

4. ЧЕТВЕРТАЯ ЛЕКЦИЯ, 27 СЕНТЯБРЯ 2022 Г.

4.1. Делимость в кольцах главных идеалов. В этом разделе A — кольцо главных идеалов.

Дадим определение наибольшего общего делителя двух элементов. Привычное определение 1.2 здесь уже не работает, т.к. в произвольном кольце непонятно, что такое «наибольший». Поэтому придётся обобщать определение 1.3.

Определение 4.1. Пусть $a, b \in A$. *Наибольшим общим делителем* элементов a, b (обозначение: (a, b)) называется такой элемент d , что $d \mid a$ и $d \mid b$, и при этом d делится на *любой другой* общий делитель элементов a и b .

При таком определении а priori неясно, что НОД двух элементов вообще существует. Однако это несложно доказать.

Предложение 4.2. В кольце главных идеалов у любых двух элементов $a, b \in A$ существует наибольший общий делитель, который выражается через них в виде $d = ax + by$.

Доказательство. Рассмотрим идеал $(a, b) \subset A$. Он главный; пусть он порождён элементом d . Это значит, что $d = ax + by$. Докажем, что d — НОД элементов a и b . Действительно, поскольку $a, b \in (a, b) = (d)$, оба этих элемента делятся на d . Пусть e — какой-то другой общий делитель a и b . Поскольку $e \mid a$ и $e \mid b$, получаем, что $e \mid ax + by = d$, что и требовалось. $\square$

Определение 4.3. Если $(a, b) = 1$, то a и b называются *взаимно простыми*.

4.2. Существование и единственность разложения на простые. Введем понятие *ассоциированных* элементов. Два элемента a и b называются ассоциированными (обозначение: $a \sim b$), если $a = bs$, где s обратим. Иными словами, элементы a и b ассоциированы, если идеалы (a) и (b) совпадают.

Простое число — это такое число, которое делится на единицу и на себя. Обобщим это понятие на произвольные кольца.

Определение 4.4. Необратимый ненулевой элемент p кольца A называется *простым*, если его нельзя представить в виде $p = ab$, где a и b — необратимые элементы. Иными словами, всякий делитель простого элемента p ассоциирован либо с 1, либо с p .

Замечание 4.5. Простые элементы в кольце многочленов обычно называют *неприводимыми*.

Наша ближайшая цель — доказать существование и единственность разложения элемента в произведение простых в кольцах главных идеалов. Сначала докажем следующую лемму.

Лемма 4.6. Пусть A — кольцо главных идеалов, элемент p прост, и $p \mid a_1 \dots a_n$. Тогда $p \mid a_i$ при некотором i .

Доказательство. Сначала докажем лемму при $n = 2$. Пусть $p \mid ab$. Допустим, что $p \nmid a$; покажем, что $p \mid b$. Действительно, если p не делит a , то p и a взаимно просты. Напишем линейное выражение их НОДа:

$$1 = px + ay.$$

Домножим обе части равенства на b :

$$b = pbx + aby.$$

Правая часть делится на p , так как ab делится на p . Значит, b делится на p .

Случай произвольного n доказывается индукцией по числу сомножителей. $\square$

Отсюда следует единственность разложения элемента кольца главных идеалов на простые множители (с точностью до ассоциированности) — аналог основной теоремы арифметики. Доказательство в этом случае также почти не отличается от случая кольца целых чисел.

Теорема 4.7. Пусть A — кольцо главных идеалов, $a \in A$ — необратимый элемент, причём

$$a = p_1 \dots p_n = q_1 \dots q_m,$$

где p_i, q_i простые. Тогда $n = m$, причём $q_1, \dots, q_m$ можно перенумеровать так, что каждый из q_i станет ассоциированным с соответствующим p_i .

Доказательство. Пусть $n \leq m$. Докажем теорему индукцией по n . База: при $n = 1$ доказывать нечего.

