

A Relations

In mathematical terms a relation on a set S is simply a subset $R \subseteq S \times S$. This definition is deceptively simple, but captures the real-world nature of relations remarkably. Of course, if one wants interesting mathematics one must restrict to relations with certain properties. The two most important types of relations in mathematics are equivalence relations and order relations.

A.1 Basic definitions and properties

Definition A.1.1 A relation R on a set S is a subset $R \subseteq S \times S$. We will write xRy to mean $(x, y) \in R$.

Definition A.1.2 A relation R on S is *reflexive* if xRx for every $x \in S$, *symmetric* if $xRy \Rightarrow yRx$ for every $x, y \in S$, *antisymmetric* if $xRy \wedge yRx \Rightarrow x = y$ for every $x, y \in S$ and *transitive* if $xRy \wedge yRz \Rightarrow xRz$ for every $x, y, z \in S$.

- (i) R is called an *equivalence relation* if it is reflexive, symmetric and transitive.
- (ii) R is called a *partial ordering* if it is reflexive, antisymmetric and transitive.

Example A.1.3 Recall the relation \leq on \mathbb{Z} from Chapter 1 given by $x \leq y \iff y - x \in \mathbb{N}$. Since $0 \in \mathbb{N}$, \leq is reflexive. It is antisymmetric since if $x \in \mathbb{Z}$ and $x \in \mathbb{N}$, $-x \in \mathbb{N}$ then $x = 0$. It is transitive, as $x, y \in \mathbb{N}$ implies $x + y \in \mathbb{N}$. So \leq is a partial ordering on \mathbb{Z} .

Example A.1.4 Let S be a set.

- (i) The relation $R = S \times S$ is reflexive, symmetric and transitive, but it is not antisymmetric if S contains more than one element.
- (ii) If the two relations $R_1, R_2 \subseteq S \times S$ both have one of the properties of Definition A.1.2 then the intersection $R_1 \cap R_2 \subseteq S \times S$ has the same property.

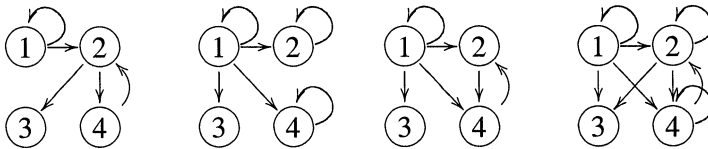
Example A.1.5 Let $I \subseteq R$ be an ideal in a commutative ring R . Then we define the relation (congruence modulo an ideal)

$$x \equiv y \pmod{I} \iff x - y \in I.$$

This relation is reflexive since $0 \in I$, symmetric since $x \in I \implies -x \in I$ and transitive since $x, y \in I \implies x + y \in I$. In short, congruence modulo I is an equivalence relation because I is a subgroup of R . As a special case we may take $I = d\mathbb{Z}$ in \mathbb{Z} . Then $x \equiv y \pmod{I}$ if and only if $x \equiv y \pmod{d}$. So congruence modulo an integer is an equivalence relation.

Example A.1.6 Suppose that R_1 and R_2 are relations on a set M . Then $R_1 \circ R_2$ is the relation on M given by $\{(x, z) \in M \times M \mid (x, y) \in R_1, (y, z) \in R_2 \text{ for some } y \in M\}$. If R is a relation on M , we define R^n iteratively by $R^n = R \circ R^{n-1}$, where $n \in \mathbb{N}$ and $R^0 = M \times M$.

Let $S = \{1, 2, 3, 4\}$ and $R = \{(1, 2), (2, 4), (4, 2), (1, 1), (2, 3)\}$. Then R can be shown diagrammatically, the nodes correspond to the elements of S and the arrows to elements of the relation R . Below you will find diagrams of the relations R, R^2, R^3 and $R \cup R^2 \cup R^3$:



Notice that $R \cup R^2 \cup R^3$ is a transitive relation but R is not.

A.2 Equivalence relations

Let \sim be an equivalence relation on a set S . Given $x \in S$, we let

$$[x] = \{s \in S \mid s \sim x\} \subseteq S.$$

This subset is called the *equivalence class* containing x and x is called a *representative* for $[x]$. The set of equivalence classes

$$\{[x] \mid x \in S\}$$

is denoted S/\sim .

Remark A.2.1 When dealing with equivalence relations, the symbol \sim is often used instead of R (xRy is denoted by $x \sim y$).

Example A.2.2 Let I be an ideal of a commutative ring R and let \equiv denote equivalence modulo the ideal I (see Example A.1.5). Then R/\equiv equals R/I .

You may have noticed that $[x]$ is defined as *the* equivalence class containing x . How can we be sure that there is just one equivalence class containing x ? This is in fact a consequence of the following lemma.

Lemma A.2.3 Let \sim be an equivalence relation on S and $x, y \in S$. Then $[x] = [y]$ if and only if $x \sim y$.

