Московский педагогический
государственный университет

Л. М. Цыбуля, Е. Е. Ширшова

АЛГЕБРА:
ОСНОВНЫЕ СТРУКТУРЫ АЛГЕБРЫ, ЛИНЕЙНАЯ АЛГЕБРА

Москва
2022

Министерство просвещения Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский педагогический государственный университет»

Л. М. Цыбуля, Е. Е. Ширшова

Алгебра: основные структуры алгебры, линейная алгебра

Курс лекций

Учебное пособие

МПГУ
Москва • 2022

УДК 512(075.8)
ББК 22.14я73-2
Ц938

Рецензенты:

А. А. Фомин, профессор, доктор физико-математических наук, заведующий кафедрой алгебры Московского педагогического государственного университета

И. А. Пинчук, доцент, кандидат физико-математических наук, доцент кафедры высшей алгебры, элементарной математики и методики преподавания математики Московского государственного областного университета

Цыбуля, Лилия Михайловна.

Ц938 Алгебра: основные структуры алгебры, линейная алгебра. Курс лекций : учебное пособие / Л. М. Цыбуля, Е. Е. Ширшова. — Москва : МПГУ, 2022. — 112 с.

ISBN 978-5-4263-1058-2

Учебное пособие содержит конспективное изложение части основного курса алгебры в соответствии с Федеральным государственным образовательным стандартом высшего образования, а также перечнем профессиональных компетенций, установленных в качестве обязательных. В пособии отражены темы: основные алгебраические структуры, действия над матрицами, линейные и евклидовы пространства, линейные отображения и действия над ними.

Пособие подготовлено на кафедре алгебры МПГУ и предназначено для студентов учреждений высшего образования, изучающих математические дисциплины.

УДК 512(075.8)
ББК 22.14я73-2

ISBN 978-5-4263-1058-2

Оглавление

Предисловие

Предлагаемое пособие является второй частью курса лекций по дисциплине «Алгебра». Оно логически продолжает материал первой части «Алгебра: системы линейных уравнений, арифметические пространства, многочлены с комплексными коэффициентами» и существенно на него опирается. Если читатель не знаком с указанным пособием, то необходимые сведения он может найти в одном из учебников, перечисленных в списке литературы.

В начале данного пособия вводятся основные структуры алгебры: группы, кольца и поля. Изучение этих понятий основывается на рассмотренных ранее свойствах числовых множеств, функций, арифметических векторов, комплексных чисел, многочленов. Определяется понятие неприводимости многочленов над полями, исследуются свойства отношения сравнимости по модулю таких многочленов, что позволяет строить примеры нечисловых полей. Далее излагаются свойства кольца матриц над полем, на которых в дальнейшем базируются новые методы решения систем линейных уравнений.

Изучение основ линейной алгебры опирается на хорошо известное из первой части курса лекций понятие арифметического пространства. Это позволяет сэкономить время для изучения скалярного произведения векторов и свойств линейных отображений (операторов). Раздел линейных операторов тесно связан с действиями над матрицами. На множестве всех обратимых линейных операторов вводится структура мультипликативной группы, так называемой полной линейной группы — примера группы, важного для многих разделов математики.

Авторы стремились избегать излишней формализации, поэтому часто выбирали технически несложные доказательства. Пособие снабжено большим количеством подробно разобранных примеров и решений задач. Оно может быть использовано как для чтения лекций и проведения практических занятий, так и для самостоятельного изучения.

Искренне благодарим своих коллег, которые способствовали написанию данного пособия.

1. Основные алгебраические структуры

1.1. Бинарная операция

Нам понадобятся понятия функции и декартова квадрата множества. Пусть далее $A \neq \varnothing$.

Определение 1.1.1. *Бинарной операцией* на множестве A называется любая функция $f : A \times A \to A$.

Другими словами:

Бинарная операция — закон, по которому каждой упорядоченной паре элементов множества ставится в соответствие единственный третий элемент того же множества.

Если функция f существует, то говорят, что

на множестве задана бинарная операция, или, что множество замкнуто относительно операции f.

Функцию обозначают кружочком, звездочкой, плюсом, точкой и т.д.

Примеры.

1) Сложение на $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ является бинарной операцией.

