Items in this supplement are numbered R.1, R.2, and so on. After you have proved them, you are free to use them. If you use a result from this document later in the class, you should cite it by number, e.g. "by Theorem R.13". The Rules of the Game still apply.

Relations

So far, we have encountered many ways to compare two integers. Given $a, b \in \mathbb{Z}$, we ask if $a \mid b$, or if $a < b$, or if $a \equiv b \pmod{n}$ for some fixed $n > 0$. Each of these is a rule that, given an ordered pair (a, b) of integers, has a yes or no answer. We can abstract this idea by introducing the notion of a relation on a set. Given two sets A and B, the **Cartesian product** of A and B is the set $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$.

R.1 Definition. Let A be a set. A **relation** on A is a subset R of $A \times A$. If $(a, b) \in R$, we write $a \sim_R b$ (or just $a \sim b$ if the context is clear) and say that a **is related to** b. If $(a, b) \notin R$, we write $a \not\sim_R b$.

Note that a relation is a *set*, and that the notation $a \sim b$ is making a claim about membership in that set.

R.2 Exercise. Let $A = \{1, 2, 3\}$ and let R be the relation on A given by

$$R = \{(1,1), (1,2), (2,1), (2,2), (3,2), (3,3)\}.$$

Answer each of the following, and say which pair you are appealing to.

(a) Is $1 \sim_R 2$? Is $3 \sim_R 2$? Is $2 \sim_R 3$?

(b) How many relations are there on A? (You do not need to list them.)

R.3 Exercise. Each of the following defines a relation on $\mathbb{Z}$. For each one, write down two ordered pairs that belong to it and two that do not.

(a) Define $R_1 \subseteq \mathbb{Z} \times \mathbb{Z}$ as follows: $(a, b) \in R_1$ if and only if $a \mid b$.

(b) Define $R_2 \subseteq \mathbb{Z} \times \mathbb{Z}$ as follows: $(a, b) \in R_2$ if and only if $a \equiv b \pmod{5}$.

Once the set theoretic definition of relation is understood, it is common to omit entirely the underlying set of ordered pairs. For instance, we might simply define a relation $\sim$ on $\mathbb{Z}$ via $a \sim b$ if and only if $a \leq b$.

R.4 Definition. Let $\sim$ be a relation on a set A. We say $\sim$ is

(a) **reflexive** if $a \sim a$ for every $a \in A$;

(b) **symmetric** if for all $a, b \in A$, whenever $a \sim b$ we have $b \sim a$; and

(c) **transitive** if for all $a, b, c \in A$, whenever $a \sim b$ and $b \sim c$ we have $a \sim c$.

R.5 Exercise. For each of the following relations, determine which of the three properties in R.4 it has. Prove each property that holds, and give an explicit counterexample for each one that fails.

(a) $\sim$ on $\mathbb{Z}$, where $a \sim b$ if and only if $a \leq b$.

(b) $\sim$ on $\mathbb{Z}$, where $a \sim b$ if and only if $a < b$.

(c) $\sim$ on $\mathbb{Z}$, where $a \sim b$ if and only if $a = b$ or $a = -b$.

(d) $\sim$ on $\mathbb{R}^2$, where $\mathbf{v} \sim \mathbf{w}$ if and only if $\mathbf{v} \cdot \mathbf{w} = 0$; that is, $\mathbf{v}$ and $\mathbf{w}$ are orthogonal.

(e) $\sim$ on $\mathbb{Z}$, where $a \sim b$ if and only if $ab \geq 0$.

(f) $\sim$ on $\{1, 2, 3\}$, the relation from R.2.

A single counterexample is enough to show that a property fails. To show that a property holds you must argue about arbitrary elements!

R.6 Exercise. For each of the following, find a set and a relation on that set with exactly the properties named. Justify your answer.

(a) Reflexive and symmetric, but not transitive.
(b) Reflexive and transitive, but not symmetric.
(c) Symmetric and transitive, but not reflexive.
(d) None of the three.

R.7 Exercise. Part (c) of R.6 shows that the following statement is false.

> **Claim.** If a relation $\sim$ on a set A is symmetric and transitive, then it is reflexive.
>
> **"Proof."** Let $a \in A$ and suppose $a \sim b$. By symmetry, $b \sim a$. Since $a \sim b$ and $b \sim a$, transitivity gives $a \sim a$. Therefore $\sim$ is reflexive. $\square$

Identify the flaw in this argument.

R.8 Definition. A relation $\sim$ on a set A is an **equivalence relation** on A if it is reflexive, symmetric, and transitive.

R.9 Theorem. Let n be an integer with $n > 0$. Then congruence modulo n is an equivalence relation on $\mathbb{Z}$.

