Алгебра и теория чисел

Иванова Ольга Юрьевна[1]

08.09.2023 - ...

[1]"Записал Сергей Киселев"

Оглавление

Глава 1

Множества

Лекция 1: Операции над множествами

08.09.2023

1.1 Операции над множествами

Обозначение. $x \in A$ означает, что элемент x принадлежит множеству A.

$x \notin A$ означает, что элемент x не принадлежит множеству A.

Определение 1. $\emptyset$, пустое множество - множество, не содержащее ни одного элемента.

Определение 2. Множество B называют подмножеством A, если любой элемент B принадлежит A.

Обозначение. $B \subset A$

Пример. $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$

Операции.

1. Пересечение множеств A и B - это множество из элементов принадлежащих A и B.

   Обозначение. $A \cap B$

2. Объединение множеств A и B - множество из элементов A или B.

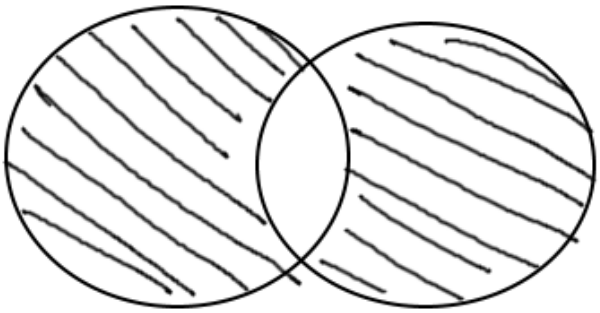
   Обозначение. $A \cup B$

3. Разность множеств A и B - множество элементов A, не принадлежащих B.

   Обозначение. $A \setminus B$

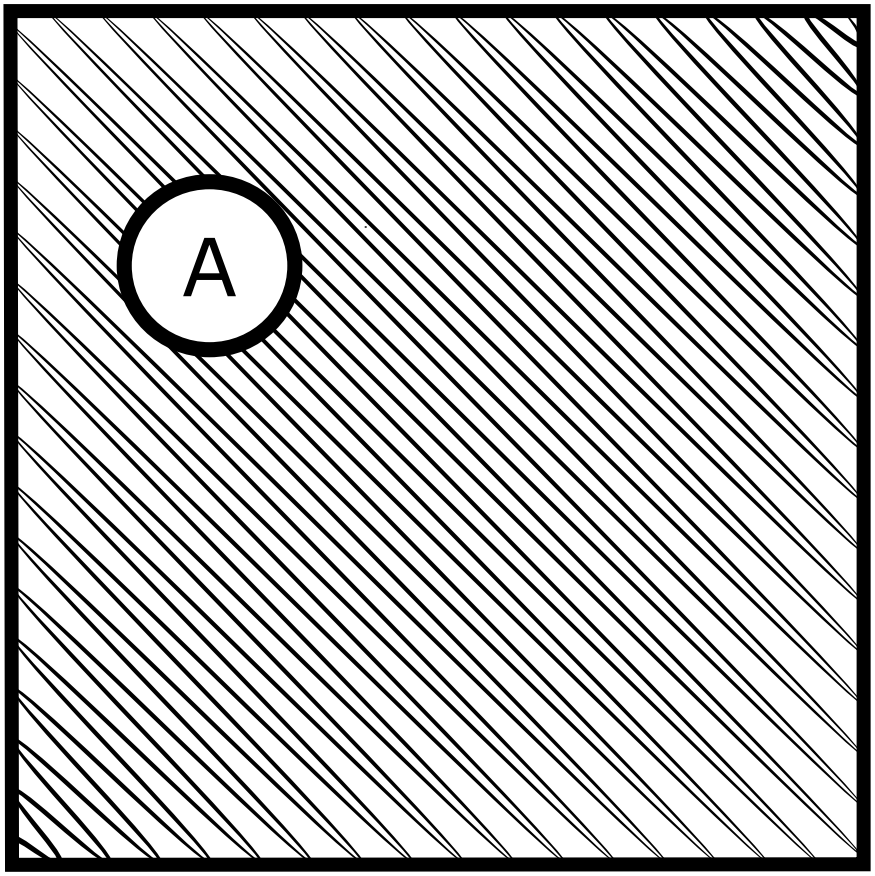
4. Симметрическая разность

Пример. $A \triangle B = (A \setminus B) \cup (B \setminus A)$
$A \triangle B = (A \cup B) \setminus (A \cap B)$



5. Дополнение

Если предположить, что все множества являются поднмножествами некоторого универсального множества, дополнение множества A - это множество элементов U, не принадлежащих A.



