Любое конечное расширение поля является алгебраическим.*

*Доказательство.* Действительно, если  $L$  — конечное расширение поля  $K$ , то  $L_K$  — конечномерно. Рассмотрим произвольный элемент  $g \in L$ . Все степени элемента  $g$  не могут быть линейно независимы, поэтому существует некоторая линейная комбинация этих степеней

$$\alpha_0 + \alpha_1 g + \alpha_2 g^2 + \cdots + \alpha_n g^n = 0.$$

Это означает алгебраичность элемента  $g$ . □

УПРАЖНЕНИЕ 2. Является ли алгебраическим расширением  $\mathbb{R}$  над  $\mathbb{Q}$ ?

ЗАМЕЧАНИЕ 2. Напомним, что если  $K$  — поле,  $K[x]$  — кольцо многочленов,  $f(x) \in K[x]$  — произвольный многочлен степени  $n$ , то факторкольцо  $L = K[x]/(f(x))$  является полем тогда и только тогда, когда многочлен  $f(x)$  неприводим над  $K$ . В этом случае  $L$  является конечным расширением поля  $K$  степени  $n$  (*простое расширение*).

ТЕОРЕМА 2. Если  $L$  — конечное расширение поля  $K$ , а  $M$  — конечное расширение поля  $L$ , то  $M$  — конечное расширение поля  $K$ , причем

$$\dim_K M = \dim_K L \cdot \dim_L M.$$

*Доказательство.* Пусть базис  $M$  над  $L$  —  $f_1, \dots, f_k$ , базис  $L$  над  $K$  —  $e_1, \dots, e_m$ . Покажем, что базис  $M$  над  $K$  —  $\{f_i e_j \mid i = 1, \dots, k, j = 1, \dots, m\}$ .

То, что данное множество порождает все  $M$  над  $K$ , очевидно.  
Докажем линейную независимость. Пусть

$$\sum_{i,j} \alpha_{ij} f_i e_j = 0,$$

где  $\alpha_{ij} \in K$ .

Тогда

$$\sum_i (\alpha_{i,1} e_1 + \dots + \alpha_{i,m} e_m) f_i = 0.$$

Так как  $f_1, \dots, f_k$  — базис  $M$  над  $L$ , то все коэффициенты при  $f_1, \dots, f_k$  равны нулю, но каждый коэффициент — это линейная комбинация элементов базиса  $L$  над  $K$ , то все  $\alpha_{i,j}$  равны нулю, что и требовалось.  $\square$

ТЕОРЕМА 3. Если  $L$  — расширение поля  $K$ ,  $M$  — расширение поля  $L$ , а  $M$  — конечное расширение поля  $K$ , то расширения  $L$  над  $K$  и  $M$  над  $L$  — конечны.

*Доказательство.* Пусть одно из расширений  $L$  над  $K$  или  $M$  над  $L$  бесконечно. Это означает, что один из базисов  $f_1, \dots$  поля  $M$  над полем  $L$  или  $e_1, \dots$  поля  $L$  над  $K$  бесконечен.

Точно так же, как в предыдущем доказательстве, мы тогда можем показать, что элементы вида  $f_i e_j$  линейно независимы.

Однако их число бесконечно, а по условию поле  $M$  над  $K$  — конечно.  $\square$

ТЕОРЕМА 4. Если поле  $L$  порождается над  $K$  конечным числом алгебраических элементов  $u_1, \dots, u_n$ , то оно является конечным расширением поля  $K$ .

*Доказательство.* Для начала поймем, что достаточно доказать утверждение при условии, что мы добавляем только одну переменную, так как добавление  $n$  переменных эквивалентно последовательному добавлению по одной переменной к все более расширяющимся полям.

Если мы рассматриваем поле  $K(u)$ , и оно является бесконечным расширением поля  $K$ , то существует сколько угодно линейно независимых над  $K$  дробей вида  $f_i(u)/g_i(u)$ . Линейная независимость дробей

$$f_1(u)/g_1(u), \dots, f_n(u)/g_n(u)$$

равносильна линейной независимости многочленов

$$h(u)f_1(u)/g_1(u), \dots, h(u)f_n(u)/g_n(u),$$

где

$$h(u) = \text{НОК}(g_1(u), \dots, g_n(u)),$$

что для любого  $n$  не может выполняться. Противоречие.  $\square$

ЛЕММА 4. Пусть  $L$  — какое-либо расширение поля  $K$ . Совокупность  $\bar{K}$  всех элементов поля  $L$ , алгебраических над  $K$ , является подполем, алгебраически замкнутым в  $L$  (в том смысле, что любой элемент поля  $L$ , алгебраический над  $\bar{K}$ , принадлежит  $\bar{K}$ ).

*Доказательство.* Нам нужно доказать только, что сумма, разность, произведение и частное двух алгебраических над  $K$  — алгебраические над  $K$ . Это практически прямое следствие предыдущей леммы, так как все эти функции от пар алгебраических элементов входят в конечное расширение, которое является алгебраическим.  $\square$

ТЕОРЕМА 5. Поле  $\overline{Q}$  алгебраических чисел (всех комплексных чисел, являющихся корнями многочленов с рациональными коэффициентами) алгебраически замкнуто.

