

12. Двенадцатая лекция, 28 февраля 2019 г.

12.1. Факторкольца. Ранее мы рассматривали конструкцию факторгруппы по нормальной подгруппе. Для колец есть её непосредственный аналог: факторкольцо по идеалу.

Пусть A — произвольное коммутативное кольцо, $I \subset A$ — идеал. Определим на множестве элементов из A следующее отношение: будем говорить, что $x \equiv y \pmod I$, 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:

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

ПРЕДЛОЖЕНИЕ 12.1. *Заданные таким образом операции определены корректно, т.е. сумма и произведение классов не зависят от выбора их представителей.*

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

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

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 12.2. 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 .

12.2. Гомоморфизмы.

ОПРЕДЕЛЕНИЕ 12.3. Пусть A, B — два произвольных кольца. Отображение $f: A \rightarrow B$ называется *гомоморфизмом*, если оно сохраняет операции: а именно,

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

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

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

ЗАМЕЧАНИЕ 12.4. В определении мы *не требуем*, чтобы единица переходила в единицу. Так, например, вложение $A \rightarrow A \oplus A$, $a \mapsto (a, 0)$ — гомоморфизм, хотя единицу в единицу он не переводит.

УПРАЖНЕНИЕ 12.5. Докажите, что $\text{Im } f \subset B$ — подкольцо в B , а $\text{Ker } f \subset A$ — 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*.

ПРИМЕР 12.6. Важный пример гомоморфизма — отображение факторизации $\pi: A \rightarrow A/I$, $\pi(a) = a + I$, где I — произвольный идеал в кольце A . Ясно, что π — эпиморфизм.

Следующая теорема утверждает, что всякий эпиморфизм является отображением факторизации по некоторому идеалу. Аналоги этой теоремы для факторгрупп и факторпространств уже разбирались ранее.

ТЕОРЕМА 12.7 (о гомоморфизме колец). Пусть $f: A \rightarrow B$ — гомоморфизм колец. Тогда $\text{Im } f \simeq A/\text{Ker } f$. Более точно, отображение $\varphi: \text{Im } f \rightarrow A/\text{Ker } f$, при котором $b = f(a) \in \text{Im } f$ отображается в $\pi(a) = a + \text{Ker } f$, есть изоморфизм.

ДОКАЗАТЕЛЬСТВО. Из теоремы о гомоморфизме групп следует, что отображение φ является изоморфизмом абелевых групп. Осталось проверить, что оно сохраняет умножение. Действительно, 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. $\square$

ПРИМЕР 12.8. Рассмотрим отображение

$$\varphi: \mathbb{K}[x] \rightarrow \mathbb{K}, \quad f(x) \mapsto f(a)$$

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

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

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

ПРИМЕР 12.9. Рассмотрим теперь отображение вычисления значения *вещественного* многочлена в точке i :

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

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

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

УПРАЖНЕНИЕ 12.10. Чему изоморфно факторкольцо $\mathbb{R}[x]/(x^2 + px + q)$? (ответ зависит от знака дискриминанта квадратного трёхчлена).

12.3. Китайская теорема об остатках. Сначала напомним понятие прямой суммы колец.

ОПРЕДЕЛЕНИЕ 12.11. *Прямая сумма* $A \oplus B$ колец A и B — это кольцо, элементами 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 12.12 (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

$$f: A \rightarrow A/(u) \oplus A/(v), \quad f(x) = (x + (u), x + (v)).$$

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. $\square$

12.4. Максимальные и простые идеалы.

ОПРЕДЕЛЕНИЕ 12.13. Идеал $\mathfrak{m} \subset A$ называется максимальным, если он не содержится ни в каком большем идеале (не совпадающем со всем кольцом).

ОПРЕДЕЛЕНИЕ 12.14. Идеал $\mathfrak{p} \subset A$ называется простым, если для любых двух элементов $a, b \in A$, таких, что $ab \in \mathfrak{p}$, верно, что либо $a \in \mathfrak{p}$, либо $b \in \mathfrak{p}$.

