

3.1 Groups

Several structures met so far behave alike: the integers under addition, the non-zero rationals under multiplication, the units of $\mathbb{Z}/n\mathbb{Z}$ (*Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 3.5), and the bijections of a set under composition (*Sets, Relations, and Cardinality*, Chapter 1). This section names their common structure, a group, and proves its basic laws once, from three axioms, so that they hold in all of these at once. It then makes two habits honest: dropping brackets from a product of many factors, and writing powers g^n with $n \in \mathbb{Z}$.

Throughout the chapter $\mathbb{N}$ is ω , and $\mathbb{Z}$, $\mathbb{Q}$ are the integers and rationals built in *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Chapter 2. Induction and recursion on $\mathbb{N}$ are Logic and Proof, Axiom 4.2.1 and Sets, Relations, and Cardinality, Theorem 2.3.1, read on ω through *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Corollary 1.7.3 (b). Strong induction, Logic and Proof, Theorem 4.2.2, holds on ω too, since its proof uses only Logic and Proof, Axiom 4.2.1 and the order facts *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Theorem 1.6.1 (a), (b), (d).

3.1.1 Four situations side by side

Look at four situations in which two things are combined into a third.

- In $(\mathbb{Z}, +)$ we add integers. The integer 0 does nothing, $a + 0 = a$, and $-a$ undoes a , $a + (-a) = 0$.
- In $\mathbb{Q} \setminus \{0\}$ we multiply. The rational 1 does nothing, and a^{-1} undoes a .
- Among the units of $\mathbb{Z}/12\mathbb{Z}$, which are $[1], [5], [7], [11]$ by *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Theorem 3.5.1 (the classes of the integers coprime to 12), we multiply classes. The class $[1]$ does nothing, and each unit undoes itself: $[5][5] = [25] = [1]$, $[7][7] = [49] = [1]$ and $[11][11] = [121] = [1]$, since $25 = 2 \cdot 12 + 1$, $49 = 4 \cdot 12 + 1$ and $121 = 10 \cdot 12 + 1$.
- Among the bijections $X \rightarrow X$ of a set we compose. The identity map id_X does nothing, and each bijection f is undone by its inverse f^{-1} (*Sets, Relations, and Cardinality*, Definition 1.5.2).

The objects differ, and so do the ways of combining them, but the rules used are the same three: the combining is associative, one element changes nothing, and every element can be undone. So we give the pattern a name.

A group is a set with one way of combining two elements into a third, in which combining is associative, some element does nothing, and every element can be undone.

Definition 3.1.1. Group

A **group** is a set G together with a **binary operation** on G , that is, a function $G \times G \rightarrow G$, $(a, b) \mapsto ab$ (*Sets, Relations, and Cardinality*, Definition 1.4.1, with $G \times G$ the Cartesian product of Sets, Relations, and Cardinality, Definition 1.3.2), such that:

- (G1) (**Associativity**) $(ab)c = a(bc)$ for all $a, b, c \in G$;
- (G2) (**Identity**) there is an element $e \in G$ with $ea = ae = a$ for every $a \in G$;
- (G3) (**Inverses**) for every $a \in G$ there is $b \in G$ with $ab = ba = e$, where e is the element of (G2).

The group is **abelian** if moreover $ab = ba$ for all $a, b \in G$.

In words: the operation is a function on pairs, so the combination of two elements of G lies

in G again. This “closure” is not a fourth axiom; it is built into the phrase “binary operation $G \times G \rightarrow G$ ”. (G1) says that the two ways of combining three elements in a fixed order agree. (G2) asks for an element that changes nothing, from **both** sides. (G3) asks that each element can be undone, again from both sides, back to that same e .

We write a group as $(G, \cdot)$, or simply G when the operation is clear, and call ab the **product** of a and b , whatever the operation is. When the operation is an addition we write $a + b$, 0 and $-a$ in place of ab , e and the inverse of a . This **additive notation** is used only for abelian groups.

