1 Идеалы и факторкольца

Определение 1. *Подкольцом* K кольца R называется подмножество, замкнутое относительно сложения и умножения.

Пример 1. Подкольцом кольца целых чисел служат, например, чётные числа, поскольку сумма и произведение чётных чётно.

Пример 2. В кольце многочленов $\mathbb{R}[x]$ можно рассмотреть все многочлены без свободного члена: $a_n x^n + ... + a_1 x$. Проверьте, если вам не очевидно, что это множество является подкольцом в $\mathbb{R}[x]$.

Пример 3. Также в кольце многочленов $\mathbb{R}[x]$ можно рассмотреть все многочлены по модулю многочлена x^n. Это множество будет состоять, очевидно, из всех многочленов степени не выше $n-1$. Проверьте, если вам не очевидно, что это тоже подкольцо. Оно обозначается $\mathbb{R}[x]/x^n$.

Напомним, как строится кольцо вычетов $\mathbb{Z}_n$. Жило-было государство целых чисел $\mathbb{Z}$. Для заданного числа n можно разделить жителей этого государства на n различных народностей. Чтобы понять, к какой народности относится тот или иной житель a нужно его представить в виде $a = r + (n)$, где в слагаемое (n) входит наибольший натуральный кусок, делящийся на n, то бишь остаток при делении a на n. Таким образом, на государство целых чисел мы можем смотреть по модулю добавления кратных n, т. е. как на $\mathbb{Z}/n\mathbb{Z}$.

Обобщая конструкцию кольца вычетов $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ и последний пример, можно рассмотреть отношения эквивалентности, согласованные с операциями, в абстрактных кольцах. Пусть $I \subset A$ — подкольцо кольца A. Мы хотим соорудить множество

$$A/I = \{a + (I) | a \in A\},$$

состоящее из классов эквивалентности по модулю элементов подкольца I, причём так, чтобы это множество само являлось кольцом, а не абы чем! Для каждого элемента $a + (I)$ множества A/I элемент a называется представителем элемента $a + (I)$. Представители определены неоднозначно, с точностью до прибавления элементов подкольца I.

Стало быть, чтобы A/I было корректным кольцом, нам нужно следить, чтобы результат операций над элементами множества A/I не зависел от выбора представителей — когда мы складываем и умножаем вычеты, например, по модулю 5 (остатки) нам ведь не важно, сложим (или умножим) мы 3 и 4 или 18 и (-6), ведь результат будет одинаков по модулю прибавления чисел, кратных 5.

Посмотрим, для каких I результат не будет зависеть от выбора представителей. Пусть $a \equiv a' (\mathrm{mod}\ I)$ и $b \equiv b' (\mathrm{mod}\ I)$ — это означает, как и с числами, что $a' = a + u$ и $b' = b + v$, где $u, v \in I$, т. е. элементы a и a' представляют элемент $a + (I)$, а элементы b и b' представляют элемент $b + (I)$. Теперь запишем сумму элементов $a' + b'$:

$$a' + b' = (a + u) + (b + v) = (a + b) + (u + v),$$

т. к. относительно сложения кольцо коммутативно. И вот, мы видим, что результат по модулю прибавления элементов из множества I одинаков — не зависит от представителей факторцольца для любого I. Затем запишем умножение:

$$a'b' = (a + u)(b + v) = ab + av + ub + uv.$$

Здесь мы уже видим, что ответ отличается от $ab + uv$ на слагаемое $av + ub$, которое, вообще говоря, не обязано лежать в I. Но мы можем потребовать, чтобы это было так, сказав, что $aI \subset I$ и $Ia \subset I$ для любого $a \in A$. В этом случае $av \in I$ и $ub \in I$, и значит, их сумма тоже лежит в I, т. е.

$$ab + av + ub + uv = ab + (I),$$

и произведение в A/I не зависит от представителей.

Определение 2. Подкольцо I кольца A называется *идеалом* (двусторонним), если для любого элемента $a \in A$ выполнены включения $aI \subset I$ и $Ia \subset I$. То есть идеалы — это засасывающие множества по умножению в кольце: если вы умножились на элемент идеала, то вас засосало в идеал.

Пример 4. В любом кольце идеалом является, очевидно, множество, состоящее из одного нуля, а также множество, совпадающее со всем кольцом — это тривиальные идеалы. Факторкольцо по нулевому идеалу — это оно же и будет. А фактор кольца по нему самому — это нуль.

Пример 5. В кольце целых чисел множества $n\mathbb{Z}$ (все кратные n числа) — идеал. Факторкольцом $\mathbb{Z}/n\mathbb{Z}$ будет кольцо остатков по модулю n, обозначаемое символом $\mathbb{Z}_n$.

