Федеральное агентство по образованию
Уральский государственный экономический университет

Ю. Б. Мельников

Алгебраические операции. Алгебры

Раздел **электронного учебника**
для сопровождения лекции

Изд. 2-е, испр. и доп.

e-mail: melnikov@k66.ru,
melnikov@r66.ru
сайты:
http://melnikov.k66.ru,
http://melnikov.web.ur.ru

Екатеринбург
2009

I Понятие алгебраической операции **4**

II Некоторые типы алгебраических операций **27**

III Некоторые классические алгебры **34**

III.1 Группоид 36
III.2 Полугруппа 38
III.3 Группа 39
III.4 Примеры группоидов, полугрупп и групп 41
III.5 Абелевы (коммутативные) группы 51
III.6 Неабелевы (некоммутативные) группы 54
III.7 Об ограничении операции на подмножество 58
III.8 Дистрибутивность 64
III.9. Кольцо 65

III.10Тело 77
III.11Поле 78
III.12Об идентификации алгебры по ее носителю 81

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Как найти ответ на этот вопрос?

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Как найти ответ на этот вопрос?

1) Дедуктивный вариант: найти определение в учебнике, энциклопеции и др.

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Как найти ответ на этот вопрос?

1) Дедуктивный вариант: найти определение в учебнике, энциклопеции и др. **Неинтересно.**

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Как найти ответ на этот вопрос?

1) Дедуктивный вариант: найти определение в учебнике, энциклопеции и др. **Неинтересно.**

2) Индуктивный вариант: рассмотреть примеры и попытаться формализовать результат в виде определения.

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Как найти ответ на этот вопрос?

1) Найти определение в учебнике, энциклопеции и др. **Неинтересно.**

2) Индуктивный вариант: рассмотреть примеры и попытаться формализовать результат в виде определения.

Такое учебное исследование гораздо полезнее, а результат усваивается лучше.

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Рассмотрим для примера операцию сложения целых чисел.

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Рассмотрим для примера операцию сложения целых чисел.

Конкретизируем ситуацию:

$2 + 3 = 5$;

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Рассмотрим для примера операцию сложения целых чисел.

Конкретизируем ситуацию:

$2 + 3 = 5;$

$4 + 7 = 11;$

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Рассмотрим для примера операцию сложения целых чисел.

Конкретизируем ситуацию:

$2 + 3 = 5$;

$4 + 7 = 11$;

$\bullet + \bullet = \bullet$.

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Рассмотрим для примера операцию сложения целых чисел.

Конкретизируем ситуацию:

$2 + 3 = 5$;

$4 + 7 = 11$;

$\bullet + \bullet = \bullet$.

Формализуем:

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Рассмотрим для примера операцию сложения целых чисел.

Конкретизируем ситуацию:

$2 + 3 = 5$;

$4 + 7 = 11$;

$\bullet + \bullet = \bullet$.

Формализуем: паре чисел — слагаемых суммы — мы сопоставляем число.

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Рассмотрим для примера операцию сложения целых чисел.

Конкретизируем ситуацию:

$2 + 3 = 5$;

$4 + 7 = 11$;

$\bullet + \bullet = \bullet$.

Формализуем: паре чисел — слагаемых суммы — мы сопоставляем число.

Какая стандартная математическая конструкция описывает такую ситуацию?

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Рассмотрим для примера операцию сложения целых чисел.

Конкретизируем ситуацию:

$2 + 3 = 5$;

$4 + 7 = 11$;

$\bullet + \bullet = \bullet$.

Формализуем: паре чисел — слагаемых суммы — мы сопоставляем число.

Какая стандартная математическая конструкция описывает такую ситуацию?

Понятие **функция**!

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Рассмотрим для примера операцию сложения целых чисел.

Конкретизируем ситуацию:

$2 + 3 = 5$;

$4 + 7 = 11$;

$\bullet + \bullet = \bullet$.

Формализуем: паре чисел — слагаемых суммы — мы сопоставляем число.

Какая стандартная математическая конструкция описывает такую ситуацию?

Понятие **функция**! Всегда ли у этой функции два аргумента?

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Рассмотрим для примера операцию сложения целых чисел.

Конкретизируем ситуацию:

$2 + 3 = 5$;

$4 + 7 = 11$;

$\bullet + \bullet = \bullet$.

Формализуем: паре чисел — слагаемых суммы — мы сопоставляем число.

Какая стандартная математическая конструкция описывает такую ситуацию?

Понятие **функция**! Всегда ли у этой функции два аргумента?

Нет, например, у операции

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Рассмотрим для примера операцию сложения целых чисел.

Конкретизируем ситуацию:

$2 + 3 = 5$;

$4 + 7 = 11$;

$\bullet + \bullet = \bullet$.

Формализуем: паре чисел — слагаемых суммы — мы сопоставляем число.

Какая стандартная математическая конструкция описывает такую ситуацию?

Понятие **функция**! Всегда ли у этой функции два аргумента?

Нет, например, у операции $(-x)$ *один аргумент.*

I Понятие алгебраической операции

Что такое «алгебраическая операция»?

Рассмотрим для примера операцию сложения целых чисел.

Конкретизируем ситуацию:

$2 + 3 = 5$;

$4 + 7 = 11$;

$\bullet + \bullet = \bullet$.

Формализуем: паре чисел — слагаемых суммы — мы сопоставляем число.

