Лекция 2, 17 сентября (вторая половина)

Дополнительные св-ва полей:

(1) $0\cdot a = 0 \quad \forall a$ ← в любом кольце

(2) $(-1)\cdot a = -a$ ← эл-т против. к a ← в любом кольце с единицей?

↑ эл-т, против. к 1

Проверка: $0\cdot a = (0+0)\cdot a = 0\cdot a + 0\cdot a$

к обеим частям добавить элемент $-0\cdot a$, против. к $0\cdot a$

$$0 = 0\cdot a$$

$$a + (-1)\cdot a = 1\cdot a + (-1)\cdot a = (1-1)\cdot a = 0\cdot a = 0$$

Если из определения поля убрать св-во (4) умножения, т.е. не требовать существования обратных эл-тов a^{-1}, то множество с такими двумя операциями наз. **коммутативным кольцом с 1**.

Например: $\mathbb{Z}$ обратные есть только у ± 1.

$\mathbb{Q}[x]$ – многочлены с коэфф-тами в $\mathbb{Q}$

$a_0+a_1x+\ldots+a_kx^k$

обратимы только константы.

$\mathbb{Z}[x]$ обратимы только ± 1.

Если выкинуть из аксиом существование 1 и требование $0 \neq 1$, то то, что получится наз. коммутативным кольцом

Примеры: Чётные числа, многочлены с нулевым свободным членом.

Целые числа $\mathbb{Z}$

a делится на b $(a \,\vdots\, b)$ или b делит a $(b|a)$ если $\exists c:$

$$a=bc$$

Как решать уравнение $\boxed{ax+by=c}$ с данными $a,b,c\in\mathbb{Z}$?

Рассмотрим множество всех чисел,

представимых в виде $ax+by$

$$(a,b) := \{ z = ax+by \mid x, y \in \mathbb{Z} \}$$

- $a \in (a,b)$, $b \in (a,b)$
- замкнуто относительно сложения
- если $k \in (a,b) \Rightarrow$ все кратные $mk \in (a,b)$

$k = ax+by \qquad mk = ma \cdot x + mb \cdot y$

$(a,b) \subset \mathbb{Z}$ — это подкольцо

В частности,

- все числа из (a,b) делятся на любой общий делитель чисел a и b

---

Пусть $d \in (a,b)$ самое маленькое натуральное число. Все числа из (a,b) делятся на d:

$$m \in (a,b)$$

$$\underset{\underset{(a,b)}{\cap}}{m} = q \cdot \underset{\underset{(a,b)}{\cap}}{d} + r, \text{ где } r < d$$

$$r = m - qd \in (a,b) \Rightarrow r = 0.$$

Число d таково, что оно делит a и b и делится на любой общий делитель a и b.

Уравнение $ax+by=c$ разрешимо $\Leftrightarrow c \,\vdots\, d$

---

d наз. наибольшим общим делителем.

наибольший общ. ч.п. $a|b$.

Явно найти d можно при помощи алгоритма Евклида:

$$a \geq b$$

$E_0 = a$, $E_1 = b$, $E_2 =$ остаток от деления a на b,

$E_k =$ остатку от деления E_{k-2} на E_{k-1}

$E_0 > E_1 > \dots$ до тех пор, пока очередное E_{r+1} не обратится в нуль (т.е. пока E_{r-1} не разделится на E_r)

Упр. на дом: Последнее ненулевое E_r это и есть НОД(a,b), т.е. E_r делит и a и b и делится на любой другой общий делитель.

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = c$$

НОД$(a_1, \dots, a_n) = d$ – наименьшее натуральное число, представимое в виде

$a_1x_1 + \dots + a_nx_n$ с целыми $x_1, \dots, x_n$

Оно автоматически делит все числа, представимые в таком виде (включая $a_1, a_2, \dots, a_n$), и делится на любой общий делитель чисел $a_1, \dots, a_n$

$$\text{НОД}(a,b) = 1 \Leftrightarrow \exists\, x, y \in \mathbb{Z} : ax+by=1$$

⊛ **Опр.** Числа a и b в любом комм. кольце K с 1 наз. взаимно-простыми, если $\exists\, x, y \in K : ax+by=1$.

