Рекомендуемая литература по алгебре.

1. Ван-дер-Варден Б.Л. Современная алгебра.
2. Ленг С. Алгебра.
3. Кострикин А.И. Введение в алгебру.
4. Гельфанд И.М. Линейная алгебра.
5. Кострикин А.И., Манин Ю.И. Линейная алгебра.
6. Серр Ж.-П. Линейные представления конечных групп.
7. Серр Ж.-П. Курс арифметики.
8. Атья М., Макдональд. Коммутативная алгебра.

Часть 1. Моноиды и группы

Определение 1.1. Моноид — это тройка $(M, \circ, 1)$, состоящая из множества M, бинарной операции $\circ$ на M (т.е. отображения $M \times M \to M$, $(x, y) \mapsto x \circ y$) и элемента $e \in M$, таких что выполнены следующие свойства:

M1: Ассоциативность: $\forall x, y, z \in M \quad (x \circ y) \circ z = x \circ (y \circ z)$.
M2: Аксиома единицы: $\forall x \in M \quad x \circ e = e \circ x = x$.

Примеры 1.2.
1. $(\mathbb{Z}, +, 0)$ (варианты: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_{\geqslant 0}$, $\mathbb{Q}_{\geqslant 0}$, $\mathbb{R}_{\geqslant 0}$, $\mathbb{Z}/n\mathbb{Z}$, $\dots$).
2. $(\mathbb{Z}, \cdot, 1)$ (варианты: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_{\geqslant 0}$, $\mathbb{Q}_{\geqslant 0}$, $\mathbb{R}_{\geqslant 0}$, $\mathbb{Z}_{>0}$, $\mathbb{Q}_{>0}$, $\mathbb{R}_{>0}$, $\mathbb{Z}/n\mathbb{Z}$, $\dots$).
3. $M = \mathrm{Map}(X, X)$ — множество отображений из множества X в себя, $\circ$ — операция композиции отображений, $e = \mathrm{Id}_X$ — тождественное отображение.
4. $M = \mathrm{Map}(X, M')$ — множество отображений из множества X в моноид M', $\circ$ — поточечное умножение ($(f \circ g)(x) = f(x) \circ' g(x)$, где $\circ'$ — операция в M'), $e \equiv e'$ — функция, тождественно равная единице моноида M'.

Легко убедиться, что единица во всяком моноиде единственна. Действительно, если e' — другая единица, то $e' = e' \cdot e = e$. Поэтому при задании моноида можно не указывать его единицу — достаточно лишь проверить ее существование.

Лемма 1.3. *Если $x_1, \dots, x_n$ — элементы моноида, то все способы расстановки скобок в произведении $x_1 \circ \dots \circ x_n$ дают одинаковый результат.*

Доказательство — индукция по n.

Определение 1.4. Моноид M называется коммутативным, если $\forall x, y \in M \quad x \circ y = y \circ x$.

Как правило, в коммутативных моноидах операция записывается аддитивно ($x \circ y =: x + y$), а в некоммутативных мультипликативно ($x \circ y =: xy$).

Произведение n одинаковых элементов $x \circ \dots \circ x$ обозначается через x^n, при этом удобно положить $x^0 = e$. Легко проверить, что

$$x^n \circ x^m = x^{n+m} \tag{1.5}$$

для всех неотрицательных m и n. При аддитивной записи операции в моноиде пользуются обозначением nx вместо x^n. При этом свойство (1.5) приобретает вид $nx + mx = (n + m)x$.

Элемент x в моноиде M называется обратимым, если существуют элемент y (левый обратный), такой что $y \circ x = e$; и элемент z (правый обратный), такой что $x \circ z = e$.

Лемма 1.6. *Если x — обратим, то всякий левый обратный к x равен всякому правому обратному к x.*

Доказательство: $y = y \circ e = y \circ (x \circ z) = (y \circ x) \circ z = e \circ z = z$.

Тем самым, для любого обратимого элемента x существует единственный элемент, являющийся одновременно правым и левым обратным к x. Этот элемент обозначается x^{-1} (при аддитивной записи: $-x$) и называется обратным к x. Далее, удобно обозначить $(x^{-1})^n$ через x^{-n} (при аддитивной записи $-nx$). Тогда свойство (1.5) становится верным при любых целых n и m.

Определение 1.7. Группа — это моноид, в котором все элементы обратимы.

