Last time:

Relations:

- Closures of relations (Section 9.4)
- Equivalence relations (Section 9.5)

Today:

- Partial orders (Section 9.6)
- Exam tips
- Midway evaluation

Number theory:

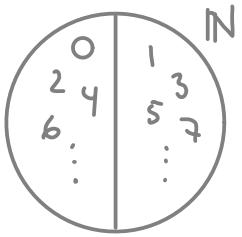
- Divisibility & congruence (Section 4.1)

Next two lectures:

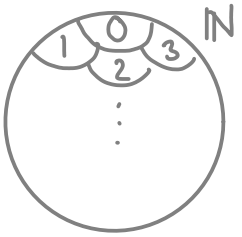
- Primes (Section 4.3)
- Solving congruences (Section 4.4)

Equivalence Relations

Ex: $\{(a,b) \in \mathbb{N} \times \mathbb{N} \mid a \text{ and } b \text{ have the same parity}\}$



Ex: $\{(a,b) \in \mathbb{N} \times \mathbb{N} \mid a = b\}$



Theorem 9.5.1:

If R is an equivalence relation, then

$$\begin{array}{ll} aRb & \text{(i)} \\ \Updownarrow & \\ [a]_R = [b]_R & \text{(ii)} \\ \Updownarrow & \\ [a]_R \cap [b]_R \neq \emptyset & \text{(iii)} \end{array}$$

Specifically,

$$[a]_R \cap [b]_R \neq \emptyset \quad \Rightarrow \quad [a]_R = [b]_R$$

Theorem 9.5.2

For any set A,

(i) If R is an equivalence relation on A, then the equivalence classes of R form a partition of A.

(ii) If P is a partition of A, then there exists an equivalence relation on A whose equivalence classes form a partition of A.

Proof:

(i): Equivalence classes $\longrightarrow$ partition

The eq. classes cover all of A:

$\forall a \in A: a \in [a]$, since R is reflexive

The eq. classes are disjoint:

Contraposition:

$$[a] \cap [b] \neq \emptyset \Rightarrow [a] = [b]$$
$$\Updownarrow$$
$$[a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset$$

, by Thm 9.5.1

(ii): Partition $\longrightarrow$ equivalence relation:

If P is a partition of A, then
$R = \{(a,b) \mid a \text{ and } b \text{ are in the same set in } P\}$
is an equivalence relation:

Reflexive:

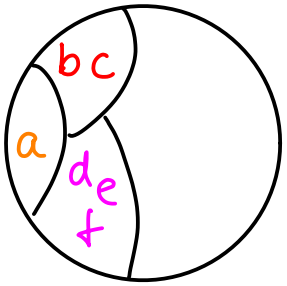
Any $a \in A$ is in the same set as a.

Symmetric:

If b is in the same set as c, then
c is in the same set as b.

Transitive:

If d is in the same set as e and
e is in the same set as f, then
d is in the same set as f.



Moreover, each set $S \in P$ is the equivalence class of each of the elements in S.

Partial Orders

(Afsnit 9.6)

Def 9.6.1

If a relation R on a set A is
- reflexive,
- antisymmetric, and
- transitive,

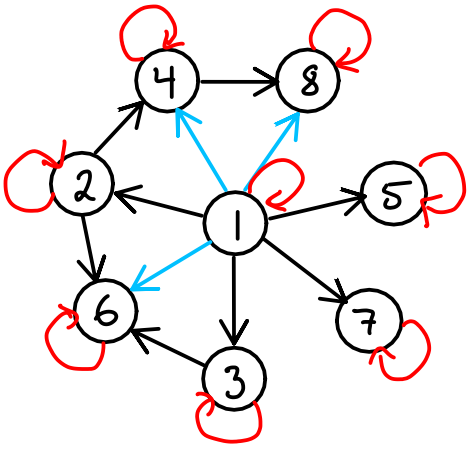
R is a partial order (or ordering) and (A,R) is a partially ordered set (poset).