Пример 6. В кольце многочленов $\mathbb{R}[x]$ рассмотрим множество многочленов, обозначаемое (P), делящихся на фиксированный многочлен P. Легко понять, что (P) — идеал, и можно рассмотреть факторкольцо $\mathbb{R}[x]/(P)$, состоящее из многочленов с точностью до бования кратных P многочленов.

Задача 1. Докажите, что в поле нет нетривиальных (т. е. отличных от нуля и всего поля) идеалов.

Определение 3. Отображение колец $f : A \to B$ называется *гомоморфизмом*, если оно «уважает» сложение и умножение, т. е.

$$f(a + b) = f(a) + f(b),$$

$$f(ab) = f(a)f(b).$$

Задача 2. Пусть есть гомоморфизм колец $f : A \to B$. Назовём множество $\mathrm{Ker} f = \{a \in A | f(a) = 0\}$ *ядром* этого гомоморфизма. Докажите, что $\mathrm{Ker} f$ — идеал кольца A.

Задача 3. Пусть есть гомоморфизм колец $f : A \to B$. Назовём множество $\mathrm{Im} f = \{b \in B | \text{существует } a \in A : f(a) = b\}$ *образом* этого гомоморфизма. Докажите, что $\mathrm{Im} f$ — подкольцо кольца B.

Задача 4. Рассмотрим отображение $\pi : A \to A/I$, где $I \subset A$ — идеал в A, причём $\pi(a) = a + (I)$ — просто элементу кольца A ставим в соответствие представителя кольца A/I. Проверьте, что это отображение является гомоморфизмом колец.

Определение 4. *Изоморфизмом* колец называется гомоморфизм колец, который является ещё и взаимно однозначным отображением множеств (т. е. биекцией).

Пример 7. Кольцо $\mathbb{R}[x]/(x-1)$ изоморфно кольцу всех действительных чисел $\mathbb{R}$ посредством изоморфизма

$$f : \mathbb{R}[x]/(x-1) \to \mathbb{R},$$
$$P(x) + (x-1) \cdot Q(x) \mapsto P(1).$$

Задача 5. Поймите, почему это изоморфизм.

Описанный выше пример можно обобщить при помощи *теоремы о гомоморфизме*:

Теорема 1 (о гомоморфизме)**.** *Пусть $f : A \to B$ — гомоморфзм колец. Тогда*

$$\text{Im } f \cong A/\text{Ker } f.$$

Более точно, имеется изоморфизм

$$\varphi : \text{Im} f \to A/\text{Ker } f,$$

ставящий в соответствие каждому элементу $b = f(a) \in \text{Im } f$ класс $a + \text{Ker } f$.

Задача 6. Докажите, что $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$. И вообще, пусть x^2+px+q — квадратный трёхчлен с действительными коэффициентами и отрицательным дискриминантом. Докажите, что $\mathbb{R}/(x^2+px+q) \cong \mathbb{C}$.

2 Рождественская теорема Ферма

Задача 7. Пусть $\mathbb{F}$ — некоторое поле. Докажите, что кольцо $\mathbb{F}[x]/(P)$ — поле $\Leftrightarrow$ многочлен P неприводим над $\mathbb{F}$ (т. е. не раскладывается в произведение непостоянных многочленов).

Задача 8. Докажите, что для числа $a \in \mathbb{Z}$ существует такое число $x \in \mathbb{Z}$, что $a \equiv x^2 (\text{mod } p)$, где $p \in \mathbb{Z}$ — простое число $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$.

Задача 9. Когда уравнение $x^2 + 1 = 0$ имеет решение в $\mathbb{Z}_p$, где p — простое целое число?

Задача 10. Докажите, что $\mathbb{Z}[i]/(p) \cong \mathbb{Z}_p[x]/(x^2+1)$.

Задача 11. Какие целые простые числа просты и в гауссовых числах?

Задача 12 (Собственно, рождественская теорема Ферма)**.** Докажите, что простое натуральное число p представимо в виде суммы двух квадратов целых чисел тогда и только тогда, когда $p = 4k + 1$.

Задача 13 (Обобщение)**.** Докажите, что натуральное число n представимо в виде суммы двух квадратов целых чисел тогда и только тогда, когда в его разложение на простые множители в $\mathbb{Z}$ все множители вида $4k + 3$ входят в чётной степени.

Задача 14. В зависимости от простых чисел $p_i,\ i = 1, ..., s$ найдите количество представлений числа $p_1...p_s$ в виде суммы двух квадратов.