INTRODUCTION TO PROOFS

formerly called Foundation and Proofs

Notes by Dr. Lynne H. Walling

4. Set operations

Throughout this section, we rely on basic results from §2.

Suppose that A, B are subsets of some set X.

Recall: $A \cup B$ denotes the union of A and B, meaning

$$A \cup B = \{x \in X : \ x \in A \text{ or } x \in B \ \}.$$

So for $x \in X$, $x \in A \cup B$ if and only if $x \in A \vee x \in B$.
$A \cap B$ denotes the intersection of A and B, meaning

$$A \cap B = \{x \in X : \ x \in A \text{ and } x \in B \ \}.$$

So for $x \in X$, $x \in A \cap B$ if and only if $x \in A \wedge x \in B$. When $A \cap B = \emptyset$ we say A and B are disjoint.
$A \setminus B$ denotes the difference of A and B, meaning

$$A \setminus B = \{x \in X : \ x \in A \text{ and } x \notin B \ \}.$$

So for $x \in X$, $x \in A \setminus B$ if and only if $x \in A \wedge x \notin B$.
A^c denotes the complement of A, meaning

$$A^c = \{x \in X : \ x \notin A \ \}.$$

We have the following simple proposition.

Theorem 4.1. *Let X be a set, and for $x \in X$, let $P(x)$ be the proposition that x satisfies condition P, and let $Q(x)$ be the proposition that x satisfies condition Q. Set*

$$A = \{x \in X : \ P(x) \ \}, \ B = \{x \in X : \ Q(x) \ \}.$$

Then

$$A \cap B = \{x \in X : \ P(x) \wedge Q(x) \ \} \text{ and } A \cup B = \{x \in X : \ P(x) \vee Q(x) \ \}.$$

Proof. For $x \in X$, we have $x \in A$ if and only if $P(x)$; similarly, $x \in B$ if and only if $Q(x)$. Thus

$$\begin{aligned} A \cap B &= \{x \in X : \ x \in A \wedge x \in B \ \} \\ &= \{x \in X : \ P(x) \wedge Q(x) \ \} \end{aligned}$$

and

$$\begin{aligned} A \cup B &= \{x \in X : \ x \in A \vee x \in B \ \} \\ &= \{x \in X : \ P(x) \vee Q(x) \ \}. \end{aligned}$$

□

Proposition 4.2. *Suppose A, B, C are subsets of a set X.*

(a) $A \cap (B \cap C) = (A \cap B) \cap C$.
(a) $A \cup (B \cup C) = (A \cup B) \cup C$.

(Thus the set operations $\cup$ and $\cap$ are associative.)

Proof. We prove (a) and leave (b) as an exercise.

Suppose $x \in X$. Let P be the propostion $x \in A$, Q the proposition $x \in B$, and R the propostion $x \in C$. Recall that $P \wedge (Q \wedge R) \iff (P \wedge Q) \wedge R$. Thus:

$$\begin{aligned} x \in A \cap (B \cap C) &\iff (x \in A) \wedge (x \in B \cap C) \\ &\iff (x \in A) \wedge (x \in B \wedge x \in C) \\ &\iff P \wedge (Q \wedge R) \\ &\iff (P \wedge Q) \wedge R \\ &\iff (x \in A \wedge x \in B) \wedge x \in C \\ &\iff (x \in A \cap B) \wedge (x \in C) \\ &\iff x \in (A \cap B) \cap C. \end{aligned}$$

Thus the elements of X that are in $A \cap (B \cap C)$ are exactly the elements of X that are in $(A \cap B) \cap C$, so $A \cap (B \cap C) = (A \cap B) \cap C$. □

Theorem 4.3. *Let A, B, C be subsets of a set X.*

(a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
(b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Proof. We prove (a) and leave (b) as an exercise.

