Disc Math - §15 - Relations

Def. A binary relation on a set S is a subset of $S \times S$.

not: $(x,y) \in \rho \Leftrightarrow x \rho y$.

ex: $S = \{-1, 2, 3\}$ The relation of strict inequality is $\rho^{<} = \{(-1,2), (-1,3), (2,$

The relation of equality is $\rho^{=} = \{(-1,-1), (2,2), (3,3)\}$.

ex: On $\mathbb{Z}$ consider the relation ρ: $m \rho n \Leftrightarrow m - n \in \mathbb{Z}_{even}$.

Then $\rho = \{\mathbb{Z}_{even} \times \mathbb{Z}_{even} \cup \mathbb{Z}_{odd} \times \mathbb{Z}_{odd}\} \subset \mathbb{Z} \times \mathbb{Z}$.

Def: More generally:

i) Given two sets S and T a binary relation from S to T is a subset of $S \times T$.

ii) Given sets $S_1, S_2, \ldots, S_n$, $n \geq 2$ an n-ary relation on $S_1 \times S_2 \times \ldots \times S_n$ is a subset of $S_1 \times S_2 \times \ldots \times S_n$.

ex: $\{(m,n) \in \mathbb{Z} \times \{\mathbb{N} \cup \{0\}\} \mid m^2 = n\}$ is a binary relation on $\mathbb{Z} \times \{\mathbb{N} \cup \{0$

Operations on relations.

Let ρ, σ be two relations on S. Since $\rho, \sigma \subset S \times S$ we can form $\rho \cup \sigma$, $\rho \cap \sigma$, ρ' etc.

ex: On $\mathbb{Z}$: $m \rho n \Leftrightarrow m = n$; $m \sigma n \Leftrightarrow m < n$ Then

$m (\rho \cup \sigma) n \Leftrightarrow m \leq n$; $\rho \cap \sigma = \emptyset$; $m \rho' n \Leftrightarrow m \neq n$; $m \sigma' n \Leftrightarrow m \geq$

rem: All Boolean algebra identities hold.

Properties of relations.

Def: Let ρ be a binary relation on a set S. Then

i) ρ is reflexive if $\forall x,\ x \in S \to (x,x) \in \rho$

ii) ρ is symmetric if $\forall x, y \in S$, $(x,y) \in \rho \to (y,x) \in \rho$

iii) ρ is transitive if $\forall x, y, z \in S$, $\{(x,y) \in \rho \wedge (y,z) \in \rho\} \to (x,z) \in \rho$.

iv) ρ is antisymmetric if $\forall x, y \in S$, $\{(x,y) \in \rho \wedge (y,x) \in \rho\} \to x = y$.

ex: $S = \{a, b, c\}$, $\rho = \{(a,b), (b,c), (a,c)\}$: not reflexive, not symmetric, transitive, antisymmetric.

ex: On $\mathbb{Z}$, $\rho = \{(m,n) \mid 2 \mid (m-n)\}$ → reflexive, symmetric, transitive, but not antisymmetric.

ex: On $P(\mathbb{N})$, $A \rho B \Leftrightarrow A \subseteq B$ → reflexive, not symmetric, transitive, antisymmetric.

ex: The empty relation $\emptyset \in S \times S$ → ~~not~~ reflexive, symmetric, transitive antisymmetric.

ex: On $\mathbb{N}$, $\rho = \{(m,n) \mid m = n\}$ → reflexive, symmetric, transitive, antisymmet

Closures of relations.

Def: A binary relation ρ^* on a set S is the closure of a relation ρ on S wrt property P if

1) ρ^* has the property P. 2) $\rho \subseteq \rho^*$

3) ρ^* is the smallest (in a sense of subset of $S \times S$) relation containi ρ and having property P.

ex: $S = \{1,2,3\}$, $\rho = \{(1,1), (1,2), (1,3), (3,1), (2,3)\}$. This relation is not reflexive, not symmetric, not transitive.

i) The closure of ρ with respect to reflexivity is

$$\rho_1 = \{(1,1), (1,2), (1,3), (3,1), (2,3), (2,2), (3,3)\}$$

ii) The closure of ρ wrt symmetry is:

$$\rho_2 = \{(1,1), (1,2), (1,3), (3,1), (2,3), (2,1), (3,2)\}.$$

iii) The closure of ρ wrt reflexivity and symmetry is:

$$\rho_3 = \{(1,1), (1,2), (1,3), (3,1), (2,3), (2,2), (3,3), (2,1), (3,2)\}.$$

iv) The transitive closure may require more than one step:

First add: $(3,2), (3,3), (2,1)$. This is still not transitive, add $(2,2)$.

