Федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО»

Институт компьютерных наук и технологий
Кафедра «Компьютерные интеллектуальные технологии»

В.Г. ПАК

ДИСКРЕТНАЯ МАТЕМАТИКА

СЛАЙДЫ ВИДЕОЛЕКЦИЙ ДЛЯ СТУДЕНТОВ II КУРСА ЗАОЧНОГО ОТДЕЛЕНИЯ БАКАЛАВРИАТА НАПРАВЛЕНИЯ ПОДГОТОВКИ «ПРИКЛАДНАЯ ИНФОРМАТИКА»

Санкт-Петербургский политехнический университет Петра Великого
2018

Содержание курса

Введение

Тема 1. Теория множеств

Тема 2. Комбинаторика

Тема 3. Булевы функции

Тема 4. Минимизация булевых функций

Тема 5. Реализация булевых функций схемами из функциональных элементов и релейно-контактными схемами

Тема 6. Основы теории графов

Федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО»

Институт компьютерных наук и технологий
Кафедра «Компьютерные интеллектуальные технологии»

ЛЕКЦИЯ №1

ВВЕДЕНИЕ. ПРЕДМЕТ ДИСКРЕТНОЙ МАТЕМАТИКИ. ОСНОВЫ ТЕОРИИ МНОЖЕСТВ. ОТНОШЕНИЯ

СЛАЙДЫ ВИДЕОЛЕКЦИЙ ДЛЯ СТУДЕНТОВ II КУРСА ЗАОЧНОГО ОТДЕЛЕНИЯ БАКАЛАВРИАТА НАПРАВЛЕНИЯ ПОДГОТОВКИ «ПРИКЛАДНАЯ ИНФОРМАТИКА»

Санкт-Петербургский политехнический университет Петра Великого
2018

Содержание

Введение

Дискретная математика – раздел фундаментальной математики, в котором исследуются *дискретные структуры*, т.е. структуры, составленные из пространственно или логически отделённых друг от друга компонентов.

Примеры дискретных структур: графы, конечные и счётные множества, семейства множеств, классические логики.

Разделы дискретной математики:

1) теория множеств;
2) комбинаторика;
3) теория графов;
4) математическая логика;
5) теория кодирования;
6) теория абстрактных алгебраических структур.

Тема 1. Теория множеств

§1. Основы теории множеств

1.1. Понятие множества

Множество – совокупность объектов (элементов), рассматриваемая как единое целое.

Обозначения множеств: A, B, C, … , A_1, A_2, … . Обозначения элементов множеств: a, b, , c … , a_1, a_2, … .

Элемент a принадлежит множеству A: $a \in A$.

Элемент a не принадлежит множеству A: $a \notin A$.

Определение. Множества A и B называются *равными*, если они содержат одинаковые элементы: $A = B$.

Определение. Множество A называется *подмножеством* множества B (A включено в B, A содержится в B, B содержит A), если любой элемент A является элементом B: $A \subseteq B \;\Leftrightarrow\; \forall a\colon\, a \in A \;\Rightarrow a \in B$.

Если $A \subseteq B$ и $A \neq B$, то пишут $A \subset B$.

Очевидно, что $A = B \;\Leftrightarrow A \subseteq B \,\&\, B \subseteq A$.