You should be able to prove R.9 in three lines by citing results you already have. Say which result gives you which property.

R.10 Exercise. Which of the relations in R.5 are equivalence relations?

Equivalence Classes

An equivalence relation sorts the elements of a set into groups of things that the relation cannot tell apart. The next definition names those groups. Notice that it makes sense for any relation at all, but that it will only behave well when the relation is an equivalence relation.

R.11 Definition. Let $\sim$ be an equivalence relation on a set A and let $a \in A$. The **equivalence class of** a, written $[a]$, is the set

$$[a] \;:=\; \{\, b \in A \;:\; b \sim a \,\}.$$

Any element of $[a]$ is called a **representative** of that class.

R.12 Exercise. Let $\sim$ be the relation on $\mathbb{Z}$ from R.5(c), where $a \sim b$ if and only if $a = b$ or $a = -b$. Write down $[0]$, $[1]$, and $[-7]$ by listing their elements. How many distinct equivalence classes are there?

The next theorem uses two standard set operations. Given sets X and Y, the **intersection** of X and Y is the set $X \cap Y = \{x : x \in X \text{ and } x \in Y\}$, and we say X and Y are **disjoint** if $X \cap Y = \varnothing$. Given a collection of sets X_i indexed by a set I, the **union** of that collection is the set

$$\bigcup_{i \in I} X_i \;=\; \{\, x : x \in X_i \text{ for some } i \in I \,\}.$$

R.13 Theorem. Let $\sim$ be an equivalence relation on a set A and let $a, b \in A$. Then

(a) $a \in [a]$; in particular, no equivalence class is empty;

(b) $a \sim b$ if and only if $[a] = [b]$;

(c) if $[a] \neq [b]$, then $[a] \cap [b] = \varnothing$; and

(d) $\displaystyle\bigcup_{x \in A} [x] = A$.

Partitions

Together, parts (a), (c), and (d) of R.13 tell us that an equivalence relation cuts A into nonempty subsets which are pairwise disjoint and whose union is equal to A. This leads to the following definition.

R.14 Definition. Let A be a set. A collection Ω of subsets of A is a **partition** of A if

(a) every $X \in \Omega$ is nonempty;

(b) for all $X, Y \in \Omega$, if $X \neq Y$ then $X \cap Y = \varnothing$; and

(c) $\displaystyle\bigcup_{X \in \Omega} X = A$.

Each $X \in \Omega$ is called a **block** of the partition. Note that Ω is a set of sets; any element $X \in \Omega$ satisfies $X \subseteq A$.

R.15 Exercise. Let $A = \{1, 2, 3, 4, 5\}$.

(a) Find a partition of A with two blocks, and one with four blocks.

(b) Find a collection of subsets of A that is *not* a partition of A. Which property fails? Can you find other examples that fail in distinct ways?

R.16 Exercise. For each of the following, give a partition of $\mathbb{Z}$ with the stated property, or explain why none exists.

(a) Finitely many blocks, each of them infinite.

(b) Infinitely many blocks, each of them finite.

(c) Infinitely many blocks, each of them infinite.

Give a one-line proof of the next result, which uses the new language to summarize the work you've done.

R.17 Theorem. Let $\sim$ be an equivalence relation on a set A. Then the collection of equivalence classes of $\sim$ is a partition of A.

By Theorem R.17, every equivalence relation determines a partition of the set. Now we will try to go the other way.

R.18 Exercise. Let $A = \{1, 2, 3, 4\}$ and consider the partition $\Omega = \{\{1, 2\}, \{3\}, \{4\}\}$ of A. Determine an equivalence relation on A whose equivalence classes are precisely the blocks of Ω. Is there more than one way to do it?

The next theorem may be the first time you have encountered an existence and uniqueness statement. Proving one takes two steps. First you must show *existence*: that an object exists with the specified property. Then you must show *uniqueness*: that any two objects with that property are actually equal.

R.19 Theorem. Let Ω be a partition of a nonempty set A. Then there exists a unique equivalence relation on A whose equivalence classes are precisely the blocks of Ω.

Back to the Integers

In Exercise 1.8 you characterized all the integers m satisfying each of $m \equiv 0, 1, 2, 3, \text{and } 4 \pmod 3$.

R.20 Exercise.

(a) Find all the equivalence classes modulo 3 and compare with your solution to that exercise. How many equivalence classes are there?

(b) The five sets you found there are not all distinct. Which coincide, and which result of this supplement can be used to determine this without any computation?

(c) Verify directly that the distinct sets among them form a partition of $\mathbb{Z}$.

(d) How many equivalence classes are there modulo n? You do not need to prove your claim.

We will return to part (d) in Chapter 3.