Переход. Поскольку $p_1 \mid q_1 \dots q_m$, в силу предыдущей леммы p_1 делит некоторый q_i . Без ограничения общности будем считать, что $i = 1$. Поскольку q_1 также прост, получаем, что $p_1 \tilde{q}_1$. Стало быть, обе части равенства $p_1 \dots p_n = q_1 \dots q_m$ можно сократить на p_1 и получить равенство $p_2 \dots p_n = sq_2 \dots q_m$, где s обратим. Мы свели теорему к случаю $n - 1$ сомножителя, а для него она верна по предположению индукции. $\square$

Теперь докажем существование разложения элемента в произведение простых. Это утверждение, которое в $\mathbb{Z}$ очевидно, в случае произвольного кольца главных идеалов приходится доказывать. Кроме того, бывают кольца (не являющиеся кольцами главных идеалов), в которых разложения элемента в произведение простых не существует.

Теорема 4.8. В кольце главных идеалов каждый ненулевой необратимый элемент может быть разложен на простые множители.

Доказательство. Пусть это не так, и существуют элементы, которые не раскладываются в произведение простых. Назовём их *плохими*. Пусть a_0 — плохой элемент. Тогда он раскладывается в произведение двух необратимых элементов (иначе он был бы простым), причём хотя бы один из сомножителей обязан также быть плохим. Пусть $a_0 = a_1 b_1$, и a_1 плохой. То же самое верно про a_1 : он раскладывается в произведение $a_2 b_2$, где a_2 плохой, и так далее до бесконечности. Мы получили бесконечный ряд элементов

$$a_0, a_1, \dots, a_n, \dots,$$

где $a_i \mid a_{i-1}$. Поэтому имеет место бесконечная строго возрастающая цепочка идеалов

$$(a_0) \subset (a_1) \subset \dots \subset (a_n) \subset \dots$$

Докажем, что в кольце главных идеалов такой цепочки быть не может. Рассмотрим объединение всех идеалов цепочки: $I = \bigcup_{i=0}^{\infty} (a_i)$. Это тоже идеал (почему?). Пусть $I = (d)$ (ведь A — кольцо главных идеалов!). Тогда элемент d лежит в каком-то из (a_n) для некоторого n . Стало быть, $(a_n) = (a_{n+1}) = I$ — противоречие с тем, что цепочка строго возрастает. Стало быть, всякий элемент разлагается на простые множители. $\square$

Замечание 4.9. Это же рассуждение проходит для существенно более широкого класса колец: так называемых *нётеровых колец*, в которых каждый идеал конечно порождён. Поэтому в нётеровых кольцах имеет место существование разложения в произведение простых — а вот единственности там может и не быть.

Определение 4.10. Целостное кольцо, в котором каждый ненулевой необратимый элемент разлагается в произведение простых, причём единственным (в смысле теоремы 4.8) образом, называется *факториальным*.

Это определение позволяет объединить теоремы 4.8 и 4.7:

Теорема 4.11. *Всякое кольцо главных идеалов факториально.*

4.3. 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 $x \equiv y \pmod I$, 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 4.12. *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 4.13. 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 .

4.4. Гомоморфизмы.

Определение 4.14. 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 4.15. 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 4.16. 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*.

Несложно доказать следующее предложение.

Предложение 4.17. *Гомоморфизм $f: A \rightarrow B$ является мономорфизмом тогда и только тогда, когда $\text{Ker } f = \{0\}$.*

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 $a - a' \in \text{Ker } f$. Если $\text{Ker } f = 0$, это даёт равенство $a = a'$, то есть a — мономорфизм. $\square$

Пример 4.18. 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. Аналог этой теоремы для факторпространств уже разбирался ранее в курсе линейной алгебры и геометрии.

Теорема 4.19 (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. 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 $a - a' \in \text{Ker } f$, 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 $a \equiv a' \pmod{\text{Ker } f}$, 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. $\square$

Пример 4.20. 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 4.21. Рассмотрим теперь отображение вычисления значения *вещественного* многочлена в точке i :

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

Это гомоморфизм, причём 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,

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