Лекция 19. Кольца и алгебры. Часть 2.

Продолжим изучение колец и алгебр. Как и в теории групп, для сравнения разных алгебраических объектов, принадлежащих к одному классу, используется понятие гомоморфизма.

Определение. *Гомоморфизм колец (алгебр)* – это отображение $\varphi\colon A \to B$ (где A и B – кольца/алгебры), для которого: $\forall x, y \in A$:

- $\varphi(x + y) = \varphi(x) + \varphi(y)$
- $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$

для алгебр добавляется еще одно свойство: $\forall \lambda \in K$:

- $\varphi(\lambda \cdot x) = \lambda \cdot \varphi(x)$

для колец/алгебр с единицей требуется выполнения еще одного условия (единица в A переходит в единицу в B):

- $\varphi(1) = 1$

Образ гомоморфизма:

$$Im\ \varphi = \{b = \varphi(a) \mid a \in A\}$$

Ядро гомоморфизма:

$$Ker\ \varphi = \{a \in A \mid \varphi(a) = 0\}$$

В частности, если рассматривать A и B как группы по сложению, то получаем привычные понятия образа и ядра гомоморфизма групп. Если A и B алгебры, то φ является линейным отображением – получаем понятия образа и ядра линейного отображения, знакомые из линейной алгебры. Как и для групп, верно следующее утверждение.

Предложение 1. Для любого гомоморфизма колец/алгебр $\varphi\colon A \to B$:

- $Im\ \varphi \subseteq B$ – подкольцо/подалгебра
- $Ker\ \varphi \lhd A$ – двусторонний идеал

Доказательство.
1) Как мы знаем из теории групп, $Im\ \varphi$ и $Ker\ \varphi$ – подгруппы по сложению. Для того, чтобы доказать, что $Im\ \varphi$ – подкольцо, остается проверить замкнутость относительно умножения:

$$b, b' \in Im\ \varphi \Rightarrow b = \varphi(a), b' = \varphi(a') \Rightarrow bb' = \varphi(aa') \in Im\ \varphi$$

Если $Im\ \varphi$ – подалгебра, нужно еще проверить замкнутость относительно умножения на скаляры:

$$b \in Im\ \varphi \Rightarrow \lambda b = \varphi(\lambda a) \in Im\ \varphi$$

Таким образом, $Im\ \varphi$ – подкольцо/подалгебра в B.

2) Для того, чтобы доказать, что $Ker\ \varphi$ – двусторонний идеал, остается проверить замкнутость относительно умножения справа и слева на любые элементы A:

$$a \in Ker\ \varphi, a' \in A \Rightarrow \varphi(aa') = \varphi(a)\varphi(a') = 0 \cdot \varphi(a') = 0 \Rightarrow aa' \in Ker\ \varphi$$
$$a \in Ker\ \varphi, a' \in A \Rightarrow \varphi(a'a) = \varphi(a')\varphi(a) = \varphi(a') \cdot 0 = 0 \Rightarrow a'a \in Ker\ \varphi$$

Если A – алгебра, нужно еще проверить замкнутость относительно умножения на скаляры:

$$\varphi(\lambda a) = \lambda \cdot \varphi(a) = \lambda \cdot 0 = 0 \Rightarrow \lambda a \in Ker\ \varphi$$

Следовательно, $Ker\ \varphi \lhd A$. ■

Таким образом, идеалы естественно возникают как ядра гомоморфизмов колец/алгебр. Верно и обратное. Пусть $I \lhd A$, тогда, как и для групп, можно рассмотреть каноническую проекцию из A в факторкольцо/факторалгебру A/I, которая каждому элементу ставит в соответствие его смежный класс (класс вычетов) по модулю идеала I.

Каноническая проекция:

$$\pi\colon\ A \to A/I$$
$$a \mapsto a + I$$

Каноническая проекция – гомоморфизм (следует из определения операций в A/I: операции над смежными классами определяются через операции над представителями этих смежных классов). Ядром этого гомоморфизма является сам идеал I, а образ совпадает с A/I:

$$Ker\ \pi = I$$
$$Im\ \pi = A/I$$

Таким образом, двусторонние идеалы = ядра гомоморфизмов. По аналогии с теорией групп, существует и следующая теорема.