Какая стандартная математическая конструкция описывает такую ситуацию?

Понятие **функция**! Всегда ли у этой функции два аргумента?

Нет, например, у операции $(-x)$ *один аргумент.*

Получаем определение.

I Понятие алгебраической операции

Определение 1. *n-местной или n-арной* **алгебраической операцией** *на непустом множестве Ω называется* ***функция*** *с областью определения $\underbrace{\Omega \times \Omega \times \ldots \times \Omega}_{n \text{ множителей}}$, область значений которой включается в Ω.*

I Понятие алгебраической операции

Определение 1. *n-местной или n-арной* **алгебраической операцией** *на непустом множестве Ω называется* ***функция*** *с областью определения $\underbrace{\Omega \times \Omega \times \ldots \times \Omega}_{n \text{ множителей}}$, область значений которой включается в Ω.*

Например, операция сложения целых чисел отображает $\mathbb{Z} \times \mathbb{Z}$ в $\mathbb{Z}$, она *паре* целых чисел a, b ставит в соответствие целое число $a + b$.

I Понятие алгебраической операции

Определение 1. *n-местной или n-арной* **алгебраической операцией** *на непустом множестве Ω называется* ***функция*** *с областью определения $\underbrace{\Omega \times \Omega \times \ldots \times \Omega}_{n \text{ множителей}}$, область значений которой включается в Ω.*

Какие виды алгебраических операций наиболее интересны для изучения?

I Понятие алгебраической операции

Определение 1. *n-местной или n-арной* **алгебраической операцией** *на непустом множестве Ω называется* ***функция*** *с областью определения $\underbrace{\Omega \times \Omega \times \ldots \times \Omega}_{n \text{ множителей}}$, область значений которой включается в Ω.*

Какие виды алгебраических операций наиболее интересны для изучения?

Во-первых, в соответствии со стратегией приоритетного изучения экстремальных ситуаций наиболее интересны операции с экстремальным количеством операндов.

I Понятие алгебраической операции

Определение 1. *n-местной или n-арной* **алгебраической операцией** *на непустом множестве Ω называется* ***функция*** *с областью определения $\underbrace{\Omega \times \Omega \times \ldots \times \Omega}_{n \text{ множителей}}$, область значений которой включается в Ω.*

Какие виды алгебраических операций наиболее интересны для изучения?

Во-первых, в соответствии со стратегией приоритетного изучения экстремальных ситуаций наиболее интересны операции с экстремальным количеством операндов.

Во-вторых, операции с часто встречающимися свойствами, например, операции, для которых выполняется переместительный и сочетательный законы (коммутативность, ассоциативность).

II Некоторые типы алгебраических операций

Определение 1. *n-местной или n-арной* **алгебраической операцией** *на непустом множестве Ω называется* ***функция*** *с областью определения $\underbrace{\Omega \times \Omega \times \ldots \times \Omega}_{n \text{ множителей}}$, область значений которой включается в Ω.*

Если $n = 1$, то алгебраическая операция называется **унарной**, если $n = 2$ — то **бинарной** алгебраической операцией. Особую роль играют 0-арные операции, то есть константы. Например, числа 1 и 0 играют особую роль в теории целых чисел, их можно рассматривать как значения соответствующих 0-арных операций. Разумеется, 0-арные операции сейчас можно рассматривать, как некоторые «математические выкрутасы». Однако в дальнейшем мы увидим, что такой подход оказывается очень полезным.

II Некоторые типы алгебраических операций

Определение 1. *n-местной или n-арной* **алгебраической операцией** *на непустом множестве Ω называется* ***функция*** *с областью определения $\underbrace{\Omega \times \Omega \times \ldots \times \Omega}_{n \text{ множителей}}$, область значений которой включается в Ω.*

Примерами алгебраических операций на множестве действительных чисел являются операции *сложения*, *умножения*, *вычитания*. Деление [1] операцией не является, так как деление на 0 не определено, то есть пары вида $(x, 0)$ не входят в ее область определения. Это пример так называемой **частичной операции**, которые мы здесь рассматривать не будем.

[1] **функция**, паре (x, y) ставящая в соответствие действительное число $\frac{x}{y}$.

II Некоторые типы алгебраических операций

Определение 1. *n-местной или n-арной* **алгебраической операцией** *на непустом множестве Ω называется* ***функция*** *с областью определения $\underbrace{\Omega \times \Omega \times \ldots \times \Omega}_{n \text{ множителей}}$, область значений которой включается в Ω.*

Вычитание на множестве натуральных чисел не является алгебраической операцией, это тоже частичная операция, так как, например, число $-2 = 3 - 5$ не является натуральным числом, то есть пара $(3, 5)$ не входит в область определения функции »вычитание».

II Некоторые типы алгебраических операций

Определение 1. *n-местной или n-арной* **алгебраической операцией** *на непустом множестве Ω называется* ***функция*** *с областью определения $\underbrace{\Omega \times \Omega \times \ldots \times \Omega}_{n \text{ множителей}}$, область значений которой включается в Ω.*

Обычно образ элемента x относительно операции f обозначают через $f(x)$. Для бинарных алгебраических операций обычно используют другой способ обозначения образа: вместо $f(x, y)$ его обозначают через $x * y$, где $*$ — обозначение алгебраической операции. Например, мы пишем $x + y$, $x \cdot y$, $x - y$ и т.п.

