

0.5 Relations, Equivalence Classes, and Quotients

Mathematics constantly declares different-looking things to be “the same”: $\frac{1}{2}$ and $\frac{2}{4}$ are the same number, 14:00 and 2 p.m. are the same time, and in Chapter 4 two vectors will count as the same when their difference lies in a fixed subspace. This section makes “the same, for present purposes” precise. The notion is an equivalence relation. Gluing equivalent things together produces a new set, the quotient, and the one real danger of working with quotients is defining a function on them that secretly depends on a choice. We will learn to check for that.

0.5.1 Relations

Before we can say what a good notion of sameness is, we need a word for any way of comparing two elements of a set, good or bad. Examples are $\leq$ on numbers, “divides” on integers, and “has the same birthday as” on people. What such a comparison really amounts to is the list of pairs that are related, and a list of pairs is a subset of the Cartesian product (Definition 0.3.10).

Definition 0.5.1. Relation

A **relation** on a set X is a subset $R \subseteq X \times X$. When $(x, y) \in R$ we say x **is related to** y and write $x R y$, or $x \sim y$ when the relation is fixed.

Example. Relations

- (a) On $\mathbb{Z}$: $a \leq b$. The pairs $(1, 2)$ and $(2, 2)$ belong to the relation, $(2, 1)$ does not.
- (b) On $\mathbb{Z}$: $a \mid b$ (“ a divides b ”), meaning $b = ka$ for some $k \in \mathbb{Z}$. So $3 \mid 12$ and $3 \mid 0$, but $3 \nmid 5$.
- (c) On $\mathbb{R}$: $x \sim y$ if $x^2 + y^2 = 1$. As a subset of $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ this relation is the unit circle, so a relation can literally be a picture.
- (d) On any set X : the **empty relation** $R = \emptyset$, in which nothing is related to anything, and the **full relation** $R = X \times X$, in which everything is related to everything. These two extremes are useful test cases for every property below.

Every subset of $X \times X$ is a relation, so the definition has no nonexamples. The interesting question is which properties a given relation has.

0.5.2 Equivalence relations

What must any reasonable notion of “ x is the same as y ” satisfy? Think of “has the same birthday as”. Everyone has the same birthday as themselves. If you share a birthday with me, I share one with you. If x shares a birthday with y , and y with z , then x shares one with z . Those three features are exactly what we ask for.

An equivalence relation is a way of declaring elements “the same” that behaves like equality: everything is the same as itself, sameness goes both ways, and it can be chained.

Definition 0.5.2. Equivalence relation

A relation $\sim$ on a set X is an **equivalence relation** if it satisfies the following three conditions.

- (E1) **Reflexive:** $x \sim x$ for every $x \in X$.
- (E2) **Symmetric:** for all $x, y \in X$, if $x \sim y$ then $y \sim x$.
- (E3) **Transitive:** for all $x, y, z \in X$, if $x \sim y$ and $y \sim z$ then $x \sim z$.

In words: (E1) asks every single element to be related to itself, with no exceptions. (E2) says the relation cannot be one-way. (E3) says a chain of two links can be shortened to one link, and so, by applying it repeatedly, can any finite chain. When $x \sim y$ we say x and y are **equivalent**.

The standard move for checking an equivalence relation is to write three short paragraphs, one per condition, each starting from its hypothesis (“Let $x \in X$.”, “Suppose $x \sim y$.”, “Suppose $x \sim y$ and $y \sim z$.”).

Example. Equivalence relations

Show that each of the following is an equivalence relation.

- (a) Equality on any set X : $x \sim y$ if $x = y$.
- (b) **Congruence modulo n** on $\mathbb{Z}$, for a fixed integer $n \geq 1$: $a \equiv b \pmod{n}$ if $n \mid a - b$.
- (c) “Same length” on the set S of finite strings of the letters a, b : $u \sim v$ if u and v have the same number of letters.
- (d) “Same value”: for a function $f: X \rightarrow Y$, put $x \sim_f x'$ if $f(x) = f(x')$.
- (e) Fractions: on $P = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, put $(a, b) \sim (c, d)$ if $ad = bc$.

Solution.

- (a) Every x equals itself; $x = y$ gives $y = x$; $x = y$ and $y = z$ give $x = z$. Equality is the degenerate case: it is the equivalence relation that identifies nothing new, and the model the other examples imitate.
- (b) *Reflexive.* Let $a \in \mathbb{Z}$. Then $a - a = 0 = 0 \cdot n$, so $n \mid a - a$. *Symmetric.* Suppose $a - b = kn$ with $k \in \mathbb{Z}$. Then $b - a = (-k)n$, so $n \mid b - a$. *Transitive.* Suppose $a - b = kn$ and $b - c = \ell n$ with $k, \ell \in \mathbb{Z}$. Then $a - c = (a - b) + (b - c) = (k + \ell)n$, so $n \mid a - c$. For $n = 2$ this is “same parity”: $a \equiv b \pmod{2}$ says a and b are both even or both odd.
- (c) This is the special case of (d) in which $f: S \rightarrow \mathbb{N}$ sends a string to its length, so it follows from (d), whose proof does not use (c).
- (d) *Reflexive:* $f(x) = f(x)$. *Symmetric:* $f(x) = f(x')$ gives $f(x') = f(x)$. *Transitive:* $f(x) = f(x')$ and $f(x') = f(x'')$ give $f(x) = f(x'')$. Each condition is inherited from the same property of equality in Y . Many equivalence relations are of this form: “same distance from the origin” on $\mathbb{R}^2$ is $\sim_f$ for $f(x, y) = x^2 + y^2$.
- (e) *Reflexive:* $ab = ba$, so $(a, b) \sim (a, b)$. *Symmetric:* $ad = bc$ gives $cb = da$, which says $(c, d) \sim (a, b)$. *Transitive:* suppose $ad = bc$ and $cf = de$. Multiplying the first equation by f and the second by b gives $adf = bcf = bde$. Hence $d(af - be) = 0$. Since $d \neq 0$, we

