Отношения порядка

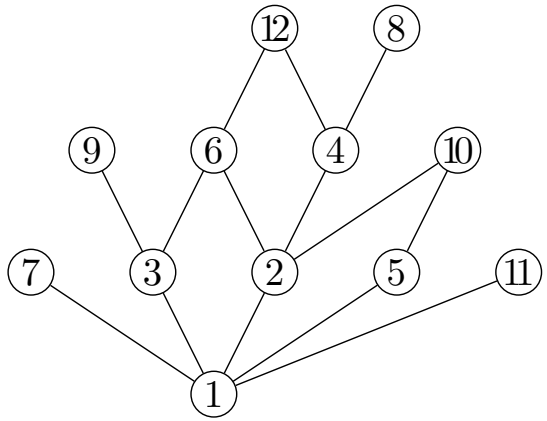
Бинарное отношение $\rho \subseteq A^2$ называется отношением порядка, если оно

- рефлексивно
  - $a \rho a$ для любого $a \in A$
- транзитивно
  - $a \rho b, b \rho c \Rightarrow a \rho c$ для любых $a, b, c \in A$
- антисимметрично
  - $a \rho b, b \rho a \Rightarrow a = b$ для любых $a, b \in A$
  - антисимметричность — совсем не то же самое, что отсутствие симметричности!
- Для отношений порядка обычно используется инфиксная запись
  - и значки, похожие на $\leqslant$: $\subseteq, \preccurlyeq, \trianglelefteq, \sqsubseteq, \ldots$
  - для записи условия ($a \preccurlyeq b$ и $a \neq b$) часто «стирают палочку» и пишут $a \prec b$
- Упорядоченное множество (ЧУМ) — это пара $(A, \preccurlyeq)$, состоящая из множества и отношения порядка на нем
- Эту структуру удобно рисовать, используя отношение покрытия
  - $a \triangleleft b$ (b покрывает a), если $a \preccurlyeq b$; $a \neq b$; $a \preccurlyeq c \preccurlyeq b \Longrightarrow (c = a$ или $c = b)$
- Диаграмма Хассе ЧУМа $(A, \preccurlyeq)$ — это (ор)граф отношения покрытия
  - стрелки на ребрах диаграммы Хассе не рисуют
  - ориентация ребра определяется расположением вершин ниже/выше
  - ⋆ это можно сделать, потому что граф — ациклический
- В бесконечных множествах отношение покрытия не всегда отражает порядок. . .
  - ! Докажите, что отношения покрытия для ЧУМов $(\mathbb{R}, \leqslant), (\mathbb{Q}, \leqslant)$ пусты

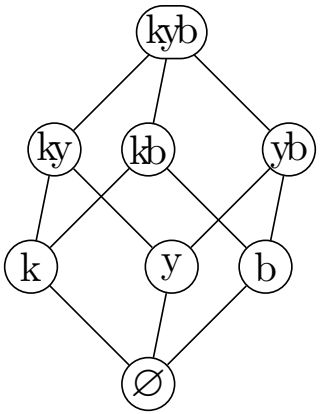
Примеры диаграмм Хассе

$(\mathbb{N}, \leqslant)$

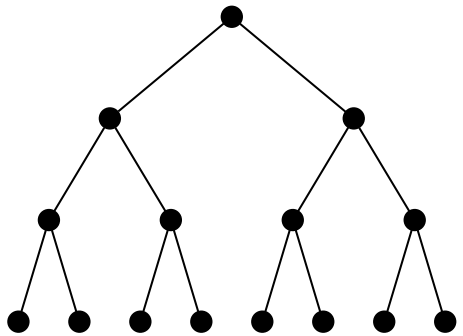
$(\{1, 2, \ldots, 12\}, |)$



$(2^{\{k,y,b\}}, \subseteq)$



Какое-то дерево



Изоморфизм ЧУМов

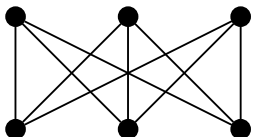
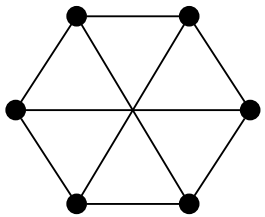
- Изоморфизм упорядоченных множеств $(A_1, \preccurlyeq_1)$ и $(A_2, \preccurlyeq_2)$ — это биекция $f : A_1 \to A_2$ такая, что
  - $a \preccurlyeq_1 b \iff f(a) \preccurlyeq_2 f(b)$ для любых $a, b \in A_1$
  - говорят, что f сохраняет порядок
- ⋆ Упорядоченные множества $(A_1, \preccurlyeq_1)$ и $(A_2, \preccurlyeq_2)$ в этом случае называются изоморфными
- Изоморфность ЧУМов — это отношение эквивалентности:
  - тождественная функция — изоморфизм ЧУМа с самим собой (рефлексивность)
  - если $f : A_1 \to A_2$ — изоморфизм, то и $f^{-1} : A_2 \to A_1$ — изоморфизм (симметричность)
  - композиция $f \circ g$ изоморфизмов $f : A_1 \to A_2$ и $g : A_2 \to A_3$ — изоморфизм (транзитивность)
- Значит, все ЧУМы разбиваются на классы изоморфных ЧУМов
- ★ С математической точки зрения изоморфные ЧУМы ничем не отличаются: это множества одинакового размера с одинаковой структурой, представленной отношением порядка
  - мы изучаем ЧУМы (и другие структуры) с точностью до изоморфизма
- Пример: ЧУМы $(\mathbb{R}, \leqslant)$ и $(\mathbb{R}^+, \leqslant)$ изоморфны, в качестве изоморфизма можно взять $f(x) = e^x$

