# Дискретная математика

*Лекция 3*

Мокеев Дмитрий Борисович

# Множества и отношения

# Отношения эквивалентности

*Отношение* $R$ *на множестве* $A$ *называется отношением эквивалентности, если оно*

- *рефлексивно,*
- *симметрично,*
- *транзитивно.*

# Отношения эквивалентности

*Отношение* $R$ *на множестве* $A$ *называется* *отношением эквивалентности*, *если оно*

- *рефлексивно,*
- *симметрично,*
- *транзитивно.*

Какие из этих отношений являются отношениями эквивалентности?

$$=,\quad <,\quad \leq,\quad \|,\quad |,\quad \subseteq,\quad \times$$

## Пример

Рассмотрим следующее отношение $R$ на $\mathbb{Z}$:
$x\,R\,y$ тогда и только тогда, когда $x - y$ четно.

$R$ является отношением эквивалентности.
Доказательство транзитивности:

$$x\,R\,y \quad \Leftrightarrow \quad x - y = 2k$$
$$y\,R\,z \quad \Leftrightarrow \quad y - z = 2m$$
$$x - z = 2(k + m) \quad \Rightarrow \quad x\,R\,z$$

Если $x\,R\,y$, то говорят, что $x$ *сравнимо* с $y$ *по модулю* 2, и пишут

$$x \equiv y \pmod 2.$$

# Разбиения

*Семейство* $\mathcal{P}$ *подмножеств множества* $A$ *называется разбиением* $A$, *если*

1) подмножества, составляющие $\mathcal{P}$, *попарно не пересекаются*;

2) объединение всех подмножеств из $\mathcal{P}$ *равно* $A$.

Другими словами:

семейство $\mathcal{P}$ является *разбиением* множества $A$, если *каждый* элемент $A$ принадлежит *точно одному* множеству из $\mathcal{P}$.

Элементы семейства $\mathcal{P}$ называются *частями* разбиения.

Пример $A = \{0,1,2,3,4,5,6,7,8,9\},$

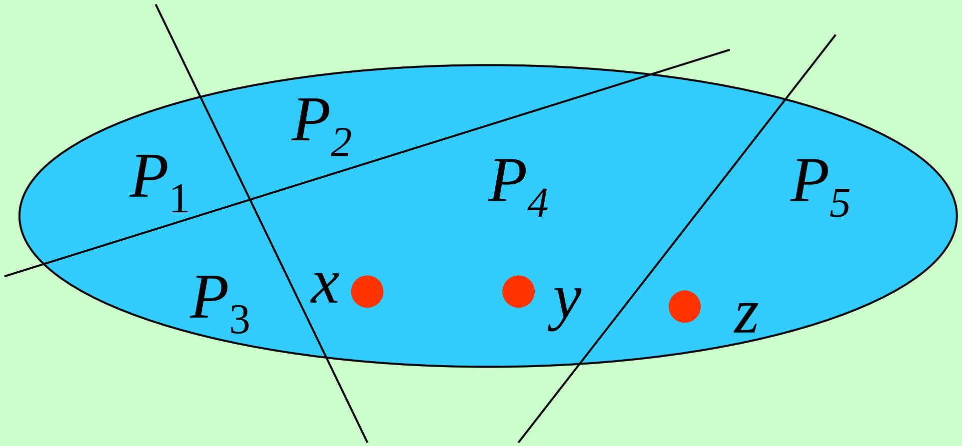
$$P_1 = \{0,3,6,9\},$$
$$P_2 = \{1,2,4\},$$
$$P_3 = \{5\},$$
$$P_4 = \{7,8\}.$$

$\mathcal{P} = \{P_1, P_2, P_3, P_4\}$ – разбиение множества $A$ на четыре части.

$$A = P_1 \sqcup P_2 \sqcup P_3 \sqcup P_4$$

Пусть $\mathcal{P}$ – разбиение множества $A$.
Определим отношение $R$ на $A$:
$x\,R\,y \iff x$ и $y$ принадлежат одной части разбиения.

$R$ является отношением эквивалентности.