ПРИМЕР 12.15. Простые идеалы в $\mathbb{Z}$ — это идеалы вида (p) , где p простое. Они же являются и максимальными (проверьте это!).

ПРЕДЛОЖЕНИЕ 12.16. 1) Идеал $\mathfrak{p}$ прост тогда и только тогда, когда $A/\mathfrak{p}$ — область целостности.

2) Идеал $\mathfrak{m}$ максимален тогда и только тогда, когда $A/\mathfrak{m}$ — поле.

ДОКАЗАТЕЛЬСТВО. 1) Пусть $\mathfrak{p}$ прост, $ab \in \mathfrak{p}$. Значит, a или b лежат в $\mathfrak{p}$. Рассмотрим их образы при отображении факторизации $A \rightarrow A/\mathfrak{p}$. Получим, что из $[ab] = [0]$ следует, что $[a] = [0]$ или $[b] = [0]$, что и означает, что $A/\mathfrak{p}$ целостное. Обратное утверждение доказывается точно так же.

2) Пусть $\mathfrak{m}$ максимален. Докажем, что всякий ненулевой элемент $[a] \in A/\mathfrak{m}$ обратим. Действительно, $a \notin \mathfrak{m}$. Рассмотрим идеал $a + \mathfrak{m} = \{ax + m \mid x \in A, m \in \mathfrak{m}\}$. Этот идеал содержит $\mathfrak{m}$ и не совпадает с ним (поскольку содержит ещё и a), значит, он совпадает со всем кольцом. Поэтому $1 = ax + m$ для некоторых $x \in A, m \in \mathfrak{m}$. Получаем, что в $A/\mathfrak{m}$ элемент $[x]$ есть $[a]^{-1}$, так как $[1] = [a][x] + [m] = [a][x]$. Обратное утверждение доказывается аналогично (проделайте это!). $\square$

СЛЕДСТВИЕ 12.17. Всякий максимальный идеал прост.

УПРАЖНЕНИЕ 12.18. Приведите пример простого, но не максимального идеала.

Оказывается, что в кольцах главных идеалов верно и обратное к следствию 12.17. Это вытекает из следующей теоремы.

ТЕОРЕМА 12.19. Пусть A — кольцо главных идеалов, $u \in A$ — необратимый элемент. Тогда $A/(u)$ является полем тогда и только тогда, когда u неприводим.

ДОКАЗАТЕЛЬСТВО. Пусть u приводим: $u = vw$, где v и w необратимы. Тогда в $A/(u)$ получаем: $[v][w] = [u] = [0]$, причём $[v] \neq [0]$ и $[w] \neq [0]$ — значит, $A/(u)$ не область целостности, и тем более не поле.

Обратно, пусть u неприводим. Это значит, что для любого $x \notin (u)$ верно, что $(x, u) = 1$, следовательно, найдутся a и b , для которых $ax + bu = 1$. Значит, в $A/(u)$ получаем, что $[a][x] = [1]$, т.е. $[a]$ обратим. $\square$

12.5. Простота и неприводимость. Можно определить понятие простого элемента в кольце:

ОПРЕДЕЛЕНИЕ 12.20. Элемент $p \in A$ называется *простым*, если порожденный им главный идеал $(p) \subset A$ прост.

Ясно, что из простоты следует неприводимость. Также из теоремы ?? получается, что в кольцах главных идеалов простота эквивалентна неприводимости. Однако в общем случае это может быть неверно:

ПРИМЕР 12.21. Рассмотрим кольцо $\mathbb{Z}[\sqrt{-5}]$. Оно не факториально. Например, элемент 6 имеет два различных разложения на неприводимые:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Поэтому элемент 2 будет неприводимым, но не простым: 2 нельзя представить как произведение двух не ассоциированных с ним элементов, а кратный ему элемент 6 (лежащий в идеале (2)) — можно.

УПРАЖНЕНИЕ 12.22. Докажите, что в факториальном кольце всякий неприводимый элемент прост.

E-mail address: esmirnov@hse.ru