

**ЛЕКЦИЯ 16**

**КОНЕЧНЫЕ ПОЛЯ**

**АЛГЕБРЫ И АЛГЕБРЫ С ДЕЛЕНИЕМ**

**АЛГЕБРА КВАТЕРНИОНОВ**

**ТЕОРЕМА ФРОБЕНИУСА**

## КОНЕЧНЫЕ ПОЛЯ

ЛЕММА 1. Если поле  $\mathbb{F}$  состоит из  $q$  элементов, то каждый элемент поля  $\mathbb{F}$  является корнем многочлена  $x^q - x$ .

*Доказательство.* Очевидно, что ноль является корнем рассматриваемого многочлена. Рассмотрим ненулевой элемент  $z \in \mathbb{F}$ . Так как мультипликативная группа поля  $\mathbb{F}$  состоит из  $q - 1$  элемента, то по теореме Лагранжа  $z^{q-1} = 1$ . Значит,  $z$  является корнем уравнения  $x^q - x = 0$ .  $\square$

ЛЕММА 2. Для любого поля  $F$  и любого его автоморфизма  $\varphi$  неподвижные точки этого автоморфизма образуют подполе в  $F$ .

*Доказательство.* Прямая проверка.  $\square$

ТЕОРЕМА 1. Для любого простого  $p$  и натурального  $n$  существует поле из  $p^n$  элементов, и все такие поля изоморфны (обозначение:  $\mathbb{F}_{p^n}$ ).

*Доказательство.* Рассмотрим поле  $L$  разложения многочлена  $x^{p^n} - x$  над полем  $\mathbb{Z}_p$ .

У данного многочлена нет кратных корней (так как его производная равна  $-1$  и взаимно проста с самим многочленом), поэтому все корни многочлена  $x^{p^n} - x$ , лежащие в  $L$ , различны.

Количество таких корней равно  $q = p^n$ .

Докажем, что множество этих корней образует поле.

Действительно, если  $a^q = a$  и  $b^q = b$ , то  $(ab)^q = ab$ ,  $(a/b)^q = a/b$ , поэтому данное множество замкнуто относительно умножения и деления на ненулевые элементы.

Если  $a^q = a$  и  $b^q = b$ , то  $(a + b)^q = (a + b)^{p^n} = a^q + b^q = a + b$ , то есть множество корней замкнуто относительно сложения и (аналогично) вычитания.

Таким образом, мы нашли искомое поле из  $p^n$  элементов.

Теперь докажем, что все поля из  $p^n$  элементов изоморфны.

Как мы показали выше, поле из  $p^n$  элементов обязательно является полем разложения многочлена  $x^{p^n} - x$ . Так как мы доказали, что поле разложения многочлена единственно с точностью до изоморфизма, единственность доказана полностью. □

**ТЕОРЕМА 2.** *Поле  $\mathbb{F}_{p^n}$  содержит  $\mathbb{F}_{p^m}$  в качестве подполя тогда и только тогда, когда  $m|n$ .*

*Доказательство.* Если поле  $L = \mathbb{F}_{p^n}$  содержит подполе  $K = \mathbb{F}_{p^m}$  то  $L$  является линейным пространством над  $K$ , откуда следует, что  $p^n$  есть степень числа  $p^m$ . Отсюда следует, что  $m|n$ .

Пусть, наоборот,  $m$  делит  $n$ .

Тогда

$$p^n - 1 = (p^m)^k - 1 = (p^m - 1)t,$$

откуда

$$x^{p^n} - x = x(x^{p^n-1} - 1) = x(x^{p^m t-1} - 1) = (x^{p^m} - x)T.$$

Таким образом, многочлен  $x^{p^m} - x$  делит многочлен  $x^{p^n} - x$ .

Если рассмотреть все элементы поля  $\mathbb{F}_{p^n}$ , которые являются корнями многочлена  $x^{p^m} - x$  (их ровно  $p^m$ ), то они образуют подполе. □

**ТЕОРЕМА 3.** *Мультипликативная группа конечного поля является циклической.*

*Доказательство.* Предположим, что у конечного поля  $\mathbb{F}$  из  $q = p^n$  элементов мультипликативная группа не является циклической.

$\mathbb{F}^*$  — это абелева группа. Если она не является циклической, то существует число  $s < q - 1$  такое, что  $z^s = 1$  для любого  $z \in \mathbb{F}^*$ .

Это означает, что все элементы поля  $\mathbb{F}$  являются корнями многочлена

$$x^{s+1} - x.$$

Таким образом, у многочлена степени  $< q$  есть  $q$  корней, что невозможно.  $\square$

## АЛГЕБРЫ И АЛГЕБРЫ С ДЕЛЕНИЕМ

**ОПРЕДЕЛЕНИЕ 1.** *Алгеброй* над полем  $K$  называется множество  $A$  с операциями сложения, умножения и умножения на элементв поля  $K$ , обладающими следующими свойствами:

- 1) относительно сложения и умножения на элементы поля  $A$  является векторным пространством;
- 2) относительно сложения и умножения  $A$  есть кольцо;
- 3)  $(\lambda a)b = a(\lambda b) = \lambda(ab)$  для любых  $\lambda \in K$ ,  $a, b \in A$ .

