

Дискретная математика

Козырнов Александр Дмитриевич, ИУ7-32Б

5 января 2024 г.

Оглавление

1	Множества, отношения, алгебры	4
1.1	Опр. множества и операций над ним	4
1.1.1	Условие	4
1.1.2	Определение множества	4
1.1.3	Равенство множеств	4
1.1.4	Операции над множествами	4
1.1.5	Методы доказательства теоретико-множественных тождеств	4
1.2	Неупорядоченная и упорядоченная пары, кортеж, Декартово произведение.	6
1.2.1	Условие	6
1.2.2	Виды вар	6
1.2.3	Кортеж	6
1.3	Отображение, частичное отображение	7
1.3.1	Условие	7
1.3.2	Отображение	7
1.4	Соответствие	8
1.4.1	Соответствие	8
1.4.2	График и граф соответствия	8
1.4.3	Бинарные и n-арные (n-местные) отношения	8
1.4.4	Связь отношения, соответствия, отображения	8
1.5	Композиция соответствий, их свойства	9
1.5.1	Условие	9
1.5.2	Композиция соответствий	9
1.5.3	Обратное соответствие	9
1.5.4	Свойства и их доказательства	9
1.6	Специальные свойства бинарных отношений	11
1.6.1	Свойства	11
1.7	Классификация бинарных отношений на множестве	12
1.7.1	Классификация	12
1.8	Отношение эквивалентности, класс эквивалентности, фактор-множество	13
1.8.1	Условие	13
1.8.2	Отношение эквивалентности	13
1.8.3	Класс эквивалентности	13
1.8.4	Фактор-множество	13
1.9	Отношение порядка и предпорядка. Грани множества	14
1.9.1	Условие	14
1.9.2	Отношение предпорядка и порядка	14
1.9.3	Наименьший, наибольший, минимальный, максимальный элементы	14
1.9.4	Верхняя и нижняя грани	14
1.10	Точная верхняя грань последовательности. Индуктивно упорядоченное множество	16

1.10.1	Условие	16
1.10.2	Индуктивно упорядоченное множество	16
1.10.3	Точная верхняя грань последовательности	16
1.10.4	Теорема о неподвижной точке	16
1.11	Алгебры, операции на множестве, свойства операций	18
1.11.1	Условие	18
1.11.2	Операции на множестве	18
1.11.3	Алгебры	18
1.12	Группоид, полугруппа, моноид, группа. Единственность нейтрального, обратного элементов	20
1.12.1	Условие	20
1.12.2	Группоид - группа	20
1.13	Циклическая полугруппа (группа)	21
1.13.1	Циклическая группа и полугруппа	21
1.14	Кольца	23
1.14.1	Условие	23
1.14.2	Кольца, группа и моноид кольца	23
1.14.3	Теорема о тождествах кольца	23
1.15	Тела и поля	25
1.15.1	Условие	25
1.15.2	Тело и поле	25
1.15.3	Область целостности. (+делители нуля)	25
1.15.4	Поля вычетов. Решение систем ЛУ в полях вычета	25
1.16	Подполугруппа, подмоноид, подгруппа. Примеры. Циклические подгруппы.	27
1.16.1	Под[группа, моноид, полугруппа]	27
1.16.2	Циклические подгруппы	28
1.17	Смежные классы подгруппы. Теорема Лагранжа	29
1.17.1	Условие	29
1.17.2	Смежные классы	29
1.18	Полукольцо. Идемпотентное полукольцо	30
1.18.1	Условие	30
1.18.2	Полукольца	30
1.19	Замкнутое полукольцо. Итерация элемента	31
1.19.1	Условие	31
1.19.2	Замкнутое полукольцо	31
1.19.3	Итерация элемента	31
1.20	Непрерывность сложения в замкнутом полукольце. Теорема о наименьшем решении ЛУ	32
1.20.1	Условие	32
1.20.2	Непрерывность сложения	32
1.20.3	Теорема о наименьшем решении	32
1.21	Квадратные матрицы размером n над идемпотентным полукольцом. Решение СЛУ в замкнутых полукольцах	34
1.21.1	Условие	34
1.21.2	Ответ	34
2	Элементы теории графов	36
2.1	Основные понятия теории графов	36
2.1.1	Условие	36
2.1.2	Неориентированный граф	36
2.1.3	Ориентированный граф	36
2.1.4	Подграф	37
2.2	Связность неорграфа, компонента связности неорграфа	38

2.2.1	Условие	38
2.2.2	Ответ	38
2.3	Связность орграфа (слабая сильная).	
	Компонента связности (слабая, сильная)	39
2.3.1	Условие	39
2.3.2	Связность орграфа	39
2.4	Поиск в глубину. Древесные и обратные ребра	40
2.4.1	Условие	40
2.4.2	Алгоритм	40
2.4.3	Типы дуг	40
2.5	Поиск в глубину в орграфе. Классификация дуг в орграфе.	42
2.5.1	Условие	42
2.5.2	Алгоритм	42
2.5.3	Классификация дуг	42

Множества, отношения, алгебры

1.1 Опр. множества и операций над ним

1.1.1 Условие

Множества, подмножества. Способы определения множеств. Равенство множеств. Операции над множествами (объединение, пересечение, разность, симметрическая разность, дополнение). Методы доказательства теоретико-множественных тождеств.

1.1.2 Определение множества

Множества мы будем обозначать большими буквами латинского алфавита (X, Y, Z, \dots), элементы множества малыми буквами (x, y, z, \dots). Принадлежность элемента x множеству X (неопределяемое понятие) будем обозначать $x \in X$. Аналогично $x \notin X$ обозначает, что элемент x не принадлежит множеству X .

По определению считается $\emptyset \subseteq A$ и $A \subseteq U$

1.1.3 Равенство множеств

$$A = B \Leftrightarrow (\forall x)(x \in A \Leftrightarrow x \in B)$$

Пример:

$$\{1, 3, 5\} = \{5, 1, 3\} = \{1, 1, 3, 3, 5, 5\}$$

Также возможно определить равенство через подмножество.

$$A \subseteq B \Leftrightarrow (\forall x)(x \in A \Rightarrow x \in B) - \text{опр. нестрогого включения } A \text{ в } B.$$

Тогда

$$A = B \Leftrightarrow (A \subseteq B) \ \& \ (B \subseteq A)$$

1.1.4 Операции над множествами

- объединение $A \cup B \Leftrightarrow \{x : x \in A \vee x \in B\}$
- пересечение $A \cap B \Leftrightarrow \{x : x \in A \ \& \ x \in B\}$
- разность $A \setminus B \Leftrightarrow \{x : x \in A \ \& \ x \notin B\}$
- симметрическая разность $A \Delta B \Leftrightarrow (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$
- дополнение $\overline{A} \Leftrightarrow \{x : x \notin A\} = U \setminus A$

1.1.5 Методы доказательства теоретико-множественных тождеств

- Метод двух включений (На примере декартового умножения)
 $A \times (B \cap C) = (A \times B) \cap (A \times C)$
Доказательство
 $(x, y) \in A \times (B \cap C) \Leftrightarrow (x \in A) \ \& \ (y \in (B \cap C)) \Leftrightarrow (x \in A) \ \& \ (y \in$

$$B) \ \& \ (y \in C) \Leftrightarrow ((x, y) \in A \times B) \ \& \ ((x, y) \in A \times C) \Leftrightarrow (x, y) \in (A \times B) \cap (A \times C)$$

- Методом Характеристических функций ($\chi_{A \times B \cap C}$)
- Методом эквивалентных преобразований ($\cap, \cup, \ \& \ , \ \backslash \ , \dots$)

1.2 Неупорядоченная и упорядоченная пары, кортеж, Декартово произведение.

