

3.4 Ideals, Quotient Rings, and the Integers Modulo n

Sets, Relations, and Cardinality, Section 2.5 turned the school integers into a clock, $\mathbb{Z}/n$, and checked by hand that its sum and product are well defined (*Sets, Relations, and Cardinality*, Proposition 2.5.5). Chapter 2 made the same kind of check twice more, for $\mathbb{Z}$ and for $\mathbb{Q}$, each time through Theorem 2.2.1 and a computation special to the formula. This section makes the check **once**, for every commutative ring and every subset of the right kind, called an ideal. The integers modulo n , now a ring, are the first example. Chapter 5 builds $\mathbb{R}$ in the same shape, from classes of Cauchy sequences of rationals that differ by a null sequence, and checks its operations there directly; *Algebraic Preliminaries*, Chapter 5 runs division with remainder, gcd and unique factorization again for polynomials over a field.

Throughout, R is a commutative ring (Definition 2.3.1), with $a - b := a + (-b)$.

3.4.1 What a quotient needs

Let $I \subseteq R$, and call a and b related when they differ by an element of I :

$$a \sim_I b \quad :\Longleftrightarrow \quad a - b \in I.$$

For $R = \mathbb{Z}$ and I the multiples of n , this is congruence modulo n . We want two things: $\sim_I$ should be an equivalence relation, and the sum and product of classes should be computable on representatives. Each wish makes a demand on I .

- **Reflexivity**, $a - a \in I$, needs $0 \in I$.
- **Symmetry**: $b - a = -(a - b)$, so it needs I to be closed under negatives.
- **Transitivity**: $a - c = (a - b) + (b - c)$, so it needs I to be closed under sums.
- **The sum on classes**. Changing a to a' changes $a + b$ to $a' + b$, and the difference is $a - a'$ again: no new demand.
- **The product on classes**. Changing a to a' changes ab to $a'b$, and the difference is $(a - a')b$: an element of I multiplied by an **arbitrary** element of R . So I must swallow such products.

The last demand contains the second: $-x = (-1)x$. Three clauses remain, and they get a name.

An ideal is a set of allowed errors: it contains 0, it is closed under adding errors, and an error multiplied by anything is still an error.

Definition 3.4.1. Ideal

Let R be a commutative ring. A subset $I \subseteq R$ is an **ideal** of R if

- (I1) $0 \in I$;
- (I2) **for all** $a, b \in I$, $a + b \in I$;
- (I3) **for all** $a \in I$ and **all** $r \in R$, $ra \in I$.

In words: (I1) and (I2) say that I contains 0 and is closed under addition; (I3), **absorption**, says that multiplying an element of I by any element of the ring, inside I or not, lands in I . The ring element r in (I3) ranges over all of R , and that is what separates (I3) from mere closure under multiplication, where r would have to lie in I .

Two consequences are used constantly. First, an ideal is closed under negatives and differences: for $a \in I$, $-a = (-1)a \in I$ by (I3), since $(-1)a = -(1 \cdot a) = -a$ by Proposition 2.3.2 (c) and (F7) with (F6); then $a - b = a + (-b) \in I$ for $a, b \in I$, by (I2). Second, if $1 \in I$, then $I = R$, since every $r = r \cdot 1 \in I$ by (I3).

Examples.

- The degenerate cases: $\{0\}$ and R itself are ideals of R . For $\{0\}$: $0 + 0 = 0$ and $r \cdot 0 = 0$ (Proposition 2.3.2 (b)). For R , every clause asks for an element of R . They are the two extremes: “no error allowed” and “everything allowed”.
- For $n \in \mathbb{Z}$, the multiples $n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$ form an ideal of $\mathbb{Z}$ (Definition 3.2.1): $0 = 0 \cdot n$; $kn + ln = (k + l)n$; $r(kn) = (rk)n$. In particular the even integers $2\mathbb{Z}$ form an ideal.
- For $a, b \in \mathbb{Z}$, the combinations $a\mathbb{Z} + b\mathbb{Z}$ form an ideal of $\mathbb{Z}$, by the closure properties in Definition 3.2.1; Theorem 3.4.2 below records this.