II Некоторые типы алгебраических операций

Бинарная алгебраическая операция $*$ называется

коммутативной, если выполняется тождество $x * y = y * x$;

ассоциативной, если выполняется тождество $(x * y) * z = x * (y * z)$.

II Некоторые типы алгебраических операций

Бинарная алгебраическая операция $*$ называется

коммутативной, если выполняется тождество $x * y = y * x$;

ассоциативной, если выполняется тождество $(x * y) * z = x * (y * z)$.

Заметим, что сейчас мы осуществили *качественный скачок* в нашем развитии. В самом деле, до сих пор в выражениях типа $(x * y) * z = x * (y * z)$ мы рассматривали в качестве переменных только буквы x, y, z, причем считали их числами. Сейчас мы уже можем считать, что x, y, z — не обязательно числа. Но главное достижение состоит в другом. Начиная с этого места мы в качестве переменной можем рассматривать *обозначение операции* $*$. Например, тождество $(x * y) * z = x * (y * z)$ будет справедливым, если x, y, z целые числа, а под операцией $*$ понимается суммирование чисел. А можно вместо $*$ подставить операцию умножение чисел.

II Некоторые типы алгебраических операций

Бинарная алгебраическая операция $*$ называется

коммутативной, если выполняется тождество $x * y = y * x$;

ассоциативной, если выполняется тождество $(x * y) * z = x * (y * z)$.

Следующий решительный шаг, который мы сделаем существенно позднее, состоит в превращении в «переменную» обозначения отношения, например символа $=$. В данной работе последняя идея не будет развиваться сколько-нибудь систематически, однако мы отметим, что на самом деле впервые с этой ситуацией Вы встречались еще в средней школе. Например, равенство треугольников — это все-таки »не совсем равенство», иногда важно, например, *где* нарисован треугольник, а не только его геометрические характеристики.

III Некоторые классические алгебры

Определение 2. Алгеброй *(в широком смысле) называется упорядоченная пара* $\mathcal{A} = \langle A, \mathcal{F} \rangle$*, где* A *— некоторое непустое множество, называемое* **носителем** *алгебры* $\mathcal{A}$*, и* $\mathcal{F}$ *— множество операций алгебры* $\mathcal{A}$*, определенных на* A*.*

III Некоторые классические алгебры

Определение 2. Алгеброй *(в широком смысле) называется упорядоченная пара* $\mathcal{A} = \langle A, \mathcal{F} \rangle$*, где* A *— некоторое непустое множество, называемое* **носителем** *алгебры* $\mathcal{A}$*, и* $\mathcal{F}$ *— множество операций алгебры* $\mathcal{A}$*, определенных на* A*.*

На одном и том же непустом множестве можно определить различные алгебры. Например, на множестве натуральных чисел можно определить алгебру $\langle \mathbb{N}, \{+\} \rangle$, а можно — алгебру $\langle \mathbb{N}, \{\cdot, 1\} \rangle$. Можно рассмотреть и «более богатую» (в смысле множества операций) алгебру $\langle \mathbb{N}, \{+, \cdot, 1\} \rangle$. Зачем же рассматривать «бедные» алгебры, если есть такая «богатая» алгебра? Ниже мы приведем некоторые ответы на этот вопрос.

III.1 Группоид

Определение 3. *Пусть A — некоторое непустое множество, $*$ — бинарная операция на этом множестве. Тогда алгебра $\langle A, \{*\}\rangle$ называется* **группоидом**.

Группоидами являются алгебры $\langle \mathbb{N}, \{+\}\rangle$, $\langle \mathbb{Z}, \{\cdot\}\rangle$, $\langle \mathbb{N}, \{-\}\rangle$, $\langle \mathbb{Q}, \{\max\}\rangle$, где $\max$ — бинарная операция, выбирающая из элементов x, y максимальный, и т.п.

III.1 Группоид

Определение 4. *Пусть A — некоторое непустое множество, $*$ — бинарная операция на этом множестве. Тогда алгебра $\langle A, \{*\}\rangle$ называется* **группоидом**.

Группоидами являются алгебры $\langle \mathbb{N}, \{+\}\rangle$, $\langle \mathbb{Z}, \{\cdot\}\rangle$, $\langle \mathbb{N}, \{-\}\rangle$, $\langle \mathbb{Q}, \{\max\}\rangle$, где $\max$ — бинарная операция, выбирающая из элементов x, y максимальный, и т.п.

Напомним, что здесь обозначение $*$ рассматривается, как *переменная*, но, в отличие от переменных $x, y, \ldots$, *значением* переменной $*$ может быть только бинарная операция.

III.2 Полугруппа

Определение 5. *Группоид* $\langle A, \{*\}\rangle$ *называется* **полугруппой**, *если* $*$ *— ассоциативная операция, то есть выполняется тождество* $(x * y) * z = x * (y * z)$.

Иногда говорят, что A — полугруппа **относительно операции** $*$. При этом равенство $(x * y) * z = x * (y * z)$ называют **аксиомой полугруппы**.