*Доказательство.* Рассмотрим какой-нибудь многочлен с алгебраическими коэффициентами. Подполе поля  $\overline{Q}$ , содержащее все коэффициенты этого многочлена, является конечным расширением поля  $Q$ . Так как два последовательных конечных расширения дают конечное расширение, то корень многочлена — алгебраический над  $Q$ .  $\square$

## ПОЛЕ РАЗЛОЖЕНИЯ МНОГОЧЛЕНА

ОПРЕДЕЛЕНИЕ 2. Расширение  $L$  поля  $K$  называется *полем разложения* многочлена  $f \in K[x]$  (не обязательно неприводимого), если  $f$  разлагается в  $L[x]$  на линейные множители и поле  $L$  порождается над  $K$  его корнями.

Гомоморфизмы (в частности, изоморфизмы) расширений поля  $K$ , тождественные на  $K$ , называются *гомоморфизмами (изоморфизмами) над  $K$* .

ТЕОРЕМА 6. Поле разложения любого многочлена  $f \in K[x]$  существует.

*Доказательство.* Разложим многочлен  $f(x)$  на неприводимые множители над полем  $K$ . Рассмотрим один из неприводимых множителей —  $h(x)$ .

Рассмотрим поле  $K_1 = K[x]/(h(x))$ . Как мы знаем, это поле является расширением поля  $K$ , в котором у многочлена  $h(x)$  появляется (хотя бы один) корень. Таким образом, многочлен  $f(x)$  над полем  $K_1$  разложится на большее число неприводимых сомножителей.

Последовательными расширениями мы можем добиться того, чтобы все сомножители стали линейными.  $\square$



**ПРЕДЛОЖЕНИЕ 1.** Пусть  $P(\alpha)$  — расширение поля  $P$ , полученное присоединением корня  $\alpha$  неприводимого многочлена  $h \in P[x]$ , и  $\varphi$  — гомоморфизм поля  $P$  в некоторое поле  $\mathbb{F}$ . Гомоморфизм  $\varphi$  продолжается до гомоморфизма  $\psi : P(\alpha) \rightarrow \mathbb{F}$  ровно столькоими способами, сколько различных корней имеет в  $\mathbb{F}$  многочлен  $\varphi(h)$ , полученный из  $h$  применением к его коэффициентам гомоморфизма  $\varphi$ .

*Доказательство.* Искомое продолжение  $\psi$ , если оно существует, задается формулой

$$\begin{aligned} \psi(a_0 + a_1\alpha + \dots + a_m\alpha^m) &= \\ &= \varphi(a_0) + \varphi(a_1)\beta + \dots + \varphi(a_m)\beta^m, \quad (a_0, a_1, \dots, a_m \in P), \end{aligned}$$

где  $\beta = \psi(\alpha)$  — некоторый элемент поля  $\mathbb{F}$ .

Применяя эту формулу к равенству  $h(\alpha) = 0$ , получаем, что  $\varphi(h)(\beta) = 0$ .

Обратно, если  $\beta \in \mathbb{F}$  — корень многочлена  $\varphi(h)$ , то данная формула корректно определяет гомоморфизм  $\psi : P(\alpha) \rightarrow \mathbb{F}$ .  $\square$

**ТЕОРЕМА 7.** Поле разложения любого многочлена  $f \in K[x]$  единственно с точностью до изоморфизма над  $K$ .

*Доказательство.* Пусть  $L$  — поле разложения многочлена  $f(x)$  над  $K$ , построенное с помощью простых расширений

$$K = K_0 \subset K_1 \subset \dots \subset K_s = L.$$

Пусть при этом поле  $K_i$  получается из поля  $K_{i-1}$  присоединением неприводимого множителя  $f_i$  многочлена  $f$  над  $K_{i-1}$ .

Пусть теперь  $M$  — другое поле разложения того же многочлена.

Построим последовательность гомоморфизмов

$$\varphi_i : K_i \rightarrow M \quad (i = 0, 1, \dots, s)$$

так, чтобы

$$\varphi_0 = \text{id}, \quad \varphi_i|_{K_{i-1}} = \varphi_{i-1}.$$

По предыдущему предложению  $i$ -й шаг этого построения будет возможен, если многочлен  $\varphi_{i-1}(f_i)$  имеет корень в  $M$ . Так как  $f_i$  делит  $f$  в кольце  $K_{i-1}[x]$ , то многочлен  $\varphi_{i-1}(f_i)$  делит  $f$  в  $M[x]$ .

Но многочлен  $f$  разлагается в  $M[x]$  на линейные множители и, следовательно, любой его делитель положительной степени имеет корень в  $M$ . Таким образом, искомые гомоморфизмы существуют.

Последний из них

$$\varphi_s = \varphi : L \rightarrow M$$

является изоморфизмом, так как, по определению поля разложения, поле  $M$  является минимальным расширением поля  $K$ , над которым многочлен разлагается на линейные множители.  $\square$

**УПРАЖНЕНИЕ 3.** Какая степень может быть у поля разложения кубического многочлена над полем  $K$ ,  $\text{char } K \neq 2$ ?