**ПРИМЕР 1.** Всякое расширение  $L$  поля  $K$  является алгеброй над  $K$ .

Множество функций  $\mathbf{F}(X, K)$  функций на множестве  $X$  со значениями в поле  $K$  является алгеброй над  $K$  относительно обычных операций сложения и умножения функций и умножения функции на число. Эта алгебра коммутативна, ассоциативна и обладает единицей (тождественно равная единице функция).

Кольцо квадратных матриц над полем является алгеброй над этим полем.

ОПРЕДЕЛЕНИЕ 2. Ассоциативное кольцо с единицей, в котором каждый ненулевой элемент имеет обратный, называется телом. Алгебра, являющаяся телом, называется *алгеброй с делением*.

Всякое тело  $D$  можно рассматривать как алгебру с делением над своим центром

$$\mathbf{Z}(D) := \{z \in D \mid \forall a \in D \quad za = az\},$$

который, очевидно, является полем.

Если  $D$  — алгебра с делением над полем  $K$ ,  $1$  — ее единица, то элементы вида  $\lambda \cdot 1$ ,  $\lambda \in K$ , образуют подкольцо, изоморфное  $K$  и содержащееся в центре  $\mathbf{Z}(D)$  алгебры  $D$ .

Обычно эти элементы отождествляют с соответствующими элементами поля  $K$ . При таком соглашении  $K \subseteq \mathbf{Z}(D)$ . Алгебра называется *центральной*, если она совпадает со своим центром.

## АЛГЕБРА КВАТЕРНИОНОВ

Алгебра кватернионов  $\mathbb{H}$  была открыта Гамильтоном в 1843 г.

Она порождается над  $\mathbb{R}$  элементами  $i$  и  $j$ , удовлетворяющими соотношениям

$$i^2 = -1, \quad j^2 = -1, \quad ij = -ji.$$

Легко видеть, что базис алгебры  $\mathbb{H}$  над  $\mathbb{R}$  составляют элементы

$$1, i, j, k = ij,$$

причем элементы  $i, j, k$  попарно антикоммутируют, их квадраты равны  $-1$ .

Покажем, что алгебра кватернионов является алгеброй с делением.

Для этого для любого кватерниона

$$q = a + bi + cj + dk, \quad a, b, c, d \in \mathbb{R}$$

определим *сопряженный* кватернион по формуле

$$\bar{q} = a - bi - cj - dk.$$

Легко видеть, что отображение  $q \mapsto \bar{q}$ , которое называется стандартной *инволюцией*, является антиавтоморфизмом алгебры  $\mathbb{H}$ :

$$\overline{q_1 q_2} = \bar{q}_1 \cdot \bar{q}_2$$

(по линейности достаточно проверить это равенство на базисных элементах).

Число

$$N(q) = q\bar{q} = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}$$

называется *нормой* кватерниона  $q$ .

Ясно, что  $q$  обратим тогда и только тогда, когда  $N(q) \neq 0$  (и в этом случае  $q^{-1} = \bar{q}/N(q)$ ).

Однако, как мы видим, кватернион обратим всегда, когда он ненулевой.

Значит, алгебра кватернионов является алгеброй с делением.

## ТЕОРЕМА ФРОБЕНИУСА

**ПРЕДЛОЖЕНИЕ 1.** В ассоциативной алгебре  $A$  с единицей размерности  $n$  над полем  $K$  каждый элемент является корнем многочлена  $\mu_a \in K[x]$  степени  $\leq n$ .

Элемент  $a \in A$  обратим тогда и только тогда, когда  $\mu_a(0) \neq 0$ .

Если в  $A$  нет делителей нуля, то  $A$  — алгебра с делением. Если при этом поле  $K$  алгебраически замкнуто, то  $n = 1$  и  $A = K$ .

*Доказательство.* Так как алгебра  $A$  конечномерна, то элементы

$$1, a, a^2, \dots$$

не могут быть все линейно независимыми над  $K$ .

Значит, найдется унитарный многочлен

$$\mu_a(x) = x^m + \alpha_1 x^{m-1} + \dots + \alpha_m$$

наименьшей степени  $m \geq n$  с коэффициентами  $\alpha_i \in K$  такой, что  $\mu_a(a) = 0$ .

Если  $\alpha_m \neq 0$ , то соотношение  $\mu_a(a) = 0$ , переписанное в виде

$$(-\alpha_m^{-1}(a^{m-1} + \alpha_1 a^{m-1} + \dots + \alpha_{m-1})) a = 1,$$

показывает, что  $a$  — обратимый элемент.

