Лекции курса «Алгебра», лекторы И. В. Аржанцев и Р. С. Авдеев
ФКН НИУ ВШЭ, 1-й курс ОП ПМИ, 4-й модуль, 2014/2015 учебный год

Лекция 6

Кольца. Делители нуля, обратимые элементы, нильпотенты и идемпотенты. Поля и алгебры. Идеалы и факторкольца. Теорема о гомоморфизме. Центр алгебры матриц над полем. Простота алгебры матриц над полем.

Определение 1. *Кольцом* называется множество R с двумя бинарными операциями «+» (сложение) и «×» (умножение), обладающими следующими свойствами:

1) $(R, +)$ является абелевой группой (называемой *аддитивной группой* кольца R);

2) выполнены *левая и правая дистрибутивности*, т.е.

$$a(b+c) = ab + ac \quad \text{и} \quad (b+c)a = ba + ca \quad \text{для всех } a, b, c \in R.$$

В этом курсе мы рассматриваем только ассоциативные кольца с единицей, поэтому дополнительно считаем, что выполнены ещё два свойства:

3) $a(bc) = (ab)c$ для всех $a, b, c \in R$ (*ассоциативность умножения*);

4) существует такой элемент $1 \in R$ (называемый *единицей*), что

$$a1 = 1a = a \text{ для всякого } a \in R. \tag{1}$$

Замечание 1. В произвольном кольце R выполнены равенства

$$a0 = 0a = 0 \text{ для всякого } a \in R. \tag{2}$$

В самом деле, имеем $a0 = a(0+0) = a0 + a0$, откуда $0 = a0$. Аналогично устанавливается равенство $0a = 0$.

Замечание 2. Если кольцо R содержит более одного элемента, то $0 \neq 1$. Это следует из соотношений (1) и (2).

Примеры колец:

(1) числовые кольца $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$;
(2) кольцо $\mathbb{Z}_n$ вычетов по модулю n;
(3) кольцо $\mathrm{Mat}(n \times n, \mathbb{R})$ матриц с коэффициентами из $\mathbb{R}$;
(4) кольцо $\mathbb{R}[x]$ многочленов от переменной x с коэффициентами из $\mathbb{R}$;
(5) кольцо $\mathbb{R}[[x]]$ *формальных степенных рядов* от переменной x с коэффициентами из $\mathbb{R}$:

$$\mathbb{R}[[x]] := \{\sum_{i=0}^{\infty} a_i x^i \mid a_i \in \mathbb{R}\};$$

(6) кольцо $\mathcal{F}(M, \mathbb{R})$ всех функций из множества M во множество $\mathbb{R}$ с операциями поточечного сложения и умножения:

$$(f_1 + f_2)(m) := f_1(m) + f_2(m); \quad (f_1 f_2)(m) := f_1(m) f_2(m) \quad \text{для всех} \quad f_1, f_2 \in \mathcal{F}(M, \mathbb{R}), m \in M.$$

Замечание 3. В примерах (3)–(6) вместо $\mathbb{R}$ можно брать любое кольцо, в частности $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_n$.

Замечание 4. Обобщая пример (4), можно рассматривать кольцо $\mathbb{R}[x_1, \ldots, x_n]$ многочленов от нескольких переменных $x_1, \ldots, x_n$ с коэффициентами из $\mathbb{R}$.

Определение 2. Кольцо R называется *коммутативным*, если $ab = ba$ для всех $a, b \in R$.

Все перечисленные в примерах (1)–(6) кольца, кроме $\mathrm{Mat}(n \times n, \mathbb{R})$ при $n \geqslant 2$, коммутативны.

Пусть R — кольцо.

Определение 3. Элемент $a \in R$ называется *обратимым*, если найдётся такой $b \in R$, что $ab = ba = 1$.

Замечание 5. Все обратимые элементы кольца R образуют группу относительно операции умножения.

Определение 4. Элемент $a \in R$ называется *левым* (соответственно *правым*) *делителем нуля*, если $a \neq 0$ и найдётся такой $b \in R$, $b \neq 0$, что $ab = 0$ (соответственно $ba = 0$).

Замечание 6. В случае коммутативных колец понятия левого и правого делителей нуля совпадают, поэтому говорят просто о делителях нуля.

Замечание 7. Все делители нуля в R необратимы: если $ab = 0$, $a \neq 0$, $b \neq 0$ и существует a^{-1}, то получаем $a^{-1}ab = a^{-1}0$, откуда $b = 0$ — противоречие.

Определение 5. Элемент $a \in R$ называется *нильпотентом*, если $a \neq 0$ и найдётся такое $m \in \mathbb{N}$, что $a^m = 0$.

