

2.5 Equivalence Relations and Partitions

Section 2.4 sorted relations by four properties: reflexive, symmetric, antisymmetric and transitive (Definition 2.4.1). This section studies the relations that have the first, second and fourth. They are the relations that say two things are “the same” in some respect, and each of them cuts its set into disjoint pieces of mutually “same” elements. We prove that the pieces always form a partition, and that every partition arises from exactly one such relation. Then we build the integers modulo n , and meet the check that every definition on pieces needs: that it does not depend on which element names the piece. Section 1.4 promised that check for functions defined on classes; here it is.

2.5.1 Arithmetic on a clock

On a twelve-hour clock, five hours after nine o'clock it is two o'clock. People say “ $9 + 5 = 2$ on a clock”, and nobody is confused. Read as a statement about integers, it is false: $9 + 5 = 14$. So what is it a statement about?

The clock does not distinguish 2 from 14, or from 26 or -10 : all of them put the hand in the same place. Two integers name the same hour when they differ by a multiple of 12. The sentence “ $9 + 5 = 2$ ” is then about hours, and an hour is not one integer but a whole collection of them, $\{\dots, -10, 2, 14, 26, \dots\}$. The addition adds collections: take any integer from the first, any from the second, add them, and see which collection the sum lands in.

Two things have to be checked before this is mathematics. First, “differ by a multiple of 12” must behave like “is the same as”: it must cut the integers into separate collections, and no integer may land in two of them. Second, the answer must not depend on the choice: if we take 21 for “nine” and -7 for “five”, the sum 14 must still name two o'clock. It does, since $21 + (-7) = 14$. The first check is the theory of equivalence relations and partitions. The second is called **well-definedness**, and it comes at the end of the section.

2.5.2 Equivalence relations

Equality has three properties that every argument with “=” uses silently: $x = x$; if $x = y$, then $y = x$; and if $x = y$ and $y = z$, then $x = z$ (Logic and Proof, Proposition 5.7.1). They are exactly what lets us replace a thing by an equal thing, as often as we like, in either direction. “Same hour on the clock”, “same remainder on division by 3” and “same absolute value” all have the same three properties, although none of them is equality. They deserve a common name.

An equivalence relation declares things the same in a way that behaves like equality.

Definition 2.5.1. Equivalence Relation

Let X be a set. An **equivalence relation on X** is a relation $\sim$ on X (Definition 1.3.3) that is reflexive, symmetric and transitive on X (Definition 2.4.1):

(Eq1) **for every** $x \in X$, $x \sim x$;

(Eq2) **for all** $x, y \in X$, if $x \sim y$, then $y \sim x$;

(Eq3) **for all** $x, y, z \in X$, if $x \sim y$ and $y \sim z$, then $x \sim z$.

When $x \sim y$, we say that x is **equivalent** to y (under $\sim$).

In words: (Eq1) says everything is the same as itself. (Eq2) says “the same” has no direction:

if x counts as the same as y , then y counts as the same as x . (Eq3) says sameness passes along a chain: two things that are each the same as a third are linked through it. In symbols, (Eq1)–(Eq3) are

$$\begin{aligned}\forall x \in X \quad x \sim x, \quad \forall x, y \in X \quad (x \sim y \rightarrow y \sim x), \\ \forall x, y, z \in X \quad ((x \sim y \wedge y \sim z) \rightarrow x \sim z).\end{aligned}$$

The symbol $\sim$ is a letter for a relation, like R in Section 2.4; it is written between its arguments because it is read like $=$. Nothing needs checking for well-definedness: the definition names a property of a set of pairs.

Example. Four equivalence relations

Check (Eq1)–(Eq3) for each relation.

- (a) Equality on any set X : $x \sim y$ if and only if $x = y$.
- (b) The relation $X \times X$ on a set X , which relates every x to every y .
- (c) “Same absolute value” on $\mathbb{R}$: $x \sim y$ if and only if $|x| = |y|$.
- (d) The empty relation $\emptyset$ on the empty set.

Solution.

- (a) (Eq1)–(Eq3) are the three properties of equality recalled above: $x = x$ is $=I$, and symmetry and transitivity are Logic and Proof, Proposition 5.7.1.
- (b) Every pair (x, y) with $x, y \in X$ lies in $X \times X$, so each of (Eq1)–(Eq3) has a conclusion of the form $(u, v) \in X \times X$ with $u, v \in X$, and that conclusion is true. This is the coarsest sameness: everything is the same as everything.
- (c) Each of (Eq1)–(Eq3) for $\sim$ is the same property for equality, applied to the numbers $|x|, |y|, |z|$. For instance, (Eq3): if $|x| = |y|$ and $|y| = |z|$, then $|x| = |z|$ by transitivity of $=$. Here $3 \sim -3$, and $3 \not\sim 2$.
- (d) Each of (Eq1)–(Eq3) begins “for every element of X ”, and $X = \emptyset$ has none, so all three hold vacuously. The empty relation **is** an equivalence relation on $\emptyset$.

Part (d) is the degenerate case, and it is worth keeping: it says that the definition makes no demand on an empty set, so the theorems below hold for $X = \emptyset$ without a separate case. On a **non-empty** set the empty relation is not an equivalence relation: (Eq1) fails at any element x , since $(x, x) \notin \emptyset$. The same set of pairs passes on one set and fails on another, because (Eq1) speaks about every element of X .

Part (c) is an instance of a pattern that returns later in this section, with the fibers of a function: “ $x \sim y$ when some quantity attached to x equals the same quantity attached to y ”. Any such relation inherits (Eq1)–(Eq3) from equality.

A non-example by minimal change. On $\mathbb{R}$, let $x \sim y$ mean $x - y \in \mathbb{Z}$, and let $x R y$ mean $x - y \in \mathbb{N}$. The first is an equivalence relation, as an example later in this section checks. The second changes one letter. It is still reflexive, since $x - x = 0 \in \mathbb{N}$ by $((\mathbb{N})0)$, and still transitive: if $x - y \in \mathbb{N}$ and $y - z \in \mathbb{N}$, then $x - z = (x - y) + (y - z) \in \mathbb{N}$ by Lemma 2.1.1 (b). But it is not symmetric: $1 R 0$, since $1 - 0 = 1 \in \mathbb{N}$, while $0 - 1 = -1$, and $-1 \notin \mathbb{N}$ because every natural number is ≥ 0 (Lemma 2.1.1 (a)). The clause that fails is (Eq2). The relation R is the order $y \leq x$ restricted to pairs at integer distance; it has a direction, and sameness has none.

