4. Четвертая лекция, 27 сентября 2021 г.

4.1. **Факторкольца.** Ранее мы рассматривали конструкцию кольца вычетов $\mathbb{Z}/m\mathbb{Z}$. Сейчас мы введем ее обобщение: факторкольцо по идеалу.

Пусть A — произвольное коммутативное кольцо, $I \subset A$ — идеал. Определим на множестве элементов из A следующее отношение: будем говорить, что $x \equiv y \mod I$, если $x - y \in I$. Ясно, что это отношение эквивалентности. Классы эквивалентности — это множества вида $x + I = \{x + a \mid a \in I\}$. Иногда мы также будем обозначать класс $x + I$ через $[x]$. Обозначим множество этих классов через A/I.

На классах эквивалентности из A/I можно определить операции сложения и умножения:

$$(x + I) + (y + I) = (x + y) + I; \qquad (x + I)(y + I) = xy + I.$$

Предложение 4.1. *Заданные таким образом операции определены корректно, т.е. сумма и произведение классов не зависят от выбора их представителей.*

Доказательство. Проверим корректность умножения: пусть $x \equiv x' \mod I$ и $y \equiv y' \mod I$. Тогда $x' = x' + a$, $y' = y + b$, где $a, b \in I$. Поэтому

$$x'y' = (x + a)(y + b) = xy + ay + xb + ab \equiv xy \mod I,$$

поскольку ay, xb и ab лежат в I. Корректность сложения проверяется аналогично. $\square$

Таким образом, на A/I вводятся операции сложения и умножения, что задаёт на нём структуру кольца. Полученное кольцо называется *факторкольцом* кольца A по идеалу I.

Ясно, что нулём и единицей в A/I являются $0 + I$ и $1 + I$ соответственно.

Упражнение 4.2. Докажите утверждение, обратное к предыдущему предложению: пусть $I \subset A$ — абелева подгруппа по сложению, причем операция умножения, заданная на классах эквивалентности из A/I, определена корректно. Покажите, что I — идеал в A.

4.2. **Гомоморфизмы.**

Определение 4.3. Пусть A, B — два произвольных кольца. Отображение $f\colon A \to B$ называется *гомоморфизмом*, если оно сохраняет операции: а именно,

$$f(x + y) = f(x) + f(y), \qquad f(xy) = f(x)f(y).$$

Пусть A, B — два произвольных кольца. Отображение $f\colon A \to B$ называется *гомоморфизмом*, если оно сохраняет операции: а именно,

$$f(x + y) = f(x) + f(y), \qquad f(xy) = f(x)f(y).$$

Замечание 4.4. В определении мы *не требуем*, чтобы единица переходила в единицу. Так, например, вложение $A \to A \oplus A$, $a \mapsto (a, 0)$ — гомоморфизм, хотя единицу в единицу он не переводит.

Упражнение 4.5. Докажите, что $\operatorname{Im} f \subset B$ — подкольцо в B, а $\operatorname{Ker} f \subset A$ — идеал в A.

Говорят, что гомоморфизм инъективен/сюръективен/биективен, если он инъективен/сюръективен/биективен как отображение множеств. Такие гомоморфизмы ещё называют соответственно *мономорфизмами*, *эпиморфизмами* и *изоморфизмами*.

Несложно доказать следующее предложение.

Предложение 4.6. *Гомоморфизм* $f\colon A \to B$ *является мономорфизмом тогда и только тогда, когда* $\operatorname{Ker} f = \{0\}$.

Доказательство. Часть «только тогда» очевидна. Часть «тогда» требует некоторой проверки: пусть $f(a) = f(a')$; тогда $f(a-a') = f(a) - f(a') = 0$, то есть $a - a' \in \operatorname{Ker} f$. Если $\operatorname{Ker} f = 0$, это даёт равенство $a = a'$, то есть a — мономорфизм. □

Пример 4.7. Важный пример гомоморфизма — отображение факторизации $\pi\colon A \to A/I$, $\pi(a) = a+I$, где I — произвольный идеал в кольце A. Ясно, что π — эпиморфизм.

Следующая теорема утверждает, что всякий эпиморфизм является отображением факторизации по некоторому идеалу. Аналог этой теоремы для факторпространств уже разбирался ранее в курсе линейной алгебры и геометрии.