Замечание 8. Всякий нильпотент в R является делителем нуля: если $a \neq 0$, $a^m = 0$ и число m наименьшее с таким свойством, то $m \geqslant 2$ и $a^{m-1} \neq 0$, откуда $aa^{m-1} = a^{m-1}a = 0$.

Определение 6. Элемент $a \in R$ называется *идемпотентом*, если $a^2 = a$.

Определение 7. *Полем* называется коммутативное ассоциативное кольцо K с единицей, в котором всякий ненулевой элемент обратим.

Замечание 9. Тривиальное кольцо $\{0\}$ полем не считается, поэтому $0 \neq 1$ в любом поле.

Примеры полей: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Предложение 1. *Кольцо вычетов $\mathbb{Z}_n$ является полем тогда и только тогда, когда n — простое число.*

Доказательство. Если число n составное, то $n = mk$, где $1 < m, k < n$. Тогда $\overline{m}\overline{k} = \overline{n} = \overline{0}$. Следовательно, $\overline{k}$ и $\overline{m}$ — делители нуля в $\mathbb{Z}_n$, ввиду чего не все ненулевые элементы там обратимы.

Если $n = p$ — простое число, то возьмём произвольный ненулевой вычет $\overline{a} \in \mathbb{Z}_p$ и покажем, что он обратим. Рассмотрим вычеты

$$\overline{1}\overline{a}, \overline{2}\overline{a}, \ldots, \overline{(p-1)}\overline{a}. \tag{3}$$

Если $\overline{ra} = \overline{sa}$ при $1 \leqslant r, s \leqslant p-1$, то число $(r-s)a$ делится на p. В силу взаимной простоты чисел a и p получаем, что число $r-s$ делится на p. Тогда из условия $|r-s| \leqslant p-2$ следует, что $r = s$. Это рассуждение показывает, что все вычеты (3) попарно различны. Поскольку все они отличны от нуля, среди них должна найтись единица: существует такое $b \in \{1, \ldots, p-1\}$, что $\overline{b}\overline{a} = \overline{1}$. Это и означает, что вычет $\overline{a}$ обратим. □

Определение 8. *Алгеброй* над полем K (или кратко K-*алгеброй*) называется множество A с операциями сложения, умножения и умножения на элементы поля K, обладающими следующими свойствами:

1) относительно сложения и умножения на элементы из K множество A есть векторное пространство;

2) относительно сложения и умножения A есть кольцо;

3 $(\lambda a)b = a(\lambda b) = \lambda(ab)$ для любых $\lambda \in K$ и $a, b \in A$.

Размерностью алгебры A называется её размерность как векторного пространства над K. (Обозначение: $\dim_K A$.)

Примеры. 1) Алгебра матриц $\mathrm{Mat}(n \times n, K)$ над произвольным полем K. Её размерность равна n^2.
2) Алгебра $K[x]$ многочленов от переменной x над произвольным полем K. Её размерность равна ∞.

Определение 9. *Подкольцом* кольца R называется всякое подмножество $R' \subseteq R$, замкнутое относительно операций сложения и умножения (т. е. $a + b \in R'$ и $ab \in R'$ для всех $a, b \in R'$) и являющееся кольцом относительно этих операций. *Подполем* называется всякое подкольцо, являющееся полем.

Например, $\mathbb{Z}$ является подкольцом в $\mathbb{Q}$, а скалярные матрицы образуют подполе в кольце $\mathrm{Mat}(n \times n, \mathbb{R})$.

Замечание 10. Если K — подполе поля F, то F является алгеброй над K. Так, поле $\mathbb{C}$ является бесконечномерной алгеброй над $\mathbb{Q}$, тогда как над $\mathbb{R}$ имеет размерность 2.

Определение 10. *Подалгеброй* алгебры A (над полем K) называется всякое подмножество $A' \subseteq A$, замкнутое относительно всех трёх имеющихся в A операций (сложения, умножения и умножения на элементы из K) и являющееся алгеброй (над K) относительно этих операций.

Легко видеть, что подмножество $A' \subseteq A$ является алгеброй тогда и только тогда, когда оно является одновременно подкольцом и векторным подпространством в A.

Гомоморфизмы колец, алгебр определяются естественным образом как отображения, сохраняющие все операции.

Упражнение 1. Сформулируйте точные определения гомоморфизма колец и гомоморфизма алгебр.

Определение 11. *Изоморфизмом* колец, алгебр называется всякий гомоморфизм, являющийся биекцией.