III.3 Группа

Определение 6. *Пусть A — некоторое непустое множество, $*$ — бинарная операция, определенная на этом множестве, e — 0-местная операция на A, то есть e — некоторый элемент из A. Алгебра $\langle A, \{*, e\}\rangle$ называется* **группой**, *если выполняются следующие утверждения (***аксиомы группы***):*

G1. $(x * y) * z = x * (y * z)$, *то есть $*$ — ассоциативная операция.*

G2. $x * e = e * x = x$ *(аксиома существования* ***нейтрального*** *элемента);*

G3. *для каждого элемента $x \in A$ существует такой элемент $\tilde{x}$, что $x * \tilde{x} = \tilde{x} * x = e$ (аксиома существования* ***обратного элемента****).*

При этом операция $*$ называется **групповой операцией**.

III.3 Группа

Ясно, что группа является полугруппой. Множество целых чисел является группой относительно операции сложения и числа 0, то есть группой является алгебра $\langle \mathbb{Z}, \{+, 0\} \rangle$. Во множестве натуральных чисел с операцией сложения нет «нейтрального» элемента, поэтому группой относительно операции сложения множество $\mathbb{N}$ не является. Но полугруппой множество $\mathbb{N}$ относительно операции $+$ является. Во множестве натуральных чисел относительно операции умножения нейтральным элементом является, очевидно, число 1, так как $n \cdot 1 = 1 \cdot n = n$. Однако обратный элемент существует не для любого числа из $\mathbb{N}$ (имеется в виду обратный элемент, являющийся натуральным числом).

III.4 Примеры группоидов, полугрупп и групп

Пример 1. *Рассмотрим на множестве* $A = \{a, b, c\}$ *операции, заданные таблицами:*

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\ominus$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\odot$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Выяснить, какие из этих операций являются коммутативными и какие из группоидов $\langle A, \{+\}\rangle$, $\langle A, \{*\}\rangle$, $\langle A, \{\ominus\}\rangle$, $\langle A, \{\odot\}\rangle$, *являются полугруппами. Выяснить, в каких из этих группоидов имеются нейтральные элементы и какие из них становятся группами после добавления во множество операций соответствующего нейтрального элемента.*

Решение.

III.4 Примеры группоидов, полугрупп и групп

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\ominus$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\odot$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Решение. Эти таблицы (так называемые **таблицы Кэли**) задают операцию следующим образом.

III.4 Примеры группоидов, полугрупп и групп

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\ominus$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\odot$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Решение. Эти таблицы (так называемые **таблицы Кэли**) задают операцию следующим образом. Рассмотрим, например, таблицу для операции $+$. Элемент $x + y$ стоит в строке, самый левый элемент которой (отделенный вертикальной чертой от остальных элементов строки) равен x, и в столбце, самый верхний элемент которого (отделенный горизонтальной чертой от остальных элементов столбца) равен y. В частности, из таблиц следует, что $a + b = b$, $b \ominus a = a$, $b \odot a = b$, $a \odot b = c$.

III.4 Примеры группоидов, полугрупп и групп

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\ominus$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\odot$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Решение. Как нетрудно увидеть, коммутативными являются операции $+, *, \ominus$, а операция $\odot$ коммутативной не является, так как, например, $a \odot b = c$, но $b \odot a = b$.

III.4 Примеры группоидов, полугрупп и групп

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\ominus$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\odot$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Решение. Непосредственная проверка ассоциативности операции является громоздкой даже для такого «маленького» (всего три элемента в носителе!) группоида. Поэтому мы проведем эту проверку только относительно операции $+$, к тому же не для всех элементов. Имеем

$$\begin{array}{llll}
a+(a+a)=a+a=a, & (a+a)+a=a+a=a & \Rightarrow & a+(a+a)=(a+a)+a, \\
a+(a+b)=a+b=b, & (a+a)+b=a+b=b, & \Rightarrow & a+(a+b)=(a+a)+b, \\
a+(a+c)=a+c=c, & (a+a)+c=a+c=c, & \Rightarrow & a+(a+c)=(a+a)+c.
\end{array}$$

III.4 Примеры группоидов, полугрупп и групп

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\ominus$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\odot$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Решение.

$$\begin{array}{llll}
a+(a+a)=a+a=a, & (a+a)+a=a+a=a & \Rightarrow & a+(a+a)=(a+a)+a,\\
a+(a+b)=a+b=b, & (a+a)+b=a+b=b, & \Rightarrow & a+(a+b)=(a+a)+b,\\
a+(a+c)=a+c=c, & (a+a)+c=a+c=c, & \Rightarrow & a+(a+c)=(a+a)+c.
\end{array}$$

Нетрудно подсчитать, что требуется перебрать 27 вариантов значений переменных x, y, z, то есть нам представит написать еще 24 строчек. Вы теперь уже достаточно грамотный, и мы можем с чистой совестью переложить эту работу на Вас. Здесь мы ограничимся тем, что разболтаем «военную тайну»: операции $+, *, \ominus$ ассоциативны, а операция $\odot$ — не ассоциативная. Последнее легко проверяется: $(a \odot b) \odot c = c \odot c = a$, но $a \odot (b \odot c) = a \odot c = b$.

III.4 Примеры группоидов, полугрупп и групп

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\ominus$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\odot$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Решение. Таким образом, группоиды $\langle A, \{+\}\rangle$, $\langle A, \{*\}\rangle$ и $\langle A, \{\ominus\}\rangle$, являются полугруппами. Группоид $\langle A, \{\odot\}\rangle$ полугруппой не является, так как, например, $(a \odot b) \odot b = c \odot b = b$, но $a \odot (b \odot b) = a \odot a = a$, то есть $(a \odot b) \odot b \neq a \odot (b \odot b)$.

