Relations

A binary relation on a set A is a subset $R \subseteq A \times A$, where elements (a, b) are written as $a \sim b$.

Example: $A = \mathbb{Z}$ and $R = \{a \sim b \mid a < b\}$.
In words:

Let $\sim$ be the relation on $\mathbb{Z}$ given by $a \sim b$ if $a < b$.

(Note that we use language like in definitions, where "if" actually means "if and only if".)

Example: $A = \mathbb{R}$ and $R = \{a \sim b \mid a = b\}$.
In words:

Let $\sim$ be the relation on $\mathbb{R}$ given by $a \sim b$ if $a = b$.

Example: $A = \mathbb{Z}$ and $R = \{a \sim b \mid a \equiv b \pmod 3\}$.
In words:

Let $\sim$ be the relation on $\mathbb{Z}$ given by $a \sim b$ if $a \equiv b \pmod 3$.

More examples of (binary) relations:

1. For A a number system, let $a \sim b$ if $a = b$. R, S, T
2. For A a number system, let $a \sim b$ if $a < b$. not R, not S, T
3. For $A = \mathbb{R}$, let $a \sim b$ if $ab = 0$. not R, S, not T
4. For A a set of people, let $a \sim b$ if a is a (full) sibling of b. not R, S, T
5. For A a set of people, let $a \sim b$ if a and b speak a common language. R, S, not T

A binary relation on a set A is...

(R) reflexive if $a \sim a$ for all $a \in A$;

(S) symmetric if $a \sim b$ implies $b \sim a$;

(T) transitive if $a \sim b$ and $b \sim c$ implies $a \sim c$, i.e.

$$(a \sim b \wedge b \sim c) \Rightarrow a \sim c$$

An equivalence relation on a set A is a binary relation that is reflexive, symmetric, *and* transitive. (Only #1)

Fix $n \in \mathbb{Z}_{>0}$ and define the relation on $\mathbb{Z}$ given by

$$\text{“}a \sim b \quad \text{if } a \equiv b \pmod{n}.\text{”}$$

Is $\sim$ is an equivalence relation?

Check: we have $a \equiv b \pmod{n}$ if and only if $a - b = kn$ for some $k \in \mathbb{Z}$.

reflexivity: $a - a = 0 = 0 \cdot n$ ✓

symmetry: If $a - b = kn$, then $b - a = -kn = (-k)n$. ✓

transitivity: If $a - b = kn$ and $b - c = \ell n$, then

$$a - c = (a - b) + (b - c) = kn + \ell n = (k + \ell)n. ✓$$

Yes! This is an equivalence relation!

Let A be a set. Consider the relation on $\mathcal{P}(A)$ by

$$S \sim T \qquad \text{if} \qquad S \subseteq T$$

Is $\sim$ is an equivalence relation?

Check: This is reflexive and transitive, but not symmetric.
So no, it is not an equivalence relation.

Is

$$S \sim T \qquad \text{if} \qquad S \subseteq T \text{ or } S \subseteq T$$

an equivalence relation on $\mathcal{P}(A)$?

Check: This is reflexive and symmetric, but not transitive.
So still no, it is not an equivalence relation.

Is

$$S \sim T \qquad \text{if} \qquad |S| = |T|$$

an equivalence relation on $\mathcal{P}(A)$?

Read: Why reflexivity doesn't follow from symmetry and transitivity.

Let $\sim$ be an equivalence relation on a set A, and let $a \in A$. The set of all elements $b \in A$ such that $a \sim b$ is called the equivalence class of a, denoted by $[a]$.

Example: Consider the equivalence relation on $A = \{a, b, c\}$ given by

$$a \sim a, \quad b \sim b, \quad c \sim c, \quad a \sim c, \quad \text{and} \quad c \sim a.$$

Then

$$[a] = \{a, c\} = [c], \quad \text{and}$$
$$[b] = \{b\}$$

are the two equivalence classes in A (with respect to this relation).

