

3.2 Subgroups and the Subgroups of the Integers

Section 3.1 defined groups and proved their basic laws. After a structure comes the substructure. The even integers sit inside $(\mathbb{Z}, +)$ and form a group on their own, with the same addition; so do the multiples of 7, of 12, and of 0, which is just $\{0\}$. Are there any other subgroups of $\mathbb{Z}$? *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 3.4 answered the same question for ideals, which are closed under multiplication by every integer (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Theorem 3.4.2). Here the multiplication is gone, and the answer is the same: this section proves that the subgroups of $(\mathbb{Z}, +)$ are exactly the sets $n\mathbb{Z}$ with $n \in \mathbb{N}$.

3.2.1 Subgroups

A subset of a group can fail to be a group with the inherited operation in three ways: a product can leave it, the identity can be missing, or an inverse can be missing. The definition rules out all three.

A subgroup is a subset that contains the identity and is closed under products and inverses.

Definition 3.2.1. Subgroup

Let G be a group. A subset $H \subseteq G$ is a **subgroup** of G if $e \in H$, and $ab \in H$ and $a^{-1} \in H$ for all $a, b \in H$.

In words: the identity of G is in H ; multiplying two elements of H never leaves H ; and the inverse in G of an element of H lies in H . We say “ H is a subgroup of G ” in words and use no symbol for it; in this chapter $\leq$ always means the order of $\mathbb{Z}$.

Then the operation of G restricts to a binary operation $H \times H \rightarrow H$, and H is a group with it: (G1) holds in H because it holds in G , and (G2), (G3) hold because e and the inverses lie in H . The identity of the group H is the identity e of G , and the inverse of a in H is its inverse in G , by the uniqueness in Theorem 3.1.1 (1) and (2). Three conditions are a lot to check; in practice one checks that H is non-empty and a single combined condition.

Theorem 3.2.1. Subgroup Test

Let G be a group and $H \subseteq G$. Then H is a subgroup of G if and only if $H \neq \emptyset$ and $ab^{-1} \in H$ for all $a, b \in H$.

Proof. ($\Rightarrow$) If H is a subgroup, then $e \in H$, so $H \neq \emptyset$. For $a, b \in H$ we have $b^{-1} \in H$, and then $ab^{-1} \in H$, since H is closed under products.

($\Leftarrow$) Suppose $H \neq \emptyset$ and $ab^{-1} \in H$ for all $a, b \in H$. Pick $h \in H$. Taking $a = b = h$ gives $e = hh^{-1} \in H$. For $b \in H$, taking $a = e$ gives $b^{-1} = eb^{-1} \in H$. For $a, b \in H$, we now know $b^{-1} \in H$, so $ab = a(b^{-1})^{-1} \in H$ by Theorem 3.1.1 (3). Hence H is a subgroup. This proves the theorem. ■

In additive notation the test reads: $H \neq \emptyset$ and $a - b \in H$ for all $a, b \in H$, where $a - b := a + (-b)$.

Example. Subgroups

Check that each of the following is a subgroup.

- (a) $\{e\}$ and G , in any group G .
- (b) $n\mathbb{Z}$ in $(\mathbb{Z}, +)$, for $n \in \mathbb{Z}$; more generally $a\mathbb{Z} + b\mathbb{Z}$, for $a, b \in \mathbb{Z}$ (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Definition 3.2.1).
- (c) $\{1, -1\}$ and $\mathbb{Q}_{>0}$ in $(\mathbb{Q} \setminus \{0\}, \cdot)$.
- (d) $\{[0], [2], [4]\}$ in $(\mathbb{Z}/6\mathbb{Z}, +)$; $\{[1], [3]\}$ in $(\mathbb{Z}/8\mathbb{Z})^\times$.
- (e) In the group of bijections of a set X (Example (Groups) (c)), the bijections σ that fix a chosen point $x_0 \in X$, that is, $\sigma(x_0) = x_0$.
- (f) $\{1, i, -1, -i\}$, the unit circle $\mathbb{T}$, and, for $n \geq 1$, the set μ_n of n -th roots of unity, in $(\mathbb{C} \setminus \{0\}, \cdot)$ (Chapter 1).

Solution. In each case we use [Theorem 3.2.1](#), or [Definition 3.2.1](#) directly.

(a) $\{e\}$ is non-empty, and $ee^{-1} = e$. G is non-empty, since $e \in G$, and $ab^{-1} \in G$ because the operation is a binary operation. The **trivial subgroup** $\{e\}$ is the smallest subgroup of every group: by the definition, every subgroup contains e .