get $af = be$, that is, $(a, b) \sim (e, f)$. Transitivity is exactly where second entries must be nonzero: with $d = 0$ allowed, $(1, 1) \sim (0, 0) \sim (2, 1)$ but $(1, 1) \not\sim (2, 1)$.

Minimal changes to these examples show that each condition can fail on its own.

Example. Relations that are not equivalence relations

Decide which of (E1)–(E3) each relation satisfies.

- (a) $\leq$ on $\mathbb{Z}$.
- (b) On $\mathbb{R}$: $x \sim y$ if $|x - y| \leq 1$.
- (c) On $\mathbb{R}$: $x \sim y$ if $xy > 0$.

Solution.

- (a) Change “=” to “ $\leq$ ”. Reflexivity survives ($a \leq a$) and so does transitivity ($a \leq b \leq c$ gives $a \leq c$). **Symmetry fails:** $1 \leq 2$ but $2 \not\leq 1$.
- (b) Change “ $|x - y| = 0$ ” (which is equality) to “ $|x - y| \leq 1$ ”. Reflexivity survives, since $|x - x| = 0$, and so does symmetry, since $|y - x| = |x - y|$. **Transitivity fails:** $0 \sim 1$ and $1 \sim 2$, but $|0 - 2| = 2 > 1$. “Close to” cannot be chained; many small steps make a big one.
- (c) Symmetry holds, since $yx = xy$. Transitivity holds: if $xy > 0$ and $yz > 0$, then $xy^2z > 0$, and since $y^2 > 0$ this gives $xz > 0$. **Reflexivity fails, at exactly one point:** $0 \cdot 0 = 0$, so $0 \not\sim 0$. On $\mathbb{R} \setminus \{0\}$ the same rule is an equivalence relation (“same sign”).

Warning. A tempting argument claims that (E1) follows from (E2) and (E3): “if $x \sim y$, then $y \sim x$ by symmetry, so $x \sim x$ by transitivity.” The gap is the word “if”. The argument needs some y with $x \sim y$, and there may be none. In [Example \(Relations that are not equivalence relations\)](#) (c), the element 0 is related to nothing, which is exactly why it escapes. Reflexivity must always be checked on its own.

Quick check. On $\mathbb{Z}$, define $a \sim b$ if $ab \geq 0$. Is $\sim$ an equivalence relation?

Solution. No. It is reflexive ($a^2 \geq 0$) and symmetric, but not transitive: $1 \sim 0$ and $0 \sim -1$ since both products are 0, yet $1 \cdot (-1) = -1 < 0$, so $1 \not\sim -1$. Compare [Example \(Relations that are not equivalence relations\)](#) (c): moving from $>$ to $\geq$ repairs reflexivity at 0 but lets 0 link the positives to the negatives.

Why these three conditions. They are precisely what the next subsection needs. Reflexivity will guarantee that every element lies in its own class, so no class is empty and nothing is lost. Symmetry and transitivity together will guarantee that two classes are either identical or disjoint. Drop any one of them and the picture of X cut cleanly into pieces falls apart, as the

nonexamples above show.

Remark. Two equivalence relations on matrices are central later: *row equivalence*, which records that one matrix can be reached from another by row operations, and *similarity*, which records that two square matrices describe the same linear map in different coordinates. Both are introduced once matrices are available, later in this chapter, and studied in Chapters 3 and 4.

0.5.3 Equivalence classes and partitions

Once we have decided which elements count as the same, it is natural to collect everything that is the same as a given element into one set.

Definition 0.5.3. Equivalence class

Let $\sim$ be an equivalence relation on X , and let $x \in X$. The **equivalence class** of x is

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

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

The word “representative” is chosen carefully. A class is one set, but it usually has many names: $[x] = [y]$ is possible with $x \neq y$.

Example. Equivalence classes

- (a) For equality on X , $[x] = \{x\}$. Every class has one element.
- (b) For congruence modulo 3 on $\mathbb{Z}$:

$$[0] = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

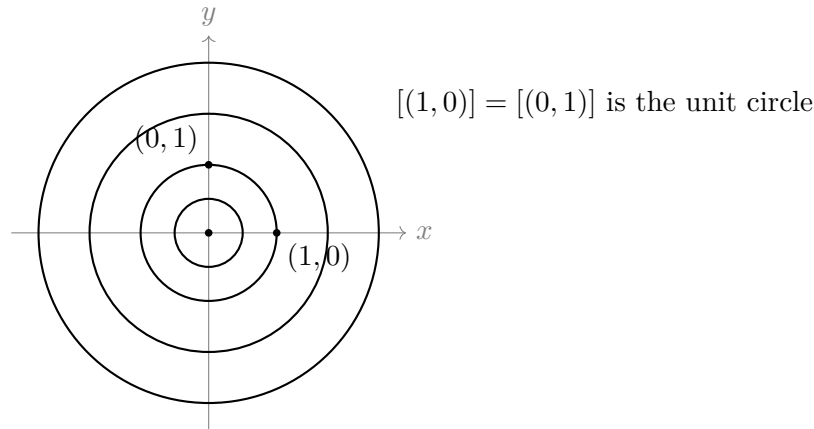
$$[1] = \{\dots, -5, -2, 1, 4, 7, \dots\},$$

$$[2] = \{\dots, -4, -1, 2, 5, 8, \dots\}.$$

Here $[0] = [3] = [-3]$ and $[2] = [-1]$: one class, many names.

