Лекция 19.

Гайфуллин Сергей Александрович

МГУ

2 декаря, 2020

Определение.

Кольцо – это множество R с двумя бинарными операциями $+$ и $\cdot$ такими, что $(R, +)$ является абелевой группой и $a(b+c) = ab + ac$, $(a+b)c = ac + bc$.

Примеры:

1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ – это поля.

2) $\mathbb{Z}, \mathbb{Z}_n, \mathbb{R}[x]$ – коммутативные кольца.

3) $\mathrm{Mat}_n(F), \mathbb{C}[G]$ – вообще говоря не коммутативные, но ассоциативные кольца.

4) $(\mathbb{R}^3, +, [,])$ – не ассоциативное кольцо.

Определение.

Если $a, b \in R$ и выполнено $a \neq 0$, $b \neq 0$, $ab = 0$, то элемент a называется левым делителем нуля, а элемент b – правым делителем нуля.
Объединение множества левых и правых делителей нуля называется множеством делителей нуля.

Лемма. Обратимые элементы не являются делителями нуля.

Доказательство. Пусть $a \neq 0$, $b \neq 0$, $ab = 0$. В пусть при этом элемент a обратим. Тогда $b = a^{-1}ab = a^{-1}0 = 0$.
Противоречие.

Определение.

Элемент $x \neq 0$ называется нильпотентным, если существует натуральное n такое, что $x^n = 0$.

Так как $x^n = x \cdot x^{n-1} = x^{n-1} \cdot x$, нильпотент является (двусторонним) делителем нуля.

Примеры.

1) В кольце $\mathbb{Z}_6$ выполнено $2 \cdot 3 = 0$, то есть 2 и 3 – делители нуля (но не нильпотенты).
2) В кольце $\mathbb{Z}_4$ выполнено $2^2 = 0$, то есть 2 – нильпотент.
3) В кольце $\mathrm{Mat}_2(\mathbb{R})$ выполнено $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, то есть это делители нуля (не нильпотенты).
4) В кольце $\mathrm{Mat}_2(\mathbb{R})$ выполнено $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, то есть это нильпотент.

Определение.

Алгебра над полем F – это множество A с тремя операциями. Две из них бинарные: сложение и умножение. А последняя – умножение на число (элемент поля F). При этом выполнены следующие свойства.

1) $(a+b)+c=a+(b+c)$;
2) существует $0 \in A$ такой, что $a+0=0+a=a$;
3) $\forall a \in A$ существует $-a \in A$: $a+(-a)=(-a)+a=0$;
4) $a+b=b+a$;
5) $a(b+c)=ac+ac$;
6) $(a+b)c=ac+bc$;
7) $\lambda(a+b)=\lambda a+\lambda b$;
8) $(\lambda+\mu)a=\lambda a+\mu a$;
9) $(\lambda\mu)a=\lambda(\mu)a$;
10) $1a=a$;
11) $\lambda(ab)=(\lambda a)b$.

Примеры.

1) $\mathrm{Mat}_{n\times n}(F)$;
2) $F[x_1, \ldots, x_n]$;
3) $F[G]$;
4) $F \subset K$; (Например, $\mathbb{C}$ – алгебра над $\mathbb{R}$);
5) $\mathbb{H}$ – алгебра кватернионов.

$\mathbb{H} = \langle 1, i, j, k\rangle_{\mathbb{R}}$, где умножение базисных элементов происходит как в Q_8. $\mathbb{H}$ – ассоциативная не коммутативная 4-мерная алгебра с единицей над $\mathbb{R}$.

Пусть $q = a + bi + cj + dk$. Определим сопряженный кватернион $\overline{q} = a - bi - cj - dk$. Тогда $q\overline{q} = a^2 - (bi + cj + dk)^2 = a^2 + b^2 + c^2 + d^2 = |q|^2$.

Определение.

Алгебра называется алгеброй с делением, если любой ненулевой элемент в ней обратим.

$\mathbb{H}$ – алгебра с делением.

Определение.

Гомоморфизм колец – это отображение $\varphi\colon R \to S$ такое, что для любых $r_1, r_2 \in R$ выполнено $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$ и $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$.
Гомоморфизм алгебр – это гомоморфизм колец $\varphi\colon A \to B$ такой, что, $\varphi(\lambda a) = \lambda\varphi(a)$.
Изоморфизм – это биективный гомоморфизм.

Замечание.

