Замечание Заметка Доказательство

Contents

Использованная литература и не только: Э. Б. Винберг. Курс алгебры. А. Л. Городенцев алгебра про бинарные отношения `https://www.csd.uwo.ca/~mmorenom/cs2214_moreno/notes/9-handout.pdf` `https://economics.hse.ru/data/2019/09/16/1541173496/%D0%A1%D0%B5%D0%BC%D0%B8%D0%BD%D0%B0%D1%80%202%20-%20%D0%B1%D0%B8%D0%BD%D0%B0%D1%80%D0%BD%D1%8B%D0%B5%20%D0%BE%D1%82%D0%BD%D0%BE%D1%88%D0%B5%D0%BD%D0%B8%D1%8F%20(%D0%BD%D0%B0%20%D1%81%D0%B0%D0%B9%D1%82).pdf` лекция по алгебры НМУ: `https://www.youtube.com/watch?v=T45ZtSk3d38`

1 вводные определения

Определение 1.1 *Алгебра изучает алгебраические структуры. Алгебраической структурой мы будем называть множество $\mathbb{M}$ вместе с набором операций.*

1.1 Отображения / Функции

1.1.1 Основные определения

Определение 1.2 *Отображение $f : \mathbb{X} \to \mathbb{Y}$. Существует правило, сопоставляющее каждой точке $x \in \mathbb{X}$ однозначно определяемую точку $y = f(x) \in \mathbb{Y}$, называемую образом точки x при отображении f.*

$\mathrm{Hom}(\mathbb{X}, \mathbb{Y})$ — *множество всех отображений из множества $\mathbb{X}$ в $\mathbb{Y}$.*

Определение 1.3 *Множество всех точек $x \in \mathbb{X}$, образ которых равен данной точке $y \in \mathbb{Y}$, называется полным прообразом точки y (или слоем отображения f над y):*

$$f^{-1}(y) := \{x \in \mathbb{X} \mid f(x) = y\}$$

Определение 1.4 *Множество точек $y \in \mathbb{Y}$ с непустым прообразом называется образом отображения $\mathbb{X} \xrightarrow{f} \mathbb{Y}$:*

$$\operatorname{im} f := \{y \in \mathbb{Y} \mid f^{-1}(y) \neq \varnothing\} = \{y \in \mathbb{Y} \mid \exists x \in \mathbb{X} : f(x) = y\}$$

Определение 1.5 *Равенство отображений:*

$$f = g \iff \forall x \in \mathbb{X}(f(x) = g(x))$$

Утверждение 1.6 *если множество* $\mathbb{X}$ *состоит из* n *элементов, в множество* $\mathbb{Y}$ *из* m $|\mathrm{Hom}(\mathbb{X}, \mathbb{Y})| = m^n$

1. $W_m(n)$ — количество всех n буквенных слов, которые можно записать при помощи алфавита из m-букв.
2. Выпишем все эти слова на m страницах, и на каждой i странице разместим слова на букву соответствующие i. Слов на каждой странице окажется $W_m(n)$
3. $W_m(n) = m * W_m(n-1) = m^2 * W(n-2) = ... = m^{n-1} * W(1) = m^n$

1.1.2 Сюръекция, инъекция, биекция

Определение 1.7 *Отображение* $f : \mathbb{X} \to \mathbb{Y}$ *называется сюръекцией (наложением), если* $\mathrm{im}\, f = \mathbb{Y}$. *Обозначение:* $\mathbb{X} \twoheadrightarrow \mathbb{Y}$.

Определение 1.8 *Отображение* $f : \mathbb{X} \to \mathbb{Y}$ *называется инъекцией (вложением), если* $f(x_1) \neq f(x_2)$ *при* $x_1 \neq x_2$. *Обозначение:* $\mathbb{X} \hookrightarrow \mathbb{Y}$.

Определение 1.9 *Отображение* $f : \mathbb{X} \to \mathbb{Y}$ *называется биекцией, если оно одновременно сюръективно и инъективно. Обозначение:* $\mathbb{X} \xrightarrow{\sim} \mathbb{Y}$.

1.1.3 Эндоморфизмы и автоморфизмы

Определение 1.10 *Эндоморфизм — отображение множества в себя:* $\mathbb{X} \to \mathbb{X}$. *Множество эндоморфизмов обозначается* $\mathrm{End}(\mathbb{X}) = \mathrm{Hom}(\mathbb{X}, \mathbb{X})$.