Suppose $x \in X$. Let P be the propostion $x \in A$, Q the proposition $x \in B$, and R the proposition $x \in C$. Recall that $P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R)$. Then:

$$\begin{aligned} x \in A \cap (B \cup C) &\iff x \in A \wedge x \in B \cup C \\ &\iff x \in A \wedge (x \in B \vee x \in C) \\ &\iff P \wedge (Q \vee R) \\ &\iff (P \wedge Q) \vee (P \wedge R) \\ &\iff (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \\ &\iff (x \in A \cap B) \vee (x \in A \cap C) \\ &\iff x \in (A \cap B) \cup (A \cap C). \end{aligned}$$

Thus the elements of $A \cap (B \cup C)$ are exactly the elements of $(A \cap B) \cup (A \cap C)$, and hence $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. □

Proposition 4.4. *Suppose A, B are subsets of a set X.*

(a) $A \smallsetminus B = A \cap B^c$.
(b) $(A \smallsetminus B)^c = A^c \cup B$.

Proof. We prove (a) and leave (b) as an exercise.

Suppose $x \in X$; then we have

$$\begin{aligned} x \in A \smallsetminus B &\iff x \in A \wedge x \notin B \\ &\iff x \in A \wedge x \in B^c \\ &\iff x \in A \cap B^c, \end{aligned}$$

Thus the elements of X that are in $A \smallsetminus B$ are exactly the elements of X that are in $A \cap B^c$, so $A \smallsetminus B = A \cap B^c$. □

Theorem 4.5. *(De Morgan's Laws) Suppose A, B are subsets of a set X.*

(a) $A \smallsetminus (B \cup C) = (A \smallsetminus B) \cap (A \smallsetminus C)$.
(b) $A \smallsetminus (B \cap C) = (A \smallsetminus B) \cup (A \smallsetminus C)$.
(c) $(A \cap B)^c = A^c \cup B^c$. *(Thus for $x \in X$, $x \notin A \cap B \iff x \notin A \vee x \notin B$.)*
(d) $(A \cup B)^c = A^c \cap B^c$. *(Thus for $x \in X$, $x \notin A \cup B \iff x \notin A \wedge x \notin B$.)*

Proof. We prove (a), (d) and leave (b), (c) as exercises.

(a) Suppose $x \in X$. As an easy exercise using truth tables, one shows that with P, Q, R propositions, $P \wedge (Q \wedge R) \iff (P \wedge Q) \wedge (P \wedge R)$. Thus:

$$\begin{aligned}
x \in A \smallsetminus (B \cup C) &\iff (x \in A) \wedge (x \notin B \cup C) \\
&\iff (x \in A) \wedge \neg(x \in B \cup C) \\
&\iff (x \in A) \wedge \neg(x \in B \vee x \in C) \\
&\iff (x \in A) \wedge (x \notin B \wedge x \notin C) \\
&\iff (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) \\
&\iff (x \in A \smallsetminus B) \wedge (x \in A \smallsetminus C) \\
&\iff x \in (A \smallsetminus B) \cap (A \smallsetminus C).
\end{aligned}$$

Thus the elements of $A \smallsetminus (B \cup C)$ and $(A \smallsetminus B) \cap (A \smallsetminus C)$ are the same, meaning $A \smallsetminus (B \cup C) = (A \smallsetminus B) \cap (A \smallsetminus C)$.

(d) Suppose $x \in X$. Thus:

$$\begin{aligned}
x \in (A \cup B)^c &\iff \neg(x \in A \cup B) \\
&\iff \neg(x \in A \vee x \in B) \\
&\iff \neg(x \in A) \wedge \neg(x \in B) \\
&\iff x \in A^c \wedge x \in B^c \\
&\iff x \in A^c \cap B^c.
\end{aligned}$$

Since $x \in (A \cup B)^c$ if and only if $x \in A^c \cap B^c$, we have $(A \cup B)^c = A^c \cap B^c$. (Note that we have also shown that $x \in (A \cup B)^c \iff x \in A^c \wedge x \in B^c$, so $x \notin A \cup B \iff x \notin A \wedge x \notin B$.) □

Notation: It is often convenient to denote the elements of a set using indices, or subscripts. For example, suppose A is a set with 5 elements; we can denote these elements as a_1, a_2, a_3, a_4, a_5. Then we can write

$$A = \{a_i : \ i \in I \} \text{ where } I = \{1, 2, 3, 4, 5\};$$

here I is called an indexing set. This notation is particularly useful when dealing with infinite sets. For instance, we will see that there are infinitely many primes within the set of integers; ordering the primes in increasing order, let p_i denote the ith prime where $i \in \mathbb{Z}_+$. Then

$$\{p_i : \ i \in \mathbb{Z}_+ \}$$

denotes the set of all primes. Alternatively, we sometimes denote this set with the notation $\{p_i\}_{i \in \mathbb{Z}_+}$.

