# CS1231S Chapter 7

# Modular arithmetic and partial orders

## 7.1 Modular arithmetic

**Definition 7.1.1.** A *representative* of an equivalence class is an element of the equivalence class.

**Exercise 7.1.2.** Let $A$ be a set and $\sim$ be an equivalence relation on $A$. Prove that an element $x \in A$ is a representative of an equivalence class $S$ if and only if $[x] = S$. 7a

**Example 7.1.3.** We proved in Exercise 6.2.18 that the relation $\sim$ on $\mathbb{Z}$ defined by setting

$$x \sim y \quad \Leftrightarrow \quad x = y \text{ or } x = -y$$

for all $x, y \in \mathbb{Z}$ is an equivalence relation. Note $x \sim y$ means $|x| = |y|$. From Exercise 6.4.10, we know

$$[0] = \{0\}, \quad [1] = \{1, -1\} = [-1], \quad [2] = \{2, -2\} = [-2], \quad \ldots$$

and so $\mathbb{Z}/{\sim} = \big\{\{0\}, \{1, -1\}, \{2, -2\}, \ldots\big\}$. Define addition and multiplication on $\mathbb{Z}/{\sim}$ as follows: whenever $[x], [y] \in \mathbb{Z}/{\sim}$,

$$[x] + [y] = [x + y] \quad \text{and} \quad [x] \cdot [y] = [x \cdot y].$$

Then $+$ is not well defined because $[1] = [1]$ and $[2] = [-2]$, but

$$[1] + [2] = [1 + 2] = [3] \neq [-1] = [1 + (-2)] = [1] + [-2].$$

Note $\cdot$ is well defined because whenever $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}/{\sim}$, 7b

$$[x_1] = [x_2] \text{ and } [y_1] = [y_2] \quad \Rightarrow \quad [x_1 \cdot y_1] = [x_2 \cdot y_2].$$

**Definition 7.1.4.** Let $n \in \mathbb{Z}^+$. The quotient $\mathbb{Z}/{\sim_n}$, where $\sim_n$ is the congruence-mod-$n$ relation on $\mathbb{Z}$, is denoted $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$. Define addition and multiplication on $\mathbb{Z}_n$ as follows: whenever $[x], [y] \in \mathbb{Z}_n$,

$$[x] + [y] = [x + y] \quad \text{and} \quad [x] \cdot [y] = [x \cdot y].$$

**Proposition 7.1.5.** Addition and multiplication are well defined on $\mathbb{Z}_n$ for all $n \in \mathbb{Z}^+$, i.e., whenever $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$,

$$[x_1] = [x_2] \text{ and } [y_1] = [y_2] \quad \Rightarrow \quad [x_1] + [y_1] = [x_2] + [y_2] \text{ and } [x_1] \cdot [y_1] = [x_2] \cdot [y_2].$$

**Proof.** 1. Let $[x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}_n$ such that $[x_1] = [x_2]$ and $[y_1] = [y_2]$.

2. Then Lemma 6.4.4 implies $x_1 \equiv x_2 \pmod{n}$ and $y_1 \equiv y_2 \pmod{n}$.
3. Use the definition of congruence to find $k, \ell \in \mathbb{Z}$ such that $x_1 - x_2 = nk$ and $y_1 - y_2 = n\ell$.
4. 4.1. Note $(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2) = nk + n\ell = n(k + \ell)$, where $k + \ell \in \mathbb{Z}$.
   4.2. So the definition of congruence tells us $x_1 + y_1 \equiv x_2 + y_2 \pmod{n}$.
   4.3. Hence $[x_1] + [y_1] = [x_1 + y_1] = [x_2 + y_2] = [x_2] + [y_2]$ by Lemma 6.4.4.
5. 5.1. Note $(x_1 \cdot y_1) - (x_2 \cdot y_2) = (nk + x_2)(n\ell + y_2) - x_2 y_2 = n^2 k\ell + nky_2 + n\ell x_2 + x_2 y_2 - x_2 y_2 = n(nk\ell + ky_2 + \ell x_2)$, where $nk\ell + ky_2 + \ell x_2 \in \mathbb{Z}$.
   5.2. So the definition of congruence tells us $x_1 \cdot y_1 \equiv x_2 \cdot y_2 \pmod{n}$.
   5.3. Hence $[x_1] \cdot [y_1] = [x_1 \cdot y_1] = [x_2 \cdot y_2] = [x_2] \cdot [y_2]$ by Lemma 6.4.4. □

