Seminar 22, 04.03.24

Кольцо – мн-во R с опер. $+$ и $\cdot$, т.к. $(R, +)$ – абелева группа

и $x(y+z) = x\cdot y + x\cdot z$

$(y+z)x = y\cdot x + zx$ $\quad \forall x, y, z \in R$

Кольцо R наз:

- ассоциативным, если $(R, \cdot)$ – полугруппа
- унитальным, если $(R, \cdot)$ – моноид (Кольцо с единицей)
- коммутативным, если $(R, \cdot)$ – коммутативно

В основном под кольцом будем понимать ассоц. кольцо с единицей.

Пример не ассоц. некоммут. кольца без единицы: евклидово пространство со сложением векторов и вект. умнож.

Пусть R – кольцо. Группа обратимых элементов моноида $(R, \cdot)$ наз. мультипликативной группой кольца R и обознач. $R^{\times}$.

Элемент $x \in R$ наз. обратимым, если $x \in R^{\times}$. Заметим, что $0 \notin R^{\times}$, кроме одного случая.

Кольцо R наз. нулевым, если $R = \{0\}$

① R – нулевое кольцо $\Longleftrightarrow$ $1 = 0$.

□ „$\Rightarrow$" Очев.

„$\Leftarrow$" $x \in R \Rightarrow x = x \cdot 1 = x \cdot 0 = 0$ ■

Ненулевое коммут. кольцо R наз. полем.

...(какая-то теория из лекции)...

Примеры колец: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_n$

Если R, S - кольца, то $M_n(R)$, $R[x]$, $R \oplus S$ $(R \times S)$

② Что является кольцом?

1) $R = \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\} \subseteq \mathbb{R}$ с обычными $+$ и $\cdot$.

□ Очевидно, группа по сложению

$(x + y\sqrt{2})(a + b\sqrt{2}) = (xa + 2yb) + \sqrt{2}(ay + xb) \in \mathbb{R} \Rightarrow$ да ■

2) $R = \{a + y\sqrt[3]{2} \mid x, y \in \mathbb{Q}\} \subseteq \mathbb{R}$ с обычными $+$ и $\cdot$.

□ Очевидно, группа по сложению.

$\sqrt[3]{4} = \sqrt[3]{2} \cdot \sqrt[3]{2} \in \mathbb{R}$, т.е.

$\sqrt[3]{4} = x + \sqrt[3]{2}\, y$ Обозначим: $\alpha = \sqrt[3]{2} \Rightarrow \alpha^2 + \alpha y + x = 0$,

т.е. $\exists$ мн-н $f(t) \in \mathbb{Q}[t]$ степени 2, т.ч. $f(\alpha) = 0$. Но $\alpha^3 - 2 = 0$

$\Rightarrow f(t) \mid t^3 - 2$. Но $t^3 - 2$ неприводим над $\mathbb{Q} \Rightarrow$ (!) $\Rightarrow$ нет. ■

HSE

③ Мн-во матриц порядка $n \geqslant 2$, у которых последние 2 строки нулевые с обычными + и $\cdot$.

□ Группа по сложению.

$$\begin{pmatrix} & * & \\ 0\,0 & \dots & 0\,0 \\ 0\,0 & \dots & 0\,0 \end{pmatrix}\begin{pmatrix} & * & \\ 0\,0 & \dots & 0\,0 \\ 0\,0 & \dots & 0\,0 \end{pmatrix} = \begin{pmatrix} & * & \\ 0\,0 & \dots & 0\,0 \\ 0\,0 & \dots & 0\,0 \end{pmatrix}$$

Единица – это $\begin{pmatrix} 1 & & 0 \\ 0 & \ddots & 1 \\ 0\,0 & \dots & 0\,0 \\ 0\,0 & \dots & 0\,0 \end{pmatrix}$ => Да ■

④ Мн-во функций $\mathbb{R} \to \mathbb{R}$, непрерывных на отрезке $[a;b]$, относит. обычных + и $\cdot$ для функций.

□ Из мат. анализа известно, что для f, g непр. на $[a;b]$ $f+g$, $f \cdot g$, $-f$ непр. на $[a;b]$.

Очев. $f(x) \equiv 1$ и $f(x) \equiv 0$ непр. на $[a;b]$. => Да ■

⑤ Мн-во всех многочленов из $\mathbb{R}[t]$ с обычным слож. и умножением.

$(f \circ g)(t) = f(g(t))$

□ Очев. группа по слож.

$f, g \in \mathbb{R}[t] \Rightarrow f \circ g \in \mathbb{R}[t]$

Единица по умножению – это t

Ассоц. следует из ассоц. композиции.

Но нет дистрибутивности: $1 \circ (1+1) = 1$
$1 \circ 1 + 1 \circ 1 = 2$ ($\neq$) => Нет.

■

③ Разделить с остатком: $f(x) = x^3 - 3x^2 - x - 1$; $g(x) = 3x^2 - 2x + 1$

$$\begin{array}{r|l} - x^3 - 3x^2 - x - 1 & 3x^2 - 2x + 1 \\ \cline{2-2} x^3 - \frac{2}{3}x^2 + \frac{1}{3}x & \frac{1}{3}x - \frac{7}{9} \\ \cline{1-1} - -\frac{7}{3}x^2 - \frac{4}{3}x - 1 & \\ -\frac{7}{3}x^2 + \frac{14}{9}x - \frac{7}{9} & \\ \cline{1-1} -\frac{26}{9}x + \frac{2}{9} & \end{array}$$

Алгоритм Евклида нахождения НОД двух эл-тов f, g: кольца $F[x]$, F - поле ($\mathbb{Z}$).