В теории групп нормальные подгруппы обладают тем свойством, что по ним можно «факторизовать». В этом смысле аналогами нормальных подгрупп в теории колец служат идеалы.

Определение 12. Подмножество I кольца R называется (*двусторонним*) *идеалом*, если оно является подгруппой по сложению и $ra \in I$, $ar \in I$ для любых $a \in I$, $r \in R$.

Замечание 11. В некоммутативных кольцах рассматривают также левые и правые идеалы.

В каждом кольце R есть *несобственные* идеалы $I = 0$ и $I = R$. Все остальные идеалы называются *собственными*.

Упражнение 2. Пусть R — кольцо и I — идеал в R. Докажите, что следующие три условия эквивалентны:

(1) $I = R$;

(2) I содержит хотя бы один обратимый элемент;

(3) $I \ni 1$.

Пусть R — коммутативное кольцо. С каждым элементом $a \in R$ связан идеал $(a) := \{ra \mid r \in R\}$ (проверьте, что это действительно идеал!).

Определение 13. Идеал I называется *главным*, если существует такой элемент $a \in R$, что $I = (a)$. (В этой ситуации говорят, что I порождён элементом a.)

Пример. В кольце $\mathbb{Z}$ подмножество $k\mathbb{Z}$ ($k \in \mathbb{Z}$) является главным идеалом, порождённым элементом k. Более того, все идеалы в $\mathbb{Z}$ являются главными.

Замечание 12. Главный идеал (a) является несобственным тогда и только тогда, когда $a = 0$ или a обратим.

Более общо, с каждым подмножеством $S \subseteq R$ связан идеал

$$(S) := \{r_1a_1 + \ldots + r_ka_k \mid a_i \in S, r_i \in R, k \in \mathbb{N}\}.$$

(Проверьте, что это действительно идеал!) Это наименьший по включению идеал в R, содержащий подмножество S. В этой ситуации говорят, что идеал $I = (S)$ порождён подмножеством S.

Вернёмся к случаю произвольного кольца R. Поскольку любой идеал I является подгруппой абелевой группы $(R, +)$, мы можем рассмотреть факторгруппу R/I. Введём на ней умножение по формуле

$$(a + I)(b + I) := ab + I.$$

Покажем, что это определение корректно. Пусть элементы $a', b' \in R$ таковы, что $a'+I = a+I$ и $b'+I = b+I$. Проверим, что $a'b' + I = ab + I$. Заметим, что $a' = a + x$ и $b' = b + y$ для некоторых $x, y \in I$. Тогда

$$a'b' + I = (a + x)(b + y) + I = ab + ay + xb + xy + I = ab + I,$$

поскольку $ay, xb, xy \in I$ в силу определения идеала.

Упражнение 3. Проверьте, что множество R/I является кольцом относительно имеющейся там операции сложения и только что введённой операции умножения.

Определение 14. Кольцо R/I называется *факторкольцом* кольца R по идеалу I.

Пример. $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

Пусть $\varphi\colon R \to R'$ — гомоморфизм колец. Тогда определены его ядро $\operatorname{Ker}\varphi = \{r \in R \mid \varphi(r) = 0\}$ и образ $\operatorname{Im}\varphi = \{\varphi(r) \mid r \in R\} \subseteq R'$.

Лемма 1. *Ядро* $\operatorname{Ker}\varphi$ *является идеалом в* R.

Доказательство. Так как φ — гомоморфизм абелевых групп, то $\operatorname{Ker}\varphi$ является подгруппой в R по сложению. Покажем теперь, что $ra \in \operatorname{Ker}\varphi$ и $ar \in \operatorname{Ker}\varphi$ для произвольных элементов $a \in \operatorname{Ker}\varphi$ и $r \in R$. Имеем $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$, откуда $ra \in \operatorname{Ker}\varphi$. Аналогично получаем $ar \in \operatorname{Ker}\varphi$. □

Упражнение 4. Проверьте, $\operatorname{Im}\varphi$ — подкольцо в R'.