III.4 Примеры группоидов, полугрупп и групп

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\ominus$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\odot$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Решение. Очевидно, что в группоиде $\langle A, \{+\}\rangle$ элемент a является нейтральным. В группоиде $\langle A, \{*\}\rangle$ также имеется нейтральный элемент: это b. А вот в группоидах $\langle A, \{\ominus\}\rangle$ и $\langle A, \{\odot\}\rangle$ нет ни одного нейтрального элемента (легко показать, что если в группе нейтральный элемент существует, то он единственный).

III.4 Примеры группоидов, полугрупп и групп

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\ominus$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\odot$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Решение. Из рассмотренных четырех группоидов только $\langle A, \{+\}\rangle$ является группой. Обратные элементы задаются следующей таблицей:

x	a	b	c
$\tilde{x}$	a	c	b

.

III.4 Примеры группоидов, полугрупп и групп

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\ominus$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\odot$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Решение. Обсудим некоторые интересные особенности рассмотренных группоидов. Алгебра $\langle A, \{+, a\}\rangle$ является **группой** с ***коммутативной*** групповой операцией. Такие группы играют настолько важную роль, что для них используется специальное название.

III.5 Абелевы (коммутативные) группы

Определение 7. ***Группа*** *с* ***коммутативной*** *групповой операцией называется* **коммутативной группой** *или* **абелевой группой**.

III.5 Абелевы (коммутативные) группы

Определение 7. ***Группа*** *с* ***коммутативной*** *групповой операцией называется* **коммутативной группой** *или* **абелевой группой**.

Не все группы коммутативны.

III.5 Абелевы (коммутативные) группы

Определение 7. ***Группа*** *с* ***коммутативной*** *групповой операцией называется* **коммутативной группой** *или* **абелевой группой**.

Не все группы коммутативны. Например, множество $\{\alpha, \beta, \gamma, \delta, \varepsilon, \zeta\}$ с операцией $\circ$, заданной таблицей

$\circ$	α	β	γ	δ	ε	ζ
α	α	β	γ	δ	ε	ζ
β	β	γ	α	ε	ζ	δ
γ	γ	α	β	ζ	δ	ε
δ	δ	ζ	ε	α	γ	β
ε	ε	δ	ζ	β	α	γ
ζ	ζ	ε	δ	γ	β	α

, является некоммутативной группой.

III.6 Неабелевы (некоммутативные) группы

Определение 7. ***Группа*** *с* ***коммутативной*** *групповой операцией называется* **коммутативной группой** *или* **абелевой группой**.

Не все группы коммутативны. Например, множество $\{\alpha, \beta, \gamma, \delta, \varepsilon, \zeta\}$ с операцией $\circ$, заданной таблицей

$\circ$	α	β	γ	δ	ε	ζ
α	α	β	γ	δ	ε	ζ
β	β	γ	α	ε	ζ	δ
γ	γ	α	β	ζ	δ	ε
δ	δ	ζ	ε	α	γ	β
ε	ε	δ	ζ	β	α	γ
ζ	ζ	ε	δ	γ	β	α

, является некоммутативной группой. Можно эту группу задать иначе.

III.6 Неабелевы (некоммутативные) группы

Можно иначе задать группу

$\circ$	α	β	γ	δ	ε	ζ
α	α	β	γ	δ	ε	ζ
β	β	γ	α	ε	ζ	δ
γ	γ	α	β	ζ	δ	ε
δ	δ	ζ	ε	α	γ	β
ε	ε	δ	ζ	β	α	γ
ζ	ζ	ε	δ	γ	β	α

Рассмотрим множество всех взаимно однозначных отображений множества $\{1, 2, 3\}$ на себя.

III.6 Неабелевы (некоммутативные) группы

Можно иначе задать группу

$\circ$	α	β	γ	δ	ε	ζ
α	α	β	γ	δ	ε	ζ
β	β	γ	α	ε	ζ	δ
γ	γ	α	β	ζ	δ	ε
δ	δ	ζ	ε	α	γ	β
ε	ε	δ	ζ	β	α	γ
ζ	ζ	ε	δ	γ	β	α

Пусть β обозначает отображение, заданное таблицей

x	1	2	3
$\beta(x)$	2	3	1

, и δ обозначает отображение, заданное таблицей

x	1	2	3
$\delta(x)$	1	3	2

.

В качестве операции $\circ$ возьмем **суперпозицию функций**. Тогда достаточно положить $\alpha(x) \equiv x$, $\gamma(x) \equiv (\beta \circ \beta)(x) \equiv \beta(\beta(x))$, $\varepsilon(x) \equiv (\beta \circ \delta)(x) = \delta(\beta(x))$, $\zeta(x) \equiv (\beta \circ \beta \circ \delta)(x) = \delta(\beta(\beta(x)))$.

III.6 Неабелевы (некоммутативные) группы

Можно иначе задать группу

$\circ$	α	β	γ	δ	ε	ζ
α	α	β	γ	δ	ε	ζ
β	β	γ	α	ε	ζ	δ
γ	γ	α	β	ζ	δ	ε
δ	δ	ζ	ε	α	γ	β
ε	ε	δ	ζ	β	α	γ
ζ	ζ	ε	δ	γ	β	α

Можно предложить и другие интерпретации элементов $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta$ с тем, чтобы получить ту же групповую операцию.