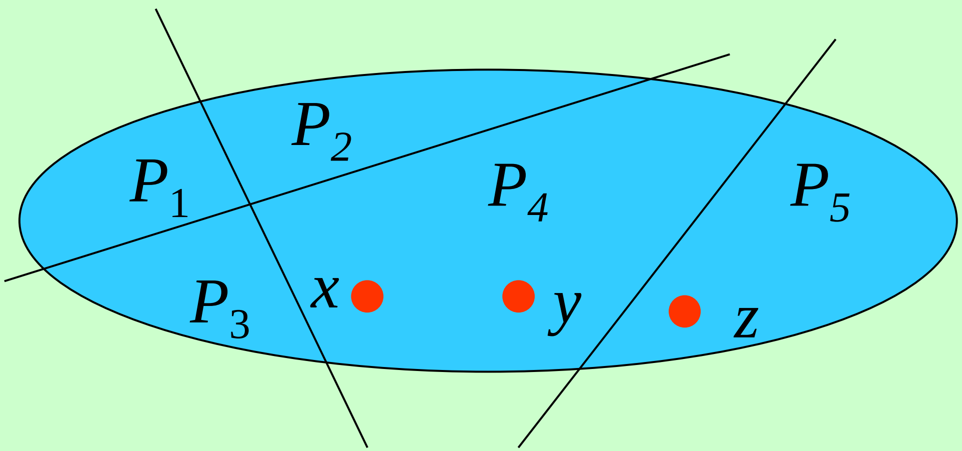



$(x, y) \in R$

$(x, z) \notin R$

Пусть $\mathcal{P}$ – разбиение множества $A$.
Определим отношение $R$ на $A$:
$x\,R\,y \;\Leftrightarrow\; x$ и $y$ принадлежат одной части разбиения.

$R$ является отношением эквивалентности.




$(x, y) \in R$

$(x, z) \notin R$

*Все отношения эквивалентности устроены подобным образом!*

**Теорема о факторизации.**

*Пусть* $R$ *– отношение эквивалентности на множестве* $A$. *Существует такое разбиение* $\mathcal{P}$ *множества* $A$, *что* $\forall x, y \in A \;\; x\,R\,y$ *тогда и только тогда, когда они принадлежат одной части разбиения* $\mathcal{P}$.

**Теорема о факторизации.**

*Пусть* $R$ *– отношение эквивалентности на множестве* $A$*. Существует такое разбиение* $\mathcal{P}$ *множества* $A$*, что* $\forall x, y \in A \quad x\, R\, y$ *тогда и только тогда, когда они принадлежат одной части разбиения* $\mathcal{P}$.

**Доказательство** проведем в три этапа:

1. Построим семейство $\mathcal{P}$ подмножеств множества $A$.

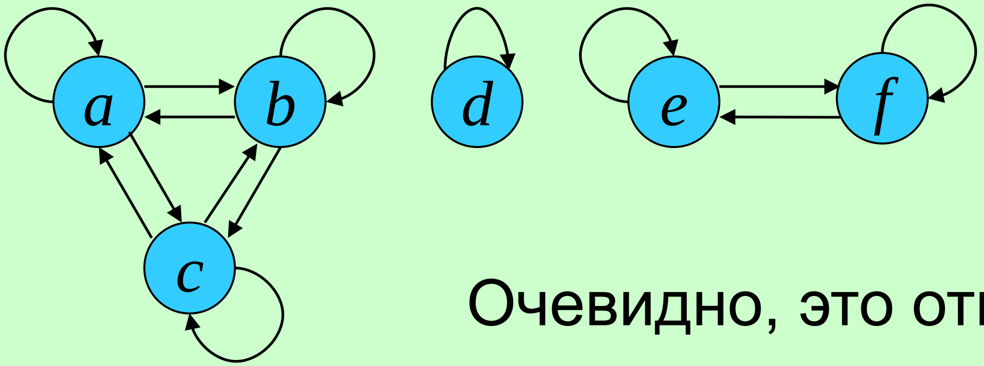
Положим $[x] = \{y\colon x\,R\,y\}$ для каждого $x \in A$,

$$\mathcal{P} = \{[x]\colon x \in A\}.$$

Замечание: может быть $x \neq y$, но $[x] = [y]$.

---

**Например**, пусть $R$ – отношение, представленное графом:




Очевидно, это отношение эквивалентности.

Здесь $[a] = [b] = [c] = \{a, b, c\}$, $[d] = \{d\}$,
$[e] = [f] = \{e, f\}$,

$$\mathcal{P} = \big\{\{a, b, c\}, \{d\}, \{e, f\}\big\}.$$

**Теорема о факторизации.**

*Пусть* $R$ *– отношение эквивалентности на множестве* $A$*. Существует такое разбиение* $\mathcal{P}$ *множества* $A$*, что* $\forall x, y \in A$ $x \, R \, y$ *тогда и только тогда, когда они принадлежат одной части разбиения* $\mathcal{P}$*.*

**Доказательство** проведем в три этапа:

1. Построим семейство $\mathcal{P}$ подмножеств множества $A$.

2. Покажем, что $\mathcal{P}$ является разбиением множества $A$.

1) Так как отношение $R$ рефлексивно, то $x \in [x]$ для всех $x \in A$.
Поэтому каждый элемент $x \in A$ принадлежит хотя бы одному подмножеству из $\mathcal{P}$, т.е. объединение всех множеств из $\mathcal{P}$ равно $A$:

$$\bigcup_{x \in A} [x] = A.$$

2) Теперь покажем, что если $[x] \neq [y]$, то $[x]$ и $[y]$ не пересекаются.