1.2.1 Условие

Неупорядоченная пара, упорядоченная пара, кортеж. Декартово произведение множеств

1.2.2 Виды вар

Неупорядоченная пара

$A, B \neq \emptyset, a \in A, b \in B$

Тогда $\{a, b\}$ - неупорядоченная пара на множествах A и B

$$\begin{cases} \{a, b\} = \{a\}, |\{a\}| = 1, \text{ если } a = b \\ |\{a, b\}| = 2, \text{ если } a \neq b \end{cases}$$

$$\{a, b\} = \{c, d\} \Leftrightarrow ((a = c) \& (b = d)) \vee ((a = d) \& (b = c))$$

$$\text{То есть } \{1, 2\} = \{2, 1\}$$

Упорядоченная пара

$A, B \neq \emptyset, a \in A, b \in B$

Тогда (a, b) - упорядоченная пара на множествах A и B

$$(a, b) = (c, d) \Leftrightarrow (a = c) \& (b = d)$$

То есть $(a, b) \neq (b, a)$

Ее можно свести к множеству: $(a, b) \Leftrightarrow \{\{a\}, \{a, b\}\}$

1.2.3 Кортеж

$A_1, A_2, \dots, A_n, n \geq 1$

Тогда (a_1, a_2, \dots, a_n) , где $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$ - кортеж

- Равенство кортежей:

$$(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n) \Leftrightarrow (\forall i = \overline{1, n})(a_i = b_i)$$

- Определение:

$$A_1 \times A_2 \times \dots \times A_n \Leftrightarrow \{(x_1, x_2, \dots, x_n) : (\forall i = \overline{1, n})(x_i \in A_i)\}$$

По определению если $(\exists i = \overline{1, n})(A_i = \emptyset)$, то $A_1 \times A_2 \times \dots \times A_n = \emptyset$

- Степень кортежа:

Если $A_1 = A_2 = \dots = A_n, n \geq 1$, то $A_1 \times A_2 \times \dots \times A_n = A^n$

$A^0 \Leftrightarrow \{\lambda\}$, где λ - пустой кортеж, $A \neq \emptyset$

Некоторые свойства декартового умножения:

- $\overline{A \times B} = (\overline{A} \times \overline{B}) \cup (\overline{A} \times B) \cup (A \times \overline{B})$

- $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$

- $A \times B \neq B \times A$

1.3 Отображение, частичное отображение

1.3.1 Условие

Отображения: область определения, область значений. Инъективное, сюръективное и биективное отображения. Частичное отображение

1.3.2 Отображение

Отображение - это соответствие, которое всюду определено и функционально по второй компоненте

Пусть $\rho \subseteq A \times B$, тогда

- Область определения: $D(\rho) \Leftarrow \{x : x \in A, (x, y) \in \rho\}$
- Область значений: $R(\rho) \Leftarrow \{y : y \in B, (x, y) \in \rho\}$

$f : A \rightarrow B$ - частичное отображение, или отображение, где $D(\rho) \neq A$

$f : A \rightarrow B$ - просто отображение

Виды отображений:

- Инъективное отображение:

Если отображение функционально и по первой компоненте, то она называется инъекцией

$$(\forall x \in A)(\exists! y = f(x)) \ \& \ (\forall y \in R(f))(\exists! x \in A)(y = f(x))$$

- Сюръективное отображение:

Это такое отображение, где $R(f) = B$, то есть

$$(\forall y \in B)(\exists x \in A)(y = f(x))$$

- Биективное отображение:

Это такое отображение, которое инъективно и сюръективно.

$$(\forall x \in A)(\exists! y = f(x)) \ \& \ (\forall y \in B)(\exists! x)(y = f(x))$$

1.4 Соответствие

Условие

Соответствия. График и граф соответствия, область определения, область значения. Сечение соответствия. Сечение соответствия по множеству. Функциональность соответствия по компоненте. Бинарные и n -арные отношения. Связь между отношениями, соответствиями и отображениями.

1.4.1 Соответствие

$\rho \subseteq A \times B$ - соответствие из A в множество B , причем $A, B \neq \emptyset$

- Область определения: $D(\rho) \Leftarrow \{x : x \in A, (x, y) \in \rho\}$
- Область значений: $R(\rho) \Leftarrow \{y : y \in B, (x, y) \in \rho\}$
- Сечение по $a \in A$: $\rho(a) \Leftarrow \{y : (a, y) \in \rho\}$
- Сечение по множеству $C \subseteq D(\rho)$: $\rho(C) \Leftarrow \{(x, y) : x \in C, (x, y) \in \rho\}$

Соответствие $\rho = A \times B$ называют функциональным по второй компоненте, если $\forall(x, y) \text{ и } (x', y') : x = x' \Rightarrow y = y'$

Соответствие $\rho = A \times B$ называют функциональным по первой компоненте, если $\forall(x, y) \text{ и } (x', y') : y = y' \Rightarrow x = x'$

1.4.2 График и граф соответствия

СДЕЛАТЬ

1.4.3 Бинарные и n -арные (n -местные) отношения

n -местное (n -арное) отношение на множествах $A_1, A_2, \dots, A_n, n \geq 1$:
 $\rho \subseteq A_1 \times A_2 \times \dots \times A_n$

Бинарное отношение: $\rho = A^2, A \neq \emptyset$, иногда записывается как $x\rho y$

Свойства

- Рефлексивность
 $(\forall x \in A)(x\rho x)$, то есть диагональ $id_A \subseteq \rho$
- Иррефлексивность
 $id_A \cap \rho = \emptyset$
- Симметричность
 $\forall(x, y) \in A, x\rho y \Rightarrow y\rho x$, то есть $\rho = \rho^{-1}$
- Антисимметричность
 $\forall(x, y) \in A, x\rho y \ \& \ y\rho x \Rightarrow x = y$, например $x \leq y \ \& \ y \leq x \Rightarrow x = y$
- Транзитивность
 $(\forall x, y, z \in A)(x\rho z \ \& \ z\rho y \Rightarrow x\rho y)$, например $x = z, z = y \Rightarrow x = y$

1.4.4 Связь отношения, соответствия, отображения

Соответствие - это бинарное отношения вида $\rho = A \times B$ или $\rho = A \times A$.

Отображение - это соответствие, которое всюду определено и функционально по второй компоненте.

1.5 Композиция соответствий, их свойства

1.5.1 Условие

Композиция соответствий, обратное соответствие и их свойства (с доказательством)

1.5.2 Композиция соответствий

$$\rho \subseteq A \times B, \sigma \subseteq C \times D$$

Тогда композиция:

- $\rho \circ \sigma \Rightarrow \{(x, y) : (x, z) \in \rho \ \& \ (z, y) \in \sigma\}$
- $\rho = A \times B, \sigma = B \times C, \rho \circ \sigma = A \times C$
- $f : A \rightarrow B, g : B \rightarrow C, f \circ g : A \rightarrow C$

причем $R(\rho) \cap D(\sigma) \neq \emptyset$

Покажем, что $f \circ g(x) = g(f(x))$

$$f \circ g = \{(x, y) : (\exists z)((x, z) \in f) \ \& \ ((z, y) \in g)\} = \{(x, y) : (\exists z)(z = f(x), y = g(z))\} = \{(x, y) : y = g(f(x))\}$$