Non-examples by minimal change. $\mathbb{N} \subseteq \mathbb{Z}$ satisfies (I1) and (I2), but (I3) fails at $a = 1$, $r = -1$: $(-1) \cdot 1 = -1 \notin \mathbb{N}$, since $-1 < 0$ ($1 > 0$ by Proposition 2.3.5 (e), as $1 \neq 0$ in $\mathbb{Z}$ by Theorem 2.3.1, then (a)) while $\mathbb{N} = \{x \in \mathbb{Z} : x \geq 0\}$ (Theorem 2.3.4 (b)). And $\mathbb{Z} \subseteq \mathbb{Q}$ satisfies (I1), (I2) and is even closed under negatives and products, but (I3) fails at $a = 1$, $r = 1/2$: $(1/2) \cdot 1 = 1/2 \notin \mathbb{Z}$. (If $1/2 = m \in \mathbb{Z}$, then $2m = 1$, but $1 = 2 \cdot 0 + 1$ is odd and so not of the form $2m$, by Corollary 3.1.3 (a).) In both cases the ring element r comes from **outside** the subset, which is exactly what (I3) allows.

Why these clauses. Each clause was forced by one of the five wishes above, and dropping one loses its wish: without (I1) or (I2), $\sim_I$ is not reflexive or not transitive; without (I3), the product on classes can fail, as the warning after the next theorem shows for $\mathbb{Z} \subseteq \mathbb{Q}$.

3.4.2 The quotient ring

The payoff is a single theorem that builds a ring of classes from any ideal. We write $[a]$, or $[a]_I$ when the ideal must be named, for the class of a under $\sim_I$, and R/I for the quotient set $R/\sim_I$ (Sets, Relations, and Cardinality, Definition 2.5.4).

Theorem 3.4.1. Quotient Ring by an Ideal

Let R be a commutative ring and I an ideal of R .

- Setting $a \sim_I b \iff a - b \in I$ defines an equivalence relation $\sim_I$ on R , and the class of a is $[a] = a + I := \{a + x : x \in I\}$.
- The rules $[a] + [b] := [a + b]$, $[a] \cdot [b] := [ab]$ and $-[a] := [-a]$ are well defined on $R/I := R/\sim_I$.
- R/I , with these operations, is a commutative ring with zero $[0]$ and one $[1]$. The **quotient map** $\pi: R \rightarrow R/I$, $\pi(a) := [a]$, satisfies $\pi(a + b) = \pi(a) + \pi(b)$, $\pi(ab) = \pi(a)\pi(b)$ and $\pi(1) = [1]$.
- $[a] = [0]$ if and only if $a \in I$. In particular $[1] = [0]$ if and only if $I = R$.

In words: (a) and (b) say that classes modulo an ideal can be added, multiplied and negated through any representatives; (c) says that the result obeys every ring law, and that passing to classes respects the operations; (d) says that the elements of I are exactly those that become 0, and that the quotient collapses to the zero ring exactly when I is everything.

Idea. A change of representative is an element of I . The equivalence-relation clauses ask that such changes can be reversed and chained, which is closure under negatives and sums. The operations ask that a change in one argument produce a change in the output: for the sum the change is the same element of I , and for the product it is that element multiplied by the other argument, which (I3) keeps in I . The ring laws are then laws of R read on classes.

Before reading on: where is “ $ra \in I$ for every $r \in R$ ” used, and why does closure under $+$ not suffice for the product?

Proof. (a) Let $a, b, c \in R$. (Eq1): $a - a = 0 \in I$, by (F4) and (I1). (Eq2): if $a - b \in I$, then $b - a = -(a - b) \in I$, since I is closed under negatives; here $(a - b) + (b - a) = 0$ by (F1)–(F4), so $b - a = -(a - b)$ by the uniqueness of negatives (Proposition 2.3.2 (a)). (Eq3): if $a - b \in I$ and $b - c \in I$, then $a - c = (a - b) + (b - c) \in I$, by (F2)–(F4) and (I2). So $\sim_I$ is an equivalence relation (Sets, Relations, and Cardinality, Definition 2.5.1). For the class: if $x \sim_I a$, then $x - a \in I$ and $x = a + (x - a) \in a + I$; conversely, for $y \in I$, $(a + y) - a = y \in I$, so $a + y \sim_I a$. Hence $[a] = a + I$.

(b) We check the hypotheses of Theorem 2.2.1 (b), with $X = R$ and the relation $\sim_I$, for the maps $(a, b) \mapsto a + b$ and $(a, b) \mapsto ab$. Let $a \sim_I a'$, so $a - a' \in I$, and let $b \in R$. Then

$$\begin{aligned}(a + b) - (a' + b) &= a - a' \in I, \\ ab - a'b &= (a - a')b = b(a - a') \in I,\end{aligned}$$

by (F1)–(F4) in the first line, and by (F9), (F6) and Proposition 2.3.2 (c) in the second, where the membership is (I3) with $r = b$: **the ideal absorbs b** . This is the first hypothesis. Since $a + b = b + a$ and $ab = ba$ ((F1), (F6)), the second hypothesis is the first with the two arguments exchanged. For the negative we check the hypothesis of Theorem 2.2.1 (a) for $a \mapsto -a$: $(-a) - (-a') = -(a - a') \in I$, by Proposition 2.3.2 (a) and closure under negatives. Hence the three rules define functions.