Предположим, что $[x] \cap [y] \neq \emptyset$. Тогда существует $z \in [x] \cap [y]$, т.е. $z\,R\,x$ и $z\,R\,y$. Так как отношение $R$ симметрично и транзитивно, то отсюда следует, что $x\,R\,y$. Теперь для любого $u \in A$ имеем:

$$u \in [x] \quad \Rightarrow \quad u\,R\,x \quad \Rightarrow \quad u\,R\,y \quad \Rightarrow \quad u \in [y]$$

и обратно. Следовательно, $[x] = [y]$.

**Теорема о факторизации.**

*Пусть $R$ – отношение эквивалентности на множестве $A$. Существует такое разбиение $\mathcal{P}$ множества $A$, что $\forall x, y \in A$ $x\,R\,y$ тогда и только тогда, когда они принадлежат одной части разбиения $\mathcal{P}$.*

**Доказательство** проведем в три этапа:

1. Построим семейство $\mathcal{P}$ подмножеств множества $A$.

2. Покажем, что $\mathcal{P}$ является разбиением множества $A$.

3. Покажем, что $x\,R\,y \Leftrightarrow x$ и $y$ принадлежат одной части разбиения $\mathcal{P}$.

Если $x\,R\,y$, то $y \in [x]$. Но $x \in [x]$, поэтому $x$ и $y$ оба принадлежат $[x]$.

Обратно, если $x \in [z]$ и $y \in [z]$ для некоторого $z$, то $x\,R\,z$ и $y\,R\,z$ . Отсюда (из симметричности и транзитивности отношения $R$) следует, что $x\,R\,y$.

Итак, если на множестве $A$ задано отношение эквивалентности $R$, то множество $A$ разбивается на части так, что любые два элемента из одной части находятся в отношении $R$, а любые два элемента из разных частей не находятся в этом отношении.

Эти части называются *классами эквивалентности*.

Семейство классов эквивалентности называется *фактор-множеством* множества $A$ по отношению $R$ и обозначается $A/R$.

## Пример 1

Пусть $n \in \mathbb{N}$. Определим следующее отношение $R_n$ на $\mathbb{N}_0$:
$x\, R_n\, y$ означает, что $n$ делит $x - y$, т.е. существует такое целое $k$, что $x - y = kn$.

(ранее был рассмотрен частный случай $n = 2$).

$R_n$ является отношением эквивалентности для любого $n$.

Если $x\, R\, y$, то говорят, что $x$ *сравнимо* с $y$ *по модулю* $n$ и пишут

$$x \equiv y \pmod{n}.$$

Два целых числа сравнимы по модулю $n$ тогда и только тогда, когда они дают одинаковые остатки при делении на $n$. Поэтому в $R_n$ имеется ровно $n$ классов эквивалентности:

$$[0] = \{0,\ n,\ 2n,\ 3n,\ \dots\},$$

$$[1] = \{1,\ n+1,\ 2n+1,\ 3n+1,\ \dots\},$$

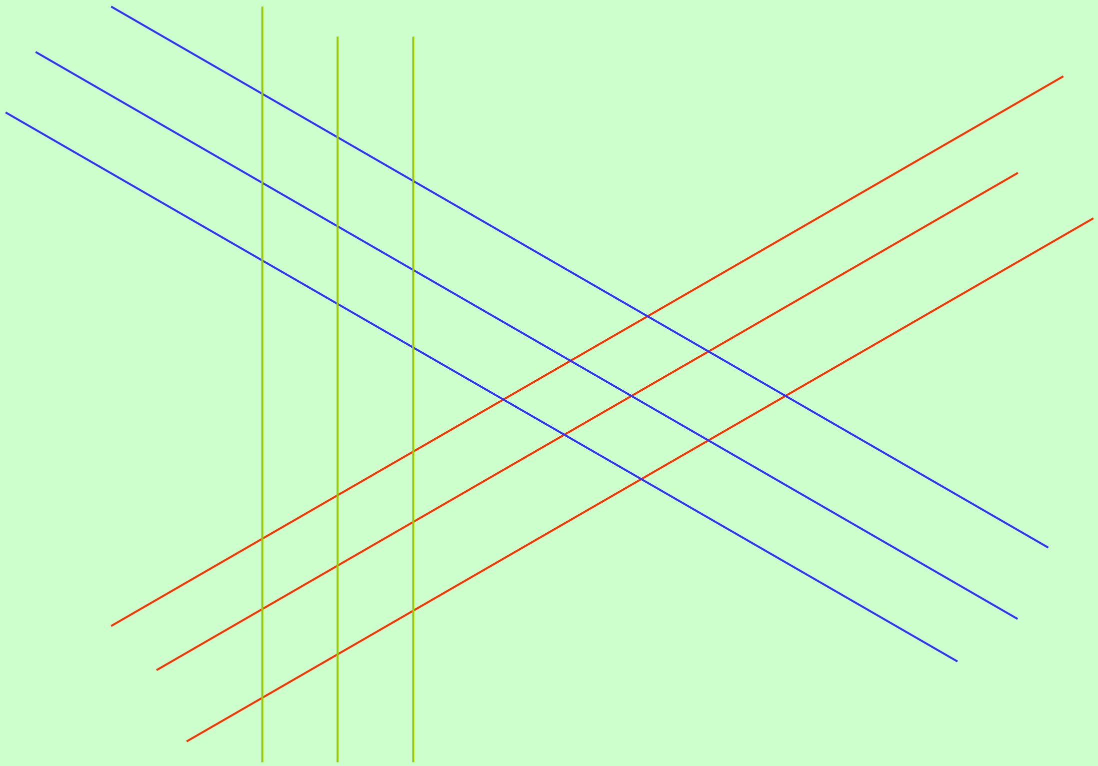
$$[2] = \{2,\ n+2,\ 2n+2,\ 3n+2,\ \dots\},$$