Теорема о гомоморфизме для колец. Пусть $\varphi\colon R \to R'$ – гомоморфизм колец. Тогда имеет место изоморфизм

$$R/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi.$$

Доказательство. Положим для краткости $I = \operatorname{Ker}\varphi$ и рассмотрим отображение

$$\pi\colon R/I \to \operatorname{Im}\varphi, \quad a + I \mapsto \varphi(a).$$

Из доказательства теоремы о гомоморфизме для групп следует, что отображение π корректно определено и является изоморфизмом абелевых групп (по сложению). Покажем, что π — изоморфизм колец. Для этого остаётся проверить, что π сохраняет операцию умножения:

$$\pi((a+I)(b+I)) = \pi(ab+I) = \varphi(ab) = \varphi(a)\varphi(b) = \pi(a+I)\pi(b+I).$$

□

Пример 1. Пусть $R = \mathcal{F}(M, \mathbb{R})$. Зафиксируем произвольную точку $m_0 \in M$ и рассмотрим гомоморфизм $\varphi\colon R \to \mathbb{R}$, $f \mapsto f(m_0)$. Ясно, что гомоморфизм φ сюръективен. Его ядром является идеал I всех функций, обращающихся в нуль в точке m_0. По теореме о гомоморфизме получаем $R/I \cong \mathbb{R}$.

Определение 15. Кольцо R называется *простым*, если в нём нет собственных (двусторонних) идеалов.

Пример. Всякое поле является простым кольцом.

Определение 16. *Центром* алгебры A над полем K называется её подмножество

$$Z(A) = \{a \in A \mid ab = ba \text{ для всех } b \in A\}.$$

Теорема 1. *Пусть K — поле, n — натуральное число и $A = \operatorname{Mat}(n \times n, K)$ — алгебра квадратных матриц порядка n над полем K.*

(1) *$Z(A) = \{\lambda E \mid \lambda \in K\}$, где E — единичная матрица (в частности, $Z(A)$ — одномерное подпространство в A);*

(2) *алгебра A проста (как кольцо).*

Доказательство. Для каждой пары индексов $i, j \in \{1, \ldots, n\}$ обозначим через E_{ij} соответствующую *матричную единицу* — такую матрицу, в которой на (i,j)-месте стоит единица, а на всех остальных местах — нули. Непосредственная проверка показывает, что

$$E_{ij}E_{kl} = \begin{cases} E_{il}, & \text{если } j = k; \\ 0, & \text{если } j \neq k. \end{cases}$$

Заметим, что матричные единицы образуют базис в A и всякая матрица $X = (x_{kl})$ представима в виде $X = \sum\limits_{k,l=1}^{n} x_{kl}E_{kl}$.

(1) Пусть матрица $X = \sum\limits_{k,l=1}^{n} x_{kl}E_{kl}$ лежит в $Z(A)$. Тогда X коммутирует со всеми матричными единицами. Выясним, что означает условие $XE_{ij} = E_{ij}X$. Имеем

$$XE_{ij} = (\sum_{k,l=1}^{n} x_{kl}E_{kl})E_{ij} = \sum_{k=1}^{n} x_{ki}E_{kj}; \qquad E_{ij}X = E_{ij}(\sum_{k,l=1}^{n} x_{kl}E_{kl}) = \sum_{l=1}^{n} x_{jl}E_{il}.$$

Сравнивая правые части двух равенств, получаем $x_{ii} = x_{jj}$, $x_{ki} = 0$ при $k \neq i$ и $x_{jl} = 0$ при $j \neq l$. Поскольку эти равенства имеют место при любых значениях i, j, мы получаем, что матрица X скалярна, т. е. $X = \lambda E$ для некоторого $\lambda \in K$. С другой стороны, ясно, что всякая скалярная матрица лежит в $Z(A)$.

(2) Пусть I — двусторонний идеал алгебры A. Если $I \neq \{0\}$, то I содержит ненулевую матрицу X. Покажем, что тогда $I = A$. Пусть индексы k, l таковы, что $x_{kl} \neq 0$. Тогда

$$E_{ik}XE_{lj} = E_{ik}(\sum_{p,q=1}^{n} x_{pq}E_{pq})E_{lj} = E_{ik}\sum_{p=1}^{n} x_{pl}E_{pj} = x_{kl}E_{ij} \in I.$$

Домножая $x_{kl}E_{ij}$ на скалярную матрицу $(x_{kl})^{-1}E$, мы получаем, что $E_{ij} \in I$. Из произвольности выбора i, j следует, что все матричные единицы лежат в I. Отсюда $I = A$, что и требовалось. □

Список литературы

[1] Э. Б. Винберг. Курс алгебры. М.: Факториал Пресс, 2002 (глава 1, § 3,4,6,8,9 и глава 9, § 2)

[2] А. И. Кострикин. Введение в алгебру. Основы алгебры. М.: Наука. Физматлит, 1994 (глава 4, § 3)

[3] А. И. Кострикин. Введение в алгебру. Основные структуры алгебры. М.: Наука. Физматлит, 2000 (глава 4, § 1,4)

[4] Сборник задач по алгебре под редакцией А. И. Кострикина. Новое издание. М.: МЦНМО, 2009 (глава 14, § 63–64)