Why these three clauses. Each clause has a job, and each failure has a witness.

- Drop (Eq1), and an element may be the same as nothing at all. On $\{1\}$, the empty relation is symmetric and transitive (Section 2.4’s warning), and 1 is related to nothing; it would sit in no piece of the cutting.
- Drop (Eq2), and the pieces overlap. The relation $\leq$ on $\{1, 2\}$ is reflexive and transitive; the set of elements below 2 is $\{1, 2\}$, the set below 1 is $\{1\}$, and the two share 1 without being equal.
- Drop (Eq3), and sameness leaks. “ $|x - y| \leq 1$ ” on $\mathbb{R}$ is reflexive and symmetric, and 0 is related to 1, 1 to 2, 2 to 3, and so on, while 0 is not related to 2. Every integer is linked to every other through a chain of steps of length 1, though few are related directly.

The name comes from “equal value”: equivalent elements are equal in whatever respect the relation measures.

Warning. An equivalence relation is an equivalence relation **on a named set**. The relation $\{(1, 1), (2, 2)\}$ is equality on $\{1, 2\}$, an equivalence relation; on $\{1, 2, 3\}$ it is the same set of pairs and not an equivalence relation, since $(3, 3)$ is missing and (Eq1) fails at 3. Before checking (Eq1), name the set.

The payoff is the object the clock was after: the collection of everything that counts as the same as a given element.

2.5.3 Equivalence classes

An equivalence class is everything that counts as the same as one element.

Definition 2.5.2. Equivalence Class

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

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

When the relation must be named, we write $[a]_\sim$. Any element of a class is called a **representative** of it.

The class is a subset of X , by specification (Definition 1.1.3). Its definition fixes the order of the letters as $x \sim a$; by (Eq2) the order does not matter, and $x \in [a]$ holds exactly when $a \sim x$.

For the four relations of [Example \(Four equivalence relations\)](#): under equality, $[a] = \{a\}$; under $X \times X$, $[a] = X$ for every $a \in X$; under “same absolute value”, $[3] = \{-3, 3\}$ and $[0] = \{0\}$; and on the empty set there are no elements and so no classes.

Quick check. On $\{1, 2, \dots, 30\}$, let $x \sim y$ mean that x and y have the same last digit. List the classes. How many are there, and how many elements has each?

Solution. The classes are $\{1, 11, 21\}$, $\{2, 12, 22\}$, $\dots$, $\{9, 19, 29\}$ and $\{10, 20, 30\}$: ten classes,

three elements each. Each class is the class of any of its elements; for instance $[11] = [21] = [1]$.

The quick check shows the features the theorem below proves in general: every class is non-empty, no number is in two classes, and every number is in one. A family of subsets with these three features has a name.

Definition 2.5.3. Partition

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

- (P1) every block is **non-empty**: $P \neq \emptyset$ for every $P \in \mathcal{P}$;
- (P2) the blocks are **pairwise disjoint**: for all $P, Q \in \mathcal{P}$, if $P \neq Q$, then $P \cap Q = \emptyset$;
- (P3) the blocks cover X : $\bigcup \mathcal{P} = X$.

Here $\bigcup \mathcal{P}$ is the union of the set of sets $\mathcal{P}$ (Definition 1.2.4): the set of points lying in some block. Since every block is a subset of X , the union is always a subset of X , and (P3) says that every $x \in X$ lies in **some** block. With (P2), it lies in **exactly one**: if $x \in P$ and $x \in Q$, then $P \cap Q \neq \emptyset$, so $P = Q$.

Examples: $\{\{1, 2\}, \{3\}\}$ is a partition of $\{1, 2, 3\}$. For a non-empty X , $\{X\}$ is a partition with one block, and $\{\{x\} : x \in X\}$ is one with a block for each point. The even and the odd integers form a partition of $\mathbb{Z}$ with two blocks, because every integer is even or odd and not both (Theorem 2.2.3 with $n = 2$). For $X = \emptyset$, the empty set of blocks $\mathcal{P} = \emptyset$ is a partition: (P1) and (P2) are vacuous, and $\bigcup \emptyset = \emptyset$.

Non-examples by minimal change. $\{\{1, 2\}, \{2, 3\}\}$ covers $\{1, 2, 3\}$ and its sets are non-empty, but 2 lies in both, so (P2) fails. $\{\{1, 2\}, \{3\}, \emptyset\}$ satisfies (P2) and (P3), and fails (P1). Without (P1), “the block containing x ” would still be unique, but a partition could carry useless empty blocks, and the correspondence with equivalence relations below would break, since no class is empty.

A partition is a set of subsets of X . So is the set of all classes of an equivalence relation, and it gets its own name.

Definition 2.5.4. Quotient Set

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

$$X/\sim := \{C \in \mathcal{P}(X) : C = [a] \text{ for some } a \in X\}.$$

The **quotient map** is $q: X \rightarrow X/\sim$, $q(a) := [a]$.

The quotient set is a set by specification inside $\mathcal{P}(X)$ (Definition 1.1.3, Definition 1.2.2), and it is often written $\{[a] : a \in X\}$. The quotient map is a function by Definition 1.4.1: each $a \in X$ has the value $[a]$, which lies in $X/\sim$, and only that value. It is **surjective**: an element of $X/\sim$ is $[a]$ for some $a \in X$, and then it is $q(a)$ (Definition 1.4.4). The quotient map forgets everything about a except which class it lies in, and that is the point of it. Read “ $X/\sim$ ” as “ X with equivalent elements identified”.

2.5.4 The classes form a partition

Here is the theorem the clock needs. It also says exactly when two names give the same class.

Theorem 2.5.1. Equivalence Classes Partition the Set

Let $\sim$ be an equivalence relation on a set X .

- (a) For every $a \in X$, $a \in [a]$; in particular every class is non-empty.
- (b) For all $a, b \in X$, $[a] = [b]$ **if and only if** $a \sim b$.
- (c) For all $a, b \in X$, if $[a] \cap [b] \neq \emptyset$, then $[a] = [b]$.
- (d) The quotient set $X/\sim$ is a partition of X .

Idea. Each property of $\sim$ does one job. Reflexivity puts a in its own class, which gives (a) and the covering. For (b), a class is determined by any one of its elements: if $a \sim b$, then anything the same as a is the same as b , by transitivity, and the reverse needs symmetry first. For (c), a common element c of two classes has $c \sim a$ and $c \sim b$; symmetry turns the first around, transitivity joins the two, and (b) finishes. Then (d) is (a), (c) and the covering, read against the three clauses of [Definition 2.5.3](#).