$$\vdots$$

$$[n-1] = \{n-1,\ 2n-1,\ 3n-1,\ 4n-1,\ \dots\}.$$

## Пример 2

Отношение $\|$ является отношением эквивалентности. Каждый класс эквивалентности состоит из всех прямых одного направления.



# Отношения порядка

*Отношение* $R$ на множестве $A$ *называется* *отношением порядка*, если оно

- рефлексивно,
- антисимметрично,
- транзитивно.

Если $R$ есть отношение порядка и $x\ R\ y$, то говорят "$x$ *предшествует* $y$" или "$x$ меньше $y$".

# Отношения порядка

*Отношение* $R$ на множестве $A$ *называется* *отношением порядка*, если оно

- рефлексивно,
- антисимметрично,
- транзитивно.

Если $R$ есть отношение порядка и $x\,R\,y$, то говорят "$x$ *предшествует* $y$" или "$x$ меньше $y$".

Какие из этих отношений являются отношениями порядка?

$$=,\quad <,\quad \leq,\quad |,\quad \in,\quad \subseteq,\quad \|$$

# Строгий порядок

*Отношение* $R$ на множестве $A$ *называется* *отношением строгого порядка*, если оно

- антирефлексивно,
- антисимметрично,
- транзитивно.

Сравнение отношения $<$ и $\leq$.

# Строгий порядок

*Отношение* $R$ на множестве $A$ *называется* *отношением строгого порядка*, если оно

- антирефлексивно,
- антисимметрично,
- транзитивно.

Сравните отношения $<$ и $\leq$.

Замечание: строгий порядок *не является* частным случаем порядка.

# Строгий порядок

*Отношение* $R$ на множестве $A$ *называется* *отношением строгого порядка*, если оно

- антирефлексивно,
- антисимметрично,
- транзитивно.

Сравните отношения $<$ и $\leq$.

Замечание: строгий порядок *не является* частным случаем порядка.

Является ли отношение $|$ порядком или строгим порядком?

# Упорядоченное множество

Множество $A$ с заданным на нем отношением порядка $R$ называется *упорядоченным множеством*.

Точнее, упорядоченное множество – это пара $(A, R)$.

Примеры: $(\mathbb{Z}, \leq)$;

$(2^A, \subseteq)$ для любого множества $A$;

$(\mathbb{N}, \mid)$.

Есть важное различие между $(\mathbb{Z}, \le)$ и $(2^A, \subseteq)$.

Для любых $x, y \in \mathbb{Z}$ выполняется хотя бы одно из неравенств $x \le y$, $y \le x$.

Для $X, Y \in 2^A$ может быть $X \not\subseteq Y$ и $Y \not\subseteq X$. Например:

$$X = \{a, b\}, \qquad Y = \{a, c\}.$$

Пусть $(A, R)$ – упорядоченное множество и $x, y \in A$. $x$ и $y$ *сравнимы*, если $x\,R\,y$ или $y\,R\,x$, иначе они *несравнимы.*

В $(\mathbb{Z}, \le)$ любые два элемента сравнимы.

В $(2^A, \subseteq)$ имеются несравнимые элементы.

Порядок $R$ на множестве $A$ называется *линейным порядком*, если любые два элемента сравнимы, иначе он называется *частичным порядком*.

В первом случае $(A, R)$ есть *линейно упорядоченное множество*, во втором оно является *частично упорядоченным множеством*.