Лемма 1.8. *Если M — моноид, то множество M^* обратимых элементов в M является группой.*

Доказательство: Достаточно проверить, что множество M^* замкнуто относительно операции $\circ$, то есть что для любых обратимых элементов $x, y \in M$ произведение $x \circ y$ — тоже обратимо. Действительно, ясно, что

$$(x \circ y) \circ (y^{-1} \circ x^{-1}) = (y^{-1} \circ x^{-1}) \circ (x \circ y) = e,$$

то есть элемент $y^{-1} \circ x^{-1}$ является обратным к $x \circ y$. $\square$

Примеры 1.9. 1. $\mathbf{1} = \{ e \}$.
2. $(\mathbb{Z}, +)$ (варианты: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}, \ldots$).
3. $(\mathbb{Q}^*, \cdot)$ (варианты: $\mathbb{R}^*$, $\mathbb{C}^*$, $(\mathbb{Z}/n\mathbb{Z})^*$ $\mathbb{Q}_{>0}$, $\mathbb{R}_{>0}$, $\mu_n = \{ z \in \mathbb{C} \mid z^n = 1 \}$, $\mathbf{S}^1 = \{ z \in \mathbb{C} \mid |z| = 1 \}, \ldots$).
4. Группа перестановок (симметрическая группа) $\mathfrak{S}_n$ — множество изоморфизмов из n-элементного множества $\{ 1, \ldots, n \}$ на себя с операцией композиции отображений.
5. $G = \mathrm{Map}(X, G')$ — множество отображений из множества X в группу G'.
6. Группы автоморфизмов (см. лемму 3.5).

Лемма 1.10. *Если в группе G выполнено одно из равенств $x \circ y = x \circ z$ или $y \circ x = z \circ x$, то $y = z$.*

Доказательство: если $x \circ y = x \circ z$, то $y = e \circ y = (x^{-1} \circ x) \circ y = x^{-1} \circ (x \circ y) = x^{-1} \circ (x \circ z) = (x^{-1} \circ x) \circ z = e \circ z = z$. Второй случай разбирается аналогично.

Группа называется коммутативной, если она коммутативна как моноид. Коммутативные группы также называются абелевыми.

Часть 2. Кольца и поля

Определение 2.1. Кольцо— это набор $(R, +, \cdot, 0, 1)$, состоящий из множества R, бинарных операций $+$ (сложение) и $\cdot$ (умножение) на R и элементов $0, 1 \in R$, таких что выполнены следующие свойства:

R1: $(R, +, 0)$ — абелева группа.
R2: $(R, \cdot, 1)$ — моноид.
R3: Дистрибутивность (билинейность) умножения: $\forall x, y, z \in R \quad x \cdot (y+z) = x \cdot y + x \cdot z$, $(x+y) \cdot z = x \cdot z + y \cdot z$.

Умножение в кольце часто записывают в виде $xy = x \cdot y$. Кольцо называется коммутативным, если коммутативна операция умножения.

Примеры 2.2. 1. $\{ 0 \}$.
2. $\mathbb{Z}$ (варианты: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}, \ldots$).
3. $R = \mathrm{Map}(X, R')$ — множество отображений из множества X в кольцо R' с поточечными операциями.
4. $R = R'[x] = \{ a_n x^n + \cdots + a_1 x + a_0 \mid a_0, \ldots, a_n \in R' \}$ — кольцо многочленов (полиномов) с коэффициентами в кольце R'.
5. $R = R'[[x]] = \{ a_0 + a_1 x + \cdots + a_n x^n + \ldots \mid a_0, \ldots, a_n \in R' \}$ — кольцо формальных степенных рядов с коэффициентами в кольце R'.
6. $R = \mathrm{Mat}_{n \times n}(R')$ — кольцо матриц размера n на n с коэффициентами в кольце R'. Элементы R — это таблицы вида $\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}$, $a_{ij} \in R'$ с покомпонентным сложением; умножением, задаваемым формулой

$$\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & \ldots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \ldots & b_{nn} \end{pmatrix} = \begin{pmatrix} c_{11} & \ldots & c_{1n} \\ \vdots & \ddots & \vdots \\ c_{n1} & \ldots & c_{nn} \end{pmatrix}, \text{ где } c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \tag{2.3}$$

нулевой матрицей в качестве 0 и диагональной матрицей с единицами на диагонале в качестве 1.

7. Кольца эндоморфизмов (см. лемму 3.5).

Лемма 2.4. *Если R — кольцо, то* $\forall x \in R \quad 0 \cdot x = x \cdot 0 = 0.$

Доказательство: $0 + 0 \cdot x = 0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$ и остается применить лемму 1.10 к аддитивной группе кольца.

Определение 2.5. Кольцо, в котором $0 \neq 1$ и все элементы кроме нуля являются группой относительно умножения, называется **телом**, а если оно к тому же коммутативно, то **полем**.