Example. Groups

Check that each of (a)–(d) is a group, and decide which are abelian.

- (a) $(R, +)$ for a commutative ring R (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.1); in particular $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{Z}/n\mathbb{Z}, +)$ for $n \in \mathbb{Z}_{>0}$.
- (b) $(\mathbb{Q} \setminus \{0\}, \cdot)$, and $(F \setminus \{0\}, \cdot)$ for any field F ; in particular $(\mathbb{Z}/p\mathbb{Z} \setminus \{[0]\}, \cdot)$ for a prime p .
- (c) The set of bijections $X \rightarrow X$ of a set X , under composition $\circ$.
- (d) A one-element set $\{e\}$ with $ee := e$.
- (e) (A fifth situation, described here and checked in Section 3.4.) The four rotations of a square about its center, by no turn, a quarter turn, a half turn and three quarter turns. Label the corners $1, 2, 3, 4$ in order around the square; the quarter turn moves each label to the next corner, which is the bijection $i \mapsto i + 1$ for $i < 4$, $4 \mapsto 1$ of $\{1, 2, 3, 4\}$. Two rotations in a row make a rotation, the rotation by no turn changes nothing, and each rotation is undone by turning back.

Solution. (a) Recall the clauses (F1)–(F4) of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.1: addition is commutative (F1) and associative (F2), $a + 0 = a$ (F3), and $a + (-a) = 0$ (F4). Addition is a function $R \times R \rightarrow R$ by the definition, so it is a binary operation. (G1) is (F2). For (G2), $a + 0 = a$ is (F3), and $0 + a = a + 0 = a$ by (F1). For (G3), $a + (-a) = 0$ is (F4), and $(-a) + a = 0$ by (F1). The group is abelian by (F1). The instances: $\mathbb{Z}$ is a commutative ring by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.3.1, $\mathbb{Q}$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.4.3, $\mathbb{R}$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 5.3.3, and $\mathbb{Z}/n\mathbb{Z}$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.4.3 (a).

(b) Let F be a field (in the form of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.1; Chapter 2 restates the definition as Definition 2.1.1), for instance $F = \mathbb{Q}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.4.3). The first thing to check is that multiplication lands in $F \setminus \{0\}$. If $x \neq 0$ and $y \neq 0$, then x is a unit by (F8), and a unit is not a zero divisor (the paragraph after Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.5.1), so $xy \neq 0$. So a product of two non-zero elements is non-zero, and multiplication restricts to a binary operation on $F \setminus \{0\}$. (G1) is (F5). For (G2), $1 \neq 0$ in a field, so $1 \in F \setminus \{0\}$, and $a \cdot 1 = 1 \cdot a = a$ by (F7) and (F6). For (G3), let $a \neq 0$; then $aa^{-1} = a^{-1}a = 1$ by (F8) and (F6), and $a^{-1} \neq 0$, since $a^{-1} = 0$ would give $1 = a \cdot 0 = 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (b)). The group is abelian by (F6). For a prime p , $\mathbb{Z}/p\mathbb{Z}$ is a field by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.2, so $\mathbb{Z}/p\mathbb{Z} \setminus \{[0]\}$ is a group under multiplication.

(c) Composition of two bijections $X \rightarrow X$ is a bijection $X \rightarrow X$ by Sets, Relations, and Cardinality, Theorem 1.4.4 (c), so $\circ$ is a binary operation on the set of bijections. (G1) holds by Sets, Relations, and Cardinality, Proposition 1.4.3, and the same result gives $f \circ \text{id}_X =$

$f = \text{id}_X \circ f$, so id_X , a bijection, satisfies (G2). For (G3), a bijection f has a two-sided inverse f^{-1} by Sets, Relations, and Cardinality, Theorem 1.5.4, with $f^{-1} \circ f = \text{id}_X$ and $f \circ f^{-1} = \text{id}_X$ (Sets, Relations, and Cardinality, Definition 1.5.2). These two equations also say that f is a two-sided inverse of f^{-1} , so f^{-1} is a bijection, again by Sets, Relations, and Cardinality, Theorem 1.5.4.