Изоморфизм: лирическое отступление

★ Изоморфизм и изоморфность — универсальные понятия, используемые для любых структур, заданных отношениями и/или операциями на множествах
  - например, для групп, линейных пространств или графов

- Пример (линейные пространства): $\mathbb{F}_n[x]$ vs $\mathbb{F}^{n+1}$
  - многочлены степени $\leqslant n$ и векторы длины $(n+1)$ над тем же полем

  Изоморфизм: $f(a_0 + a_1x + \cdots + a_nx^n) = (a_0, a_1, \ldots, a_n)$
  - $f(p(x) + q(x)) = f(p(x)) + f(q(x))$; $f(c \cdot p(x)) = c \cdot f(p(x))$
- Пример (группы): $\mathbb{C}_n$ vs $\mathbb{Z}_n$
  - комплексные корни n-й степени из единицы и классы вычетов по $\bmod n$
  - $\mathbb{C}_n = (\{\varepsilon_k = e^{\frac{2\pi k}{n} i} \mid k = 0, \ldots, n-1\}, \cdot)$; $\mathbb{Z}_n = (\{0, \ldots, n-1\}, \oplus)$

  Изоморфизм: $f(\varepsilon_k) = k$
  - $f(\varepsilon_k \cdot \varepsilon_m) = f(\varepsilon_{k+m})$; $f(\varepsilon_k^{-1}) = f(\varepsilon_{n-k}) = n - k$
- Пример (графы):  vs 

  Изоморфизм: придумайте сами
  - есть ребро (u, v) в левом графе $\Longleftrightarrow$ есть ребро $(f(u), f(v))$ в правом графе

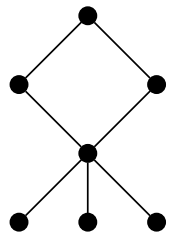
Что сохраняет изоморфизм ЧУМов?

- ⋆ Минимальные элементы:
  - a — минимальный в ЧУМе $(A, \preccurlyeq)$, если $\forall b \in A : (b \preccurlyeq a \Rightarrow b = a)$
  - для изоморфизма f, $f(b) \preccurlyeq f(a) \Leftrightarrow b \preccurlyeq a$, откуда $b = a$, $f(b) = f(a)$, т.е. $f(a)$ — минимальный по определению
- ⋆ Наименьший элемент:
  - a — наименьший в ЧУМе $(A, \preccurlyeq)$, если $\forall b \in A : a \preccurlyeq b$
  - для изоморфизма f, $f(a) \preccurlyeq f(b) \Leftrightarrow a \preccurlyeq b$ правая часть верна $\forall b$, f — биекция, т.е. $f(a)$ — наименьший по определению

... Такие же рассуждения работают для максимальных и наибольшего элементов

- ⋆ Отношение покрытия:
  - пусть $a \lhd b$
  - $f(a) \preccurlyeq f(b)$ и $f(a) \neq f(b)$
  - если $\exists c : f(a) \preccurlyeq f(c) \preccurlyeq f(b)$, то $a \preccurlyeq c \preccurlyeq b \Rightarrow c \in \{a, b\} \Rightarrow f(c) \in \{f(a), f(b)\}$
  - $f(a) \lhd f(b)$ по определению

★ Из сохранения покрытия следует, что ЧУМы изоморфны как орграфы



? Сколькими способами можно изоморфно отобразить на себя ЧУМ ?