Before reading on: which property of $\sim$ does each line use?

Proof. (a) Let $a \in X$. By (Eq1), $a \sim a$, so $a \in [a]$ by [Definition 2.5.2](#). Hence $[a] \neq \emptyset$.

(b) ($\Rightarrow$) Suppose $[a] = [b]$. By (a), $a \in [a] = [b]$, so $a \sim b$.

($\Leftarrow$) Suppose $a \sim b$. ($\subseteq$) Let $x \in [a]$, so $x \sim a$. With $a \sim b$, (Eq3) gives $x \sim b$, so $x \in [b]$. ($\supseteq$) Let $x \in [b]$, so $x \sim b$. By (Eq2) applied to $a \sim b$, $b \sim a$; with $x \sim b$, (Eq3) gives $x \sim a$, so $x \in [a]$. Hence $[a] = [b]$ by Proposition 1.1.1.

(c) Suppose $[a] \cap [b] \neq \emptyset$, and let $c \in [a] \cap [b]$. Then $c \sim a$ and $c \sim b$. By (Eq2), $a \sim c$; with $c \sim b$, (Eq3) gives $a \sim b$. By (b), $[a] = [b]$.

(d) We check the clauses of [Definition 2.5.3](#) for $\mathcal{P} := X/\sim$, a set of subsets of X by [Definition 2.5.4](#).

(P1) Every element of $X/\sim$ is $[a]$ for some $a \in X$, and is non-empty by (a).

(P2) Let $C, D \in X/\sim$ with $C \neq D$, say $C = [a]$ and $D = [b]$. If $C \cap D \neq \emptyset$, then $C = D$ by (c), which is false. Hence $C \cap D = \emptyset$.

(P3) Every class is a subset of X , so $\bigcup X/\sim \subseteq X$. Conversely, let $x \in X$. Then $x \in [x]$ by (a), and $[x] \in X/\sim$, so $x \in \bigcup X/\sim$. Hence $\bigcup X/\sim = X$ by Proposition 1.1.1.

This proves the theorem. ■

Part (b) is the rule we will use most. It turns a statement about classes, $[a] = [b]$, into a statement about elements, $a \sim b$, and back. On the clock: $[14] = [2]$ because $14 - 2 = 12$ is a multiple of 12. By (b), the quotient map q of [Definition 2.5.4](#) has $q(a) = q(b)$ exactly when

$a \sim b$. So q is injective only when every class has a single element: two different elements x, y of one class $[c]$ have $[x] = [c] = [y]$ by (b), so $q(x) = q(y)$. Part (c) says that two classes are either equal or disjoint; there is no third possibility. That is what the relations of “Why these three clauses” lacked: for $\leq$, the sets $[2] = \{1, 2\}$ and $[1] = \{1\}$ given by the formula of [Definition 2.5.2](#) overlap and differ, and with $a = 2$, $b = 1$, $c = 1$ the line of (c) that fails is the one that uses (Eq2) (Exercise A1(c)).

Warning. A class has many names. In the quick check, $[1]$, $[11]$ and $[21]$ are one set, and nothing about that set prefers 1. So any argument or definition that starts from “ $[a]$ ” and then uses a itself (its size, its sign, its last digit) must be shown not to depend on which representative was chosen. “The smallest element of $[a]$ ” makes sense for the last-digit classes; “ $[a+1]$ ” as a function of the class $[a]$ needs a proof, which the section supplies for congruences under “Operations on classes”.

2.5.5 Every partition comes from one equivalence relation

The theorem turns an equivalence relation into a partition. The reverse is just as natural: given the blocks, call two points “the same” when they lie in a common block.

Theorem 2.5.2. Partitions and Equivalence Relations Correspond

Let X be a set.

- (a) Let $\mathcal{P}$ be a partition of X . For $x, y \in X$, let $x \sim_{\mathcal{P}} y$ mean that there is a block $P \in \mathcal{P}$ with $x \in P$ and $y \in P$. Then $\sim_{\mathcal{P}}$ is an equivalence relation on X , and its classes are the blocks: $X/\sim_{\mathcal{P}} = \mathcal{P}$.
- (b) Let $\sim$ be an equivalence relation on X . Then $\sim_{X/\sim}$, the relation of (a) for the partition $X/\sim$, is $\sim$ itself.
- (c) Hence every partition of X is the quotient set of **exactly one** equivalence relation on X , namely $\sim_{\mathcal{P}}$.

Idea. For (a), (Eq1) and (Eq2) are immediate from (P3) and the symmetry of “lie in a common block”. The real work is (Eq3): x, y lie in one block and y, z in another, and we need one block holding x and z . The two blocks share y , so (P2) makes them equal. The classes are the blocks because each point lies in exactly one block. Then (b) is [Theorem 2.5.1](#) (b) in disguise, and (c) puts (a) and (b) together.

Proof. (a) (Eq1) Let $x \in X$. By (P3), $x \in \bigcup \mathcal{P}$, so $x \in P$ for some $P \in \mathcal{P}$; this block contains x and x , so $x \sim_{\mathcal{P}} x$. (Eq2) If a block contains x and y , it contains y and x . (Eq3) Let $x \sim_{\mathcal{P}} y$ and $y \sim_{\mathcal{P}} z$. Take a block P with $x, y \in P$, and a block Q with $y, z \in Q$. Then $y \in P \cap Q$, so $P \cap Q \neq \emptyset$, and $P = Q$ by (P2). Hence $x, z \in P$, and $x \sim_{\mathcal{P}} z$.

Now the classes. Let $x \in X$, and let P be a block with $x \in P$ (one exists by (P3)). We show $[x] = P$, the class taken under $\sim_{\mathcal{P}}$. ($\subseteq$) Let $y \in [x]$, so $y \sim_{\mathcal{P}} x$: some block Q contains y and x . Then $x \in P \cap Q$, so $Q = P$ by (P2), and $y \in P$. ($\supseteq$) Let $y \in P$. Then P contains y and

x , so $y \sim_{\mathcal{P}} x$, and $y \in [x]$.

So every class is a block: $[x]$ is the block containing x . Conversely, every block P is non-empty by (P1); for any $x \in P$, the argument just given shows $P = [x]$. Hence $X/\sim_{\mathcal{P}} = \mathcal{P}$, each inclusion being one of the last two sentences.