Пример. $U = \mathbb{Z}$
A - множество чётных чисел
$\overline{A}$ - множество нечётных чисел

Порядок действий

1. Дополнение
2. Пересечение
3. Объединение, рахность, симметрическая разность

Приоритет слева направо.

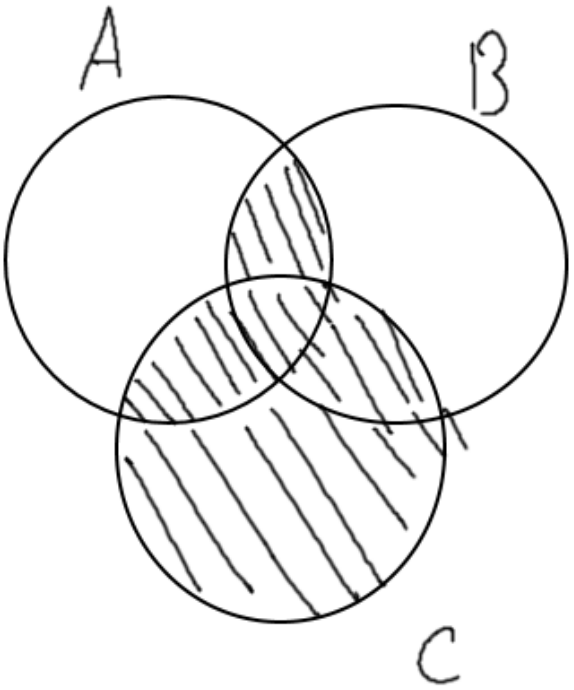
Пример. $U = \{1,2,3,4,5\}$ $A = \{1,2,3\}$ $B = \{3,4\}$ $C = \{4,5\}$
$\overline{A \cup B \cap \overline{C} \setminus \overline{B}}$

1. $\overline{C} = \{1,2,3\}$
2. $\overline{B} = \{1,2,5\}$
3. $B \cap \overline{C} = \{3\}$

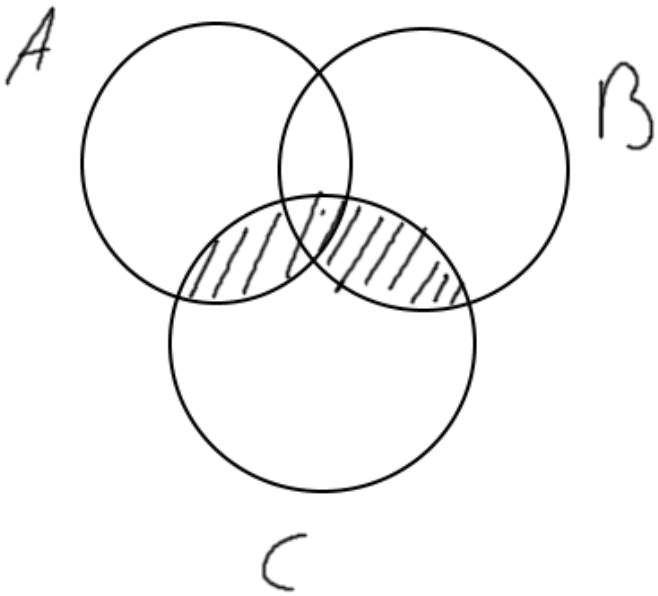
4. $A \cup B \cap \overline{C} = \{1, 2, 3\}$
5. $A \cup B \cap \overline{C} \setminus \overline{B} = \{3\}$
6. $\dots = \{1, 2, 4, 5\}$

Свойства:

1. Дистрибутивность
   (a) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$



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



Доказательство. Положим $D = (A \cap B) \cup C$

$E = (A \cup C) \cap (B \cup C)$

Докажем, что $C \subset E$

Пусть $x \in D$, тогда выполняется

(a) $x \in A \cup B$ или

(b) $x \in C$

Если выполнено 1, то x $\in A \cup B$ => $x \in A$ => $x \in A \cup C \in A \cap B$ => $A \in B$ => $x \in B \cup C$ => $x \in (A \cup C) \cap (B \cup C)$

Если выполнено 2, то $x \in C$ => $x \in AcupC$ => $x \in (A \cup C) \cap (B \cup C)$

$x \in C$ => $x \in B \cup c$

$x \in E$ => $x \in A \cup C$ и $x \in B \cup C$

Случай 1. $x \notin C$

- $x \notin C$, $x \in A \cup C$ => $x \in A$

- $x \neq C$, $x \in B \cup C => x \in B$

$=> x \in A \cap B = .x \in B$

Случай 2. $x \in C$

$=> x \in (A \cap B) \cup C => x \in D$ □

2. Законы де Моргана
   (a) $\overline{A \cup B} = \overline{A} \cap \overline{B}$
   (b) $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Прямым или декартовым произведеним множеств A и B называют множество упорядоченных пар (a, b), где $a \in A$, $b \in B$