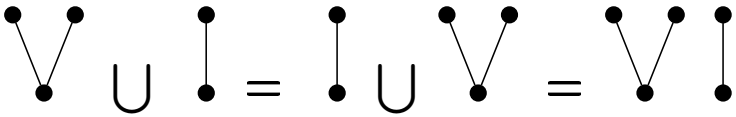
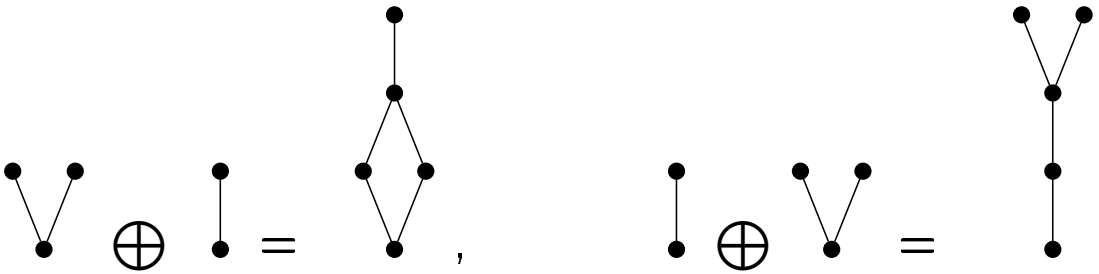
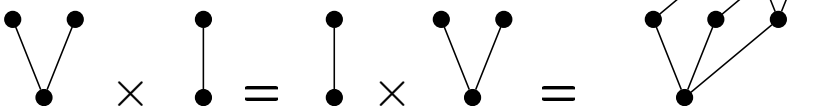
Двойственный ЧУМ и подЧУМ

- ⋆ Если $\preccurlyeq$ — отношение порядка, то и $\preccurlyeq^{-1}$, обозначаемое $\succcurlyeq$, — отношение порядка
- ЧУМ $(A, \succcurlyeq)$ называется двойственным к ЧУМу $(A, \preccurlyeq)$
  - ⋆ диаграмма Хассе для $(A, \succcurlyeq)$ получается переворачиванием диаграммы для $(A, \preccurlyeq)$
  - иначе говоря, надо переориентировать все ребра этого графа
- Если $(A, \succcurlyeq)$ и $(A, \preccurlyeq)$ изоморфны, то это — самодвойственный ЧУМ
- ! Найдите все (с точностью до изоморфизма) трехэлементные самодвойственные ЧУМы

- Пусть $\preccurlyeq$ — отношение порядка на A и $\varnothing \neq B \subseteq A$
- Пусть $\preccurlyeq_{|B} = \{(a, b) \in B^2 \mid a \preccurlyeq b\}$ — ограничение $\preccurlyeq$ на B
  - Тогда $(B, \preccurlyeq_{|B})$ — ЧУМ (почему?); он называется подЧУМом ЧУМа $(A, \preccurlyeq)$

Операции над ЧУМами

Из одних ЧУМов можно получать другие (более сложные) при помощи различных операций. Пусть $(A_1, \preccurlyeq_1)$ и $(A_2, \preccurlyeq_2)$ — ЧУМы, $A_1 \cap A_2 = \varnothing$.

- Объединение ЧУМов — это ЧУМ $(A_1 \cup A_2, \preccurlyeq) = (A_1, \preccurlyeq_1) \cup (A_2, \preccurlyeq_2)$ такой, что
  - $(a \preccurlyeq b) \Leftrightarrow (a \preccurlyeq_1 b$ или $a \preccurlyeq_2 b)$
- Сумма ЧУМов — это ЧУМ $(A_1 \cup A_2, \preccurlyeq) = (A_1, \preccurlyeq_1) \oplus (A_2, \preccurlyeq_2)$ такой, что
  - $(a \preccurlyeq b) \Leftrightarrow (a \preccurlyeq_1 b$ или $a \preccurlyeq_2 b$ или $(a \in A_1$ и $b \in A_2))$
- Произведение ЧУМов — это ЧУМ $(A_1 \times A_2, \preccurlyeq) = (A_1, \preccurlyeq_1) \times (A_2, \preccurlyeq_2)$ такой, что
  - $(a, b) \preccurlyeq (c, d) \Leftrightarrow (a \preccurlyeq_1 c$ и $b \preccurlyeq_2 d)$
- Пример:
- 
- 
- 

Линейный порядок

- Бинарное отношение $\rho \in A^2$ называется линейным, если
  - $a \neq b \Rightarrow (a \,\rho\, b$ или $b \,\rho\, a)$ для любых $a, b \in A$
- Отношение порядка, являющееся линейным, называют линейным порядком
  - множество с линейным порядком называют линейно упорядоченным (ЛУМ)
- Примеры:
  - обычный порядок $\leqslant$ на любом числовом множестве
  - лексикографический («словарный») порядок на множестве Σ^* конечных слов над линейно упорядоченным алфавитом Σ
  - радиксный порядок на Σ^*: упорядочиваем слова по длине, а слова одной длины — лексикографически

Теорема о линейном порядке

Теорема

Произвольное отношение порядка $\preccurlyeq$ на произвольном множестве A можно дополнить до отношения линейного порядка на A.