1.5.3 Обратное соответствие

$\rho^{-1} \Rightarrow \{(x, y) : (y, x) \in \rho\}$ - обратное соответствие

Если $\rho = A \times B$, то $\rho^{-1} = B \times A$

1.5.4 Свойства и их доказательства

- $\rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau$
Рассмотрим $(\rho \circ (\sigma \circ \tau))(x) : (\rho \circ (\sigma \circ \tau))(x) = \rho((\sigma \circ \tau)(x)) = \rho(\sigma(\tau(x)))$
Рассмотрим $((\rho \circ \sigma) \circ \tau)(x) : ((\rho \circ \sigma) \circ \tau)(x) = ((\rho \circ \sigma)(f(x))) = \rho(\sigma(\tau(x)))$
Как можем заметить, результат получен одинаковый
- $\rho \circ \sigma \neq \sigma \circ \rho$
Пусть $\rho = A \times B, f : A \rightarrow B$ и $\sigma = B \times C, g : B \rightarrow C$
Тогда $\rho \circ \sigma : A \rightarrow C$
Получаем $\sigma \circ \rho : B \rightarrow B$ при условии, что $B \cap A \neq \emptyset$, иначе $\sigma \circ \rho = \emptyset$
В обоих случаях $R(\rho \circ \sigma) \neq R(\sigma \circ \rho), D(\rho \circ \sigma) \neq D(\sigma \circ \rho) \Rightarrow \rho \circ \sigma \neq \sigma \circ \rho$
в общем случае
- $\rho \circ (\sigma \cup \tau) = (\rho \circ \sigma) \cup (\rho \circ \tau)$
 $(x, y) \in \rho \circ (\sigma \cup \tau) \Rightarrow (\exists z)((x, z) \in \rho) \wedge ((z, y) \in \sigma \cup \tau) \Rightarrow (\exists z)((x, z) \in \rho) \wedge ((z, y) \in \sigma) \vee ((z, y) \in \tau) \Rightarrow (\exists u)((x, u) \in \rho) \wedge ((u, y) \in \sigma) \vee (\exists v)((x, v) \in \rho \wedge (v, y) \in \tau) \Rightarrow (\rho \circ \sigma) \cup \rho \circ \tau$
- $\rho \circ (\sigma \cap \tau) \subseteq (\rho \circ \sigma) \cap (\rho \circ \tau)$
Доказательство Аналогично прошлому доказательству
- $(\rho^{-1})^{-1} = \rho$
 $\rho^{-1} \Rightarrow \{(y, x) : (x, y) \in \rho\}$
Тогда $(\rho^{-1})^{-1} \Rightarrow \{(x, y) : (y, x) \in \rho^{-1}\} \Rightarrow \{(x, y) : (x, y) \in \rho\} \Rightarrow \rho$
- $(\rho \circ \sigma)^{-1} = \sigma^{-1} \circ \rho^{-1}$
Пусть $\rho : A \rightarrow B, \sigma : B \rightarrow C$, тогда $\rho \circ \sigma : A \rightarrow C$
Тогда $(\rho \circ \sigma)^{-1} : C \rightarrow A$
 $\rho^{-1} : B \rightarrow A, \sigma^{-1} : C \rightarrow B$
Из этого следует $\sigma^{-1} \circ \rho^{-1} : C \rightarrow A$, что равно $(\rho \circ \sigma)^{-1} : C \rightarrow A$

- $\rho \subseteq A^2$

1.6 Специальные свойства бинарных отношений

Условие

Специальные свойства бинарных отношений на множестве (рефлексивность, иррефлексивность, симметричность, антисимметричность, транзитивность).

1.6.1 Свойства

- Рефлексивность
 $(\forall x \in A)(x\rho x)$, то есть диагональ $id_A \subseteq \rho$
- Иррефлексивность
 $id_A \cap \rho = \emptyset$
- Симметричность
 $\forall (x, y) \in A, x\rho y \Rightarrow y\rho x$, то есть $\rho = \rho^{-1}$
- Антисимметричность
 $\forall (x, y) \in A, x\rho y \ \& \ y\rho x \Rightarrow x = y$, например $x \leq y \ \& \ y \leq x \Rightarrow x = y$
- Транзитивность
 $(\forall x, y, z \in A)(x\rho z \ \& \ z\rho y \Rightarrow x\rho y)$, например $x = z, z = y \Rightarrow x = y$

1.7 Классификация бинарных отношений на множестве

Условие

Классификация бинарных отношений на множестве: эквивалентность, толерантность, порядок, предпорядок, строгий порядок

1.7.1 Классификация

- Отношение эквивалентности
 - Рефлексивность
 - Симметричность
 - Транзитивность
- Отношение Толерантности
 - Рефлексивность
 - Симметричность
- Отношение Порядка
 - Рефлексивность
 - Антисимметричность
 - Транзитивность
- Отношение Предпорядка
 - Рефлексивность
 - Транзитивность

1.8 Отношение эквивалентности, класс эквивалентности, фактор-множество

1.8.1 Условие

Отношение эквивалентности. Класс эквивалентности. Фактор-множество.

1.8.2 Отношение эквивалентности

Отношение эквивалентности можно охарактеризовать так:

- Рефлексивность
- Симметричность
- Транзитивность

1.8.3 Класс эквивалентности

$[x]_\rho \Leftarrow \{y : y\rho x\}$ - класс эквивалентности элемента x по отношению ρ .
Причем $(\forall x \in A)(x \in [x]_\rho)$

Пример: $[(x_0, y_0)]_\rho = \{(x, y) : x^2 + y^2 = x_0^2 + y_0^2\}$, где x_0, y_0 не изменяются (константы). График такого класса эквивалентности представляет собой окружность радиуса $x_0^2 + y_0^2$

Теорема Класс эквивалентности для любого произвольного отношения эквивалентности попарно не пересекаются

Это означает, что два класса эквивалентности не имеют общих элементов, или $[x]_\rho \cap [z]_\rho = \emptyset$.

Говорят, что некоторое семейство подмножеств создает разбиение множества A , если: 1) все подмножества не пусты, 2) каждый элемент из A (множества) принадлежит хотя бы одному из классов эквивалентности, 3) Классы попарно не пересекаются (что было сказано выше).

1.8.4 Фактор-множество

A/ρ - это фактор-множество

$A/\rho \Leftarrow \{[x]_\rho : x \in A\}$, где $[x]_\rho$ - это элемент класс эквивалентности

То есть простыми словами фактор-множество - это все классы эквивалентности:
 $A/\rho = \{[x_1]_\rho, [x_2]_\rho, \dots, [x_n]_\rho\}$ - то есть множество множеств. Также по определению это является разбиением множества (см. выше)

1.9 Отношение порядка и предпорядка. Грани множества

1.9.1 Условие

Отношения предпорядка и порядка. Наибольший, максимальные, наименьший и минимальные элементы. Точная нижняя и верхняя грани множества

1.9.2 Отношение предпорядка и порядка

Отношение Порядка

- Рефлексивность
- Антисимметричность
- Транзитивность

Отношение Предпорядка

- Рефлексивность
- Транзитивность

Если отношение порядка таково, что несравнимых элементов нет, то отношение является линейным порядком

Знаки сравнимости:

- Знаки нестрогого порядка: \leq, \geq
- Знаки строгого порядка: $<, >$
 $a < b \Leftrightarrow a \leq b \ \& \ a \neq b$
- Отношение несравнимости $a \asymp b \Leftrightarrow a \not\leq b \ \& \ a \not\geq b$

1.9.3 Наименьший, наибольший, минимальный, максимальный элементы

Элемент $a \in A$ называется наименьшим, если $(\forall x \in A)(x \leq a)$

Элемент $a \in A$ называется наибольшим, если $(\forall x \in A)(x \geq a)$

Элемент $a \in A$ называется минимальным, если $(\forall x \in A)(a \leq x \vee a \asymp x)$

Элемент $a \in A$ называется максимальным, если $(\forall x \in A)(a \geq x \vee a \asymp x)$

Теорема. Если наименьший (наибольший) элемент существует, то он единственный

Прошу заметить, что минимальных и максимальных элементов может быть бесконечность!