Обозначение. $A \times B$

Пример. 1. $A = \{1, 2\}$, $B = \{x, y\}$
$A \times B = \{(1, x), (1, y), (2, x), (2, y)\}$

2. $A = \{1, 2\}$, $B = \{1\}$
$A \times B = \{(x, y) | x, y \in \mathbb{R}\}$

3. $A = B = R$
$A \times B = \{(x, y) | x, y \in \mathbb{R}\}$

Св-во: между элементами множеств $(A \times B) \times C$ и $A \times (B\ timesC)$ есть взаимно однозначное соответствие.

Определение 3. $A \times B \times C$ - Это $(A \times B) \times C$
$A^n = A \times A \times ...A$

Пример. $0, 1^3$ элементов (0,0,0), (0,0,1), ..., (1,1,1)

1.2 Отображения

Определение 4. Отображением или функцией из множества X в множество Y называют правило, которое каждому элементу множества X сопоставляет ровно один элемент из множества Y.

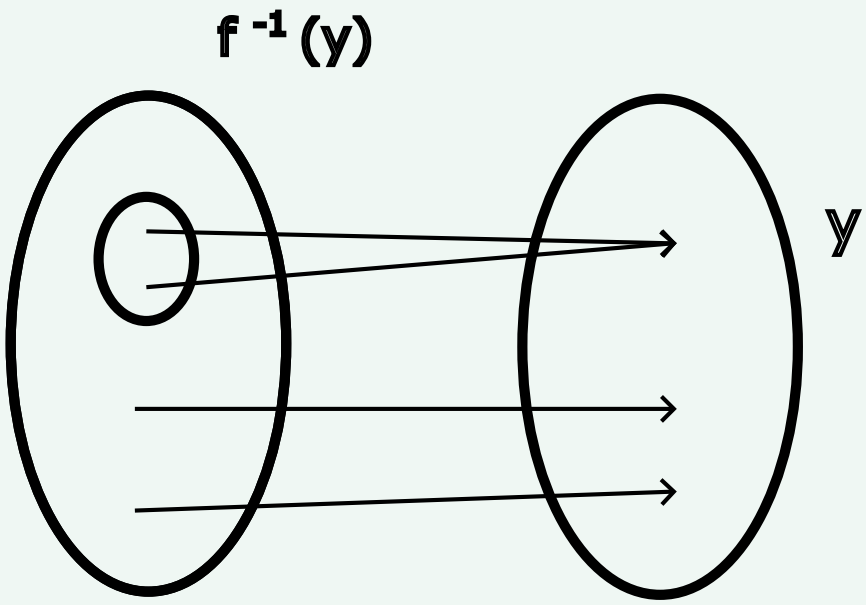
Пример. 1. $X = \{a, b, c, d\}$ $Y = \{1, 2, 3\}$
$f(a) = 1$
$f(b) = 2$
$f(c) = 1$
$f(d) = 1$

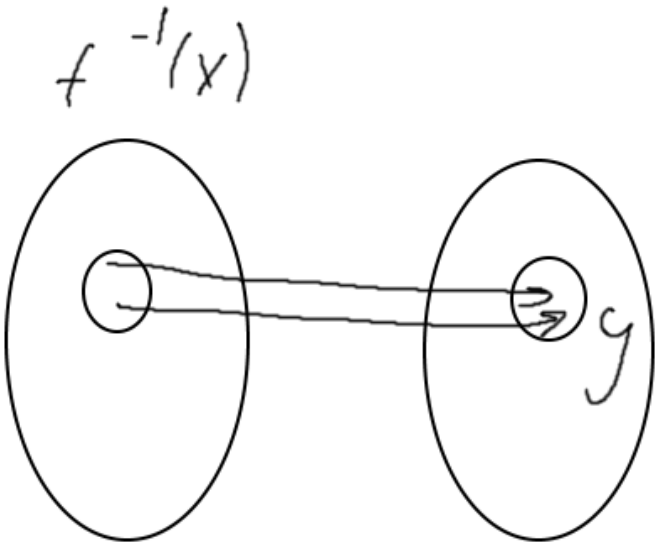
2. $X = Y = \mathbb{R}$
   $f(x) = x^2 =$

Определение 5. Образом отображения f называют множество элементов $f(x)$ т.к. $\{f(x)|x \in X\}$