- (c) For “same length” on strings of a, b , the class of ab is $\{aa, ab, ba, bb\}$, and the class of the empty string contains only the empty string.
- (d) For the full relation $X \times X$ on a nonempty set X , there is a single class, $[x] = X$.
- (e) For “same distance from the origin” on $\mathbb{R}^2$, the class of (x, y) is the circle of radius $\sqrt{x^2 + y^2}$ centered at the origin. The class of the origin is the one-point set $\{(0, 0)\}$.

In example (e), the classes look like this. Each circle is one class; the origin on its own is another.



The picture suggests two facts: every point lies on exactly one circle, and two different circles never meet. Both hold for every equivalence relation, and the proof is where the three conditions do their work.

Lemma 0.5.1. Classes are equal or disjoint

Let $\sim$ be an equivalence relation on X , and let $a, b \in X$.

- (a) $[a] = [b]$ if and only if $a \sim b$.
- (b) Either $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

Proof.

- (a) $(\Rightarrow)$ Suppose $[a] = [b]$. By reflexivity $a \sim a$, so $a \in [a] = [b]$, which means $a \sim b$.
 $(\Leftarrow)$ Suppose $a \sim b$. Let $x \in [a]$, so $x \sim a$. Since $a \sim b$, transitivity gives $x \sim b$, so $x \in [b]$. Hence $[a] \subseteq [b]$. By symmetry $b \sim a$, and swapping the roles of a and b in the argument gives $[b] \subseteq [a]$. By Theorem 0.3.1, $[a] = [b]$.
- (b) Suppose $[a] \cap [b] \neq \emptyset$, and let $c \in [a] \cap [b]$. Then $c \sim a$ and $c \sim b$. By symmetry $a \sim c$, and by transitivity $a \sim b$. By (a), $[a] = [b]$.

■

Part (a) is the working form of the lemma: to show two classes are equal, show one representative is equivalent to the other. The picture of nonoverlapping pieces that cover everything has its own name.

Definition 0.5.4. Partition

A **partition** of a set X is a collection $\mathcal{P}$ of subsets of X , called **blocks**, such that:

- (P1) every block is **nonempty**;
- (P2) **distinct** blocks are disjoint: if $B, B' \in \mathcal{P}$ and $B \neq B'$, then $B \cap B' = \emptyset$;
- (P3) the blocks cover X : every $x \in X$ lies in some block.

By (P2) and (P3), every element of X lies in **exactly one** block. For example, $\{\{1, 3\}, \{2\}\}$ is a partition of $\{1, 2, 3\}$, while $\{\{1, 2\}, \{2, 3\}\}$ is not, because the distinct blocks share 2 and (P2) fails.

Quick check. Is $\{\{1, 2, 3\}, \emptyset\}$ a partition of $\{1, 2, 3\}$? Is $\{\{1\}, \{2\}\}$?

Solution. Neither. The first contains the empty block, so (P1) fails, even though (P2) and (P3) hold. The second does not cover 3, so (P3) fails.

The main theorem says that equivalence relations and partitions are two descriptions of the same thing: “which elements are the same” and “how X is cut into pieces”.

Theorem 0.5.2. Equivalence relations and partitions

Let X be a set.

- (a) If $\sim$ is an equivalence relation on X , then the set of its equivalence classes is a partition of X .
- (b) If $\mathcal{P}$ is a partition of X , then the relation “ $x \sim_{\mathcal{P}} y$ if x and y lie in the same block” is an equivalence relation on X , and its equivalence classes are exactly the blocks of $\mathcal{P}$.
- (c) The two constructions undo each other: starting from $\sim$, the relation defined in (b) by the partition in (a) is $\sim$ again.

Idea. Part (a) is the lemma plus reflexivity: (P1) and (P3) come from $x \in [x]$, and (P2) is Lemma 0.5.1 (b). Part (b) runs the other way, and each block condition pays for one equivalence condition: covering gives reflexivity, and disjointness gives transitivity, because a middle element y can lie in only one block. Part (c) is Lemma 0.5.1 (a) read as a sentence about blocks.

Proof.