(b) $0 = 0n \in n\mathbb{Z}$ (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Proposition 2.3.2 (b), with (F6)). For $kn, ln \in n\mathbb{Z}$,

$$kn - ln = kn + (-l)n = (k - l)n \in n\mathbb{Z},$$

by Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Proposition 2.3.2 (c), then (F9) with (F6). In the same way $0 = a0 + b0 \in a\mathbb{Z} + b\mathbb{Z}$, and $(ax + by) - (ax' + by') = a(x - x') + b(y - y')$. So both are subgroups, by the additive form of the test. For instance $2\mathbb{Z}$ is the set of even integers, and $0\mathbb{Z} = \{0\}$.

(c) For $\{1, -1\}$: $(-1)(-1) = 1$ (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Proposition 2.3.2 (c)), so each of $1, -1$ is its own inverse, and the products $1 \cdot 1 = 1$, $1 \cdot (-1) = -1$, $(-1)(-1) = 1$ lie in the set; so it is a subgroup by the definition. For $\mathbb{Q}_{>0}$: it contains 1, which is positive (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Proposition 2.3.5 (e)). Let $a, b > 0$. Then $b^{-1} > 0$ by Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Proposition 2.5.2 (a). So $ab^{-1} > 0$ by (O4), $\mathbb{Q}$ being an ordered field (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Theorem 2.5.1).

(d) For classes, $[a] - [b] = [a - b]$ (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Theorem 3.4.1 (b)). For $a, b \in \{0, 2, 4\}$, the difference $a - b$ is one of $0, \pm 2, \pm 4$, and $[-2] = [4]$, $[-4] = [2]$ in $\mathbb{Z}/6\mathbb{Z}$ (since $6 \mid -2 - 4$ and $6 \mid -4 - 2$). So every difference lies in $\{[0], [2], [4]\}$. For $\{[1], [3]\}$: $[3]^{-1} = [3]$, since $[3][3] = [9] = [1]$, so the four quotients $[1][1]^{-1} = [1]$, $[1][3]^{-1} = [3]$, $[3][1]^{-1} = [3]$, $[3][3]^{-1} = [1]$ lie in the set.

(e) The identity map fixes x_0 , so the set is non-empty. Let σ and τ fix x_0 . Applying τ^{-1} to $\tau(x_0) = x_0$ gives $x_0 = \tau^{-1}(x_0)$, so $(\sigma \circ \tau^{-1})(x_0) = \sigma(x_0) = x_0$. Section 3.4 uses this subgroup for $X = \{1, \dots, n + 1\}$ and $x_0 = n + 1$.

(f) $\mathbb{C}$ is a field (Theorem 1.2.4), so $(\mathbb{C} \setminus \{0\}, \cdot)$ is a group by Example (Groups) (b). Recall that $i^2 = -1$ (Proposition 1.1.1, with the identification of $\mathbb{R}$ inside $\mathbb{C}$ made after it).

For $\{1, i, -1, -i\}$: products of two of ± 1 are ± 1 , products of ± 1 with $\pm i$ are $\pm i$, and products of two of $\pm i$ are $\pm i^2 = \mp 1$ (signs by Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.2 (c)). So the set is closed under products, and it contains 1. Each of 1, -1 is its own inverse, and $i(-i) = -i^2 = 1$, so $i^{-1} = -i$ and $(-i)^{-1} = i$. It is a subgroup by the definition.

For $\mathbb{T} = \{u \in \mathbb{C} : |u| = 1\}$: by Proposition 1.5.1 (a), which rests on the modulus rule $|zw| = |z||w|$ of Theorem 1.2.2 (d), $1 \in \mathbb{T}$, $uv \in \mathbb{T}$ for $u, v \in \mathbb{T}$, and each $u \in \mathbb{T}$ is non-zero with $u^{-1} = \bar{u} \in \mathbb{T}$. So $\mathbb{T} \subseteq \mathbb{C} \setminus \{0\}$, and $\mathbb{T}$ is a subgroup by the definition.

For μ_n , the set of $z \in \mathbb{C}$ with $z^n = 1$ (Chapter 1's notation, after Example (Roots of Unity)): $0 \notin \mu_n$, since $0^n = 0^{n-1} \cdot 0 = 0 \neq 1$ for $n \geq 1$; so $\mu_n \subseteq \mathbb{C} \setminus \{0\}$, and there z^n is the power of Definition 3.1.3, defined by the same recursion. Also $1 \in \mu_n$. For $\zeta, \eta \in \mu_n$, since $\mathbb{C} \setminus \{0\}$ is abelian,

$$(\zeta\eta^{-1})^n = \zeta^n(\eta^{-1})^n = \zeta^n(\eta^n)^{-1} = 1 \cdot 1^{-1} = 1,$$

by Proposition 3.1.3 (d) and (b). So $\zeta\eta^{-1} \in \mu_n$, and μ_n is a subgroup by the test. Chapter 1 also notes that $\mu_n \subseteq \mathbb{T}$. Its Section 1.6, Exercise R2 builds a bijection $\mathbb{Z}/n\mathbb{Z} \rightarrow \mu_n$ that sends sums to products; in the words of Section 3.3 this is an isomorphism of groups. That exercise rests on the facts about cosine and sine that Chapter 1 borrows, and nothing in this chapter cites it.

