Лекция 21

Пример 1 (Комплексные представления S_3)**.** $|S_3| = 6 = n_1^2 + \ldots + n_k^2$. *При этом, так как* $|S_3/S_3'| = 2$, *есть два одномерных представления группы* S_3. *Легко видеть, что это тривиальное представление (все переходит в 1) и знаковое (четные перестановки переходят в 1, а нечетные – в* -1*). Получаем, что есть еще ровно одно двумерное неприводимое представление. Мы знаем, что у* S_3 *есть неприводимое представление, полученное из изоморфизма* S_3 *и* D_3.

Заметим, что в S_3 *есть ровно 3 класса сопряженности.*

Пример 2 (Комплексные представления S_4)**.** $|S_4| = 24 = n_1^2 + \ldots + n_k^2$. *При этом* $|S_4/S_4'| = 2$, *и значит, у* S_4 *есть ровно 2 одномерных представления: тривиальное и знаковое. При этом 22 единственным образом раскладывается в сумму квадратов целых чисел* ≥ 2, *а именно* $22 = 2^2 + 3^2 + 3^2$. *Значит, у* S_4 *есть 2 одномерных, одно двумерное и два трехмерных неприводимых комплексных представлений. Двумерное неприводимое представление* S_4 *получается как композиция сюръективного гомоморфизма* $S_4 \to S_3$ *и неприводимого двумерного представления* S_3. *Трехмерные представления получаются из того, что* S_4 *изоморфна группе симметрий правильного тетраэдра и группе вращений куба. Надо проверить, что эти представления неприводимы и не изоморфны.*

Трехмерное представление, если оно приводимо, может разлагаться в прямую сумму либо двумерного и одномерного, либо трех одномерных. Так или иначе должно быть одномерное инвариантное подпространство, то есть собственный вектор общий для всех операторов представления. Можно убедиться непосредственно выписав несколько операторов в некотором базисе, что данные представления неприводимы.

Другой подход к доказательству неприводимости ρ *– это посчитать* (χ_ρ, χ_ρ) *и убедиться, что получится 1. Действительно, если* $\rho = m_1\rho_1 \oplus m_k\rho_k$ *– разложение на неприводимые, то* $(\chi_\rho, \chi_\rho) = \sum m_j^2$. *Для группы симметрий тетраэдра 6 операторов – это симметрии относительно плоскости (след 1), 6 – это зеркальные повороты на* $\frac{\pi}{2}$ *(след 1), восемь – повороты вокгру оси на* $\frac{\pi}{3}$ *(след 0), три – повороты вокгру оси на* π *(след* -1*) и один – тождественное преобразование (след 3). Итого*

$$(\chi_\rho, \chi_\rho) = \frac{1}{24}(6 \cdot 1^2 + 6 \cdot 1^2 + 8 \cdot 0^2 + 3 \cdot (-1)^2 + 1 \cdot 3^2) = 1.$$

Аналогично для куба 6 операторов – вращения на $\frac{\pi}{2}$ *(след 1), 9 операторов – вращения на* π *(след* -1*), 8 операторов – вращения на* $\frac{\pi}{3}$ *(след 0) и один – тождественное преобразование (след 3). Итого*

$$(\chi_\rho, \chi_\rho) = \frac{1}{24}(6 \cdot 1^2 + 9 \cdot (-1)^2 + 8 \cdot 0^2 + 1 \cdot 3^2) = 1.$$

То, что данные представления не изоморфны следует, например, из того, что в представлении, построенном по тетраэдру, определители некоторых операторов равны -1. *Для представления, построенного по кубу, определители всех операторов равны 1. Определитель оператора не меняется при сопряжении, а значит, должен быть одинаков у изоморфных представлений.*

Определение 1. Кольцо – это множество R с двумя бинарными операциями $+$ и $\cdot$ такими, что $(R, +)$ является абелевой группой и $a(b + c) = ab + ac$, $(a + b)c = ac + bc$.

Пример 3. *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. 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 (в кольце с единицей) 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 3. 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 4. *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 4. *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 5. *1)* $\mathrm{Mat}_{n\times n}(F)$ *– алгебра над* F*;*
2) $F[x_1, \ldots, x_n]$ *– алгебра над* F*;*
3) $F[G]$ *– алгебра над* F*;*
4) Если $F \subset K$ *– вложение полей, то* K *– алгебра над* F*. (Например,* $\mathbb{C}$ *– алгебра над* $\mathbb{R}$*);*

5) $\mathbb{H}$ *– 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 5. Алгебра называется *алгеброй с делением*, если любой ненулевой элемент в ней обратим.

Из доказанного выше получаем следующую лемму.

Лемма 2. $\mathbb{H}$ – *алгебра с делением.*

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 $\varphi(r_1r_2) = \varphi(r_1)\varphi(r_2)$.

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 6. *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 3. *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 $u+v = \sum(r_i+r'_i)m_i \in (M)$, $-u = \sum(-r_i)m_i \in M$, $ru = \sum rr_i m_i \in (M)$. 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 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 4. *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 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.

□

Определение 10. 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 $(r_1, r_2) + (r_1', r_2') = (r_1 + r_1', r_2 + r_2')$, $(r_1, r_2) \cdot (r_1', r_2') = (r_1 \cdot r_1', r_2 \cdot r_2')$.

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

Пример 7 (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. $\mathbb{R}[x]/(x^2-1) \cong \mathbb{R} \oplus \mathbb{R} \ncong \mathbb{C}$. *Для доказательства надо рассмотреть гомоморфизм* $\varphi\colon \mathbb{R}[x] \to \mathbb{R} \oplus \mathbb{R}$, $\varphi(f(x)) = (f(1), f(-1))$.

Теорема 2. *Пусть* F *– поле. Кольцо* $F[x]/(f)$ *является полем тогда и только тогда, когда многочлен* f *неприводим.*

Доказательство. Ясно, что $F[x]/(f)$ – коммутативное ассоциативное кольцо с единицей.

Если $f(x) = g(x)h(x)$, где $g(x)$ и $h(x)$ меньшей степни, то $g + (f) \neq 0 + (f)$, $h + (f) \neq 0 + (f)$, но $(g + (f)) \cdot (h + (f)) = 0 + (f)$. То есть в факторкольце есть делители нуля. Значит, это не поле.

Пусть теперь f неприводим и $g(x)$ не делится на $f(x)$, что эквивалентно тому, что $g(x) + (f(x)) \neq 0$. Найдем обратный к элементу $g + (f)$. Заметим, что НОД$(f, g) = 1$. Следовательно, существуют $u(x)$ и $v(x)$ такие, что $u(x)f(x) + v(x)g(x) = 1$. В факторкольце имеем $(u + (f))(f + (f)) + (v + (f))(g + (f)) = 1 + (f)$. Но $f + (f) = 0 + (f)$. Отсюда $(v + (f))(g + (f)) = 1 + (f)$. $\square$