(b) Both relations are subsets of $X \times X$, so we show that they contain the same pairs (Definition 1.1.1). Let $x, y \in X$. If $x \sim y$, then the class $[y] \in X/\sim$ contains y by Theorem 2.5.1 (a) and, by Definition 2.5.2, x ; so $x \sim_{X/\sim} y$. Conversely, if $x \sim_{X/\sim} y$, some class $[a]$ contains x and y , so $x \sim a$ and $y \sim a$. By (Eq2), $a \sim y$, and by (Eq3), $x \sim y$.

(c) By (a), $\mathcal{P}$ is the quotient set of $\sim_{\mathcal{P}}$. Suppose $\mathcal{P} = X/\sim$ for an equivalence relation $\sim$. Then, by (b), $\sim$ is $\sim_{X/\sim}$, the relation of (a) for the partition $X/\sim = \mathcal{P}$; that is, $\sim$ is $\sim_{\mathcal{P}}$. So there is exactly one such relation. This proves the theorem. ■

So the two passages undo each other. Going from $\sim$ to $X/\sim$ and back gives $\sim$ again, by (b); going from $\mathcal{P}$ to $\sim_{\mathcal{P}}$ and back gives $\mathcal{P}$ again, by (a). An equivalence relation and a partition are two descriptions of one structure: the relation says which pairs are the same, and the partition lists the piles. This is the move *classes from a relation, a relation from classes*, and we choose whichever description makes the next step easier.

The transitivity step in (a) is where (P2) does its real work (the classes part uses it again, the same way), and it is the step that a hasty proof skips. If the blocks were allowed to overlap, as in the cover $\{\{1, 2\}, \{2, 3\}\}$ of $\{1, 2, 3\}$, then “lie in a common set” would relate 1 to 2 and 2 to 3 but not 1 to 3.

2.5.6 Congruence modulo n

Back to the clock, with any number of hours. The divisibility notation $d \mid m$, “there is $k \in \mathbb{Z}$ with $m = kd$ ”, is Definition 2.2.1.

Definition 2.5.5. Congruence Modulo n

Let $n \in \mathbb{Z}_{>0}$. Integers a and b are **congruent modulo n** , written $a \equiv b \pmod{n}$, if $n \mid a - b$, that is, if $a - b = kn$ for some $k \in \mathbb{Z}$.

So $14 \equiv 2 \pmod{12}$, since $14 - 2 = 1 \cdot 12$; $-10 \equiv 2 \pmod{12}$, since $-10 - 2 = (-1) \cdot 12$; and $7 \not\equiv 2 \pmod{12}$, since 5 is not a multiple of 12 (the multiples $12k$ are 0 for $k = 0$, at least 12 for $k \geq 1$ and at most -12 for $k \leq -1$, by discreteness, Proposition 2.1.2 (c)). The symbol $\equiv$ here always carries its modulus, so it does not clash with the semantic equivalence $\varphi \equiv \psi$ of *Logic and Proof*, Chapter 4.

Remark. Why $n \geq 1$? The condition makes sense for $n = 0$, but it says nothing new: $0 \mid a - b$ means $a - b = k \cdot 0 = 0$, so “congruence modulo 0” is equality on $\mathbb{Z}$. Its classes would be the singletons $\{a\}$, a copy of $\mathbb{Z}$ and not $\mathbb{Z}$ itself, and the count of classes proved below would fail. Excluding $n = 0$ keeps that count exact.

Proposition 2.5.3. Congruence Is an Equivalence Relation

For every $n \in \mathbb{Z}_{>0}$, congruence modulo n is an equivalence relation on $\mathbb{Z}$.

Proof. (Eq1) $a - a = 0 = 0 \cdot n$, and $0 \in \mathbb{Z}$. (Eq2) If $a - b = kn$ with $k \in \mathbb{Z}$, then $b - a = (-k)n$, and $-k = 0 - k \in \mathbb{Z}$ by Proposition 2.1.2 (a). (Eq3) If $a - b = kn$ and $b - c = ln$ with $k, l \in \mathbb{Z}$, then $a - c = (a - b) + (b - c) = (k + l)n$, and $k + l \in \mathbb{Z}$ by Proposition 2.1.2 (a). ■

The quotient set is written $\mathbb{Z}/n$, “the integers modulo n ”. Its elements are the **residue classes** $[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\} = \{a + kn : k \in \mathbb{Z}\}$; the second form holds because $x \equiv a$ means $x - a = kn$, that is, $x = a + kn$. When two moduli are in play we write $[a]_n$ for the class of a in $\mathbb{Z}/n$. For example, $[2]_{12} = \{\dots, -22, -10, 2, 14, 26, \dots\}$, the integers that name two o’clock.

How many classes are there? The clock has twelve positions, and the division algorithm says why: each integer has exactly one remainder among $0, 1, \dots, 11$.

Proposition 2.5.4. The Integers Modulo n

Let $n \in \mathbb{Z}_{>0}$. For every $a \in \mathbb{Z}$ there is **exactly one** $r \in \{0, \dots, n - 1\}$ with $[a] = [r]$ in $\mathbb{Z}/n$, namely the remainder of a on division by n . Hence

$$\mathbb{Z}/n = \{[0], [1], \dots, [n - 1]\},$$

and the n classes listed are pairwise different.

Here $n - 1 \in \mathbb{N}$ by Lemma 2.1.1 (c), since $n \neq 0$, so $\{0, \dots, n - 1\}$ is the set of Section 2.1.

Proof. Let $a \in \mathbb{Z}$. By Theorem 2.2.3 there are $q, r \in \mathbb{Z}$ with $a = qn + r$ and $0 \leq r < n$. Since $r \geq 0$, $r \in \mathbb{N}$ (Proposition 2.1.2 (b)); since $r < n$, $r + 1 \leq n$ by discreteness (Proposition 2.1.2 (c)), so $r \leq n - 1$. Hence $r \in \{0, \dots, n - 1\}$. Also $a - r = qn$, so $a \equiv r \pmod{n}$, and $[a] = [r]$ by Theorem 2.5.1 (b).

For uniqueness, let $r, s \in \{0, \dots, n - 1\}$ with $[a] = [r]$ and $[a] = [s]$. Then $[r] = [s]$, so $r \equiv s \pmod{n}$ by Theorem 2.5.1 (b): $r - s = kn$ for some $k \in \mathbb{Z}$. So the integer r can be written both as $r = 0 \cdot n + r$ and as $r = kn + s$, and both remainders r and s satisfy $0 \leq r, s < n$. By the uniqueness in Theorem 2.2.3, $s = r$.