Обозначение. $Imf, f(X)$

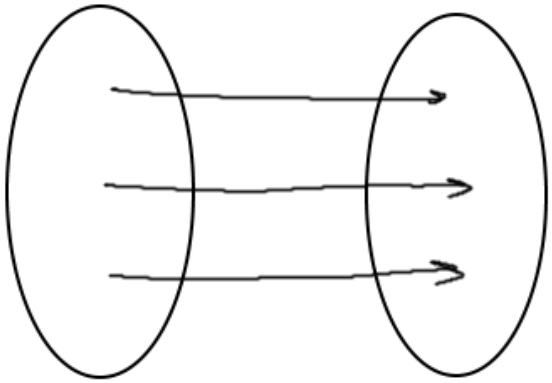
Определение 6. Прообразом элемента $y \in X$ называют множество элементов множества X, которые переходят в y, т.е.
$\{x \in X|f(x) = y\}$





Обозначение. $f^{-1}(y)$
Если $y_1 \subset y$, то
$f^{-1}(y_1) = \{x \in X | f(x) \in y_1\}$

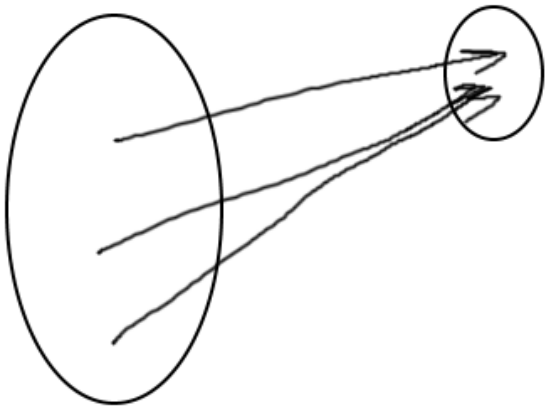
Определение 7. Отображением f называют иньективным, если прообраз любого элемента содержит не более одного элемента.



Др. названия:

- f - иньекция
- f является отображением в

Определение 8. Отображение f называется сюрьективным, если если прообраз любого элемента содержит хотя бы один элемент.



Др. названия:

- f - сюръекция
- f является отображением на

Определение 9. Отображение f называется биективным, если прообраз любого элемента состоит ровно из одного элемента.

Др. названия:

- f - биекция
- f - взаимно однозначное отображение

Замечание. f биекция <=> f - инъекция и сюръекция.

Пример. $f : \mathbb{Z} \to \mathbb{Z}$

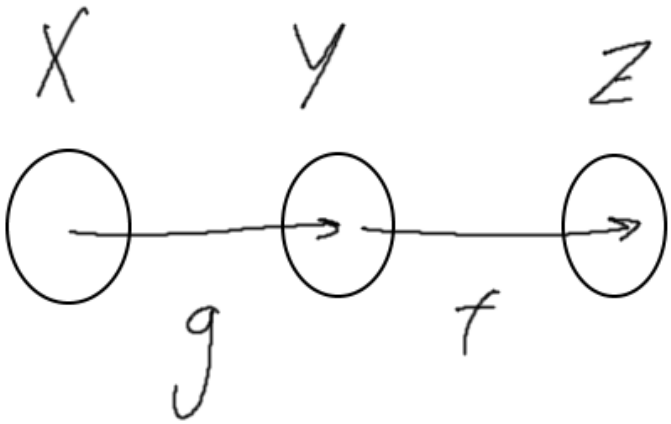
1. $f(x) = x + 1$ - биекция
2. $f(x) = x^2$ - не иньекция, не биекция

$f^{-1}(4) = \{2. - 2\}$
$f^{-1}(5) = \emptyset$
$\alpha \subset 2$

3. $f(x) = 2x$ - инъекция, не сюръекция
   $f^{-1} = \emptyset$
   $x_1 \neq x_2 => 2x_1 \neq 2x_2$
4. $f(x) = [\frac{x}{2}]$ не иньекция
   $[\frac{0}{2}] = [\frac{1}{2}]$
   $2n \in f^{-1}(n)$
   $=>$
   $f^{-1}(n) \neq \emptyset$

Определение 10. Тождественное отображение $e_x : x \to x_1, e_x(x) = x$

Определение 11. Пусть $y : X - Y, f : X \to Z$



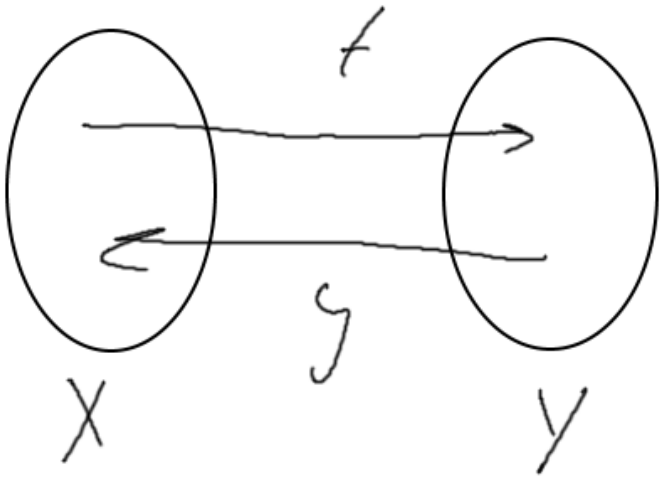
отображение композиция fog определяется как
$(fog)(x) = f(g(x))$