(We say there are two, *not three*, since "the equivalence classes" refers to the sets themselves, not to the elements that generate them.)

Let $\sim$ be an equivalence relation on a set A, and let $a \in A$. The set of all elements $b \in A$ such that $a \sim b$ is called the equivalence class of a, denoted by $[a]$.

Example: We showed that

$$\text{“}a \sim b \quad \text{if } a \equiv b \pmod 5\text{”}$$

is an equivalence relation on $\mathbb{Z}$. Then

$$[0] = \{5n \mid n \in \mathbb{Z}\} = 5\mathbb{Z} \qquad [1] = \{5n + 1 \mid n \in \mathbb{Z}\} = 5\mathbb{Z} + 1$$
$$[2] = \{5n + 2 \mid n \in \mathbb{Z}\} = 5\mathbb{Z} + 2 \qquad [3] = \{5n + 3 \mid n \in \mathbb{Z}\} = 5\mathbb{Z} + 3$$
$$[4] = \{5n + 4 \mid n \in \mathbb{Z}\} = 5\mathbb{Z} + 4$$
$$[5] = \{5n + 5 \mid n \in \mathbb{Z}\} = \{5m \mid m \in \mathbb{Z}\} = [0] = [-5] = [10] = \cdots$$
$$[6] = \{5n + 6 \mid n \in \mathbb{Z}\} = \{5m + 1 \mid m \in \mathbb{Z}\} = [1] = [-4] = [11] = \cdots$$
$$\vdots$$

In general, if $x \in [y]$, that means $y \sim x$.
So $x \sim y$. So $y \in [x]$.
Claim: $x \in [y]$ if and only if $[x] = [y]$.

We call any element a of a class C representative of C (since we can write $C = [a]$ for any $a \in C$).

Theorem. The equivalence classes of A partition A into subsets, meaning

1. the equivalence classes are subsets of A:
$$[a] \subseteq A \text{ for all } a \in A;$$
2. any two equivalence classes are either equal or disjoint:
$$\text{for all } a, b \in A, \text{ either } [a] = [b] \text{ or } [a] \cap [b] = \varnothing; \text{ and}$$
3. the union of all the equivalence classes is all of A:
$$A = \bigcup_{a \in A} [a].$$

We say that A is the disjoint union of equivalency classes, written
$$A = \bigsqcup_{a \in A} [a], \qquad \text{LaTeX: \textbackslash bigsqcup, \textbackslash sqcup}$$

For example, in our last example, there are exactly 5 equivalence classes: $[0]$, $[1]$, $[2]$, $[3]$, and $[4]$. Any other seemingly different class is actually one of these (for example, $[5] = [0]$). And
$$[0] \cup [1] \cup [2] \cup [3] \cup [4] = \mathbb{Z}.$$
So $\boxed{\mathbb{Z} = [0] \sqcup [1] \sqcup [2] \sqcup [3] \sqcup [4]}$.

Ok, so what **are** numbers, anyway?

Recall from the homework, the Zermelo-Fraenkel axioms of set theory, which tells us how to compare sets, put sets in other sets, and to take unions, intersection, and power sets of sets. ✓

Set theoretic definition of the natural numbers. ($\mathbb{Z}_{\geqslant 0}$)
Let $0 = \varnothing$.
Given n, define the successor to n as $S(n) = n \cup \{n\}$.
(By "successor to n" we basically mean $n + 1$.)
Let $\mathbb{N}$ be the set of all sets generated by 0 and S.
For example,
$$\begin{aligned}
1 &= 0 \cup \{0\} = \varnothing \cup \{\varnothing\} = \{\varnothing\}, \\
2 &= 1 \cup \{1\} = \{\varnothing\} \cup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\}, \\
3 &= 2 \cup \{2\} = \{\varnothing, \{\varnothing\}\} \cup \{\{\varnothing, \{\varnothing\}\}\} \\
&= \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\},
\end{aligned}$$
and so on. (Note that we identified n with $|n|$.) Compute 4.
Think: Given $n, m \in \mathbb{N}$, are $n \cup m$ and/or $n \cap m$ elements of $\mathbb{N}$? If so, what elements are they?