Let $\{A_i\}_{i\in I}$ be a collection of subsets of a set X where I is an indexing set. Then we write $\cup_{i\in I}A_i$ to denote the union of all the sets A_i, $i \in I$. That is,

$$\cup_{i\in I}A_i = \{x \in X : \exists i \in I \text{ so that } x \in A_i \}.$$

Somewhat similarly, we write $\cap_{i\in I}A_i$ to denote the intersection of all the sets A_i, $i \in I$. That is,

$$\cap_{i\in I}A_i = \{x \in X : \forall i \in I,\ x \in A_i \}.$$

Proposition 4.6. *Let X be a set with subset A, and an indexed collection of subsets $\{B_i\}_{i\in I}$, where I is an indexing set. Then we have:*

(a) $A \setminus \cap_{i\in I}B_i = \cup_{i\in I}(A \setminus B_i)$.
(b) $A \setminus \cup_{i\in I}B_i = \cap_{i\in I}(A \setminus B_i)$.

Proof. We prove (a) and leave (b) as an exercise.

We know $x \in \cap_{i\in I}B_i$ if and only if $\forall i \in I$, $x \in B_i$. So $\neg(x \in \cap_{i\in I}B_i)$ if and only if $\exists i \in I$ so that $x \notin B_i$.

Suppose $x \in A \setminus \cap_{i\in I}B_i$. Then $x \in A$, and for some $i \in I$, we have $x \notin B_i$. So for some $i \in I$, $x \in A \setminus B_i$. Thus $x \in \cup_{i\in I}(A \setminus B_i)$. This shows that $A \setminus \cap_{i\in I}B_i \subseteq \cup_{i\in I}(A \setminus B_i)$.

Now suppose that $x \in \cup_{i\in I}(A \setminus B_i)$. Thus for some $i \in I$, we have $x \in A \setminus B_i$. So for some $i \in I$, $x \in A$ and $x \notin B_i$. Since $\exists i \in I$ so that $x \notin B_i$, we have $x \notin \cap_{i\in I}B_i$. Thus $x \in A \setminus \cap_{i\in I}B_i$. This shows that $\cup_{i\in I}(A \setminus B_i) \subseteq A \setminus \cap_{i\in I}B_i$. Together with the result of the preceding paragraph, we get $A \setminus \cap_{i\in I}B_i = \cup_{i\in I}(A \setminus B_i)$. □

Theorem 4.7. *Suppose $f : X \to Y$ and $X = U \cup V$. Then $f(X) = f(U) \cup f(V)$. Further, if f is injective and $U \cap V = \emptyset$, then $f(U) \cap f(V) = \emptyset$.*

Proof. Since $U, V \subseteq X$, clearly $f(U), f(V) \subseteq f(X)$, so $f(U) \cup f(V) \subseteq f(X)$. On the other hand, take $x \in X$. Then $x \in U$ or $x \in V$, so $f(x) \in f(U)$ or $f(x) \in f(V)$. Therefore $f(x) \in f(U) \cup f(V)$; as this holds for all $x \in X$, we have $f(X) \subseteq f(U) \cup f(V)$. Hence $f(X) = f(U) \cup f(V)$.

Now suppose f is injective and $U \cap V = \emptyset$. For the sake of contradiction, suppose there is some $y \in f(U) \cap f(V)$. Thus there is some $u \in U$ so that $y = f(u)$, and there is some $v \in V$ so that $y = f(v)$. Hence $f(u) = y = f(v)$. Since f is injective, we have $u = v$. Hence $u \in U \cap V$ [as $u = v$ and $v \in V$], contradicting the assumption that $U \cap V = \emptyset$. Thus there cannot be any $y \in f(U) \cap f(V)$, meaning $f(U) \cap f(V) = \emptyset$. □

Definition. Suppose $f : X \to Y$, $V \subseteq Y$. We define the inverse image of V under f as

$$f^{-1}(V) = \{x \in X : f(x) \in V \}.$$

Note that $f^{-1}(\emptyset) = \emptyset$.