- Иными словами, для порядка $\preccurlyeq$ на множестве A существует линейный порядок $\sqsubseteq$ на A такой, что $\preccurlyeq \subseteq \sqsubseteq$
- В общем случае — сложное доказательство, опирается на аксиому выбора
- Доказательство для конечных множеств: алгоритм топологической сортировки
  - рассмотрим диаграмму Хассе ЧУМа $(A, \preccurlyeq)$ как орграф
  - возьмем любой минимальный элемент (исток в орграфе), присвоим ему номер 1 и удалим из орграфа
  - продолжим процедуру в цикле, присваивая наименьший незанятый номер любому истоку оставшегося орграфа
  - нумерация вершин задает линейный порядок, содержащий исходный $\square$

Условие минимальности и другие

Пусть $\preccurlyeq$ — отношение порядка на множестве A; $\preccurlyeq$ удовлетворяет

- условию минимальности, если
  - для любого непустого подмножества $B \subseteq A$ в ЧУМе $(B, \preccurlyeq_{|B})$ есть минимальный элемент
- условию индуктивности, если
  - любое свойство $P = P(a)$ элементов множества A, такое что
  - ⋆ $P(a)$ для любого минимального элемента A (база)
  - ⋆ если $P(b)$ для любого элемента b такого, что $b \prec a$, то $P(a)$ (шаг) выполнено для всех элементов A
- условию обрыва убывающих цепей, если
  - любая последовательность элементов A с условием
  - $\cdots \prec a_n \prec \cdots \prec a_2 \prec a_1$ конечна

Теорема

Условия минимальности, индуктивности и обрыва убывающих цепей эквивалентны.

- Доказательство $\Rightarrow$

Доказательство теоремы об эквивалентных условиях

- Минимальность $\Rightarrow$ индуктивность (от противного)
  - ⋆ Пусть P — свойство, для которого не выполняется индуктивность, т.е. выполнены база и шаг индукции, но есть хотя бы один элемент a такой, что $\neg P(a)$
  - ⋆ Пусть $B = \{a \mid \neg P(a)\}$; в B есть минимальный элемент, назовем его b
  - ⋆ b не минимален в A, потому что $\neg P(b)$ противоречит базе
  - $\Rightarrow$ тогда $P(a)$ для всех $a \prec b$, и $\neg P(b)$ противоречит шагу
- Индуктивность $\Rightarrow$ обрыв убывающих цепей (по индукции)
  - ⋆ Пусть $P(a)$ означает, что все убывающие цепи, такие что $a_1 = a$, конечны
  - ⋆ для минимального a цепь одна и состоит из a — база выполнена
  - ⋆ если для всех элементов, меньших a, цепи конечны, то a увеличивает длину каждой из таких цепей на 1, т.е. цепи, начинающиеся с a, тоже конечны — шаг выполнен
  - $\Rightarrow$ по индукции $P(a)$ выполнено для всех a, а это и есть условие обрыва
- Обрыв убывающих цепей $\Rightarrow$ минимальность (в лоб)
  - ⋆ Найдем минимальный элемент в произвольном непустом $B \subseteq A$
  - ⋆ возьмем произвольный $a_1 \in B$; если он минимальный — OK
  - ⋆ иначе существует $a_2 \in B$ такой, что $a_2 \prec a_1$; если он минимальный — OK
  - ⋆ иначе существует $a_3 \in B$ такой, что $a_3 \prec a_2 \prec a_1$ ...
  - ⋆ процесс будет конечным, так как бесконечных убывающих цепей нет
  - $\Rightarrow$ минимальный элемент будет найден за конечное число шагов

Заключительные замечания

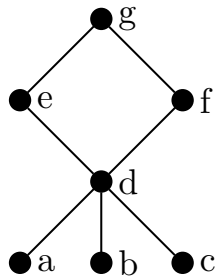
- Наличие свойств минимальности/индуктивности/ обрыва убывающих цепей — это хорошо
  - ⋆ главная ценность — можно доказывать по индукции
- Все конечные ЧУМы обладают этими свойствами
- Есть важные бесконечные ЧУМы, которые ими не обладают
  - ⋆ например, $(\mathbb{Z}, \leqslant)$ и $([0,1], \leqslant)$
  - ⋆ есть и положительные примеры: $(\mathbb{N}, \leqslant)$, $(\mathbb{N}, |)$
  - ⋆ но есть и отрицательные: лексикографический порядок на Σ^* ($|\Sigma| > 1$)
  - ⋆ но есть и положительные: радиксный порядок на Σ^* (например, для конечных Σ)

! Используя лексикографический порядок, приведите «доказательство» по индукции, что все слова из $\{0,1\}^*$ состоят только из нулей

Инфимум и супремум

Пусть $(A, \preccurlyeq)$ — произвольное упорядоченное множество (ЧУМ), $B \subseteq A$