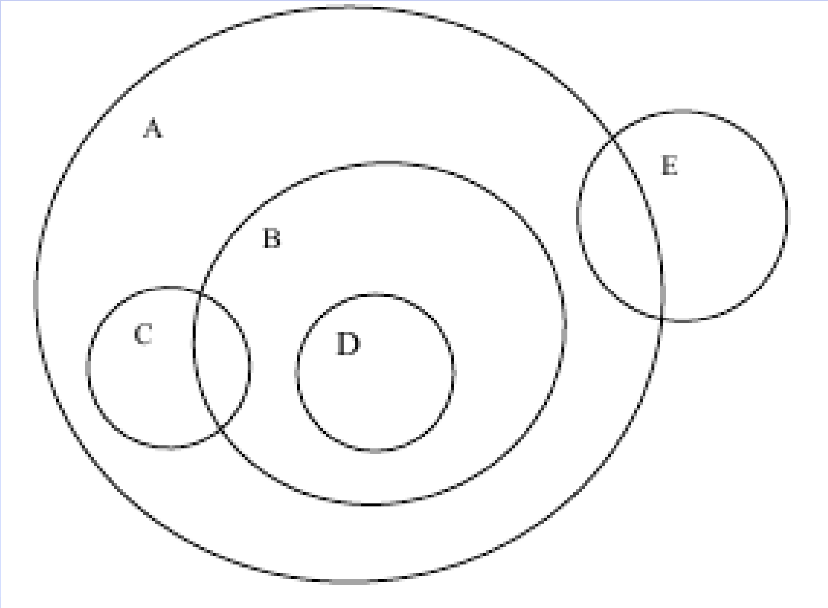
1.1. Понятие множества

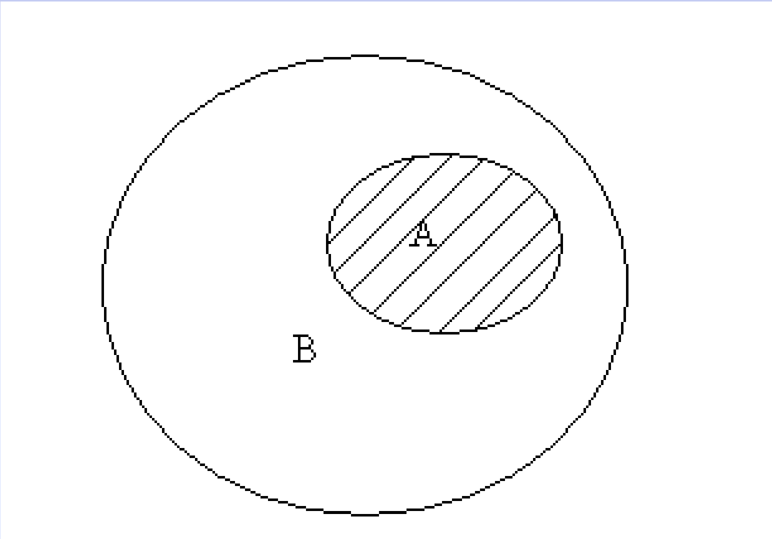
Определение. Множество, не содержащее элементов, называется *пустым*: $\emptyset$. Очевидно, что для любого множества A $\emptyset \subseteq A$ и $A \subseteq A$.

Определение. Множества $\emptyset$ и A называются *несобственными подмножествами* A, все остальные подмножества A называются *собственными*.

Определение. *Универсальным множеством* (*универсумом*) называется множество $\mathcal{U}$, содержащее любое множество как подмножество.

Круги Эйлера (диаграммы Эйлера-Венна)



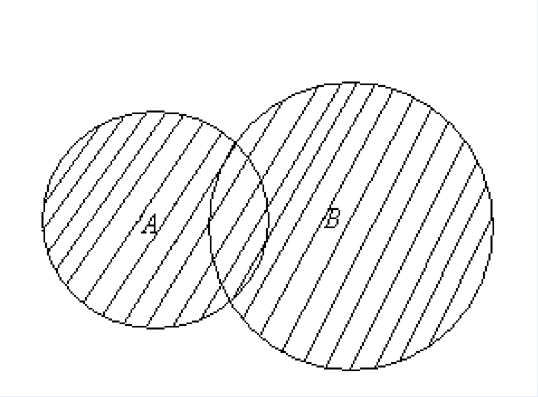


1.2. Способы задания множеств

1. Перечисление элементов.
$A = \{a;\ b;\ t;\ 4;\ 12\}$, $B = \{\text{крокодил}; \text{удав}; \text{бегемот}; \text{улитка}\}$.
2. Задание свойства (свойств) элементов.
$D = \{z \in \mathbb{Z} \mid z = 3k + 1, k \in \mathbb{Z}\}$ ($\mathbb{Z}$ - множество целых чисел).
3. Через операции над множествами.