Теорема 4.8 (о гомоморфизме колец)**.** *Пусть* $f\colon A \to B$ *— гомоморфизм колец. Тогда* $\operatorname{Im} f \simeq A/\operatorname{Ker} f$. *Более точно, отображение* $\varphi\colon\ \operatorname{Im} f \to A/\operatorname{Ker} f$, *при котором* $b = f(a) \in \operatorname{Im} f$ *отображается в* $\pi(a) = a + \operatorname{Ker} f$, *есть изоморфизм.*

Доказательство. Во-первых, отображение φ определено корректно, т.е. не зависит от выбора элемента a в слое над b. Действительно, если $b = f(a) = f(a')$, то $a - a' \in \operatorname{Ker} f$, т.е. $\pi(a) = \pi(a')$.

Во-вторых, φ — инъективное отображение: если $\varphi(b) = \varphi(b')$, и $b = f(a)$, $b' = f(a')$, мы получаем, что $a \equiv a' \mod \operatorname{Ker} f$, то есть $f(a) = f(a')$. То, что φ — сюръекция, следует из того, что π — сюръекция и $\pi = \varphi \circ f$. Значит, φ является биекцией (множеств).

Осталось проверить, что φ сохраняет сложение и умножение. Выполним вторую проверку (первая выполняется аналогично). Пусть $f(x) = u$, $f(y) = v$. Тогда $f(xy) = uv$, и

$$\varphi(uv) = \pi(xy) = \pi(x)\pi(y) = \varphi(u)\varphi(v),$$

что и требовалось. □

Пример 4.9. Рассмотрим отображение

$$\varphi\colon \mathbb{K}[x] \to \mathbb{K}, \qquad f(x) \mapsto f(a)$$

вычисления значения многочлена в точке a. Ясно, что это гомоморфизм, причём сюръективный (значение многочлена в данной точке может быть любым). При этом по теореме Безу ядро φ есть

$$\operatorname{Ker}\varphi = \{f \in \mathbb{K}[x] \mid f(a) = 0\} = (x-a).$$

Значит, $\mathbb{K}[x]/(x-a) \cong \mathbb{K}$.

Пример 4.10. Рассмотрим теперь отображение вычисления значения *вещественного* многочлена в точке i:

$$\mathbb{R}[x] \to \mathbb{C}, \qquad f(x) \mapsto f(i).$$

Это гомоморфизм, причем также сюръективный (проверьте это!). Кроме того, если $f(i) = 0$, то $f(-i) = f(\bar{i}) = \overline{f(i)} = 0$, поэтому $f(x) \vdots (x-i)(x+i) = x^2+1$. Значит,

$$\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}.$$

4.3. **Китайская теорема об остатках.** Сначала определим прямую сумму колец.

Определение 4.11. *Прямая сумма* $A \oplus B$ колец A и B — это кольцо, элеменами которого являются пары (a, b), где $a \in A$, $b \in B$, а сложение и умножение задаются покомпонентно.

Заметим, что подкольца $\{(a, 0)\} \cong A$ и $\{(0, b)\} \cong B$ являются идеалами в $A \oplus B$.

Вернёмся к кольцам главных идеалов. В них также имеет место аналог китайской теоремы об остатках, который очень просто формулируется и доказывается с помощью понятия факторкольца.

Теорема 4.12 (Китайская теорема об остатках)**.** *Пусть A — кольцо главных идеалов, элементы $u, v \in A$ взаимно просты. Тогда*

$$A/(uv) \simeq A/(u) \oplus A/(v).$$

Доказательство. Поскольку u и v взаимно просты, через них можно линейно выразить единицу:

$$1 = au + bv.$$

Рассмотрим гомоморфизм

$$f\colon A \to A/(u) \oplus A/(v), \qquad f(x) = (x + (u), x + (v)).$$

Тогда $f(bv) = f(1 - au) = (1, 0)$, $f(au) = f(1 - bv) = (0, 1)$. Следовательно, гомоморфизм f сюръективен. Очевидно, что его ядро — это идеал (uv). Поэтому требуемое утверждение следует из теоремы о гомоморфизме колец. □

Упражнение 4.13. Чему изоморфно факторкольцо $\mathbb{R}[x]/(x^2 + px + q)$? (ответ зависит от знака дискриминанта квадратного трёхчлена).