1.9.4 Верхняя и нижняя грани

$\mathcal{A} = (A, \leq)$ - отношение порядка.

$B \subseteq A$ - отношение порядка на подмножестве B (индуцированный порядок)

Верхняя грань B^∇ - верхний конус B . $B^\nabla \Leftrightarrow \{x : (\forall b \in B)(b \leq x)\}$,
где x - это **верхняя грань**

Нижняя грань B^Δ - нижний конус B . $B^\Delta \Leftrightarrow \{x : (\forall b \in B)(b \geq x)\}$,
где x - это **нижняя грань**

Если из всех верхних граней есть наименьшая, то она называется точная верхняя грань или супремум. Если из всех нижних граней есть наибольшая, то она называется точная нижняя грань или инфимум.

1.10 Точная верхняя грань последовательности. Индуктивно упорядоченное множество

1.10.1 Условие

Точная верхняя грань последовательности. Индуктивное упорядоченное множество. Теорема о неподвижной точке (с доказательством). Пример вычисления неподвижной точки

1.10.2 Индуктивно упорядоченное множество

Определение. Упорядоченное множество $\mathcal{A} = (A, \leq)$ называют индуктивно упорядоченным, если

- 1) Оно имеет наименьший элемент
- 2) Любая неубывающая последовательность элементов A имеет супремум (\sup)

1.10.3 Точная верхняя грань последовательности

Определение. $\lim_{n \rightarrow \infty} a_n = \sup(a_n)$ - точная верхняя грань последовательности

1.10.4 Теорема о неподвижной точке

Теорема. f называется непрерывным, если для любой неубывающей последовательности $a_0 \leq a_1 \leq \dots \leq a_n \leq \dots$ и $f(\sup a_n) = \sup f(a_n)$

Теорема (о монотонности). Всякое непрерывное отображение одного ИУМ в другое монотонно

Теорема (о неподвижной точке). Всякое непрерывное отображение ИУМ в себя имеет наименьшую неподвижную точку

Доказательство. Пусть A - ИУМ, $f : A \rightarrow A$ - непрерывно. Обозначим Θ наименьшим элементом A .

Построим последовательность:

$\Theta, f(\Theta), f(f(\Theta)), \dots, f^n(\Theta), n \geq 0$, где $f^n \Theta = f(f^{n-1}(\Theta))$

Докажем, что наша последовательность не убывает

$\Theta \leq f(\Theta)$, так как Θ - наименьший элемент

Тогда $f^{n-1}(\Theta) \leq f^n(\Theta)$, тогда в силу монотонности f верно $f(f^{n-1}(\Theta)) \leq f(f^n(\Theta)) \Rightarrow f^n(\Theta) \leq f^{n+1}(\Theta)$.

Положим $a = \sup_{n \geq 0} f^n(\Theta)$

Вычислим $f(a)$

$$\begin{aligned} f(a) &= f(\sup f^n(\Theta)) = \sup f(f^n(\Theta)) = \\ &= \sup f^{n+1}(\Theta) = \sup \{f(\Theta), f(f(\Theta)), \dots\} = \\ &= \sup f^n(\Theta) = a \end{aligned}$$

Из этого следует, что a - неподвижная точка, то есть $f(a) = a$

Пусть $(\exists b \in A)(f(b) = b)$

Тогда $\Theta \leq b, f(\Theta) \leq f(b), \dots$

То есть $(\forall n \geq 0)(f^n(\Theta) \leq b)$. Отсюда b - верхняя грань $\{f^n(\Theta)\}$. Так как $a = \sup f^n(\Theta)$, то $a \leq b$

Ч.Т.Д

Пример вычисления (из лекции):

На отрезке $[0, 1]$ рассмотрим уравнение $x = \frac{1}{2}x + \frac{1}{4}$

В данном случае $\Theta = 0$, так как 0 - наименьшее число.

Строим последовательность: $0, f(0), f^2(0), \dots = 0, \frac{1}{4}, \frac{3}{8}, \frac{7}{16}, \dots$

Получаем формулу: $f^n(0) = \frac{2^n - 1}{2^{n+1}}$

Найдем супремум: $\sup f^n(0) = \lim_{n \rightarrow \infty} f^n(0) = \frac{1}{2}$

1.11 Алгебры, операции на множестве, свойства операций

1.11.1 Условие

Операции на множестве. Понятие алгебраической структуры. Свойства операций (ассоциативность, коммутативность, идемпотентность). Нуль и нейтральный элемент (единица) относительно операции. Примеры. Универсальная алгебра, носитель, сигнатура. Примеры. Однотипные алгебры.

1.11.2 Операции на множестве

Определение. n -арная операция на множестве $A \neq \emptyset : \omega : A^k \rightarrow A, k \geq 0$

Простыми словами: A^k - это количество операторов (k операторов), а ω - это функция, которая из k элементов делает результат в виде 1-го элемента. Причем как и k операторов, так и результат находится в множестве A

Нулярная операция ($k = 0$) - это фиксированное значение $\omega(\lambda)$

Свойства операций:

- 1) Результат всегда существует
- 2) Результат принадлежит тому же множеству

Пусть $*$ - операция алгебры, Тогда:

- Ассоциативность
 $a * (b * c) = (a * b) * c$
- Коммутативность
 $a * b = b * a$
- Идемпотентность
 $a * a = a^n = a$

Относительно операции есть особые элементы. Пусть $*$, $+$ - операции алгебры, Тогда:

- Нуль (ноль, нулевой элемент)
 $a * 0 = 0$ и $a + 0 = a$
- Нейтральный элемент по отношению к операции $*$
 $a * \epsilon = a$

1.11.3 Алгебры

Определение. $\mathcal{A} = (A, \Omega)$ - это (Универсальная) алгебра, где A - это носитель, Ω - это сигнатура

$\Omega = \Omega^{(0)} \cup \Omega^{(1)} \cup \dots \cup \Omega^{(n)} \cup \dots$ - это все i -арные операции, где $i = \overline{0, \infty}$.

Носитель A - это всевозможные значения, которые можно получить с помощью операций, а также значения, которые могут принимать операторы.

Определение (Из интернета). Универсальной алгеброй называется совокупность непустого множества A и произвольного набора Ω заданных на A алгебраических операций. Записывается в таком виде: $\mathcal{A} = (A, \Omega)$

Примеры алгебр:

1) Числовые алгебры $(R, +, *, 0, 1)$

2.1) Векторные алгебры $\mathcal{L} = (L, +, \alpha, \theta)$

2.2) Векторные алгебры $\mathcal{V} = (V^3, +, \times, \bar{0})$

3) Матричные алгебры $\mathcal{M} = (\mathbb{M}, +, *, 0, E)$

Определение. Тип алгебры - это кортеж, составленный из арностей сигнатуры алгебры, то есть: $(\alpha_1, \alpha_2, \dots, \alpha_n)$

Алгебры, имеющих один и тот же тип алгебры, называются однотипными.

1.12 группоид, полугруппа, моноид, группа. Единственность нейтрального, обратного элементов

1.12.1 Условие

Группоиды, полугруппы, моноиды. Единственность нейтрального элемента. Обратный элемент. Группа. Единственность обратного элемента в группе

1.12.2 Группоид - группа

$\mathcal{A} = (G, *)$, где $*$ - бинарная операция.

Если операция \mathcal{A} 'замкнута' (то есть результат есть в носителе A), то \mathcal{A} - **группоид**.