$(\mathbb{Z}, \leq)$ – линейно упорядоченное множество,

$(2^A, \subseteq)$ – частично упорядоченное множество.

Порядок $R$ на множестве $A$ называется *линейным порядком*, если любые два элемента сравнимы, иначе он называется *частичным порядком*.

В первом случае $(A, R)$ есть *линейно упорядоченное множество*,
во втором оно является *частично упорядоченным множеством*.

$(\mathbb{Z}, \leq)$ – линейно упорядоченное множество,

$(2^A, \subseteq)$ – частично упорядоченное множество.

Упорядоченное множество $(\mathbb{N}, \mid)$ линейно или частично упорядочено?
А множество $(\mathbb{Z}, \mid)$?

# Непосредственное предшествование

Пусть $(A, R)$ – упорядоченное множество, $x\,R\,y$ и $x \neq y$.

Элемент $x$ *непосредственно предшествует* элементу $y$, если *не существует* такого элемента $z$, отличного от $x$ и $y$, что $x\,R\,z$ и $z\,R\,y$.

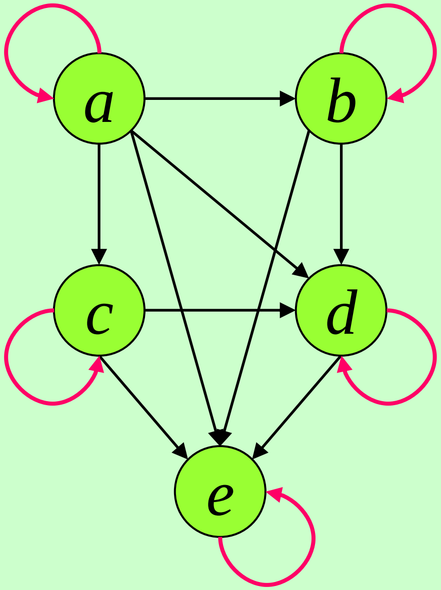
Отношение непосредственного предшествования для отношения $R$ будем обозначать $R^*$.

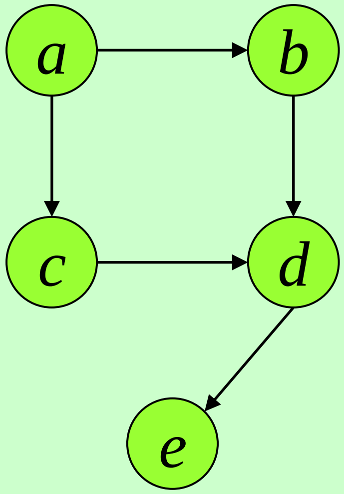
## Примеры

1. $(\mathbb{Z}, \leq)$

2. $(\mathbb{R}, \leq)$

3.




$R$ $R^*$

$aRe$ $aR^*c,\ cR^*d,\ dR^*e$

**Теорема о конечных упорядоченных множествах.**

*Пусть* $(A, R)$ – *конечное упорядоченное множество,* $a$ и $b$ – *различные элементы множества* $A$ *и* $aRb$. *Тогда существует последовательность* $z_1, z_2, \dots , z_n$ *элементов множества* $A$ *такая, что* $z_1 = a$, $z_n = b$ *и* $z_k R^* z_{k+1}$ *для* $k = 1, \dots , n-1$.

**Доказательство.** Обозначим

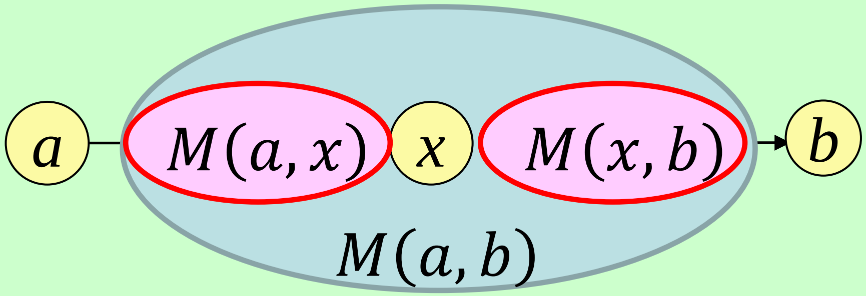
$$M(a,b) = \{x : \ x \neq a, \ x \neq b, \ aRx, \ xRy\}.$$

Пусть $|M(a,b)| = m$. Проведем индукцию по $m$.

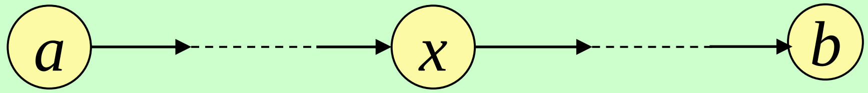
1) $m = 0$. Тогда $aR^*b$ и полагаем $z_1 = a$, $z_2 = b$.