Если A – алгебра с единицей 1_A, то поле F вкладывается в A по правилу $f \mapsto f1_A$. Поэтому если A – алгебра с единицей, то любой гомоморфизм колец $A \to B$ в алгебру B автоматически является гомоморфизмом алгебр.

Упражнение.

Докажите, что алгебра $\mathbb{H}$ изоморфна алгебре вещественных матриц вида

$$\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & -c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix},$$

а также алгебре комплексных матриц вида

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}.$$

Определение.

Пусть R – кольцо. Подмножество I в R называется левым идеалом, если I – подгруппа по сложению и для любых $r \in R, i \in I$ выполнено $ri \in I$.

Пусть R – кольцо. Подмножество I в R называется правым идеалом, если I – подгруппа по сложению и для любых $r \in R, i \in I$ выполнено $ir \in I$.

Идеал двусторонний, если он и левый и правый идеал.

Пример.

Пусть $x \in R$ рассмотрим $I = (x) = \{rx\}$. Легко видеть, что I – левый идеал.

Аналогично, $J = \{xr\}$ – правый идеал.

Пусть M – подмножество R. Тогда

$I = (M) = \{\sum r_i m_i \mid r_i \in R, m_i \in M\}$ – левый идеал M.

Лемма. (M) – минимальный левый идеал, содержащий M.

Доказательство. Пусть $u = \sum r_i m_i$ и $v = \sum r_i m_i'$ – произвольные элементы в (M). Тогда
$u + v = \sum r_i(m_i + m_i') \in (M)$.
$ru = \sum r r_i m_i \in (M)$.
Таким образом, (M) – левый идеал.
Если J – левый идеал, содержащий M, то $r_i m_i \in J$, а значит, $\sum r_i m_i \in J$. То есть $(M) \subset J$.

Определение.

Пусть $\varphi\colon R \to S$ – гомоморфизм. Ядро φ – это полный прообраз нуля, то есть $\operatorname{Ker}\varphi = \{r \in R \mid \varphi(r) = 0\}$. Образ гомоморфизма – это множество образов всех элементов.

Лемма. Пусть $\varphi\colon R \to S$ – гомоморфизм. Тогда ядро – это двусторонний идеал в R, а образ – подкольцо в S.

Доказательство. Пусть $u, v \in \operatorname{Ker}\varphi$. Тогда
$\varphi(u+v) = \varphi(u) + \varphi(v) = 0$, то есть $u+v \in \operatorname{Ker}\varphi$.
$\varphi(ru) = \varphi(r)\varphi(u) = \varphi(r)0 = 0, \qquad \varphi(ur) = 0\varphi(r) = 0.$
То есть $ru, ur \in \operatorname{Ker}\varphi$. Значит, ядро – это двусторонний идеал.
$\varphi(a) + \varphi(b) = \varphi(a+b)$, $\varphi(a)\varphi(b) = \varphi(ab)$ Значит, образ – подкольцо.

Определение.

Факторкольцо R/I кольца R по двустороннему идеалу I – это множество смежных классов $r + I$ с операциями

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I;$$

$$(r_1 + I)(r_2 + I) = (r_1 r_2) + I.$$

Теорема о гомоморфизме. Пусть $\varphi\colon R \to S$ – гомоморфизм колец. Тогда $R/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$.

Доказательство. Построим отображение $\Psi\colon R/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi$, $r + \operatorname{Ker}\varphi \mapsto \varphi(r)$. Надо проверить 1) что это отображение корректно, 2) что это гомоморфизм, 3) что это биекция.

1) Пусть $r + \operatorname{Ker}\varphi = s + \operatorname{Ker}\varphi$. Это означает, что $r - s \in \operatorname{Ker}\varphi$. Тогда $\varphi(r) = \varphi(s)$.

2) $\Psi((r + \operatorname{Ker}\varphi) + (s + \operatorname{Ker}\varphi)) = \Psi((r + s) + \operatorname{Ker}\varphi) =$
$= \varphi(r + s) = \varphi(r) + \varphi(s)$,
$\Psi((r + \operatorname{Ker}\varphi)(s + \operatorname{Ker}\varphi)) = \Psi((rs) + \operatorname{Ker}\varphi) = \varphi(rs) = \varphi(r)\varphi(s)$.

3) $\operatorname{Ker}\Psi = \{r + \operatorname{Ker}\varphi \mid \varphi(r) = 0\}$. То есть $\operatorname{Ker}\Psi$ состоит только из одного смежного класса $\operatorname{Ker}\varphi$. Это доказывает инъективность.

Сюръективность Ψ очевидна.