Определение 1.11 *Автоморфизм — биективный эндоморфизм:* $\mathbb{X} \xrightarrow{\sim} \mathbb{X}$. *Множество автоморфизмов обозначается* $\mathrm{Aut}(\mathbb{X})$.

Определение 1.12 *Тождественный автоморфизм* $\mathrm{Id}_{\mathbb{X}} : \mathbb{X} \to \mathbb{X}$ *определяется условием:*

$$\forall x \in \mathbb{X} \;\; \mathrm{Id}_{\mathbb{X}}(x) = x$$

Утверждение 1.13 *У n-мерного множества имеется ровно* $n!$ *автоморфизмов.*

Определена биекция $\mathbb{X} \xrightarrow{f} \mathbb{X}$ записанная n-буквенными словами в n-буквенном алфавите, содержащем каждую букву ровно один раз.

1. Пусть общее их общее количество это $V(n)$. Выпишем их по алфавиту n страницах, разместив на i страницах соответствующие буквы. Тогда на каждой странице окажется $V(n)$ слов..
2. $V(n) = n * V(n-1) = n * (n-1) * V(n-2) = ...n * (n-1)(n-2) * ...2 * 1 = n!$

1.1.4 Слои отображений

Определение 1.14 *Задание отображения $f : \mathbb{X} \to \mathbb{Y}$ равносильно разбиению $\mathbb{X}$ в дизъюнктивное объединение непустых подмножеств $f^{-1}(y)$, занумерованных точками $y \in \mathrm{im}(f)$:*

$$\mathbb{X} = \bigsqcup_{y \in \mathrm{im}(f)} f^{-1}(y)$$

1.2 Бинарные операции

Определение 1.15 *Бинарной операцией на множестве $\mathbb{M}$ называется отображение:*

$$* : \mathbb{M} \times \mathbb{M} \to \mathbb{M}$$

Результат применения операции к паре (a, b) обозначается $a * b$.

Пара $(\mathbb{S}, *)$ называется алгеброй.

- Аддитивная форма записи: операция обозначается знаком $+$.
- Мультипликативная форма записи: операция обозначается знаком $\cdot$ или $*$.

Определение 1.16 *Множество с заданной на нём бинарной операцией называется группоидом.*

Примеры группоидов:

1. $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$
2. Множество векторов на плоскости с операцией сложения.
3. Множество отображений $\mathrm{Map}(M, M)$ с операцией композиции.

1.3 Гомоморфизмы и изоморфизмы

Определение 1.17 *Пусть даны две алгебраические структуры: $(\mathbb{M}, \circ)$ и $(\mathbb{N}, *)$. Отображение $f : \mathbb{M} \to \mathbb{N}$ называется гомоморфизмом, если:*

$$\forall a, b \in \mathbb{M}(f(a \circ b) = f(a) * f(b))$$

Определение 1.18 *Гомоморфизм f называется изоморфизмом, если он биективен. Обозначение: $(\mathbb{M}, \circ) \simeq (\mathbb{N}, *)$.*

Пример изоморфизма:

$$a \mapsto 2^a, \quad (\mathbb{Q}, +) \simeq (\mathbb{R}^+, \cdot)$$

Утверждение 1.19 *Свойства изоморфных алгебр:*

1. *Образ нейтрального элемента — нейтральный элемент.*
2. *Образ симметричного элемента — симметричный элементу образу.*
3. *Образ полугруппы — полугруппа.*
4. *Образ группы — группа.*
5. *Сохраняется коммутативность.*

#+begin$_{\text{example}}$

1.4 Бинарные отношения

Пусть задано бинарное отношение Φ на множестве $\mathbb{A}$. Краткая запись: $(x, y) \in \Phi \equiv x\Phi y$.