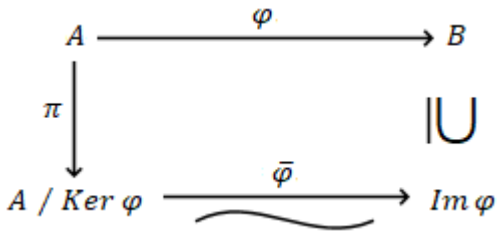
Основная теорема о гомоморфизмах колец/алгебр. Пусть $\varphi\colon\ A \to B$ – гомоморфизм колец/алгебр. Тогда ∃! изоморфизм

$$\bar{\varphi}\colon\ A/\ Ker\ \varphi \twoheadrightarrow Im\ \varphi,$$

для которого $\varphi = \bar{\varphi} \circ \pi$, где $\pi\colon\ A \to A\ /\ Ker\ \varphi$ – каноническая проекция. Другими словами,

$$\varphi(a) = \bar{\varphi}(a + Ker\ \varphi)$$

Еще короче теорему можно сформулировать с помощью коммутативной диаграммы:



Доказательство.
Из теории групп мы знаем, что существует единственный изоморфизм аддитивных групп $\bar{\varphi}$ с нужными свойствами (см. основную теорему о гомоморфизмах групп, лекция 2). Остается проверить, что $\bar{\varphi}$ – гомоморфизм колец/алгебр.

$\bar{\varphi}$ – гомоморфизм колец:

$$\bar{\varphi}\big((x + Ker\,\varphi) \cdot (y + Ker\,\varphi)\big) = \bar{\varphi}(xy + Ker\,\varphi) = \varphi(xy) = \varphi(x) \cdot \varphi(y) =$$

$$= \bar{\varphi}(x + Ker\,\varphi) \cdot \bar{\varphi}(y + Ker\,\varphi)$$

$\bar{\varphi}$ – гомоморфизм алгебр:

$$\bar{\varphi}\big(\lambda \cdot (x + Ker\,\varphi)\big) = \bar{\varphi}(\lambda x + Ker\,\varphi) = \varphi(\lambda x) = \lambda \cdot \varphi(x) = \lambda \cdot \varphi(x + Ker\,\varphi)$$

■

Пример. Рассмотрим алгебру $\mathcal{F}(X, K)$. Выберем $x_0 \in X$ и рассмотрим гомоморфизм вычисления значения функции в данной точке:

$$\varphi\colon \mathcal{F}(X, K) \to K$$
$$f \mapsto f(x_0)$$

Его ядро и образ:

$$Ker\,\varphi = I(x_0)$$
$$Im\,\varphi = K$$

По основной теореме о гомоморфизмах,

$$\mathcal{F}(X, K)/I(x_0) \simeq K$$

Еще одно понятие, которое можно перенести из теории групп в теорию колец/алгебр – это понятие прямой суммы.

Определение. Прямая сумма колец/алгебр

$$A = A_1 \oplus \cdots \oplus A_s$$

- их прямая сумма как аддитивных групп (если A – кольцо), или как векторных пространств (если A – алгебра) с умножением по правилу: $\forall a_i, b_i \in A_i$ $(i = 1, \dots, s)$:

для внутренней прямой суммы: если

$$a = a_1 + \cdots + a_s$$
$$b = b_1 + \cdots + b_s$$

то

$$ab = a_1 b_1 + \cdots + a_s b_s$$

для внешней прямой суммы: если

$$a = (a_1, \dots, a_s)$$
$$b = (b_1, \dots, b_s)$$

то

$$ab = (a_1 b_1, \dots, a_s b_s)$$

Как и в случае групп, понятия внешней и внутренней прямой суммы колец/алгебр эквивалентны. Прямая сумма колец/алгебр данного типа (коммутативные, ассоциативные, с единицей и т.д.) часто имеет тот же тип. В частности, имеет место следующий факт: пусть $A_1, \dots, A_s$ – ассоциативные кольца с единицей, тогда $A_1 \oplus \cdots \oplus A_s$ – ассоциативное кольцо/алгебра с единицей $(1, \dots, 1)$.

