Лекция 12

Определение 1. *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 1. 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 2. 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 1. *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 1. *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 $(M) \subset J$. $\square$

Определение 3. 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 2. *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 $\varphi(ru) =$

$\varphi(r)\varphi(u) = \varphi(r)0 = 0, \qquad \varphi(ur) = 0\varphi(r) = 0$. 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 4. 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 2. 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 5. 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 6. 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 2 (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* $\varphi\colon \mathbb{R}[x] \to \mathbb{R} \times \mathbb{R}$, $\varphi(f(x)) = (f(1), f(-1))$.

Далее переходим к изучению коммутативных ассоциативных колец с единицей. Все кольца далее являются коммутативными ассоциативными и с единицей, не будем писать это для краткости, но будем это предполагать. Так как кольцо коммутативно, понятия левого, правого и двустороннего идеалов совпадают. Будем использовать обозначение $I \lhd R$ для идеала I в кольце R. Напомним, что минимальны идеал, содержащи некоторое подмножество S в кольце R имеет вид

$$(S) = \left\{ \sum_{i=1}^{k} r_i s_i \mid r_i \in R, s_i \in S, k \in \mathbb{N} \right\}.$$

Будем называть данный идеал *идеалом, порожденным* S.

Определение 7. Идеал, порожденный одним элементом, называется *главным*.

Пример 3. *Идеал* (n) *в кольце* $\mathbb{Z}$ *состоит из чисел, делящихся на* n.

Лемма 3. *Идеал в кольце содержащий обратимый элемент совпадает со всем кольцом.*

Доказательство. Пусть $I \lhd R$ – левый идеал некоторого кольца и пусть $a \in I$ – обратимый элемент. Тогда $a^{-1}a = 1 \in I$. Но тогда для любого $r \in R$ имеем $r = r1 \in I$. □

Предложение 1. *Кольцо* R *не имеет нетривиальных (то есть отличных от* $\{0\}$ *и* R*) идеалов тогда и только тогда, когда это поле.*

Доказательство. Пусть R – поле. Тогда любой ненулевой идеал содержит обратимый элемент, и следовательно, совпадает с R.

Пусть теперь R кольцо без нетривиальных идеалов. Рассмотрим $r \neq 0 \in R$. Тогда можно рассмотреть идеал (r). Так как в этом идеале содержится $r \neq 0$, это ненулевой идеал. Значит, $(r) = R$. Тогда $1 \in (r)$, что означает $1 = xr$. □

Определение 8. Кольцо (коммутативное ассоциативное с единицей) называется *областью целостности* или, что то же самое *целостным кольцом*, если в нем нет делителей нуля.

Определение 9. Идеал I в кольце R называется *простым*, если из того, что $ab \in I$ следует, что $a \in I$ или $b \in I$.

Пример 4. *Идеал (n) в кольце $\mathbb{Z}$ является простым тогда и только тогда, когда число n простое.*

Предложение 2. *Факторкольцо R/I не имеет делителей нуля тогда и только тогда, когда I – простой идеал.*

Доказательство. Пусть $a+I$ и $b+I$ – ненулевые смежные классы. Это значит, что $a, b \notin I$. Тогда $(a+I)(b+I) = 0$ равносильно $ab \in I$. Но существование таких a и b, что $a, b \notin I$, а $ab \in I$ равносильно тому, что идеал I не простой. □

Определение 10. Идеал I в кольце R называется *максимальным*, если не существует идеала $J \lhd R$ такого, что $I \subsetneq J \subsetneq R$.

Лемма 4. *Пусть $\psi\colon R \to S$ – гомоморфизм колец. Пусть J – идеал в S. Тогда полный прообраз $\psi^{-1}(J)$ – это идеал в R.*

Доказательство. Пусть $a, b \in \psi^{-1}(J)$. Тогда $\psi(a+b) = \psi(a) + \psi(b) \in J$ и $\psi(-a) = -\psi(a) \in J$, то есть $a+b \in \psi^{-1}(J)$ и $-a \in \psi^{-1}(J)$. Кроме того $\psi(ra) = \psi(r)\psi(a) \in J$, $\psi(ar) = \psi(a)\psi(r) \in J$, то есть $ra, ar \in \psi^{-1}(J)$. □

Лемма 5. *Пусть $\psi\colon R \to S$ – сюръективный гомоморфизм колец. И пусть I – идеал в R. Тогда $\psi(I)$ – идеал в S.*

Доказательство. Пусть $a = \psi(x)$, $b = \psi(y)$, где $x, y \in I$. Тогда $x + y \in I$ и $\psi(x+y) = a + b \in \psi(I)$. И $-a = \psi(-x) \in \psi(I)$. Для любого $s \in S$ имеем $s = \psi(r)$ для некоторого $r \in R$. Тогда $sa = \psi(rx) \in \psi(I)$. □

Теорема 2. *Пусть R – коммутативное кольцо с единицей. Факторкольцо R/I – поле тогда и только тогда, когда I – максимальный идеал.*

Доказательство. Рассмотрим канонический гомоморфизм (колец) $\pi_I\colon R \to R/I$, $\operatorname{Ker}\pi_I = I$. Существование собственного идеала J такого, что $I \subsetneq J \subsetneq R$ равносильно существованию промежуточного идеала $\{0\} \subsetneq L \subsetneq R/I$ такого, что $\pi_I^{-1}(L) = J$. Но существование такого L равносильно тому, что R/I – не поле. □