Finally, every element of $\mathbb{Z}/n$ is $[a]$ for some $a \in \mathbb{Z}$, hence equal to one of $[0], \dots, [n - 1]$; and if $[r] = [s]$ with $r, s \in \{0, \dots, n - 1\}$, the uniqueness just proved, applied to $a = r$, gives $r = s$. This proves the proposition. ■

So $\mathbb{Z}/12$ has exactly the twelve classes $[0], \dots, [11]$, one for each position of the hand. (The clock face writes 12 where we write $[0]$, and $[12] = [0]$.) The uniqueness also gives a test that is often quicker than the definition: $a \equiv b \pmod{n}$ **if and only if** a and b leave the same remainder on division by n . Indeed, if $a \equiv b$, then $[a] = [b]$, and the one r with $[a] = [r]$ is also the one with $[b] = [r]$; conversely, if both leave the remainder r , then $[a] = [r] = [b]$. With $n = 2$, the two

classes of $\mathbb{Z}/2$ are the even integers $[0]$ and the odd integers $[1]$: the partition of $\mathbb{Z}$ into evens and odds is the quotient set of congruence modulo 2.

2.5.7 Two more sources of equivalence relations

Congruence is one way to manufacture an equivalence relation. Here is the most general way, and a second example on the real line that later chapters return to.

Example. The fibers of a function

Let $f: X \rightarrow Y$ be a function, and for $x, y \in X$ let $x \sim_f y$ mean $f(x) = f(y)$. Show that $\sim_f$ is an equivalence relation on X , and describe its classes. Then show that every equivalence relation $\sim$ on X is of this form, for a suitable function.

Solution. (Eq1)–(Eq3) for $\sim_f$ are the properties of equality applied to the values $f(x), f(y), f(z)$, exactly as in [Example \(Four equivalence relations\)](#) (c): $f(x) = f(x)$; $f(x) = f(y)$ gives $f(y) = f(x)$; and $f(x) = f(y), f(y) = f(z)$ give $f(x) = f(z)$ (Logic and Proof, Proposition 5.7.1).

The class of $a \in X$ is

$$[a] = \{x \in X : f(x) = f(a)\} = f^{-1}(\{f(a)\}),$$

the preimage of the one-point set $\{f(a)\}$ (Definition 1.6.2). Such a preimage $f^{-1}(\{y\})$ is called the **fiber** of f over y . So the classes of $\sim_f$ are the fibers over the points y of the range $f(X)$. A fiber over a point outside the range is empty, and is not a class: (P1) is what excludes it.

For the converse, let $\sim$ be an equivalence relation on X , and take for f the quotient map $q: X \rightarrow X/\sim$ of [Definition 2.5.4](#). Then, for $x, y \in X$,

$$x \sim_q y \iff q(x) = q(y) \iff [x] = [y] \iff x \sim y,$$

where the last step is [Theorem 2.5.1](#) (b). So $\sim_q$ and $\sim$ contain the same pairs, and are equal (Definition 1.1.1).

Two instances. For $f(x) = |x|$ on $\mathbb{R}$, $\sim_f$ is “same absolute value”, and the fiber over 3 is the class $\{-3, 3\}$. For the map $\mathbb{Z} \rightarrow \{0, 1, 2\}$ sending each integer to its remainder on division by 3 (a function by the uniqueness in Theorem 2.2.3), $\sim_f$ is congruence modulo 3, by the remainder test above. The example says that “the same in some respect” always means “equal value of some function”: an equivalence relation is the same thing as a function, up to the names of its values.

Example. The reals modulo the integers

On $\mathbb{R}$, let $x \sim y$ mean $x - y \in \mathbb{Z}$. Show that $\sim$ is an equivalence relation. Find the classes of 0, of $\frac{1}{2}$ and of $\sqrt{2}$, and show that these three classes are different.

Solution. An equivalence relation. (Eq1) $x - x = 0 \in \mathbb{Z}$. (Eq2) If $x - y \in \mathbb{Z}$, then $y - x = 0 - (x - y) \in \mathbb{Z}$, by Proposition 2.1.2 (a). (Eq3) If $x - y \in \mathbb{Z}$ and $y - z \in \mathbb{Z}$, then

$x - z = (x - y) + (y - z) \in \mathbb{Z}$, by Proposition 2.1.2 (a).

The classes. $[0] = \{x \in \mathbb{R} : x - 0 \in \mathbb{Z}\} = \mathbb{Z}$. Next, $x \in [\frac{1}{2}]$ means $x - \frac{1}{2} = k$ for some $k \in \mathbb{Z}$, so

$$[\frac{1}{2}] = \{k + \frac{1}{2} : k \in \mathbb{Z}\} = \{\dots, -\frac{3}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{3}{2}, \dots\},$$

and in the same way $[\sqrt{2}] = \{\sqrt{2} + k : k \in \mathbb{Z}\} = \{\dots, \sqrt{2} - 1, \sqrt{2}, \sqrt{2} + 1, \dots\}$.

Three different classes. By Theorem 2.5.1 (b), two classes $[x]$ and $[y]$ are equal exactly when $x - y \in \mathbb{Z}$. A real number t with $0 < t < 1$ is not an integer: if it were, discreteness (Proposition 2.1.2 (c)) applied to $0 < t$ would give $1 \leq t$. Now $\frac{1}{2} - 0 = \frac{1}{2}$ lies strictly between 0 and 1, so $[\frac{1}{2}] \neq [0]$. Since $\sqrt{2} \geq 0$ and $(\sqrt{2})^2 = 2$, Logic and Proof, Theorem 2.4.5 rules out $\sqrt{2} \leq 1$ (it would give $2 \leq 1$) and $2 \leq \sqrt{2}$ (it would give $4 \leq 2$), so $1 < \sqrt{2} < 2$, and $0 < \sqrt{2} - 1 < 1$; then $\sqrt{2} - 1 \notin \mathbb{Z}$, and therefore $\sqrt{2} - 0 \notin \mathbb{Z}$ (else $\sqrt{2} - 1$ would be a difference of integers), so $[\sqrt{2}] \neq [0]$. Finally, in the same way $\sqrt{2} \leq \frac{1}{2}$ would give $2 \leq \frac{1}{4}$, and $\frac{3}{2} \leq \sqrt{2}$ would give $\frac{9}{4} \leq 2$, so $\frac{1}{2} < \sqrt{2} < \frac{3}{2}$, and $0 < \sqrt{2} - \frac{1}{2} < 1$, and $[\sqrt{2}] \neq [\frac{1}{2}]$.