- (a) Let $\mathcal{P} = \{[x] : x \in X\}$. For every $x \in X$, reflexivity gives $x \in [x]$. Hence every class is nonempty, which is (P1), and every element lies in some class, which is (P3). If $[a] \neq [b]$, then $[a] \cap [b] = \emptyset$ by Lemma 0.5.1 (b), which is (P2). Hence $\mathcal{P}$ is a partition of X .
- (b) *Reflexive.* Let $x \in X$. By (P3), x lies in some block, so $x \sim_{\mathcal{P}} x$. *Symmetric.* “ x and y lie in a common block” does not depend on the order of x and y . *Transitive.* Suppose $x, y \in B$ and $y, z \in B'$ for blocks B, B' . Then $y \in B \cap B'$, so $B = B'$ by (P2). Hence $x, z \in B$, and $x \sim_{\mathcal{P}} z$.
Now let $B \in \mathcal{P}$ and $x \in B$; we show $[x] = B$, where the class is taken for $\sim_{\mathcal{P}}$. ($\subseteq$) If $y \in [x]$, then y and x lie in a common block B' ; since $x \in B \cap B'$, (P2) gives $B' = B$, so $y \in B$. ($\supseteq$) If $y \in B$, then y and x both lie in B , so $y \sim_{\mathcal{P}} x$ and $y \in [x]$. Hence $[x] = B$ by Theorem 0.3.1. Every class $[x]$ is therefore the block containing x , which exists by (P3); and every block B is a class, namely $[x]$ for any $x \in B$, which exists by (P1). So the classes are exactly the blocks.
- (c) Let $\sim$ be an equivalence relation, and let $\approx$ be the relation built by (b) from the classes of $\sim$. If $x \sim y$, then $x, y \in [y]$, so $x \approx y$. Conversely, if $x \approx y$, then $x, y \in [z]$ for some z ; thus $x \sim z$ and $y \sim z$, and symmetry and transitivity give $x \sim y$. Hence $\approx$ and $\sim$ are the same relation. This proves the theorem.

So whenever you meet an equivalence relation, you may think of it as a way of cutting the set into nonoverlapping pieces, and vice versa. Exercise C2 uses this to count equivalence relations by counting partitions instead.

0.5.4 Quotient sets

Now we take the decisive step: treat each piece as a single new element. The time of day is the classic case. Hours counted from some starting moment are integers, but a clock only records the class of the hour modulo 12.

Definition 0.5.5. Quotient set

Let $\sim$ be an equivalence relation on X . The **quotient set** of X by $\sim$ is the set of all equivalence classes,

$$X/\sim := \{[x] : x \in X\}.$$

The function $\pi: X \rightarrow X/\sim$, $\pi(x) = [x]$, is the **quotient map**.

The elements of $X/\sim$ are sets, but once the quotient is formed we stop looking inside them and treat each class as a single point. The quotient map is surjective, since every class is $[x] = \pi(x)$ for some x . By [Lemma 0.5.1](#) (a), $\pi(x) = \pi(y)$ exactly when $x \sim y$: the quotient map makes equivalent elements literally equal.

Example. Quotient sets

- (a) For an integer $n \geq 1$, the quotient of $\mathbb{Z}$ by congruence modulo n is written $\mathbb{Z}/n\mathbb{Z}$. Show that it has exactly n elements, namely $[0], [1], \dots, [n-1]$.
- (b) Describe the quotient of the set S of strings in a, b by “same length”, and of $\mathbb{R}^2$ by “same distance from the origin”.

Solution.

- (a) Let $a \in \mathbb{Z}$. By division with remainder (Exercise (C2: Division with remainder)), $a = qn + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r \leq n-1$. Then $a - r = qn$, so $a \equiv r \pmod{n}$, and $[a] = [r]$ by [Lemma 0.5.1](#) (a). Hence every class is one of $[0], \dots, [n-1]$. These are distinct: if $0 \leq r < s \leq n-1$, then $0 < s - r < n$, so $s - r$ is not a multiple of n , hence $r \not\equiv s$ and $[r] \neq [s]$ by [Lemma 0.5.1](#) (a). So $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots, [n-1]\}$ has exactly n elements.
- (b) Two strings are identified exactly when they have the same length, so there is one class for each length $k \in \mathbb{N}$: the set of all 2^k strings of length k . Similarly, $\mathbb{R}^2$ modulo “same distance” has one class for each radius $r \in [0, \infty)$: the circle of radius r , or the origin when $r = 0$. In both cases the quotient is “the same as” the set of values $\mathbb{N}$ or $[0, \infty)$, and the next subsection makes that precise.

0.5.5 Functions on a quotient

We want to compute with classes. On a clock, “three hours after 11 o’clock” is 2 o’clock, which is really addition on $\mathbb{Z}/12\mathbb{Z}$. The natural way to define such an operation is through representatives: to add two classes, pick an element of each, add them, and take the class of the result. The danger is that a class has many representatives, and different choices might give different answers. When they do, the “definition” does not define a function at all.

Here is that failure in its simplest form.

Example. The numerator is not well defined

Let $P = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ with $(a, b) \sim (c, d)$ if $ad = bc$, as in [Example \(Equivalence relations\)](#) (e). Its classes are the rational numbers: the class of (a, b) is the fraction a/b , with all its other names. Is “ $[(a, b)] \mapsto a$ ” a function $P/\sim \rightarrow \mathbb{Z}$?

Solution. No. Since $1 \cdot 4 = 2 \cdot 2$, we have $(1, 2) \sim (2, 4)$, so $[(1, 2)] = [(2, 4)]$ by [Lemma 0.5.1](#) (a). The rule assigns to this one class the value 1 through one name and 2 through the other. So it does not assign **exactly one** value to each element of the domain, and Definition 0.4.1 fails. “The numerator of $\frac{1}{2}$ ” is a statement about how a fraction is written, not about the number.