(c) Every element of R/I is a class $[a]$ (Sets, Relations, and Cardinality, Definition 2.5.4). Each axiom of Definition 2.3.1 other than (F8) is an equation, and by (b) both of its sides, read on classes, are the classes of the two sides of the same equation in R . For example, for (F9),

$$[a]([b] + [c]) = [a][b + c] = [a(b + c)] = [ab + ac] = [ab] + [ac] = [a][b] + [a][c],$$

using (F9) in R in the middle; for (F3), $[a] + [0] = [a + 0] = [a]$; for (F4), $[a] + (-[a]) = [a] + [-a] = [a + (-a)] = [0]$; for (F7), $[a][1] = [a \cdot 1] = [a]$. The laws (F1), (F2), (F5) and (F6) go the same way. So R/I is a commutative ring with zero $[0]$ and one $[1]$. The equations for π are the definitions in (b) read from right to left, and $\pi(1) = [1]$ by definition of π .

(d) $[a] = [0]$ holds if and only if $a \sim_I 0$ (Sets, Relations, and Cardinality, Theorem 2.5.1 (b)), that is, $a - 0 \in I$; and $a - 0 = a + 0 = a$, since $-0 = 0$ ($0 + 0 = 0$ and Proposition 2.3.2 (a)). So $[a] = [0] \iff a \in I$. In particular $[1] = [0] \iff 1 \in I$. If $1 \in I$, then $I = R$, since $r = r \cdot 1 \in I$ for every $r \in R$ by (I3); and if $I = R$, then $1 \in I$. This proves the theorem. ■

The answer to the prompt. Absorption with an arbitrary $r \in R$, the full force of (I3), is used exactly once in the proof of (a) and (b): in the product, at $ab - a'b = (a - a')b$, where the change

of representative $a - a' \in I$ is multiplied by an arbitrary $b \in R$. Elsewhere (I3) enters only with $r = -1$, through closure under negatives ($-x = (-1)x$), and otherwise the proof uses (I1) and (I2). Closure under $+$ does not suffice for the product because b need not lie in I : the product changes by a multiple of the error, not by a sum of errors.

We call this move **compute on representatives; the ideal absorbs the change**. It is the move of Chapter 2's "one argument at a time", now with the change of representative recorded as one element of I .

Warning. Closure under $+$ and $-$ is not enough for the product. $\mathbb{Z} \subseteq \mathbb{Q}$ contains 0 and is closed under sums and negatives, and these are all that the proof of (a) and of the sum and negative in (b) used. So " $x - y \in \mathbb{Z}$ " relates rationals by an equivalence relation, and $[x] + [y] := [x + y]$ is well defined on its classes. But $[x][y] := [xy]$ is **not**: $[1/2] = [3/2]$, since $3/2 - 1/2 = 1 \in \mathbb{Z}$, while

$$\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}, \quad \frac{3}{2} \cdot \frac{1}{2} = \frac{3}{4}, \quad \frac{3}{4} - \frac{1}{4} = \frac{1}{2} \notin \mathbb{Z}.$$

One class, two products in different classes. The missing clause is (I3): $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$.

3.4.3 The ideals of the integers

In $\mathbb{Z}$ every ideal is as simple as possible: the multiples of one number. The proof is the move that gave the gcd in Section 3.2.

Theorem 3.4.2. Ideals of the Integers

- (a) For all $a, b \in \mathbb{Z}$, $a\mathbb{Z} + b\mathbb{Z}$ is an ideal of $\mathbb{Z}$. In particular $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for every $n \in \mathbb{Z}$.
- (b) Every ideal I of $\mathbb{Z}$ equals $n\mathbb{Z}$ for **exactly one** $n \in \mathbb{N}$: $n = 0$ if $I = \{0\}$, and otherwise n is the least positive element of I .

Idea. For (b), take the least positive element n of I . Its multiples lie in I by absorption. Conversely, divide any $a \in I$ by n : the remainder $a - qn$ lies in I and is smaller than n , so it is not positive, and it is 0. This is **least positive element, then divide** once more.

Proof. (a) $0 = a \cdot 0 + b \cdot 0 \in a\mathbb{Z} + b\mathbb{Z}$ (Proposition 2.3.2 (b)), and Definition 3.2.1 shows that $a\mathbb{Z} + b\mathbb{Z}$ is closed under sums and under multiplication by any integer. These are (I1)–(I3). Since $n\mathbb{Z} = n\mathbb{Z} + 0\mathbb{Z}$ (Definition 3.2.1), $n\mathbb{Z}$ is an ideal.