Лемма. Мультипликативная группа прямой суммы ассоциативных колец с единицей изоморфна прямому произведению мультипликативных групп этих колец:

$$(A_1 \oplus \cdots \oplus A_s)^\times \simeq A_1^\times \times \cdots \times A_s^\times$$

Доказательство.
Элемент $(a_1, \dots, a_s)$ обратим в $A_1 \oplus \cdots \oplus A_s \Leftrightarrow \exists b_i \in A_i$:

$$(a_1, \dots, a_s)(b_1, \dots, b_s) = (a_1 b_1, \dots, a_s b_s) = (1, \dots, 1) \Leftrightarrow \forall i\colon\ a_i b_i = 1$$
$$(b_1, \dots, b_s)(a_1, \dots, a_s) = (b_1 a_1, \dots, b_s a_s) = (1, \dots, 1) \Leftrightarrow \forall i\colon\ b_i a_i = 1$$

То есть, $\forall i\colon\ a_i b_i = b_i a_i = 1$, что равносильно тому, что $\forall i\ a_i$ обратим в A_i. Таким образом, элемент прямой суммы обратим тогда и только тогда, когда обратимы его компоненты. Это и устанавливает изоморфизм между $(A_1 \oplus \cdots \oplus A_s)^\times$ и $A_1^\times \times \cdots \times A_s^\times$ (так как в обоих случаях умножение происходит покомпонентно). ■

Китайская теорема об остатках для колец вычетов.

Пусть $m_1, \dots, m_s \in \mathbb{N}$ попарно взаимно просты, $m = m_1 \cdot \ldots \cdot m_s$. Тогда

$$\mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$$

- изоморфизм колец.

Доказательство.
Рассмотрим отображение

$$\psi\colon\ \mathbb{Z} \to \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$$
$$\psi(n) = (n \bmod m_1, \dots, n \bmod m_s)$$

Это гомоморфизм колец (так как при сложении и умножении целых чисел вычеты этих чисел по соответствующим модулям тоже складываются (соответственно, перемножаются), а наборы вычетов складываются покомпонентно).

Как было показано ранее (при доказательстве китайской теоремы об остатках для групп – см. лекцию 4):

$$Ker\,\psi = m\mathbb{Z}$$
$$Im\,\psi = \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$$

По основной теореме о гомоморфизмах колец,

$$\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$$
$$\bar{\psi}(n\ mod\ m) = (n\ mod\ m_1, \dots, n\ mod\ m_s)$$

■

Следствие (мультипликативное свойство функции Эйлера). Функция Эйлера мультипликативна:

$$\varphi(m) = \varphi(m_1) \cdot \ldots \cdot \varphi(m_s)$$

В частности, если $m = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$, где $p_1, \dots, p_s$ – различные простые числа, $k_1, \dots, k_s \in \mathbb{N}$, то

$$\varphi(m) = \varphi\left(p_1^{k_1}\right) \cdot \ldots \cdot \varphi\left(p_s^{k_s}\right) = \left(p_1^{k_1} - p_1^{k_1-1}\right) \cdot \ldots \cdot \left(p_s^{k_s} - p_s^{k_s-1}\right)$$

Доказательство.
По китайской теореме об остатках для колец:

$$\mathbb{Z}_m \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_s}$$

тогда по лемме

$$\mathbb{Z}_m^\times \simeq \mathbb{Z}_{m_1}^\times \times \cdots \times \mathbb{Z}_{m_s}^\times.$$

Следовательно,

$$\varphi(m) = |\mathbb{Z}_m^\times| = \left|\mathbb{Z}_{m_1}^\times\right| \cdot \ldots \cdot \left|\mathbb{Z}_{m_s}^\times\right| = \varphi(m_1) \cdot \ldots \cdot \varphi(m_s)$$

■

В теории групп было понятие простой группы (т.е. группы, в которой нет нетривиальных нормальных подгрупп). Аналогичное понятие можно определить и для колец/алгебр.