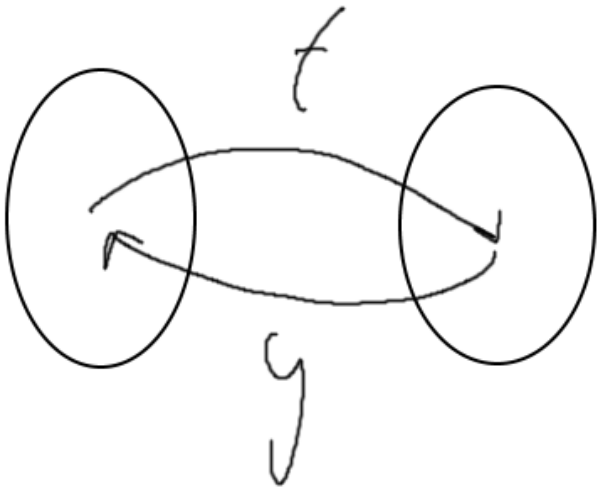
Пример. $X = Y = \mathbb{Z} = \mathbb{R}$
$f(x) = x + 1, y(x) = x$
$(fog)(x) = x^2 + 1$
$(gof)(x) = (x + 1)^2$

Замечание. $(fog)oh = fo(goh)$

Обозначение. $fogoh$

Определение 12. Пусть $f : X \to Y, y : Y \to V$
Отображение y называют образом к отображениб f, если
$fog = e$
$gof = e$





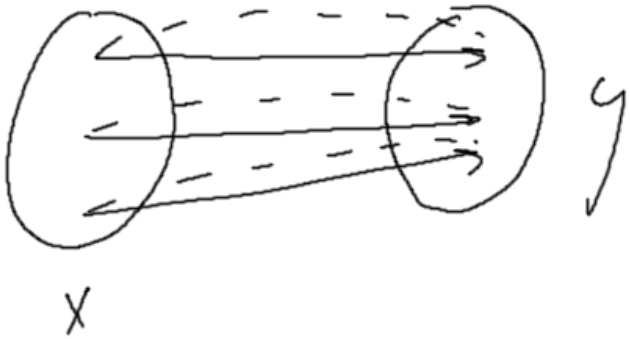
Пример. $X = Y = [0; +\infty]$
$f(x) = x^2, y(x) = \sqrt{x}$

Определение 13. Обратное отображение к f обозначается f^{-1}
(Корректность, т.е. единственность отображения обратных - ниже)

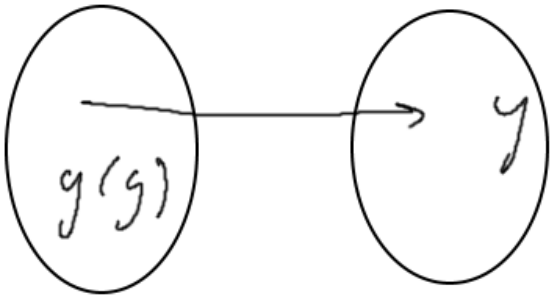
Теорема 1. (Существование обр. отображения)
Обратное отображение к f существует тогда и только тогда, когда f является биекцией.

Доказательство. 1. Доказать, что если f биекция, то существует y, обратное к f

Пусть $y \in X \exists! x$, такой, что $f(x) = y$



Положим $y(y) = x$



Теорема 2. (Единственности обратного отображения)
Пусть f - Биекция $X \to Y$. Тогда не существует различных отображений y_1, y_2 являющихся обратными к A.