1.3. Операции над множествами

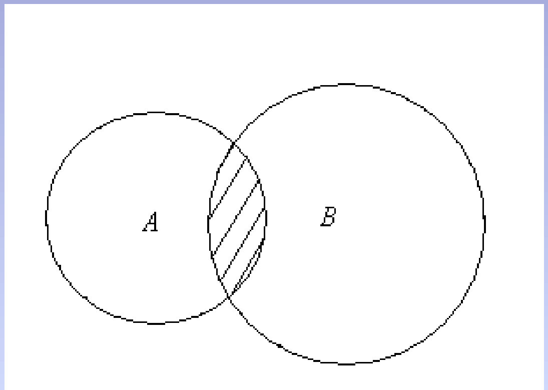
1. Объединение (сумма) множеств.
Определение. *Объединением* множеств A и B называются множество, содержащее элементы, принадлежащие либо A, либо B: $A \cup B$.



1.3. Операции над множествами

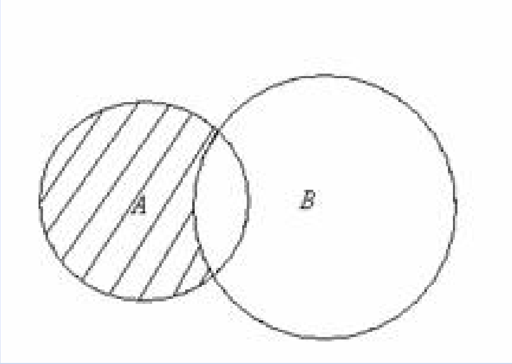
2. Пересечение (произведение) множеств.

Определение. *Пересечением* множеств A и B называются множество, содержащее элементы, принадлежащие A и B одновременно: $A \cap B$.



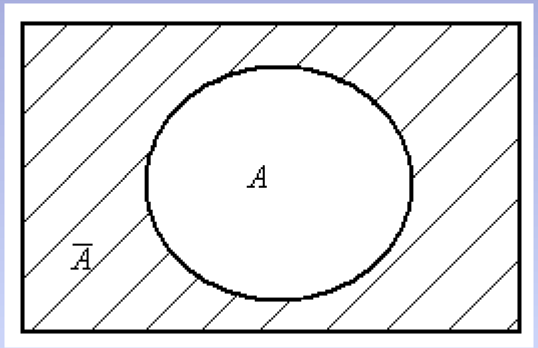
3. Разность множеств.

Определение. *Разностью* множеств A и B называются множество, содержащее элементы A, не принадлежащие B: $A \backslash B$.

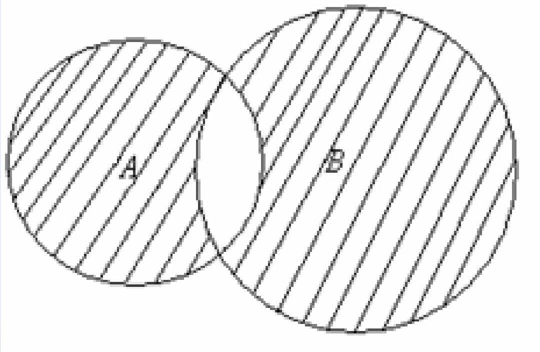


1.3. Операции над множествами

4. Дополнение (отрицание) множества.
Определение. *Дополнением* множества A называются множество, содержащее элементы, не принадлежащие A: $\bar{A}$.



5. Симметрическая разность множеств.
Определение. *Симметрической разностью* множеств A и B называются множество, содержащее элементы, принадлежащие либо A, либо B, но не A и B одновременно: $A \dot{-} B$.



Замечания.

1. Операции объединения и пересечения естественным образом обобщаются на любое конечное число множеств: $A_1 \cup A_2 \cup \cdots \cup A_n$, $A_1 \cap A_2 \cap \cdots \cap A_n$.
2. Из определений операций следуют очевидные тождества:
   a) $A \setminus \mathrm{B} = A \cap \bar{B}$;
   b) $\bar{A} = \mathcal{U} \setminus \mathrm{A}$;
   c) $A \dotdiv B = (A \cup B) \setminus (A \cap B) = (A \setminus \mathrm{B}) \cup (B \setminus \mathrm{A})$.

Определение. *Булеаном* множества A называется семейство всех подмножеств A: $\mathcal{P}(A)$.

1.4. Алгебра множеств

Множества и введённые операции над ними образуют *алгебру множеств*. Определим формулы этой алгебры следующими рекуррентными правилами.