## 7.2 Functions

**Definition 7.2.1.** Let $A, B$ be sets. A *function* or a *map* from $A$ to $B$ is an assignment to each element of $A$ exactly one element of $B$. We write $f\colon A \to B$ for "$f$ is a function from $A$ to $B$". Suppose $f\colon A \to B$.

(1) Let $x \in A$. Then $f(x)$ denotes the element of $B$ that $f$ assigns $x$ to. We call $f(x)$ the *image* of $x$ under $f$. If $y = f(x)$, then we say that $f$ *maps* $x$ *to* $y$, and we may write $f\colon x \mapsto y$.

(2) Here $A$ is called the *domain* of $f$, and $B$ is called the *codomain* of $f$.

**Convention 7.2.2.** Instead of $+(x, y)$ and $\cdot(x, y)$, people usually write $x + y$ and $x \cdot y$ respectively.

**Convention 7.2.3.** In mathematics, one can read

> Define $f\colon A \to B$ by .... Then $f$ is well defined.

as

> The condition "..." defines a function $f\colon A \to B$. We use "..." to define $f$.

Similarly, one can read

> Define $f\colon A \to B$ by .... We show that $f$ is well defined. [Insert proof here.]

as

> We show that the condition "..." defines a function $f\colon A \to B$. [Insert proof here.] We use "..." to define $f$.

**Example 7.2.4.** Define $f\colon \mathbb{Z}^+ \to \mathbb{Z}$ by setting, for each $x \in \mathbb{Z}$,

$$f(x) = x^3 - 23x.$$

Then the domain of $f$ is $\mathbb{Z}^+$ and codomain of $f$ is $\mathbb{Z}$. We know $f(1) = 1^3 - 23 \times 1 = -22$ and $f(2) = 2^3 - 23 \times 2 = -38$.

**Definition 7.2.5.** Let $A$ be a set. Then the *identity function* on $A$, denoted $\mathrm{id}_A$, is the function $A \to A$ which satisfies, for all $x \in A$,

$$\mathrm{id}_A(x) = x.$$

**Remark 7.2.6.** The domain and the codomain of $\mathrm{id}_A$ are both $A$.

**Question 7.2.7.** Define $f\colon \mathbb{Q} \to \mathbb{Q}$ by setting $f(x) = 2^x$ for all $x \in \mathbb{Q}$. Why is $f$ not well defined? ✎ 7c

**Question 7.2.8.** Define $g\colon \mathbb{Q} \to \mathbb{Q}$ by setting 7d

$$g(x) = \frac{x^2+1}{x^2+2x+1}$$

for all $x \in \mathbb{Q}$. Why is $g$ not well defined?

**Question 7.2.9.** Define $h\colon \mathbb{Q} \to \mathbb{Z}$ by setting $h(m/n) = m$ for all $m, n \in \mathbb{Z}$ where $n \neq 0$. 7e
Why is $h$ not well defined?

## 7.3 Partial orders

**Definition 7.3.1.** Let $A$ be a set and $R$ be a relation on $A$.

(1) $R$ is *antisymmetric* if $\forall x, y \in A \ \ (x \mathrel{R} y \wedge y \mathrel{R} x \Rightarrow x = y)$.

(2) $R$ is a *(non-strict) partial order* if $R$ is reflexive, antisymmetric, and transitive.