K - комм. кольцо с 1.

Если $K=\mathbb{Z}$, то это равносильно отсутствию у a и b общих делителей, кроме ± 1

В произвольном K из взаимной простоты вытекает, что любой общий делитель a и b обратим

$$a = \alpha \cdot d, \quad b = \beta \cdot d$$

$$ax+by=1 \Rightarrow \alpha d x + \beta d y = 1$$

$$d\underline{(\alpha x + \beta y)} = 1$$

у d есть обратный!

Однако неверно, что два элемента без необратимых общих делителей взаимно просты в смысле Опр. ⊛ !

$\mathbb{Q}[x,y]$ $\quad a = x \quad b = y$

$$\nexists f,g : \underbrace{f(x,y)\cdot x + g(x,y)\cdot y}_{\text{степень} > 0} = 1$$

Факт: Если a и b взаимно просты, то

(1) $a \mid bc \Rightarrow a \mid c$

(2) $c \,\vdots\, a$ и $c \,\vdots\, b \Rightarrow c \,\vdots\, ab$

Ещё одно свойство: если a взаимно прост с каждым из $b_1, b_2, \ldots, b_m$, то a взаимно прост и с $b = b_1 b_2 \ldots b_m$

в любом К.К. с единицей

$$ax + by = 1$$

↓ умножим на c

$$\boxed{c = \underline{ac}x + \underline{bc}y} \Rightarrow (1) \text{ и } (2)$$

$\forall i \;\exists x_i, y_i : \quad x_i a + y_i b_i = 1$

$$(x_1 a + y_1 b_1) \ldots (x_m a + y_m b_m) = 1$$

Перемножим все эти равенства.

$$a\cdot\underbrace{(\ldots)}_{K}+\underbrace{y_1\ldots y_m}_{K}b_1\ldots b_m=1$$

a и $b_1\ldots b_m$ взаимно просты.

Кольца вычетов: $\mathbb{Z}/(n)$ — фактор множества $\mathbb{Z}$ по отношению эквивалентности, объединяющему в один класс все числа с одинаковым остатком от деления на n

$$x\equiv y \pmod n \Leftrightarrow x-y \,\vdots\, n$$

$[x]$ класс числа $x\in\mathbb{Z}$ mod n.

$$[x]+[y]:=[x+y]$$
$$[x][y]:=[xy]$$

Правила дают один и тот же результат, независимо от способа записи класса, т.е. $[x_1]=[x_2]$, $[y_1]=[y_2]$ $\Rightarrow$

$$[x_1+y_1]=[x_2+y_2]$$ (проверьте!)
$$[x_1y_1]=[x_2y_2]$$

в $\mathbb{Z}/(6)$ $\quad [2]\cdot[3]=[0]$

Элемент $a\in K$ наз. делителем нуля, если $\exists b\neq 0 : ab=0$

Бывают ненулевые делители нуля!

в $\mathbb{Z}/(8)$ $\quad [2]^3=[2][2][2]=[8]=[0]$

Элемент $a\in K$ наз. нильпотентным если $\exists n\in\mathbb{N} : a^n=0$

(все нильпотенты явл. делителями нуля).

Зам: Элемент $[a]^{\neq 0}\in\mathbb{Z}/(n)$ обратим $\Longleftrightarrow$ НОД $(a,n)=1 \Longleftrightarrow [a]$ не делитель нуля.

Док-во: НОД $(a,n)=1 \Longleftrightarrow \exists x,y\in\mathbb{Z}$ $ax+ny=1$

$$\Updownarrow$$

$$[x]\cdot[a]=1$$

$ab=0$ и $\exists a^{-1} \Rightarrow b=0$

обратимый эл-та a не может делить 0 в любом к.к. с единицей

если $a=kd$, $n=md$ $\quad [m]\neq 0$

$[m]\cdot[a]=[kmd]=[kn]=0$