Now non-examples, each a minimal change of an example. The set $\mathbb{N} \subseteq \mathbb{Z}$ contains 0 and is closed under $+$, but $0 - 1 = -1 \notin \mathbb{N}$: the inverses are missing. The odd integers fail more badly: they do not contain 0, which is even ($0 = 2 \cdot 0$) and so not odd (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Corollary 3.1.3 (a)). And $\mathbb{Z}_{>0} \subseteq \mathbb{Q}_{>0}$ is non-empty and closed under multiplication, but $2^{-1} = 1/2 \notin \mathbb{Z}$: an integer m with $2m = 1$ would make 1 even, and $1 = 2 \cdot 0 + 1$ is odd. Each fails the test at one clause, and each is an infinite set; for a **finite** non-empty subset, closure under products alone suffices (Exercise C1).

Subgroups can be combined. If two subgroups are given, the elements they share form a subgroup again, and so do the elements shared by any family of subgroups:

Proposition 3.2.2. Intersections of Subgroups

Let G be a group and $(H_i)_{i \in I}$ a family of subgroups of G . Then $\bigcap_{i \in I} H_i$, taken inside G (Sets, Relations, and Cardinality, Definition 1.2.4 (b)), is a subgroup of G .

Proof. Write $H := \bigcap_{i \in I} H_i$. Since $e \in G$ and $e \in H_i$ for every $i \in I$, $e \in H$, so $H \neq \emptyset$. Let $a, b \in H$. Then $ab^{-1} \in G$, and for each $i \in I$, $a, b \in H_i$, so $ab^{-1} \in H_i$ by Theorem 3.2.1 applied to the subgroup H_i . Hence $ab^{-1} \in H$, and H is a subgroup by Theorem 3.2.1. This proves the proposition. ■

For the empty family the intersection is G itself, which is a subgroup.

Warning. A union of two subgroups need not be a subgroup. $2\mathbb{Z} \cup 3\mathbb{Z}$ contains 3 and 2, but not $3 - 2 = 1$: $1 \notin 2\mathbb{Z}$ and $1 \notin 3\mathbb{Z}$, since neither 2 nor 3 divides 1 (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 3.1.1 (g)). Intersections are safe; unions are not.

3.2.2 The subgroup generated by one element

Fix $g \in G$. Which subgroups contain g ? Each of them contains $gg, ggg, \dots$, and their inverses, so it contains every power g^n . The powers themselves form a subgroup, and so they are the smallest possible answer.

Definition 3.2.2. Subgroup Generated by an Element

Let G be a group and $g \in G$. The **subgroup generated by g** is

$$\langle g \rangle := \{g^n : n \in \mathbb{Z}\},$$

with the powers of Definition 3.1.3. In additive notation, $\langle a \rangle = \{n \cdot a : n \in \mathbb{Z}\}$.

In $(\mathbb{Z}, +)$, $\langle n \rangle = \{k \cdot n : k \in \mathbb{Z}\} = \{kn : k \in \mathbb{Z}\} = n\mathbb{Z}$, since the group multiple $k \cdot n$ is the product kn (Proposition 3.1.3 (e)). The name is justified by the next result.

Proposition 3.2.3. The Subgroup Generated by an Element

Let G be a group and $g \in G$. Then $\langle g \rangle$ is an abelian subgroup of G that contains g , and every subgroup of G that contains g contains $\langle g \rangle$.

Idea. Both halves are the power laws at work. The test asks for $g^m(g^n)^{-1}$, which the laws turn into the single power g^{m-n} . Conversely, a subgroup containing g is closed under products and inverses, and every power is built from g by those two operations.

Proof. First, $g = g^1 \in \langle g \rangle$, so $\langle g \rangle \neq \emptyset$. For $g^m, g^n \in \langle g \rangle$,

$$g^m(g^n)^{-1} = g^m g^{-n} = g^{m-n} \in \langle g \rangle,$$

by Proposition 3.1.3 (b) and (a); so $\langle g \rangle$ is a subgroup by Theorem 3.2.1. It is abelian: $g^m g^n = g^{m+n} = g^{n+m} = g^n g^m$, by Proposition 3.1.3 (a) and (F1) in $\mathbb{Z}$.