Proof. Suppose that $[x] = [y]$. Then $x \in [x]$, since \sim is reflexive. Therefore $x \in [y]$ and $x \sim y$. Let us prove that $[x] \subseteq [y]$ if $x \sim y$. Let $s \in [x]$. Then $s \sim x$ and since $x \sim y$ we get, by the transitivity of \sim , that $s \sim y$. Thus $s \in [y]$. Using that $x \sim y \implies y \sim x$, the same proof can be repeated to show that $[y] \subseteq [x]$ if $x \sim y$. \square

Corollary A.2.4 In the notation of Lemma A.2.3, $[x] \cap [y] = \emptyset$ if $[x] \neq [y]$.

Proof. Suppose that $z \in [x] \cap [y] \neq \emptyset$. Then $z \sim x$ and $z \sim y$. By Lemma A.2.3 we have $[z] = [x]$ and $[z] = [y]$. Thus $[x] = [y]$. \square

Definition A.2.5 A partition of a set S is a collection $(S_i)_{i \in I}$ of subsets of S such that $\cup_{i \in I} S_i = S$ and $S_i \cap S_j = \emptyset$ if $i \neq j$.

The key property of equivalence relations is contained in the theorem below.

Theorem A.2.6 Let S be a set with an equivalence relation \sim . Then the set of equivalence classes

$$S/\sim = \{[x] \mid x \in S\}$$

is a partition of S . However, if $(S_i)_{i \in I}$ is a partition of S then we get an equivalence relation \sim on S such that $S/\sim = (S_i)_{i \in I}$.

Proof. We have already seen that equivalence classes are disjoint (Corollary A.2.4). We need to show that every element $x \in S$ is contained in an equivalence class. But this follows from the fact that \sim is reflexive ($x \in [x]$). Suppose that $(S_i)_{i \in I}$ is a partition of S . We define $x \sim y \iff x, y \in S_i$ for some $i \in I$. Reflexivity follows from $\cup_{i \in I} S_i = S$. Symmetry is clear. Transitivity is implied by $S_i \cap S_j = \emptyset$ if $i \neq j$. If $x \in S_i$ then $S_i = [x]$. \square

Definition A.2.7 Let \sim be an equivalence relation on a set S . Then the map

$$\pi : S \rightarrow S/\sim$$

given by $\pi(s) = [s]$ is called the canonical map.

Proposition A.2.8 *Let $f : S \rightarrow M$ be a map from a set S with an equivalence relation \sim to a set M . If $x \sim y \iff f(x) = f(y)$ then there is an injective map*

$$\tilde{f} : S/\sim \rightarrow M$$

such that $f = \tilde{f} \circ \pi$, where π is the canonical map.

Proof. Let $\tilde{f}([x]) = f(x)$. This is a definition that depends on the choice of representative $x \in [x]$. But if $[y] = [x]$ then $y \sim x$ and $f(y) = f(x)$, so our map \tilde{f} is actually well defined. It satisfies $f = \tilde{f} \circ \pi$ and is injective by construction. \square

A.2.1 Construction of the integers \mathbb{Z}

Even though it is somewhat formal, let us see how the concept of equivalence relations enables us to construct the integers \mathbb{Z} , given the natural numbers \mathbb{N} with addition and multiplication. We look at pairs $(x, y) \in \mathbb{N} \times \mathbb{N}$. The pair (x, y) will be our candidate for the integer $x - y$. We introduce the relation \sim given by

$$(x, y) \sim (x_1, y_1) \iff x + y_1 = y + x_1$$

on $\mathbb{N} \times \mathbb{N}$. You can easily check that this is an equivalence relation. The inspiration for \sim is of course that $x - y = x_1 - y_1 \iff x + y_1 = y + x_1$. We define addition and multiplication as

$$\begin{aligned}(x, y) + (x_1, y_1) &= (x + x_1, y + y_1), \\ (x, y)(x_1, y_1) &= (xx_1 + yy_1, xy_1 + yx_1).\end{aligned}$$

Now we may construct the integers as the equivalence classes

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim.$$

What about addition and multiplication? Is it safe to define

$$[(x, y)] + [(x_1, y_1)] = [(x + x_1, y + y_1)]?$$

Already at this point it is extremely important that you notice that a definition such as this is a problem. We use elements (x, y) in the equivalence classes $[(x, y)]$ to define $+$. What if we picked another element $(x', y') \in [(x, y)]$? Would the addition still give the same equivalence class?

The answer is yes. Here is a proof, which is typical of the procedure you must go through to ensure that an operation on equivalence classes is well defined. Suppose that $[(x, y)] = [(x', y')]$ and $[(x_1, y_1)] = [(x'_1, y'_1)]$. We must prove that $[(x + x_1, y + y_1)] = [(x' + x'_1, y' + y'_1)]$. Using the definition of \sim

we see that $x + x_1 + y' + y'_1 = x + y' + x_1 + y'_1 = y + x' + y_1 + x'_1$, showing that $(x + x_1, y + y_1) \sim (x' + x'_1, y' + y'_1)$, so that

$$[(x + x_1, y + y_1)] = [(x' + x'_1, y' + y'_1)].$$

The same proof (with a twist) works for multiplication. Notice that $[(m, n)] = [(m - n, 0)]$ if $m \geq n$ and that $[(m, n)] = [(0, n - m)]$ if $m \leq n$. Putting $-m = [(0, m)]$ for $m \in \mathbb{N}$ and identifying $n \in \mathbb{N}$ with $[(n, 0)]$ we have constructed the integers.