Set theoretic definition of the natural numbers. ($\mathbb{Z}_{\geqslant 0}$)

Let $0 = \varnothing$.
Given n, define the successor to n as $S(n) = n \cup \{n\}$. Let $\mathbb{N}$ be the set of all sets generated by 0 and S.
For example,

$$\begin{aligned}&1 = \{\varnothing\}, \quad 2 = \{\varnothing, \{\varnothing\}\}, \quad 3 = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\},\\ &4 = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}\},\end{aligned}$$

and so on. (Note that we identified n with $|n|$.)

Addition: Define $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by, for all $a, b \in \mathbb{N}$,

1. $a + 0 = a$; and
2. $a + S(b) = S(a + b)$.

For example,

$$\begin{aligned}a + 1 = a + S(0) = S(a + 0) = S(a);\\ a + 2 = a + S(1) = S(a + 1) = S(S(a)).\end{aligned}$$

Check that $a + 3 = S(S(S(a))) = S^3(a)$. Think: $a + b = S^b(a)$.

Given n, define the successor to n as $S(n) = n \cup \{n\}$. Let $\mathbb{N}$ be the set of all sets generated by 0 and S.
For example,

$$\begin{aligned}&1 = \{\varnothing\}, \quad 2 = \{\varnothing, \{\varnothing\}\}, \quad 3 = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\},\\ &4 = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}\},\end{aligned}$$

and so on. (Note that we identified n with $|n|$.)

Addition: Define $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by, for all $a, b \in \mathbb{N}$,

1. $a + 0 = a$; and 2. $a + S(b) = S(a + b)$.

Think: $a + b = S^b(a) = S^{a+b}(0)$.

Multiplication: Define $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by, for all $a, b \in \mathbb{N}$,

1. $n \cdot 0 = 0$; and 2. $a \cdot S(b) = (a \cdot b) + a$.

For example,

$$\begin{aligned}a \cdot 1 = a \cdot S(0) = a \cdot 0 + a = 0 + a = a;\\ a \cdot 2 = a \cdot S(1) = a \cdot 1 + a = a + a.\end{aligned}$$

Check that $a + 3 = a + a + a$. Think: $a \cdot b = S^{ab}(0)$.

Addition: Define $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by, for all $a, b \in \mathbb{N}$,

1. $a + 0 = a$; and 2. $a + S(b) = S(a + b)$.

Think: $a + b = S^b(a) = S^{a+b}(0)$.

Multiplication: Define $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by, for all $a, b \in \mathbb{N}$,

1. $n \cdot 0 = 0$; and 2. $a \cdot S(b) = (a \cdot b) + a$.

Think: $a \cdot b = S^{ab}(0)$.

Properties:

1. Addition is commutative, i.e. $a + b = b + a$ for all $a, b \in \mathbb{N}$.
2. Addition is associative, i.e. $a + (b + c) = (a + b) + c$ for all $a, b, c \in \mathbb{N}$.
3. Multiplication is commutative, i.e. $a \cdot b = b \cdot a$ for all $a, b \in \mathbb{N}$.
4. Multiplication is associative, i.e. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in \mathbb{N}$.
5. Multiplication is distributive across addition, i.e. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in \mathbb{N}$.

(These all follow from the definitions, but we'll skip proofs for the sake of time.)

Peano axioms

The natural numbers $\mathbb{N}$ are defined by the following axioms.