Now let H be a subgroup of G with $g \in H$. By Logic and Proof, Axiom 4.2.1, $g^n \in H$ for every $n \in \mathbb{N}$: $g^0 = e \in H$, and if $g^n \in H$, then $g^{n+1} = g^n g \in H$, since H is closed under products. For $n \in \mathbb{N}$, also $g^{-n} = (g^n)^{-1} \in H$ (Proposition 3.1.3 (b)), since H is closed under inverses. Every integer is n or $-n$ for some $n \in \mathbb{N}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{Z}$), Proposition 2.2.3 (c)), so $\langle g \rangle \subseteq H$. This proves the proposition. ■

So $\langle g \rangle$ is the smallest subgroup containing g . A group that equals $\langle g \rangle$ for one of its elements g is called cyclic; *Groups*, the chapter “Cyclic Groups”, studies these groups and the least $m \geq 1$ with $g^m = e$.

Examples. If $g^m = e$ for some $m \geq 1$, the subgroup $\langle g \rangle$ is finite and easy to list. Indeed, divide any $n \in \mathbb{Z}$ by m : $n = qm + r$ with $0 \leq r < m$ (Number Systems: From $\mathbb{N}$ to $\mathbb{Z}$), Theorem 3.1.2 (a)). Then

$$g^n = g^{mq} g^r = (g^m)^q g^r = e^q g^r = g^r,$$

by Proposition 3.1.3 (a) and (c), and $e^q = (g^0)^q = g^0 = e$ by (c) again. So $\langle g \rangle = \{g^0, g^1, \dots, g^{m-1}\}$.

- In $(\mathbb{Z}/6\mathbb{Z}, +)$, $k \cdot [2] = [2k]$ for $k \in \mathbb{N}$, by Proposition 3.1.3 (c) and (e) and Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Theorem 3.4.3 (d), where (e) identifies the group multiples with the ring multiples to which (d) applies: $k \cdot (2 \cdot [1]) = (2k) \cdot [1] = [2k]$. So the multiples are $[0], [2], [4]$, and $3 \cdot [2] = [6] = [0]$. By the paragraph above (with $m = 3$), $\langle [2] \rangle = \{[0], [2], [4]\}$, the subgroup of Example (Subgroups) (d).
- In $(\mathbb{Z}/7\mathbb{Z})^\times$, the powers of $[2]$ are $[1], [2], [4]$, and $[2]^3 = [8] = [1]$. So $\langle [2] \rangle = \{[1], [2], [4]\}$.
- In $(\mathbb{Z}/7\mathbb{Z})^\times$, the powers $[3]^1, \dots, [3]^6$ are $[3], [2], [6], [4], [5], [1]$, each obtained from the one before by multiplying by $[3]$ (for instance $[6][3] = [18] = [4]$). Since $\mathbb{Z}/7\mathbb{Z}$ is a field (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Theorem 3.5.2), $(\mathbb{Z}/7\mathbb{Z})^\times = (\mathbb{Z}/7\mathbb{Z}) \setminus \{[0]\}$, as in any field (the paragraph “Why this definition” after Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Definition 3.5.1), so it has the six elements $[1], \dots, [6]$ (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Theorem 3.4.3 (b)), and all of them are powers of $[3]$: $\langle [3] \rangle = (\mathbb{Z}/7\mathbb{Z})^\times$.

3.2.3 The subgroups of the integers

Every set $n\mathbb{Z} = \langle n \rangle$ is a subgroup of $(\mathbb{Z}, +)$. The theorem says that there are no others, and that n is determined by the subgroup.

Theorem 3.2.4. Subgroups of the Integers

Let H be a subgroup of $(\mathbb{Z}, +)$. Then $H = n\mathbb{Z}$ for **exactly one** $n \in \mathbb{N}$: $n = 0$ if $H = \{0\}$, and otherwise n is the least positive element of H .

Try it first (ten minutes): find the smallest subgroup of $\mathbb{Z}$ containing 6 and 15. List a few of its elements, guess what it is, and say why its least positive element should divide 6.

Idea. The attempt finds elements by subtracting: $15 - 6 = 9$, $9 - 6 = 3$, and then every multiple of 3. That suggests “the multiples of 3”, but listing gives no reason why nothing else can be in the subgroup. The guess also points at the right candidate for n : the **least positive** element, 3 here. Why should every element be a multiple of it? Divide an element a by n . The remainder is a minus a multiple of n , so it lies in the subgroup, and it is smaller than n . It cannot be positive, so it is 0. This is the move of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 3.2, **least positive element, then divide**, now with nothing but subtraction available.

*Before reading on: where is $H \neq \{0\}$ used, and why is the least **positive** element taken, not the least element?*

Proof. If $H = \{0\}$, then $H = 0\mathbb{Z}$. Suppose $H \neq \{0\}$, and pick $a \in H$ with $a \neq 0$. Then $-a \in H$, and one of $a, -a$ is positive (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Proposition 3.1.1 (h)). So $H \cap \mathbb{Z}_{>0}$ is non-empty, and it has the lower bound 0; by Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Proposition 2.3.6 it has a least element n , the least positive element of H .

