Лекция 11

Определение 1. Множество R с двумя бинарными операциями $+$ и $\cdot$ называется *кольцом*, если выполнено

1) $(a+b)+c=a+(b+c)$,
2) существует 0 такой, что $a+0=0+a=a$,
3) для каждого a существует $(-a)$ такой, что $a+(-a)=(-a)+a=0$,
4) $a+b=b+a$,
5) $a(b+c)=ab+ac$,
6) $(a+b)c=ac+bc$.

Кольцо ассоциативно, если

7) $(ab)c=a(bc)$.

Кольцо с единицей, если

8) существует 1 такой, что $1a=a1=a$.

Кольцо коммутативно, если

9) $ab=ba$.

Коммутативное ассоциативное кольцо с единицей называется *полем*, если выполнено

10) для каждого $a\neq 0$ найдется a^{-1} такой, что $aa^{-1}=a^{-1}a=1$.

Пример 1. *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.*

Замечание 1. Далее в нашем курсе мы будем рассматривать только ассоциативные кольца. Таким образом все кольца, о которых будет идти речь, предполагаются ассоциативными.

Определение 2. Пусть фиксировано поле F. Множество A называется *алгеброй* (над F), если на нем определены три операции: сложение, умножение и умножение на скаляр (элемент поля F) такие, что

1) A с операциями сложения и умножения – это кольцо,
2) A с операциями сложения и умножения на скаляр – это векторное пространство над F,
3) $(\lambda a)b=a(\lambda b)=\lambda(ab)$.

Пример 2. *Матрицы* $n\times n$ *образуют ассоциативную алгебру с единицей.*

Определение 3. 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 1. *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 4. Элемент $x\neq 0$ называется *нильпотентным*, если существует натуральное n такое, что $x^n=0$.

Замечание 2. Так как $x^n=x\cdot x^{n-1}=x^{n-1}\cdot x$, нильпотент является (двусторонним) делителем нуля.

Пример 3. *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* $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$*, 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 5. *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) $\lambda(ab) = (\lambda a)b = a(\lambda b)$.

Пример 4. *1)* $\mathrm{Mat}_{n\times n}(F)$ *– алгебра над* F*;*

2) $F[x_1, \ldots, x_n]$ *– алгебра над* F*;*

3) Если $F \subset K$ *– вложение полей, то* K *– алгебра над* F*. (Например,* $\mathbb{C}$ *– алгебра над* $\mathbb{R}$*);*

4) $\mathbb{H}$ *– алгебра кватернионов над* $\mathbb{R}$*.*

$\mathbb{H} = \langle 1, i, j, k\rangle_{\mathbb{R}}$*, 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 6. *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 3. 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 1. 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 7. 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 5. *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 2. *Пусть R – кольцо с единицей. Тогда (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 $u + v = \sum (r_i + r'_i) m_i \in (M)$, $-u = \sum (-r_i) m_i \in M$, $ru = \sum r r_i m_i \in (M)$. 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 8. 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 3. *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 $u + v \in \operatorname{Ker}\varphi$. Кроме того $\varphi(-u) = -\varphi(u) = 0$. Значит, $-u \in \operatorname{Ker}\varphi$. А также $\varphi(ru) = \varphi(r)\varphi(u) = \varphi(r)0 = 0$, $\varphi(ur) = 0\varphi(r) = 0$. То есть $ru, ur \in \operatorname{Ker}\varphi$. Значит, ядро – это двусторонний идеал.

Образ гомоморфизма замкнут относительно суммы, взятия противоположного и произведения. В самом деле $\varphi(a) + \varphi(b) = \varphi(a+b)$, $\varphi(-a) = -\varphi(a)$, $\varphi(a)\varphi(b) = \varphi(ab)$. Значит, образ – подкольцо. □

Определение 9. 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 1 (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) Проверим, что Ψ – гомоморфизм:

$$\Psi((r+\operatorname{Ker}\varphi)+(s+\operatorname{Ker}\varphi)) = \Psi((r+s)+\operatorname{Ker}\varphi) = \\ = \varphi(r+s) = \varphi(r)+\varphi(s) = \Psi(r+\operatorname{Ker}\varphi)+\Psi(s+\operatorname{Ker}\varphi)$$

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

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.