A.2.2 Construction of the rational numbers \mathbb{Q}

Now that we know the integers $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ and how to add and multiply them, how do we use equivalence relations to give a precise definition of the rational numbers \mathbb{Q} ? A fraction is given by a numerator $a \in \mathbb{Z}$ and a denominator $b \in \mathbb{Z} \setminus \{0\}$, but then again this is not totally precise; two fractions, such as $\frac{1}{2}$ and $\frac{2}{4}$, may be the same even though they do not have the same numerators and denominators.

Suppose that we impose the relation $(a, s) \sim (b, t) \Leftrightarrow at = bs$ on the set $M = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$. This is an equivalence relation and it mimics the everyday rule that you do not change a fraction if you multiply the numerator and denominator by the same non-zero number. Now define the subset

$$\frac{a}{s} = [(a, s)] = \{(b, t) \in M \mid (b, t) \sim (a, s)\} \subseteq M.$$

This subset is supposed to be our “fraction” a/s – of course no sane human being views a fraction as a huge set in this way, but read on! We have sorted out the infinite amount of identical fractions and made them into one object, just by naively putting things together that are considered the same. Now we finally define the rational numbers

$$\mathbb{Q} = M/\sim = \left\{ \frac{a}{b} \mid (a, b) \in M \right\}.$$

Does it make sense to add and multiply our fractions? Suppose that we simply define

$$\frac{a}{s} \frac{b}{t} = \frac{ab}{st}, \quad \frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}.$$

As in the construction of \mathbb{Z} given \mathbb{N} one needs to check that the multiplication and addition is independent of the choice of representatives. This is left as an exercise.

A.3 Partial orderings

Example A.3.1 Here are some more examples of well known partial orderings.

- (i) Let S be a set. Then inclusion \subseteq is a partial ordering on the set of subsets of S .
- (ii) Let R denote the relation on \mathbb{N} given by $xRy \iff x \mid y$ for $x, y \in \mathbb{N}$. Then R is a partial ordering. But R is not a partial ordering considered as a relation on \mathbb{Z} (why?).

An element $s \in S$ in a set with a partial ordering \leq is said to be *minimal* if

$$x \leq s \implies x = s$$

for every $x \in S$. An element $t \in S$ is called a *first* element if

$$t \leq x$$

for every $x \in S$. Because of antisymmetry a first element has to be unique. A first element is a minimal element. What about the other way around? The answer is no: there is no reason why (s, x) should belong to the subset of $S \times S$ given by \leq . Here are some examples with several minimal elements.

Example A.3.2 Let

$$S = \{\{0\}, \{1\}, \{0, 1\}\}$$

be a set of subsets of $\{0, 1\}$. Then the inclusion of sets \subseteq is a partial ordering on S and $\{0\}$ and $\{1\}$ are two different minimal elements of S .

Example A.3.3 Let $S = \mathbb{N} \setminus \{1\}$. The divisibility relation $xRy \iff x \mid y$ is a partial ordering on S . The fact that there are infinitely many primes in \mathbb{N} tells us that R has infinitely many minimal elements.

Definition A.3.4 A partial ordering \leq is called a *total ordering* if $x \leq y$ or $y \leq x$ for every $x, y \in S$.

An even finer condition is given by

Definition A.3.5 A partial ordering \leq on a set S is called a *well ordering* if every non-empty subset $M \subseteq S$ has a first element $m \in M$.

Definition A.3.6 Let \leq be a total ordering on a finite set M . Then we let $\max_{\leq} M$ denote the maximal element in M . Thus $x = \max_{\leq}(M)$ if and only if $x \in M$ and $x \geq y$ for every $y \in M$. Similarly we let $\min_{\leq}(M)$ denote the minimal element. When the ordering is implicit we drop the subscript and write \max and \min instead of \max_{\leq} and \min_{\leq} .

Example A.3.7 The partial ordering \leq on \mathbb{Z} is not a well ordering, since \mathbb{Z} does not have a first element. Every total ordering on a finite set is a well ordering. One of the surprising results of set theory is that there exists a well ordering on every set (can you construct one on \mathbb{Z} ? \mathbb{R} ?).

Lemma A.3.8 *Let S be a set with a well ordering \leq and $F = \{s_1, s_2, \dots\}$ a subset such that $s_1 \geq s_2 \geq s_3 \geq \dots$. Then F is finite.*

Proof. Let s denote the smallest element of F . Since $s \in F$ this means that $s = s_N$ for some $N \in \mathbb{N}$. Since $s_N \geq s_i$ for $i > N$ this implies that $s_N = s_i$ for $i > N$. Therefore F is finite. \square