Ex:

✓: $\leq$ $=$ $|$ $\subseteq$

✗: $<$ $\neq$ $\subset$ „same parity"

Ex: $(\{1,2,3,4,5,6,7,8\}, |)$ is a poset



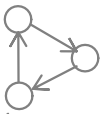
→ Follow from transitivity

↻ Follow from reflexivity

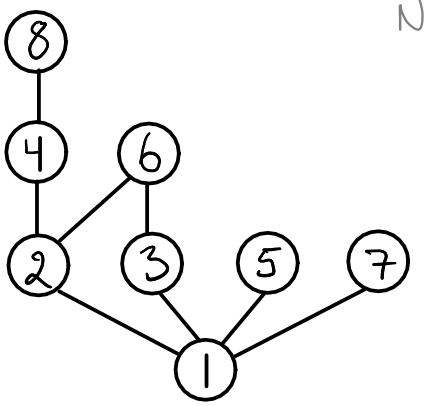
Hasse Diagram (Section 9.6.3)

Like the graph representation but:

- Edges instead of arcs.
  If aRb, then a is placed under b

  But what if there is a cycle? 
  Not possible because of antisymmetry and transitivity.

- Edges that follow from reflexivity and transitivity are left out



Note: Paths go upwards only. If you follow an edge downwards, it corresponds to following an arc in the wrong direction in the original graph.

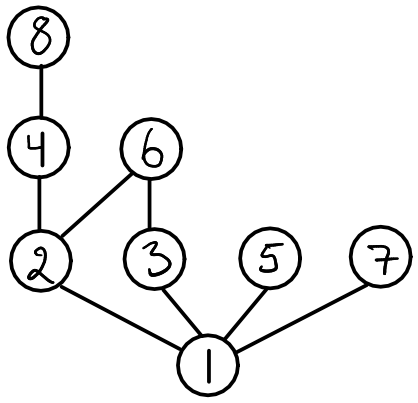
Def. 9.6.2

Let $\preceq$ be a partial order.

If $a \preceq b$ or $b \preceq a$, then a and b are comparable

Otherwise, they are incomparable.

Ex: $(\{1,2,3,4,5,6,7,8\}, |)$ (again)



2 and 5 are incomparable

6 and 8 are incomparable

2 and 8 are comparable

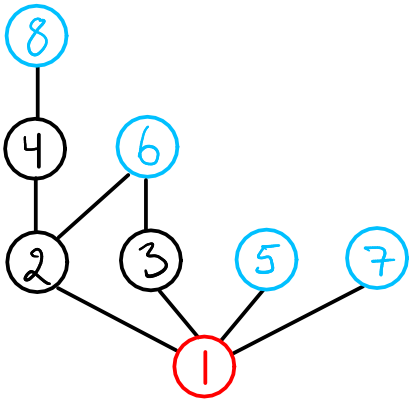
1 and 5 are comparable

Let $(S, \preceq)$ be a poset and $a \in S$.
Then, a is

- a minimal element if $\nexists b \in S - \{a\} : b \preceq a$
  i.e., for any element $b \neq a$, either $a \preceq b$ or a and b are not comparable.
- the least element if $\forall b \in S : a \preceq b$
- a maximal element if $\nexists b \in S - \{a\} : a \preceq b$
  i.e., for any element $b \neq a$, either $b \preceq a$ or a and b are not comparable.
- the greatest element if $\forall b \in S : b \preceq a$

Note: Any least element is also a minimal element, and any greatest element is also a maximal element.

Ex: $(\{1,2,3,4,5,6,7,8\}, |)$ (again)



Maximal

Least (and hence, minimal)

Total Orders (a special kind of partial orders)

Def. 9.6.3:

Let $(S, \preccurlyeq)$ be a poset.
If all pairs $a, b \in S$ are comparable, then $\preccurlyeq$ is total order.

Ex:

✓: $\leq$

✗: $=$ | $\subseteq$ $<$

Ex: $R = \{(a,b) \mid a \leq b\}$ on $\{1,2,3,4,5\}$ is a total order

Hasse diagram:

Lexicografic Order

A lexicographic order is a partial order built on one or more partial orders.

Below we will see a couple of examples, each built on just one partial order, $\preceq$ or the alphabetic order.