Picture each class as one point of a circle of circumference 1: the real line is wound around it, and two numbers land on the same point when they differ by an integer. Each class has exactly one representative in $[0, 1)$: the class of $\sqrt{2}$ meets $[0, 1)$ in $\sqrt{2} - 1$, for instance. Proving this for every class needs the integer part of a real number, which *Analysis on the Real Line*, Chapter 1 constructs; we do not use it here. With $\mathbb{Q}$ in place of $\mathbb{Z}$, the relation “ $x - y \in \mathbb{Q}$ ” is again an equivalence relation on $\mathbb{R}$, and choosing one point from each of its classes is how *Measure and Integration*, Chapter 1 builds a set of real numbers that has no length.

2.5.8 Operations on classes

Now the second check of the clock. To add hours we want to define

$$[a] + [b] := [a + b] \quad \text{in } \mathbb{Z}/n.$$

The right-hand side is computed from the representatives a and b . If another pair of representatives of the same two classes gave a different class, the “definition” would assign two answers to one input, and Definition 1.4.1 forbids that: a function gives each input **exactly one** value. So the definition is legitimate only if the answer does not depend on the representatives. That property is called **well-definedness**, and it was met in Section 1.4, where “write a rational number as p/q , then send it to its numerator p ” failed to be a function (Example (Relations that are not functions)).

Proposition 2.5.5. Congruence Respects Sums and Products

Let $n \in \mathbb{Z}_{>0}$ and $a, a', b, b' \in \mathbb{Z}$. If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

$$a + b \equiv a' + b' \pmod{n} \quad \text{and} \quad ab \equiv a'b' \pmod{n}.$$

Hence the operations $[a] + [b] := [a + b]$ and $[a][b] := [ab]$ on $\mathbb{Z}/n$ are **well defined**.

Idea. The sum is direct. For the product, the difference $ab - a'b'$ changes both factors at once; change one at a time, by adding and subtracting ab' .

Proof. Write $a - a' = kn$ and $b - b' = ln$ with $k, l \in \mathbb{Z}$. Then

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

and $k + l \in \mathbb{Z}$ by Proposition 2.1.2 (a). For the product,

$$\begin{aligned} ab - a'b' &= a(b - b') + (a - a')b' \\ &= (al + kb')n, \end{aligned}$$

and $al + kb' \in \mathbb{Z}$ by Proposition 2.1.2 (a). This proves both congruences.

For well-definedness, suppose $[a] = [a']$ and $[b] = [b']$. By Theorem 2.5.1 (b), $a \equiv a'$ and $b \equiv b'$, so $a + b \equiv a' + b'$ and $ab \equiv a'b'$ by what was just proved, and $[a + b] = [a' + b']$ and $[ab] = [a'b']$, again by Theorem 2.5.1 (b). So the class assigned to the pair of classes $([a], [b])$ is the same whichever representatives are used. ■

In the language of Definition 1.4.1: the addition of $\mathbb{Z}/n$ is the function $\mathbb{Z}/n \times \mathbb{Z}/n \rightarrow \mathbb{Z}/n$ whose graph is the set of all pairs $(([a], [b]), [a + b])$ with $a, b \in \mathbb{Z}$. Clause (Fn1) holds because every element of $\mathbb{Z}/n$ is a class $[a]$; clause (Fn2) is the proposition. The clock sentence of the opening is now a true statement: in $\mathbb{Z}/12$,

$$[9] + [5] = [14] = [2],$$

the first equality by the definition of $+$, the second because $14 - 2 = 12$. And $[21] + [-7] = [14] = [2]$ as well, as the proposition guarantees.

Well-definedness can fail, and the next example shows a failure next to a success, with the minimal change between them.

Example. A rule on classes that is not a function

Decide whether each rule defines a function: (a) $F: \mathbb{Z}/6 \rightarrow \mathbb{Z}/4$, $F([a]_6) := [a]_4$; (b) $G: \mathbb{Z}/6 \rightarrow \mathbb{Z}/3$, $G([a]_6) := [a]_3$.

Solution.

- (a) No. The class $[0]_6$ is also $[6]_6$, since $6 - 0 = 1 \cdot 6$. Read with the representative 0, the rule gives $[0]_4$; read with 6, it gives $[6]_4 = [2]_4$, since $6 - 2 = 1 \cdot 4$. And $[0]_4 \neq [2]_4$, since $2 - 0 = 2$ is not a multiple of 4 ($0 < 2 < 4$, and the multiples of 4 are 0, at least 4, or at most -4). So one input receives two values, and (Fn2) of Definition 1.4.1 fails.
- (b) Yes. If $[a]_6 = [a']_6$, then $a - a' = 6k$ for some $k \in \mathbb{Z}$ (Theorem 2.5.1 (b)), so $a - a' = 3(2k)$ with $2k \in \mathbb{Z}$ (Proposition 2.1.2 (a)), and $[a]_3 = [a']_3$. The value does not depend on the representative. What made it work is $3 \mid 6$: a multiple of 6 is a multiple of 3, while a multiple of 6, such as 6 itself, need not be a multiple of 4.

The general lesson: a rule “ $[a] \mapsto$ something computed from a ” defines a function on the classes exactly when equivalent representatives give the same output. The check always has the same shape: take $a \sim a'$, and show that the outputs agree.

2.5.9 Exercises

2.5.9.1 A. Check your understanding

Exercise. A1

Parts (a)–(d) are about [Theorem 2.5.1](#) and its proof.

- (a) Which property of $\sim$ is used to show that every class is non-empty, and which properties are used to show that two overlapping classes are equal?
- (b) Run the proof of part (c) for congruence modulo 3, with $a = 4$, $b = 10$ and the common element $c = 7$: write each line with its numbers.
- (c) On $\{1, 2, 3\}$, let $x \sim y$ mean $x \leq y$, and define $[a]$ by the formula of [Definition 2.5.2](#). Show that $[2]$ and $[1]$ overlap without being equal, and name the line of the proof of part (c) that fails, with $a = 2$, $b = 1$.
- (d) Give the idea of the proof of part (c) in two sentences.
- (e) How many classes has the relation $x^2 = y^2$ on $\{-2, -1, 0, 1, 2\}$? List them.

Solution.