By contrast, “ $[(a, b)] \mapsto 1$ if $a = 0$, and 0 otherwise” is fine. If $(a, b) \sim (c, d)$ and $a = 0$, then $bc = ad = 0$, so $c = 0$ because $b \neq 0$. By symmetry, $c = 0$ forces $a = 0$. So equivalent pairs always get the same value.

The contrast in that example is the whole story, and the following theorem turns it into a test. A function f on X passes to the quotient exactly when it cannot tell equivalent elements apart.

Theorem 0.5.3. Functions on a quotient

Let $\sim$ be an equivalence relation on X , let $\pi: X \rightarrow X/\sim$ be the quotient map, and let $f: X \rightarrow Y$ be a function.

- (a) If $f(a) = f(b)$ **whenever** $a \sim b$, then there is **exactly one** function $\bar{f}: X/\sim \rightarrow Y$ with $\bar{f}([x]) = f(x)$ for every $x \in X$, that is, $\bar{f} \circ \pi = f$.
- (b) Conversely, if some function $\bar{f}: X/\sim \rightarrow Y$ satisfies $\bar{f} \circ \pi = f$, then $f(a) = f(b)$ whenever $a \sim b$.

Idea. The formula $\bar{f}([x]) = f(x)$ leaves no freedom: if $\bar{f}$ exists, this is its value. The only question is whether the formula makes sense, since the class $C = [x]$ may also be called $[x']$. So look at **all** the values f takes on C at once, the image $f(C)$. A function needs exactly one value; $f(C)$ is nonempty because C is, and has at most one element because all elements of C are equivalent.

Proof.

- (a) Let $C \in X/\sim$. By [Definition 0.5.5](#), $C = [x]$ for some $x \in X$, so C is nonempty, and

hence the image $f(C)$ is nonempty. If $x', x'' \in C$, then $[x'] = C = [x'']$ by [Lemma 0.5.1](#) (a) applied to $x' \sim x$ and $x'' \sim x$; hence $x' \sim x''$ by the same lemma, and $f(x') = f(x'')$ by hypothesis. Therefore $f(C)$ has exactly one element, and we define $\bar{f}(C)$ to be that element. This assigns exactly one value to each class, so $\bar{f}$ is a function. For $x \in X$, we have $x \in [x]$ by reflexivity, so $\bar{f}([x]) \in f([x]) = \{f(x)\}$, that is, $\bar{f}([x]) = f(x)$.

For uniqueness, suppose $g: X/\sim \rightarrow Y$ also satisfies $g([x]) = f(x)$ for every x . Every class is $[x]$ for some x , and there $g([x]) = f(x) = \bar{f}([x])$. Hence $g = \bar{f}$.

- (b) Suppose $\bar{f} \circ \pi = f$ and $a \sim b$. By [Lemma 0.5.1](#) (a), $[a] = [b]$. Hence $f(a) = \bar{f}([a]) = \bar{f}([b]) = f(b)$, as claimed. ■

In practice we rarely name f and $\bar{f}$ separately. We write down a rule “ $[x] \mapsto (\text{expression in } x)$ ” and check that equivalent representatives give the same value. That check is what people mean when they say a function is **well defined**. For example, “same value” in [Example \(Equivalence relations\)](#) (d) satisfies the hypothesis by its very definition, so every $f: X \rightarrow Y$ induces a function $X/\sim_f \rightarrow Y$. This $\bar{f}$ is injective: $\bar{f}([x]) = \bar{f}([x'])$ means $f(x) = f(x')$, which is $x \sim_f x'$, so $[x] = [x']$. This makes precise the remark that $\mathbb{R}^2$ modulo “same distance” is “the same as” $[0, \infty)$: the induced map $[(x, y)] \mapsto \sqrt{x^2 + y^2}$ is a bijection onto $[0, \infty)$.

The most important application in this chapter is arithmetic modulo n . The operation takes two classes, so we check both representatives at once.

Example. Addition modulo n is well defined

Fix an integer $n \geq 1$. Show that the rule $[a] + [b] := [a + b]$ defines a function $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$. Then compute $[3] + [2]$ in $\mathbb{Z}/4\mathbb{Z}$.

Solution. We must show that the value $[a + b]$ depends only on the classes $[a]$ and $[b]$, not on the representatives a and b . Suppose $[a] = [a']$ and $[b] = [b']$. By [Lemma 0.5.1](#) (a), $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, so $a - a' = kn$ and $b - b' = \ell n$ for some $k, \ell \in \mathbb{Z}$. Then

$$(a + b) - (a' + b') = (a - a') + (b - b') = (k + \ell)n,$$

so $a + b \equiv a' + b' \pmod{n}$, and $[a + b] = [a' + b']$ by the same lemma. Hence every choice of representatives gives the same class, and the rule defines a function.

In $\mathbb{Z}/4\mathbb{Z}$, $[3] + [2] = [5] = [1]$, since $5 - 1 = 4$. Choosing other names gives the same answer, as it must: $[7] + [-2] = [5] = [1]$.

This is the same principle as [Theorem 0.5.3](#), applied to a function of two variables. The same check ([Exercise \(B3: Multiplication modulo \$n\$ \)](#)) shows multiplication $[a][b] := [ab]$ is well defined. With these operations, $\mathbb{Z}/p\mathbb{Z}$ for a prime p will become our first finite field later in this chapter, and the identical pattern, now with “ $v \sim w$ if $v - w \in U$ ”, will build quotient vector spaces in Chapter 4.