2) $m > 0$. Возьмем какой-нибудь элемент $x \in M(a,b)$.

Тогда $|M(a,x)| < m$ и $|M(x,b)| < m$.

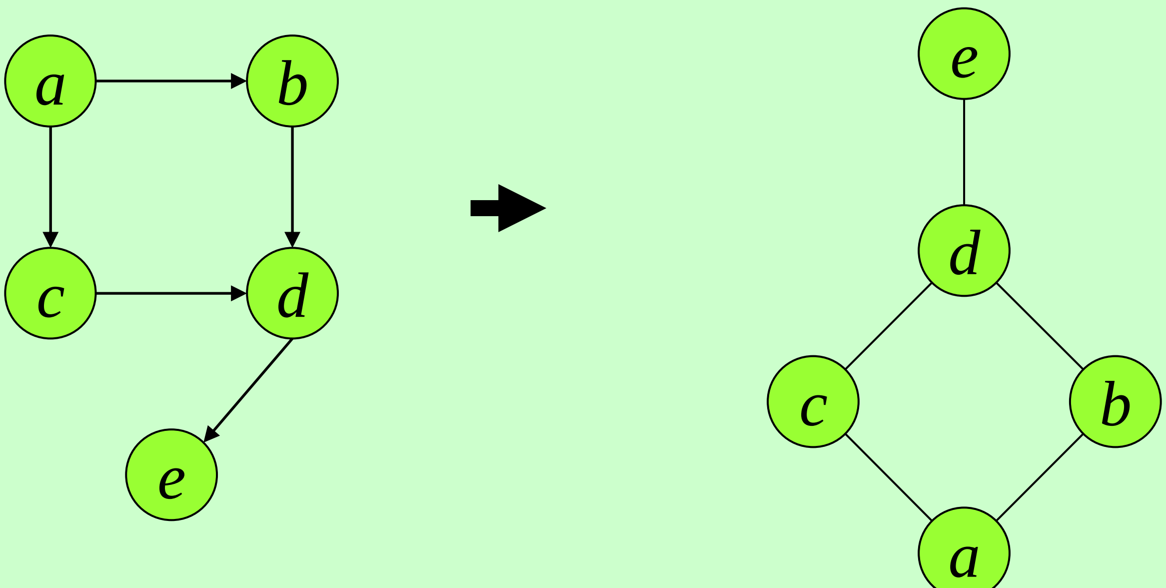



По предположению индукции, существуют последовательности элементов, связанных отношением $R^*$, соединяющие $a$ с $x$ и $x$ с $b$. Соединяя их в одну, получим последовательность, соединяющую $a$ с $b$.

