Лекция 23, 06.03.24

Теорема: (б/д - без док-ва)

Пусть $\mathbb{F}$ - произвольное поле и $f(x) \in \mathbb{F}[x]$ - многочлен из кольца многочленов над $\mathbb{F}$.

Тогда всегда $\exists$ расширение $\mathbb{F}_1$ этого поля $(\mathbb{F} \subseteq \mathbb{F}_1)$, в котором многочлен $f(x)$ имеет корень.

Пример: $\forall$ неприводимый над $\mathbb{R}$ многочлен из $\mathbb{R}[x]$ вида ax^2+bx+c $(D<0)$ имеет пару корней в $\mathbb{C}$ ($\mathbb{C}$-расширение для $\mathbb{R}$).

Факторкольцо кольца мн-нов

Пример: Многочлен $h(x) = x^2+1$ не имеет вещ. корней $\Rightarrow$ неприводим над $\mathbb{R}$

Тогда $I = \langle x^2+1 \rangle = \{(x^2+1)g(x) \mid g(x) \in \mathbb{R}[x]\}$ - главный идеал $\mathbb{R}[x]$

Рассмотрим факторкольцо $\mathbb{R}[x]/\langle x^2+1 \rangle$, покажем что

$\mathbb{R}[x]/\langle x^2+1 \rangle \cong \mathbb{C}$

□ Рассмотрим $\forall f(x) \in \mathbb{R}[x]$, и разделим его с остатком на $h(x) = x^2+1$: $f(x) = q(x)(x^2+1) + r(x)$, $\deg r(x) < \deg(x^2+1) = 2$

$\Rightarrow r(x) = a + bx$ - произвольный многочлен 1й степени $(a, b \in \mathbb{R})$

$\Rightarrow$ классы вычетов : $\overline{f(x)} = \underbrace{\overline{q(x)(x^2+1)}}_{\in I \Rightarrow \bar{0}} + \overline{r(x)}$ по идеалу $I = \langle x^2+1 \rangle$

характеризуется своими остатками от деления на x^2+1.

Сопоставим остатку $\overline{a+bx}$ компл. число $a+bi$.

Тогда $\varphi: \overline{a+bx} \mapsto a+bi$ - изоморфизм колец, т.к.

- это биекция
- это гомоморфизм колец

1) сложение - очевидно

2) умножение:

$$(\overline{a_1 + b_1 x})(\overline{a_1 + b_2 x}) = \overline{a_1 a_2} + \overbrace{\overline{b_1 b_2 x^2}}^{-b_1 b_2, \text{ т.к. } x^2+1 = 0 \bmod \langle x^2+1\rangle \Leftrightarrow x^2 = -1 \bmod \langle x^2+1\rangle} + x(\overline{a_1 b_2 + a_2 b_1}) =$$

$$= a_1 a_2 - b_1 b_2 + x(a_1 b_2 + a_2 b_1)$$

$$\xmapsto{\varphi} a_1 a_2 - b_1 b_2 + i(a_1 b_2 + a_2 b_1) = (a_1 + b_1 i)(a_2 + b_2 i) \Rightarrow \text{гом-зм колец} \blacksquare$$

Теорема: Пусть $\mathbb{F}[x]$ - кольцо многочленов с коэф-ми из поля $\mathbb{F}$, и $f(x) \in \mathbb{F}[x]$ и $\langle f(x) \rangle$ - идеал, порождённый $f(x)$.

Тогда факторкольцо $F[x]/\langle f(x) \rangle$ явл. полем $\Leftrightarrow$ мн-н $f(x)$ неприводим над $\mathbb{F}$.

□ „$\Leftarrow$" Докажем, что $\exists$ обратный по умножению, когда $f(x)$ непривод.

(т.е. $\forall$ см. класса $\overline{a(x)} \neq 0$ $\exists\, \overline{a(x)}^{-1}$).

Пусть $a(x)$ – представитель см. класса $\overline{a(x)}$, и $\deg a(x) < \deg f(x)$ (т.к. $a(x)$ – это один из остатков от деления на $f(x)$).

Т.к $f(x)$ неприводим, то $НОД(a(x), f(x)) = 1 \Rightarrow$

$\Rightarrow$ по следствию из алгоритма Евклида $\exists\, u(x), v(x) \in \mathbb{F}[x]$:

$a(x)u(x) + f(x)v(x) = 1$.

$\Rightarrow \overline{a(x)\cdot u(x)} + \overline{f(x)v(x)} = \overline{1} \mod \langle f(x)\rangle \Rightarrow \overline{a(x)}\cdot\overline{u(x)} = \overline{1} \mod \langle f(x)\rangle$

$\Rightarrow u(x)$ и есть обратный для $\overline{a(x)}$.