1. We have $0 \in \mathbb{N}$. (technically, $0 = \varnothing$)
2. There exists an a successor function $S : \mathbb{N} \to \mathbb{N}$ (namely, if $n \in \mathbb{Z}$, then $S(n) \in \mathbb{N}$) satisfying
   (i) $0 \notin S(\mathbb{N})$;
   (ii) S is injective (if $S(n) = S(m)$, then $n = m$); and
   (iii) if $X \subseteq \mathbb{N}$ satisfies $n_0 \in X$ and $S(X) \subseteq X$, we have $X = \mathbb{N}$.

Note:

(a) We have not *assumed* that 0 is the only element that is no one's successor (but it follows, in part from 1(iii)).

(b) By changing 0 out for something else (like 1), or changing $S(n)$ to something else (like $n - 1$), we can generate other sets that are basically the natural numbers all over again. This is why we're not fussy about whether $\mathbb{N}$ is $\mathbb{Z}_{\geqslant 0}$ or $\mathbb{Z}_{>0}$.

(c) The last axiom (1(iii)) is the basis of proof by induction.

The natural numbers $\mathbb{N}$ are defined by the following axioms.

1. We have $0 \in \mathbb{N}$.
2. There exists an a successor function $S : \mathbb{N} \to \mathbb{N}$ (namely, if $n \in \mathbb{Z}$, then $S(n) \in \mathbb{N}$) satisfying
   (i) $0 \notin S(\mathbb{N})$;
   (ii) S is injective (if $S(n) = S(m)$, then $n = m$); and
   (iii) if $X \subseteq \mathbb{N}$ satisfies $n_0 \in X$ and $S(X) \subseteq X$, we have $X = \mathbb{N}$.

Order on $\mathbb{N}$.

For $a, b \in \mathbb{N}$, we say $a \leqslant b$ if $b = S(S(\cdots S(a)\cdots))$.

Properties:

(i) For all $a, b \in \mathbb{N}$, we have $a \leqslant b$ or $b \leqslant a$.

(ii) If $a \leqslant b$ and $b \leqslant a$, then $a = b$.

(iii) If $a \leqslant b$ and $b \leqslant c$, then $a \leqslant c$.

(iv) If $a \leqslant b$ then $a + c \leqslant b + c$.

(v) If $a \leqslant b$ then $ac \leqslant bc$.

(These all follow from the axioms, but we'll skip proofs for the sake of time.)

Integers

Now that we have $\mathbb{N}$, we can define $\mathbb{Z}$ by formally letting

$$-\mathbb{N} = \{-n \mid n \in \mathbb{N}\}, \quad \text{where } -0 = 0;$$

and $\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$.

Extend $S : \mathbb{Z} \to \mathbb{Z}$ by defining $S(-a)$ for any $-a \in -\mathbb{N} - \{0\}$ as

$$S(-a) = -b, \quad \text{where } S(b) = a.$$

We can define the predecessor function $P : \mathbb{Z} \to \mathbb{Z}$ by $P(x) = y$ whenever $S(y) = x$. Letting $-(-x) = x$, this says that

$$S(x) = y \quad \text{if and only if} \quad P(y) = x.$$

We can also extend our definitions of $+$ and $\cdot$ to $\mathbb{Z}$.

Properties:

1. Addition and multiplication still satisfy commutativity, associativity, and distributivity.
2. We still have $a + 0 = a$ (additive identity) and $a \cdot 1 = a$ (multiplicative identity) for all $a \in \mathbb{Z}$.
3. We also have that $a + (-a) = 0$ (prove). (additive inverses)

We call any number system that has an addition and multiplication that satisfy all these properties a ring (modern algebra).