Warning: This notation does **not** mean f^{-1} is necessarily a function!

Example: Say $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ is defined by $f((x, y)) = 2x - 5y$. Then, from linear algebra, the "kernel" of f is

$$\begin{aligned} f^{-1}(\{0\}) &= \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ f((x, y)) \in \{0\} \ \} \\ &= \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ 2x - 5y = 0 \ \} \\ &= \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ y = 2x/5 \ \} \\ &= \{(x, 2x/5) : \ x \in \mathbb{R} \ \}. \end{aligned}$$

Example: Suppose still that $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ is defined by $f(x, y) = 2x - 5y$. Let $V = (0, 1)$, an open interval in $\mathbb{R}$. Then

$$\begin{aligned} f^{-1}(V) &= \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ f((x, y)) \in V \ \} \\ &= \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ 2x - 5y \in (0, 1) \ \} \\ &= \{(x, y) \in \mathbb{R} \times \mathbb{R} : \ 0 < 2x - 5y < 1 \ \} \\ &= \left\{ (x, y) \in \mathbb{R} \times \mathbb{R} : \ \frac{5}{2}y < x < \frac{5}{2}y + \frac{1}{2} \right\}. \end{aligned}$$

So we can also describe $f^{-1}(V)$ as

$$f^{-1}(V) = \left\{ \left(\frac{5}{2}y + \varepsilon, y \right) : \ \epsilon, y \in \mathbb{R}, \ 0 < \varepsilon < \frac{1}{2} \right\}.$$

Example: Define $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = |x^3|$. Take $V = [4, \infty)$. Then

$$\begin{aligned} g^{-1}(V) &= \{x \in \mathbb{R} : \ g(x) \in V \ \} \\ &= \{x \in \mathbb{R} : \ |x^3| \in [4, \infty) \ \} \\ &= \{x \in \mathbb{R} : \ x^3 \geq 4 \ \vee \ -x^3 \geq 4 \ \} \\ &= \{x \in \mathbb{R} : \ x \geq \sqrt[3]{4} \ \vee \ x \leq \sqrt[3]{-4} \ \} \\ &= (-\infty, \sqrt[3]{-4}] \cup [\sqrt[3]{4}, \infty). \end{aligned}$$

Theorem 4.8. *Let $f : X \to Y$, and let $U \subseteq X$, $V \subseteq Y$. Then we have:*

(a) *$f(f^{-1}(V)) \subseteq V$, and when f is surjective, $f(f^{-1}(V)) = V$.*
(b) *$U \subseteq f^{-1}(f(U))$, and when f is injective, $U = f^{-1}(f(U))$.*

Proof. We prove (a) and leave (b) as an exercise.

If $V = \emptyset$, then $f^{-1}(V) = \emptyset$ and $f(f^{-1}(V)) = \emptyset = V$. So suppose $V \neq \emptyset$.

Choose $y \in f(f^{-1}(V))$. Thus $y = f(w)$ for some $w \in f^{-1}(V)$. By the definition of $f^{-1}(V)$, we have $f(w) \in V$. Hence $y = f(w) \in V$. Since y was chosen arbitrarily from $f(f^{-1}(V))$, this shows that every element of $f(f^{-1}(V))$ lies in V, i.e. $f(f^{-1}(V)) \subseteq V$.

Now suppose f is surjective. We have already established that $f(f^{-1}(V)) \subseteq V$, so to show $f(f^{-1}(V)) = V$, we need to show $V \subseteq f(f^{-1}(V))$. Suppose $v \in V$. Since f is surjective, $\exists x \in X$ so that $f(x) = v$. Thus $f(x) \in V$, so $x \in f^{-1}(V)$. Hence $v = f(x) \in f(f^{-1}(V))$. Since v was chosen arbitrarily from V, this shows $V \subseteq f(f^{-1}(V))$. Since we chose v arbitrarily from V, this shows that $f(f^{-1}(V)) = V$ [under the assumption that f is surjective]. $\square$

Theorem 4.9. *Suppose $f : X \to Y$ and $V_1, V_2 \subseteq Y$. Then*

$$f^{-1}(V_1 \cap V_2) = f^{-1}(V_1) \cap f^{-1}(V_2)$$

and

$$f^{-1}(V_1 \cup V_2) = f^{-1}(V_1) \cup f^{-1}(V_2).$$

Proof. We prove the first statement and leave the second as an exercise.