$\Rightarrow$ "и" $\Rightarrow$ "и": Если $f(x)$ приводим, т.е. $f(x) = f_1(x)\cdot f_2(x)$, где $\deg f_1 < \deg f$, $\deg f_2 < \deg f$, то тогда $\overline{f_1(x)}$, $\overline{f_2(x)}$ – смежные классы и $\overline{f_1(x)}\cdot\overline{f_2(x)} = \overline{f(x)} = \overline{0}$

$\Rightarrow$ в $F[x]/\langle f(x)\rangle$ есть делители нуля $\Rightarrow$ это не поле ■

Теорема: (б/д)

1) Число эл-тов в конечном поле F_q ($|F_q| = q$) всегда имеет вид $q = p^n$, где p – простое число, $n \in \mathbb{N}$

2) Для $\forall p$ – простого и $\forall n \in \mathbb{N}$ $\exists!$ (с точностью до изоморфизма) поле из p^n элементов.

Теорема: (б/д) $\forall$ конечное поле F_q ($|F_q| = q$), где $q = p^n$, p – простое, $n \in \mathbb{N}$, может быть реализовано в виде $\mathbb{Z}_p[x]/\langle h(x)\rangle$, где $h(x)$ – неприводимый мн-н n-й степени из $\mathbb{Z}_p[x]$.

(Он всегда $\exists$ ет $\forall n \in \mathbb{N}$ и $\forall p$ – простого)

Идея док-ва: $\mathbb{Z}_p[x]/\langle h(x)\rangle$ – поле по предыдущей теореме.

Элементов в этом поле столько, сколько $\exists$ разл. остатков от деления на $h(x)$.

т.е. многочленов вида $a_{n-1}x^{n-1} + \dots + a_1 x^1 + a_0$, $a_i = \overline{0, p-1}$, $i = \overline{0, n-1}$

$\Rightarrow$ их p^n элементов.

Пример: Поле из 4х элементов

Замечание: $\mathbb{Z}_4$ – не явл. полем ($\bar{2}\cdot\bar{2} = \bar{0}$)

$F_4 = F_{2^2}$, $p=2$, $n=2$ $\Rightarrow$ рассм. $\mathbb{Z}_2[x]$

Заметим, что $h(x) = x^2 + x + 1$ неприводим над $\mathbb{Z}_2$

($h(0) = h(1) = 1$ $\Rightarrow$ нет корней)

$\Rightarrow$ $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ – и есть поле из 4х эл-тов.

Все элементы: $\bar{0}$, $\bar{1}$, $\bar{x}$, $\overline{x+1}$ (т.е. все мн-ны вида $ax+b, a,b \in \mathbb{Z}_2$)

+	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

·	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	$\bar{x}$

$\cong V_4$ (группа Клейна)

$\bar{x}\cdot\bar{x} \mod(x^2+x+1) = -x-1 = \overline{x+1} \mod(x^2+x+1)$

$\bar{x}(\overline{x+1}) = \overline{x^2+x} = \bar{1}$

$(\overline{x+1})(\overline{x+1}) = \overline{x^2+2x+1} = \overline{x^2+1} = \bar{x}$ ($2x = 0$)

Вопрос: Бывают ли беск. поля положительной характеристики?

Да, бывают

$$Z_p(x) = \left\{ \frac{h_1(x)}{h_2(x)} \mid h_1, h_2 \in Z_p[x],\ h_2 \neq 0 \right\}$$ - поле рац. дробей

$\operatorname{char} Z_p(x) = p$, $|Z_p(x)| = \infty$

$$\underset{\text{поле}}{Z_p} \subseteq \underset{\substack{\text{кольцо} \\ \text{многочленов}}}{Z_p[x]} \subseteq Z_p(x)$$

Линейная алгебра

Пусть V – произвольное множество, на котором заданы 2 операции "сложение" и "умножение на число" (т.е. на эл-т из поля F).

Это означает, что $\forall x, y \in V$ и $\forall \lambda \in F$ определены сумма $x + y \in V$ и $\lambda \cdot x \in V$ - произв. на число.

Опр: Мн-во V (с опер. слож. и умн. на число) наз. <u>линейным (векторным) пространством (ЛП)</u> над полем F, если выполнены следующие 8 свойств (аксиом ЛП).

$\forall x, y, z \in V$ и $\lambda, \mu \in F$

1) $x + y = y + x$
2) $(x + y) + z = x + (y + z)$
3) $\exists$ нейтр. эл-т по слож. $0 \in V : x + 0 = 0 + x = x$
4) $\forall x \in V$ $\exists$ противоположный $(-x) \in V : x + (-x) = (-x) + x = 0$

} абелева группа по сложению

5) $1 \cdot x = x \quad \forall x \in V$ – нейтральность $1 \in F$

6) $\lambda(\mu x) = (\lambda\mu)x$ – ассоц. ум-ния на число

7) $(\lambda + \mu)x = \lambda x + \mu x$ – дистриб. относ. суммы чисел

8) $\lambda(x+y) = \lambda x + \lambda y$ – дистриб. относ. суммы векторов.

Пример:

V_3 – геометрические векторы