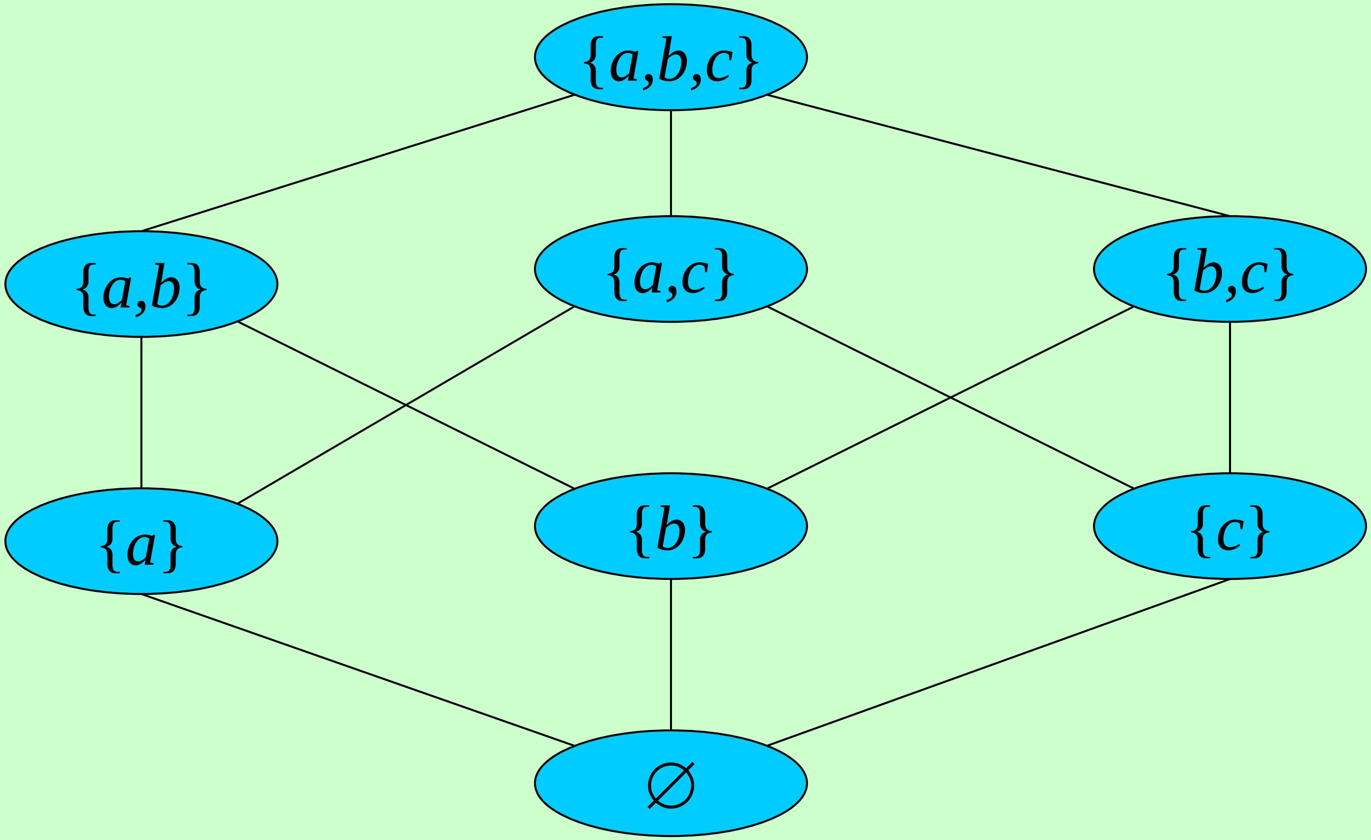


Граф отношения $R^*$ называется *диаграммой Хассе* или *диаграммой непосредственных предшествований* отношения $R$.

Обычно вершины на диаграмме располагают так, чтобы меньший (предшествующий) элемент находился *ниже* большего. Тогда отношение между элементами можно изображать линией, а не стрелкой.



# Диаграмма Хассе упорядоченного множества $(2^{\{a,b,c\}}, \subseteq)$



# Максимальные и минимальные элементы

$x \in A$ называется *максимальным* элементом упорядоченного множества $(A, R)$, если не существует такого $y$, что $y \neq x$ и $x\,R\,y$.

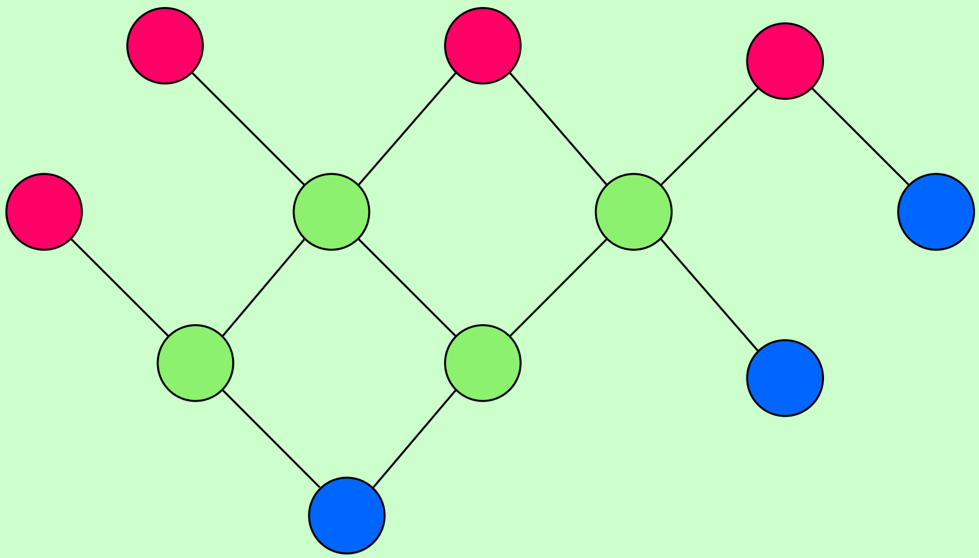
Иначе говоря, не существует элемента *больше* $x$.

$x$ – *минимальный* элемент, если не существует элемента *меньше* $x$.

$(\mathbb{Z}, \leq)$ не имеет ни максимальных, ни минимальных элементов.

$(\mathbb{N}, \leq)$ имеет один минимальный элемент и ни одного максимального.

Каждое *конечное* упорядоченное множество имеет максимальные и минимальные элементы.



**Теорема.** *Если* $(A, R)$ *– конечное упорядоченное множество и* $x \in A$, *то существует максимальный элемент* $y$ *такой, что* $x\,R\,y$.