Пусть $\deg f \geq \deg g$ $(|f| \geq |g|)$

$f = g \cdot q + r$ для нек. q, r и $\deg r < \deg g$

Заменяем $(f_0, g_0) = (f, g) \to (f_1, g_1) = (g, r)$ и продолжаем. В какой-то момент $g_n \mid f_n \Rightarrow НОД(f, g) = g_n$

Обратный ход в алг. Евклида позволяет получить выражение $НОД(f, g) = a \cdot f + b g$ для нек. a, b.

④ $f(x) = 3x^3 - 2x^2 + x + 2$ $\quad g(x) = x^2 - x + 1$

$f_0 = f$, $g_0 = g$

$f_0 = q_0 \cdot g_0 + r_0$

$f_0 = (3x+1) g_0 + (-x+1)$

$f_1 = x^2 - x + 1$ $\quad g_1 = -x + 1$

$f_1 = -x \cdot g_0 + 1$

$f_2 = -x + 1$ $\quad g_2 = 1$

$НОД(f, g) = -x + 1$

$-x + 1 = f_0 - (3x+1) g_0 =$

$= f - (3x+1) g$ - лин. выражение

HSE

⑤ Над $F_2 = \mathbb{Z}_2 = \{0; 1\}$

$f(x) = x^5 + x^4 + 1 \qquad g(x) = x^4 + x^2 + 1$

Замечание: В F_2 $\quad -x = x \quad \forall x \quad (2 = 1+1 = 0)$

$f_0 = f \quad g_0 = g$

$$\begin{array}{r|l}
x^5 + x^4 + 1 & x^4 + x^2 + 1 \\
\cline{2-2}
-\ x^5 + x^3 + x & x + 1 \\
\cline{1-1}
x^4 + x^3 + x + 1 & \\
-\ x^4 + x^2 + 1 & \\
\cline{1-1}
x^3 + x^2 + x &
\end{array}$$

$f_0 = (x^3 + x^2 + x) g_0 + (x+1)$

$f_1 = x^4 + x^2 + 1, \quad g_1 = x + 1$

$f_1 = (x^3 + x^2) g_1 + (1) \qquad НОД(f, g) = x + 1$

Подмножество $\mathfrak{a}$ кольца R наз. **левым идеалом**, если $\mathfrak{a} \subseteq R$ — подгруппа по сложению и $\forall x \in R$ $\forall a \in \mathfrak{a}$ $\quad x \cdot a \in \mathfrak{a}$

Аналогично можно определить правый и двусторонний идеал.

Идеал $\underset{\text{коммут.}}{\mathfrak{a} \subseteq R}$ наз. **главным**, если $\exists x \in R : \mathfrak{a} = \{r \cdot x \mid r \in R\}$

$\mathfrak{a}$ порождён x, пишут $\mathfrak{a} = (x)$.

⑥ Найти все идеалы в кольце:

1) $\mathbb{Z}$

$\triangleright$ $\mathfrak{a} \subseteq \mathbb{Z}$ - идеал $\Rightarrow$ $\mathfrak{a}$ подгруппа $\Rightarrow$ $\exists n \in \mathbb{N} : \mathfrak{a} = n\mathbb{Z}$ - уже идеал. Значит, любой идеал - это (n) $\blacksquare$

2) $F[x]$, f - поле

$\square$ $\mathfrak{a} \subseteq F[x]$ - идеал

Пусть $\mathfrak{a} \neq \{0\}$

Возьмём $f \in \mathfrak{a} \setminus \{0\}$ минимальной степени.

Тогда, если $g \in \mathfrak{a}$, поделим g на f с остатком:

$$\underset{\mathfrak{a}}{\underset{\cap}{g}} = \underbrace{q \cdot f}_{\underset{\mathfrak{a}}{\cap}} + r \quad , \quad \deg r < \deg f$$

$$r = g - q \cdot f \in \mathfrak{a} \Rightarrow r = 0, \text{ т.е. } f \mid g \Rightarrow \mathfrak{a} = (f). \blacksquare$$

Пусть $\alpha \in \mathbb{C}$ - алгебраическое число, т.е. $\exists f \in \mathbb{Q}[t] \setminus \{0\}$, т.ч. $f(\alpha) = 0$. Среди всех таких мн-в сущ. единственный минимальной степени со старшим коэфф. 1.

$$q_\alpha(x) = x^d + a_1 x^{d-1} + \ldots + a_d$$

Если $f \in \mathbb{Q}[t] \setminus \{0\}$, т.ч. $f(\alpha) = 0$, то $f = s \cdot q_\alpha + r$ $\deg r < \deg q_\alpha$

$$0 = f(\alpha) = s(\alpha) \cdot \underbrace{q_\alpha(\alpha)}_{\overset{\shortparallel}{0}} + r(\alpha) \Rightarrow r(\alpha) = 0 \Rightarrow r = 0$$

$\Rightarrow$ любой f делится на q_α $\Rightarrow$ $\alpha = \sqrt[3]{2}$, $q_\alpha(t) = t^3 - 2$.