- Элемент $a \in A$ — нижняя грань множества B, если $a \preccurlyeq b$ для любого $b \in B$
  - $\bot(B) = \{a \in A \mid a$ — нижняя грань $B\}$
- Элемент $a \in A$ — верхняя грань множества B, если $b \preccurlyeq a$ для любого $b \in B$
  - $\top(B) = \{a \in A \mid a$ — верхняя грань $B\}$
- Пример:



  - $\bot(\{a, c, d\}) = \varnothing$; $\top(\{a, c, d\}) = \{d, e, f, g\}$
  - $\bot(\{d, e\}) = \{a, b, c, d\}$; $\top(\{d, e\}) = \{e, g\}$
- Инфимум подмножества $B \subseteq A$ — это его наибольшая нижняя грань
  - $(\bot(B), \preccurlyeq_{|\bot(B)})$ — это подЧУМ в $(A, \preccurlyeq)$
  - если он имеет наибольший элемент — это $\inf(B)$
  - если нет — $\inf(B)$ не определен
  - ⋆ в примере $\inf(\{d, e\}) = d$, $\inf(\{a, c, d\})$ не определен
- Супремум подмножества $B \subseteq A$ — это его наименьшая верхняя грань
  - ⋆ в примере $\sup(\{d, e\}) = e$, $\sup(\{a, c, d\}) = d$

★ Инфимум и супремум — двойственные понятия; в двойственном ЧУМе $(A, \succcurlyeq)$ они поменяются ролями

Полурешетки

- Если в ЧУМе $(A, \preccurlyeq)$ для любой пары элементов существует супремум, то $(A, \preccurlyeq)$ называется верхней полурешеткой
  - ⋆ в этом случае часто вместо $\sup(a, b)$ пишут $a \vee b$ и говорят «объединение a и b»
  - англоязычный термин — join
- объединение — бинарная алгебраическая операция

Теорема

Операция $\vee$ в ЧУМе ассоциативна, коммутативна и идемпотентна.

Доказательство:

- $a \vee a = a$ (идемпотентность) очевидна, т.к. $\{a, a\} = \{a\}$ и $\sup(\{a\}) = a$
- $a \vee b = b \vee a$ (коммутативность) очевидна, т.к. $\{a, b\} = \{b, a\}$
- докажем, что $(a \vee b) \vee c = a \vee (b \vee c)$ (ассоциативность)
  - заметим, что $(a \preccurlyeq x \text{ и } b \preccurlyeq x) \Leftrightarrow \sup(\{a, b\}) \preccurlyeq x$
  - $x \in \top(\{\sup(\{a, b\}), c\}) \Leftrightarrow a \preccurlyeq x, b \preccurlyeq x, c \preccurlyeq x \Leftrightarrow x \in \top(\{a, b, c\})$

  $\Rightarrow \top(\{\sup(\{a, b\}), c\}) = \top(\{a, b, c\})$
  - аналогично, $\top(\{a, \sup(\{b, c\})\}) = \top(\{a, b, c\})$

  $\Rightarrow \top(\{\sup(\{a, b\}), c\}) = \top(\{a, \sup(\{b, c\})\})$

  $\Rightarrow \sup(\{\sup(\{a, b\}), c\}) = \sup(\{a, \sup(\{b, c\})\})$

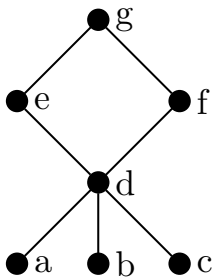
□

★ Итак, $(A, \vee)$ — полугруппа
  - ⋆ полурешетка = коммутативная полугруппа идемпотентов

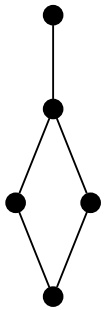
Полурешетки (2)

- Нижняя полурешетка определяется двойственным условием:
  - для любой пары элементов ЧУМа $(A, \preccurlyeq)$ существует инфимум
  - обозначение: $a \wedge b$ (пересечение, meet)

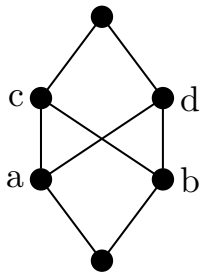
Примеры:



Верхняя полурешетка



И верхняя, и нижняя



Ни та, ни другая

- ЧУМ, двойственный к верхней полурешетке, является нижней полурешеткой
- Корневое дерево — это всегда полурешетка (например, верхняя)
- В дереве $a \vee b = LCA(a, b)$ — это ближайший общий предок вершин a и b
  - ⋆ структура данных, построенная по дереву и эффективно отвечающая на запросы «найти $LCA(a, b)$» — важный элемент многих сложных алгоритмов
  - ⋆ простейшее приложение: расстояние между вершинами a, b равно $depth(a) + depth(b) - 2 \cdot depth(LCA(a, b))$