**Доказательство**.

$x$ максимальный $\longrightarrow$ полагаем $y = x$

$x$ не максимальный $\longrightarrow$ существует $y_1 \neq x$, больший $x$

$y_1$ максимальный $\longrightarrow$ полагаем $y = y_1$

$y_1$ не максимальный $\longrightarrow$ существует $y_2 \neq y_1$, больший $y_1$

…

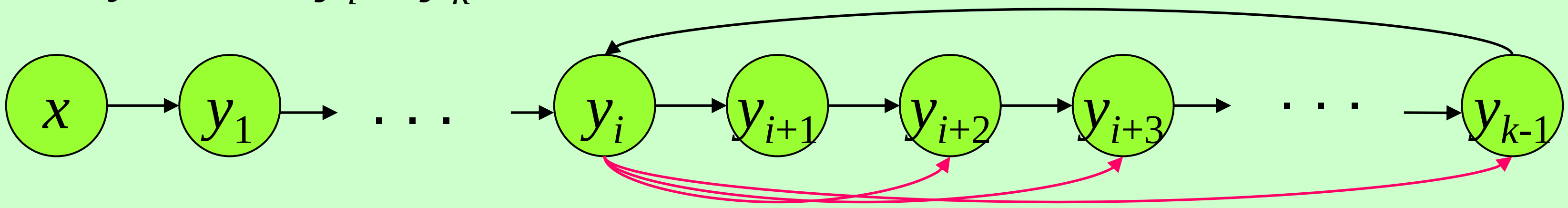
и т.д.

Получаем последовательность элементов

$$x, y_1, y_2, \ldots,$$

в которой каждый следующий элемент *больше* предыдущего. Докажем, что все элементы в этой последовательности *различны*.

Допустим, $y_i = y_k$, $i < k$.




Ввиду *транзитивности* должно быть:

$$y_i \; R \; y_{i+2}, \quad y_i \; R \; y_{i+3}, \ldots, \quad y_i \; R \; y_{k-1}.$$

Так как $y_i = y_k$, то $y_k \; R \; y_{k-1}$. Но в то же время $y_{k-1} \; R \; y_k$.

Это противоречит *антисимметричности*.

Таким образом, все элементы последовательности

$$x, y_1, y_2, \ldots$$

различны. Так как множество $A$ *конечно*, то и эта последовательность *конечна*:

$$x, y_1, y_2, \ldots, y_n.$$

Но тогда $y_n$ – максимальный элемент и полагаем $y = y_n$.

---

# Наибольшие и наименьшие элементы

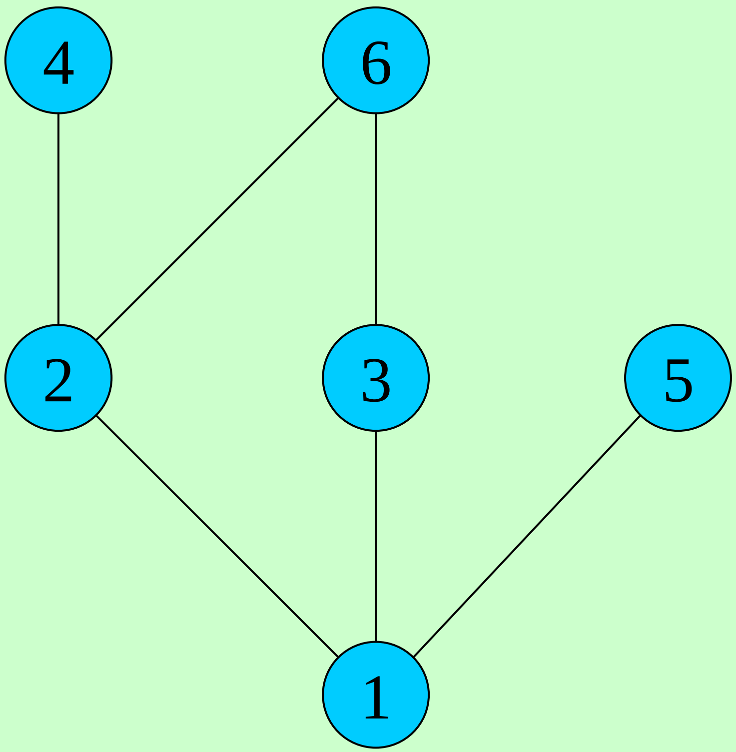
$x \in A$ называется *наибольшим* элементом упорядоченного множества $(A, R)$, если для каждого $y \in A$ выполняется $y\,R\,x$.

Иначе говоря $x$ больше любого другого элемента из $A$.

$x$ – *наименьший* элемент, если он меньше любого другого элемента из $A$.

Частично упорядоченное множество

$(\{1,2,3,4,5,6\},\ |\ )$




Линейно упорядоченное множество

$(\{1,2,3,4,5,6\},\ \leq)$