Кольцо многочленов

F $\quad \mathbb{F}_2 = \mathbb{Z}_2$

$f_i : \mathbb{Z}_2 \to \mathbb{Z}_2$

$f_1 : x \mapsto x \qquad f_1(x) = x$

$f_2 : x \mapsto x^2 \qquad f_2(x) = x^2$

x	0	1
f_1	0	1
f_2	0	1

$a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$

$R[x]$ – многочлены с коэфф. из кольца R

$(a_0, a_1, a_2, a_3 \dots)$ $\quad a_i \in R$ $\quad$ почти все $a_i = 0$ за исключением конеч. числа

$(a_0, a_1, a_2 \dots) + (b_0, b_1, b_2, b_3 \dots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2 \dots)$

$(c_0, c_1, c_2 \dots) = (a_0, a_1, a_2 \dots) \cdot (b_0, b_1, b_2 \dots)$

$$c_k = \sum_{i+j=k} a_i \cdot b_j$$

$c_0 = a_0 \cdot b_0$

$c_1 = a_0 \cdot b_1 + a_1 \cdot b_0$

$c_2 = a_0 \cdot b_2 + a_1 b_1 + a_2 b_0$

Теорема:

если R - кольцо, то

1) $R[x]$ – кольцо

2) R - ассоц, то $R[x]$ - ассоц.

3) R - коммут, то $R[x]$ - коммут

4) R - с единиц, то $R[x]$ - с единиц

нейтр. эл. по слож: $(0,0,0,0\dots)$

$$-(a_1, a_2, a_3\dots) = (-a_1, -a_2, -a_3\dots)$$

дистрибутивность: аккуратное раскр. скобок

если R - ассоц. кольцо:

$$\left.\begin{array}{l}(a(bc))_k \\ ((ab)c)_k\end{array}\right\} = \sum_{i+j+l=k} a_i b_j c_l$$

если R - коммут кольцо: очев.

$$1 \in R \quad (1, 0,0,0\dots)$$

$$x^0 = (1,0,0,0\dots)$$

$$x^1 = (0,1,0,0\dots) = x$$

$$x^2 = (0,0,1,0,0,0,\dots)$$

$$(a_0, a_1, a_2, a_3\dots) = a_0x^0 + a_1x^1 + a_2x^2 + a_3x^3\dots + a_nx^n = f$$

стандартная запись многочлена

$$R \xhookrightarrow{\text{изоморфное вложение}} R[x]$$

$$m \mapsto (m,0,0,0\dots)$$

$$\underset{\text{подкольцо}}{R} \le R[x]$$

$\underset{\text{степень}}{\deg}(f)$ - наибольший номер ненулевого a_i

если $f \overset{\text{тождественно}}{\equiv} 0$ (т.е. все $a_i = 0$), то $\deg(f) = -\infty$

$$\deg : R[x] \to \mathbb{N}_0 \cup \{-\infty\}$$

Далее R – коммут. ассоц. кольцо с 1. пр.: $\mathbb{Z}[x], \mathbb{R}[x], \mathbb{C}[x], \mathbb{Q}[x]$

$f, g \in R[x]$

Лемма:

1) $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$

2) $\deg(f\cdot g) \leq \deg f + \deg g$

$\underbrace{\langle R, +, \cdot \rangle \quad \langle Q, +, \cdot \rangle}_{\text{два разн. кольца}}$

$f: R \to Q$ гомоморфизм колец: если

$$1)\ f(\overset{\text{из } R}{x+y}) = \overset{\text{из } Q}{f(x) + f(y)}$$

$$2)\ f(\overset{\text{из } R}{x\cdot y}) = \overset{\text{из } Q}{f(x)\cdot f(y)}$$

ev_c – гомоморфизм вычисления/эвалюации

$$ev_c: R[x] \to R$$
$$\hat{f} \longmapsto f(c)$$

$$ev_c(f+g) = ev_c(f) + ev_c(g)$$

$$ev_c(fg) = ev_c(f)\cdot ev_c(g)$$

Корень многочлена: $f(c) = 0$

Опр.:

поле F наз. алгебраически замкнутым если любой $\overset{\deg f>0}{f} \in F[x]$ имеет корень

$\mathbb{R}$ не алг. замкнуто (квадратн. многочлен с $D < 0$)

$\mathbb{F}_k$ – конечное поле из k эл.: $a_1, a_2 \ldots a_k$

Пр.: $\mathbb{Z}_3, \mathbb{Z}_5 \ldots \mathbb{Z}_p$

$$\nexists\ (x-a_1)(x-a_2)\dots(x-a_k)+1 \neq 0 \qquad \forall a_k$$

Лемма:

Конечное поле никогда не явл. алг-и замкнутым.