Некоммутативные тела встречаются достаточно редко; простейший пример — тело кватернионов $\mathbb{H}$. С полями дело обстоит значительно лучше.

Примеры 2.6. Примеры полей.

1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$,
2. $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, где p — простое число.
3. $\mathbb{Q}[i] = \{\, x + yi \in \mathbb{C} \mid x, y \in \mathbb{Q} \,\}, \mathbb{Q}[\sqrt{2}] = \{\, x + y\sqrt{2} \in \mathbb{R} \mid x, y \in \mathbb{Q} \,\}$.
4. $K = K'(x) = \left\{ \dfrac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x],\ g(x) \not\equiv 0 \right\}$ — поле рациональных функций с коэффициентами в поле K'.
5. $K = K'((x)) = \{\, a_{-n}x^{-n} + \cdots + a_{-1}x^{-1} + a_0 + a_1 x + \cdots + a_n x^n + \ldots \mid a_i \in K' \,\}$ — поле (формальных) рядов Лорана с коэффициентами в поле K'.

Часть 3. Гомоморфизмы

Определение 3.1. Гомоморфизм групп (моноидов) $f : G \to G'$ — это отображение, такое что $f(e) = e'$ и $\forall x, y \in G \quad f(x \circ y) = f(x) \circ' f(y)$. Гомоморфизм колец (полей) $f : R \to R'$ — это отображение, являющееся гомоморфизмом их аддитивной группы и мультипликативного моноида.

Примеры 3.2.

1. Если G — группа, а $x \in G$, то отображение $n \mapsto x^n$ является гомоморфизмом групп $\mathbb{Z} \to G$.
2. Если R — кольцо, а $x \in R$, то отображение $n \mapsto nx := x + \cdots + x$ является гомоморфизмом колец $\mathbb{Z} \to R$.
3. Проекция $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ является гомоморфизмом колец.
4. Отображения $\exp : \mathbb{R} \to \mathbb{R}_{>0}$, $\exp : \mathbb{C} \to \mathbb{C}^*$ и $\ln : \mathbb{R}_{>0} \to \mathbb{R}$ являются гомоморфизмами групп.
5. Отображение вычисления $ev_x : \mathrm{Map}(X, G) \to G,\ f \mapsto f(x)$ является гомоморфизмом групп.
6. Если R — коммутативное кольцо, и $r \in R$, то отображение вычисления $ev_r : R[x] \to R$, $a_n x^n + \cdots + a_1 x + a_0 \mapsto a_n r^n + \cdots + a_1 r + a_0$ является гомоморфизмом колец.
7. Всякий элемент кольца R можно рассматривать как многочлен степени 0, а всякий многочлен можно рассматривать как формальный степенной ряд, все члены которого, начиная с некоторого места равны нулю. Тем самым задаются гомоморфизмы колец $R \to R[x]$ и $R[x] \to R[[x]]$.

Лемма 3.3. *Композиция гомоморфизмов является гомоморфизмом. Если $f : M \to M'$ — гомоморфизм моноидов, а $x \in M$ — обратимый элемент, то $f(x) \in M'$ — обратим и $f(x)^{-1} = f(x^{-1})$.*

Доказательство: $f(g(x \circ y)) = f(g(x) \circ g(y)) = f(g(x)) \circ f(g(y))$, откуда следует первая часть леммы. Для доказательства второй части достаточно заметить, что $f(x^{-1}) \circ f(x) = f(x^{-1} \circ x) = f(e) = e'$, $f(x) \circ f(x^{-1}) = f(x \circ x^{-1}) = f(e) = e'$, то есть $f(x^{-1}) = f(x)^{-1}$. □

Гомоморфизм (моноидов, групп, колец, полей, и т.д.) $f : M \to M'$ называется **эпиморфизмом** (сюръекцией, наложением), если $\forall z \in M'\ \exists x \in M$ т.ч. $f(x) = z$. Гомоморфизм f называется **мономорфизмом** (инъекцией, вложением), если из равенства $f(x) = f(y)$, $x, y \in M$, следует $x = y$. Гомоморфизм $f : M \to M'$ называется **изоморфизмом**, если существует гомоморфизм $g : M' \to M$, такой что $g \circ f = \mathrm{Id}_M$, $f \circ g = \mathrm{Id}_{M'}$.