We have

$$\begin{aligned} f^{-1}(V_1 \cap V_2) &= \{x \in X : \ f(x) \in V_1 \cap V_2 \ \} \\ &= \{x \in X : \ f(x) \in V_1 \wedge f(x) \in V_2 \ \}. \end{aligned}$$

On the other hand,

$$\begin{aligned} f^{-1}(V_1) \cap f^{-1}(V_2) &= \{x \in X : \ f(x) \in V_1 \ \} \cap \{x \in X : \ f(x) \in V_2 \ \} \\ &= \{x \in X : \ f(x) \in V_1 \wedge f(x) \in V_2 \ \}. \end{aligned}$$

Therefore $f^{-1}(V_1 \cap V_2) = f^{-1}(V_1) \cap f^{-1}(V_2)$.

Alternatively, one could present this argument as follows:

$$\begin{aligned} f^{-1}(V_1 \cap V_2) &= \{x \in X : \ f(x) \in V_1 \cap V_2 \ \} \\ &= \{x \in X : \ f(x) \in V_1 \wedge f(x) \in V_2 \ \} \\ &= \{x \in X : \ f(x) \in V_1 \ \} \cap \{x \in X : \ f(x) \in V_2 \ \} \\ &= f^{-1}(V_1) \cap f^{-1}(V_2). \end{aligned}$$

□

5. Partitioning sets, equivalence relations, and congruences

According to standard usage of English, partitioning a set means we break it into non-overlapping pieces. More precisely, we have the following.

Definition. A partition of a nonempty set X is a collection $\{A_i : \ i \in I \ \}$ of nonempty subsets of X so that

(1) $\forall x \in X$, $\exists i \in I$ so that $x \in A_i$;
(2) $\forall x \in X$, $\forall i, j \in I$, if $x \in A_i \wedge x \in A_j$ then $A_i = A_j$.

(In some texts the subsets A_i are called blocks of the partition.)

Example: Let $X = \{1, 2, 3, 4, 5, 6\}$. Then

$$\{\{1\}, \ \{2, 3\}, \ \{4, 5, 6\}\}$$

is a partition of X.

Partitions of sets are inextricably linked to "equivalence relations"; to define these, we first need some other definitions.

Definitions. A relation $\sim$ on a nonempty set X corresponds to a subset $R_\sim$ of $X \times X$; we write $x \sim y$ when $(x, y) \in R_\sim$, and we say x is related to y. Given a relation $\sim$ on X, we say:

(1) $\sim$ is reflexive if: $\forall x \in X$, we have $x \sim x$;
(2) $\sim$ is symmetric if: $\forall x, y \in X$, $x \sim y \implies y \sim x$;
(3) $\sim$ is transitive if: $\forall x, y, z \in X$, $(x \sim y \wedge y \sim z) \implies x \sim z$.

A relation is an equivalence relation if it is reflexive, symmetric, and transitive.

Example: Let $X = \mathbb{Z}$, and let $R_\sim = \{(x, x) : x \in \mathbb{Z}\}$. So $\forall x \in \mathbb{Z}$, $x \sim x$ (so $\sim$ is reflexive). Also, $\forall x, y \in \mathbb{Z}$, $(x \sim y) \implies (x = y)$. We claim that $\sim$ is an equivalence relation on $\mathbb{Z}$: We already noted $\sim$ is reflexive. Suppose $x, y \in \mathbb{Z}$ so that $x \sim y$. Thus $(x, y) \in R_\sim$, so $x = y$. Hence $(y, x) = (x, x) \in R_\sim$, so $y \sim x$. Thus $\sim$ is symmetric. Suppose $x, y, z \in \mathbb{Z}$ so that $x \sim y$ and $y \sim z$. Thus $x = y$, and $y = z$, so $x = y = z$. Hence $(x, z) = (x, x) \in R_\sim$, so $x \sim z$. Thus $\sim$ is transitive. So $\sim$ is an equivalence relation.

