Лекция 3
Специальные бинарные отношения

1. Отношение эквивалентности. Классы эквивалентности.
2. Отношения порядка.
3. Упорядоченные множества.

© I.Krivtsova
ITMO University

Литература

1. Бухштаб А.А. Теория чисел. СПб., 2020:

https://e.lanbook.com/book/147139

2. Нестеренко Ю.В. Теория чисел. М., 2008.

1. Отношение эквивалентности

Пусть $X \neq \varnothing$.

- **Определение 1**

Бинарное отношение Q на X называется отношением эквивалентности, если оно:

- ✓ рефлексивно,
- ✓ симметрично,
- ✓ транзитивно.

Обозначение: $x \equiv y$ или $x \sim y$.

Пусть Q – отношение эквивалентности на X, $x \in X$.

- **Определение 2**

Классом эквивалентности, порожденным элементом x, называется подмножество множества X, состоящее из тех элементов y, для которых $x \sim y$.

Обозначение: $[x]$.

$$[x] = \{y \in X: \ x \sim y\}.$$

- **Определение 3**

  Множество всех классов эквивалентности по данному отношению Q на X называется фактор-множеством множества X по отношению Q.

  Обозначение: $X\,/\,Q$.

Систему представителей всех классов эквивалентности называют трансверсалом множества X по отношению Q.

СР

Может ли $[x]$ на X быть пустым множеством? Объясните.

Пусть $x, y \in \boldsymbol{Z}$, $n \in \boldsymbol{N}$.

- **Определение 4**

Числа x и y называются сравнимыми (равными) по модулю n, если разность $(x - y)$ делится на n.

Обозначение: $x \equiv y \ (mod\ n)$

или $x = y \ (mod\ n)$.

Число n называется *модулем*, каждое из чисел x и y называется *вычетом по модулю* n.

$$x = y \ (mod\ n) \Leftrightarrow x - y = t \cdot n, \text{ где } t \in \mathbf{Z}.$$

Если какое-либо число $z \in \boldsymbol{Z}$ несравнимо с y по модулю n, то z называется *невычетом y по модулю n*.

Пример

Рассмотрим на $\mathbf{Z}$ отношение

$$Q:\ x = y\ (mod\ n).$$

- рефлексивно:

$$\forall x \in \mathbf{Z} \quad x = x\ (mod\ n);$$

- симметрично:

$$\forall x, y \in \mathbf{Z} \quad x = y\ (mod\ n) \Rightarrow y = x\ (mod\ n);$$

- транзитивно:

$$\forall x, y, z \in \mathbf{Z} \ \ x = y\ (mod\ n),\ y = z\ (mod\ n) \Rightarrow x = z\ (mod\ n).$$

Q – отношение эквивалентности на $\mathbf{Z}$.

Пусть

$x=y \ (mod\ n) \Leftrightarrow x - y = t \cdot n$, где $t \in \mathbf{Z} \ \Rightarrow y = x - t \cdot n$;

$y=z \ (mod\ n) \Leftrightarrow y - z = k \cdot n$, где $k \in \mathbf{Z}$

$\Rightarrow x - t \cdot n - z = k \cdot n, \ \ x - z = (t + k) \cdot n \Leftrightarrow (x - z) \vdots \ n$

$\Rightarrow x=z \ (mod\ n)$

Отношение Q порождает следующие классы эквивалентности на $\mathbf{Z}$:

вместе с числом x в этом же классе содержатся все числа y, равные x по модулю n, т.е. числа вида $y = x+t\cdot n$, где $t\in\mathbf{Z}$.

Пусть $a, b \in \mathbf{Z}$.

- **Теорема** (свойство евклидовости)

Для $\forall a \in \mathbf{Z}, \forall b \in \mathbf{Z}, b \neq 0$ существуют *единственные* целые частное q и остаток r такие, что

$$a = b \cdot q + r, \quad 0 \leq r < |b|.$$

$\forall x \in \mathbf{Z} \quad x = t \cdot n + r$, где $t, r \in \mathbf{Z}$,

$0 \le r < n$.