III.7 Об ограничении операции на подмножество

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\ominus$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\odot$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Вернемся к группоидам примера 1. В группоиде $\langle A, \{\ominus\}\rangle$ операция «очень однообразная»: это **функция**-константа, каждой паре элементов из $\{a, b, c\}$ ставящая в соответствие один-единственный элемент a.

III.7 Об ограничении операции на подмножество

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\ominus$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\odot$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

В группоиде $\langle A, \{\odot\}\rangle$ операция $\odot$ обладает одним полезным свойством: для любых двух элементов $u, v \in \{a, b, c\}$ разрешимы уравнения $u \odot x = v$ и $y \odot u = v$ относительно переменных x, y. Здесь уместно подчеркнуть, что в группе аксиомы **G2**, **G3** широко используются именно для решения таких уравнений! Это свойство «роднит» группоид $\langle A, \{\odot\}\rangle$ с группой, хотя этот группоид не является не только группой, но даже не является полугруппой.

III.7 Об ограничении операции на подмножество

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\ominus$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\odot$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Но особый интерес представляет для нас группоид $\langle A, \{*\}\rangle$. Рассмотрим подмножество $B = \{b, c\}$ и **ограничение**[1] $\star$ операции $*$ на это подмножество:

x	b	c
b	b	c
c	c	b

. Нетрудно понять, что $\langle \{b, c\}, \{\star, b\}\rangle$ является группой.

[1]Напомним, что ограничение $\star$ получается из $*$, если мы «забудем», как действует $*$ на все элементы, не принадлежащие B. Например, $c \star b = c * b = c$, а вот $c \star a$ неопределена, так как $a \notin B$.

III.7 Об ограничении операции на подмножество

В большинстве случаев введение нового символа, например, $\star$ для обозначения **ограничения** $*$ на $\{b, c\}$, представляется неким «излишеством», т.к. для любых элементов $x, y \in B$ по определению **ограничения** имеем $x \star y = x * y$. Поэтому обычно вместо символа $\star$ можно пользоваться прежним символом $*$. По этому поводу мы примем специальное соглашение.

III.7 Об ограничении операции на подмножество

Соглашение 1. *Для уменьшения количества обозначений мы вместо символа, обозначающего* ***ограничение*** *операции на подмножество (например, символа* $\star$*, обозначающего ограничение* $*$ *на* $\{b, c\}$*) будем использовать символ исходной операции (в рассматриваемом примере это* $*$*).*

III.7 Об ограничении операции на подмножество

Соглашение 1. *Для уменьшения количества обозначений мы вместо символа, обозначающего* ***ограничение*** *операции на подмножество (например, символа $\star$, обозначающего ограничение $*$ на $\{b, c\}$) будем использовать символ исходной операции (в рассматриваемом примере это $*$).*

Это соглашение позволяет не вводить новый символ и использовать вместо него символ, обозначающий исходную операцию. В применении к рассматриваемому примеру мы будем говорить об операции $*$ *на подмножестве* B, хотя $*$ — операция на A, и, строго говоря, надо говорить о $\star$ на множестве B. «Грамматические вольности» такого рода могут привести к серьезным недоразумениям, но в ситуациях, которые мы будем рассматривать, этого не произойдет.

III.8 Дистрибутивность

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\ominus$	a	b	c
a	a	a	a
b	a	a	a
c	a	a	a

$\odot$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

Но самое интересное состоит в том, что операции $+$ и $*$ своеобразно «взаимодействуют» между собой. А именно, несложно проверить (перебором 27 вариантов), что на $A = \{a, b, c\}$ выполняются тождества $a * (b + c) = a * b + a * c$ и $(b + c) * a = b * a + c * a$. Эти формулы называются **дистрибутивностью**.

III.9. Кольцо

Определение 8. Кольцом *или* **ассоциативным кольцом** *называется алгебра* $\langle K, \{+, \cdot, 0\}\rangle$ *для которой выполняются следующие утверждения (***аксиомы кольца***):*

1. $x + y = y + x$ *(коммутативность «сложения»);*

III.9. Кольцо

Определение 8. Кольцом *или* **ассоциативным кольцом** *называется алгебра* $\langle K, \{+, \cdot, 0\}\rangle$ *для которой выполняются следующие утверждения (***аксиомы кольца***):*

1. $x + y = y + x$ *(коммутативность «сложения»);*
2. $x + (y + z) = (x + y) + z$ *(ассоциативность «сложения»);*

Значит, $\langle K, \{+\}\rangle$ **— полугруппа**

III.9. Кольцо

Определение 8. Кольцом *или* **ассоциативным кольцом** *называется алгебра* $\langle K, \{+, \cdot, 0\}\rangle$ *для которой выполняются следующие утверждения (***аксиомы кольца***):*

1. $x + y = y + x$ *(коммутативность «сложения»);*
2. $x + (y + z) = (x + y) + z$ *(ассоциативность «сложения»);*
3. *в* K *существует элемент, который мы обозначим 0, такой, что для любого* x *из* K *выполняется соотношение* $x + 0 = x$ *(наличие нулевого элемента);*

III.9. Кольцо

Определение 8. Кольцом *или* **ассоциативным кольцом** *называется алгебра* $\langle K, \{+, \cdot, 0\}\rangle$ *для которой выполняются следующие утверждения (***аксиомы кольца***):*