(b) *Existence.* If $I = \{0\}$, then $I = 0\mathbb{Z}$, since $k \cdot 0 = 0$ for every k (Proposition 2.3.2 (b)). Otherwise I has an element $a \neq 0$, and $-a \in I$ as well; one of a , $-a$ is positive (Proposition 3.1.1 (h)). So $I \cap \mathbb{Z}_{>0}$ is non-empty, with lower bound 0, and has a least element n (Proposition 2.3.6). By (I3), $kn \in I$ for every $k \in \mathbb{Z}$, so $n\mathbb{Z} \subseteq I$. Conversely, let $a \in I$. By Theorem 3.1.2 (a), $a = qn + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then $r = a + (-q)n \in I$, by (I3) and (I2). If $r > 0$, then r is a positive element of I smaller than n , against the choice of n . So $r = 0$, and $a = qn \in n\mathbb{Z}$. Hence $I = n\mathbb{Z}$.

Uniqueness. Let $n\mathbb{Z} = m\mathbb{Z}$ with $n, m \in \mathbb{N}$. Then $n = 1 \cdot n \in m\mathbb{Z}$, so $m \mid n$; likewise $n \mid m$. By Proposition 3.1.1 (f), $n = m$. ■

Remark. For $I = a\mathbb{Z} + b\mathbb{Z}$ with $(a, b) \neq (0, 0)$, (b) says $a\mathbb{Z} + b\mathbb{Z} = n\mathbb{Z}$ where n is the least positive combination. That is Theorem 3.2.1 (a), (d), (e), with $n = \gcd(a, b)$: the theorem of Section 3.2 was this one in disguise.

3.4.4 The ring of integers modulo n

Now the clock of *Sets, Relations, and Cardinality*, Section 2.5 can be rebuilt on the constructed $\mathbb{Z}$, as an instance of the general theorem.

Definition 3.4.2. The Integers Modulo n

Let $n \in \mathbb{Z}_{>0}$. The ring $\mathbb{Z}/n\mathbb{Z}$ is the quotient ring of $\mathbb{Z}$ by the ideal $n\mathbb{Z}$ (Theorem 3.4.1, Theorem 3.4.2 (a)).

Its relation is congruence modulo n of *Sets, Relations, and Cardinality*, Definition 2.5.5, read on the constructed $\mathbb{Z}$: $a - b \in n\mathbb{Z}$ means $a - b = kn$ for some $k \in \mathbb{Z}$, that is, $n \mid a - b$, that is, $a \equiv b \pmod{n}$. Its elements are the classes $[a] = a + n\mathbb{Z}$, written $[a]_n$ when two moduli are in play. Its operations, $[a] + [b] = [a + b]$ and $[a][b] = [ab]$, are those of *Sets, Relations, and Cardinality*, Proposition 2.5.5; there they were checked by hand for the school integers, and here they are a consequence of Theorem 3.4.1 (b). The set $\mathbb{Z}/n\mathbb{Z}$ of *Sets, Relations, and Cardinality* is the same construction on the school $\mathbb{Z}$; from now on we write $\mathbb{Z}/n\mathbb{Z}$, to recall the ideal.

Theorem 3.4.3. The Ring of Integers Modulo n

Let $n \in \mathbb{Z}_{>0}$.

- (a) $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with zero $[0]$ and one $[1]$.
- (b) For each $a \in \mathbb{Z}$ there is **exactly one** $r \in \{0, \dots, n-1\}$ with $[a] = [r]$, namely the remainder of a on division by n . The map $\{0, \dots, n-1\} \rightarrow \mathbb{Z}/n\mathbb{Z}$, $r \mapsto [r]$, is a bijection, so $\mathbb{Z}/n\mathbb{Z}$ is finite with n elements (*Sets, Relations, and Cardinality*, Definition 3.1.2).
- (c) $[1] \neq [0]$ if and only if $n \geq 2$.
- (d) $k \cdot [1] = [k]$ for every $k \in \mathbb{N}$, where $k \cdot x$ is the k -th multiple in the commutative ring $\mathbb{Z}/n\mathbb{Z}$; in particular $n \cdot [1] = [0]$.
- (e) If $n \geq 2$, no relation $<$ makes $\mathbb{Z}/n\mathbb{Z}$ an ordered commutative ring.