Пример алгебры, который не имеет свойств группоида - это скалярное умножение векторов.

Если операция группоида ассоциативная, то этот группоид - **полугруппа**

Пусть ϵ - нейтральный элемент в полугруппе, тогда по отношению к его операции верно: $\epsilon * a = a * \epsilon = a$

Если в полугруппе есть нейтральный элемент, то он является **моноидом**.

Теорема (о единственности нейтрального элемента) Если полугруппа имеет нейтральный элемент, то он единственный

Доказательство ϵ', ϵ'' - нейтральные элементы.

$\epsilon' * \epsilon'' = \epsilon''$, так как ϵ' - нейтральный

$\epsilon'' * \epsilon' = \epsilon'$, так как ϵ'' - нейтральный

Тогда $\epsilon' = \epsilon''$

Пусть существует обратный элемент к a такой, что $a * a' = a' * a = \epsilon$

Если каждый элемент моноида обратим, то это **группа**

Теорема (о единственности обратного элемента) Если элемент моноида обратим, то обратный к нему единственный

Доказательство a', a'' - обратные элементы к a

$a'' = a'' * \epsilon = a'' * (a * a') = (a'' * a) * a' = \epsilon * a' = a'$

1.13 Циклическая полугруппа (группа)

Условие

Циклическая полугруппа (группа). Образующий элемент. Примеры конечных и бесконечных циклических полугрупп и групп. Порядок конечной группы. Порядок элемента. Теорема о равенстве порядка образующего элемента конечной циклической группы порядку группы.

1.13.1 Циклическая группа и полугруппа

Определение. Группа $\mathcal{J} = (G, *, 1)$ называется циклической, если $(\exists a \in G)(\exists n \in \mathbb{Z})(\forall g \in G)(g = a^n)$, где a - образующий элемент.

$\mathcal{J} = [a] = [a^{-1}]$, где a - образующий элемент.

Образующий элемент не может существовать без обратного элемента. Если есть a , то есть a^{-1}

Примеры циклических групп:

- Бесконечная
 $(\mathbb{Z}, +, 0), n \geq 0 : n = 1 + 1 + 1 + \dots + 1 = n * 1$
- Конечная
 $\mathbb{Z}_3^* = (\{1, 2\}, *_3, 1)$ - мультипликативная группа вычетов по модулю 3

Определение. Полугруппа $\mathcal{J} = (G, *, 1)$ называется циклической, если $(\exists a \in G)(\exists n \in \mathbb{Z})(\forall g \in G)(g = a^n)$, где a - образующий элемент.

В отличие от циклической группы Циклическая полугруппа не имеет обратных элементов, отчего образующие элементы не имеют обратных к себе, то есть неверно $\exists a \Rightarrow \exists a^{-1}$

Примеры циклических полугрупп:

- Бесконечная
 $(\mathbb{N}_0, +, 0), n \geq 0 : n = 1 + 1 + 1 + \dots + 1 = n * 1$, где \mathbb{N}_\times - множество натуральных чисел начиная с нуля.
- Конечная
Полугруппа \mathcal{P} по операции сложения положительных натуральных чисел

Порядок конечной группы - это количество ее элементов, или $|G|$.

Порядком элемента конечной группы элемента a называется наименьшее $n > 0$, при котором $a^n = \epsilon$

Теорема (о равенстве порядка...). Порядок образующего элемента конечной циклической группы равен порядку группы

Доказательство. Пусть есть $[a]$ - конечная циклическая группа с образующим элементом a . Рассмотрим $\{1, a, a^2, \dots, a^{n-1}\}$

Пусть найдутся 2 такие степени, что $a^p = a^q$, $0 < p < q < n$, где n - порядок элемента a

Тогда

$$\begin{aligned}a^p &= a^q \\a^p * a^{-q} &= a^p * a^{-p} \\a^{p-q} &= 1, \text{ но } p - q < n\end{aligned}$$

По определению n - наименьшая степень, при которой $a^n = 1 \Rightarrow$ противоречие.

1.14 Кольца

1.14.1 Условие

Кольца. Аддитивная группа и мультипликативный моноид кольца. Коммутативное кольцо. Кольца вычетов. Теорема о тождествах кольца (аннулирующем свойстве нуля, свойстве обратного по сложению при умножении, дистрибутивности вычитания относительно умножения).

1.14.2 Кольца, группа и моноид кольца

$\mathcal{R} = (R, +, *, 0, 1)$ - так выглядит кольцо

Аксиомы кольца:

- 1) $a + (b + c) = (a + b) + c$ - ассоциативность сложения
- 2) $a + b = b + a$ - коммутативность сложения
- 3) $a + 0 = a$ - 0 нейтральный элемент для сложения
- 4) $(\forall a \in R)(\exists a^{-1} \in R) : a + a' = 0$ - для любого числа по сложению есть обратный к нему
- 5) $a * (b * c) = (a * b) * c$ - ассоциативность умножения
- 6) $a * 1 = a$ - 1 нейтральный элемент умножения
- 7) $a * (b + c) = a * b + a * c$ - коммутативность умножения по сложению

Как можем заметить из аксиом кольца, операция сложения на носителе R создает группу, а операция умножения - моноид. Поэтому аддитивной группой кольца называется такая алгебра $\mathcal{G} = (R, +, 0)$, являющаяся группой, а мультипликативным моноидом такая - $\mathcal{M} = (R, *, 1)$, являющаяся моноидом. (Буквы алгебр неважны, поэтому можно не указывать)

Кольцо называется коммутативным, если его операция $*$ является коммутативной, то есть верно $a * b = b * a$

Кольца вычетов - это такие кольца, где все значения носителя меньше числа, по модулю которого идет вычет. Например кольцо вычетов по модулю 3 выглядит так: $\mathcal{Z}_3 = (\{0, 1, 2\}, +, *, 1, 0)$. В нем никогда не будет числа 3 и больше. $2 * 2 = 4 \% 3 = 1$

1.14.3 Теорема о тождествах кольца

- 1) $a * 0 = 0$

Доказательство. Пусть Θ - неизвестная, значение которой нужно найти.

$$a + a * \Theta = a * 1 + a * \Theta = a(1 + \Theta) = a * 1 = a.$$

Найдем значение $\Theta : a + a * \Theta = a \Rightarrow a * \Theta = a - 1 \Rightarrow \Theta = 0$, где 0 - ноль кольца

- 2) $(-a) * b = (-ab)$

Доказательство. $(-a)b + ab = ((-a) + a)b = 0 * b = 0 \Rightarrow (-a)b$ -
обратное к $ab \Rightarrow (-a)b = -(ab)$

3) $a * (b - c) = ab - ab$

Доказательство. $a * (b - c) = a * (b + (-c)) = ab + b(-c) = ab - bc$

1.15 Тела и поля

1.15.1 Условие

Тела и поля. Примеры полей. Область целостности. Теорема о конечной области целостности (с доказательством). Поля вычетов. Решение систем линейных уравнений в поле вычетов.

1.15.2 Тело и поле

Определение. Кольцо, в котором все ненулевые элементы обратимы по умножению, называется **телом**.

Определение. Тело с коммутативным умножением называется **полем**.

Пример поля - это обычная числовая прямая вещественных чисел.

1.15.3 Область целостности. (+делители нуля)

Определение. Областью целостности, или целостным кольцом, называют коммутативное кольцо без делителей нуля.

Определение. Делители нуля на примере: $a \neq 0, b \neq 0$,
 $a * b = 0 \vee b * a = 0$

Почему они называются делителями нуля? А потому, что обычное число состоит из простых и они являются его делителем. Вот с нулем в поле может случиться такая же ситуация - он состоит из ненулевых чисел.

