Лекция 1 октября (первая половина)

K - комм. кольцо

В $K[t]$ можно поделить "столбиком" с остатком любой многочлен $f(t) \in K[t]$ на многочлен $g(t) = a_m t^m + \ldots$ с обратимым в K к-том a_m.

$$f = q \cdot g + r \quad \text{, где } r \text{ либо } \underline{\text{нулевой}}$$

$$\text{либо } \deg r < \deg g$$

Если в K нет делителей нуля, то многочлены q и r с таким свойством однозначно определяются по g и f.

__Пример 1__ В любом кольце K с единицей на приведённые многочлены можно делить

$$g(t) = \underset{\substack{\uparrow \\ \text{ст. к-т единица.}}}{t^m} + \ldots$$

$$\forall \alpha \in K \quad \underset{\substack{\big\downarrow \\ x=\alpha}}{f(x)} = \underline{(x-\alpha)}\, q(x) + r \text{, где } \left[\begin{array}{l} r = 0 \\ \deg r = 0 \end{array}\right. \underset{r \in K}{\Downarrow}$$

$f(\alpha)=r$

Вычислять $f(\alpha)$ как остаток от деления столбиком $f(x)$ на $x-\alpha$ гораздо быстрее чем подставлять $x=\alpha$ в

$$\underline{f(x) = b_m x^m + b_{m-1}x^{m-1} + \dots + b_1 x + b_0}$$

$$r = f(\alpha) = b_0 + \alpha(b_1 + \alpha(b_2 + \dots)))$$

Пример: Если $\Bbbk$ – поле, то в $\Bbbk[x]$ можно делить с остатком на любой $\neq 0$ многочлен

$\Bbbk[x] \sim \mathbb{Z}$ делимость устроена "одинаково"

У любого набора многочленов $f_1, \dots, f_m$ есть НОД$(f_1, \dots, f_m)$ – это такой приведённый многочлен d, который

(1) делит все f_i

(2) делится на любой общий делитель всех f_i (у d самая большая степень среди всех общих делителей)

(3) $d = \underline{f_1 \cdot h_1 + f_2 \cdot h_2 + \dots + f_m \cdot h_m}$ для некоторых $h_1, \dots, h_m \in \Bbbk[x]$

Док-во: $(f_1, \dots, f_m) \subset \Bbbk[x]$

$$\overset{\shortparallel}{\left\{ g \in \Bbbk[x] \;\middle|\; g = \sum f_i h_i \text{ для некот. } h_i \in \Bbbk[x] \right\}}$$

Это подкольцо, содержащее вместе с каждым элементом все его кратные, т.е. это идеал в $\mathbb{k}[x]$.

Пусть $d \in (f_1, \dots, f_m)$ – это ненулевой многочлен наименьшей степени, приведённый. Тогда d делит все многочлены из $(f_1, \dots, f_m)$

$$\forall g \in (f_1, \dots, f_m) \quad g = d \cdot q + r \quad \left[\begin{array}{l} \text{либо } r = 0 \\ \text{либо } \deg r < \deg d \end{array}\right.$$

$$r = \underset{\underset{\text{идеал}}{\cap}}{g} - \underset{\cap}{dq} \Rightarrow r \text{ лежит в идеале} \Downarrow r = 0$$

Т.е. идеал $(f_1, \dots, f_m)$ состоит из кратных элемента d (такие идеалы наз. главными)

$\Downarrow$

d делит все $f_1, \dots, f_m$

d представляется в виде $f_1h_1 + \dots + f_mh_m$

d делится на любой общий делитель многочленов $f_1, \dots, f_m$

НОД(g, f) для данных g, f можно искать при помощи алгоритма Евклида точно также, как в $\mathbb{Z}$.

Кольца вычетов $\Bbbk[x]/(f)$

элементы — это классы $[h]_f = [h]$

$$[h_1] = [h_2] \Leftrightarrow h_1 - h_2 \,\vdots\, f \text{ в } \Bbbk[x]$$

это отношение эквивалентности и на классах корректно определены

$$[h_1] + [h_2] = [h_1 + h_2]$$
$$[h_1] \cdot [h_2] = [h_1 h_2]$$

(доказать корректность! — упр.)

Классы биективно соответствуют остаткам от деления на f, т.е. многочленам степени $< \deg f$.