Тогда $x - r = t \cdot n \Leftrightarrow x = r \ (mod\ n)$.

Вывод:

Каждое целое число попадает в тот же класс эквивалентности по отношению Q, что и остаток от его деления на n.

Остатки от деления целых чисел на n порождают попарно различные классы эквивалентности

$$[0],\ [1], \ldots,\ [n-1],$$

которые называются *классами вычетов по модулю n*.

$$[r] = \{x \in \mathbf{Z} : \ x = t \cdot n + r,\ t \in \mathbf{Z},\ 0 \le r < n\}.$$

Фактор-множество множества $\boldsymbol{Z}$ по отношению Q :

$$\boldsymbol{Z}_{[\boldsymbol{n}]} = \{[0], [1], \ldots, [n-1]\}$$

– *множество классов вычетов по модулю* n.

Пример

Рассмотрим на $\boldsymbol{Z}$ отношение

$$Q:\ x = y\ (mod\ 3).$$

$[0]=\{\ldots, -6, -3, 0, 3, 6,\ldots\}$,

$[1]=\{\ldots, -5, -2, 1, 4, 7,\ldots\}$,

$[2]=\{\ldots, -4, -1, 2, 5, 8,\ldots\}$.

$\boldsymbol{Z}_{[3]} = \{\ [0], [1], [2]\ \}$ – множество классов вычетов по модулю n=3.

- **Определение 5**

Вычетом класса называется любое из чисел, принадлежащих этому классу.

Различают *полную* и *приведенную* системы вычетов.

Система чисел, взятых по одному из каждого класса по некоторому модулю n, называется полной системой вычетов.

Полные системы вычетов:

- система наименьших неотрицательных вычетов $0, 1, 2, \ldots, n-1$;
- система наименьших положительных вычетов

$$1, 2, \ldots, n;$$

- система наименьших по абсолютной величине вычетов при *нечетном n*:

$$-\frac{n-1}{2}, \; \ldots \; , \; -2, \; -1, \; 0, \; 1, \; 2, \; \ldots \; \frac{n-1}{2};$$

- система наименьших по абсолютной величине вычетов при *четном n*:

$$-\frac{n}{2}+1, \; \ldots \; , \; -2, \; -1, \; 0, \; 1, \; 2, \; \ldots \; \frac{n}{2}.$$

Пример

Полные системы вычетов по модулю $n=3$:

- система наименьших неотрицательных вычетов: $0, 1, 2$;
- система наименьших положительных вычетов: $1, 2, 3$;
- система наименьших по абсолютной величине вычетов при *нечетном* n:

$$-1, 0, 1$$

Пусть $a \neq 0$, $b \neq 0$.

- **Определение**

Целое число $d>0$ называется **наибольшим общим делителем** чисел a и b при выполнении следующих условий:

1) $d \mid a$, $d \mid b$;
2) $c \mid a$ и $c \mid b \Rightarrow c \mid d$.

Обозначение: (a,b) или НОД(a,b).

*

- **Теорема**

Если целые числа $a \neq 0$ и $b \neq 0$, то существуют целые числа x и y такие, что

$$\text{НОД}(a,b) = ax + by$$

$$x = y \ (mod\ n) \Leftrightarrow x - y = t \cdot n \Rightarrow \ y = x - t \cdot n,\ t \in \mathbf{Z}$$

$\Rightarrow$ любой делитель чисел x и n является общим делителем чисел y и n, и наоборот.

Вывод:

Множество общих делителей x и n совпадает со множеством общих делителей y и n.

В частности, НОД(x,n) = НОД(y,n).

- **Определение 6**

Наибольшим делителем класса называется наибольший общий делитель какого-либо числа этого класса и модуля.

- **Определение 7**

Классами, взаимно простыми с модулем, называются классы, у которых наибольший общий делитель с модулем равен единице.

Классы, взаимно простые с модулем, состоят из взаимно простых с модулем чисел.

