INTRODUCTION TO PROOFS

formerly called Foundation and Proofs

Notes by Dr. Lynne H. Walling

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 $\forall x \in \mathbb{Z}$, $x \sim x$ ($\sim$ 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 $a \equiv c \pmod{n}$, $b \equiv d \pmod{n}$. Then*

$$a + b \equiv c + d \pmod{n},\ ab \equiv cd \pmod{n}.$$

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

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