Теорема. Конечная область целостности является полем

Доказательство. $\mathcal{R} = (R, +, *, 0, 1)$ - конечная область целостности.

По определению примем, что $f_a(x) = ax, a \neq 0$ и $f_a : R \setminus \{0\} \rightarrow R \setminus \{0\}$

Докажем, что f_a - инъекция:

Пусть $ax = ay$, тогда $f_a(x) = f_a(y)$

Тогда $ax - ay = a(x - y) = 0 \Rightarrow x - y = 0 \Rightarrow x = y$, то есть $f_a(x) = f_a(y) \Rightarrow x = y$ - инъекция.

Поскольку носитель - это конечное множество, то его инъекция считается биекцией: $(\forall y \neq 0)(\exists! x)(y = ax)$

В частности при $y = 1 : (\exists! x)(ax = 1)$, то есть $x = a^{-1}$. Из этого следует, что оно обратимо по умножению, значит, это поле.

1.15.4 Поля вычетов. Решение систем ЛУ в полях вычета

Поля вычетов - это такие поля, где все значения носителя меньше числа, по модулю которого идет вычет. Например поле вычетов по модулю 3 выглядит так: $\mathbb{Z}_3 = (\{0, 1, 2\}, +, *, 1, 0)$. В нем никогда не будет числа 3 и больше. $2 * 2 = 4 \% 3 = 1$

Пример решения в поле вычетов:

$$\mathbb{Z}_{19} : \begin{cases} 11x - 5y + z = 1 \\ 21x + 4y - z = 2 \\ 5x - 6z = 5 \end{cases}$$

Решаем методом Лагранжа с помощью матрицы коэффициентов:

$$\left(\begin{array}{ccc|c} 1 & -5 & 1 & 1 \\ -2 & 4 & -1 & 2 \\ 5 & 0 & 6 & 5 \end{array} \right)$$

Ответ: $(x, y, z) = \begin{pmatrix} 2 \\ 18 \\ 20 \end{pmatrix}$

Алгоритм:

- 1) Списываем коэффициенты перед x, y, z в матрицу, а также свободный член
- 2) Решаем ее методом Лагранжа, учитывая, что все операции по модулю поля вычета
- 2.1) Если число отрицательное (пусть -2 при кольце вычетов 19), то оно равно $-(19 + (-2)) = -17$

1.16 Подполугруппа, подмоноид, подгруппа. Примеры. Циклические подгруппы.

Условие

Подполугруппа, подмоноид, подгруппа. Примеры. Циклические подгруппы.

1.16.1 Под[группа, моноид, полугруппа]

$\mathcal{J} = (G, *, 1)$ - группа.

$H \subseteq G$ замкнуто, если:

- 1) $1 \in H$
- 2) $(\forall x \in H)(x^{-1} \in H)$
- 3) $(\forall x, y \in H)(x * y \in H)$

Тогда $\mathcal{H} = (H, *, 1)$ - подгруппа группы \mathcal{J}

Более понятным языком. Есть подмножество носителя $H \subseteq G$. Если в подмножестве H есть единица группы, для всех x из множества H есть x^{-1} в H , а также для любой пары из H результат операции из группы \mathcal{J} есть в множестве H , то \mathcal{H} - подгруппа группы \mathcal{J} .

Вкратце про остальные два. Пусть есть группа $\mathcal{J} = (G, *, 1)$ и пусть есть $H \subseteq G$

Подмоноид:

- 1) Если $1 \in H$
- 2) Если $(\forall x, y \in H)(x * y \in H)$

То есть тоже самое, что и подгруппа, но без обратного элемента.

Подполугруппа:

- 1) Если $(\forall x, y \in H)(x * y \in H)$

Тожe самое, что и подмоноид, но только без требования к $1 \in H$.

Если все подытожить, то подгруппа обладает нейтральным элементом группы, для каждого числа есть к нему обратное в подгруппе, операция замкнута на носителе подгруппы. Подмоноид - это полугруппа без обратного элемента в носителе подгруппы. Подполугруппа не обладает к тому же еще и нейтральным элементом.

Пример. $(\mathbb{Z}, +, 0)$ - группа сложения целых чисел.

Тогда подгруппа этой группы: $\mathcal{H} = \{2n : n \in \mathbb{Z}\}$ - подгруппа всех четных чисел

Пример. $(\mathbb{N}, +, 0)$ - группа сложения натуральных чисел.

Тогда подмоноид этой группы: $\mathcal{H} = \{2n : n \in \mathbb{N}\}$ - подмоноид всех четных положительных чисел. Это является моноидом потому, что все числа натуральные, значит, в этом множестве нет обратных к любому числу по сложению (в натуральном множестве нет отрицательных). Однако число 0, являющееся нейтральным, присутствует в моноиде \Rightarrow подмоноид.

Пример. $(\mathbb{N}, +, 0)$ - группа сложения натуральных чисел.

Тогда подполугруппа этой группы: $\mathcal{H} = \{n : n \in \mathbb{Z} \ \& \ n \geq 1\}$ - подполугруппа всех положительных чисел начиная с 1. Тут нет нейтральных элементов и нет обратных к любому элементу множества. Единственное, что выполняется здесь, это замкнутость операции.

1.16.2 Циклические подгруппы

$\mathcal{J} = (G, *, 1)$ - группа.

$$a \in G$$

$\mathcal{H} = \{a^n : n \in \mathbb{Z}\}$ - замкнута, так как:

- $1 = a^0 \in H$
- $a^p * a * q = a^{p+q} \in H$
- $(a^p)^{-1} = a^{-p} \in H$

a - образующий элемент циклической группы. Тогда $[a]$ - циклическая подгруппа группы \mathcal{J}

1.17 Смежные классы подгруппы. Теорема Лагранжа

1.17.1 Условие

Смежные классы подгруппы по элементу. Теорема Лагранжа.

1.17.2 Смежные классы

Пусть \mathcal{H} - подгруппа группы $\mathcal{J} = (G, *, \epsilon)$. Пусть $a \in G$.

Тогда правый смежный класс: $a\mathcal{H}$

Тогда левый смежный класс: $\mathcal{H}a$

В общем случае $a\mathcal{H} \neq \mathcal{H}a$. Если они равны, то это нормальная подгруппа.

Теорема. Порядок любой конечной группы делится на порядок любой ее подгруппы

Доказательство Докажем 4 леммы:

1) Лемма 1

$$(\forall h \in H)(hH = H)$$

Доказательство:

$$\text{Пусть } x \in hH; x = hh_1, h_1 \in H, hh_1 \in H.$$

$$\text{Пусть } x \in H \Rightarrow x = hh^{-1}x = h(h^{-1}x) \in hH$$

2) Лемма 2

$$abH = a(bH)$$

Доказательство:

Является прямым следствием ассоциативности операции группы.

3) Лемма 3

Левые смежные классы образуют разбиение группы (носителя группы)

Доказательство:

$$(\forall a \in G)(a \in aH), \text{ так как } 1 \in H$$

Пусть $aH \cap bH \neq \emptyset \Rightarrow (\exists c)(c \in aH \cap bH)$. Тогда $c = ah_1 = bh_2$, где $h_1, h_2 \in H$.

$$b = abh_1h_2^{-1} \Rightarrow bH = (ah_1h_2^{-1})H = (ah_1)(h_2^{-1}H) = (ah_1)H = aH.$$

4) Лемма 4

Все левые смежные классы находятся в однозначном соответствии (то есть два таких класса образуют биекцию)

Доказательство:

$$\varphi : H \rightarrow aH$$

$$\varphi(h) = ah$$

φ - сюръекция, так как $(\forall x \in H)(x = ah = \varphi(h))$

Пусть $\varphi(h_1) = \varphi(h_2) \Rightarrow ah_1 = ah_2 \Rightarrow h_1 = h_2 \Rightarrow \varphi$ - инъекция

Отсюда φ - биекция.

