ЛЕКЦИЯ 18

ЕДИНСТВЕННОСТЬ ПОЛЯ РАЗЛОЖЕНИЯ МНОГОЧЛЕНА

КОНЕЧНЫЕ ПОЛЯ

АЛГЕБРЫ С ДЕЛЕНИЕМ, АЛГЕБРА КВАТЕРНИОНОВ

ЕДИНСТВЕННОСТЬ ПОЛЯ РАЗЛОЖЕНИЯ МНОГОЧЛЕНА

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

Доказательство. Искомое продолжение ψ, если оно существует, задается формулой

$$\psi(a_0 + a_1\alpha + \cdots + a_m\alpha^m) = \\ = \varphi(a_0)+\varphi(a_1)\beta+\cdots+\varphi(a_m)\beta^m, \quad (a_0, a_1, \ldots, a_m \in P),$$

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 $\psi : P(\alpha) \to \mathbb{F}$. □

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. □

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

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 $x^q - x = 0$. □

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

Доказательство. Прямая проверка. □

Теорема 2. *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 ровно $q = p^n$.

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. $\square$

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.

Предложение 2. *В ассоциативной алгебре A с единицей размерности n над полем K каждый элемент является корнем многочлена $\mu_a \in K[x]$ степени $\leqslant n$.*

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

$$1, a, a^2, \ldots$$

не могут быть все линейно независимыми над K.

Значит, найдется унитарный многочлен

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

наименьшей степени $m \leqslant n$ 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

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

показывает, что a — обратимый элемент.

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

$$(a^{m-1} + \alpha_1 a^{m-2} + \cdots + \alpha_{m-1})a = 0 \Longrightarrow$$
$$\Longrightarrow a^{m-1} + \alpha_1 a^{m-2} + \cdots + \alpha_{m-1} = 0,$$

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 $A = K$. $\square$