Integers

Now that we have $\mathbb{N}$, we can define $\mathbb{Z}$ by formally letting

$$-\mathbb{N} = \{-n \mid n \in \mathbb{N}\}, \quad \text{where } -0 = 0;$$

and $\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$. Extend $S : \mathbb{Z} \to \mathbb{Z}$ by defining $S(-a)$ for any $-a \in -\mathbb{N} - \{0\}$ as

$$S(-a) = -b, \quad \text{where } S(b) = a.$$

We can define the predecessor function $P : \mathbb{Z} \to \mathbb{Z}$ by $P(x) = y$ whenever $S(y) = x$. Letting $-(-x) = x$, this says that

$$S(x) = y \quad \text{if and only if} \quad P(y) = x.$$

We can also extend our definition of order to $\mathbb{Z}$. The only modification is:

(i) For all $a, b \in \mathbb{N}$, we have $a \leqslant b$ or $b \leqslant a$.

(ii) If $a \leqslant b$ and $b \leqslant a$, then $a = b$.

(iii) If $a \leqslant b$ and $b \leqslant c$, then $a \leqslant c$.

(iv) If $a \leqslant b$ then $a + c \leqslant b + c$.

(v) If $a \leqslant b$ and $c \in \mathbb{N}$, then $ac \leqslant bc$.

These properties make $\mathbb{Z}$ an ordered ring.

Rational numbers

Let

$$Q = \mathbb{Z} \times (\mathbb{Z} - \{0\}),$$

and define an equivalence relation on Q by

$$(a, b) \sim (x \cdot a, x \cdot b) \quad \text{for all} \quad x \in \mathbb{Z} - \{0\}.$$

Under this equivalence relation, write

$$\frac{a}{b} = [(a, b)].$$

Then rational numbers are

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

(Note that we get lazy, and write $\frac{a}{1} = a$.)

Define $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ and $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ by

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d} \qquad \text{and} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

Let $Q = \mathbb{Z} \times (\mathbb{Z} - \{0\})$ and define an equivalence relation on Q by

$$(a, b) \sim (x \cdot a, x \cdot b) \quad \text{for all} \quad x \in \mathbb{Z} - \{0\}.$$

Under this equivalence relation, write $\frac{a}{b} = [(a, b)]$ (writing $\frac{a}{1} = a$). Then rational numbers are

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

Define $+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ and $\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ by

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + b \cdot c}{b \cdot d} \qquad \text{and} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}.$$

Again...

1. Addition and multiplication still satisfy commutativity, associativity, and distributivity.
2. We still have $x + 0 = x$ (additive identity) and $x \cdot 1 = x$ (multiplicative identity) for all $x \in \mathbb{Q}$.
3. We also have that $x + (-x) = 0$. (additive inverses)

So $\mathbb{Q}$ is also a ring. In addition, for all $a/b \in \mathbb{Q}$,

$$\frac{a}{b} \cdot \frac{b}{a} = 1 \qquad \text{(multiplicative inverses)}.$$

This makes $\mathbb{Q}$ a field (again, modern algebra).

Order on $\mathbb{Q}$

Define $-\frac{a}{b} = \frac{-a}{b}$ (you can show $\frac{-a}{b} = \frac{a}{-b}$).

We define $\leqslant$ on $\mathbb{Q}$ by the following: for $a, b, c, d \in \mathbb{N}$, we have

1. $\frac{a}{b} \leqslant \frac{c}{d}$ whenever $a \cdot d \leqslant b \cdot c$;
2. $-\frac{a}{b} \leqslant \frac{c}{d}$; and
3. $-\frac{a}{b} \leqslant -\frac{c}{d}$ whenever $\frac{c}{d} \leqslant \frac{a}{b}$.

Then, again,

(i) For all $a, b \in \mathbb{N}$, we have $a \leqslant b$ or $b \leqslant a$.

(ii) If $a \leqslant b$ and $b \leqslant a$, then $a = b$.

(iii) If $a \leqslant b$ and $b \leqslant c$, then $a \leqslant c$.

(iv) If $a \leqslant b$ then $a + c \leqslant b + c$.

(v) If $a \leqslant b$ and $0 \leqslant c$, then $ac \leqslant bc$.

This makes $\mathbb{Q}$ into an ordered field.