Определение. Кольцо/алгебра A называется *простым*, если $A \neq \{0\}$ и в A не существует нетривиальных двусторонних идеалов $I \lhd A$, кроме тривиальных: $I = \{0\}$ и $I = A$.

Теорема 1. Коммутативное ассоциативное кольцо с единицей A просто $\Leftrightarrow$ A – поле.

Доказательство.

⇒:
Пусть $x \in A$, $x \neq 0$. Рассмотрим множество элементов, кратных x:

$$I = \{a \cdot x \mid a \in A\} = A \cdot x$$

Легко видеть, что это идеал: $I \lhd A$, при этом $I \neq \{0\}$, так как I содержит по крайней мере $x = 1 \cdot x$. Следовательно (так как A просто), $I = A$. Отсюда следует, что существует $y \in A$: $y \cdot x = 1$, т.е. x обратим. Таким образом, A – поле.

⇐:
Пусть $I \lhd A$, $I \neq \{0\}$. Выберем $x \in A$, $x \neq 0$. Тогда $x \cdot x^{-1} = 1 \in I$. Но если идеал содержит 1, тогда он содержит и любой элемент кольца A, так как $\forall a \in A$: $a = a \cdot 1 \in I$. Следовательно, $I = A$, т.е. A – простое кольцо. ■

Отметим, что в случае некоммутативных колец аналогичное утверждение верно только в одну сторону: всякое тело является простым ассоциативным кольцом с единицей. Обратное неверно – существуют простые некоммутативные ассоциативные кольца с единицей, которые не являются телами, и важный пример такого кольца (и алгебры) доставляет следующая теорема.

Теорема 2. Алгебра $Mat_n(K)$ проста.

Доказательство.
Пусть $I \lhd Mat_n(K), I \neq \{0\}$. Выберем $A \in I, A \neq \{0\}$. Разложим матрицу A по базису, т.е. представим в виде линейной комбинации матричных единиц:

$$A = \sum_{i,j=1}^{n} a_{ij} E_{ij}$$

Так как $A \neq \{0\}$, то $\exists k, l$: $a_{kl} \neq 0$.

Умножим A слева и справа на матричные единицы: $\forall p, q \in \{1, \dots, n\}$ рассмотрим произведение:

$$E_{pk} \cdot A \cdot E_{lq} = a_{kl} \cdot E_{pk} \cdot E_{kl} \cdot E_{lq} = a_{kl} \cdot E_{pq} \in I$$

- таким образом, если в ненулевом идеале лежит какая-то ненулевая матрица, то там лежит и матричная единица: $E_{pq} \in I$ для произвольных $p, q \in \{1, \dots, n\}$. Следовательно, I содержит все матричные единицы, которые образуют базис алгебры матриц, т.е. $I = Mat_n(K)$. ■

Коммутативная алгебра.

Далее сосредоточим внимание на изучении коммутативных ассоциативных колец с единицей. Наука, их изучающая, называется коммутативной алгеброй.

Пусть A – коммутативное ассоциативное кольцо с единицей. Пусть задано семейство элементов $f_j \in A \quad (j \in J)$. По аналогии с определением подгруппы, порожденной семейством элементов, можно ввести понятие идеала, порожденного семейством элементов.

Определение. Идеал, *порожденный семейством элементов* кольца/алгебры $I = (f_j \mid j \in J) \lhd A$ – наименьший идеал, содержащий это семейство.