The multiples in (d) are those of Section 2.3, defined there by recursion for every commutative ring R ($0 \cdot x := 0$, $(k+1) \cdot x := k \cdot x + x$), before Proposition 2.3.5; the recursion uses no order, so it applies to $\mathbb{Z}/n\mathbb{Z}$, which for $n \geq 2$ carries no order compatible with its arithmetic, by (e).

Idea. Most of the work is done: (a) is the general theorem, and (b) is division with remainder read on classes, the remainder naming the class and its uniqueness making the naming one-

to-one. Then (c) asks when 1 is a multiple of n , (d) is an induction along the recursion that defines multiples, and (e) puts (c) and (d) against the rule that $n \cdot 1 > 0$ in an ordered ring.

Proof. (a) [Theorem 3.4.1](#) (c), since $n\mathbb{Z}$ is an ideal ([Theorem 3.4.2](#) (a)).

(b) *Existence.* By [Theorem 3.1.2](#) (a), $a = qn + r$ with $0 \leq r < n$. Then $a - r = qn \in n\mathbb{Z}$, so $[a] = [r]$. Also $r \in \mathbb{N}$ by [Theorem 2.3.4](#) (b), and $r + 1 \leq n$ by discreteness ([Theorem 2.3.4](#) (c)), so $r \leq n - 1$ by (O3); that is, $r \in \{0, \dots, n - 1\}$.

Uniqueness. Let $r, s \in \{0, \dots, n - 1\}$ with $[r] = [s]$. Then $r - s = kn$ for some $k \in \mathbb{Z}$, so $r = kn + s$ and $r = 0 \cdot n + r$ are two divisions of r by n , with remainders s and r , each at least 0 and less than n . By the uniqueness in [Theorem 3.1.2](#) (a), $s = r$.

So the map $\varphi: \{0, \dots, n - 1\} \rightarrow \mathbb{Z}/n\mathbb{Z}$, $r \mapsto [r]$, is surjective (existence: every class is some $[a]$, [Sets, Relations, and Cardinality](#), [Definition 2.5.4](#)) and injective (uniqueness), hence a bijection ([Sets, Relations, and Cardinality](#), [Definition 1.4.5](#)). Since $n \geq 1$, adding -1 gives $n - 1 \geq 0$ (O3), so $n - 1 \in \mathbb{N}$ by [Theorem 2.3.4](#) (b), and the third example after [Sets, Relations, and Cardinality](#), [Definition 3.1.2](#), with $n - 1$ in place of its n , gives the bijection $\psi: \{1, \dots, n\} \rightarrow \{0, \dots, n - 1\}$, $k \mapsto k - 1$. The composite $\varphi \circ \psi: \{1, \dots, n\} \rightarrow \mathbb{Z}/n\mathbb{Z}$ is a bijection ([Sets, Relations, and Cardinality](#), [Theorem 1.4.4](#) (c)), so $\mathbb{Z}/n\mathbb{Z}$ has n elements.

(c) By [Theorem 3.4.1](#) (d), $[1] = [0]$ if and only if $1 \in n\mathbb{Z}$, that is, $n \mid 1$. By [Proposition 3.1.1](#) (g) and $n > 0$, this happens exactly when $n = 1$. As $n \geq 1$ by discreteness, $n \neq 1$ means $n \geq 2$.

(d) By Logic and Proof, [Axiom 4.2.1](#) (through [Corollary 1.7.3](#) (b)) on k . Base: $0 \cdot [1] = [0]$, by the recursion. Step: if $k \cdot [1] = [k]$, then

$$(k + 1) \cdot [1] = k \cdot [1] + [1] = [k] + [1] = [k + 1],$$

by the recursion, the hypothesis, and the definition of $+$ in [Theorem 3.4.1](#) (b) (the sum $k + 1$ is the same in $\mathbb{N}$ and in $\mathbb{Z}$, [Proposition 2.2.3](#) (a)). Finally $[n] = [0]$, since $n - 0 = 1 \cdot n \in n\mathbb{Z}$.

(e) Let $n \geq 2$, and suppose $<$ made $\mathbb{Z}/n\mathbb{Z}$ an ordered commutative ring. By (c), $[1] \neq [0]$, so [Proposition 2.3.5](#) (h), applied with $n \geq 1$, gives $n \cdot [1] > [0]$. By (d), $n \cdot [1] = [0]$, and $[0] > [0]$ contradicts (O1). This proves the theorem. ■

Part (e) is the general clause after Example (A field with two elements that cannot be ordered), now applied to a ring that this volume has built: $\mathbb{Z}/2\mathbb{Z}$ has the tables of that example, with $[0]$, $[1]$ for 0, 1. Part (b) says that the elements of $\mathbb{Z}/n\mathbb{Z}$ can be listed as $[0], [1], \dots, [n - 1]$, and that to compute with classes we may always reduce to remainders.

