# Лекция 20.

Гайфуллин Сергей Александрович

МГУ

8 декаря, 2020

## Определение.

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: $(a, 0) \cdot (0, b) = (0, 0)$.

## 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 $\varphi$ сюръективен и $\operatorname{Ker}\varphi = I_1 \times \ldots \times I_n$.

## Примеры применения теоремы о гомоморфизме колец.

**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 $\varphi$ 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.** 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 $g(x) + (f(x)) \neq 0$. 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 $(v + (f))(g + (f)) = 1 + (f)$.

Заметим, что $F[x]/(f)$ – алгебра над $F$.

**Лемма.** Базис этой алгебры $\{1+(f), x+(f), \ldots, x^{n-1}+(f)\}$, где $n = \deg f$.

**Доказательство.** Пусть $g(x) \in F[x]$. Поделим $g$ на $f$ с остатком: $g(x) = q(x)f(x) + r(x)$. Тогда $g + (f) = r + (f)$. Но $\deg\ r(x) \leq n-1$. Значит, $r(x)$ является линейной комбинацией $1, x, \ldots, x^{n-1}$. Мы доказали, что $\{1+(f), x+(f), \ldots, x^{n-1}+(f)\}$ – полная система.
Докажем линейную независимость. Пусть $\sum_{i=0}^{n-1} \alpha_i(x^i + (f)) = 0$. Положим $h(x) = \sum_{i=0}^{n-1} \alpha_i x^i$. Тогда $h + (f) = 0 + (f)$. Это значит, что $h \in (f)$, то есть $h$ делится на $f$, чего не может быть, так как $\deg\ h(x) < \deg\ f(x)$.

Если мы имеем алгебру $A$ размерности $n$ над полем $\mathbb{Z}_p$, то $|A| = p^n$. В самом деле, пусть $\{e_1, \ldots, e_n\}$ – базис $A$. Тогда $A = \{\lambda_1 e_1 + \ldots + \lambda_n e_n \mid \lambda_i \in \mathbb{Z}_p\}$. Каждый коэффициент $\lambda_i$ принимает $p$ значений. Значит, всего $p^n$ вариантов.

## Пример.

Рассмотрим многочлен $f(x) = x^2 + x + 1$ в кольце $\mathbb{Z}_2[x]$. Проверим, что у $f(x)$ нет корней в $\mathbb{Z}_2$. Действительно, $f(0) = 1$, $f(1) = 1$. Так как $f$ – многочлен второй степени и у него нет корней, он неприводим. Значит, кольцо $\mathbb{Z}_2[x]/(x^2 + x + 1)$ является полем из 4 элементов. Построим таблицы сложения и умножения.

| + | 0 | 1 | x | x+1 |
|---|---|---|---|---|
| 0 | 0 | 1 | x | x+1 |
| 1 | 1 | 0 | x+1 | x |
| x | x | x+1 | 0 | 1 |
| x+1 | x+1 | x | 1 | 0 |

| · | 0 | 1 | x | x+1 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | x | x+1 |
| x | 0 | x | **x+1** | **1** |
| x+1 | 0 | x+1 | **1** | **x** |

Например, $(x + (f)) \cdot (x + (f)) = x^2 + (f) = x + 1 + (f)$.

**Определение.**

Кольцо $R$ называется *простым*, если в $R$ нет других (двусторонних) идеалов, кроме $\{0\}$ и $R$.

**Теорема.** Кольцо квадратных матриц $n \times n$ над полем является простым.

**Доказательство.** Пусть $I$ – ненулевой идеал в кольце матриц. Возьмем $A \neq 0 \in I$. Тогда найдутся $i$ и $j$ такие, что $a_{ij} \neq 0$. Рассмотрим $E_{ki}AE_{jl} = B \in I$. Несложно видеть, что $B = a_{ij}E_{kl}$. Так как $a_{ij} \neq 0$, получаем, $E_{kl} \in I$. Но так как числа $k$ и $l$ произвольные, все матричные единицы лежат в $I$. Но тогда для любой матрицы $X$ имеем $X = \sum x_{ij}E_{ij} \in I$.

Заметим, что нетривиальные односторонние (например, левые) идеалы к кольце матриц есть. Например, множество матриц, у которых первый столбец нулевой, является левым идеалом.

**Задача.**

Опишите все левые и правые идеалы в кольце матриц.

**Лемма.** Левый (правый) идеал в кольце с единицей, содержащий обратимый элемент совпадает со всем кольцом.

**Доказательство.** Пусть $I \triangleleft R$ – 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.** Коммутативное (ассоциативное) кольцо с единицей является простым 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 $R$ – простое коммутативное кольцо. 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.**

Коммутативное кольцо с единицей называется *областью цеелостности* или, что то же самое *целостным кольцом*, если в нем нет делителей нуля.

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

**Пример.**

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

**Предложение.** 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.**

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

**Лемма.** 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.** 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.** 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.

## Определение.

Пусть $R$ – область целостности, не являющаяся полем. Тогда $R$ называется евклидовым кольцом, если задана функция (евклидова норма) $N\colon R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ такая, что
1) $N(ab) \geq N(a)$ для любых $a, b \in R \setminus \{0\}$
2) для любых $a, b \in R$, $b \neq 0$ возможно "деление с остатком то есть существуют такие $q, r \in R$, что $a = bq + r$, причем либо $N(r) < N(b)$, либо $r = 0$.

## Примеры.

1) $R = \mathbb{Z}$, $N(a) = |a|$.
2) $R = F[x]$, $N(f) = \deg f$.
3) **Задача.** Докажите, что $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ – евклидово кольцо с нормой $N(z) = |z|$.
4) **Задача.** Для каких $c \in \mathbb{R}$ кольцо $\mathbb{Z}[ci] = \{a + bci \mid a, b \in \mathbb{Z}\}$ является евклидовым кольцом с нормой $N(z) = |z|$?

**Определение.**

Коммутативное кольцо $R$ с единицей назовем кольцом главных идеалов, если любой идеал в нем главный, то есть равен $(r)$ для некоторого $r \in R$.

**Пример.**

Идеал $(x, y)$ в $F[x, y]$ не является главным.

**Теорема.**

Евсклидово кольцо является кольцом главных идеалов.