The transitive closure is

$$\rho_4 = \{(1,1), (1,2), (1,3), (3,1), (2,3), (3,2), (3,3), (2,1), (2,2)\}$$

rem: There is no antisymmetric closure of a relation (but there is a quotening procedure).

Partial orderings.

Def: A binary relation on a set S that is reflexive, antisymmetric and transitive is called a partial ordering on S.

A set S with partial ordering ρ is called a partially ordered set (poset).

ex: $\mathbb{N}, m \leq n$; $P(\mathbb{N}), A \subseteq B$; $\mathbb{N}, m | n$.

not: The relation in a general poset S is typically denoted by $\preceq$. If $x \preceq y \wedge x \neq y$ we write $x \prec y$ and say that x is the predecessor of y and y is a successor of x. If $x \prec y$ and $\nexists z$ s.t. $x \prec z \prec y$, then x is an immediate predecessor of y.

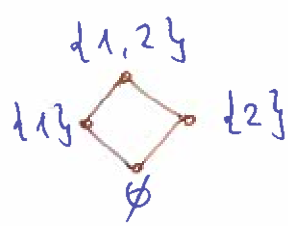
ex: $P(\mathbb{N}), A \subseteq B$ then $\{1,2,3\}$ is an immediate predecessor of $\{1,2,3,8\}$.

def: If $S, \preceq$ is a poset and $A \subseteq S$ then $\preceq$ restricted to $A \times A$ is a partial ordering on A called the restriction of $\preceq$ to A.

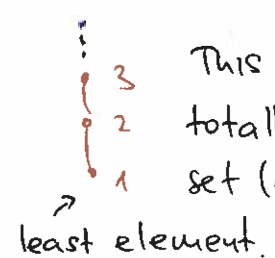
ex: $\mathbb{Z}, m \leq n$ restricts to $\mathbb{N}, m \leq n$.

rem: Finite (small) posets can be visualized via their Hasse diagrams. (only connect immediate predecessors)

ex: $P(\{1,2\}), \subseteq$

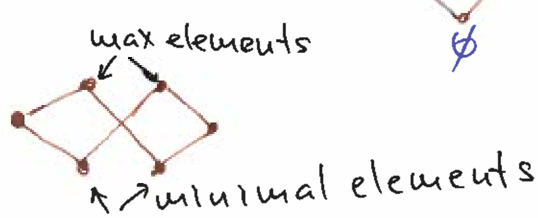


ex: $\mathbb{N}, \leq$



This is a totally ordered set (a chain)

ex:



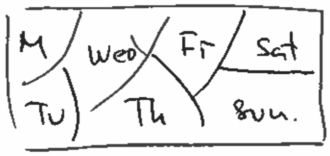
Equivalence relations.

Def: A binary relation on a set S that is reflexive, symmetric and transitive is called an equivalence relation on S.

ex: $\mathbb{Z}$, $m \rho n \Leftrightarrow 2 \mid (m-n)$ is an equivalence relation.

ex: Students in this class, A was born on the same day of the week as

Now notice that the students split into groups:



Def: A partition of a set S is a collection of disjoint subsets of S whose union is S.

def: Let ρ be an equivalence relation on a set S. For $x \in S$, the set $\{y \mid y \rho x\} = [x]$ is called the equivalence class of x.

ex: $\mathbb{Z}$, $m \rho n \Leftrightarrow 2(m-n)$. What is $[1]$, $[3]$, $[-2]$?

Th: An equivalence relation ρ on a set S determines a partition of S. Conversely a partition of a set S determines an equivalence relation on S.