Warning. A rule written in terms of a representative is not automatically a function on classes. Define it, then check it. For example, “ $[a] \mapsto a$ ” from $\mathbb{Z}/5\mathbb{Z}$ to $\mathbb{Z}$ is not a function, because $[0] = [5]$ would be sent to both 0 and 5. The check is not a formality: forgetting it

is the most common error in any argument that uses quotients.

Quick check. Which of these rules defines a function? (i) $\mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z}$, $[a]_6 \mapsto [a]_3$. (ii) $\mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}$, $[a]_6 \mapsto [a]_4$. Here the subscript records the modulus.

Solution.

- (i) Yes. If $[a]_6 = [a']_6$, then $a - a' = 6k = 3(2k)$, so $[a]_3 = [a']_3$.
- (ii) No. $[0]_6 = [6]_6$, but $[0]_4 \neq [6]_4 = [2]_4$, since $6 - 0 = 6$ is not a multiple of 4. The first works because $3 \mid 6$; the second fails because $4 \nmid 6$.

0.5.6 Exercises

0.5.6.1 A. Check your understanding

Exercise. A1

- (a) State the three conditions for a relation $\sim$ on X to be an equivalence relation.
- (b) True or false: a symmetric and transitive relation is automatically reflexive. Give a reason.
- (c) True or false: if two equivalence classes $[a]$ and $[b]$ have an element in common, then $a \sim b$.
- (d) You want to define a function on $X/\sim$ by a formula in a representative x . What must you check?
- (e) How many elements does $\mathbb{Z}/5\mathbb{Z}$ have? Is $[12] = [-3]$ in $\mathbb{Z}/5\mathbb{Z}$?

Solution.

- (a) Reflexive: $x \sim x$ for every $x \in X$. Symmetric: $x \sim y$ implies $y \sim x$. Transitive: $x \sim y$ and $y \sim z$ imply $x \sim z$.
- (b) False. On $\mathbb{R}$, $x \sim y$ if $xy > 0$ is symmetric and transitive, but $0 \not\sim 0$; see [Example \(Relations that are not equivalence relations\)](#) (c) and the warning after it.
- (c) True. By [Lemma 0.5.1](#) (b) the classes are equal, and by part (a) of the same lemma $a \sim b$.
- (d) That equivalent representatives give the same value: if $x \sim x'$, the formula gives the same result for x and x' . By [Theorem 0.5.3](#) this is exactly what is needed.
- (e) Five, by [Example \(Quotient sets\)](#) (a). Yes: $12 - (-3) = 15 = 3 \cdot 5$, so $12 \equiv -3 \pmod{5}$, and both classes equal $[2]$.

0.5.6.2 B. Practice

Exercise. B1: Which are equivalence relations?

Determine which of the following are equivalence relations. For those that are, describe the equivalence classes. For those that are not, name a condition that fails with a specific witness.

- (a) On $\mathbb{Z}$: $a \sim b$ if $a + b$ is even.
- (b) On $\mathbb{Z}$: $a \sim b$ if $a - b$ is odd.
- (c) On $\mathbb{R}$: $x \sim y$ if $x - y \in \mathbb{Z}$.
- (d) On $\{1, 2, 3, \dots\}$: $m \sim n$ if m and n have a common divisor greater than 1.
- (e) On the set of all subsets of $\{1, 2, 3\}$: $A \sim B$ if A and B have the same number of elements.

Solution.

- (a) Equivalence relation. *Reflexive*: $a + a = 2a$ is even. *Symmetric*: $b + a = a + b$. *Transitive*: if $a + b$ and $b + c$ are even, then $a + c = (a + b) + (b + c) - 2b$ is a sum of even integers, hence even (Proposition 0.2.1). There are two classes: the even integers and the odd integers. (In fact $a + b$ is even exactly when $a - b = (a + b) - 2b$ is even, so this is congruence modulo 2.)
- (b) Not an equivalence relation. Reflexivity fails: $0 - 0 = 0$ is even, so $0 \not\sim 0$. (Transitivity also fails: $0 \sim 1$ and $1 \sim 2$, but $0 - 2$ is even.)
- (c) Equivalence relation. *Reflexive*: $x - x = 0 \in \mathbb{Z}$. *Symmetric*: if $x - y = k \in \mathbb{Z}$, then $y - x = -k \in \mathbb{Z}$. *Transitive*: if $x - y = k$ and $y - z = \ell$ with $k, \ell \in \mathbb{Z}$, then $x - z = k + \ell \in \mathbb{Z}$. The class of x is $\{x + k : k \in \mathbb{Z}\}$, the points at integer distance from x in either direction. Each class contains exactly one number in $[0, 1)$, namely $x - \lfloor x \rfloor$.
- (d) Not an equivalence relation. Reflexivity fails at 1: the only positive divisor of 1 is 1. Transitivity also fails: $2 \sim 6$ (common divisor 2) and $6 \sim 3$ (common divisor 3), but 2 and 3 have no common divisor greater than 1.
- (e) Equivalence relation, since it is “same value” (Example (Equivalence relations) (d)) for the function $A \mapsto |A|$. There are four classes: $\{\emptyset\}$; $\{\{1\}, \{2\}, \{3\}\}$; $\{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$; $\{\{1, 2, 3\}\}$.