Ex: (Points)

$(1,5) \preceq (2,3)$

$(1,2) \preceq (1,3)$

$(2,3,4,5) \preceq (2,3,5,4)$

Ex II: (Strings)

discreet $\preceq$ discrete

discreet $\preceq$ discreetness

discrete $\preceq$ discretion

Exam

January 26

DM547, MM537: 3 hours

DM549, DS820: 4 hours

Internet not allowed (except for accessing the test)

Tips

- Start by getting an overview of the exam
- Use paper and pen while taking the exam
- Justify your answers (it may help to even write down your reasoning)
- Use old exams to practise

Number theory

Section 4.1: Divisibility, Congruence & Modular Arithmetic

Section 4.3: Primes

Section 4.4: Solving Congruences

Applications:

- Cryptology
- Hashing (DM573 weeks 39-40 and DM578)
- Pseudo random numbers
- ⋮

Divisibility

Ex:

$3 \mid 15$: $\frac{15}{3} = 5 \iff 15 = 5 \cdot 3$

$3 \nmid 16$: $\frac{16}{3} = 5, \bar{3}$

$3 \mid 24$: $\frac{24}{3} = 8 \iff 24 = 8 \cdot 3$

Def 4.1.1: For any $a, b \in \mathbb{Z}$, $a \neq 0$,

$$a \mid b \iff \frac{b}{a} \in \mathbb{Z} \iff \exists k \in \mathbb{Z} : b = k \cdot a$$

„a divides b"

„a is a factor in b"

„b is a multiple of a"

Theorem 4.1.1

For any $a,b,c \in \mathbb{Z}$, $a \neq 0$,

(i) $a|b \wedge a|c \Rightarrow a|(b+c)$

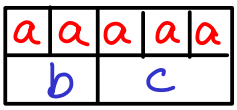
(ii) $a|b \Rightarrow \forall k \in \mathbb{Z} : a|kb$

(iii) $a|b \wedge b|c \Rightarrow a|c$

Proof:

(i): If a and b are multiples of m, then a+b is also a multiple of m:

$$
\begin{array}{ll}
 & a|b \wedge a|c \\
\text{Def. 4.1.1} \Updownarrow & b = k\cdot a \wedge c = \ell\cdot a, \quad k,\ell \in \mathbb{Z} \\
\Downarrow & b+c = (k+\ell)\cdot a, \quad k+\ell \in \mathbb{Z} \\
\text{Def. 4.1.1} \Updownarrow & a|(b+c)
\end{array}
$$



(ii): Exercise 3

(iii): Exercise 4

□

Theorem 4.1.1

For any $a, b, c \in \mathbb{Z}$, $a \neq 0$,

(i) $a \mid b \wedge a \mid c \Rightarrow a \mid (b+c)$

(ii) $a \mid b \Rightarrow \forall k \in \mathbb{Z} : a \mid kb$

(iii) $a \mid b \wedge b \mid c \Rightarrow a \mid c$

$\Rightarrow$

Corollary 4.1.1

$a \mid b \wedge a \mid c \Rightarrow$
$\forall k, \ell \in \mathbb{Z} : a \mid (kb + \ell c)$

Proof of Corollary 4.1.1:

For any $k, \ell \in \mathbb{Z}$,

$a \mid b \Rightarrow a \mid kb$ (by (ii))

$a \mid c \Rightarrow a \mid \ell c$ (by (ii))

$\Rightarrow a \mid (kb + \ell c)$ (by (i))

□

Ex:

By Cor. 4.1.1,

$3 \mid 27 \wedge 3 \mid 30 \Rightarrow 3 \mid 111$,

since $111 = 3 \cdot 27 + 30$

Ex: Dividing 16 by 3 leaves a remainder of 1:

$16 = 3 \cdot 5 + 1$

Thus,

$16 \text{ div } 3 = 5$

$16 \text{ mod } 3 = 1$

Theorem 4.1.2: (The Division Algorithm) which is not an algorithm!

For any $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$,

$\exists! \, q, r : (a = d \cdot q + r \wedge 0 \leq r < d)$

Def. 4.1.2

dividend: a — divisor: d — quotient: q — remainder: r

$q = a \text{ div } d$

$r = a \text{ mod } d$ „a modulo d"

Ex: Dividing -16 by 3 leaves a remainder of 2:

$-16 = 3 \cdot (-6) + 2$

Thus,

$-16 \text{ div } 3 = -6$

$-16 \text{ mod } 3 = 2$