Example. Multiplication modulo six and modulo five

Write out the multiplication table of $\mathbb{Z}/6\mathbb{Z}$. Find the pairs of non-zero classes whose product is $[0]$, and the classes $[a]$ for which some $[b]$ has $[a][b] = [1]$. Then do the same for $\mathbb{Z}/5\mathbb{Z}$.

Solution. By [Theorem 3.4.3](#) (b), the classes of $\mathbb{Z}/6\mathbb{Z}$ are $[0], \dots, [5]$, and $[a][b] = [ab] = [r]$, where r is the remainder of ab on division by 6. For instance $[4][5] = [20] = [2]$, since $20 = 3 \cdot 6 + 2$. Writing r for $[r]$, the table is

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

The non-zero classes with product $[0]$ are $[2][3] = [6] = [0]$ and $[3][4] = [12] = [0]$, with their mirror images $[3][2]$, $[4][3]$. So $\mathbb{Z}/6\mathbb{Z}$ has zero divisors, unlike $\mathbb{Z}$ (Proposition 2.3.5 (f)). Also $[4][4] = [16] = [4]$: a class can equal its own square without being $[0]$ or $[1]$. The entry 1 occurs only in the rows of $[1]$ and $[5]$: $[1][1] = [1]$ and $[5][5] = [25] = [1]$. So exactly $[1]$ and $[5]$ have a partner with product $[1]$.

For $\mathbb{Z}/5\mathbb{Z}$ the same method gives

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

No product of non-zero classes is $[0]$, and every non-zero class has a partner with product $[1]$: $[1][1] = [1]$, $[2][3] = [6] = [1]$, $[4][4] = [16] = [1]$. Moreover $5 \cdot [1] = [0]$ by [Theorem 3.4.3](#) (d), so $\mathbb{Z}/5\mathbb{Z}$ cannot be ordered, by (e).

The classes with a partner of product $[1]$ are the **units** of Section 3.5, which finds them for every n and shows that for a prime n , as for 5, every non-zero class is one. Chapter 6 uses the ring $\mathbb{Z}/5\mathbb{Z}$, with $5 \cdot [1] = [0]$, as a field that no order can fit.

Quick check. In $\mathbb{Z}/12\mathbb{Z}$, compute $[7] + [8]$ and $[7][8]$, each as $[r]$ with $0 \leq r \leq 11$. How many elements has $\mathbb{Z}/1\mathbb{Z}$?

Solution. $[7] + [8] = [15] = [3]$, since $15 = 1 \cdot 12 + 3$; and $[7][8] = [56] = [8]$, since $56 = 4 \cdot 12 + 8$. The ring $\mathbb{Z}/1\mathbb{Z}$ has one element, by [Theorem 3.4.3](#) (b): every integer is congruent to 0 modulo 1, so $[0] = [1]$, and it is a zero ring, like the ring $\{0\}$ of Section 2.3.

Warning. A class is not its remainder. $[3]$ in $\mathbb{Z}/12\mathbb{Z}$ is the set $3 + 12\mathbb{Z} = \{\dots, -9, 3, 15, \dots\}$, not the integer 3, and the same symbol $[3]$ in $\mathbb{Z}/5\mathbb{Z}$ is a different set. A comparison such as “ $[3] < [8]$ ” cannot be read off the remainders and respect the arithmetic: by [Theorem 3.4.3](#)

(e) no order makes $\mathbb{Z}/12\mathbb{Z}$ an ordered ring. Reducing to remainders is a way of **naming** classes, not a way of turning them back into integers.

3.4.5 Exercises

3.4.5.1 A. Check your understanding

Exercise. A1

These questions are about the proof of [Theorem 3.4.1](#).

- (a) Where is the clause “ $ra \in I$ for every $r \in R$ ” used?
- (b) Run the product check of (b) with $R = \mathbb{Z}$, $I = 6\mathbb{Z}$, $a = 2$, $a' = 8$ and $b = 5$: verify $a \sim_I a'$, compute $ab - a'b$, and say why it lies in I .
- (c) For $\mathbb{Z} \subseteq \mathbb{Q}$, which step of the proof fails, and which clause of [Definition 3.4.1](#) is missing?
- (d) Give the idea of the proof in two sentences.

Solution.