Определение 1.20 *Отношение Φ называется:*

1. *Рефлексивным, если* $\forall x \in \mathbb{A}(x\Phi x)$.
2. *Симметричным, если* $\forall x, y \in \mathbb{A}(x\Phi y \implies y\Phi x)$.
3. *Транзитивным, если* $\forall x, y, z \in \mathbb{A}(x\Phi y \wedge y\Phi z \implies x\Phi z)$.
4. *Отношением эквивалентности, если оно рефлексивно, симметрично и транзитивно.*
5. *Иррефлексивным, если* $\forall x \in \mathbb{A}\neg(x\Phi x)$.
6. *Антисимметричным, если* $\forall x, y \in \mathbb{A}(x\Phi y \wedge y\Phi x \implies x = y)$.
7. *Отношением порядка, если оно рефлексивно, антисимметрично и транзитивно.*
8. *Линейным порядком, если оно является отношением порядка и связно:* $\forall x, y \in \mathbb{A}(x \neq y \implies x\Phi y \vee y\Phi x)$.

2 Алгебраические структуры

2.1 Основные аксиомы

Рассмотрим множество $\mathbb{R}$ с двумя бинарными операциями: сложением $(+)$ и умножением $(\cdot)$.

1. $\forall a, b, c \in \mathbb{R}(a + (b + c) = (a + b) + c)$.
2. $\exists 0 \in \mathbb{R}\ \forall a \in \mathbb{R}(a + 0 = 0 + a = a)$.
3. $\forall a \in \mathbb{R}\ \exists!(-a) \in \mathbb{R}(a + (-a) = (-a) + a = 0)$.
4. $\forall a, b \in \mathbb{R}(a + b = b + a)$.
5. $\forall a, b, c \in \mathbb{R}(a(bc) = (ab)c)$.
6. $\exists 1 \in \mathbb{R}(1 \neq 0)\ \forall a \in \mathbb{R}(a \cdot 1 = 1 \cdot a = a)$.
7. $\forall a \in \mathbb{R}(a \neq 0)\ \exists! a^{-1} \in \mathbb{R}(aa^{-1} = a^{-1}a = 1)$.
8. $\forall a, b \in \mathbb{R}(ab = ba)$.
9. $\forall a, b, c \in \mathbb{R}(a(b + c) = ab + ac)$.
10. $\forall a, b \in \mathbb{G}\ \exists! c \in \mathbb{G}(c = a * b)$.

Определение 2.1 *При условии соблюдении 10 аксиомы:*

- *Аддитивная полугруппа: множество с операцией, удовлетворяющей аксиоме 1.*
- *Аддитивная группа: множество с операцией, удовлетворяющей аксиомам 1–3.*
- *Абелева группа: группа, удовлетворяющая аксиоме 4.*
- *Кольцо: множество с двумя операциями, удовлетворяющее аксиомам 1–3, 5, 9.*
- *Поле: коммутативное ассоциативное кольцо с единицей, удовлетворяющее аксиомам 1–9.*

2.2 Простейшие свойства групп

Утверждение 2.2 *Если в группоиде S существует нейтральный элемент (θ) — он единственный.*

допустим, есть два нейтральных элемента θ и λ: $\theta = \theta * \lambda \wedge \lambda = \lambda * \theta \implies \lambda = \theta$

Утверждение 2.3 *Если в полугруппе S существует для элемента a существует симметричный/противоп — он единственный.*

Допустим, для a есть два противоположных элемента a'$_1$ и a'$_2$, в таком случае: $a * a'_1 = e \wedge a * a'_2 = e \implies a * a'_1 = a * a'_2 \implies a'_1 = a'_2$

Для любых a, b уравнение x * a = b имеет единственное решение, равное b * a'(где a' - обратный элемент a), называющееся в аддитивной группе вычитанием и в мультипликативной делением.

$$(a + x = b) \iff ((x + a) + (-a) = b + (-a)) \iff$$
$$\iff (x + (a + (-a)) = b + (-a)) \iff (x + 0 = b + (-a)) \iff (x = b + (-a)).$$

Выражение $b + (-a)$ обычно записывается как $b - a$.

Утверждение 2.4 *В мультипликативной форме записи понятие натуральной степени элемента можно вести в полугруппе, понятие целой степени — в группе.*

Для нулевой степени нужен нейтральный элемент, а для отрицательной — обратный, для натуральной степени достаточно ассоциативности.

2.3 Подгруппы

//это минимальное определение подгруппы

Определение 2.5 *Подмножество $\mathbb{H} \subset \mathbb{G}$ называется подгруппой, если:*

1. $\mathbb{H} \neq \varnothing$.
2. $\forall x, y \in \mathbb{H}(xy^{-1} \in \mathbb{H})$.