($\supseteq$) Since $n \in H$ and $n\mathbb{Z} = \langle n \rangle$ (Proposition 3.1.3 (e)), Proposition 3.2.3 gives $n\mathbb{Z} \subseteq H$.

($\subseteq$) Let $a \in H$. Since $n > 0$, Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Theorem 3.1.2

(a) gives $q, r \in \mathbb{Z}$ with $a = qn + r$ and $0 \leq r < n$. Here $qn \in n\mathbb{Z} \subseteq H$, so $r = a - qn \in H$, since H is a subgroup. If $r > 0$, then r is a positive element of H smaller than n , against the choice of n . So $r = 0$, and $a = qn \in n\mathbb{Z}$.

Hence $H = n\mathbb{Z}$. For uniqueness, let $n\mathbb{Z} = m\mathbb{Z}$ with $n, m \in \mathbb{N}$. Then $n = 1 \cdot n \in m\mathbb{Z}$, so $m \mid n$, and in the same way $n \mid m$; hence $n = m$ by Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Proposition 3.1.1 (f). This proves the theorem. ■

The answer to the prompt. The hypothesis $H \neq \{0\}$ is used once, in the first paragraph: it supplies a non-zero element, hence a positive one, so that the set of positive elements of H is non-empty and has a least element. The least element of H itself does not exist when $H \neq \{0\}$: if m were least, then $m - n \in H$ and $m - n < m$. And $0 \in H$ is useless as a divisor, since division with remainder needs a positive divisor; the minimality of n among the **positive** elements is exactly what forces $r = 0$.

Remark. This is the statement of Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Exercise (C2: Closed under subtraction), an exercise in *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 3.4, promoted to a theorem, and it is the additive half of Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Theorem 3.4.2 (b). In $\mathbb{Z}$, being an ideal comes free: every subgroup $H = n\mathbb{Z}$ of $\mathbb{Z}$ is an ideal (Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Definition 3.4.1), since for $jn \in H$ and $k \in \mathbb{Z}$, $k(jn) = (kj)n \in n\mathbb{Z}$ by (F5).

The theorem turns questions about subgroups of $\mathbb{Z}$ into questions about one number: the least positive element.

Quick check. Which $n \in \mathbb{N}$ has $n\mathbb{Z} = 6\mathbb{Z} \cap 15\mathbb{Z}$?

Solution. $n = 30$. The intersection is a subgroup (Proposition 3.2.2), and it contains $30 = 5 \cdot 6 = 2 \cdot 15 \neq 0$, so by Theorem 3.2.4 it is $n\mathbb{Z}$ with n its least positive element, the least positive common multiple of 6 and 15. The positive multiples of 15 below 30 are 15 alone, and $15 = 2 \cdot 6 + 3$ is not a multiple of 6 (by the uniqueness of the remainder in Number Systems: From $\backslash(\backslash n\mathbb{N}\backslash)$ to $\backslash(\backslash n\mathbb{R}\backslash)$, Theorem 3.1.2 (a)), while 30 is. So $n = 30$.

3.2.4 Exercises

3.2.4.1 A. Check your understanding

Exercise. A1

These parts are about the proof of Theorem 3.2.4.

- (a) Where is the minimality of n used?
- (b) Run the proof on $H = 4\mathbb{Z} + 6\mathbb{Z}$: find n , and the division of 6 by n .
- (c) The conclusion fails for the subset $\mathbb{N}$ of $\mathbb{Z}$. Which condition of Definition 3.2.1 does $\mathbb{N}$

lack, and which step of the proof breaks?

- (d) State the idea of the proof in two sentences.

Solution.

- (a) In the step ($\subseteq$): the remainder r lies in H and $0 \leq r < n$, and minimality forbids $r > 0$, so $r = 0$.
- (b) H is a subgroup (Example (Subgroups) (b)). Its least positive element is $n = 2$: $2 = 6 - 4 \in H$, and $1 \notin H$, since every element $4x + 6y = 2(2x + 3y)$ is even and 1 is odd (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 3.1.3 (a)). Dividing 6 by 2 gives $6 = 3 \cdot 2 + 0$, with remainder 0, as the proof predicts. So $H = 2\mathbb{Z}$.
- (c) $\mathbb{N}$ lacks inverses: $1 \in \mathbb{N}$, but $-1 \notin \mathbb{N}$. The step ($\supseteq$) breaks: there $n = 1$, and $n\mathbb{Z} \subseteq H$ went through $n\mathbb{Z} = \langle n \rangle$ and Proposition 3.2.3, which needs a subgroup; indeed $-1 = (-1) \cdot 1 \notin \mathbb{N}$. The first paragraph's step $-a \in H$ also fails for $\mathbb{N}$ (take $a = 1$), but harmlessly: a non-zero $a \in \mathbb{N}$ is already positive, so $n = 1$ still exists. The step whose failure breaks the conclusion is ($\supseteq$). The other inclusion still holds for $\mathbb{N}$: each $a \in \mathbb{N}$ is $a = a \cdot 1 + 0$, so $\mathbb{N} \subseteq 1\mathbb{Z} = \mathbb{Z}$.
- (d) The least positive element n of H is the only candidate. Division by n leaves a remainder in H smaller than n , so the remainder is 0 and every element is a multiple of n .

