Лекция 21, 21.02.24

Пример: $M_n(\mathbb{R})$ – матричное кольцо (некоммут., но с "1")

$\mathbb{R}[X]$ – кольцо многочленов на $\mathbb{R}$

$(\mathbb{Z}_n, +, \cdot)$ – кольцо вычетов по mod n. "+": $\bar{k} + \bar{l} = \overline{(k+l)}$

$\mathbb{Z}_4$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	0	1	2	3
$\bar{1}$	1	2	3	0
$\bar{2}$	2	3	0	1
$\bar{3}$	3	0	1	2

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	0	0	0	0
$\bar{1}$	0	1	2	3
$\bar{2}$	0	2	0	2
$\bar{3}$	0	3	2	1

$(\mathbb{Z}_4 \setminus \{0\}, \cdot)$ – не группа, т.к. $\bar{2}$ не обратим

Опр: Если $a \cdot b = 0$, при этом $a \neq 0$ и $b \neq 0$ в кольце K, то a наз. левым делителем 0, а b – правым делителем 0.

Пример: в $\mathbb{Z}_4$ $\bar{2}$ – делитель 0.

Утв: $\forall a \in K \quad a \cdot 0 = 0 \cdot a = 0$ в кольце K (т.е. 0 – поглощ. эл-т)

□ $a + 0 = a$ (0 – нейтр. по слож.)

$a(a+0) = a \cdot a$ (домножили слева на a)

$a^2 + a \cdot 0 = a^2$ (по дистрибутивности)

$-a^2 + a^2 + a \cdot 0 = -a^2 + a^2$ (прибавили $-a^2$ – обр. по слож.)

$0 + a \cdot 0 = 0$

$a \cdot 0 = 0$

Умножение на 0 слева аналогично ■

Замечание: Если в кольце K с единицей $0 = 1$, то $K = \{0\}$ (кольцо тривиально) (т.к. $\forall a \in K \quad a = a \cdot 1 = a \cdot 0 = 0$).

Опр: Коммут. кольцо с единицей ($\neq 0$) и без делителей нуля наз. целостным кольцом (областью целостности).

Пример: $\mathbb{Z}_3$, $\mathbb{Z}$ – области целостности.

Утв: Коммут. кольцо с „1" ($\neq 0$) явл. целостным $\Leftrightarrow$ в нём выполняется закон сокращения, т.е. из $ab = ac$ и $a \neq 0 \Rightarrow b = c$.

□ „$\Rightarrow$" $ab = ac \Leftrightarrow a(b-c) = 0$, нет делителей 0 $\Rightarrow b = c$.

„$\Leftarrow$" если $ab = 0$ и $a \neq 0$, то $b = 0$, т.к. $ab = 0 = a \cdot 0 \Rightarrow b = 0$ по зак. сокр. ■

Опр: Эл-т a кольца K с единицей наз. обратимым, если

$\exists a^{-1} \in K \quad a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Утв: Все обратимые эл-ты кольца образуют группу по умнож.

Обознач.: $U(K)$ - мультипликативная подгруппа кольца.

$(1 \in U(K),\ (a^{-1})^{-1} = a \Rightarrow a^{-1} \in U(K),\ (ab)^{-1} = b^{-1} \cdot a^{-1} \Rightarrow ab \in U(K))$

Опр: Поле P - это коммутативное кольцо с единицей, в котором каждый эл-т кроме нуля обратим

Пример: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ ($\mathbb{Z}$ - не поле)

$P^{\times} = (P \setminus \{0\}, \cdot)$ - абелева группа по умнож.

Поле - это где пшеница растёт, либо эл-т класса в C#!!!

Опр: Подмножество L кольца K ($L \subseteq K$) наз. подкольцом, если оно само явл. кольцом относит. "+" и "·", заданных в K.

Замечание: $L \subseteq K$ - подкольцо в $K \Leftrightarrow$ выполнены 2 условия:

1) $\forall x, y \in L \quad x - y \in L$ (крит. подгр. в $(K, +)$: $\forall h_1, h_2 \in H,\ h_1 h_2^{-1} \in H$)

2) $\forall x, y \in L \quad x \cdot y \in L$

Опр: Подполе (не путать с подпольем) - подмножество в поле P, которое само явл. полем относит. опер. ("+", "·") в P.

Пример: $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ - подполя в $\mathbb{C}$ ($\mathbb{Z}$ - не поле, но подкольцо в них).

Алгоритм Евклида

Рассмотрим $K[x]$ - кольцо многочленов от переменной x с коэфф. из K, где K - целостное кольцо.

Замечание: $K[x]$ - коммут. кольцо с „1"

Пусть $g(x) \in K[x]$ - многочлен со старшим коэф., обратимым в K.