Whether it is abelian depends on X ; the fold below decides it.

☞ **Second reading** · When is the group of bijections abelian?

If X has three distinct elements x, y, z , let f swap x and y and fix every other point, and let g swap y and z and fix every other point. Each is its own inverse ($f \circ f = \text{id}_X$), so each is a bijection. Then $(f \circ g)(x) = f(g(x)) = f(y) = x$, while $(g \circ f)(x) = g(f(x)) = g(x) = x$. So $f \circ g = g \circ f$, and the group is **not** abelian. If X has at most two elements, there are at most two bijections, id_X and the swap, and any two of them commute, since each commutes with id_X and with itself. Section 3.4 meets this group again for $X = \{1, \dots, n\}$ and computes in it.

(d) All three axioms reduce to $ee = e$: $(ee)e = e = e(ee)$, e is an identity, and e is its own inverse. This **trivial group** is the degenerate case. It is abelian, and it reappears in Section 3.2 as the smallest subgroup of every group.

(e) is not checked here. Section 3.4 writes the four rotations as permutations of $\{1, 2, 3, 4\}$, and its Exercise B3 shows that they behave exactly like $\mathbb{Z}/4\mathbb{Z}$ under addition.

Remark. The invertible $n \times n$ matrices over a field form a group under matrix multiplication; *Spaces and Maps*, the chapter “Matrices”, proves it. Nothing in this volume uses it.

Now non-examples, each a minimal change of an example above.

Example. Not Groups

For each of the following, say which of (G1)–(G3), or the binary operation itself, fails: $(\mathbb{Z}, \cdot)$; $(\mathbb{N}, +)$; $\mathbb{Z}$ with $a * b := a - b$; $\mathbb{Z}/6\mathbb{Z} \setminus \{[0]\}$ under multiplication.

Solution. $(\mathbb{Z}, \cdot)$. Replace addition by multiplication in (a). Multiplication is a binary operation on $\mathbb{Z}$, it is associative by (F5), and 1 is an identity by (F7) and (F6) (Number Systems: From $\mathbb{N}$ to $\mathbb{Z}$, Theorem 2.3.1). But (G3) fails at $a = 2$: if $2b = 1$ for some $b \in \mathbb{Z}$, then $2 \mid 1$, and Number Systems: From $\mathbb{N}$ to $\mathbb{Z}$, Proposition 3.1.1 (g) gives $2 = 1$ or $2 = -1$, which is false.

$(\mathbb{N}, +)$. Keep addition but shrink $\mathbb{Z}$ to $\mathbb{N}$. Addition still lands in $\mathbb{N}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{Z}$, Proposition 2.2.3 (a)), it is associative, and 0 is an identity, by (F1)–(F3) in $\mathbb{Z}$. But (G3) fails at $a = 1$: in $\mathbb{Z}$ the only b with $1 + b = 0$ is -1 (uniqueness of negatives, Number Systems: From $\mathbb{N}$ to $\mathbb{Z}$, Proposition 2.3.2 (a)), and $-1 < 0$, so $-1 \notin \mathbb{N}$ by Number Systems: From $\mathbb{N}$ to $\mathbb{Z}$, Theorem 2.3.4 (b).

$a * b := a - b$ on $\mathbb{Z}$. It is a binary operation, but (G1) fails: $(1 * 1) * 1 = 0 - 1 = -1$, while $1 * (1 * 1) = 1 - 0 = 1$.

$\mathbb{Z}/6\mathbb{Z} \setminus \{[0]\}$ under multiplication. Replace the prime p of (b) by 6. Here the operation itself fails: $[2]$ and $[3]$ lie in the set, but $[2][3] = [6] = [0]$ does not (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Example (Multiplication modulo six and modulo five)), so (G1)–(G3) are not even in question.