(3) Suppose $R$ is a partial order. Let $x, y \in A$. Then $x, y$ are *comparable (under $R$)* if

$$x \mathrel{R} y \quad \text{or} \quad y \mathrel{R} x.$$

(4) $R$ is a *(non-strict) total order* or a *(non-strict) linear order* if $R$ is a partial order and every pair of elements is comparable, i.e.,

$$\forall x, y \in A \ \ (x \mathrel{R} y \vee y \mathrel{R} x).$$

(5) We say that the ordered pair $(A, R)$ is a *partially ordered set*, or a *poset* for short, if $R$ is a partial order on $A$.

**Note 7.3.2.** A total order is always a partial order.

**Example 7.3.3.** Let $R$ denote the non-strict less-than relation on $\mathbb{Q}$, i.e., for all $x, y \in \mathbb{Q}$,

$$x \mathrel{R} y \quad \Leftrightarrow \quad x \leqslant y.$$

Then $R$ is antisymmetric. In fact, it is a total order.

**Example 7.3.4.** Let $R'$ denote the strict less-than relation on $\mathbb{Q}$, i.e., for all $x, y \in \mathbb{Q}$,

$$x \mathrel{R'} y \quad \Leftrightarrow \quad x < y.$$

Is $R'$ antisymmetric? Is $R'$ a partial order? Is $R'$ a total order? 7f

**Example 7.3.5.** Let $R$ denote the equality relation on a set $A$, i.e., for all $x, y \in A$,

$$x \mathrel{R} y \quad \Leftrightarrow \quad x = y.$$

Then $R$ is antisymmetric. It is a partial order, but not a total order unless $|A| \leqslant 1$.

**Example 7.3.6.** Fix $n \in \mathbb{Z}^+$. Let $R'$ denote the congruence-mod-$n$ relation on $\mathbb{Z}$, i.e., for all $x, y \in \mathbb{Z}$,

$$x \mathrel{R'} y \quad \Leftrightarrow \quad x \equiv y \pmod{n}.$$

Then $R'$ is not antisymmetric because $0 \mathrel{R'} n$ and $n \mathrel{R'} 0$ but $0 \neq n$.

**Example 7.3.7.** Let $R$ denote the divisibility relation on $\mathbb{Z}$, i.e., for all $x, y \in \mathbb{Z}$,

$$x \mathrel{R} y \quad \Leftrightarrow \quad x \mid y.$$

Is $R$ antisymmetric? Is $R$ a partial order? Is $R$ a total order? 7g

**Example 7.3.8.** Let $R'$ denote the divisibility relation on $\mathbb{Z}^+$, i.e., for all $x, y \in \mathbb{Z}^+$,

$$x\ R'\ y \quad \Leftrightarrow \quad x \mid y.$$

Is $R$ antisymmetric? Is $R$ a partial order? Is $R$ a total order? 7h

**Example 7.3.9.** Let $R$ denote the subset relation on a set $U$ of sets, i.e., for all $x, y \in U$,

$$x\ R\ y \quad \Leftrightarrow \quad x \subseteq y.$$

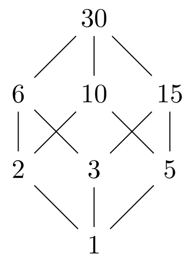
Then $R$ is antisymmetric. It is always a partial order, but it may not be a total order.

**Notation 7.3.10.** We often use $\preccurlyeq$ to denote a partial order. This symbol is often defined and redefined to mean different partial orders in different situations. We may read $\preccurlyeq$ as "curly less than or equal to" or simply "less than or equal to" if there is no risk of ambiguity. If $\preccurlyeq$ denotes a partial order, then we write $x \prec y$ for $x \preccurlyeq y \wedge x \neq y$.