1. $x + y = y + x$ *(коммутативность «сложения»);*
2. $x + (y + z) = (x + y) + z$ *(ассоциативность «сложения»);*
3. *в* K *существует элемент, который мы обозначим 0, такой, что для любого* x *из* K *выполняется соотношение* $x + 0 = x$ *(наличие нулевого элемента);*

Значит, $\langle K, \{+\}\rangle$ **— полугруппа с нейтральным элементом (с «единицей»).**

III.9. Кольцо

Определение 8. Кольцом *или* **ассоциативным кольцом** *называется алгебра* $\langle K, \{+, \cdot, 0\}\rangle$ *для которой выполняются следующие утверждения (***аксиомы кольца***):*

1. $x + y = y + x$ *(коммутативность «сложения»);*
2. $x + (y + z) = (x + y) + z$ *(ассоциативность «сложения»);*
3. *в* K *существует элемент, который мы обозначим 0, такой, что для любого* x *из* K *выполняется соотношение* $x + 0 = x$ *(наличие нулевого элемента);*
4. *для любого* x *из* K *существует такой элемент* $(-x)$*, что* $(-x) + x = 0$ *(элемент, обратный относительно +);*

Значит, $\langle K, \{+\}\rangle$ **— группа.**

III.9. Кольцо

Определение 8. Кольцом *или* **ассоциативным кольцом** *называется алгебра* $\langle K, \{+, \cdot, 0\}\rangle$ *для которой выполняются следующие утверждения (***аксиомы кольца***):*

1. $x + y = y + x$ *(коммутативность «сложения»);*
2. $x + (y + z) = (x + y) + z$ *(ассоциативность «сложения»);*
3. *в* K *существует элемент, который мы обозначим 0, такой, что для любого* x *из* K *выполняется соотношение* $x + 0 = x$ *(наличие нулевого элемента);*
4. *для любого* x *из* K *существует такой элемент* $(-x)$*, что* $(-x) + x = 0$ *(элемент, обратный относительно* $+$*);*

III.9. Кольцо

Определение 8. Кольцом *или* **ассоциативным кольцом** *называется алгебра* $\langle K, \{+, \cdot, 0\}\rangle$ *для которой выполняются следующие утверждения (***аксиомы кольца***):*

1. $x + y = y + x$ *(коммутативность «сложения»);*
2. $x + (y + z) = (x + y) + z$ *(ассоциативность «сложения»);*
3. *в* K *существует элемент, который мы обозначим 0, такой, что для любого* x *из* K *выполняется соотношение* $x + 0 = x$ *(наличие нулевого элемента);*
4. *для любого* x *из* K *существует такой элемент* $(-x)$*, что* $(-x) + x = 0$ *(элемент, обратный относительно* $+$*);*

Значит, $\langle K, \{+\}\rangle$ **— абелева (коммутативная) группа — аддитивная группа кольца.**

III.9. Кольцо

Определение 8. Кольцом *или* **ассоциативным кольцом** *называется алгебра* $\langle K, \{+, \cdot, 0\}\rangle$ *для которой выполняются следующие утверждения (***аксиомы кольца***):*

1. $x + y = y + x$ *(коммутативность «сложения»);*
2. $x + (y + z) = (x + y) + z$ *(ассоциативность «сложения»);*
3. *в* K *существует элемент, который мы обозначим 0, такой, что для любого* x *из* K *выполняется соотношение* $x + 0 = x$ *(наличие нулевого элемента);*
4. *для любого* x *из* K *существует такой элемент* $(-x)$*, что* $(-x) + x = 0$ *(элемент, обратный относительно +);*
5. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ *(ассоциативность «умножения»);*

III.9. Кольцо

Определение 8. Кольцом *или* **ассоциативным кольцом** *называется алгебра* $\langle K, \{+, \cdot, 0\}\rangle$ *для которой выполняются следующие утверждения (***аксиомы кольца***):*

1. $x + y = y + x$ *(коммутативность «сложения»);*
2. $x + (y + z) = (x + y) + z$ *(ассоциативность «сложения»);*
3. *в* K *существует элемент, который мы обозначим 0, такой, что для любого* x *из* K *выполняется соотношение* $x + 0 = x$ *(наличие нулевого элемента);*
4. *для любого* x *из* K *существует такой элемент* $(-x)$*, что* $(-x) + x = 0$ *(элемент, обратный относительно +);*
5. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ *(ассоциативность «умножения»);*

Значит, $\langle K, \{\cdot\}\rangle$ **— полугруппа.**

III.9. Кольцо

Определение 8. Кольцом *или* **ассоциативным кольцом** *называется алгебра* $\langle K, \{+, \cdot, 0\}\rangle$ *для которой выполняются следующие утверждения (***аксиомы кольца***):*

1. $x + y = y + x$ *(коммутативность «сложения»);*
2. $x + (y + z) = (x + y) + z$ *(ассоциативность «сложения»);*
3. *в* K *существует элемент, который мы обозначим 0, такой, что для любого* x *из* K *выполняется соотношение* $x + 0 = x$*;*
4. *для любого* x *из* K *существует такой элемент* $(-x)$*, что* $(-x) + x = 0$ *(элемент, обратный относительно +);*
5. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ *(ассоциативность «умножения»);*
6. $x \cdot (y + z) = x \cdot y + x \cdot z, \quad (y + z) \cdot x = y \cdot x + z \cdot x$ *(левая и правая дистрибутивности).*

III.9 Кольцо

Часто это определение формулируют следующим образом: *кольцом называется непустое множество K с операциями, которые мы обозначим $+$ и $\cdot$, в котором имеется элемент, который мы обозначим символом 0, причем выполняются приведенные выше аксиомы кольца.*

$\langle K, \{+, 0\}\rangle$ называется **аддитивной группой кольца.**

$\langle K, \{\cdot\}\rangle$ называется **мультипликативной полугруппой кольца.**

III.9 Кольцо

Иногда в определении кольца отказываются от **аксиомы 5 (ассоциативность «умножения»)** и заменяют ее какой-нибудь другой. В этом случае говорят о **неассоциативных кольцах**.