Warning. Check closure first. “ $\mathbb{Z}_{>0}$ under subtraction” is not a group, and not because an axiom fails: 1 and 2 are positive integers, but $1 - 2 = -1$ is not, so subtraction is not a binary operation on $\mathbb{Z}_{>0}$ at all. Before checking (G1)–(G3), check that combining two elements of the set gives an element of the set.

3.1.2 The basic laws, proved once

The rules we proved separately for functions (uniqueness of inverses) and for rings (uniqueness of 0, of $-a$, of u^{-1}) follow from the three axioms alone. We prove them once:

Theorem 3.1.1. Basic Properties of Groups

Let G be a group and $a, b, c \in G$.

- (1) The identity element of G is unique.
- (2) The inverse of a is unique. We denote it by a^{-1} .
- (3) $(a^{-1})^{-1} = a$ and $(ab)^{-1} = b^{-1}a^{-1}$.
- (4) **(Cancellation)** If $ab = ac$, then $b = c$. If $ba = ca$, then $b = c$.
- (5) The equations $ax = b$ and $ya = b$ have **exactly one** solution $x \in G$ and **exactly one** solution $y \in G$: $x = a^{-1}b$ and $y = ba^{-1}$.

Idea. Uniqueness is proved by taking two candidates and showing they are equal. For the identity, play the two identity properties against each other. For inverses, the only tools are (G1)–(G3), so insert e in a clever form and regroup. The candidate $b^{-1}a^{-1}$ for the inverse of ab is found by undoing the last step first, as with putting on socks and then shoes.

Proof. For (1), suppose e and e' both satisfy (G2). Then $e = ee'$, using that e' is an identity, and $ee' = e'$, using that e is one. Hence $e = e'$.

For (2), suppose b and b' both satisfy (G3) for a : $ab = ba = e$ and $ab' = b'a = e$. Multiply the equation $ab' = e$ on the left by b , and regroup by (G1):

$$b = be = b(ab') = (ba)b' = eb' = b',$$

where the first and last equalities are (G2), and $ba = e$ is used in the fourth.

For (3), the equations $aa^{-1} = a^{-1}a = e$ say that a is an inverse of a^{-1} , so $(a^{-1})^{-1} = a$ by

(2). Next, by (G1) twice, then (G3), (G2) and (G3),

$$(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1} = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e,$$

and in the same way $(b^{-1}a^{-1})(ab) = ((b^{-1}a^{-1})a)b = (b^{-1}(a^{-1}a))b = (b^{-1}e)b = b^{-1}b = e$. By (2), $(ab)^{-1} = b^{-1}a^{-1}$.

For (4), suppose $ab = ac$. Multiplying on the left by a^{-1} and using (G1),

$$b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = ec = c.$$

The second statement follows by multiplying on the right by a^{-1} .

For (5), $x = a^{-1}b$ is a solution, since $a(a^{-1}b) = (aa^{-1})b = eb = b$ by (G1), (G3) and (G2). If $ax = b$ and $ax' = b$, then $ax = ax'$, so $x = x'$ by (4). In the same way $y = ba^{-1}$ solves $ya = b$, since $(ba^{-1})a = b(a^{-1}a) = b$, and it is the only solution by the second half of (4). This proves the theorem. ■

Parts (2) and (4) use one move, and we give it a name: **multiply by the inverse**. To remove a factor from one side of an equation in a group, multiply both sides **on the same side** by its inverse, then regroup with (G1). The side matters, since a group need not be abelian; there is no “dividing by a ”.

Part (2) is the argument of Sets, Relations, and Cardinality, Proposition 1.5.3, that a left inverse and a right inverse of a function agree, with functions erased; the uniqueness of the inverse of a unit in Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Definition 3.5.1 is the same argument once more. Part (1) is the argument for the uniqueness of 0 and 1 in Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{N}\setminus)$, Proposition 2.3.2 (a). That is the point of the definition: a proof that uses only (G1)–(G3) holds in every group at once.

