Лекция 18. Кольца и алгебры. Часть 1.

Определение. *Кольцо* – это множество A с двумя бинарными операциями (сложением и умножением), для которых выполнены следующие аксиомы:

1) относительно сложения, A – абелева группа,
2) умножение дистрибутивно:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(b + c) \cdot a = b \cdot a + c \cdot a$$

Определение. *Алгебра* над полем K – это множество A с тремя операциями: сложение, умножение, умножение на элементы поля K (скаляры), для которых выполнены следующие аксиомы:

1) относительно сложения и умножения на скаляры, A – векторное пространство над K,
2) умножение билинейно, т.е. выполнены свойства:

- дистрибутивность:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(b + c) \cdot a = b \cdot a + c \cdot a$$

- однородность: $\forall a, b \in A,\ \forall \lambda \in K$

$$(\lambda \cdot a) \cdot b = a \cdot (\lambda \cdot b) = \lambda \cdot (a \cdot b)$$

В зависимости от дополнительных свойств умножения, выделяют разные классы колец и алгебр: коммутативные, ассоциативные, с единицей, и т.д.

Примеры.

1) $\mathbb{Z}$ (целые числа) - коммутативное, ассоциативное кольцо с единицей без делителей нуля (область целостности).

2) $\mathbb{Z}_m$ (вычеты по модулю m) - коммутативное, ассоциативное кольцо с единицей. Если m – простое число, то $\mathbb{Z}_m$ является полем (поле – ненулевое коммутативное ассоциативное кольцо с единицей, каждый ненулевой элемент которого обратим).

3) $K[x_1, \dots, x_n]$ (многочлены от n переменных над полем K) – коммутативная, ассоциативная алгебра с единицей без делителей нуля.

4) $\mathcal{F}(X, K)$ (функции на множестве X со значениями в поле K) – коммутативная, ассоциативная алгебра с единицей.

5) $Mat_n(K)$ (матрицы $n \times n$ над полем K) – некоммутативная, ассоциативная алгебра с единицей.

6) E (трехмерное евклидово пространство) с операцией векторного умножения:

$$(a, b) \mapsto [a, b]$$

Свойства векторного умножения:

1) билинейность
2) антикоммутативность:

$$[a, b] = -[b, a]$$

3) тождество Якоби: $\forall a, b, c \in E$:

$$[[a, b], c] + [[b, c], a] + [[c, a], b] = 0$$

E – *алгебра Ли* над $\mathbb{R}$ (алгебра Ли – алгебра, в которой умножение антикоммутативно и удовлетворяет тождеству Якоби). Названа так в честь Софуса Ли (M. S. Lie, 1842-1899) – норвежского математика 19 века.

Замечание. Если A – ненулевая алгебра с единицей над полем K, то $1 \neq 0$ (действительно, если бы выполнялось равенство $1 = 0$, то $\forall a \in A$: $a = a \cdot 1 = a \cdot 0 = 0$). Тогда существует вложение поля K в качестве подалгебры в алгебру A:

$$K \hookrightarrow A$$
$$\lambda \mapsto \lambda \cdot 1$$

Это действительно вложение, так как если $\lambda \cdot 1 = \mu \cdot 1$, то $(\lambda - \mu) \cdot 1 = 0$, откуда следует, что $\lambda - \mu = 0$, то есть, $\lambda = \mu$.

Таким образом, мы можем рассматривать ненулевую алгебру с единицей над полем K как кольцо с единицей, которое содержит K в качестве подкольца.

Возникает вопрос о необходимости введения понятия алгебры. Дело в том, что алгебры удобнее колец – с ними проще работать, поскольку в алгебре есть дополнительная структура векторного пространства и можно использовать мощные методы линейной алгебры. Особенно это удобно в конечномерной ситуации.

Структурные константы.

Определение. Пусть A – конечномерная алгебра над полем K, $dim\, A = n$. Выберем в A базис $(e_1, \dots, e_n)$. Тогда $\forall i, j \in \{1, \dots, n\}$:

$$e_i \cdot e_j = c_{ij}^1 e_1 + \dots + c_{ij}^n e_n$$

Коэффициенты $c_{ij}^{\mathrm{k}} \in K \ \ (i,j,k \in \{1,\dots,n\})$ называются *структурными константами* алгебры A в базисе $(e_1,\dots,e_n)$.