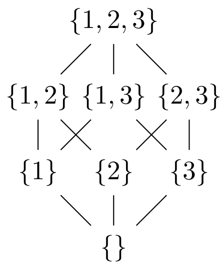
**Definition 7.3.11.** Let $\preccurlyeq$ be a partial order on a set $A$. A *Hasse diagram* of $\preccurlyeq$ satisfies the following condition for all $x, y \in A$:

> If $x \prec y$ and no $z \in A$ is such that $x \prec z \prec y$, then $x$ is placed below $y$ and there is a line joining $x$ to $y$, else no line joins $x$ to $y$.

**Example 7.3.12.** Consider $\{d \in \mathbb{Z}^+ : d \mid 30\}$ partially ordered by the divisibility relation $\mid$. A Hasse diagram is as follows:




**Example 7.3.13.** Consider $\mathcal{P}(\{1, 2, 3\})$ partially ordered by the inclusion relation $\subseteq$. A Hasse diagram is as follows:




**Example 7.3.14.** Consider $\{1, 2, 3, 4\}$ partially ordered by the non-strict less-than relation $\leqslant$. A Hasse diagram is as follows:

## 7.4 Linearization

**Definition 7.4.1.** Let $\preccurlyeq$ be a partial order on a set $A$, and $c \in A$.

(1) $c$ is a *minimal element* if no $x \in A$ is strictly $\preccurlyeq$-less than $c$, i.e.,

$$\forall x \in A \ \ (x \preccurlyeq c \Rightarrow c = x).$$

(2) $c$ is a *maximal element* if no $x \in A$ is strictly $\preccurlyeq$-bigger than $c$, i.e.,

$$\forall x \in A \ \ (c \preccurlyeq x \Rightarrow c = x).$$

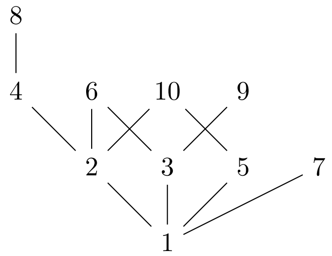
(3) $c$ is the *smallest element* (or the *minimum element*) if all $x \in A$ are $\preccurlyeq$-bigger than or equal to $c$, i.e.,

$$\forall x \in A \ \ (c \preccurlyeq x).$$

(4) $c$ is the *largest element* (or the *maximum element*) if all $x \in A$ are $\preccurlyeq$-less than or equal to $c$, i.e.,

$$\forall x \in A \ \ (x \preccurlyeq c).$$

**Example 7.4.2.** The divisibility relation $|$ on $\{1, 2, \ldots, 10\}$ is represented by the Hasse diagram




- The only minimal element is 1.
- The maximal elements are $6, 7, 8, 9, 10$.
- The smallest element is 1.
- There is no largest element.

**Example 7.4.3.** (1) $\mathbb{Q}^+$ under the non-strict less-than relation $\leqslant$ has neither a minimal element nor a maximal element.

(2) $\mathbb{Z}^+$ under the non-strict less-than relation $\leqslant$ has a smallest element but no maximal element.

**Proposition 7.4.4.** Consider a partial order $\preccurlyeq$ on a set $A$.

(1) A smallest element is minimal.

(2) There is at most one smallest element.

**Proof.** (1) 1. Let $c$ be a smallest element.
2. Take any $x \in A$ such that $x \preccurlyeq c$.
3. By smallestness, we know $c \preccurlyeq x$ too.
4. So $c = x$ by antisymmetry.

(2) 1. Let $c, c'$ be smallest elements.
2. Then $c \preccurlyeq c'$ and $c' \preccurlyeq c$ by the smallestness of $c$ and $c'$ respectively.
3. So $c = c'$ by antisymmetry. $\square$

**Exercise 7.4.5.** Show the statements analogous to Proposition 7.4.4 for largest and maximal elements. 7i

**Proposition 7.4.6.** With respect to any partial order $\preccurlyeq$ on a nonempty finite set $A$, one can find a minimal element.