Теорема (осн. теорема алгебры):

поле $\mathbb{C}$ алгебраически замкнуто

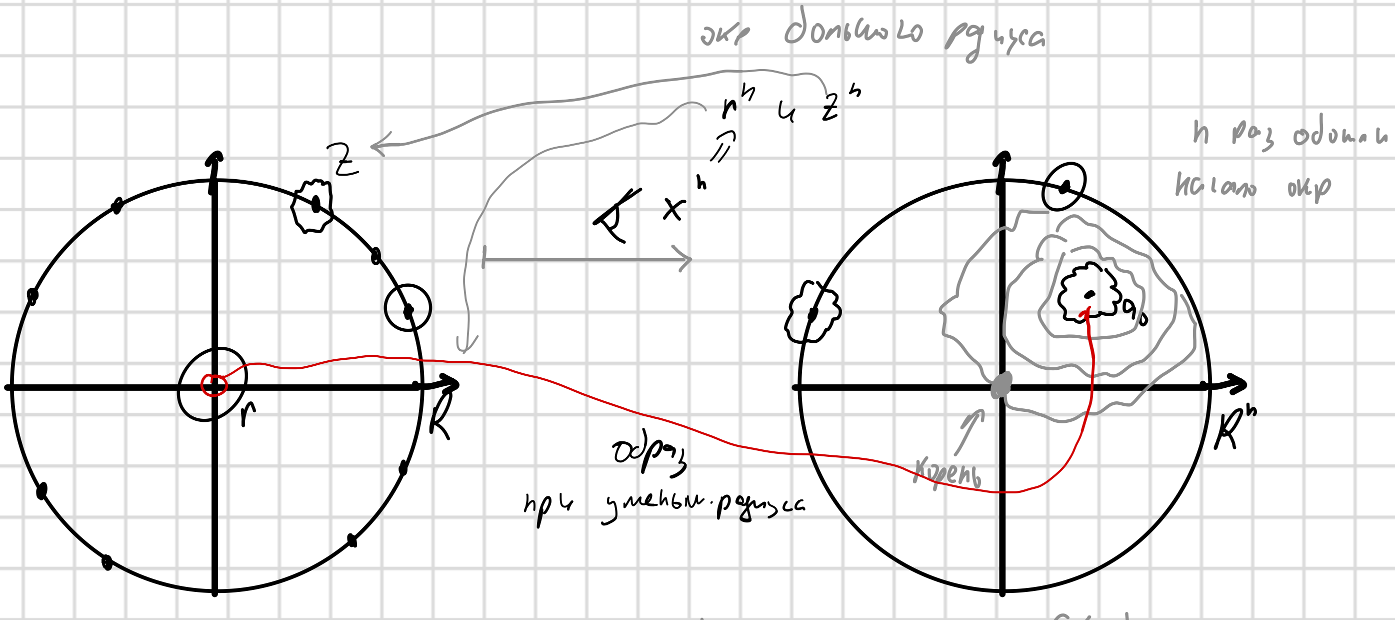
Следствие:

$\forall f \in \mathbb{C}[x]$ $\deg f = n > 0$ имеет ровно n корней (с учетом кратности)

Идея док-ва: („дама с собачкой")

$$f = \underbrace{x^n}_{\text{дама}} + \underbrace{a_{n-1}x^{n-1} + \dots + a_1 x + a_0}_{\text{собачка}}$$

$a_i \in \mathbb{C}$ $\quad \exists\, a_0 \neq 0$ (если $a_0 = 0$, то корень $= 0$)



был момент, когда $f(c)=0$

$$\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2} \qquad z = a + bi$$

$$\overline{z^n} = \overline{z}^{\,n} \qquad \overline{z} = a - bi$$

$$f = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$$

$$a_i \in \mathbb{R}$$

$c \in \mathbb{C} \setminus \mathbb{R} \quad Im(c) \neq 0$ $\qquad \overline{a_i} = a$

Тогда $\bar{c}$ это тоже корень f

$$f(\bar{c}) = \overline{a_n c^n + a_{n-1} c^{n-1} + \ldots + a_1 c + a_0} = \bar{0} = 0$$

Вывод: любой многочлен раскладывается над $\mathbb{R}$ на линейные и квадратичные с отр. дискр-ом

$x_0 \in \mathbb{R}$

корень $f(x_0) = 0$

$f(x) = (x - x_0) S(x)$

$$(x-c)(x-\bar{c}) = x^2 - (c+\bar{c})x + c\bar{c} = x^2 - 2\,\underbrace{Re(c)}_{\in \mathbb{R}} \cdot x + \underbrace{|\bar{c}|^2}_{\in \mathbb{R}}$$

если есть мнимые корень

Следствие: любой многочлен нечетной степени с вещественными коэфф-и имеет как минимум один вещественный корень.

Пр.:

$$\mathbb{C} \quad x^4 - 1 = (x^2-1)(x^2+1) = \underbrace{(x-1)}_{лин}\underbrace{(x+1)}_{лин}\underbrace{(x^2+1)}_{кв.\ с\ D<0} = (x-1)(x+1)(x-i)(x+i)$$

сопряжен