Структурные константы однозначно определяют умножение в алгебре A. В самом деле, $\forall x,y \in A$:

$$x = x_1e_1 + \cdots + x_ne_n$$
$$y = y_1e_1 + \cdots + y_ne_n$$
$$x \cdot y = \sum_{i,j=1}^{n} x_iy_j \cdot e_i \cdot e_j = \sum_{i,j,k=1}^{n} c_{ij}^{k} \cdot x_iy_j \cdot e_k$$

Так как структурные константы однозначно определяют умножение, то они однозначно определяют и все свойства этого умножения. Например:

коммутативность $\Leftrightarrow e_i \cdot e_j = e_j \cdot e_i \ \ \forall i,j \in \{1,\dots,n\} \Leftrightarrow c_{ij}^{k} = c_{ji}^{k} \ \ \forall i,j,k \in \{1,\dots,n\}$
антикоммутативность $\Leftrightarrow e_i \cdot e_j = -e_j \cdot e_i \ \forall i,j \in \{1,\dots,n\} \Leftrightarrow c_{ij}^{k} = -c_{ji}^{k} \ \forall i,j,k \in \{1,\dots,n\}$

Упражнение. Охарактеризовать ассоциативность и тождество Якоби в терминах структурных констант.

Примеры.

1) $A = Mat_n(K)$. Базис – матричные единицы E_{ij} $(i,j = 1,\dots,n)$:

$$E_{ij} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & 1 & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \begin{matrix} \\ i \\ \\ \end{matrix}$$
$$\qquad\qquad\quad j$$

Матричные единицы перемножаются по правилу: $E_{ij} \cdot E_{kl} = \begin{cases} E_{il} \text{ при } j = k \\ 0 \text{ при } \ j \neq k \end{cases}$

Структурные константы:

$$c_{ij,kl}^{pq} = \begin{cases} 1 \text{ при } i = p, j = k, q = l \\ 0, \text{иначе} \end{cases}$$

2) Пусть G – конечная группа. *Групповая алгебра* $K \cdot G$ – векторное пространство с базисом e_g $(g \in G)$ и билинейным умножением, заданным на базисе правилом:

$$e_g \cdot e_h = e_{g \cdot h}$$

т.е. базисные элементы перемножаются в соответствии с тем, как перемножаются элементы группы, которые нумеруют эти базисные векторы.

Структурные константы:

$$c_{g,h}^{u} = \begin{cases} 1 \text{ при } u = g \cdot h \\ 0, \text{ иначе} \end{cases}$$

Таким образом, всякий элемент a групповой алгебры $K \cdot G$ единственным способом разлагается в линейную комбинацию базисных:

$$a = \sum_{g \in G} \lambda_g \cdot e_g = \sum_{g \in G} \lambda_g \cdot g$$

где $\lambda_g \in K$ (для краткости иногда вместо e_g пишут соответствующий ему элемент $g \in G$ – получаем формальные линейные комбинации элементов группы).

Можно воспринимать групповую алгебру как множество формальных линейных комбинаций элементов конечной группы G с коэффициентами из поля K, которые складываются и перемножаются по формальным правилам.

$K \cdot G$ – ассоциативная алгебра с единицей $1 = e$ (нейтральный элемент в G), $dim\, K \cdot G = |G|$, алгебра $K \cdot G$ коммутативна $\Leftrightarrow$ G абелева.

3) *Алгебра кватернионов* $\mathbb{H}$ - четырехмерная алгебра над $\mathbb{R}$ с базисом $(1, i, j, k)$, причем 1 – единица в $\mathbb{H}$ (нейтральный элемент по умножению), i, j, k – кватернионные единицы. В $\mathbb{H}$ операция умножения задана на базисе по правилам:

$$\begin{gathered} i^2 = j^2 = k^2 = -1, \\ i \cdot j = k, \qquad j \cdot i = -k \\ j \cdot k = i, \qquad k \cdot j = -i \\ k \cdot i = j, \qquad i \cdot k = -j \end{gathered}$$

Таблицу умножения в $\mathbb{H}$ можно запомнить с помощью следующей картинки:

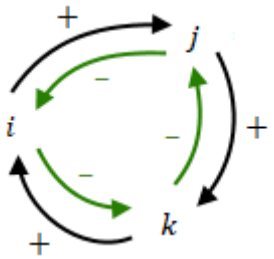


Рис. 18.1. Умножение кватернионных единиц

- произведение двух кватернионных единиц равно третьей, следующей за ними по циклу, причем если мы идем по часовой стрелке, то произведение будет со знаком “+”, а если против часовой стрелки, то со знаком “−“.