□

Замечание 4. Если в кольце забыть про умножение, то получится абелева группа по сложению. При этом гомоморфизм колец – это гомоморфизм абелевых групп по сложению. Таким образом факторкольцо – это факторгруппа по умножению, что избавляет нас от проверки корректности и от проверки, что Ψ – гомоморфизм по сложению в предыдущей теореме.

Определение 10. Как и в случае групп, если I – двусторонний идеал в кольце R, то гомоморффизм $\pi_I\colon R \to R/I$, $r \mapsto r+I$, называется каноническим гомоморфизмом.

Определение 11. Прямое произведение колец R_1 и R_2 – это кольцо $R_1 \times R_2$, состоящее из множества пар (r_1, r_2), $r_1 \in R_1$, $r_2 \in R_2$ с операциями

$$(r_1,r_2)+(r_1',r_2') = (r_1+r_1', r_2+r_2'), \qquad (r_1,r_2)\cdot(r_1',r_2') = (r_1\cdot r_1', r_2\cdot r_2').$$

В $R_1 \times R_2$ всегда есть делители нуля: $(a,0)\cdot(0,b)=(0,0)$.

Пример 6 (Примеры применения теоремы о гомоморфизме колец.)**. 1.** *Рассмотрим гомоморфизм* $\varphi\colon R_1 \times R_2 \to R_2$, $\varphi(r_1,r_2)=r_2$. *Имеем,* $\operatorname{Ker}\varphi = R_1 \times \{0\}$. *По теореме о гомоморфизме* $(R_1\times R_2)/(R_1\times\{0\}) \cong R_2$.

2. Теорема о факторизации прямого произведения. *Пусть* $R_1,\ldots,R_n$ – *кольца. И в каждом* R_j *фиксирован идеал* I_j. *Тогда*

$$(R_1\times\ldots\times R_n)/(I_1\times\ldots\times I_n) \cong R_1/I_1\times\ldots\times R_n/I_n.$$

Доказательство. *Рассмотрим гомоморфизм* $\varphi\colon R_1\times\ldots\times R_n \to R_1/I_1\times\ldots\times R_n/I_n$, $\varphi(r_1,\ldots,r_n)=(r_1+I_1,\ldots,r_n+I_n)$.

Гомоморфизм φ *сюръективен и* $\operatorname{Ker}\varphi = I_1\times\ldots\times I_n$.

3. *Пусть* F – *поле. Рассмотрим идеал* $(x-c)$ *в кольце* $F[x]$. *Тогда* $F[x]/(x-c)\cong F$. *Для доказательство рассмотрим гомоморфизм* $\varphi\colon F[x]\to F$, $\varphi(f(x))=f(c)$. *Легко видеть, что* $\operatorname{Ker}\varphi=(x-c)$ *и* $\operatorname{Im}\varphi = F$.

4. *Докажем, что* $\mathbb{R}[x]/(x^2+1)\cong\mathbb{C}$. *Для этого рассмотрим гомоморфизм* $\varphi\colon\mathbb{R}[x]\to\mathbb{C}$, *определенный по правилу* $\varphi(f(x))=f(i)$. *Так как образ всех линейных многочленов*

$a+bx$ дает все комплексные числа $a+bi$, гомоморфизм φ сюръективен. Докажем, что $\operatorname{Ker}\varphi$ *совпадает с* (x^2+1). *Пусть* $f(x) \in \operatorname{Ker}\varphi$. *Поделим* $f(x)$ *на* x^2+1 *с остатком. Получим* $f(x) = q(x)(x^2+1)+ax+b$. *Тогда* $0 = \varphi(f(x)) = f(i) = q(i)\cdot 0 + ai + b = ai + b$.

Значит, $a = b = 0$, *то есть* $f(x)$ *делится на* x^2+1.

5. $\mathbb{R}[x]/(x^2-1) \cong \mathbb{R}\times\mathbb{R} \ncong \mathbb{C}$. *Для доказательства надо рассмотреть гомоморфизм* $\varphi\colon \mathbb{R}[x] \to \mathbb{R}\times\mathbb{R}$, $\varphi(f(x)) = (f(1), f(-1))$.