Система чисел, взятых по одному из каждого класса, взаимно простого с модулем, называется приведенной системой вычетов по некоторому модулю n.

Пример

При $n=3$.

- По модулю 3 имеем три класса вычетов:

  [0], [1], [2];

- классы, взаимно простые с модулем:

  [1], [2];

- приведенная система вычетов:

  -5, 14.

2. Отношения порядка

- **Определение 8**

Бинарное отношение Q на X называется отношением нестрогого (частичного) порядка, если оно:

- ✓ рефлексивно,
- ✓ антисимметрично,
- ✓ транзитивно.

Обозначение: $x \preceq y$.

Говорят, что элемент x *предшествует или равен* элементу y, а элемент y *следует за или равен* элементу x.

- **Определение 9**

Бинарное отношение Q на X называется отношением строгого порядка, если оно:

- ✓ антирефлексивно,
- ✓ антисимметрично,
- ✓ транзитивно.

Обозначение: $x \prec y$.

Говорят, что элемент x *строго предшествует* элементу y, а элемент y *строго следует за* элементом x.

$$\forall x, y \in X \;\; x \prec y \;\Leftrightarrow\; x \preceq y \text{ и } x \neq y.$$

Пример

Пусть $X \subseteq \boldsymbol{R}$.

Отношение Q: $x \leq y$ – *естественный числовой порядок*.

При этом говорят, что *элемент* x *не больше элемента* y.

Если Q: $x < y$, то говорят, что *элемент* x *строго меньше элемента* y.

- **Определение 10**

Бинарное отношение Q: $x \succeq y$ на X называется отношением, двойственным к отношению частичного порядка, если:

$$\forall x, y \in X \;\; x \succeq y \;\Leftrightarrow\; y \preceq x$$

СР Свойства отношения Q: $x \succeq y$

- ?
- ?
- ?

Отношение Q: $x \succ y$, ассоциированное с двойственным отношением, определяется так:

$$\forall x, y \in X \;\; x \succ y \;\Leftrightarrow\; x \succeq y \text{ и } x \neq y$$

СР Свойства отношения Q: $x \succ y$

- ?
- ?
- ?

Пример

Пусть $X \subseteq \boldsymbol{R}$.

Отношение Q: $x \geq y$ – двойственное к отношению частичного порядка $\leq$.

Говорят, что элемент x *не меньше* элемента y.

Если Q: $x > y$, то говорят, что *элемент x строго больше элемента y*.

Пусть $X \neq \varnothing$ – конечное множество,
Q – отношение частичного порядка на X.

- **Определение 11**

Бинарное отношение Q на X называется отношением доминирования, если

$$xQy \Leftrightarrow x, y \in X \;\; x \prec y \text{ и } \nexists z \in X \text{ такой,}$$
$$\text{что } x \prec z \prec y.$$

Обозначение: $x \lhd y$.

Говорят, что элемент x *непосредственно предшествует* элементу y, а элемент y *непосредственно следует за* (доминирует над) элементом x.

Отношение $\lhd$ называют *отношением доминирования, ассоциированным с отношением* $\preceq$ *частичного порядка* на X.

CP Свойства отношения Q: $x \lhd y$

- ?
- ?
- ?

3. Упорядоченные множества

Пусть $X \neq \varnothing$

- **Определение 11**

Множество X с заданным на нем бинарным отношением порядка Q называется упорядоченным.

Обозначение: $< X, Q >$.

Множество X, на котором зафиксирован некоторый частичный порядок, называется частично упорядоченным множеством (ч.у.м.).

Обозначение: $< X, \preceq >$.

Определение 12

Элементы x и y ч.у.м. $< X, \preceq >$ называются:

- сравнимыми по отношению частичного порядка, если $x \preceq y$ или $y \preceq x$;
- несравнимыми – в противном случае.

- **Определение 13**

Отношение частичного порядка на X, для которого любые два элемента сравнимы, называется отношением линейного порядка.