Кватернионы придумал английский математик Гамильтон (W.R. Hamilton, 1805-1865) как обобщение комплексных чисел. Однако, при этом не все свойства комплексных чисел удается сохранить: алгебра кватернионов $\mathbb{H}$ - некоммутативная ассоциативная алгебра с единицей над $\mathbb{R}$. Свойство ассоциативности (не вполне очевидное) можно проверить перебором на базисных векторах. Мы построим матричную модель алгебры кватернионов (т.е. алгебру, изоморфную алгебре кватернионов), про которую заранее известно, что умножение в ней ассоциативно.

Модель алгебры кватернионов

$$\mathbb{H} \simeq \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \mid a, b \in \mathbb{C} \right\} \subset Mat_2(\mathbb{C})$$

- вещественное четырехмерное подпространство в пространстве $Mat_2(\mathbb{C})$. Изоморфизм задается на базисе следующим соответствием:

$$1 \leftrightarrow E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad i \leftrightarrow I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad j \leftrightarrow J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad k \leftrightarrow K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Матрицы E, I, J, K действительно образуют базис в пространстве матриц вида $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$, $a, b \in \mathbb{C}$, так как они соответствуют выбору вместо чисел a и b соответствующих базисных элементов $1, i$.

Упражнение. Проверить, что для матриц E, I, J, K выполнены правила умножения кватернионных единиц $1, i, j, k$.

Следовательно, множество матриц вида $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$, $a, b \in \mathbb{C}$ образует подалгебру (над $\mathbb{R}$) в алгебре $Mat_2(\mathbb{C})$, изоморфную $\mathbb{H}$. Умножение матриц ассоциативно, поэтому и умножение в $\mathbb{H}$ ассоциативно. Исследуем и другие свойства алгебры кватернионов.

Определение. Пусть $q = \alpha \cdot 1 + \beta \cdot i + \gamma \cdot j + \delta \cdot k$, где $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ - произвольный кватернион. *Сопряженным кватернионом* называется $\bar{q} = \alpha \cdot 1 - \beta \cdot i - \gamma \cdot j - \delta \cdot k$. *Кватернионная норма*:

$$N(q) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$$

Сопряженный кватернион – аналог сопряженного комплексного числа, кватернионная норма – аналог квадрата модуля комплексного числа.

Свойства кватернионного сопряжения и кватернионной нормы:

1) $\bar{\bar{q}} = q$,
2) $\bar{q} = q \Leftrightarrow q \in \mathbb{R}$,
3) $\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2}$,

4) $\overline{q_1 \cdot q_2} = \overline{q_2} \cdot \overline{q_1}$

Доказательство.
Левая и правая части билинейно (над $\mathbb{R}$) зависят от q_1 и q_2, поэтому достаточно проверить свойство 4 для базисных кватернионов q_1 и q_2. Если один из них равен 1 ,то равенство $\overline{q_1 \cdot q_2} = \overline{q_2} \cdot \overline{q_1}$ очевидно, а если оба кватерниона равны мнимым кватернионным единицам, то рассмотрим два случая:
а) если $q_1 = q_2$, то

$$\overline{q_1 \cdot q_2} = \overline{q_1^2} = \overline{-1} = -1,$$
$$\overline{q_2} \cdot \overline{q_1} = \overline{q_1} \cdot \overline{q_1} = (-q_1) \cdot (-q_1) = q_1^2 = -1$$

б) если $q_1 \neq q_2$, например, $q_1 = i$, $q_2 = j$, то

$$\overline{q_1 \cdot q_2} = \overline{i \cdot j} = \bar{k} = -k$$
$$\overline{q_2} \cdot \overline{q_1} = \bar{j} \cdot \bar{i} = (-j) \cdot (-i) = j \cdot i = -k$$

5) $N(q) = q \cdot \bar{q} = \bar{q} \cdot q$ – проверяется непосредственно.

6) Если $q \neq 0$, то $N(q) \neq 0$ и существует обратный кватернион:

$$q^{-1} = \frac{\bar{q}}{N(q)}$$

Итак, в алгебре кватернионов любой ненулевой элемент имеет обратный. Такие алгебры (кольца) называются телами.

Определение. Назовем *телом* ненулевое ассоциативное кольцо с единицей, в котором каждый ненулевой элемент имеет обратный (иными словами, тело – это некоммутативное поле).

Определение. *Алгебра с делением* – это алгебра, являющаяся телом.