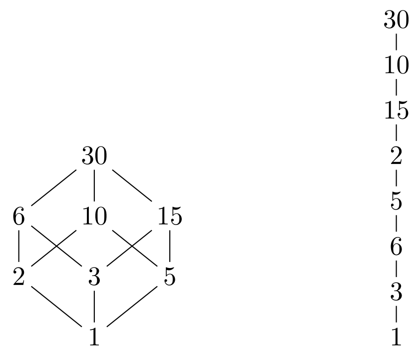
**Proof (optional material).** 1. Take any $c_0 \in A$. This is possible since $A \neq \varnothing$.
2. If $c_0$ is not minimal, then find $c_1 \in A$ such that $c_1 \prec c_0$.
3. Continue this process: if $c_n$ is not minimal, then find $c_{n+1} \in A$ such that $c_{n+1} \prec c_n$.
4. Note that $c_{n+1} \neq c_i$ for any $i \in \{0, 1, \ldots, n\}$ because if $i \in \{0, 1, \ldots, n\}$ such that $c_{n+1} = c_i$, then
    4.1. $c_n \prec c_{n-1} \prec \cdots \prec c_i = c_{n+1}$;
    4.2. so $c_n \preccurlyeq c_{n+1}$ by transitivity;
    4.3. so $c_n = c_{n+1}$ by antisymmetry as $c_{n+1} \prec c_n$;
    4.4. so we have a contradiction with $c_{n+1} \prec c_n$.
5. Since $A$ is finite, this process must end, say with $c_n$.
6. $c_n$ must be minimal for this process to end. □

**Exercise 7.4.7.** Convince yourself that the statement analogous to Proposition 7.4.6 is true for maximal elements. 7j

**Definition 7.4.8.** Let $A$ be a set and $\preccurlyeq$ be a partial order on $A$. A *linearization* of $\preccurlyeq$ is a total order $\preccurlyeq^*$ on $A$ such that

$$\forall x, y \in A \quad (x \preccurlyeq y \Rightarrow x \preccurlyeq^* y).$$

**Question 7.4.9.** Is the total order $\preccurlyeq^*$ represented by the right Hasse diagram a linearization of the partial order $\preccurlyeq$ represented by the left Hasse diagram? 7k




**Theorem 7.4.10.** Let $A$ be a set and $\preccurlyeq$ be a partial order on $A$. Then there exists a total order $\preccurlyeq^*$ on $A$ such that for all $x, y \in A$,

$$x \preccurlyeq y \quad \Rightarrow \quad x \preccurlyeq^* y.$$

**Algorithm 7.4.11** (Kahn's Algorithm (1962))**.** Input: a finite set $A$, a partial order $\preccurlyeq$ on $A$.

(1) Set $A_0 := A$ and $i := 0$.

(2) Repeat until $A_i = \varnothing$:

  (2.1) use Proposition 7.4.6 to find a minimal element $c_i$ of $A_i$ with respect to $\preccurlyeq$;
  (2.2) set $A_{i+1} := A_i \setminus \{c_i\}$;
  (2.3) set $i := i + 1$.

Output: a linearization $\preccurlyeq^*$ of $\preccurlyeq$ defined by setting, for all indices $i, j$,

$$c_i \preccurlyeq^* c_j \quad \Leftrightarrow \quad i \leqslant j.$$

**Note 7.4.12.** In step (2.1) of Kahn's Algorithm, there may be several minimal elements to choose from. Different choices give different linearizations.

**Example 7.4.13.** Consider $\{d \in \mathbb{Z}^+ : d \mid 30\}$ partially ordered by the divisibility relation $\mid$ as in Example 7.3.12.