3.2.4.2 B. Practice

Exercise. B1: Put the proof in order

The following lines contain the proof of the direction ($\Leftarrow$) of Theorem 3.2.1, shuffled, together with two lines that do not belong. Write the seven correct lines in an order that makes a proof, say which other orders are also admissible, and say why each of the other two lines fails.

- (i) For $a, b \in H$, we know $b^{-1} \in H$.
- (ii) Hence H is a subgroup of G .
- (iii) Choose $h \in H$.
- (iv) Taking $a = e$ and $b = h$: $h^{-1} = eh^{-1} \in H$; so $e = hh^{-1} \in H$.
- (v) Suppose $H \neq \emptyset$ and $ab^{-1} \in H$ for all $a, b \in H$.
- (vi) So $ab = a(b^{-1})^{-1} \in H$, by Theorem 3.1.1 (3).
- (vii) For $b \in H$, taking $a = e$: $b^{-1} = eb^{-1} \in H$.
- (viii) $ab \in H$, because H is closed under products.
- (ix) Taking $a = b = h$: $e = hh^{-1} \in H$.

Solution. The admissible order is (v), (iii), (ix), (vii), (i), (vi), (ii). Each line uses the one before it: (iii) uses $H \neq \emptyset$ from (v); (ix) uses the h of (iii); (vii) takes $a = e$, which needs $e \in H$ from (ix); (i) is (vii) applied to an arbitrary b ; (vi) needs $b^{-1} \in H$ from (i); and (ii) collects $e \in H$, inverses and products. So no other order is admissible: the dependencies form a single chain.

The distractor (iv) is circular. It takes $a = e$ in the hypothesis, which is allowed only once

$e \in H$ is known, and then concludes $e \in H$. Placed before (ix), it uses what it is meant to prove; placed after (ix), its first half is a special case of (vii) and its second half repeats (ix).

The distractor (viii) assumes what is being proved: closure under products is one of the three conditions of [Definition 3.2.1](#) that the direction ($\Leftarrow$) must establish, and the hypothesis (v) does not state it.

Exercise. B2: Subgroups of the integers modulo twelve

Determine which of the following subsets of $(\mathbb{Z}/12\mathbb{Z}, +)$ are subgroups. Justify your answer.

- (a) $\{[0], [4], [8]\}$.
- (b) $\{[0], [3], [6], [9]\}$.
- (c) $\{[0], [5]\}$.
- (d) $\{[0], [6]\}$.

Then show that every subgroup of $\mathbb{Z}/12\mathbb{Z}$ that contains $[5]$ is all of $\mathbb{Z}/12\mathbb{Z}$.

Solution. We use the additive form of [Theorem 3.2.1](#), with $[a] - [b] = [a - b]$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), [Theorem 3.4.1](#) (b)).

- (a) A subgroup. For $a, b \in \{0, 4, 8\}$, $a - b \in \{0, \pm 4, \pm 8\}$, and $[-4] = [8]$, $[-8] = [4]$, since 12 divides $-4 - 8$ and $-8 - 4$.
- (b) A subgroup. For $a, b \in \{0, 3, 6, 9\}$, $a - b \in \{0, \pm 3, \pm 6, \pm 9\}$, and $[-3] = [9]$, $[-6] = [6]$, $[-9] = [3]$.
- (c) Not a subgroup: $[0] - [5] = [-5] = [7]$, which is not in the set (the remainders 7, 0, 5 are distinct, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), [Theorem 3.4.3](#) (b)). Equally, $[5] + [5] = [10]$ is not in the set.
- (d) A subgroup: $[6] - [6] = [0]$, $[0] - [6] = [-6] = [6]$, and the other differences are $[0]$ and $[6]$.

Now let H be a subgroup with $[5] \in H$. By [Proposition 3.2.3](#), $\langle [5] \rangle \subseteq H$, so $5 \cdot [5] \in H$. By [Proposition 3.1.3](#) (c) and (e) and Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), [Theorem 3.4.3](#) (d), $5 \cdot [5] = 5 \cdot (5 \cdot [1]) = 25 \cdot [1] = [25] = [1]$, since $25 = 2 \cdot 12 + 1$. So $[1] \in H$, and then $k \cdot [1] = [k] \in H$ for every $k \in \mathbb{N}$ ([Proposition 3.2.3](#), [Proposition 3.1.3](#) (e) and Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), [Theorem 3.4.3](#) (d) again). Taking $k = 0, 1, \dots, 11$ gives every class of $\mathbb{Z}/12\mathbb{Z}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), [Theorem 3.4.3](#) (b)). Hence $H = \mathbb{Z}/12\mathbb{Z}$.