3.1.3 Products of many factors

Part (3) had to write every bracket out. To write $g_1g_2 \cdots g_r$ with no brackets at all, we must say which product it means, and then check that the brackets do not matter. The definition uses the recursion that defined finite sums and products of reals.

Definition 3.1.2. Product of a List

Let G be a group and $r \in \mathbb{N}$. A **list** of length r in G is a function $\{1, \dots, r\} \rightarrow G$, written $(g_1, \dots, g_r)$; for $r = 0$ it is the **empty list**. Its **product** $g_1g_2 \cdots g_r \in G$ is given by recursion: the product of the empty list is e , and

$$g_1 \cdots g_{j+1} := (g_1 \cdots g_j)g_{j+1} \quad \text{for } 0 \leq j < r,$$

where $g_1 \cdots g_j$ is the product of the shortened list $(g_1, \dots, g_j)$.

In words: start with e , and multiply on the right by one more entry at each stage. The product of a list of length 1 is $eg_1 = g_1$, the product of (g_1, g_2) is g_1g_2 , and $g_1g_2g_3$ means $(g_1g_2)g_3$: **the brackets are nested to the left** by definition.

This is the recursion of Sets, Relations, and Cardinality, Definition 2.3.1, stated there for prod-

ucts of real numbers and used here as a pattern with the group G in place of $\mathbb{R}$ and e in place of 1, as *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 3.3 used it for products of integers (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Definition 3.3.1). The recursion runs on $\mathbb{N}$ by Sets, Relations, and Cardinality, Theorem 2.3.1, after extending the list by $g_k := e$ for $k > r$; the “Finite lists” remark after Sets, Relations, and Cardinality, Definition 2.3.1 shows that the products up to r do not depend on the extension. That remark only multiplies on the right; it never reorders factors, so it holds in a group that is not abelian.

Proposition 3.1.2. Laws for Products of Lists

Let G be a group, and let $(g_1, \dots, g_r)$ and $(h_1, \dots, h_s)$ be lists in G .

- (a) **(Concatenation)** $(g_1 \cdots g_r)(h_1 \cdots h_s) = g_1 \cdots g_r h_1 \cdots h_s$, the product of the list $(g_1, \dots, g_r, h_1, \dots, h_s)$ of length $r + s$.
- (b) **(Brackets)** If $r \geq 1$, every bracketing of $g_1, \dots, g_r$, in this order, has the value $g_1 \cdots g_r$.
- (c) **(Inverses)** $(g_1 \cdots g_r)^{-1} = g_r^{-1} \cdots g_1^{-1}$.

Here a **bracketing** of a list of length $r \geq 1$ is a way of inserting brackets, built by one rule: a single entry g_1 is a bracketing of (g_1) , with value g_1 ; and for $r \geq 2$, a bracketing is $(B)(B')$, where B is a bracketing of a first part $(g_1, \dots, g_k)$ with $1 \leq k < r$ and B' is a bracketing of the rest $(g_{k+1}, \dots, g_r)$, with value the product of their values. For instance, $(g_1 g_2)(g_3 g_4)$ and $g_1(g_2(g_3 g_4))$ are bracketings of a list of length 4.

Idea. Each part is an induction that follows the recursion. For (a), induct on the length s of the second list: adding one entry to it multiplies both sides on the right by that entry, and (G1) moves the bracket. For (b), the outermost product of a bracketing joins two shorter bracketings, which the induction hypothesis turns into list products, and (a) joins those. For (c), part (3) of Theorem 3.1.1 reverses two factors at a time.

Proof.