Тогда $\forall f(x) \in K[x]$ $\exists!$ пара мн-нов $q(x), r(x) \in K[x]$ такие, что $f(x) = g(x)q(x) + r(x)$, где $\deg r(x) < \deg g(x)$

Т.е. $f(x)$ разделим с остатком на $g(x)$ (можно делить „уголком")

Пример: $\mathbb{Z}[x]$ $x^2+1 \;\vdots\!\!\!\big/\; 2x$ - не сможем поделить, т.к. $\nexists 2^{-1} \in \mathbb{Z}$.

Пусть $F[x]$ - кольцо многочленов над полем F.

Тогда $\forall\, a(x), b(x) \in F[x]$ справедлив <u>алгоритм Евклида</u> нахождения $НОД(a(x), b(x))$.

Будем последовательно делить с остатком:

$a = b \cdot q_1 + r_1$, где $\deg r_1 < \deg b$

$b = r_1 q_2 + r_2$, где $\deg r_2 < \deg r_1$

$\vdots$

$r_{k-2} = r_{k-1} q_k + r_k$

$r_{k-1} = \boxed{r_k} q_{k+1} + r_{k+1}$, где $r_{k+1} = 0$ ← дойдём до этого шага, т.к. степени мн-в $b, r_1, \dots, r_k$ образуют строго убыв. послед. неотр. чисел $\Rightarrow$ „упрёмся" в 0.

$НОД(a(x), b(x)) = r_k(x)$

Утв: (Следствие из алг. Евклида):

$\forall a(x), b(x) \in F[x] \quad \exists u(x), v(x) \in F[x]$ такие, что

$НОД(a,b) = a \cdot u + b \cdot v$

(Выражаем остаток r_1 через a и b в 1м равенстве, подставл. в во 2е и т.д. спускаемся к последнему)

Опр: Эл-ты a и b в произв. коммут. кольце с единицей наз. взаимно простыми, если $\exists x, y$ из того же кольца: $ax + by = 1$ (соотношение Безу)

Гомоморфизм колец, идеали

Опр: Отображение $\varphi : (K_1, +, \cdot) \to (K_2, \oplus, *)$ наз. гомоморфизмом колец, если $\forall x, y \in K_1$

1) $\varphi(x+y) = \varphi(x) \oplus \varphi(y)$

2) $\varphi(x \cdot y) = \varphi(x) * \varphi(y)$

Т.е. φ „уважает" и сложение, и умножение

Опр: Подмножество I кольца K наз. (двухсторонним) идеал, если оно:

1) Явл. подгруппой по сложению в $(K, +)$.

2) $\forall a \in I \quad \forall r \in K \quad r \cdot a \in I$ и $a \cdot r \in I$

(идеал „поглощает" эл-ты по умножению)

Пример: $2\mathbb{Z}$ - идеал в $\mathbb{Z}$ ($2\mathbb{Z}$ - подгр. в $(\mathbb{Z}, +)$, чёт. · цел. = чёт)

Замечание: $\forall$ идеал I явл. подкольцом в K.

Замечание: Пусть K – коммут. кольцо

Тогда $\forall a \in K \quad \langle a \rangle = \{r \cdot a \mid r \in K\}$ явл. идеалом (по опр.).

Опр: Идеал I наз. <u>главным</u>, если $\exists a \in K: I = \langle a \rangle$, т.е. идеал порождён одним эл-том.

Пример: В $\mathbb{R}[x] \quad \langle x^2+1 \rangle = \{(x^2+1) \cdot f(x) \mid f(x) \in \mathbb{R}[x]\}$

Замечание: Кольцо $\mathbb{Z}$ целых чисел явл. кольцом главных идеалов (в нём все идеалы главные).

□ Т.к. все подгруппы в $\mathbb{Z}$ имеют вид $k\mathbb{Z} = \langle k \rangle$
идеал порожд. $k \in \mathbb{Z}$ ■

Замечание: Любой идеал явл. нормальной подгр. в $(K, +)$.
т.к. $(K, +)$ – абелева группа, и в ней все подгр. нормальные.

$\Rightarrow$ Можно рассмотреть факторгруппу $(K/I, +)$ – с операцией сложения (т.е. $(a+I)+(b+I) = (a+b)+I \quad \forall a, b \in K$)

Введём на ней умножение:

$$(a+I)(b+I) = ab + I$$

смежные классы по слож.

Замечание: Умнож. корректно, т.к. $(a+I)(b+I) = ab + aI + Ib + I =$

$= a \cdot b + I$ $\left(\forall h \in I \ (a+h)(b+h) = ab + \underbrace{hb + ah}_{\in I \text{ по опр. идеала}} + h^2\right)$, т.к.

aI и Ib лежит в I по опр. идеала.

Опр: $(K/I, +, \cdot)$ с введёнными опер. "$+$" и "$\cdot$" наз. <u>факторкольцом</u> кольца K по идеалу I.

Пример: $\mathbb{Z}/\underbrace{k\mathbb{Z}}_{\text{идеал}} \cong \mathbb{Z}_k$ – кольцо вычетов