- (a) Non-emptiness uses only reflexivity (Eq1): $a \sim a$ puts a in $[a]$. Overlapping classes are equal by symmetry (Eq2), which turns $c \sim a$ into $a \sim c$, and transitivity (Eq3), which joins $a \sim c$ and $c \sim b$; the final step, part (b), uses (Eq2) and (Eq3) again.
- (b) Since $7 - 4 = 3$, $7 \equiv 4 \pmod{3}$, so $7 \in [4]$; since $7 - 10 = -3$, $7 \equiv 10 \pmod{3}$, so $7 \in [10]$. By (Eq2), $4 \equiv 7$ (indeed $4 - 7 = -3$). By (Eq3), $4 \equiv 10$ (indeed $4 - 10 = -6 = (-2) \cdot 3$). By part (b), $[4] = [10]$.
- (c) $[2] = \{x : x \leq 2\} = \{1, 2\}$ and $[1] = \{x : x \leq 1\} = \{1\}$. They share 1 and differ. In the proof of (c), take $c = 1$: $c \leq 2$ and $c \leq 1$ hold. The next line, “by (Eq2), $a \sim c$ ”, would need $2 \leq 1$, which is false: $\leq$ is not symmetric, and that line fails.
- (d) A common element of two classes is equivalent to both representatives, so symmetry and transitivity make the two representatives equivalent. Equivalent representatives have the same class, because each class is determined by any one of its elements.
- (e) Three: $\{0\}$, $\{-1, 1\}$ and $\{-2, 2\}$. This is the relation $\sim_f$ of [Example \(The fibers of a function\)](#) for $f(x) = x^2$, whose values on the set are 0, 1, 4, one class for each value.

2.5.9.2 B. Practice

Exercise. B1: Fractions as classes

- (a) On $\mathbb{Z} \times \mathbb{Z}_{>0}$, let $(a, b) \sim (c, d)$ mean $ad = bc$. Prove that $\sim$ is an equivalence relation, and describe the class of $(1, 2)$.
- (b) On $\mathbb{Z} \times \mathbb{N}$, let $(a, b) R (c, d)$ again mean $ad = bc$. Determine which of (Eq1)–(Eq3) hold. Justify your answer.

Solution.

- (a) (Eq1) $ab = ba$. (Eq2) If $ad = bc$, then $cb = da$. (Eq3) Let $(a, b) \sim (c, d)$ and $(c, d) \sim$

(e, f) , so $ad = bc$ and $cf = de$. Multiply the first equation by f and use the second: $adf = bcf = bde$. So $d(af - be) = 0$. Since $d \in \mathbb{Z}_{>0}$, $d \neq 0$, and we may cancel d : $af = be$, that is, $(a, b) \sim (e, f)$. The hypothesis $d \neq 0$ on the **middle** pair is used here and nowhere else.

The class of $(1, 2)$ is $\{(c, d) \in \mathbb{Z} \times \mathbb{Z}_{>0} : d = 2c\}$. Since $d > 0$, $c = d/2 > 0$, so $c \in \mathbb{Z}_{>0}$ (Proposition 2.1.2 (b)), and the class is $\{(k, 2k) : k \in \mathbb{Z}_{>0}\} = \{(1, 2), (2, 4), (3, 6), \dots\}$: the ways of writing $\frac{1}{2}$ as a fraction. Each class is “one rational number”; *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 2 builds $\mathbb{Q}$ as this quotient set.

- (b) (Eq1) and (Eq2) hold, by the same two lines as in (a), which did not use $b, d \neq 0$. (Eq3) fails: $(1, 1) R (0, 0)$, since $1 \cdot 0 = 1 \cdot 0$, and $(0, 0) R (2, 1)$, since $0 \cdot 1 = 0 \cdot 2$; but $(1, 1) \not R (2, 1)$, since $1 \cdot 1 \neq 1 \cdot 2$. The pair $(0, 0)$ is related to every pair, so it links any two; this is exactly the cancellation of (a) failing for $d = 0$.

Exercise. B2: Computing in $\mathbb{Z}/7$

In $\mathbb{Z}/7$, compute $[3] + [5]$ and $[3][5]$, each written as $[r]$ with $r \in \{0, \dots, 6\}$. Then prove that $a \equiv b \pmod{n}$ implies $a^k \equiv b^k \pmod{n}$ for every $k \in \mathbb{N}$, and use it to find the remainder of 3^{100} on division by 7. *Hint:* $3^6 = 729$.

Solution. $[3] + [5] = [8] = [1]$, since $8 - 1 = 7$; and $[3][5] = [15] = [1]$, since $15 - 1 = 2 \cdot 7$.

Powers. Let $n \in \mathbb{Z}_{>0}$, $a, b \in \mathbb{Z}$ with $a \equiv b \pmod{n}$. By Proposition 2.3.4 (d), a^k and b^k are integers. We prove $a^k \equiv b^k \pmod{n}$ by induction on $k \in \mathbb{N}$ (Logic and Proof, Axiom 4.2.1). Base: $a^0 = 1 = b^0$, and $1 \equiv 1$ by (Eq1). Step: suppose $a^k \equiv b^k$. By Definition 2.3.2, $a^{k+1} = a^k a$ and $b^{k+1} = b^k b$; the product clause of Proposition 2.5.5, applied to $a^k \equiv b^k$ and $a \equiv b$, gives $a^{k+1} \equiv b^{k+1}$.

The remainder. By Proposition 2.3.4, $3^{100} = 3^{96} \cdot 3^4 = (3^6)^{16} \cdot 3^4$. Now $729 = 104 \cdot 7 + 1$, so $3^6 \equiv 1 \pmod{7}$, and by the power fact, $(3^6)^{16} \equiv 1^{16} = 1$. Also $3^4 = 81 = 11 \cdot 7 + 4$, so $3^4 \equiv 4$. By Proposition 2.5.5, $3^{100} \equiv 1 \cdot 4 = 4 \pmod{7}$. Since $0 \leq 4 < 7$, the remainder of 3^{100} on division by 7 is 4 (Proposition 2.5.4), and $[3^{100}] = [4]$ in $\mathbb{Z}/7$. Here $1^{16} = 1$ is itself an induction: $1^0 = 1$, and $1^{k+1} = 1^k \cdot 1 = 1$.

Exercise. B3: Which rules are well defined?

Determine which of the following rules define a function. Justify your answer.