Доказательство. Доказательство: Упражнение! □

Лекция 2: Бинарные отношения

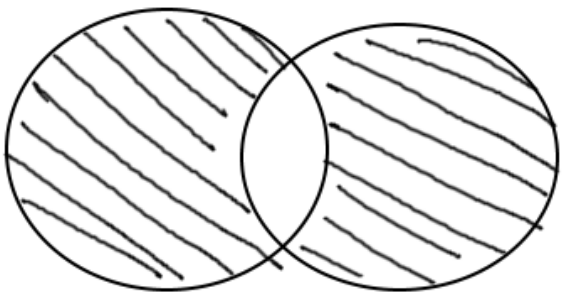
15.09.2023

1.3 Бинарные отношения

Определение 14. Бинарноным отношением между множествами X и Y называют подмножество $X \times Y$

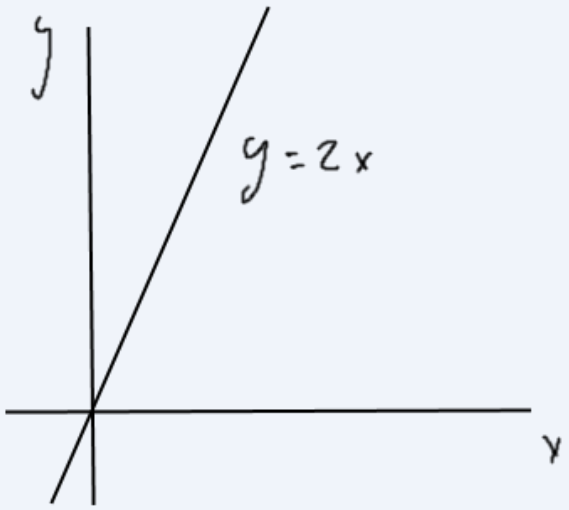
Обозначение. Пусть задано $w \subset X \times Y$. Тогда, условие $(x, y) \in w$ записывается как XwY

Обозначение. Если X = Y, то говорят, что w - отношение на X.

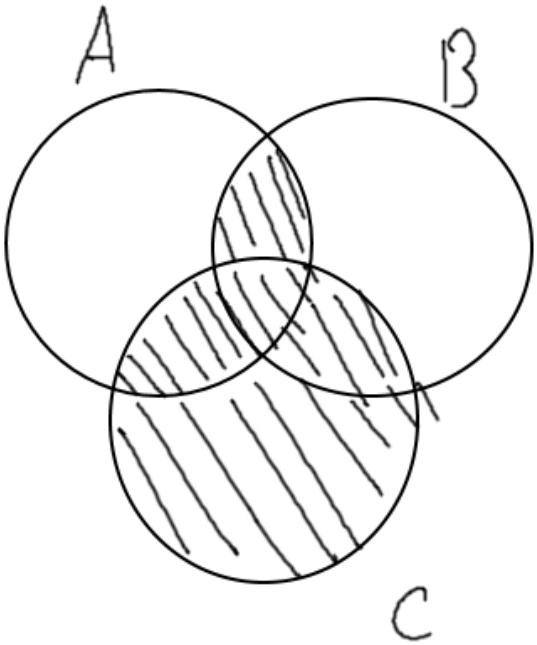


Доказательство. Пусть g_1, g_2 - отображения к R.
$q_1 \neq q_2$
$\exists g : g, (g) \neq g = (g)$
$x_i = y_1(y), x_2 := g_2(y)$
$f(x_1) = f(g_1(y)) = g = f(g_2(y)) = f(x_2)$
$f(x_1) = f(x_2)$
$x_1 \neq x_2$ □

Пример. 1. $f(x) = 2x$
xwy, если $g = f(x)$



2. xwy, если $x^2 = y$



Определение 15. Бинарное отношения w на X называется

1. Рефлексивным, если xwy и ywz
2. Симметричным, если из того что xwy и ywz следует, что xwf

Пример. 1. $=, \leq$ - рефлексивное
$<$, паралленльно на множестве прямых - не рефлексивно

2. $=, ||$ - симметрично
$leq, <$ - не симметрично

3. $=, <, \vdots$ - транзитивно
$\perp$ - на множестве прямх - не транзитивно

Определение 16. Бинарное отношение на множестве X называется отношением эквивалентности, если оно рефлексивно, симметрично и транзитивно.

Обозначение. Обычно обозначается $\sim$.

Пример. 1. $=$ на $\mathbb{R}$

2. Множество $\mathbb{Z}$ $a \sim b$, если $a - b \vdots 5$

   Обозначение. $\overline{\overline{5}}$

3. Множество проямых на плоскости $l_1 \sim l_2$, если $l_2 || l_2'$, если $L_1 = l_2$
4. Пусть множество - это множество направленных отрезков $\overline{AB} \sim \overline{CD}$, если $|\overline{AB}| = |\overline{CD}|$, $AB||CD$.
5. $f(x), g(x)$ - функции $f \sim g$, если $\lim\limits_{x \to \infty} \frac{f(x)}{f(y)} = 1$

Определение 17. Пусть на X задано отношение эквивалентности. Классом эквивалентности x называется множество элементов $\{y \in X | y \sim X\}$.