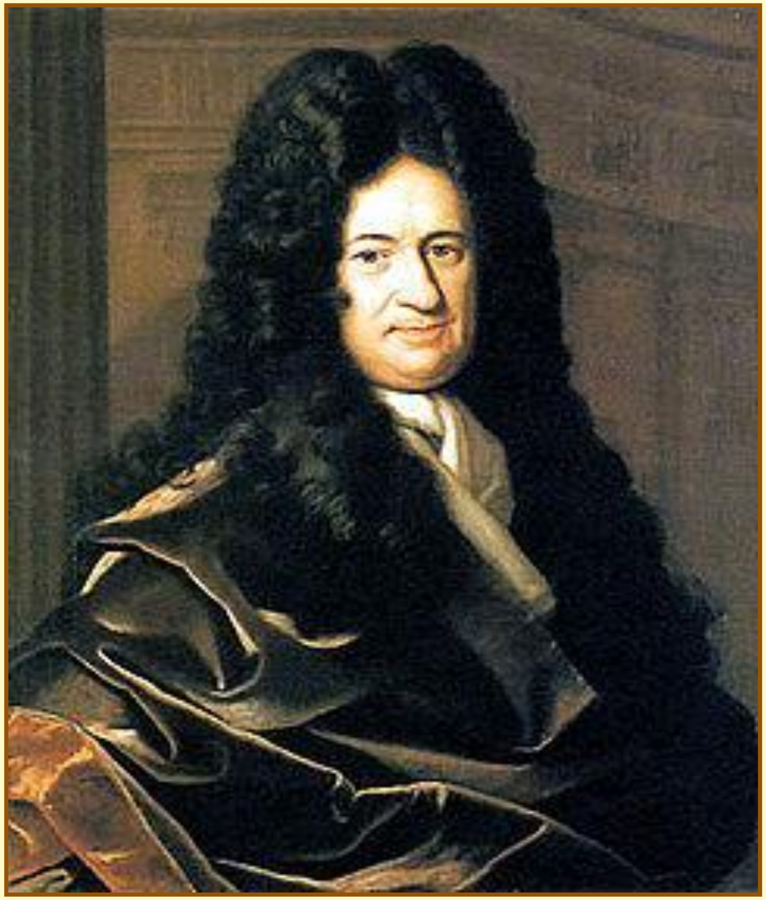
Множество X, на котором зафиксирован некоторый линейный порядок, называется линейно упорядоченным множеством (л.у.м.) или цепью.

Т.о. цепь – ч.у.м., в котором нет несравнимых элементов.

Антицепью называется ч.у.м., в котором x несравним с y для всех $x \neq y$.

Множество из одного элемента считается антицепью.

Феликс Хаусдорф
(1868-1942)



Готфрид Вильгельм Лейбниц
(1646-1716)

Конечное ч.у.м. $< X, \preceq >$ имеет **диаграмму Хассе**, если в нем строгий порядок определяется отношением доминирования:

$\forall \boldsymbol{x},\boldsymbol{y} \in X \quad \boldsymbol{x} \prec \boldsymbol{y} \Leftrightarrow \exists\, x_0, x_1, x_2 \ldots, x_n$ в X такая, что $\boldsymbol{x} = x_0 \lhd x_1 \lhd x_2 \lhd \ldots \lhd x_n = \boldsymbol{y}$.

В диаграмме Хассе:

- каждый элемент $x_i \in X$ изображают точкой на плоскости,
- если $x_i \lhd x_{i+1}$, то точку x_{i+1} располагают выше точки x_i и соединяют их отрезком (дугой).

- **Определение 14**

Два ч.у.м. $\mathcal{X} = \langle X, \preceq_X \rangle$ и $\mathcal{Y} = \langle Y, \preceq_Y \rangle$ называются изоморфными, если существует биекция $\varphi\colon X \to Y$, сохраняющая отношения частичного порядка:

$$x, y \in X \quad x \preceq_X y \iff \varphi(x) \preceq_Y \varphi(y)$$

Обозначение: $\mathcal{X} \cong \mathcal{Y}$.

Изоморфные ч.у.м. *неотличимы* как частично упорядоченные множества.