1.18 Полукольцо. Идемпотентное полукольцо

1.18.1 Условие

Полукольцо. Идемпотентное полукольцо. Естественный порядок идемпотентного полукольца

1.18.2 Полукольца

Определение (сжатое). Полукольцо - это кольцо, в котором по операции сложения нет обратного элемента

$\mathcal{S} = (S, +, *, 0, 1)$ - полукольцо.

Аксиомы полукольца:

1) $a + (b + c) = (a + b) + c$

2) $a + b = b + a$

3) $a + 0 = a$

4) $a * (b * c) = (a * b) * c$

5) $a * 1 = 1 * a = a$

6) $a * (b + c) = a * b + a * c$

7) $a * 0 = +0 * a = 0$

Определение. Полукольцо называется идемпотентным, если $a + a = a$

Естественный порядок кольца: $a \leq b \Leftrightarrow a + b = b$. Является отношением порядка, то есть Р+А+Т.

Из этого следует, что $a^n = a$

1.19 Замкнутое полукольцо. Итерация элемента

1.19.1 Условие

Замкнутое полукольцо. Итерация элемента. Примеры вычисления итерации в различных замкнутых полукольцах.

1.19.2 Замкнутое полукольцо

Определение. Идемпотентное полукольцо называется замкнутым, если:

- 1) Любая последовательность имеет точную верхнюю грань по естественному порядку
- 2) Для любых a и последовательности $\{X_n\}_{n \geq 0}$:
$$a * \sup X_n = \sup(a * X_n)$$
$$(\sup X_n) * a = \sup(X_n a)$$

Любое полукольцо, которое конечно, замкнуто.

1.19.3 Итерация элемента

Определение. Итерация - это точная верхняя грань последовательности всех ее степеней

В общем случае итерация - это бесконечное применение операции к одному и тому же элементу в какой-то степени.

Например, в полукольце бинарных операций по операции "или":
(Z_2, \vee, \wedge)

$$1^* = 1^0 \vee 1^1 \vee 1^2 \vee \dots = \sum_{i=0}^{\infty} 1^i$$

В нашем случае $1^* = 1 \vee 1 \vee 1 \vee \dots = 1$

Если в замкнутом полукольце 0 - наибольшее по естественному порядку, то итерация любого элемента равна: $a^* = 1$

1.20 Непрерывность сложения в замкнутом полукольце. Теорема о наименьшем решении ЛУ

1.20.1 Условие

Непрерывность операции сложения в замкнутом полукольце. Теорема о наименьшем решении линейного уравнения в замкнутом полукольце.

1.20.2 Непрерывность сложения

Чтобы ее определить, нужна Теорема.

Теорема (о свойствах бесконечной суммы).

- 1) $\Sigma(a_n + b_n) = \Sigma a_n + \Sigma b_n$
- 2) Для любых a и последовательности $\{b_n\}$ верно:
 $a + \Sigma b_n = \Sigma(a + b_n)$
- 3) Если $S_n = \sum_{i=0}^n a_i$, то $\Sigma S_n = \Sigma a_n$, где a_i - частичная сумма последовательности $\{a_n\}$

Доказательство.

- 1) $(a_n + b_n) + \Sigma a_n + \Sigma b_n = (a_n + \Sigma a_n) + (b_n + \Sigma b_n) = \Sigma a_n + \Sigma b_n$.

$\Sigma a_n + \Sigma b_n$ - верхняя грань $\{a_n + b_n\}$

Пусть $(\exists C)(\forall n)(a_n + b_n \leq C)$. Тогда $a_n \leq a_n + b_n \leq C$ и $b_n \leq a_n + b_n \leq C$, то есть C - верхняя грань $\{a_n\}$ и $\{b_n\}$.

$$C + \Sigma a_n + \Sigma b_n = C + \Sigma b_n = C$$

Итак, мы доказали, что $\Sigma a_n + \Sigma b_n \leq C$, то есть $\Sigma a_n + \Sigma b_n = \Sigma(a_n + b_n)$

- 2) Является прямым следствием первого, когда одна из последовательностей постоянная

Отсюда можно доказать непрерывность сложения. В следствие второго пункта сложение непрерывно: $f(x) = a + x$

$$f(\Sigma X_n) = a + \Sigma X_n = \Sigma(a + X_n) = \Sigma f(X_n)$$

1.20.3 Теорема о наименьшем решении

Теорема. Наименьшим решением $x = ax + b$ и $x = xa + b$ в замкнутых полукольцах будет соответственно $x = a^*b$ и $x = ba^*$

Доказательство. Используем формулу для вычисления наименьшей неподвижной точки и, записывая в случае замкнутого полукольца как бесконечную сумму, получим для уравнения решение в виде $x = a^*b$

$$x = \sum_{n=0}^{\infty} f^n(\Theta) - \text{где } \Theta - \text{ нуль полукольца и } f(x) = ax + b$$

Учитывая, что $f^0(\Theta) = b, f^1(\Theta) = ab + b, \dots$ получаем $\sum_{n=0}^{\infty} f^n(\Theta) = \sum_{n=1}^{\infty} (1 + a + \dots + a^n)$

Используя непрерывность умножения вынесем b :

$$\left(\sum_{n=1}^{\infty} (1 + a + \dots + a^n) \right) b$$

Так как $1 + a + \dots + a^n$ - частичная сумма $\{a^n\}_{n \geq 0}$. Тогда

$$\sum_{n=0}^{\infty} (1 + a + \dots + a^n) = \sum_{n=0}^{\infty} a^n = a^* = f^n(\Theta)$$

Из этого следует, что мы нашли точную верхнюю грань частичной суммы, значит мы нашли точную верхнюю грань последовательности. Тогда окончательно получаем $x = a^*b$ в замкнутом полукольце

Теорема. Алгебра $\mathcal{M}(\mathcal{S})$ есть идемпотентное полукольцо. Если кольцо \mathcal{S} замкнуто, то и полукольцо $\mathcal{M}(\mathcal{S})$ тоже замкнуто

Из этой теоремы следует, что мы можем решить такие уравнения:

$$X = AX + B \text{ и } X = XA + B \quad (4)$$

$$\text{То есть в } \mathcal{M}(\mathcal{S}) \implies X = A^*B \quad (5)$$

Система (3) в матричной форме (ε - столбец β - столбец):

$$\varepsilon = A\varepsilon + \beta, \text{ где } \varepsilon = (x_1, x_2, \dots, x_n)^T, \beta = (b_1, b_2, \dots, b_n)^T \quad (6)$$

Матричное уравнение может быть расписано по столбцам:

$$\varepsilon_j = A\varepsilon_j + \beta_j, 1 \leq j \leq n \quad (7)$$

Тогда в матрицах это выглядит так:

$$X = [\varepsilon_1, \varepsilon_2, \dots, \varepsilon_j, \varepsilon_n]$$

$$B = [\beta_1, \beta_2, \dots, \beta_n]$$

Матрица (4) разрешима в виде (5). (4) может быть расписано как (7). (7) разрешимо, так как вся матрица разрешима. И решение для каждого столбца $\varepsilon_j = A^*B, 1 \leq j \leq n$. То есть $\varepsilon = A^*B$

Элементы теории графов

2.1 Основные понятия теории графов

2.1.1 Условие

Основные понятия теории графов: неориентированные и ориентированные графы, цепи, пути, циклы, контуры. Подграфы.