Обозначение. $\overline{x}$, $[x]$, $((x)$

Примечание. Черта над x должна быть немного загнута вниз слева. Также первый вариант обозначения является основным.

Пример. $R, x \sim y, x - y \in \mathbb{Z}$
$x = 0, 1$
0,1; 1,1;$-0.9 \in \overline{x}$
$\overline{x} = \{y | \{y\} = \{x\}\}$

Пример. $1, 1 \in \overline{0, 1}$
$0, 1 \in \overline{1, 1}$
$\{y\} = 0, 1$

5 классов эквивалентности:
5k
5k + 1
5k + 2
5k + 3
5k + 4

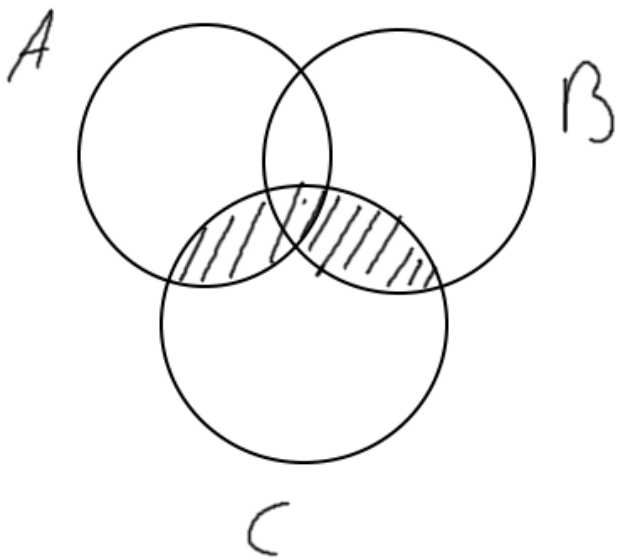
Теорема 3. (Разбиение на классы жкивалентности) На множестве X задано отношение эквивалентности . Тогда, множество X разбивается на классы эквивалентности, т.е. X является обьединением не пересекающихся подмножеств, каждое из которых является классом эквивалентности некоторого элемента.

Пример. 1. $\overline{\overline{\overline{5}}}$

$a \sim b$, если $a - b \vdots 5$

2. $=$ в каждом классе 1 элемент
3. Направленные отрезки $overline AB \sim \overline{CD}$, если $|\overline{AB}| = |\overline{CD}|$, $AB \uparrow\uparrow CD$

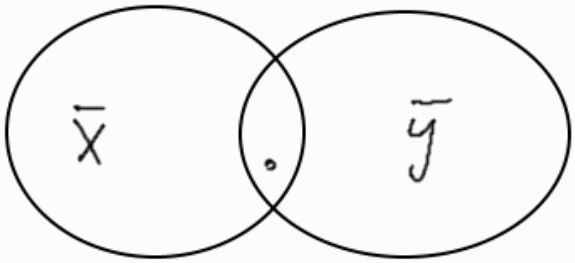
   Класс эквивалентности - вектор.
4. R $a \sim b$, если $\alpha - \beta = 2\pi\kappa$



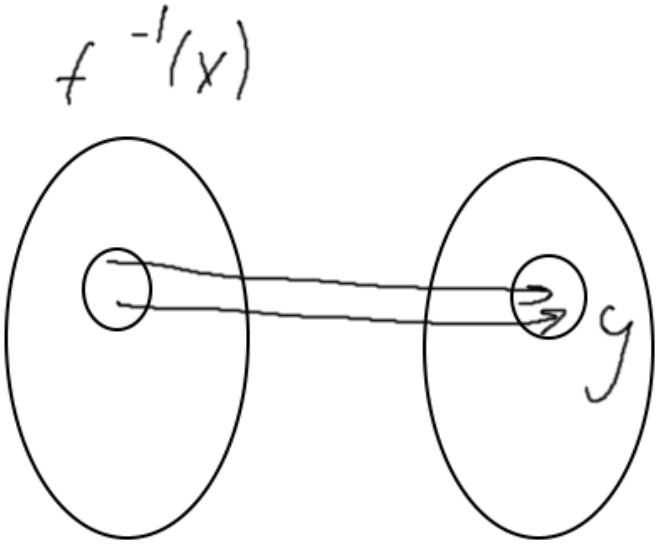
Доказательство. 1. Докажем, что любой элемент X принадлежит некоторому классу эквивалентности.