- Set $A_0 := \{d \in \mathbb{Z}^+ : d \mid 30\}$.
- 1 is the only minimal element of $A_0$. Set $c_0 := 1$ and $A_1 := A_0 \setminus \{1\}$.
- $2, 3, 5$ are the minimal elements of $A_1$. Set $c_1 := 3$ and $A_2 := A_1 \setminus \{3\}$.
- $2, 5$ are the minimal elements of $A_2$. Set $c_2 := 2$ and $A_3 := A_2 \setminus \{2\}$.
- $5, 6$ are the minimal elements of $A_3$. Set $c_3 := 6$ and $A_4 := A_3 \setminus \{6\}$.
- 5 is the only minimal element of $A_4$. Set $c_4 := 5$ and $A_5 := A_4 \setminus \{5\}$.
- $10, 15$ are the minimal elements of $A_5$. Set $c_5 := 15$ and $A_6 := A_5 \setminus \{15\}$.
- 10 is the only minimal element of $A_6$. Set $c_6 := 10$ and $A_7 := A_6 \setminus \{10\}$.
- 30 is the only (minimal) element of $A_7$. Set $c_7 := 30$ and $A_8 := A_7 \setminus \{30\}$.
- $A_8 = \varnothing$ and so we stop.

A linearization is given by $1 \preccurlyeq^* 3 \preccurlyeq^* 2 \preccurlyeq^* 6 \preccurlyeq^* 5 \preccurlyeq^* 15 \preccurlyeq^* 10 \preccurlyeq^* 30$.

**Why Kahn's Algorithm stops.** The input set $A$ is finite. Each time the repeat-until loop is run, one element is taken out of $A$. So this loop is run exactly $|A|$ times. Then the set of remaining elements is empty, and the stopping condition is satisfied.

**Proof that Kahn's Algorithm is correct (optional material).** 1. Input a finite set $A$ and a partial order $\preccurlyeq$ on $A$ to Kahn's Algorithm.
2. Suppose the run produces $A_0, A_1, \ldots, A_n, c_0, c_1, \ldots, c_{n-1}$ and $\preccurlyeq^*$.
3. Note $A = \{c_0, c_1, \ldots, c_{n-1}\}$, because the removal of $c_0, c_1, \ldots, c_{n-1}$ from $A$ makes the set empty following Kahn's Algorithm.
4. Note also that $\preccurlyeq^*$ is a total order on $A$ because it is by definition only a renaming of the total order $\leqslant$ on $\{0, 1, \ldots, n-1\}$.
5. 5.1. Take any $x, y \in A$ such that $x \preccurlyeq y$.
   5.2. Use line 2 to find $j \in \{0, 1, \ldots, n-1\}$ such that $y = c_j$.
   5.3. 5.3.1. Case 1: suppose $x = c_j$.
        5.3.2. Then $x = c_j \preccurlyeq^* c_j$ by the definition of $\preccurlyeq^*$.
   5.4. 5.4.1. Then $x \notin A_j$ as $c_j$ is minimal in $A_j$.
        5.4.2. So $x \in A \setminus A_j$, where $A \setminus A_j = \{c_0, c_1, \ldots, c_{j-1}\}$ by the choices of $A_0, A_1, \ldots, A_j$ and $c_0, c_1, \ldots, c_{j-1}$ in Kahn's Algorithm.
        5.4.3. Let $i \in \{0, 1, \ldots, j-1\}$ such that $x = c_i$.
        5.4.4. Then $x = c_i \preccurlyeq^* c_j = y$ by the definition of $\preccurlyeq^*$, as $i \leqslant j - 1 < j$.
6. Hence $\preccurlyeq^*$ is a linearization of $\preccurlyeq$. □

Here are the arrow diagrams of 8 of the binary relations on the 3-element set $A = \{a, b, c\}$. Set inclusion $\subseteq$ is a partial order on the set consisting of these 8 relations, the Hasse diagram of which is also shown.