- (a) Fix the list $(g_1, \dots, g_r)$ and write $P := g_1 \cdots g_r$. We prove the statement for every list $(h_1, \dots, h_s)$ by Logic and Proof, Axiom 4.2.1 on s . For $s = 0$, the right side is the product of $(g_1, \dots, g_r)$ itself, and the left side is $Pe = P$ by (G2). Suppose the statement holds for lists of length s , and let $(h_1, \dots, h_{s+1})$ be a list. Then

$$\begin{aligned} P(h_1 \cdots h_{s+1}) &= P((h_1 \cdots h_s)h_{s+1}) = (P(h_1 \cdots h_s))h_{s+1} \\ &= (g_1 \cdots g_r h_1 \cdots h_s)h_{s+1} = g_1 \cdots g_r h_1 \cdots h_{s+1}, \end{aligned}$$

by the recursion of Definition 3.1.2, then (G1), then the induction hypothesis for the shortened list $(h_1, \dots, h_s)$, and finally the recursion for the concatenated list at its last entry, h_{s+1} .

Parts (b) and (c) are proved in the fold below. This proves (a). ■

○ **Second reading** · Proofs of (b) and (c): brackets and inverses

Proof.

- (b) We use Logic and Proof, Theorem 4.2.2 on r , for the property “if $r \geq 1$, every bracketing of every list of length r has the value $g_1 \cdots g_r$ ”; for $r = 0$ there is nothing to prove. Let $r \geq 1$, and suppose the property holds for every smaller length. If $r = 1$, the only bracketing is g_1 , and $g_1 = eg_1$ is the product of (g_1) by (G2) and the recursion. If $r \geq 2$, a bracketing is $(B)(B')$ with B a bracketing of $(g_1, \dots, g_k)$ and B' a bracketing of $(g_{k+1}, \dots, g_r)$, where $1 \leq k < r$. Both lengths, k and $r - k$, are at least 1 and smaller than r , so by the hypothesis the value of B is $g_1 \cdots g_k$ and the value of B' is $g_{k+1} \cdots g_r$. By (a), their product is the product of the concatenated list, which is $(g_1, \dots, g_r)$. So the value of $(B)(B')$ is $g_1 \cdots g_r$. This completes the induction.
- (c) By Logic and Proof, Axiom 4.2.1 on r . For $r = 0$, both sides are e , since $ee = e$ makes e its own inverse (Theorem 3.1.1 (2)). Suppose the statement holds for lists of length r , and let $(g_1, \dots, g_{r+1})$ be a list. Then

$$\begin{aligned} (g_1 \cdots g_{r+1})^{-1} &= ((g_1 \cdots g_r) g_{r+1})^{-1} = g_{r+1}^{-1} (g_1 \cdots g_r)^{-1} \\ &= g_{r+1}^{-1} (g_r^{-1} \cdots g_1^{-1}) = g_{r+1}^{-1} g_r^{-1} \cdots g_1^{-1}, \end{aligned}$$

by the recursion, Theorem 3.1.1 (3), the induction hypothesis, and (a) with the list (g_{r+1}^{-1}) of length 1, whose product is g_{r+1}^{-1} . This proves the proposition. ■

By part (b), **from now on we drop brackets** from products in a group, regrouping in any way that keeps the order of the factors. The order itself may not change, unless the group is abelian (Exercise C3).

3.1.4 Integer powers

The commonest list is a constant one. A product of n copies of g is the power g^n , and the inverse of g^n deserves to be a power too.

Definition 3.1.3. Integer Powers

Let G be a group and $g \in G$. For $n \in \mathbb{N}$, the **power** g^n is the product of the constant list $(g, \dots, g)$ of length n ; so

$$g^0 = e, \quad g^{n+1} = g^n g \quad \text{for } n \in \mathbb{N}.$$

For $n \in \mathbb{Z}$ with $n < 0$, write $n = -m$ with $m \in \mathbb{N}$ (Number Systems: From $\mathbb{N}$ to $\mathbb{Z}$), Proposition 2.2.3 (c)), and set $g^n := (g^{-1})^m$. In additive notation the power is the **multiple** $n \cdot g$: $0 \cdot g = 0$, $(n + 1) \cdot g = n \cdot g + g$, and $(-m) \cdot g = m \cdot (-g)$.