- (a) In (b), for the product in the first argument: $ab - a'b = (a - a')b \in I$, with $a - a' \in I$ and $r = b$. (It also gives closure under negatives, which (a) and (b) use through $-x = (-1)x$; and it is used in (d), to get $I = R$ from $1 \in I$.)
- (b) $a - a' = 2 - 8 = -6 = (-1) \cdot 6 \in 6\mathbb{Z}$, so $2 \sim_I 8$. Then $ab - a'b = 10 - 40 = -30$, which is $(a - a')b = (-6) \cdot 5$, and $-30 = (-5) \cdot 6 \in 6\mathbb{Z}$. It lies in I because I absorbs the factor 5.
- (c) The product step of (b): $(a - a')b$ need not lie in $\mathbb{Z}$, as with $a = 3/2$, $a' = 1/2$, $b = 1/2$, where it is $1/2$. The missing clause is (I3): $(1/2) \cdot 1 \notin \mathbb{Z}$.
- (d) A change of representative is an element of I ; for the sum it passes through unchanged, and for the product it gets multiplied by the other argument, which absorption keeps inside I . The ring laws then hold in R/I because both sides of each are classes of the two sides of the same law in R .

3.4.5.2 B. Practice

Exercise. B1: The ring with four elements

Write the addition and multiplication tables of $\mathbb{Z}/4\mathbb{Z}$. Find its zero divisors (non-zero x with $xy = [0]$ for some non-zero y) and the classes $[a]$ with $[a][b] = [1]$ for some $[b]$.

Solution. By [Theorem 3.4.3](#) (b) the elements are $[0], [1], [2], [3]$, and each entry is the class of

the remainder of the sum or product on division by 4. Writing r for $[r]$:

+	0	1	2	3	·	0	1	2	3
0	0	1	2	3	0	0	0	0	0
1	1	2	3	0	1	0	1	2	3
2	2	3	0	1	2	0	2	0	2
3	3	0	1	2	3	0	3	2	1

For instance $[3] + [3] = [6] = [2]$ and $[3][3] = [9] = [1]$, since $6 = 1 \cdot 4 + 2$ and $9 = 2 \cdot 4 + 1$. The only zero divisor is $[2]$: $[2][2] = [4] = [0]$, and in the rows of $[1]$ and $[3]$ the entry 0 occurs only in the column of $[0]$. The classes with a partner of product $[1]$ are $[1]$ ($[1][1] = [1]$) and $[3]$ ($[3][3] = [1]$); the rows of $[0]$ and $[2]$ contain no 1.

Exercise. B2: Determine which

For each subset of $\mathbb{Z}$ below, decide whether it is an ideal of $\mathbb{Z}$. Justify your answer.

- (a) $\mathbb{N}$.
- (b) $2\mathbb{Z} \cup 3\mathbb{Z}$.
- (c) $4\mathbb{Z} + 6\mathbb{Z}$.
- (d) $\{0\}$.
- (e) $\{n \in \mathbb{Z} : 6 \mid n^2\}$, where $n^2 := nn$.

Solution.

- (a) No. (I3) fails: $1 \in \mathbb{N}$, but $(-1) \cdot 1 = -1 \notin \mathbb{N}$, since $-1 < 0$ ($1 > 0$ by Proposition 2.3.5 (e), as $1 \neq 0$ in $\mathbb{Z}$ by Theorem 2.3.1, then (a)) while $\mathbb{N} = \{x \in \mathbb{Z} : x \geq 0\}$ (Theorem 2.3.4 (b)).
- (b) No. (I2) fails: $2 \in 2\mathbb{Z}$ and $3 \in 3\mathbb{Z}$, but 5 is in neither, since $5 = 2 \cdot 2 + 1$ and $5 = 1 \cdot 3 + 2$ leave non-zero remainders (uniqueness in Theorem 3.1.2 (a)).
- (c) Yes, by Theorem 3.4.2 (a). In fact $4\mathbb{Z} + 6\mathbb{Z} = 2\mathbb{Z}$: every $4x + 6y = 2(2x + 3y)$ is even, and every $2k = 4(-k) + 6k$ is a combination.
- (d) Yes: the ideal $0\mathbb{Z}$, or directly as in the examples after Definition 3.4.1.
- (e) Yes: the set is $6\mathbb{Z}$. If $n = 6k$, then $n^2 = 6(6k^2)$. Conversely, let $6 \mid n^2$, say $n^2 = 6m$. Then $n \cdot n = 2(3m) = 3(2m)$, so $2 \mid nn$ and $3 \mid nn$. Since 2 and 3 are prime (the small-primes remark of Section 3.1), Corollary 3.3.2 (b) gives $2 \mid n$ and $3 \mid n$. As $1 = (-1) \cdot 2 + 1 \cdot 3$, $\gcd(2, 3) = 1$ (Corollary 3.2.2), so $6 = 2 \cdot 3 \mid n$ by Proposition 3.3.3. Hence the set equals $6\mathbb{Z}$, an ideal by Theorem 3.4.2 (a).