Exercise. B2: Parallel lines as classes

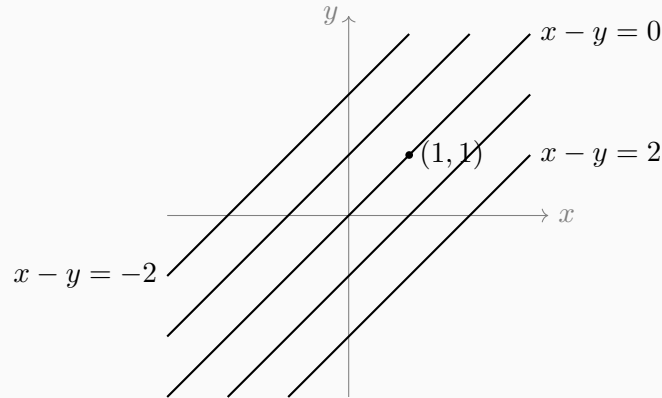
On $\mathbb{R}^2$, define $(x, y) \sim (x', y')$ if $x - y = x' - y'$.

- (a) Prove that $\sim$ is an equivalence relation.
- (b) Describe the class of (x_0, y_0) geometrically, and draw several classes.
- (c) Show that $[(x, y)] \mapsto x - y$ is a well-defined function $\mathbb{R}^2/\sim \rightarrow \mathbb{R}$, and that it is a bijection.

Solution.

- (a) This is “same value” for $f: \mathbb{R}^2 \rightarrow \mathbb{R}$, $f(x, y) = x - y$, so it is an equivalence relation by Example (Equivalence relations) (d). Directly: $x - y = x' - y'$; equality of the numbers $x - y$ and $x' - y'$ is symmetric and transitive.
- (b) Put $c = x_0 - y_0$. Then $[(x_0, y_0)] = \{(x, y) \in \mathbb{R}^2 : x - y = c\} = \{(x, y) : y = x - c\}$, the line of slope 1 through (x_0, y_0) , which meets the y -axis at $(0, -c)$. The classes are

all the lines parallel to $y = x$: each point of the plane lies on exactly one of them, as [Theorem 0.5.2](#) predicts.



- (c) Let $f(x, y) = x - y$. If $(x, y) \sim (x', y')$, then $f(x, y) = f(x', y')$ by the definition of $\sim$. By [Theorem 0.5.3](#) (a), there is a function $\bar{f}: \mathbb{R}^2/\sim \rightarrow \mathbb{R}$ with $\bar{f}([(x, y)]) = x - y$.

Injective. Suppose $\bar{f}([(x, y)]) = \bar{f}([(x', y')])$. Then $x - y = x' - y'$, so $(x, y) \sim (x', y')$, and $[(x, y)] = [(x', y')]$ by [Lemma 0.5.1](#) (a).

Surjective. Let $c \in \mathbb{R}$. Then $\bar{f}([(c, 0)]) = c - 0 = c$.

Hence $\bar{f}$ is a bijection: the set of parallel lines is labeled, one to one, by the real number c .

Exercise. B3: Multiplication modulo n

Fix an integer $n \geq 1$.

- Prove that $[a][b] := [ab]$ is a well-defined operation on $\mathbb{Z}/n\mathbb{Z}$.
- Write out the multiplication table of $\mathbb{Z}/4\mathbb{Z}$, using the representatives 0, 1, 2, 3.
- Hence find a class $[a] \neq [0]$ in $\mathbb{Z}/4\mathbb{Z}$ with $[a][a] = [0]$.

Solution.

- (a) Suppose $[a] = [a']$ and $[b] = [b']$. By [Lemma 0.5.1](#) (a), $a - a' = kn$ and $b - b' = \ell n$ for some $k, \ell \in \mathbb{Z}$. Then

$$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') = (kb + a'\ell)n,$$

so $ab \equiv a'b' \pmod{n}$ and $[ab] = [a'b']$ by the same lemma. Hence the value does not depend on the representatives, and the operation is well defined.

- (b) Reducing each product modulo 4:

$\cdot$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

For instance $[2][3] = [6] = [2]$ and $[3][3] = [9] = [1]$.

- (c) From the table, $[2][2] = [4] = [0]$, while $[2] \neq [0]$ since $4 \nmid 2$. So a product of nonzero classes can be zero in $\mathbb{Z}/4\mathbb{Z}$, something that never happens with ordinary numbers.

0.5.6.3 C. Going deeper

Exercise. C1: Squares and powers modulo n

- (a) Let $n \geq 1$. Prove that $[x] \mapsto [x^2]$ is a well-defined function $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$.
- (b) On $\mathbb{N}$, let $\equiv_3$ be congruence modulo 3. Show that the rule $[x] \mapsto [2^x]_3$ does **not** define a function from $\mathbb{N}/\equiv_3$ to $\mathbb{Z}/3\mathbb{Z}$.
- (c) On $\mathbb{N}$, let $\equiv_2$ be congruence modulo 2. Prove that $[x] \mapsto [2^x]_3$ **does** define a function from $\mathbb{N}/\equiv_2$ to $\mathbb{Z}/3\mathbb{Z}$.

Hint for (c): compute 2^2 modulo 3.

Solution.