Решетки

- Если ЧУМ $(A, \preccurlyeq)$ является и верхней, и нижней полурешеткой, то он называется решеткой
  - эту решетку записывают как $(A, \vee, \wedge)$
- Кроме того, что каждая из операций $\vee, \wedge$ коммутативна, ассоциативна и идемпотентна, они согласованы между собой:

★ Для любых $a, b \in A$, $a \wedge (a \vee b) = a \vee (a \wedge b) = a$ (тождества поглощения)

Доказательство:

$x \preccurlyeq a \Rightarrow x \preccurlyeq a \vee b$ по транзитивности

$\Rightarrow \perp(\{a, a \vee b\}) = \perp(\{a\})$

$\Rightarrow a \wedge (a \vee b) = \inf(\{a, a \vee b\}) = \inf(\{a\}) = a$ □

! двойственное тождество поглощения докажите самостоятельно

★ Можно дать альтернативное определение решетки:

Решетка — это алгебра с двумя бинарными операциями, удовлетворяющими тождествам ассоциативности, коммутативности, идемпотентности и поглощения

- Какое из определений более «правильное»?
- Решетка — это что-то типа кольца/поля или частный случай ЧУМа?

Ответы в следующем фрагменте $\Longrightarrow$

Теорема о решетке

- Пусть $(A, \vee, \wedge)$ — решетка (алгебра)
- Определим на A бинарное отношение $\preccurlyeq$ условием $a \preccurlyeq b \Leftrightarrow a \wedge b = a$

★ $\preccurlyeq$ — отношение порядка

Доказательство:

- $a \wedge a = a$ (идемпотентность) $\Rightarrow a \preccurlyeq a$ (рефлексивность)
- $a \wedge b = b \wedge a$ (коммутативность) $\Rightarrow (a \preccurlyeq b$ и $b \preccurlyeq a \Rightarrow a = b)$ (антисимметричность)
- докажем транзитивность: пусть $a \preccurlyeq b, b \preccurlyeq c$, т.е. $a \wedge b = a$, $b \wedge c = b$; тогда $a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c)$ (ассоциативность) $= a \wedge b = a \Rightarrow a \preccurlyeq c$ □

★ То же самое отношение $\preccurlyeq$ можно определить условием $a \vee b = b$:

- если $a \wedge b = a$, то $a \vee b = (a \wedge b) \vee b = b$ (поглощение)
- если $a \vee b = b$, то $a \wedge b = a \wedge (a \vee b) = a$ (снова поглощение)

⋆ Итак, получили ЧУМ $(A, \preccurlyeq)$, порожденный решеткой $(A, \vee, \wedge)$

Теорема

Пусть ЧУМ $(A, \preccurlyeq)$ порожден решеткой $(A, \vee, \wedge)$. Тогда в $(A, \preccurlyeq)$ для любой пары элементов $a, b \in A$ определены супремум и инфимум, причем $\sup(a, b) = a \vee b$ и $\inf(a, b) = a \wedge b$

- Теорема утверждает, что решетка порождает ЧУМ, который задает эту решетку
- Т.е. решетка (алгебра) и решетка (ЧУМ специального вида) — два эквивалентных способа задать один и тот же математический объект

Теорема о решетке — доказательство

- Пусть ЧУМ $(A, \preccurlyeq)$ порожден решеткой $(A, \vee, \wedge)$
- Надо доказать, что $\sup(a, b)$ существует и равен $a \vee b$ для любых $a, b \in A$

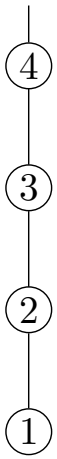
  ! аналогичную проверку для инфимума провести самостоятельно
- $a \vee b$ — верхняя грань для $\{a, b\}$:
  - $a \wedge (a \vee b) = a$ (поглощение) $\Rightarrow a \preccurlyeq (a \vee b)$ по определению
  - аналогично $b \preccurlyeq (a \vee b)$
- $a \vee b$ — наименьшая верхняя грань для $\{a, b\}$:
  - надо показать, что $x \in \top\{a, b\} \Rightarrow a \vee b \preccurlyeq x$ для любого $x \in A$
  - по второму определению $\preccurlyeq$, $x \in \top\{a, b\}$ означает $a \vee x = x$ и $b \vee x = x$
  - тогда $(a \vee b) \vee x = a \vee (b \vee x) = a \vee x = x$
    т.е. $(a \vee b) \preccurlyeq x$ по второму определению $\square$
- Доказав теорему, можно «официально» считать, что в решетке есть две операции и отношение порядка, и пользоваться этим