Note: If $\sim$ is an equivalence relation on some nonempty set X, then we necessarily have

$$\{(x, x) : x \in X\} \subseteq R_\sim$$

since $\sim$ is reflexive.

Example: Let T be the set of all triangles in $\mathbb{R} \times \mathbb{R}$. For $t_1, t_2 \in T$, consider the following relation: $t_1 \sim t_2$ if t_1 is similar to t_2, meaning there is a correspondence between the interior angles of t_1 and the interior angles of t_2 so that corresponding angles are equal. Then $\sim$ is an equivalence relation.

Example: Define a relation $\sim$ on $\mathbb{Z}$ by $x \sim y$ if $x < y$. So $\sim$ is not reflexive, as there are $x \in \mathbb{Z}$ so that $\neg(x \sim x)$; in particular, $1 \in \mathbb{Z}$ and $\neg(1 < 1)$ so $\neg(1 \sim 1)$. Also, $\sim$ is not symmetric, as there are $x, y \in \mathbb{Z}$ so that $x \sim y$ but $\neg(y \sim x)$; in particular, $2, 3 \in \mathbb{Z}$ and $2 < 3$ so $2 \sim 3$, but $\neg(3 < 2)$ so $\neg(3 \sim 2)$. However, $\sim$ is transitive: Suppose $x, y, z \in \mathbb{Z}$ so that $x \sim y$ and $y \sim z$. Thus $x < y$ and $y < z$, so $x < y < z$. Hence $x < z$, so $x \sim z$.

Definition. Suppose $\sim$ is an equivalence relation on a (nonempty) set X. For $x \in X$, we define

$$[x] = \{y \in X : y \sim x\},$$

and we call $[x]$ the equivalence class of x.

Proposition 5.1. *Suppose $\sim$ is an equivalence relation on a (nonempty) set X. For any $x, y \in X$, $[x] \neq [y]$ if and only if $[x] \cap [y] = \emptyset$.*

Proof. Take $x, y \in X$. We need to prove
(1) $[x] \neq [y] \implies [x] \cap [y] = \emptyset$, and
(2) $[x] \cap [y] = \emptyset \implies [x] \neq [y]$.
To do this, we will prove the contrapositive of each statement:
(1) $[x] \cap [y] \neq \emptyset \implies [x] = [y]$, and
(2) $[x] = [y] \implies [x] \cap [y] \neq \emptyset$.

To prove (1): Suppose $[x] \cap [y] \neq \emptyset$. Thus there is some $z \in [x] \cap [y]$. Hence $z \in [x]$, so $z \sim x$; similarly, $z \in [y]$, so $z \sim y$. Since $\sim$ is symmetric, we have $x \sim z$; since $\sim$ is transitive, we have $x \sim y$. Now choose $w \in [x]$; thus $w \sim x$, and since $x \sim y$ and $\sim$ is transitive, $w \sim y$. Hence $w \in [y]$; as this holds for all $w \in [x]$, we have $[x] \subseteq [y]$. A virtually identical argument shows that for any $w \in [y]$ we have $w \in [x]$, so $[y] \subseteq [x]$. Hence $[x] = [y]$.

To prove (2): Suppose $[x] = [y]$. We know $x \in [x]$ as $\sim$ is reflexive and so $x \sim x$. Hence $x \in [x] = [x] \cap [y]$, so $[x] \cap [y] \neq \emptyset$. □

Theorem 5.2. *Suppose $\sim$ is an equivalence relation on a (nonempty) set X. Then*

$$\Pi = \{[x] : x \in X\}$$

is a partition of X.

Proof. Take $a \in X$. Then $[a] \in \Pi$; hence every element of X is in one of the sets in Π.

Now suppose that for $a \in X$, we have $a \in [x]$ and $a \in [y]$ where $x, y \in X$. Then $[x] \cap [y] \neq \emptyset$, so by the preceding proposition we have $[x] = [y]$. Thus Π is a partition of X. □

On the other hand, we have the following.