Если $f = a_m t^m + \ldots + a_1 t + a_0$, то каждый класс однозначно записывается в виде $[h] = b_0 + b_1\theta + \ldots + b_{m-1}\theta^{m-1}$, где $\theta = [t]_f$ — класс одночлена t.

$$\beta = b_0 + b_1\theta + \ldots + b_{m-1}\theta$$

$$\gamma = c_0 + c_1\theta + \ldots + c_{m-1}\theta^{m-1}$$

$$\beta\gamma = (b_0 + b_1\theta + \ldots + b_{m-1}\theta^{m-1}) \cdot (c_0 + c_1\theta + \ldots)$$

и взять остаток от деления на f $\Leftrightarrow$

воспользоваться соотношением $f(\theta) = 0$

в $\mathbb{k}[t]/(f)$ $\quad f(t) = a_m t^m + \ldots + a_0$ — это нулевой класс

$$a_m\theta^m + \ldots + a_0 = 0 \text{ в } \frac{\mathbb{k}[t]}{(f)}$$

Пример $\mathbb{Q}[\sqrt{2}] := \dfrac{\mathbb{Q}[t]}{(t^2-2)}$ $\qquad f = t^2 - 2$

$[t] = \theta = \sqrt{2}$

$\theta^2 - 2 = 0$

$$= \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

$\sqrt{2} := \text{класс } t \pmod{t^2-2}$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

Замечание: Это поле!

$$\frac{1}{a + \sqrt{2}b} = \frac{a - \sqrt{2}b}{(a + \sqrt{2}b)(a - \sqrt{2}b)} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}$$

x^2-2 — неприводимый многочлен, не раскладывается в произведение многочленов меньшей степени

Опр: Элемент q в комм. кольце с единицей наз. неприводимым, если $q=ab$ влечёт, что a или b обратим.

$(x-a)(x-b)=x^2-2$ $\qquad$ $2=ab$

Если многочлен f неприводим, то он взаимно-прост со всеми g: $\deg g<\deg f$

т.е. $\text{НОД}(f,g)=1$ $\left(\Leftrightarrow \underbrace{1=fh_1+gh_2}_{h_1,h_2\in\Bbbk[x]} \Leftrightarrow [h_2][g]=1\right)$

$\Updownarrow$

$[g]$ обратим в $\Bbbk[x]/(f)$

Кольцо вычетов по модулю неприводимого многочлена — это поле.

Наоборот, если $f=f_1f_2$ приводим $\deg f_1, \deg f_2<\deg f$, то $\underset{\neq 0}{[f_1]}\,\underset{\neq 0}{[f_2]}=[f]=0$ в $\Bbbk[x]/(f)$ $\Rightarrow$ $\Bbbk[x]/(f)$ это не поле

Упр.: $\mathbb{Q}[x]/(x^3 \underset{\uparrow}{+} x+1)$ – поле

неприводим в $\mathbb{Q}[x]$, т.к. не имеет корней в $\mathbb{Q}[x]$

Сосчитать $(1+x)^{-1}$ – эл-т, обратный к классу $1+x \mod x^3+x+1$

Важный пример: $\mathbb{C} := \dfrac{\mathbb{R}[t]}{(t^2+1)}$

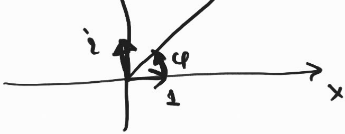
t^2+1 неприводим в $\mathbb{R}[x]$, т.к. не имеет корней в $\mathbb{R}$.

классы имеют вид $x+iy$, $x, y \in \mathbb{R}$

а $i := [t]_{t^2+1}$: $\boxed{i^2=-1}$ $\quad i=\sqrt{-1}$

$$\frac{1}{x+iy} = \frac{x-iy}{(x+iy)(x-iy)} = \frac{x}{x^2+y^2} - \frac{y}{x^2+y^2}i$$

Число $x+iy$ изображается на евклидовой $\mathbb{R}^2$ в виде координатной плоскости точки с радиус-вектором $z=(x,y)$



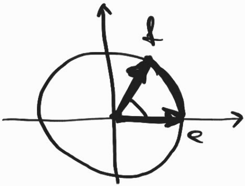
$z = x + iy =$

$= x \cdot 1 + y \cdot i$

$1, i$ — это стандартный ортонормальный базис в $\mathbb{R}^2$.

$\mathrm{Arg}\, z = \varphi + 2\pi k, k \in \mathbb{Z}$

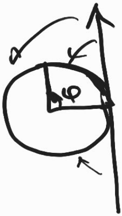
$|z|^2 = x^2 + y^2$ — длина (модуль числа z)



$|e| = |f| = 1$

Угол $\angle(e, f) = \mathrm{Arg}(f)$ — это ориентированная длина дуги единичной окружности, ведущая из конца e в конец f (с + берётся дуга, направленная против ч.с.)

Такая длина определена с точностью до целого числа оборотов, т.е. с точностью до $2\pi\mathbb{Z} \subset \mathbb{R}$



$\varphi + 2\pi\mathbb{Z} \subset \mathbb{R}$