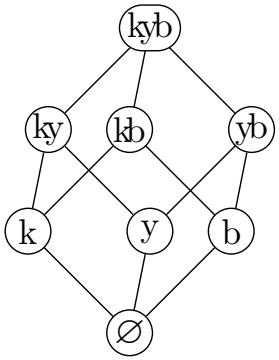
★ Поскольку определение решетки как алгебры симметрично относительно операций $\vee$ и $\wedge$, для любой решетки $(A, \vee, \wedge)$ существует двойственная решетка $(A, \wedge, \vee)$, и она порождает ЧУМ $(A, \succcurlyeq)$, двойственный к ЧУМу $(A, \preccurlyeq)$, порожденному $(A, \vee, \wedge)$

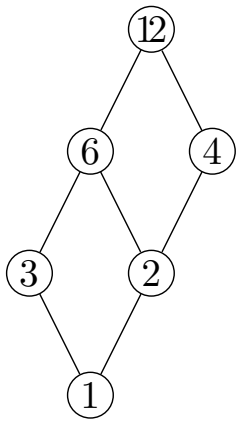
Примеры решеток

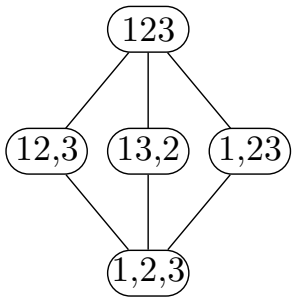
1. ЧУМ $(\mathbb{N}, \leqslant)$ — это решетка $(\mathbb{N}, \max, \min)$
   - вообще, любое линейно упорядоченное множество — решетка
2. ЧУМ $(2^A, \subseteq)$ для любого множества A — это решетка $(2^A, \cup, \cap)$
   - это самый «регулярный» тип решетки — булева алгебра
3. ЧУМ $(\mathbb{N}, |)$ — это решетка $(\mathbb{N}, \mathrm{lcm}, \gcd)$
   - часто рассматривают решетку делителей фиксированного натурального n
4. ЧУМ $(Eqv(A), \subseteq)$ отношений эквивалентности на A — это решетка разбиений
   - в решетке разбиений $\rho \wedge \sigma = \rho \cap \sigma$, $\rho \vee \sigma = \mathrm{Cl}_T(\rho \cup \sigma)$ (транзитивное замыкание)
5. ЧУМ $(Sub(L), \subseteq)$ подпространств линейного пространства L — это решетка подпространств
   - $U_1 \wedge U_2 = U_1 \cap U_2$, $U_1 \vee U_2 = U_1 + U_2$
   - аналогично определяется решетка подгрупп группы, решетка подколец кольца, . . .

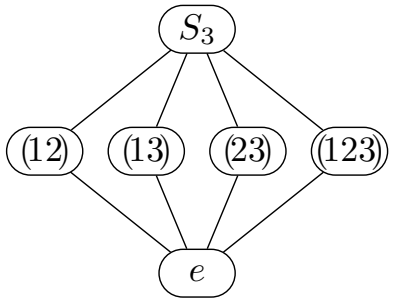
. . .











Подрешетки

- Пусть $(A, \vee, \wedge)$ — решетка. Подмножество $B \subseteq A$ замкнуто, если
  - $a \vee b \in B$, $a \wedge b \in B$ для любых $a, b \in B$
- Тогда $(B, \vee, \wedge)$ — решетка, называемая подрешеткой решетки $(A, \vee, \wedge)$

  ... надо бы писать $(B, \vee_{|B}, \wedge_{|B})$, но обычно не загромождают обозначения

★ Любое $B \subseteq A$ образует подЧУМ в ЧУМе $(A, \preccurlyeq)$, порожденном $(A, \vee, \wedge)$

  ... но этот ЧУМ не всегда — решетка! (B может не быть замкнутым)

★ Замкнутые подмножества из A образуют систему замкнутых подмножеств
  - см. фрагмент 1-4 про замыкания подмножеств

★ Чтобы найти наименьшую подрешетку, содержащую заданное $B \subseteq A$, нужно взять наименьшее замкнутое подмножество $\bar{B} \subseteq A$, содержащее B
  - $\bar{B}$ — замыкание B (фрагмент 1-4)
  - $(\bar{B}, \vee, \wedge)$ — искомая подрешетка
  - подрешетка $(\bar{B}, \vee, \wedge)$ порождена B, а B — ее порождающее множество
    - ⋆ порождающее множество обычно не единственно
- Пример: найдем подрешетку в $(\mathbb{N}, \mathrm{lcm}, \gcd)$, порожденную множеством $\{6, 10, 15\}$
  - надо добавить
    $\gcd(6,10) = 2$, $\gcd(6,15) = 3$, $\gcd(10,15) = 5$, $\gcd(2,3) = \gcd(2,5) = \gcd(3,5) = 1$
    и $\mathrm{lcm}(6,10) = \mathrm{lcm}(6,15) = \mathrm{lcm}(10,15) = 30$
  - искомая подрешетка — решетка делителей числа 30

⋆ Решетка подрешеток заданной решетки — вполне себе объект для изучения...