Exercise. B3: Integer combinations, once more

Let $a, b \in \mathbb{Z}$, not both 0. Use [Theorem 3.2.4](#) to prove that $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, where d is the least positive element of $a\mathbb{Z} + b\mathbb{Z}$. Compare the proof with the one in *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 3.2.

Solution. $a\mathbb{Z} + b\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$ ([Example \(Subgroups\)](#) (b)). It is not $\{0\}$: it contains $a = a \cdot 1 + b \cdot 0$ and $b = a \cdot 0 + b \cdot 1$, and one of them is non-zero. So by [Theorem 3.2.4](#),

$a\mathbb{Z} + b\mathbb{Z} = n\mathbb{Z}$ with n its least positive element, which is d .

This is Number Systems: From $\setminus(\setminus n\mathbb{N}\setminus)$ to $\setminus(\setminus n\mathbb{R}\setminus)$, Theorem 3.2.1 (e), whose d is the same least positive combination. The two proofs are one argument. *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* divided a and b by d and used that the remainder is again a combination; the proof of Theorem 3.2.4 divides an arbitrary element of the subgroup by n and uses only that a subgroup is closed under subtraction. The second form applies to every subgroup of $\mathbb{Z}$, not only to sets of combinations.

3.2.4.3 C. Going deeper

Exercise. C1: Finite subsets closed under products

Let G be a group, and let $H \subseteq G$ be finite, non-empty and closed under products ($ab \in H$ for all $a, b \in H$). Prove that H is a subgroup of G . Then explain why $\mathbb{N} \subseteq \mathbb{Z}$, which is non-empty and closed under $+$ but not a subgroup, does not contradict this.

The first half of a proof is given.

Let $h \in H$, and let $k := |H|$ (Sets, Relations, and Cardinality, Definition 3.1.2). The powers $h, h^2, \dots, h^{k+1}$ all lie in H , by induction on the exponent, since $h^{j+1} = h^j h$.

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

Solution. The move is **multiply by the inverse**: two equal powers $h^i = h^j$ become $e = h^{j-i}$ once h^i is removed from both sides.

Completion. The map $\{1, \dots, k+1\} \rightarrow H, j \mapsto h^j$, goes from a set with $k+1$ elements to a set with k elements, so it is not injective (Sets, Relations, and Cardinality, Corollary 3.1.3 (a)): $h^i = h^j$ for some $1 \leq i < j \leq k+1$. Multiplying both sides on the left by $(h^i)^{-1} = h^{-i}$ gives

$$e = h^{-i}h^i = h^{-i}h^j = h^{j-i}$$

(Proposition 3.1.3 (b), (a)). Since $1 \leq j-i \leq k$, h^{j-i} is one of the listed powers, so $e \in H$. Next, if $j-i \geq 2$, then $h h^{j-i-1} = h^{j-i-1}h = h^{j-i} = e$ (Proposition 3.1.3 (a)), so $h^{-1} = h^{j-i-1}$ by Theorem 3.1.1 (2), and $h^{j-i-1} \in H$ since $1 \leq j-i-1 \leq k$. If $j-i = 1$, then $h = h^1 = e$, and $h^{-1} = e \in H$. As $h \in H$ was arbitrary, H is closed under inverses; it contains e and is closed under products, so it is a subgroup by Definition 3.2.1.

The set $\mathbb{N}$ is not finite, so the result does not apply to it. Read backwards, the result even proves this: if $\mathbb{N}$ were finite, it would be a subgroup of $\mathbb{Z}$, and it is not, since $-1 \notin \mathbb{N}$.

Marking scheme. (10 points) - 1: names the move (multiply by the inverse, or cancel h^i). - 2: gets $h^i = h^j$ with $1 \leq i < j \leq k+1$ from the pigeonhole principle, cited. - 2: derives $h^{j-i} = e$ with the power laws named, and concludes $e \in H$ from $1 \leq j-i \leq k$. - 3: shows $h^{-1} \in H$: $h^{-1} = h^{j-i-1}$ when $j-i \geq 2$, and $h = e$ when $j-i = 1$. - 1: concludes that H is a subgroup, by Definition 3.2.1 or Theorem 3.2.1. - 1: explains that $\mathbb{N}$ is infinite, so the result does not apply. Fatal errors (0 for the step): $h^0 = e$ taken as one of the listed powers (the list starts at h^1); $h^{-1} \in H$ asserted without exhibiting it as a positive power; the case $j-i = 1$ mishandled so that h^0 is claimed to lie in the list.