Определение. *Формулой алгебры множеств* называется последовательность символов, построенная по правилам:

1. Любая буква, обозначающая множество, является формулой, символы $\mathcal{U}$, $\emptyset$ также есть формулы.
2. Если $\mathcal{A}$, $\mathcal{B}$ - формулы, то $(\mathcal{A} \cup \mathcal{B})$, $(\mathcal{A} \cap \mathcal{B})$, $(\mathcal{A} \backslash \mathcal{B})$, $(\mathcal{A} \dot{-} \mathcal{B})$, $(\bar{\mathcal{A}})$ также есть формулы.
3. Последовательность символов является формулой в том и только том случае, когда она получена по правилам 1 и 2.

Определение. *Подформулой* формулы называется её часть, сама являющаяся формулой.

1.4. Алгебра множеств

Правила удаления лишних скобок:

1. Внешние скобки можно опускать.
2. Если формула содержит вхождения только одной из операций $\cup$, $\cap$ или $\dot{-}$, то в ней можно опустить все скобки, операции выполняются слева направо.
3. Внешние скобки в формуле вида $(\bar{\mathcal{A}})$, где $\mathcal{A}$ – формула, можно опустить.
4. Можно опускать пары скобок, без которых возможно восстановление исходной формулы по следующим правилам. Каждое вхождение символа $\cap$ связывает наименьшие окружающие его подформулы. После расстановки скобок, относящихся к $\cap$, каждое вхождение $\cup$ относится к наименьшим подформулам слева и справа от него. Далее подобным образом расставляются скобки, относящиеся к символам $\setminus$ и $\dot{-}$.

Таким образом, вводится следующий приоритет операций (по убыванию): дополнение, $\cap$, $\cup$, $\setminus$, $\dot{-}$ (последние три равноприоритетны). Идущие подряд равноприоритетные операции выполняются слева направо.

1.4. Алгебра множеств

Приведём основные законы и правила алгебры множеств.

I. Законы коммутативности:

a) $A \cup B = B \cup A$ (коммутативность объединения);

b) $A \cap B = B \cap A$ (коммутативность пересечения);

c) $A \dotdiv B = B \dotdiv A$ (коммутативность симметрической разности).

II. Законы ассоциативности:

a) $A \cup (B \cup C) = (A \cup B) \cup C$ (ассоциативность объединения);

b) $A \cap (B \cap C) = (A \cap B) \cap C$ (ассоциативность пересечения);

c) $A \dotdiv (B \dotdiv C) = (A \dotdiv B) \dotdiv C$ (ассоциативность симметрической разности).

Замечание. Законы ассоциативности фактически уже заложены правилом 2 опускания лишних скобок.

III. Законы дистрибутивности:

a) $A \cap (B \cup C) = A \cap B \cup A \cap C$ (дистрибутивность пересечения относительно объединения);

b) $A \cup B \cap C = (A \cup B) \cap (A \cup C)$ (дистрибутивность объединения относительно пересечения).

IV. Законы идемпотентности:

a) $A \cup A = A$ (идемпотентность объединения);

b) $A \cap A = A$ (идемпотентность пересечения).

1.4. Алгебра множеств

V. Закон исключённого третьего: $A \cup \bar{A} = \mathcal{U}$.

VI. Закон противоречия: $A \cap \bar{A} = \emptyset$.

VII. Закон двойного отрицания: $\bar{\bar{A}} = A$.

VIII. Законы двойственности де Моргана:

a) $\overline{A \cup B} = \bar{A} \cap \bar{B}$;

b) $\overline{A \cap B} = \bar{A} \cup \bar{B}$.

IX. Правила поглощения:

a) $A \cup A \cap B = A$;

b) $A \cap (A \cup B) = A$.

X. Правила склеивания:

a) $A \cap B \cup A \cap \bar{B} = A$;

b) $(A \cup B\ ) \cap (A \cup \bar{B}) = A$.

XI. $A \cup \bar{A} \cap B = A \cup B$.

§2. Отношения

2.1. Декартово произведение

Определение. *Вектором* (*кортежем*) длины (размерности) n называется упорядоченная последовательность элементов: $\langle a_1, a_2, \dots, a_n \rangle$.