Theorem 5.3. *Suppose $\Pi = \{A_i : i \in I\}$ is a partition of a (nonempty) set X (so I is an indexing set). For $x, y \in X$, define $x \sim y$ if $\exists i \in I$ so that $x, y \in A_i$. Then $\sim$ is an equivalence relation on X.*

Proof. We first show $\sim$ is reflexive: Take $x \in X$. Since Π is a partition of X, there is some $i \in I$ so that $x \in A_i$. Thus $x \sim x$.

Next we show $\sim$ is symmetric: Suppose $x, y \in X$ so that $x \sim y$. Thus there is some $i \in I$ so that $x, y \in A_i$. Hence $y, x \in A_i$, so $y \sim x$.

Finally, we show $\sim$ is transitive: Suppose $x, y, z \in X$ so that $x \sim y$ and $y \sim z$. Thus there is some $i \in I$ so that $x, y \in A_i$ and some $j \in I$ so that $y, z \in A_j$. Hence $y \in A_i$ and $y \in A_j$; since Π is a partition, we must have $A_i = A_j$. Thus $x, z \in A_i$ so $x \sim z$.

This shows $\sim$ is an equivalence relation on X. □

Congruences. Here we present an explicit and fundamental example of an equivalence relation on $\mathbb{Z}$. We begin with a familiar definition.

Defintion. For $x, y \in \mathbb{Z}$, we say x divides y if $\exists z \in \mathbb{Z}$ so that $y = xz$. We write $x|y$ to denote "x divides y". Similarly, we write $x \nmid y$ to denote "x does not divide y", meaning that $\forall z \in \mathbb{Z},\ y \neq xz$.

Fix $n \in \mathbb{Z}_+$. We define a relation on $\mathbb{Z}$ as follows: For $a, b \in \mathbb{Z}$, we write $a \equiv b \pmod{n}$ if $n|a - b$. When $a \equiv b \pmod{n}$, we say a is congruent to b modulo n. We leave it as an exercise to show that this relation is in fact an equivalence relation on $\mathbb{Z}$; later we will see that the equivalence classes are $[0], [1], [2], \ldots, [n-1]$. When $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_+$, we say a and b are in the same congruence class modulo n.

This is a particularly interesting equivalence relation because of the following.

Theorem 5.4. *Fix $n \in \mathbb{Z}_+$. Suppose $a, b, c, d \in \mathbb{Z}$ so that $a \equiv c \ (mod\ n)$, $b \equiv d \ (mod\ n)$. Then*

$$a + b \equiv c + d \ (mod\ n),\ ab \equiv cd \ (mod\ n).$$

Proof. By assumption, we have $n|a - c$ and $n|b - d$. Thus for some $x, y \in \mathbb{Z}$, we have $a - c = nx$ and $b - d = ny$. Hence

$$(a + b) - (c + d) = (a - c) + (b - d) = nx + ny = n(x + y).$$

Since $x + y \in \mathbb{Z}$, this means $n|(a + b) - (c + d)$, so $a + b \equiv c + d \pmod{n}$. Also, since $a = c + nx$ and $b = d + ny$, we have

$$ab = (c + nx)(d + ny) = cd + n(cy + dx + nxy)$$

and hence $ab - cd = n(cy + dx + nxy)$. Since $cy + dx + nxy \in \mathbb{Z}$, we have $n|ab - cd$, so $ab \equiv cd \pmod{n}$. □

This result helps simplify many computations modulo a positive integer n.

Example: We compute $3^5 + 2^8 \pmod 7$ without working unnecessarily hard.

We have $3^2 \equiv 9 \equiv 2 \pmod 7$. So $3^4 = 3^2 \cdot 3^2 \equiv 2 \cdot 2 \equiv 4 \pmod 7$. Hence

$$3^5 \equiv 3^4 \cdot 3 \equiv 12 \equiv 5 \pmod 7.$$

Somewhat similarly, $2^3 \equiv 8 \equiv 1 \pmod 7$, so

$$2^6 \equiv 2^3 \cdot 2^3 \equiv 1 \cdot 1 \equiv 1 \pmod 7.$$

So $2^8 \equiv 2^6 \cdot 2^2 \equiv 1 \cdot 4 \equiv 4 \pmod 7$. Hence

$$3^5 + 2^8 \equiv 5 + 4 \equiv 2 \pmod 7.$$