3.4.5.3 C. Going deeper

Exercise. C1: Changing the modulus

Let $m, n \in \mathbb{Z}_{>0}$. Prove that there is a function $F: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ with $F([a]_n) = [a]_m$ for every $a \in \mathbb{Z}$ if and only if $m \mid n$. Show that, when it exists, F preserves sums, products and the one.

Solution. ($\Leftarrow$) Let $n = lm$. Then $n\mathbb{Z} \subseteq m\mathbb{Z}$, since $kn = (kl)m$. We apply Theorem 2.2.1 (a) with $X = Y = \mathbb{Z}$, congruence modulo n on X , congruence modulo m on Y , and $f(a) := a$: if $a - a' \in n\mathbb{Z}$, then $a - a' \in m\mathbb{Z}$. So F exists (and is unique).

($\Rightarrow$) Suppose F exists. Since $n - 0 = 1 \cdot n$, $[n]_n = [0]_n$, so

$$[n]_m = F([n]_n) = F([0]_n) = [0]_m,$$

so $n \in m\mathbb{Z}$ by Theorem 3.4.1 (d), that is, $m \mid n$.

Operations. $F([a]_n + [b]_n) = F([a + b]_n) = [a + b]_m = [a]_m + [b]_m$, by the definition of $+$ in Theorem 3.4.1 (b) on both sides; likewise for products, and $F([1]_n) = [1]_m$.

This is the general form of Sets, Relations, and Cardinality, Example (A rule on classes that is not a function): $[a]_6 \mapsto [a]_4$ fails because $4 \nmid 6$, and $[a]_6 \mapsto [a]_3$ works because $3 \mid 6$.

Marking scheme. (10 points) - 3: ($\Leftarrow$) writes $n = lm$, shows $n\mathbb{Z} \subseteq m\mathbb{Z}$, and invokes Theorem 2.2.1 (a) with $f(a) = a$. - 3: ($\Rightarrow$) uses $[n]_n = [0]_n$ and applies F to get $[n]_m = [0]_m$, hence $m \mid n$. - 3: computes F of a sum and of a product on representatives, citing the definition of the operations on both quotient rings. - 1: $F([1]_n) = [1]_m$. Fatal errors (0 for the step): defining F by a formula on representatives without checking that it does not depend on the representative; in ($\Rightarrow$), assuming $n\mathbb{Z} \subseteq m\mathbb{Z}$ (circular).

Exercise. C2: Closed under subtraction

Let $S \subseteq \mathbb{Z}$ be **non-empty**, with $a - b \in S$ for all $a, b \in S$. Prove that $S = n\mathbb{Z}$ for some $n \in \mathbb{N}$.

The first half of a proof is given.

Pick $a \in S$; then $0 = a - a \in S$. If $S = \{0\}$, then $S = 0\mathbb{Z}$. Otherwise S contains some $a \neq 0$, and $-a = 0 - a \in S$; one of $a, -a$ is positive (Proposition 3.1.1 (h)).

By Proposition 2.3.6, S has a least positive element n .

The second half is blank. *Name the move, then complete it.*

Solution. The move is **least positive element, then divide**.

$n\mathbb{Z} \subseteq S$. First, $kn \in S$ for every $k \in \mathbb{N}$, by Logic and Proof, Axiom 4.2.1 on k . Base: $0 \cdot n = 0 \in S$. Step: $-n = 0 - n \in S$, and if $kn \in S$, then $(k+1)n = kn + n = kn - (-n) \in S$, using (F9), (F7) and $-(-n) = n$ (Proposition 2.3.2 (a)). Next, every $k \in \mathbb{Z}$ is j or $-j$ for some $j \in \mathbb{N}$ (Proposition 2.2.3 (c)), and $(-j)n = -(jn) = 0 - jn \in S$ (Proposition 2.3.2 (c)).

$S \subseteq n\mathbb{Z}$. Let $a \in S$. By Theorem 3.1.2 (a), $a = qn + r$ with $0 \leq r < n$. Since $qn \in S$, $r = a - qn \in S$. If $r > 0$, it is a positive element of S smaller than n , against the choice of n . So $r = 0$ and $a = qn$.

Hence $S = n\mathbb{Z}$. No multiplication hypothesis was needed: closure under subtraction alone forces the multiples of n , and so S is automatically an ideal. The sets S of this exercise are the subgroups of $(\mathbb{Z}, +)$, which *Algebraic Preliminaries*, Chapter 3 studies.