Дистрибутивность

- В других известных нам алгебрах с двумя операциями (кольца, поля) операции связаны тождеством дистрибутивности
  - $a \cdot (b + c) = a \cdot b + a \cdot c$
  - в некоммутативном кольце выполнены левая и правая дистрибутивность
- Как насчет решеток?

Теорема

В произвольной решетке $(A, \vee, \wedge)$ выполнены неравенства $(a \wedge b) \vee (a \wedge c) \preccurlyeq a \wedge (b \vee c)$ и $a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge (a \vee c)$.

Доказательство:

- докажем первое неравенство (второе — самостоятельно)
- $(a \wedge b) \preccurlyeq a \wedge (b \vee c)$, потому что $(a \wedge b) \wedge (a \wedge (b \vee c)) = ((a \wedge b) \wedge a) \wedge (b \vee c) = a \wedge (b \wedge (b \vee c)) = a \wedge b$
- аналогично $(a \wedge c) \preccurlyeq a \wedge (b \vee c)$

$\Rightarrow (a \wedge b) \vee (a \wedge (b \vee c)) = (a \wedge c) \vee (a \wedge (b \vee c)) = a \wedge (b \vee c)$

$\Rightarrow ((a \wedge b) \vee (a \wedge c)) \vee (a \wedge (b \vee c)) = a \wedge (b \vee c)$

$\Rightarrow (a \wedge b) \vee (a \wedge c) \preccurlyeq a \wedge (b \vee c)$ □

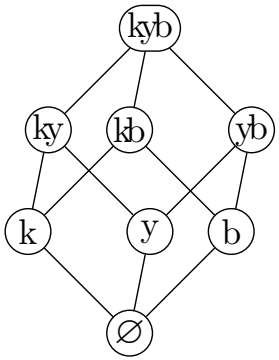
★ Если для данной решетки $(A, \vee, \wedge)$ неравенства в теореме можно заменить равенствами, то решетка называется дистрибутивной

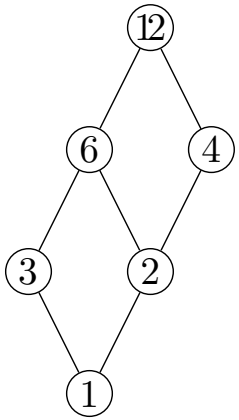
- ⋆ за 2-3 слайда выкладок можно доказать, что из одного тождества дистрибутивности в решетке следует второе

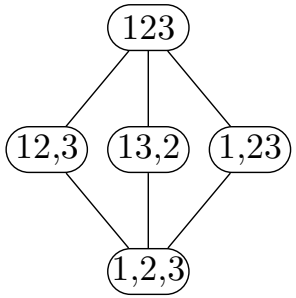
Дистрибутивность (2)

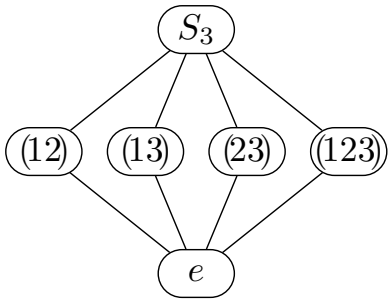
Примеры:

...









Первые три решетки дистрибутивны, последние две — нет

Теорема (без д-ва)

Решетка $(A, \vee, \wedge)$ дистрибутивна тогда и только тогда, когда в ней нет подрешеток

 (пентагон) и  (диамант).

! докажите, что пентагон и диамант не дистрибутивны

Дополнения и булевы алгебры

- Наименьший элемент решетки, если он существует, называется нулем (0)
- Наибольший элемент решетки, если он существует, называется единицей (1)
- В решетке $(A, \vee, \wedge)$ с 0 и 1 элемент b называется дополнением элемента a, если $a \vee b = 1$ и $a \wedge b = 0$
- Решетка называется решеткой с дополнениями, если в ней любой элемент имеет единственное дополнение

Теорема

В дистрибутивной решетке $(A, \vee, \wedge)$ любой элемент имеет не более одного дополнения.

Доказательство:

- заметим, что $0 \vee a = a$, $0 \wedge a = 0$, $1 \vee a = 1$, $1 \wedge a = a$ для любого $a \in A$
- пусть b и b' — дополнения a
- $b = b \vee (a \wedge b') = (b \vee a) \wedge (b \vee b') = b \vee b' = (a \vee b') \wedge (b \vee b') = (a \wedge b) \vee b' = b'$ □

- Дистрибутивная решетка с дополнениями называется булевой алгеброй

Теорема (без д-ва)

Любая конечная булева алгебра изоморфна булеану некоторого множества.

★ Число элементов в конечной булевой алгебре является степенью двойки