ЛЕКЦИЯ 19

ЕДИНСТВЕННОСТЬ ПОЛЯ ИЗ p^n ЭЛЕМЕНТОВ

ТЕОРЕМА ФРОБЕНИУСА

ЕДИНСТВЕННОСТЬ ПОЛЯ ИЗ p^n ЭЛЕМЕНТОВ

Теорема 1. *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

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

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

$$\varphi_i : K_i \to M \qquad (i = 0, 1, \ldots, s)$$

так, чтобы

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

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

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

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

Упражнение 1. Какая степень может быть у поля разложения кубического многочлена над полем K, $\operatorname{char} K \neq 2$?

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 $x^q - x = 0$. □

Лемма 2. *Для любого поля* F *и любого его автоморфизма* φ *неподвижные точки этого автоморфизма образуют подполе в* F.

Доказательство. Прямая проверка. □

Теорема 2. *Все поля из* p^n *элементов изоморфны (обозначение:* $\mathbb{F}_{p^n}$*).*

Доказательство. 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 3. *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

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

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 4. *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. □

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

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

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

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

определим *сопряженный* кватернион по формуле

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

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

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

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

Число

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

называется *нормой* кватерниона q.

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

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

Значит, алгебра кватернионов является алгеброй с делением.

ТЕОРЕМА ФРОБЕНИУСА

Докажем довольно легкое предложение, которое поможет нам в дальнейшем:

ПРЕДЛОЖЕНИЕ 1. *В ассоциативной алгебре A с единицей размерности n над полем K каждый элемент a является корнем многочлена $\mu_a \in K[x]$ степени $\leqslant n$. Пусть с дальнейшем μ_a — это аннулирующий для a многочлен наименьшей степени из $K[x]$.*

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. Рассмотрим элементы $1, a, a^2, \ldots, a^n$. Так как перед нами $n+1$ элемент n-мерного векторного пространства над K, то существует нетривиальная линейная комбинация этих элементов, равная нулю:

$$\alpha_0 \cdot 1 + \alpha_1 \cdot a + \cdots + \alpha_n \cdot a^n = 0, \quad \alpha_0, \ldots, \alpha_n \in K.$$

Таким образом, искомым многочленом является $\alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$.

Теперь будем считать, что аннулирующий многочлен μ_a имеет наименьшую возможную степень из всех многочленов, аннулирующих a.

Если $\mu_a(0) \neq 0$, то

$$\alpha_1 a + \cdots + \alpha_n a^n = -\alpha_0,$$

откуда

$$-\alpha_0^{-1}(\alpha_1 + \cdots + \alpha_n a^{n-1}) \cdot a = 1.$$

Таким образом, мы нашли в явном виде обратный элемент.

Если же $\mu_a(0) = 0$, то

$$a \cdot (\alpha_1 + \cdots + \alpha_n a^{n-1}) = 0,$$

то есть a — делитель нуля и не может быть обратим.

Получается, что если в A нет делителей нуля, то все аннулирующие многочлены ненулевых элементов имеют ненулевой свободный член, то есть соответствующие элементы все обратимы. Также понятно, что в алгебре без делитель нуля любой аннулирующий многочлен μ_a неприводим (иначе его можно было бы разложить на множители и мы бы получили делители нуля).

Значит, если поле алгебраически замкнуто, то есть все неприводимые многочлены линейны, то все элементы алгебры лежат в поле, что и требовалось. $\square$

А теперь сформулируем теорему Фробениуса:

Теорема 5 (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 многчлены 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*

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

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

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

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

$$\gamma + \delta + (uv + vu) = p(u + v) + q,$$
$$\gamma + \delta - (uv + vu) = r(u - v) + s.$$

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. $\square$

Теперь мы можем перейти к доказательству самой теоремы.

Для $u \in A'$ запишем

$$u^2 = -q(u),$$

где $q(u) \in \mathbb{R}_+$.

Кроме того, $q(u) = 0 \Leftrightarrow u = 0$. Очевидно, что

$$q(\alpha u) = \alpha^2 q(u)$$

и

$$f(u, v) := q(u + v) - q(u) - q(v) = -(uv + vu)$$

— симметричная билинейная форма на A, отвечающая положительно определенной квадратичной форме q.

Если $A = \mathbb{R}$, то рассуждения заканчиваются.

Пусть $A \neq \mathbb{R}$. Тогда $A' \neq 0$ и мы можем выбрать вектор $\mathbf{i} \in A$, для которого $q(\mathbf{i}) = 1$, т.е. $\mathbf{i}^2 = -1$.

С точностью до изоморфизма получаем равенство

$$\mathbb{R}[\mathbf{i}] = \mathbb{C} = \mathbb{R} + \mathbb{R}\mathbf{i}.$$

Если $A = \mathbb{C}$, то наши рассуждения заканчиваются.

Теперь предположим, что A — шире, чем комплексные числа (как мы видели, мы можем считать, что $\mathbb{C} \subset A$).

В этом случае A' — шире, чем $\mathbb{R}\mathbf{i}$, поэтому можно выбрать элемент $\mathbf{j} \perp \mathbb{R}\mathbf{i}$, $q(\mathbf{j}) = 1$.

В этом случае $\mathbf{j}^2 = -1$ и $\mathbf{ij} + \mathbf{ji} = -f(\mathbf{i}, \mathbf{j}) = 0$, т.е. $\mathbf{ij} = -\mathbf{ji}$. Полагая $\mathbf{k} = \mathbf{ij}$, получим $\mathbf{k}^2 = -1$, $\mathbf{ik} + \mathbf{ki} = 0 = \mathbf{jk} + \mathbf{kj}$.

Следовательно, $\mathbf{k} \in A'$ и $\mathbf{k} \perp \mathbf{i}, \mathbf{j}$. Значит, $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ линейно независимы и

$$\mathbb{R} + \mathbb{R}\mathbf{i} + \mathbb{R}\mathbf{j} + \mathbb{R}\mathbf{k} = \mathbb{H}$$

— алгебра кватернионов.

Если A шире, чем алгебра кватернионов, то существует $\mathbf{l} \in A'$ такое, что $q(\mathbf{l}) = 1$ и $\mathbf{l} \perp \mathbf{i}, \mathbf{j}, \mathbf{k}$. Другими словами,

$$\mathbf{li} = -\mathbf{il}, \quad \mathbf{lj} = -\mathbf{jl}, \quad \mathbf{lk} = -\mathbf{kl}.$$

Однако в силу ассоциативности умножения в A первые два соотношения дают

$$\mathbf{lk} = \mathbf{l}(\mathbf{ij}) = (\mathbf{li})\mathbf{j} = -(\mathbf{il})\mathbf{j} = -\mathbf{i}(\mathbf{lj}) = \mathbf{i}(\mathbf{jl}) = (\mathbf{ij})\mathbf{l} = \mathbf{kl}.$$

Получается противоречие. Значит,

$$A = \mathbb{H}.$$