Лемма 3.4. *Гомоморфизм групп (колец) является изоморфизмом $\Longleftrightarrow$ он является одновременно мономорфизмом и эпиморфизмом.*

Доказательство: всякий изоморфизм биективен, следовательно является мономорфизмом и эпиморфизмом. Обратно, если гомоморфизм является мономорфизмом и эпиморфизмом одновременно, то он биективен, следовательно существует обратное отображение, которое (легко проверить) является гомоморфизмом. $\square$

Всякий гомоморфизм из (моноида, группы, кольца, поля, и т.д.) в себя называется **эндоморфизмом**. Эндоморфизм, являющийся изоморфизмом, называется **автоморфизмом**.

Лемма 3.5. *Если M — любая алгебраическая структура (моноид, группа, кольцо, поле), то множество его автоморфизмов $\mathrm{Aut}(M)$ является группой. Если M — абелева группа, то множество ее эндоморфизмов $\mathrm{End}(M)$ является кольцом.*

Доказательство: из леммы 3.3 следует, что $\mathrm{End}(M)$ является моноидом относительно операции композиции эндоморфизмов, а $\mathrm{Aut}(M)$ является множеством его обратимых эментов, следовательно $\mathrm{Aut}(M)$ — группа. Если же M является абелевой группой, то на $\mathrm{End}(M)$ есть операция поточечного сложения ($(f+g)(x) := f(x)+g(x)$), так что $\mathrm{End}(M)$ становится кольцом. $\square$

Определение 3.6. Ядром гомоморфизма групп $f : G \to G'$ называется $\mathrm{Ker}\, f = \{\, x \in G \mid f(x) = e' \,\}$. Образом гомоморфизма групп $f : G \to G'$ называется $\mathrm{Im}\, f = \{\, y \in G' \mid y = f(x), x \in G \,\}$. Аналогично, ядром гомоморфизма колец $f : R \to R'$ называется $\mathrm{Ker}\, f = \{\, x \in R \mid f(x) = 0 \,\}$. Образом гомоморфизма колец $f : R \to R'$ называется $\mathrm{Im}\, f = \{\, y \in R' \mid y = f(x), x \in R \,\}$.

Легко видеть, что ядро и образ гомоморфизма групп $f : G \to G'$ являются **подгруппами** (то есть подмножествами, являющимися группами относительно индуцированной операции) в G и G' соотв. Аналогично, ядро и образ гомоморфизма колец $f : R \to R'$ являются **подкольцами** (то есть подмножествами, являющимися кольцами относительно индуцированных операций) в R и R' соотв.

Лемма 3.7. *Гомоморфизм f групп (колец) является мономорфизмом $\iff \mathrm{Ker}\, f = \{\, e \,\}$ ($\mathrm{Ker}\, f = \{\, 0 \,\}$ соотв.). Гомоморфизм моноидов $f : M \to M'$ является эпиморфизмом $\iff \mathrm{Im}\, f = M'$.*

Доказательство: пусть $f : M \to M'$ — гомоморфизм групп и $f(x) = f(y)$. Тогда $f(x^{-1} \circ y) = f(x^{-1}) \circ f(y) = f(x)^{-1} \circ f(y) = (f(y))^{-1} \circ f(y) = e'$, следовательно $x^{-1} \circ y \in \mathrm{Ker}\, f$. Далее очевидно.

Следствие 3.8. *Любой гомоморфизм из поля в кольцо является вложением.*

Доказательство: по лемме 3.3 любой обратимый элемент поля (относительно мультипликативной структуры) переходит в обратимый элемент. Следовательно, всякий ненулевой элемент переходит не в ноль. В частности, ядро гомоморфизма равно нулю, следовательно гомоморфизм — вложение. $\square$

Часть 4. Прямые произведения

Пусть $(M_1, \circ_1, e_1)$ и $(M_2, \circ_2, e_2)$ — моноиды. Тогда на произведении $M_1 \times M_2 = \{\, (x_1, x_2) \mid x_1 \in M_1,\ x_2 \in M_2 \,\}$ возникает структура моноида:

$$(x_1, x_2) \circ (y_1, y_2) = (x_1 \circ y_1, x_2 \circ y_2), \qquad e = (e_1, e_2).$$

Этот моноид называется **прямым произведением** моноидов M_1 и M_2.

Лемма 4.1. *Произведение групп (колец) является группой (кольцом).*

Доказательство: очевидно.

Напротив, легко проверить, что произведение полей является кольцом, но не полем. Действительно, в произведении полей $K \times L$ имеем

$$(1_K, 0_L) \cdot (0_K, 1_L) = (1_K \cdot 0_K, 0_L \cdot 1_L) = (0_K, 0_L),$$

следовательно элементы $(1_K, 0_L)$ и $(0_K, 1_L)$ необратимы.