Определение 2.6 *Пусть $\mathbb{G}$ — мультипликативная группа, a – её фиксированный элемент. Если любой элемент $g \in \mathbb{G}$ записывается в виде $g = a^n$ для некоторого $n \in \mathbb{Z}$, то $\mathbb{G} =< a >$ — циклическая группа с образующим a(или циклическая группа порождённая a)*

аналогично циклическая группа определяется в аддитивном случае: $< a >= \{na | n \in \mathbb{Z}\}$

2.4 Кольца

Утверждение 2.7 *В кольце K справедливо: $\forall a \in K(a \cdot 0 = 0 \cdot a = 0)$.*

Утверждение 2.8 $\forall a, b \in K(a(-b) = (-a)b = -ab)$.

Утверждение 2.9 *1.* $\forall a, b, c \in K(a(b - c) = ab - ac)$.

Определение 2.10

- *Кольцо называется коммутативным, если умножение коммутативно.*
- *Кольцо называется ассоциативным, если умножение ассоциативно.*
- *Область целостности — коммутативное кольцо с единицей без делителей нуля.*

Элементы кольца, обладающие свойством $a \neq 0$ $b \neq 0$ $ab = 0$ делить нуля. Коммутативное кольцо с еденицией без делителей нуля называется областью целостности.

$\mathbb{K} = \{C_0, C_1, C_2, C_3\}$

+	C_0	C_1	C_2	C_3
C_0	C_0	C_1	C_2	C_3
C_1	C_1	C_2	C_3	C_0
C_2	C_2	C_3	C_0	C_1
C_3	C_3	C_0	C_1	C_2

*	C_0	C_1	C_2	C_3
C_0	C_0	C_0	C_0	C_0
C_1	C_0	C_1	C_2	C_3
C_2	C_0	C_2	C_0	C_2
C_3	C_0	C_3	C_2	C_1

> если $1 = 0$ то $a = a1 = a0 = 0$ то есть кольцо состоит только из одного нуля, значит, если кольцо состоит из нескольких элементов то $1 \neq 0$

2.5 Подкольца

Определение 2.11 *Подмножество $K' \subset K$ называется подкольцом, если:*

1. $\forall a, b \in K' (a + b \in K')$.
2. $\forall a, b \in K' (a - b \in K')$.
3. $\forall a, b \in K' (ab \in K')$.

2.6 Поля

Определение 2.12 *Полем называется коммутативное ассоциативное кольцо с единицей, в котором всякий ненулевой элемент обратим.*

> Кольцо из одного нуля не является полем.

Утверждение 2.13 *В поле нет делителей нуля.*

2.7 Подполя

Определение 2.14 *Подмножество $P' \subset P$ называется подполем, если:*

1. $\forall a, b \in P' (a + b \in P')$.
2. $\forall a, b \in P' (ab \in P')$.
3. $\forall a, b \in P' (b \neq 0) \left(\frac{a}{b} \in P'\right)$.

3 Комплексные числа

Определение 3.1 *Поле комплексных чисел:*

$$\mathbb{C} = \{(a, b) \mid a, b \in \mathbb{R}\}$$

с операциями:

- *Сложение:* $(a, b) + (c, d) = (a + c, b + d)$.
- *Умножение:* $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$.

Теорема 3.2 *Поле $\mathbb{C}$ содержит подполе, изоморфное полю действительных чисел.*

Рассмотрим $R_1 = \{(a, 0) \mid a \in \mathbb{R}\} \subset \mathbb{C}$. Можно показать, что R_1 является подполем и изоморфно $\mathbb{R}$.

Определение 3.3 *Алгебраическая форма комплексного числа:*

$$\alpha = a + bi, \quad a, b \in \mathbb{R}$$

где $i = (0, 1)$, $i^2 = -1$.

Определение 3.4 *Комплексно сопряжённое число:*

$$\overline{\alpha} = a - bi$$

Определение 3.5 *Тригонометрическая форма комплексного числа:*

$$\alpha = r(\cos\phi + i\sin\phi), \quad r = |\alpha| = \sqrt{a^2 + b^2}, \quad \phi = \arg\alpha$$