Таким образом, $\mathbb{H}$ - конечномерная алгебра с делением над $\mathbb{R}$.

Идеалы.

В теории групп особую роль играют нормальные подгруппы. Аналогичное понятие присутствует и в теории колец и алгебр – это идеал.

Определение. Пусть A – кольцо/алгебра. *Идеалом* в A называется подмножество $I \subseteq A$, для которого:
1) I – подгруппа относительно сложения (для колец),
– векторное подпространство (для алгебр).

2) $A \cdot I \subseteq I$ – *левый* идеал,
$I \cdot A \subseteq I$ – *правый* идеал.

Если идеал одновременно является левым и правым, то говорят, что он *двусторонний*. Именно двусторонние идеалы являются полным аналогом нормальных подгрупп в теории групп. В коммутативном кольце/алгебре все идеалы – двусторонние.

Обозначение для двустороннего идеала: $I \lhd A$.

Примеры идеалов.

1) $A = \mathbb{Z}$. Идеал – это подгруппа относительно сложения, поэтому любой идеал имеет вид

$$I = m \cdot \mathbb{Z} \ (m \geq 0).$$

Это двусторонний идеал: $m \cdot \mathbb{Z} \lhd \mathbb{Z}$.

2) Нулевой идеал $I = \{0\}$. Это двусторонний идеал : $\{0\} \lhd A$.

3) Наибольший идеал $I = A$. Очевидно, что это двусторонний идеал: $A \lhd A$. Наибольший и нулевой идеалы называются тривиальными.

4) $A = Mat_n(K) \supset I = \{\text{матрицы, у которых все столбцы, кроме первого, нулевые}\}$ – левый идеал (очевидно, что I – подпространство в $Mat_n(K)$, и при умножении матрицы из I слева на произвольную матрицу из $Mat_n(K)$ мы снова получим матрицу из I). Аналогично

$$A = Mat_n(K) \supset I = \{\text{матрицы, у которых все строки, кроме первой, нулевые}\}$$

- правый идеал. Отметим, что двусторонних идеалов в алгебре матриц нет.

5) $A = \mathcal{F}(X, K)$. Для любой точки $x_0 \in X$ рассмотрим $I(x_0)$ – множество функций, которые в этой точке обращаются в ноль:

$$I(x_0) = \{f \in \mathcal{F}(X, K) \mid f(x_0) = 0\}$$

Легко видеть, что $I(x_0)$ является подпространством в $\mathcal{F}(X, K)$ и $I(x_0)$ – двусторонний идеал: $I(x_0) \lhd \mathcal{F}(X, K)$.

Факторкольцо и факторалгебра.

В теории групп нормальные подгруппы используются для построения новых групп – мы можем строить по ним факторгруппы. Аналогичная конструкция есть и в теории колец и в теории алгебр.

Определение. Пусть A – кольцо или алгебра, $I \lhd A$. *Факторкольцо/факторалгебра*:

$$A/I = \{a + I \mid a \in A\}$$

- факторгруппа по сложению. Умножение смежных классов и умножение на скаляры определяется естественно: $\forall a, b \in A,\ \forall \lambda \in K$:

$$(a + I)(b + I) = ab + I$$
$$\lambda(a + I) = \lambda a + I$$

Проверим корректность так заданного умножения смежных классов, т.е. что результат умножения не зависит от выбора представителей смежных классов: пусть

$$a + I = a' + I \Rightarrow a' = a + u,\ \ u \in I,$$
$$b + I = b' + I \Rightarrow b' = b + v,\ \ v \in I,$$

тогда

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

Здесь $av \in I,\ ub \in I, uv \in I$, значит и $av + ub + uv \in I$, то есть, $ab + I = a'b' + I$.

Аналогично проверяется корректность умножения смежных классов на скаляры (в случае алгебры):

$$\lambda a' = \lambda a + \lambda u,\ \ u \in I,$$

- здесь $\lambda u \in I$, значит $\lambda a + I = \lambda a' + I$.

Пример. $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ – кольцо вычетов.

В связи с тем, что кольцо вычетов является общим случаем факторкольца, в общем случае принята та же терминология, что и для колец вычетов.

Терминология:

смежные классы по идеалу = классы вычетов:

$$a + I = a \bmod I$$

принадлежность одному смежному классу = сравнимость по модулю идеала:

$$a \equiv b \ (mod\ I) \Leftrightarrow a - b\ \in I \Leftrightarrow a + I = b + I$$