Таким образом, два вектора равны тогда и только тогда, когда у них на соответствующих позициях находятся одинаковые элементы.

Определение. *Декартовым* (*прямым*) *произведением* множеств $A_1, A_2, \dots, A_n$ называется множество $A_1 \times A_2 \times \dots \times A_n$ всех векторов $\langle a_1, a_2, \dots, a_n \rangle$, в которых $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$: $A_1 \times A_2 \times \dots \times A_n = \{\langle a_1, \dots, a_n \rangle | a_1 \in A_1, \dots, a_n \in A_n\}$.

Если $A_1 = \dots = A_n = A$, то $A_1 \times \dots \times A_n = A^n$ - декартова (прямая) степень множества A.

Ниже приведены свойства декартова произведения.

1. Дистрибутивность относительно объединения справа и слева:
   a) $(A \cup B) \times C = (A \times C) \cup (B \times C)$;
   b) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
2. Дистрибутивность относительно пересечения справа и слева:
   a) $(A \cap B) \times C = (A \times C) \cap (B \times C)$;
   b) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

3. Дистрибутивность относительно разности справа и слева:
   a) $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$;
   b) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

Замечания.

1. Свойства 1-2 естественным образом обобщаются на любые конечные объединения и пересечения.
2. В общем случае декартово произведение некоммутативно и неассоциативно.

2.2. Бинарные отношения

Определение. *Отношением арности* n (*n-арным отношением*) на множествах $A_1, A_2, \ldots, A_n$ называется подмножество декартова произведения $A_1 \times A_2 \times \cdots \times A_n$; *$n$-арным отношением на множестве* A называется подмножество декартовой степени A^n.

Отношение арности 3 называется *тернарным*, арности 2 – *бинарным.*

Определение. *Бинарным отношением* на множествах A, B называется подмножество декартова произведения $A \times B$.

Обозначение: $\langle a; b\rangle \in R \Leftrightarrow aRb$.

Определение. *Областью определения бинарного отношения* $R \subseteq A \times B$ называется множество δ_R элементов $a \in A$, для которых aRb при некотором $b \in B$:

$$\delta_R = \{a \in A \mid aRb \text{ при некотором } b \in B\}.$$

Определение. *Областью значений бинарного отношения* $R \subseteq A \times B$ называется множество ρ_R элементов $b \in B$, для которых aRb при некотором $a \in A$:

$$\rho_R = \{b \in B \mid aRb \text{ при некотором } a \in A\}.$$

2.2. Бинарные отношения

Определение. *Обратным к бинарному отношению* R называется бинарное отношение $R^{-1} = \{\langle a; b\rangle \mid bRa\}$.

Определение. *Дополнением бинарного отношения* $R \subseteq A \times B$ называется бинарное отношение $-R = (A \times B)\backslash R$.

Определение. *Образом множества* $X \subseteq \delta_R$ *при бинарном отношении* $R \subseteq A \times B$ называется множество $R(X)$ элементов $b \in B$, для которых aRb при некотором $a \in X$:

$$R(X) = \{b \in B | aRb \text{ при некотором } a \in X\}.$$

Определение. *Прообразом множества* $Y \subseteq \rho_R$ *при бинарном отношении* $R \subseteq A \times B$ называется множество $R^{-1}(Y)$:

$$R^{-1}(Y) = \{a \in A\ |bR^{-1}a \text{ при некотором } b \in Y\} =$$
$$= \{a \in A\ |aRb \text{ при некотором } b \in Y\}.$$

Определение. *Композицией бинарных отношений* $R_1 \subseteq A \times B$ и $R_2 \subseteq B \times C$ называется бинарное отношение

$$R_1 \circ R_2 = \left\{\langle a; b\rangle \mid aR_1c \;\&\; cR_2b \text{ при некотором } c \in \rho_{R_1} \cap \delta_{R_2}\right\}.$$

2.2. Бинарные отношения

Свойства бинарных отношений:

1. $(R^{-1})^{-1} = R$;
2. 1) $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$;
   2) $(R \cap S)^{-1} = R^{-1} \cap S^{-1}$;
3. $-R^{-1} = (-R)^{-1}$;
4. $R \circ (S \circ T) = (R \circ S) \circ T$, где $R \subseteq A \times B$, $S \subseteq B \times C$, $T \subseteq C \times D$;
5. $(R \circ S)^{-1} = S^{-1} \circ R^{-1}$, где $R \subseteq A \times B$, $S \subseteq B \times C$;
6. $(R \circ S)(X) = S\big(R(X)\big)$, где $R \subseteq A \times B$, $S \subseteq B \times C$, $X \subseteq A$;
7. 1) $(R \cup S) \circ T = R \circ T \cup S \circ T$, где $R, S \subseteq A \times B$, $T \subseteq B \times C$;
   2) $R \circ (S \cup T) = R \circ S \cup R \circ T$, где $R \subseteq A \times B$, $S, T \subseteq B \times C$;
8. 1) $(R \cap S) \circ T \subseteq R \circ T \cap S \circ T$, где $R, S \subseteq A \times B$, $T \subseteq B \times C$;
   2) $R \circ (S \cap T) \subseteq R \circ S \cap R \circ T$, где $R \subseteq A \times B$, $S, T \subseteq B \times C$;
9. 1) $\delta_{R^{-1}} = \rho_R$;
   2) $\rho_{R^{-1}} = \delta_R$.

2.3. Функции

Определение. Бинарное отношение $f \subseteq A \times B$ называется *функцией из* A *в* B, если $\delta_f = A$, $\rho_f \subseteq B$ и для всех $x \in \delta_f$, $y_1, y_2 \in \rho_f$ из xfy_1 и xfy_2 следует $y_1 =$
$= y_2$.

Функцию f из A в B будем обозначать $f\colon A \to B$. Вместо xfy пишем $y = f(x)$, где x – *аргумент*, y – *значение* функции.

Определение. Функция f называется *инъекцией* ($(1-1)$-*функцией*) из A в B, если из $x_1 \neq x_2$ следует $f(x_1) \neq f(x_2)$.

Определение. Функция $f\colon A \to B$ называется *сюръекцией* A *на* B, если $\rho_f = B$.

Определение. Функция $f\colon A \to B$, являющаяся и инъекцией, и сюръекцей называется *биекцией* (*взаимно-однозначным соответствием*) между A и B.

Определение. Биекция $f\colon A \to A$ называется *подстановкой* множества A.

Свойства функций:

1. $f(A \cup B) = f(A) \cup f(B)$, где $A, B \subseteq \delta_f$;
2. $f(A \cap B) \subseteq f(A) \cap f(B)$, где $A, B \subseteq \delta_f$;
3. $f(A) \setminus f(B) \subseteq f(A \setminus B)$, где $A, B \subseteq \delta_f$;
4. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$, где $A, B \subseteq \rho_f$;

2.3. Функции

5. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$, где $A, B \subseteq \rho_f$;
6. $f^{-1}(A \backslash B) = f^{-1}(A) \backslash f^{-1}(B)$, где $A, B \subseteq \rho_f$.

Лемма 2.1. Если f – функция из A в B, то f^{-1} является функцией из $\rho_f \subseteq B$ в A тогда и только тогда, когда f – инъекция.

Следствие. Если функция f является инъекцией, то $f(A \cap B) = f(A) \cap f(B)$, $f(A \backslash B) = f(A) \backslash f(B)$, где $A, B \subseteq \delta_f$.

Лемма 2.2. Функция f является взаимно-однозначным соответствием между A и B тогда и только тогда, когда f^{-1} также является взаимно-однозначным соответствием.

Следствие. Функция f является подстановкой множества A тогда и только тогда, когда f^{-1} также является подстановкой A.

Лемма 2.3. Если f – функция из A в B, g **-** функция из $\rho_f \subseteq B$ в C, то $f \circ g$ **–** функция из A в C.

2.4. Специальные бинарные отношения

Начиная с этого пункта, рассматриваются бинарные отношения R на множестве A, т.е. подмножества A^2. Считаем, что $\delta_R = A$.

Определение. Бинарное отношение $R \subseteq A^2$ называется *рефлексивным* (*иррефлексивным*), если для всех $a \in A$ aRa (неверно, что aRa).