Выполнение **аксиом 2-4** говорит о том, что K является **группой** относительно сложения, а выполнение при этом аксиомы 1 говорит о том, что это **абелева** или, иными словами, **коммутативная группа**.

III.10 Тело

Определение 9. *Пусть A — непустое множество, $+, \cdot$ — операции на множестве A, и* $\mathbf{0}, \mathbf{1}$ *— элементы множества A. Тогда алгебра $\langle A, \{+, \cdot, \mathbf{0}, \mathbf{1}\}\rangle$ называется* **телом** *тогда и только тогда, когда выполняются следующие утверждения (аксиомы тела):*

1. $\langle A, \{+, \mathbf{0}\}\rangle$ — ***абелева (коммутативная) группа***;
2. $\langle A \backslash \{\mathbf{0}\}, \{\cdot, \mathbf{1}\}\rangle$ — ***группа*** *(вообще говоря, некоммутативная);*
3. $a \cdot (b + c) = a \cdot b + a \cdot c$ *и* $(b + c) \cdot a = b \cdot a + c \cdot a$ — *законы* ***дистрибутивности***.

При этом группа $\langle A, \{+, \mathbf{0}\}\rangle$ называется **аддитивной группой тела**, *а группа $\langle A \backslash \{\mathbf{0}\}, \{\cdot, \mathbf{1}\}\rangle$ называется* **мультипликативной группой тела**.

III.11 Поле

Итак, мы имеем такую алгебру $\langle A, \{+, *, a, b\}\rangle$, что $+$ и $*$ — такие коммутативные операции, что, во-первых, $\langle\{a, b, c\}, \{+, a\}\rangle$ и $\langle\{b, c\}, \{*, b\}\rangle$[2] — абелевы (то есть коммутативные) группы, причем для $*, +$ выполняется дистрибутивность. Такие алгебры играют особую роль в современной математике. Такая алгебра называется полем (в алгебраическом смысле).

[2] Мы воспользовались соглашением 1, поскольку, строго говоря, надо говорить об алгебре $\langle\{b, c\}, \{\star, b\}\rangle$, а не о $\langle\{b, c\}, \{*, b\}\rangle$.

III.11 Поле

Определение 10. *Пусть A — непустое множество, $+, \cdot$ — операции на множестве A, и* $\mathbf{0}, \mathbf{1}$ *— элементы множества A. Тогда алгебра $\langle A, \{+, \cdot, \mathbf{0}, \mathbf{1}\}\rangle$ называется* **полем** *тогда и только тогда, когда выполняются следующие утверждения (аксиомы поля):*

1. $\langle A, \{+, \mathbf{0}\}\rangle$ — ***абелева (коммутативная) группа***;
2. $\langle A \backslash \{\mathbf{0}\}, \{\cdot, \mathbf{1}\}\rangle$ — ***абелева (коммутативная) группа***;
3. $a \cdot (b + c) = a \cdot b + a \cdot c$ *и* $(b + c) \cdot a = b \cdot a + c \cdot a$ — *законы* ***дистрибутивности***..

При этом группа $\langle A, \{+, \mathbf{0}\}\rangle$ называется **аддитивной группой поля**, *а группа $\langle A \backslash \{\mathbf{0}\}, \{\cdot, \mathbf{1}\}\rangle$ называется* **мультипликативной группой поля**. *Следуя физической традиции, элементы поля будем называть* **скалярами**.

III.11 Поле

Помимо рассмотренного выше примера поля можно привести более важные примеры: **поле рациональных чисел** $\langle \mathbb{Q}, \{+, \cdot, 0, 1\}\rangle$, **поле действительных чисел** $\langle \mathbb{R}, \{+, \cdot, 0, 1\}\rangle$, и рассмотренное ниже **поле комплексных чисел** $\langle \mathbb{C}, \{+, \cdot, 0, 1\}\rangle$.

Перейти к лекции по матричной алгебре?

Перейти к лекции по многочленам?

III.12 Об идентификации алгебры по ее носителю

Соглашение 2. *Нередко при проведении алгебраических исследований набор операций, определенных на данном носителе, ясен из контекста. Это позволяет идентифицировать алгебру по ее носителю. Поэтому в дальнейшем в ситуации, когда из контеста ясно, какие именно операции* $f_1, f_2, \ldots$ *определены на множестве* A*, мы нередко будем писать «алгебра* A*» вместо «алгебра* $\langle A, \{f_1, f_2, \ldots\}\rangle$*».*

Спасибо за внимание!

e-mail: melnikov@k66.ru, melnikov@r66.ru
сайты: http://melnikov.k66.ru, http://melnikov.web.ur.ru

Вернуться к списку презентаций?