Обратно, предположим, что  $a \in A$  не является делителем нуля, но  $\alpha_m = 0$ . Тогда

$$\begin{aligned} (a^{m-1} + \alpha_1 a^{m-2} + \dots + \alpha_{m-1})a = 0 &\implies \\ \implies a^{m-1} + \alpha_1 a^{m-2} + \dots + \alpha_{m-1} = 0, \end{aligned}$$

что противоречит минимальности  $\mu_a(x)$ . Значит,  $\alpha_m \neq 0$ .

В частности, все элементы  $A$ , не являющиеся делителями нуля, обратимы.

Если поле  $K$  алгебраически замкнуто, то

$$\mu_a(x) = (x - c_1) \dots (x - c_m), \quad c_i \in K,$$

откуда

$$(a - c_1)b = 0, \quad b = (a - c_2) \dots (a - c_m) \neq 0.$$

Отсутствие делителей нуля оставляет только одну возможность:  $m = 1$ ,  $a - c_1 = 0$ , т.е.  $a = c_1 \in K$ . Так как это верно для любого элемента  $a \in A$ , то  $A = K$ .  $\square$

ТЕОРЕМА 4 (ТЕОРЕМА ФРОБЕНИУСА). *Над полем  $\mathbb{R}$  существует только три конечномерные ассоциативные алгебры с делением:  $\mathbb{R}$ ,  $\mathbb{C}$  и  $\mathbb{H}$ .*

Прежде, чем доказывать теорему, исследуем аддитивную структуру алгебры с делением  $A$ .

Как мы видели, у каждого элемента из  $A$  есть некоторый минимальный аннулирующий многочлен  $\mu_a(t)$ , из рассуждений прошлого предложения видно, что он обязательно неприводим.

Так как многочлены мы рассматриваем над полем  $\mathbb{R}$ , то неприводимые многочлены имеют вид

$$\mu_a(t) = t - \alpha,$$

либо

$$\mu_a(t) = t^2 - 2\alpha t + \beta,$$

где

$$\alpha^2 < \beta.$$

В первом случае  $a \in \mathbb{R}$ . Если это не так, то положим  $b = a - \alpha$ , получим тогда

$$\mu_b(t) = t^2 + (\beta - \alpha^2).$$

Значит, каждый элемент алгебры  $A$  имеет вид  $\alpha + y$ , где  $\alpha \in \mathbb{R}$ ,  $y = 0$  или  $y^2 = \gamma < 0$ ,  $\gamma \in \mathbb{R}$ .

Для дальнейшего доказательства нам понадобится лемма.

ЛЕММА 3. *Подмножество*

$$A' = \{u \in A \mid u^2 \in \mathbb{R}, u^2 \leq 0\}$$

*является векторным подпространством в  $A$ .*



*Доказательство.* Ясно, что если  $u \in A'$ ,  $\alpha \in \mathbb{R}$ , то  $\alpha u \in A'$ , поэтому достаточно убедиться, что из  $u, v \in A'$  следует  $u + v \in A'$  для двух произвольных непропорциональных векторов  $u, v$ .

Сначала проверим, что линейная зависимость

$$u = \alpha v + \beta, \quad \alpha, \beta \in \mathbb{R},$$

невозможна.

В самом деле, по условию  $uv \neq 0$ , и

$$u^2 = \gamma < 0, \quad v^2 = \delta < 0.$$

Поэтому

$$u = \alpha v + \beta \implies \gamma = u^2 = (\alpha v + \beta)^2 = \alpha^2 \delta + 2\alpha\beta v + \beta^2.$$

Так как  $v \notin \mathbb{R}$ , то  $\alpha\beta = 0$ , т.е. или  $\alpha = 0$ , или  $\beta = 0$ .

Если  $\alpha = 0$ , то  $u \in \mathbb{R}$ , а если  $\beta = 0$ , то  $u$  пропорционально  $v$ . Обе возможности были исключены.

Итак, линейная независимость  $u, v \in A'$  приводит к линейной независимости  $1, u, v$ . Оба элемента  $u + v, u - v$  — корни квадратных уравнений, т.е.

$$(u + v)^2 = p(u + v) + q, \quad (u - v)^2 = r(u - v) + s, \quad p, q, r, s \in \mathbb{R}.$$

Используя соотношения

$$(u \pm v)^2 = u^2 \pm (uv + vu) + v^2, \quad u^2 = \gamma, v^2 = \delta,$$

будем иметь

$$\begin{aligned} \gamma + \delta + (uv + vu) &= p(u + v) + q, \\ \gamma + \delta - (uv + vu) &= r(u - v) + s. \end{aligned}$$

Складывая, находим

$$(p + r)u + (p - r)v + (q + s - 2\gamma - 2\delta) = 0.$$

Но, как мы видели,  $u, v, 1$  линейно независимы, поэтому  $p = r = 0$ .

Значит,  $(u + v)^2 = q \in \mathbb{R}$ , а так как  $u + v \notin \mathbb{R}$ , то  $q < 0$ . Это и значит, что  $u + v \in A'$ , т.е.  $A'$  — подпространство в  $A$ .  $\square$