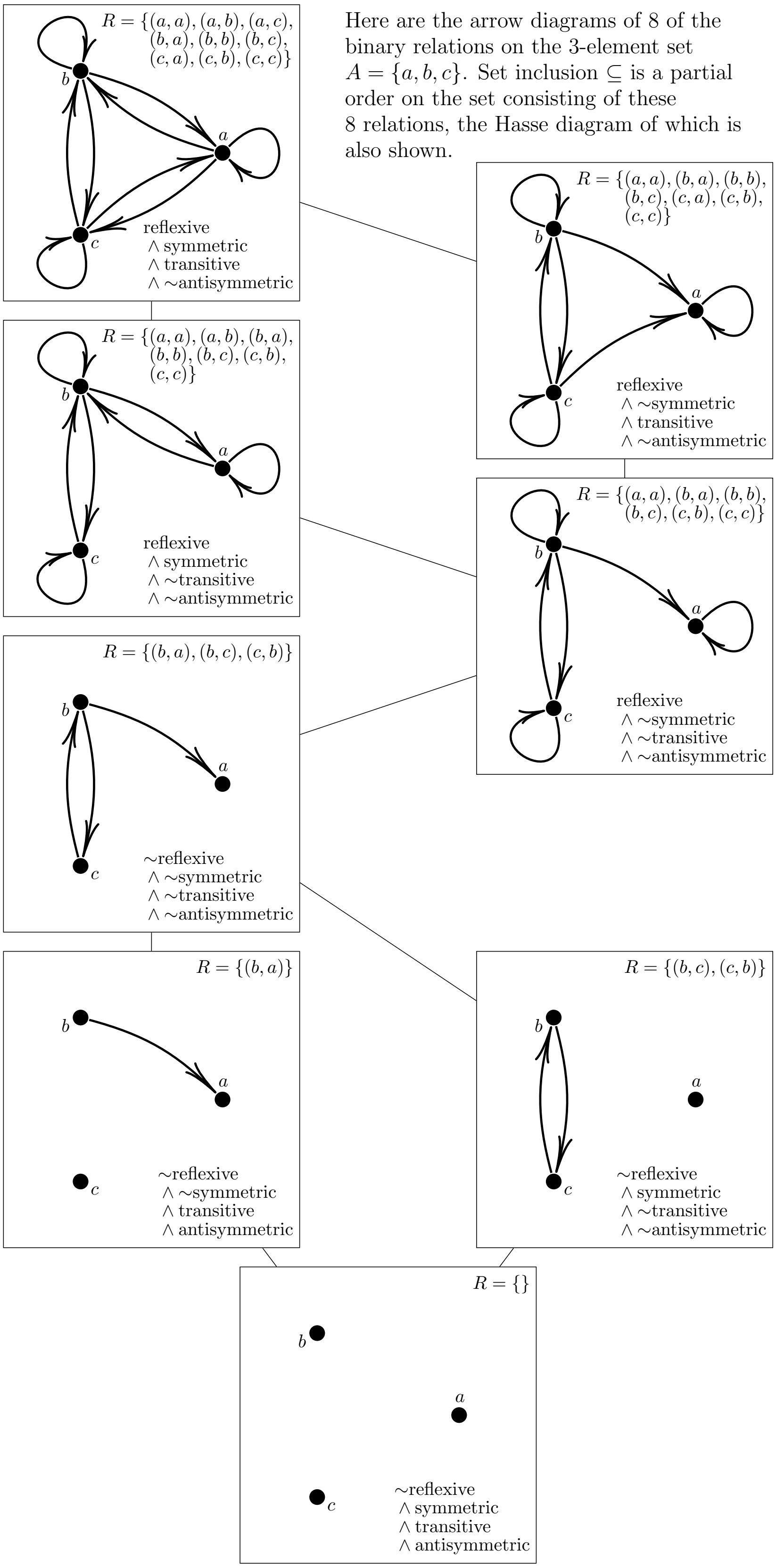



Figure 7.1: A partial order on a set of relations