Такой идеал существует, так как его можно представить в виде пересечения всех идеалов, содержащих семейство $f_j \in A$ (хотя бы один такой идеал найдется – это само кольцо/алгебра A). Можно дать его явное описание:

$$I = \{a_1 f_{j_1} + \cdots + a_s f_{j_s} \mid j_1, \ldots, j_s \in J, \;\; a_1, \ldots, a_s \in A\}$$

В самом деле, любой идеал, содержащий элементы $f_j, \;\; j \in J$, содержит и все выражения вида $a_1 f_{j_1} + \cdots + a_s f_{j_s}$ (так как идеал замкнут относительно сложения и умножения на произвольные элементы кольца), но множество всех таких выражений само является идеалом.

Определение. *Конечно порожденный* идеал – идеал, порожденный конечным семейством элементов:

$$I = (f_1, \ldots, f_m) = \{a_1 f_1 + \cdots + a_m f_m \mid a_i \in A\} = Af_1 + \cdots + Af_m$$

Существуют кольца/алгебры, в которых каждый идеал является конечно порожденным. Приведем без доказательства один из важных результатов, касающихся таких колец/алгебр.

Теорема Гильберта о базисе идеала. В алгебре многочленов $K[x_1, \ldots, x_n]$ над полем K любой идеал конечно порожден.

Немного упростим ситуацию, и будем рассматривать среди конечно порожденных идеалов самые простые – а именно, идеалы, порожденные одним элементом. Такие идеалы называются главными.

Определение. *Главный* идеал – идеал вида

$$I = (f) = \{af \mid a \in A\} = Af$$

Определение. *Кольцо главных идеалов* – целостное кольцо, в котором все идеалы главные.

Напоминание: евклидово кольцо – целостностное кольцо A, на котором задана евклидова норма:

$$N: A\backslash\{0\} \to \mathbb{Z}_+$$

со свойствами:

1) $N(a \cdot b) \geq N(a)$, равенство достигается только при $b \in A^\times$,
2) $\forall a, b \in A, b \neq 0$ существуют $q, r \in A$: $a = b \cdot q + r$ и $N(r) < N(b)$, или $r = 0$ (деление с остатком).

Примеры евклидовых колец:

1) $A = \mathbb{Z}$, норма: $N(a) = |a|$,

2) $A = K[x]$, K – поле, норма: $N(f) = deg\ f$.

Теорема 3. Всякое евклидово кольцо (в частности, $\mathbb{Z}$ и $K[x]$, K – поле) является кольцом главных идеалов.

Доказательство.
Пусть A – евклидово кольцо, $I \lhd A$. Если $I = \{0\}$, то $I = (0)$ – главный идеал. Иначе выберем $b \in I$, $b \neq 0$ с наименьшей нормой среди ненулевых элементов идеала I: $N(b) = min$ (среди элементов I).
Теперь воспользуемся вторым свойством евклидовой нормы (деление с остатком): $\forall a \in I$: $a = b \cdot q + r$, причем $N(r) < N(b)$, или $r = 0$. Но $a \in I$, $b \cdot q \in I$, следовательно, и $a - b \cdot q = r \in I$, значит, $r = 0$ (иначе это противоречит выбору b). Получаем, что $a = b \cdot q$.
Следовательно, $I = (b)$. ■

Теория делимости в евклидовых кольцах, которую мы развили в первой части курса, практически без изменений переносится на любые кольца главных идеалов. Отметим, что не всякое целостное (и даже факториальное) кольцо является кольцом главных идеалов.

Пример. $K[x_1, \dots, x_n]$ – не кольцо главных идеалов при $n > 1$.

В самом деле, рассмотрим

$$I = \{f \in K[x_1, \dots, x_n] \mid f(0, \dots, 0) = 0$$

- идеал многочленов без свободного члена. Если бы $I = (f)$, то $x_1, \dots, x_n$ должны были бы делиться на f (так как $x_1, \dots, x_n \in I$), откуда следует, что $f = c \in K$. Но если $c = 0$, то $I = \{0\}$, а если $c \neq 0$, то $I = K[x_1, \dots, x_n]$ – противоречие. Следовательно, I – не главный идеал.