$X \in \overline{X}$, т.к. $\sim$???, X x

2. Докажем, что классы не пересекаются



т.е. докажем, что если $\exists z \in \overline{x} \cap \overline{y}$, то $\overline{x} = \overline{y}$

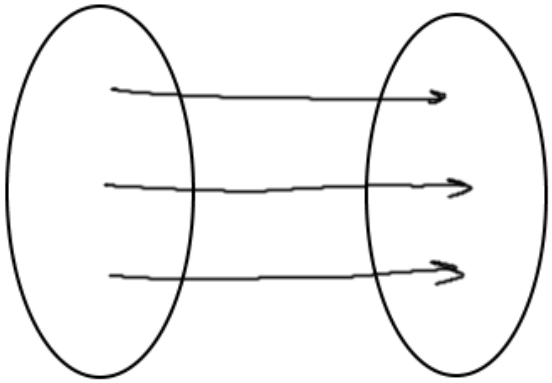


$z \in x \Rightarrow z \sim x \Rightarrow$ (симм) $x \sim z$

$z \in \overline{y} \Rightarrow$ z Y

x z, z y $\Rightarrow$ (тр) x y $\Rightarrow x \in y \Rightarrow x \in \overline{y}$

аналогично $y \in \overline{x}$



$x = \overline{y}$
Докажем, что $\overline{x} \subset y$
Пусть $\exists f \in \overline{x} => f \sim x$
$f \sim x, x = y => f \sim y$
Аналогично $\overline{y} \subset \overline{x}$
$\overline{x} = \overline{y}$ □

1.4 Множество с алгебраическими операциями

Определение 18. X - множество бинарныой алгебраической операции на X Назвается отображением $X \times X \to X$

Обозначение.
1. Буква, например $f : X \times X \to X$ пишут $f(x, y)$ или xfy
2. Спец. символ: $+$, $\cdot$, 0, * Пишут x + y, x * y
   часто вместо $x \cdot y$, x * y пишут xy

Пример. 1. $X = \mathbb{Z}$

Определить $+$, $\cdot$, -

2. X - множество отображений $\mathbb{Z} \to \mathbb{Z}$,

операция - композиция.

3. X - множество векторов

Обозначение. Множество X с операцией V обозначается (V, *)

Определение 19. Бинарная операция * на X Назвается

1. Ассоциативной, если $(x * y * z) = x * (y * z) \forall x, y, z$
2. Коммутативной, если $x * y = y * x \forall x, y$

Пример. 1. $+$, $\cdot$ - коммутативные, ассоциативные

X : y на $\mathbb{R} \setminus \{0\}$ не ассоциативно, не коммутативно

x - y на $\mathbb{R}$

x - векторное произведение

2. ассоциативны, не коммутативны o - композиция для отображения $\mathbb{Z} \to \mathbb{Z}$

Обозначение. Пусть * - ассоциативно
Тогда пишут a * b * c, a * b * c * d
Используют обозначение степени, например a^4 = a * a * a * a
Если операция обозначается $+$, пишут
$4a = a + a + a + a$

Пример. 1. (Z, $\cdot$) e = 1

2. (Z, $+$) e = 0

3. (2Z, $\cdot$) нет ? элемента, множества четных чисел

Замечание. Если операция обозначается $+$, то неитральный элемент обозначается 0.

Свойство. (единственности единичного элемента)
На x Задана операция *. Тогда существует не более одного единичного элемента.

Доказательство. Пусть e_1, e_2 - единичные, т.е.
$\forall_x \; e_1 + x = x, x + e_1 = x \; e_2 * x = x, x * e_2 = x$

$e_2 =$(ед. эл.)$e_1 * e_2 =$(ед.эл.)$e_1 => e_1 = e_2$

□

Определение 20. Полугруппой называется множество с заданной на нем бинарной ассоциативной операцией.

Определение 21. Моноидом называется полугруппа, в которой есть неитральный элемент

Пример.
1. ($\mathbb{Z}$, $+$) - моноид
2. (Z, $\cdot$) - моноид
3. ($2\mathbb{Z}$, $\cdot$) - полугруппа, не моноид
4. ($\mathbb{Z}$, -) - вектор $\subset x$ - не полугруппа

1.5 Группы

Определение 22. Множество G с бинарной операцией * называется группой, если выполнены следующие условия.

1. Операция * ассоциативна, т.е. (a * e) * c = a * (b * c) $\forall a, b, c$
2. $\exists$ единица $e : a * e = e * a = a \forall a$
3. $\forall a \exists$ Обратный элемент a' $\in G$ такой, что $a * a^-1 = a^-1 * a = e$

Обозначение. Если операция обозначается -1, то единичные жлементы обозначаются o, а обратный элемент a обозначается -a.

Определение 23. Пусть (G, *) - группа, если * коммутативна, то группа G называется коммутативной или абелевой.