Exercise. C2: Exit check: subgroups of the integers

State and prove [Theorem 3.2.4](#).

Solution (Hint 1). Look at the positive elements of H , and take the least one.

Solution (Hint 2). To show that an element $a \in H$ is a multiple of that least positive element n , divide a by n .

Solution. The statement and proof of [Theorem 3.2.4](#) are a complete answer. In outline: $H = \{0\} = 0\mathbb{Z}$, or H has a non-zero element a , and then a or $-a$, both in H , is positive; the least positive element n exists by Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Proposition 2.3.6; $n\mathbb{Z} \subseteq H$ because H is a subgroup containing n (all multiples kn , negative k included); for $a \in H$, $a = qn + r$ with $0 \leq r < n$ and $r = a - qn \in H$, so $r = 0$ by minimality; and $n\mathbb{Z} = m\mathbb{Z}$ with $n, m \in \mathbb{N}$ forces $n = m$.

Marking scheme. (10 points) - 3: the case $H = \{0\}$; otherwise the existence of a positive element, with the reason when the chosen element is negative (its inverse lies in H). - 1: the least positive element, by a cited well-ordering result for sets of integers bounded below. - 2: $n\mathbb{Z} \subseteq H$ by closure, with the negative multiples included. - 2: division of $a \in H$ by n , with the remainder shown to lie in H . - 1: minimality of n forces $r = 0$. - 1: uniqueness of $n \in \mathbb{N}$. Fatal errors (0 for the step): assuming that H is an ideal, or citing Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Theorem 3.4.2 for H (closure under multiplication by integers is not given; that it comes free is a consequence of the theorem); “the least element of H ” without positivity. A proof by induction showing $kn \in H$ for $k \in \mathbb{N}$, followed by inverses for $k < 0$, earns the 2 points for $n\mathbb{Z} \subseteq H$. A descent proof (for $a \in H$ with $a \geq 0$, strong induction on a : if $a \geq n$, then $a - n \in H$ and $0 \leq a - n < a$; negative a handled through $-a \in H$) earns the 2 points for division when it shows $a - n \in H$ and treats negative a , and the 1 point for minimality when it rules out $0 < a < n$.

Exercise. C3: Inclusions and intersections

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

- (a) Prove that $m\mathbb{Z} \subseteq n\mathbb{Z}$ if and only if $n \mid m$.
- (b) Prove that $m\mathbb{Z} \cap n\mathbb{Z} = L\mathbb{Z}$, where L is the least positive common multiple of m and n . Deduce that L divides every common multiple of m and n .

Solution (Hint 1). For (a), ask where m itself lies. For (b), ask what kind of set the intersection is.

Solution (Hint 2). For (b): $m\mathbb{Z} \cap n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ by [Proposition 3.2.2](#), and mn lies in it.

Solution.

- (a) $(\Rightarrow)$ $m = 1 \cdot m \in m\mathbb{Z} \subseteq n\mathbb{Z}$, so $m = kn$ for some $k \in \mathbb{Z}$, that is, $n \mid m$. $(\Leftarrow)$ If $m = kn$, then every $jm = (jk)n$ lies in $n\mathbb{Z}$, by (F5).
- (b) By [Proposition 3.2.2](#), $m\mathbb{Z} \cap n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$. It contains $mn = n \cdot m = m \cdot n$, which is positive by (O4), so it is not $\{0\}$. By [Theorem 3.2.4](#) it equals $L\mathbb{Z}$, with L its least positive element. Its elements are exactly the common multiples of m and n , so L is the least positive common multiple. A common multiple c lies in $m\mathbb{Z} \cap n\mathbb{Z} = L\mathbb{Z}$, so $L \mid c$.

This is Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Exercise (B2: The least common multiple), there proved by dividing c by L directly; here the division is done once and for all inside [Theorem 3.2.4](#).

Marking scheme. (10 points) - 2: (a) $(\Rightarrow)$ uses $m \in m\mathbb{Z}$ to get $m = kn$. - 1: (a) $(\Leftarrow)$ shows $jm = (jk)n \in n\mathbb{Z}$. - 2: (b) the intersection is a subgroup of $(\mathbb{Z}, +)$, by [Proposition 3.2.2](#). - 2: (b) it is not $\{0\}$ (mn is a positive element), so [Theorem 3.2.4](#) gives $L\mathbb{Z}$ with L its least positive element. - 2: (b) identifies the intersection with the set of common multiples, so L is the least positive common multiple. - 1: (b) deduces $L \mid c$ for every common multiple c . Fatal errors (0 for the step): (b) applies [Theorem 3.2.4](#) without checking that the intersection is a subgroup; (b) assumes $L = mn$ or $L = mn/\gcd(m, n)$ without proof.