- (a) Suppose $[x] = [x']$. By [Exercise \(B3: Multiplication modulo \$n\$ \)](#) (a) with $a = b = x$ and $a' = b' = x'$, we get $[x][x] = [x'][x']$, that is, $[x^2] = [x'^2]$. Hence the value depends only on the class, and the function is well defined.
- (b) In $\mathbb{N}$, $0 \equiv 3 \pmod{3}$, so $[0] = [3]$. The rule sends this class to $[2^0]_3 = [1]_3$ through the representative 0, and to $[2^3]_3 = [8]_3 = [2]_3$ through the representative 3. Since $8 - 1 = 7$ is not a multiple of 3, $[1]_3 \neq [2]_3$. So one class receives two different values, and the rule is not a function.
- (c) By [Theorem 0.5.3](#) (a), it suffices to show that $x \equiv x' \pmod{2}$ implies $2^x \equiv 2^{x'} \pmod{3}$. By symmetry of both relations we may assume $x \leq x'$, so $x' = x + 2k$ with $k \in \mathbb{N}$. First, $4^k \equiv 1 \pmod{3}$ for every $k \in \mathbb{N}$, by induction on k (Theorem 0.2.7): $4^0 = 1$, and if $4^k - 1 = 3m$, then $4^{k+1} - 1 = 4(4^k - 1) + 3 = 3(4m + 1)$. Hence

$$2^{x'} - 2^x = 2^x(4^k - 1)$$

is a multiple of 3, so $[2^{x'}]_3 = [2^x]_3$, as claimed. The difference between (b) and (c) is that the powers of 2 modulo 3 repeat with period 2, and 3 is not a multiple of 2.

Exercise. C2: Counting equivalence relations

- (a) List all partitions of $\{1, 2, 3\}$.
- (b) Hence deduce that there are exactly 5 equivalence relations on $\{1, 2, 3\}$.
- (c) Write the equivalence relation corresponding to the partition $\{\{1, 3\}, \{2\}\}$ as a subset of $\{1, 2, 3\} \times \{1, 2, 3\}$.

Solution.

- (a) Sort by the number of blocks. One block: $\{\{1, 2, 3\}\}$. Two blocks: one block is a single element and the other the remaining pair, giving $\{\{1\}, \{2, 3\}\}$, $\{\{2\}, \{1, 3\}\}$, $\{\{3\}, \{1, 2\}\}$. Three blocks: $\{\{1\}, \{2\}, \{3\}\}$. Four or more nonempty disjoint blocks

are impossible in a three-element set. That is 5 partitions.

- (b) By [Theorem 0.5.2](#) (a), every equivalence relation gives a partition, its set of classes. By [Theorem 0.5.2](#) (c), the relation can be recovered from that partition, so distinct equivalence relations give distinct partitions. By [Theorem 0.5.2](#) (b), every partition arises this way. Hence equivalence relations on $\{1, 2, 3\}$ correspond one to one with partitions, and there are exactly 5 of them.
- (c) Two elements are related exactly when they lie in a common block:

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

Exercise. C3: Intersections and unions of equivalence relations

Let R_1 and R_2 be equivalence relations on a set X , viewed as subsets of $X \times X$.

- (a) Prove that $R_1 \cap R_2$ is an equivalence relation on X .
- (b) Show by an example that $R_1 \cup R_2$ need not be an equivalence relation. Which condition fails?
- (c) For congruence modulo 2 and modulo 3 on $\mathbb{Z}$, identify $R_1 \cap R_2$ as a familiar relation.

Hint for (b): try congruence modulo 2 and modulo 3 on $\mathbb{Z}$.

Solution.

- (a) *Reflexive.* Let $x \in X$. Then $(x, x) \in R_1$ and $(x, x) \in R_2$, since both are reflexive, so $(x, x) \in R_1 \cap R_2$. *Symmetric.* Suppose $(x, y) \in R_1 \cap R_2$. Since R_1 and R_2 are symmetric, $(y, x) \in R_1$ and $(y, x) \in R_2$, so $(y, x) \in R_1 \cap R_2$. *Transitive.* Suppose $(x, y), (y, z) \in R_1 \cap R_2$. Both pairs lie in R_1 , which is transitive, so $(x, z) \in R_1$; likewise $(x, z) \in R_2$. Hence $(x, z) \in R_1 \cap R_2$.
- (b) Let R_1 be congruence modulo 2 and R_2 congruence modulo 3 on $\mathbb{Z}$. The union is still reflexive and symmetric, since each of R_1, R_2 is. But transitivity fails: $(0, 2) \in R_1$ since $2 \mid 2$, and $(2, 5) \in R_2$ since $3 \mid 3$, yet $(0, 5)$ lies in neither, because 5 is not a multiple of 2 or of 3.
- (c) $(a, b) \in R_1 \cap R_2$ means $2 \mid a - b$ and $3 \mid a - b$. This holds exactly when $6 \mid a - b$. Indeed, if $a - b = 2k$ and $a - b = 3m$ with $k, m \in \mathbb{Z}$, then $a - b = 3(a - b) - 2(a - b) = 3 \cdot 2k - 2 \cdot 3m = 6(k - m)$. Conversely, if $a - b = 6j$, then $a - b = 2(3j) = 3(2j)$. So $R_1 \cap R_2$ is congruence modulo 6. The same phenomenon, where intersections behave well and unions do not, will reappear for subspaces in Chapter 1.