2) Вычитание не является бинарной операцией на множестве $\mathbb{N}$, но является бинарной операцией на множестве $\mathbb{Z}$.

3) Умножение на множестве корней n-й степени из единицы является бинарной операцией.

4) Композиция (умножение) подстановок является бинарной операцией.

5) Рассмотрим множество классов вычетов $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$.

Положим $\overline{a} + \overline{b} = \overline{a+b}$. Покажем, что определение корректно.

Пусть $a \equiv c \pmod m$ и $b \equiv d \pmod m$.

Сравнения по одному модулю можно складывать, поэтому
$a + c \equiv b + d \pmod m$, т.е. $\overline{a+c} = \overline{b+d}$.

Вывод: *сложение классов вычетов является бинарной операцией.*

Положим $\overline{a} \cdot \overline{b} = \overline{ab}$. Покажем, что определение корректно.

Пусть $a \equiv c \pmod m$ и $b \equiv d \pmod m$.

Так как сравнения по одному модулю можно умножать,
то $ac \equiv bd \pmod m$, т.е. $\overline{ac} = \overline{bd}$.

Вывод: *умножение классов вычетов является бинарной операцией.*

Пусть на множестве A задана бинарная операция «умножение».

Определение 1.1.2. Элемент $e \in A$ называется *единицей*, если для всякого элемента $a \in A$ имеют место равенства $e \cdot a = a \cdot e = a$.

Примеры. 1) 0 — единица сложения, а 1 — единица умножения чисел.

2) Для операции вычитания не существует единицы.

3) Тождественная подстановка — единица умножения подстановок.

4) $\overline{0}$ — единица сложения, а $\overline{1}$ — единица умножения классов вычетов.

Предложение 1.1.1. Если единица есть, то она одна.

Доказательство. Пусть e, f — единицы множества A. Тогда $e = e \cdot f = f$. □

Определение 1.1.3. Если для любых элементов $a, b, c \in A$ имеет место равенство

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

то говорят, что *операция ассоциативна.*

Примеры. 1) Сложение и умножение чисел ассоциативны.

2) Вычитание не подчиняется ассоциативному закону. Например,

$$(5 - 2) - 3 = 0 \neq 6 = 5 - (2 - 3).$$

3) Умножение подстановок ассоциативно.

4) Так как сложение и умножение классов вычетов сводится к сложению и умножению целых чисел, то обе операции ассоциативны.

$$(\overline{a} + \overline{b}) + \overline{c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \overline{a} + (\overline{b} + \overline{c}).$$
$$(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a} \cdot (\overline{b} \cdot \overline{c}).$$

Теорема 1.1.1. Если операция «точка» в множестве A ассоциативна, то произведение любого конечного числа элементов множества A не зависит от расстановки скобок.

Доказательство. Пусть $a_1, a_2, \ldots, a_n$ — элементы множества A.

Докажем теорему методом математической индукции по числу n сомножителей в произведении.

1) При $n = 3$ теорема верна в силу ассоциативного закона.

2) Допустим, что утверждение теоремы справедливо для всех произведений, содержащих меньше, чем n сомножителей.

3) Рассмотрим произведение $a_1a_2\dots a_n$.

Расставим всевозможными способами скобки последнего умножения.

$$b_1 = a_1(a_2a_3\dots a_n), b_2 = (a_1a_2)(a_3\dots a_n), \dots,$$
$$b_k = (a_1a_2\dots a_k)(a_{k+1}\dots a_n), \dots,$$
$$b_{n-1} = (a_1\dots a_{n-1})a_n.$$

Заметим, что внутри скобок можно применить индуктивное предположение.

Рассмотрим

$$b_k = (a_1a_2\dots a_k)(a_{k+1}\dots a_n).$$

Так как в первой скобке меньше, чем n сомножителей, то можно применить индуктивное предположение, поставим скобку

$$b_k = \big((a_1a_2\dots a_{k-1})a_k\big)(a_{k+1}\dots a_n) = (ua_k)v.$$

Применим ассоциативный закон и индуктивное предположение, получим

$$b_k = u(a_kv) = (a_1a_2\dots a_{k-1})\big(a_k(a_{k+1}\dots a_n)\big) =$$
$$= (a_1a_2\dots a_{k-1})(a_k\dots a_n) = b_{k-1}.$$

Таким образом, $b_i = b_{i-1}$ для всех $i = 2, 3, \dots, n$. □

Определение 1.1.4. Если для любых элементов $a, b \in A$ справедливо равенство $ab = ba$, говорят, что *операция умножения коммутативна.*

Примеры. 1) Сложение и умножение чисел коммутативны.