- (a) $\mathbb{Z}/n \rightarrow \mathbb{Z}/n$, $[a]_n \mapsto [a^2]_n$, for a fixed $n \in \mathbb{Z}_{>0}$.
- (b) $\mathbb{Z}/5 \rightarrow \mathbb{Z}/10$, $[a]_5 \mapsto [a]_{10}$.
- (c) $\mathbb{Z}/10 \rightarrow \mathbb{Z}/5$, $[a]_{10} \mapsto [a]_5$.

Solution. The check in each case: take $[a] = [a']$, that is, $a \equiv a'$, and decide whether the outputs agree (Example (A rule on classes that is not a function)).

- (a) Yes. If $a \equiv a' \pmod{n}$, the product clause of Proposition 2.5.5, applied to $a \equiv a'$ twice, gives $a \cdot a \equiv a' \cdot a'$, so $[a^2]_n = [a'^2]_n$.
- (b) No. $[0]_5 = [5]_5$, since $5 - 0 = 5$. But $[0]_{10} \neq [5]_{10}$, since $5 - 0 = 5$ is not a multiple of 10.

10 ($0 < 5 < 10$). The input $[0]_5$ would get two values.

- (c) Yes. If $a - a' = 10k$ with $k \in \mathbb{Z}$, then $a - a' = 5(2k)$ with $2k \in \mathbb{Z}$ (Proposition 2.1.2 (a)), so $[a]_5 = [a']_5$. The difference from (b) is the direction: $5 \mid 10$, so a multiple of 10 is a multiple of 5, not conversely.

2.5.9.3 C. Going deeper

Exercise. C1: Exit check: classes partition

Let $\sim$ be an equivalence relation on a set X . Prove that the equivalence classes of $\sim$ form a partition of X , and that for all $a, b \in X$, $[a] = [b]$ if and only if $a \sim b$. Write the proof without looking at the text, naming the property of $\sim$ behind each step.

Solution. Non-empty. For $a \in X$, reflexivity gives $a \sim a$, so $a \in [a]$, and $[a] \neq \emptyset$.

Cover. Every class is a subset of X by definition. Every $x \in X$ lies in the class $[x]$, as just shown. So the union of all classes is X .

$[a] = [b] \iff a \sim b$. ($\Rightarrow$) $a \in [a] = [b]$, so $a \sim b$. ($\Leftarrow$) Let $a \sim b$. If $x \in [a]$, then $x \sim a$ and $a \sim b$, so $x \sim b$ by transitivity: $[a] \subseteq [b]$. By symmetry $b \sim a$; if $x \in [b]$, then $x \sim b$ and $b \sim a$ give $x \sim a$ by transitivity: $[b] \subseteq [a]$. So $[a] = [b]$.

Disjoint or equal. Let $[a] \cap [b] \neq \emptyset$, with a common element c . Then $c \sim a$ and $c \sim b$. By symmetry $a \sim c$, and by transitivity $a \sim b$. By the previous paragraph, $[a] = [b]$. Hence two different classes are disjoint.

The three paragraphs on non-emptiness, covering and disjointness are the three clauses of Definition 2.5.3, so the set of classes $X/\sim$ is a partition of X . (This is Theorem 2.5.1.)

Marking scheme. (10 points)

- 2: each class is non-empty, by reflexivity.
- 1: every element lies in some class (its own), so the classes cover X .
- 4: overlapping classes are equal: a common element c with $c \sim a$ and $c \sim b$; symmetry to reverse one of them; transitivity to link a and b ; both inclusions (or the equivalence $[a] = [b] \iff a \sim b$) to conclude equality.
- 2: $[a] = [b] \iff a \sim b$, both directions.
- 1: the conclusion names the three conditions of a partition.

A proof that shows “overlapping classes are equal” by proving $[a] \subseteq [c] \subseteq [b]$ and back directly from the definition earns the 4 points for that step if each use of symmetry and transitivity is named. So does a proof that, from $c \sim a$ and $c \sim b$, applies the ($\Leftarrow$) direction of $[a] = [b] \iff a \sim b$ twice to get $[a] = [c] = [b]$, provided that equivalence was proved independently of this step, with symmetry and transitivity named. Fatal errors (0 for the step): applying transitivity to $a \sim c$ and $b \sim c$ without reversing one by symmetry; showing only $[a] \subseteq [b]$ and concluding $[a] = [b]$.

Exercise. C2: Find the error

A student proves part of Theorem 2.5.2. Let $\mathcal{P}$ be a partition of X , and let $x \sim y$ mean that x and y lie in a common block of $\mathcal{P}$.

Claim. $\sim$ is transitive. *Proof.* (1) Let $x, y, z \in X$ with $x \sim y$ and $y \sim z$. (2) Since $x \sim y$, there is a block $P \in \mathcal{P}$ with $x \in P$ and $y \in P$. (3) Since $y \sim z$, y and z lie in a common block, and that block is P , so $z \in P$. (4) Hence x and z both lie in P , and $x \sim z$.

- (a) Is the claim true?
- (b) Which line fails, and which rule does it break?
- (c) Give a counterexample to the failing step, and repair the proof.

Solution.

- (a) The claim is true: it is the transitivity step (Eq3) in the proof of [Theorem 2.5.2](#) (a).
- (b) Line (3) fails. “ y and z lie in a common block” is an existential statement, and to use it the proof must name its witness by $\exists E$, with a **new** name. Line (3) gives the second witness the name P , already in use for the witness of line (2): this is entry (N4) of Logic and Proof, Example (What is not allowed), reusing one witness name for two $\exists E$ ’s (Logic and Proof, Definition 5.6.1). The tell is that the proof never uses (P2), the disjointness of the blocks; and without (P2) the claim is false, as (c) shows.
- (c) A counterexample to the step needs blocks that overlap, since for a partition the step’s conclusion happens to be true. Take the cover $\{\{1, 2\}, \{2, 3\}\}$ of $\{1, 2, 3\}$, which is not a partition, with $x = 1$, $y = 2$, $z = 3$. Then $1 \sim 2$ with $P = \{1, 2\}$, and $2 \sim 3$ through $\{2, 3\}$; line (3) concludes $3 \in \{1, 2\}$, which is false, and the argument “proves” $1 \sim 3$, although no set of the cover contains 1 and 3.

Repair: replace (3) and (4) by “Since $y \sim z$, there is a block $Q \in \mathcal{P}$ with $y \in Q$ and $z \in Q$. Then $y \in P \cap Q$, so $P \cap Q \neq \emptyset$, and $P = Q$ by (P2). Hence $x \in P$ and $z \in P$, so $x \sim z$.”