2.1.2 Неориентированный граф

Определение. $\mathcal{G} = (V, E)$ - неориентированный граф, где

V - конечное множество вершин графа.

E - Множество смежностей, или множество неупорядоченных пар на V , то есть подмножество множества двухэлементных подмножеств V , элементы которого называются ребрами

Определение. Цепь в неорграфе - это последовательность вершин G $v_0, v_1, \dots, v_n, \dots$ такая, что $(v_i - v_{i-1})(\forall i)(\exists v_{i+1})$, если u_{i+1} определен в последовательности. Под конечной последовательностью понимается кортеж вершин

Определение. Цепь называется простой, если все ее вершины (кроме, может быть, первой и последней) попарно различны.

Определение. Цикл - простая цепь ненулевой длины с совпадающими концами.

Определение. Ребро e называется инцидентным вершине v , если она является одним из его концов.

2.1.3 Ориентированный граф

Определение. $\mathcal{G} = (V, E)$ - ориентированный граф, где

V - конечное множество вершин графа.

E - Множество смежностей, или множество упорядоченных пар на V , то есть подмножество множества $V \times V$, элементы которого называются дугами.

Определение. Дугу (U, V) называют заходящей в вершину V и исходящей из вершины U .

Определение. Дугу называют инцидентной вершине V , если она заходит в V или исходит из V .

Определение. Путь в орграфе: последовательность вершин $u_0, u_1, u_2, \dots, u_n, \dots$, где $(\forall i \geq 0)(u_i \rightarrow u_{i+1})$, если u_{i+1} определен в последовательности.

Определение. Простой путь - это такой путь, если все его вершины (кроме, может быть, первой и последней) попарно различны.

Определение. Контур - это простой ненулевой длины путь, в котором совпадают начало и конец.

2.1.4 Подграф

Определение. Неориентированный (ориентированный) граф $\mathcal{G}_1 = (V_1, E_1)$ называют подграфом неориентированного (ориентированного) графа $\mathcal{G} = (V, E)$, если $V_1 \subseteq V, E_1 \subseteq E$.

2.2 Связность неорграфа, компонента связности неорграфа

2.2.1 Условие

Связность неориентированного графа. Компоненты связности.

2.2.2 Ответ

Определение. Неориентированный граф называют связным, если любые две его вершины U и V соединены цепью.

Определение. Компонента связности неорграфа - это максимальный связный подграф текущего графа.

2.3 Связность орграфа (слабая сильная). Компонента связности (слабая, сильная)

2.3.1 Условие

Связность, сильная и слабая связность орграфа. Компоненты связности (сильной, слабой).

2.3.2 Связность орграфа

Определение. Ориентированный граф называют связным, если для любых двух его вершин U, V вершина V достижима из U или наоборот.
 $(\forall U, V)((U \Rightarrow^* V) \vee (V \Rightarrow^* U))$

Определение. Граф является слабо связанным, если ассоциированный с ним неорграф является связным

Определение. Граф является сильно связанным, если для любых двух его вершин U, V вершина U достижима из V и наоборот
 $(\forall U, V)(U \Rightarrow^* V \ \& \ V \Rightarrow^* U)$

Определение. Компонента связности (сильная, слабая) ориентированного графа - это максимальный связный (слабо, сильно) подграф.

Теорема. Если в орграфе из u достижима v , то существует простой путь из u в v

Следствия из теоремы. Если в орграфе вершина лежит на простом замкнутом пути, то она лежит на контуре. Если в неорграфе 2 вершины соединены цепью, то существует простая цепь, соединяющая их. Если в неорграфе вершина лежит на замкнутой цепи, то она лежит на цикле.

2.4 Поиск в глубину. Древесные и обратные ребра

2.4.1 Условие

Поиск в глубину в неориентированном графе. Древесные и обратные ребра. Поиск фундаментальных циклов на основе поиска в глубину

2.4.2 Алгоритм

T - древесные ребра, FC - фундаментальные циклы

```
begin
    T, B, FC := 0; stack := 0;
    count := 1;
    for all v in V
        NEW[V] := 0;
    for all v in V
        while (exists V)(NEW[V] = 1) do
            search_D(V);
end;

proc search_D(v)
    NEW[V] := 0;
    D[V] := count; count := count + 1;
    v → stack;

    for all (w in L[V]) do
        if (NEW[w]) then begin
            {V,w} → T;
            search_D(w);
        end;
        else if ({V,w} not in T) then
            if ({V,w} not in B) then begin
                {V,w} → B;
                read(V..w) → FC;
            end;
        end;
        stack → V;
    end;
end;
```

2.4.3 Типы дуг

Определение. Лес, который строится методом поиска в глубину, называется глубинный остовный лес

Определение. Древесные дуги (T) - это те дуги, которые ведут от отца к сыну в глубинном остовном лесе.

$$\begin{aligned} D[v] &< D[w] \\ NEW[w] &= 1 \end{aligned}$$

Определение. Обратные дуги (B) - это те дуги, которые ведут от потомка к предку в глубинном остовном лесе.

$$\begin{aligned} D[v] &\geq D[w] \\ NEW[w] &= 0 \end{aligned}$$

$$\omega \in stack$$

Определение. Прямые дуги (F) - это те дуги, которые ведут от подлинного предка к подлинному потомку, НО не от отца к сыну в глубинном остоном лесу.

$$D[v] < D[\omega]$$

Определение. Поперечные дуги (C) - это все остальные дуги в глубинном остоном дереве.

$$D[v] > D[\omega]$$

$$\omega \notin stack$$

2.5 Поиск в глубину в орграфе. Классификация дуг в орграфе.

2.5.1 Условие

Поиск в глубину в орграфе. Классификация дуг. Критерий бесконтурности

2.5.2 Алгоритм

```
begin
    T,B,C,F,C := 0; stack := 0;
    for all v in V do
        NEW[v] := 1;
    const := 1;

    for all v in V do
        while (exists v)(NEW[v] = 1) do
            search_DOR(v);
end;

proc search_DOR(v)
    NEW[v] := 0;
    D[v] := const; const := const + 1;

    v -> stack;
    for all w in L[v] do
        if NEW[w] then begin
            (v,w) -> T;
            search_DOR(w);
        end;
        else begin
            if (D(v) >= D(w)) & (w in stack) then
                (v,w) -> B;
            if (D(v) < D(w)) then
                (v,w) -> F;
            if (D(v) > D(w)) & (w not in stack) then
                (v,w) -> C;
        end;
    end;
end;
```

2.5.3 Классификация дуг

Определение. Лес, который строится методом поиска в глубину, называется глубинный остовный лес

Определение. Древесные дуги (T) - это те дуги, которые ведут от отца к сыну в глубинном остовном лесе.

$$\begin{aligned} D[v] &< D[w] \\ NEW[w] &= 1 \end{aligned}$$

Определение. Обратные дуги (B) - это те дуги, которые ведут от потомка к предку в глубинном остовном лесу.

$$D[v] \geq D[w]$$

$$NEW[\omega] = 0$$

$$\omega \in stack$$

Определение. Прямые дуги (F) - это те дуги, которые ведут от подлинного предка к подлинному потомку, НО не от отца к сыну в глубинном остоном лесу.

$$D[v] < D[\omega]$$

Определение. Поперечные дуги (C) - это все остальные дуги в глубинном остоном дереве.

$$D[v] > D[\omega]$$

$$\omega \notin stack$$

Критерий бесконтурности. Ориентированный граф является бесконтурным тогда и только тогда, когда при поиске в глубину от некоторой начальной вершины множество обратных дуг оказывается пустым.