2) Сложение и умножение классов вычетов коммутативны.

3) Умножение подстановок не подчиняется коммутативному закону. Например,

$$(12)(123) = (13) \neq (23) = (123)(12).$$

Определение 1.1.5. Пусть множество A содержит единицу. Тогда элемент $a' \in A$ называют *обратным* элементу $a \in A$, если

$$a' \cdot a = a \cdot a' = e.$$

Предложение 1.1.2. Если у элемента a из множества A с ассоциативной операцией и единицей существует обратный элемент, то он является единственным.

Доказательство. Пусть a', a'' — обратные к элементу a элементы в множестве A. Тогда

$$a' = a' \cdot e = a' \cdot (a \cdot a'') = (a' \cdot a) \cdot a'' = e \cdot a'' = a''.$$

□

Теперь можно обозначить обратный элемент символом a^{-1}.

1.2. Основные свойства групп

Определение 1.2.1. *Группа* — множество G с одной ассоциативной бинарной операцией, содержащее единицу и с каждым своим элементом — обратный к этому элементу.

Если операция в группе обозначается точкой и называется умножением, то группа называется *мультипликативной*.

Если операция в группе обозначается плюсом и называется сложением, то группа называется *аддитивной*.

В этом случае единицу называют *нулем* и обозначают 0, а обратный элемент к элементу a называют *противоположным* и обозначают $-a$.

Группа с коммутативной операцией называется *коммутативной* или *абелевой*.

Если множество конечно, то группа называется *конечной* и пишут $|G| < \infty$.

Число $|G|$ элементов группы называют ее *порядком*.

Если множество G бесконечно, говорят о группе *бесконечного порядка*.

Примеры. 1) Существуют бесконечные аддитивные группы целых, рациональных, действительных и комплексных чисел и одноэлементная аддитивная группа $\{0\}$.

2) Существуют бесконечные мультипликативные группы положительных рациональных и положительных действительных чисел и конечные мультипликативные группы: $\{1\}$; $\{-1, 1\}$; группы корней n-й степени из единицы.

3) Множество линейных функций

$$G = \{f \mid f : \mathbb{R} \to \mathbb{R}, \quad f(x) = ax + b,\ a \neq 0\}$$

образует мультипликативную группу, если за умножение взять композицию функций.

Пусть

$$f, g \in G, \quad f(x) = ax + b, \quad g(x) = cx + d, \quad a \neq 0, \quad c \neq 0.$$

Тогда

$$fg(x) = g \circ f(x) = g(f(x)) = g(ax + b) = c(ax + b) + d = (ca)x + (cb + d).$$

Так как $ca \neq 0$, то $fg \in G$.

Нам известно, что композиция функций на одном множестве ассоциативна.

Если $fg(x) = f(x)$, то $ca = a$ и $cb + d = b$. Отсюда следует, что $c = 1$ и $d = 0$, т.е. функция x играет роль единицы.

Если $fg = x$, то $ca = 1$ и $cb + d = 0$. Значит, $c = a^{-1}$ и $d = -a^{-1}b$, т.е. $f^{-1} = a^{-1}x - a^{-1}b$.

Проверим,

$$ff^{-1}(x) = f(a^{-1}x - a^{-1}b) = a(a^{-1}x - a^{-1}b) + b = x.$$

Группы первых двух примеров абелевы, а группа функций нет.

Рассмотрим, например, $f(x) = 5x + 2$ и $g(x) = 7x - 3$.

$$fg(x) = 7(5x + 2) - 3 = 35x + 11 \neq 35x - 13 = 5(7x - 3) + 2 = gf(x).$$

4) Классы вычетов по модулю числа образуют абелеву аддитивную группу.

Рассмотрим

$$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}.$$

Составим таблицу сложения.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Предложение 1.2.1. Подстановки n-й степени образуют (некоммутативную при $n > 2$) мультипликативную группу S_n, называемую симметрической группой n-й степени.