Определение. Бинарное отношение R называется *симметричным*, если для всех a, $b \in A$ из aRb следует bRa.

Определение. Бинарное отношение R называется *антисимметричным*, если для всех a, $b \in A$ из aRb & bRa следует $a = b$.

Определение. Бинарное отношение R называется *транзитивным*, если для всех a, b, $c \in A$ из aRb & bRc следует aRc.

Определение. Рефлексивное, симметричное и транзитивное бинарное отношение называется *эквивалентностью*.

Лемма 2.4. Симметричное и антисимметричное бинарное отношение является транзитивным.

Лемма 2.5. Если бинарные отношения R, S симметричны, то $R \circ S$ симметрично тогда и только тогда, когда $R \circ S = S \circ R$.

2.4. Специальные бинарные отношения

Лемма 2.6. Бинарное отношение R транзитивно тогда и только тогда, когда $R \circ R \subseteq R$.

Лемма 2.7. Если бинарные отношения R, S - эквивалентности, то $R \circ S$ является эквивалентностью тогда и только тогда, когда $R \circ S = S \circ R$.

Лемма 2.8. Бинарное отношение R является эквивалентностью тогда и только тогда, когда R^{-1} - также эквивалентность.

Пусть на множестве A задана эквивалентность R.

Определение. *Классом эквивалентности* элемента $a \in A$ по R называется множество a/R всех элементов A, находящихся в отношении R с a:

$$a/R = \{b \in A | bRa\}.$$

Определение. Множество классов эквивалентности элементов A по R называется *фактор-множеством* $A\ /\ R$: $A/R = \{a\ /\ R | a \in A\}$.

Теорема 2.1. Классы эквивалентности попарно не пересекаются, и их объединение равно A.

Определение. *Разбиением множества* A называется система попарно не пересекающихся подмножеств A, объединение которых равно A.

Теорема 2.1 утверждает, что фактор-множество является разбиением A.

2.5. Отношения порядка

Определение. Бинарное отношение $R \subseteq A^2$ называется *предпорядком* (*квазипорядком*) на A, если оно рефлексивно и транзитивно.

Определение. Бинарное отношение R называется *частичным порядком*, если оно рефлексивно, транзитивно и антисимметрично. Обозначается $\leq$.

Определение. Бинарное отношение $\leq^{-1}$ называется *двойственным к порядку* $\leq$. Обозначается $\geq$.

Лемма 2.9. Порядок, двойственный к частичному, является частичным.

Определение. Частичный порядок $\leq$ называется *линейным*, если для любых $a, b \in A$ либо $a \leq b$, либо $b \leq a$.

Определение. Множество, на котором задан частичный (линейный) порядок, называется *частично* (*линейно*) *упорядоченным*.

Определение. Элемент a частично упорядоченного множества называется *максимальным* (*минимальным*), если из $a \leq x$ ($x \leq a$) следует $a = x$.

Определение. Элемент a частично упорядоченного множества A называется *наибольшим* (*наименьшим*), если $x \leq a$ ($a \leq x$) для всех $x \in A$.

Лемма 2.10. Частично упорядоченное множество имеет не более одного наибольшего (наименьшего) элемента.

2.5. Отношения порядка

Лемма 2.11. Наибольший (наименьший) элемент является единственным максимальным (минимальным).

Замечание. Обратное утверждение в общем случае неверно, т.е. максимальный (минимальный) элемент может не быть наибольшим (наименьшим).

Лемма 2.12. В линейно упорядоченном множестве элемент является наибольшим (наименьшим) тогда и только тогда, когда он максимален (минимален).

Определение. *Верхней* (*нижней*) *гранью* подмножества B частично упорядоченного множества A называется такой элемент $a \in A$, что для любого $b \in B$ $b \leq a$ ($a \leq b$).

Определение. *Точной верхней* (*точной нижней*) *гранью* подмножества B частично упорядоченного множества A называется наименьшая верхняя (наибольшая нижняя) грань B.

Обозначается $\sup B$ ($\inf B$).

Определение. Линейный порядок на множестве A называется *полным*, если каждое непустое подмножество A имеет наименьший элемент.

Определение. Множество, на котором задан полный порядок, называется *вполне упорядоченным*.