Идеалы и Модули

Определение 1. Пусть K — коммутативное кольцо с единицей. Идеал I называется *максимальным*, если он не содержится ни в каком большем идеале, кроме самого кольца.

Предложение 1 *Идеал I максимален тогда и только тогда, когда факторкольцо K/I является полем.*

Доказательство: Поле определяется тем, что всякий ненулевой идеал в нём содержит единицу, а значит совпадает со всем полем. Пусть идеал $I \subset K$ содержится в идеале I', тогда I'/I будет идеалом в K/I, значит, если K/I — поле, то $I' = I$ или $I' = K$.

Наоборот, пусть теперь I — маскимальный идеал, докажем, что всякий элемент $x \notin I$ обратим по модулю I. Заметим, что идеал $I + (x)$ содержит I и не совпадает с I. Значит, он равен K и, тем самым, содержит единицу. То есть найдётся y, такой что $xy - 1 \in I$, что и требуется.

Пример. Так как многочлен $x^2 + 1$ неразложим в $\mathbb{R}[x]$, идеал $(x^2 + 1)\mathbb{R}[x]$ является максимальным, и $\mathbb{R}[x]/(x^2 + 1)\mathbb{R}[x]$ изоморфно полю $\mathbb{C}$.

Определение 2. Целостное кольцо называется *кольцом главных идеалов*, если всякий идеал в нём является главным (порождён одним элементом).

Лемма 1 *В кольце главных идеалов всякая возрастающая цепочка идеалов $I_1 \subsetneq I_2 \subsetneq \dots$ конечна (кольца с этим свойством называют* нётеровыми*).*

Доказательство: Объединение этой цепочки тоже будет идеалом, который в свою очередь порождён элементом x. Но всякий элемент объединения принадлежит I_k для некоторого k, в том числе и x. Этот I_k и будет последним в цепочке.

Теорема 1 *Всякое кольцо главных идеалов факториально.*

Доказательство: Сначала докажем существование. Всякий элемент либо прост, либо разлагается в произведение необратимых элементов. Будем разлагать их дальше, озаботившись лишь вопросом, почему такая процедура рано или поздно остановится.

Делимость соответствует вложению идеалов, поэтому по Лемме 1 невозможно бесконечно делить элемент нашего кольца на необратимые элементы, из чего следует, что процесс завершится за конечное число шагов.

Доказательство единственности аналогично евклидовому случаю. В кольцах главных идеалов тоже определён наибольший общий делитель. Для элементов a, $b \in K$ рассмотрим идеал $aK+bK$, пусть он порождён элементом (a, b) (такой элемент определён с точностью до умножения на обратимый). Тогда (a, b) является общим делителем a и b, и кроме того всякий общий делитель a и b делит (a, b). Из определения сразу следует, что существуют u и v, такие что $(a, b) = au + bv$.

Отсюда вытекает лемма о том, что если $a|bc$ и $(a, b) = 1$, то $a|c$, дальнейшее доказательство повторяет доказательство для евклидового кольца.

Следующая задача — решение систем линейных диофантовых уравнений вида

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n &= c_1 \\ a_{21}x_1 + \dots + a_{2n}x_n &= c_2 \\ \dots & \\ a_{m1}x_1 + \dots + a_{mn}x_n &= c_m \end{cases}$$

Сведём эту задачу к более простой. Для этого мы можем переходить к равносильным системам, переставляя уравнения, а также прибавляя к одному из уравнений другое, умноженное на произвольный элемент кольца. Аналогично, можно менять местами переменные и заменять x_i на $x_i + kx_j$, не забыв потом вернуться к исходным переменным.

Коэффициенты уравнения можно записать матрицей вида $\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$, применяя к этой матрице описанные выше элементарные преобразования строк и столбцов, попробуем привести её к удобному для решения виду.

Теорема 2 *Пусть кольцо K евклидово. Тогда всякую матрицу можно привести элементарными преобразованиями строк и столбцов к* нормальной форме Смита*: матрице* $\mathrm{Diag}(a_1, a_2, \dots)$ *с нулями вне главной диагонали и числами a_1, $a_2, \dots$ на ней, таких что $a_i | a_{i+1}$ для $i = 1, 2, \dots$.*

Доказательство: Определим *норму* матрицы как минимум норм ненулевых элементов. Чтобы убедиться, что предлагаемый ниже алгоритм закончится за конечное число шагов, будем на каждом содержательном шаге уменьшать это натуральное число.

Для удобства обозначений перестановкой строк и столбцов перенесём ненулевой элемент с минимальной нормой в левый верхний угол, теперь он называется a_{11}. Если в первой строке есть элемент, не делящийся на a_{11}, то преобразованием столбцов можем получить остаток при делении на a_{11}, уменьшая тем самым норму матрицы. Снова перенесём элемент с минимальной нормой в левый верхний угол. Аналогично поступим и с первым столбцом.

В результате получим $a_{11} | a_{1j}$ и $a_{11} | a_{i1}$ для всех $1 \leqslant i \leqslant m$ и $1 \leqslant j \leqslant n$, причём a_{11} по-прежнему элемент с минимальной нормой. Теперь, вычитая из j-того столбца a_{1j}/a_{11} для $j = 2 \dots n$, затем вычитая из j-той строки a_{i1}/a_{11} для $i = 2 \dots m$, получим матрицу с единственным ненулевым элементом a_{11} в первом столбце и строке. Норма при этом не увеличится. Если она уменьшилась, повторим процедуру с начала. Рано или поздно получим матрицу, в которой элемент a_{11} имеет минимальную норму и $a_{i1} = a_{1j} = 0$ для $i, j > 1$.