Pr: $\rho \rightarrow$ the partition is the set of distinct equivalence classes of ρ.
From a partition $\rightarrow$ two elements of S are related if they are in the same cell of the partition. $\boxtimes$

ex: $S = \{a, b, c\}$, $\rho = \{(a,a), (a,b), (b,b), (b,a), (c,c)\} \rightarrow \{a,b\} \cup \{c\} = S$

ex: $\mathbb{Z}$, $m \rho n \Leftrightarrow 2(m-n)$. The associated partition is $\mathbb{Z}_{odd} \cup \mathbb{Z}_{even}$.

ex: Let $S = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$ be the set of all fractions. On S we have a relation $\frac{a}{b} \sim \frac{c}{d}$ iff $ad = bc$. This is an equivalence relation. Reflexivity and symmetry are obvious. Let $\frac{a}{b} \sim \frac{c}{d} \wedge \frac{c}{d} \sim \frac{e}{f}$. Then $ad = bc$, $cf = de$. Consider $afd = bcf = bed \Rightarrow af = be$ since $d \neq 0 \Rightarrow \frac{a}{b} \sim \frac{e}{f}$. Thus $\sim$ is also transitive. We have $S/\sim = \mathbb{Q}$.

Notice that: $\left[\frac{4}{16}\right] = \left[\frac{3}{12}\right] = \left[\frac{-21}{-84}\right] = \left[\frac{-1}{-4}\right] = \left[\frac{1}{4}\right]$.

The arithmetic of the fractions descends to arithmetic on $\mathbb{Q}$

Def: Congruence modulo n: $x, y \in \mathbb{Z}$, $n \in \mathbb{N}$

$x \equiv y \pmod{n}$ if $n \mid (x-y)$.

Prop: Congruence modulo n is an equivalence relation.

Pr: Reflexivity and symmetry are obvious. Transitivity: let $x \equiv y \pmod{n}$, $y \equiv z \pmod{n}$. Thus $x-y = kn$, $y-z = \ell n \Rightarrow x-z = (x-y)+(y-z) = (k+\ell)n$ $\Rightarrow x \equiv z \pmod{n}$. ☒

Ex: What are the equivalence classes of mod 4 → $[0], [1], [2], [3]$.

Ex: Describe mod 12 ∩ mod 10 → mod 60.

Ex: $35 \equiv 2 \pmod{3}$, $12 \equiv 0 \mod 3$, $-12 \equiv 6 \pmod{9}$

$8^4 = 3^4 \pmod{5} = 729 \pmod{5} = 4$.

rem: The arithmetic descends to the equivalence classes mod n.

$[a]+[b] = [a+b]$; $[a]-[b] = [a-b]$; $[a][b] = [ab]$; $[a]^n = [a^n]$.

Def: $\mathbb{Z}_n$ is the set of distinct equivalence classes of $\mathbb{Z}$ mod n, i.e. $\mathbb{Z}_n = \{[0], \ldots, [n-1]\}$. $\mathbb{Z}_n$ - has multiplication and addition as above (commutative ring).

Ex: In $\mathbb{Z}_{19}$: $[17]+[17] = [31] = [12]$. In $\mathbb{Z}_{19}$: $[6]\cdot[10] = [60] = [3]$

Ex: $\mathbb{Z}_3$

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

·	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

HW p345 §5.1
12, 18, 35, 38, 50, 56
58, 62, 76

Ex: $\mathbb{Z}_4$

·	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

$[2] \times [2] = [0]$

$[2]$ - is a zero divisor

$\mathbb{Z}_4$ - is a ring but not a field.

Prop: $\mathbb{Z}_p$, for p - prime is a field! Pr: Euclidean algorithm.

Ex: Find the reciprocal of $[12]$ in $\mathbb{Z}_{67}$: $67 = 5.12 + 7$, $12 = 1.7 + 5$
$7 = 1.5 + 2$, $5 = 2.2 + 1 \Rightarrow 1 = -5.67 + 28.12 \Rightarrow [12]^{-1} = [28]$ in $\mathbb{Z}_{67}$.