Теперь пусть некоторый элемент a_{ij} не делится на a_{11}. Тогда, прибавляя i-тою строку к первой, получим эти два элемента в одной строке, после чего уменьшим норму матрицы. Повторяя с самого начала, получим матрицу, в которой элемент a_{11} имеет минимальную норму, все элементы матрицы делятся на a_{11} и $a_{i1} = a_{1j} = 0$ для $i, j > 1$. Проделаем аналогичную процедуру с матрицей, составленной из остальных (вторых и далее) строк и столбцов, и так далее, получим нормальную форму Смита.

На самом деле элементарные преобразования строк и столбцов — умножение слева и справа на обратимую матрицу. Любое такое умножение переводит систему в равносильную. Это позволяет немного обобщить теорему.

Упражнение 1 *Пусть K — кольцо главных идеалов. Докажите, что умножением слева и справа на обратимые матрицы можно привести любую матрицу к нормальной форме Смита.*

Тем самым, вопрос о решении системы уравнений сводится к вопросу делимости.

некоммутативный случай

Определение 3. *Двусторонний идеал $I \subset K$* — подмножество со следующими свойствами:

1) I — подгруппа по сложению (достаточно проверить, что если a, $b \in I$, то $a - b \in I$),
2) если $a \in I$, $x \in K$, то $xa \in I$,
3) если $a \in I$, $x \in K$, $ax \in I$.

Определение 4. Подмножество, для которого выполнены аксиомы 1) и 2), называется *левым* (left) идеалом, подмножество, для которого выполнены аксиомы 1) и 3), называется *правым* (right) идеалом.

Если K коммутативно, никакой разницы между правым, левым и двусторонним идеалом нет, аксиомы 2) и 3) равносильны.

Здесь задача о ядрах отображений и о разрешимости линейных уравнений имеют разные ответы. Факторизовать кольцо можно аналогичным способом по двусторонним идеалам, а в задаче про уравнения возникает правый идеал. Тем не менее, множество классов эквивалентности по одностороннему идеалу обладает рядом примечательных свойств.

Определение 5. M — левый модуль (left module) над кольцом с единицей K, если M — абелева группа по сложению и K действует на M "умножением", так что выполнено

1) Линейность - 1: $a(m_1 \pm m_2) = am_1 \pm am_2$, $a \in K$, m_1, $m_2 \in M$.
2) Линейность - 2: $(a_1 \pm a_2)m = a_1m \pm a_2m$, a_1, $a_2 \in K$, $m \in M$.
3) Ассоциативность: $(ab)m = a(bm)$, a, $b \in K$, $m \in M$.
4) Единица: $1m = m$, $m \in M$.

Определение 6. M — правый модуль (right module) над кольцом с единицей K, если M — абелева группа по сложению и K действует на M "умножением", так что выполнено

1) Линейность - 1: $(m_1 \pm m_2)a = m_1a \pm m_2a$, $a \in K$, m_1, $m_2 \in M$.
2) Линейность - 2: $m(a_1 \pm a_2) = ma_1 \pm ma_2$, a_1, $a_2 \in K$, $m \in M$.
3) Ассоциативность: $m(ab) = (ma)b$, a, $b \in K$, $m \in M$.
4) Единица: $m1 = m$, $m \in M$.

Содержательная разница этих определений — в том, как устроена ассоциативность. При этом если K коммутативно, то никакой разницы и нет — левый модуль является правым и наоборот.

Также являются модулями всякое кольцо над своим подкольцом (и левым, и правым), и всякий левый/правый идеал над соответствующим кольцом.

Определение 7. *Отображение модулей* (modules homomorphism) $f : M_1 \to M_2$, где M_1, M_2 — модули (для определённости левые) над кольцом K, — это такое отображение множеств, что $f(m_1 + m_2) = f(m_1) + f(m_2)$, $f(am) = af(m)$.

Заметим, что естественным образом определены композиция и сумма таких отображений. Так что множество отображений модулей $\mathrm{Hom}_K(M_1, M_2)$ — абелева группа по сложению, а $\mathrm{Hom}_K(M, M)$ — кольцо с единицей.

Пример. Если K — поле, то модуль над F называется *векторным пространством (vector space)*, а отображение модулей — *линейным отображением (linear map)*.

Пример. Если $K = \mathbb{Z}$, то действие K можно восстановить из структуры абелвой группы, так что $\mathbb{Z}$-модули — это просто абелевы группы.

Пример. Модуль над $F[x]$ — векторное пространство V над F, в котором действие переменной x задаёт линейное отображение из V в V.

Определение 8. *Прямая сумма (direct sum)* $M_1 \oplus \cdots \oplus M_k$ — модуль, составленный наборами $(m_1, \ldots, m_k)$, $m_i \in M_i$, со сложением и действием по правилу

$$(m_1, \ldots, m_k) + (m'_1, \ldots, m'_k) = (m_1 + m'_1, \ldots, m_k + m'_k), \qquad a(m_1, \ldots, m_k) = (am_1, \ldots, am_k).$$

Определение 9. Модуль вида $K \oplus \cdots \oplus K$ называется *свободным* модулем и обозначается K^n, где n — число слагаемых.

Предложение 2 *Пусть K — кольцо. Отображения свободных модулей $K^n \to K^m$ однозначно задаются матрицами $n \times m$ с элементами из K, причём композиция соответствует умножению матриц.*

Доказательство: Легко проверить, что отображение однозначно определяется образами элементов $(0, \ldots, 0, 1, 0, \ldots, 0)$, где единица находится на j-том месте. Полагая образ такого элемента равным $(a_{1j}, a_{2j}, \ldots, a_{mj})$, составляем матрицу (a_{ij}).