The two clauses do not overlap, since $n < 0$ and $n \in \mathbb{N}$ exclude each other (Number Systems: From $\mathbb{N}$ to $\mathbb{Z}$), Theorem 2.3.4 (b)), and for $n < 0$ the m is $-n$, so g^n is well defined.

The new notation agrees with the old one: $g^1 = eg = g$, and $g^{-1} = (g^{-1})^1$ is the inverse of g . So $g^2 = gg$ and $g^{-2} = g^{-1}g^{-1}$.

The power laws look like school algebra, but the school proofs commute factors; here only (d) may, and it says so:

Proposition 3.1.3. Power Laws in a Group

Let G be a group, $g, h \in G$ and $m, n \in \mathbb{Z}$.

- (a) $g^m g^n = g^{m+n}$.
- (b) $(g^m)^{-1} = g^{-m} = (g^{-1})^m$.
- (c) $(g^m)^n = g^{mn}$.
- (d) If $gh = hg$, then $(gh)^n = g^n h^n$.
- (e) Let R be a commutative ring. In the group $(R, +)$, for $a \in R$ and $n \in \mathbb{N}$, the multiple $n \cdot a$ of Definition 3.1.3 is the multiple $n \cdot a$ of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Section 2.3. In $(\mathbb{Z}, +)$, $n \cdot a = na$, the product in the ring $\mathbb{Z}$, for all $n, a \in \mathbb{Z}$.

Idea. For exponents in $\mathbb{N}$, a power is a list product, and (a) is concatenation. Negative exponents are reduced to natural ones by one fact: g^m and $(g^{-1})^m$ are inverse to each other, because the factors cancel in pairs from the middle out, $g \cdots g g^{-1} \cdots g^{-1} = e$. With that, each sign case of (a) is a natural-number case for g or for g^{-1} . Parts (c) and (d) are inductions on $n \in \mathbb{N}$, extended to $n < 0$ by (b).

Second reading · Proof of the power laws

Proof. (a) for $m, n \in \mathbb{N}$. The left side is the product of the constant list of length m times that of length n . By Proposition 3.1.2 (a) it is the product of the concatenated list, the constant list of length $m + n$, which is g^{m+n} .

(b). First let $m \in \mathbb{N}$. We show $g^m (g^{-1})^m = e$ by Logic and Proof, Axiom 4.2.1 on m . For $m = 0$, $ee = e$. For the step, $g^{m+1} = g^1 g^m = gg^m$ by (a) on $\mathbb{N}$, and $(g^{-1})^{m+1} = (g^{-1})^m g^{-1}$ by the definition, so, dropping brackets (Proposition 3.1.2 (b)),

$$g^{m+1} (g^{-1})^{m+1} = g(g^m (g^{-1})^m) g^{-1} = geg^{-1} = e.$$

So $x = (g^{-1})^m$ solves $g^m x = e$. By Theorem 3.1.1 (5) the only solution is $(g^m)^{-1} e = (g^m)^{-1}$; hence $(g^m)^{-1} = (g^{-1})^m$. This is also g^{-m} : for $m > 0$ by the definition of negative powers, and for $m = 0$ because $g^0 = e = (g^{-1})^0$.

Now let $m < 0$, and write $m = -k$ with $k \in \mathbb{N}$. By the definition, $g^m = (g^{-1})^k$. The case just proved, applied to the element g^{-1} and the exponent k , gives $((g^{-1})^k)^{-1} = ((g^{-1})^{-1})^k = g^k$, by Theorem 3.1.1 (3). So $(g^m)^{-1} = g^k = g^{-m}$. Finally $(g^{-1})^m = ((g^{-1})^{-1})^k = g^k$ by the definition of negative powers, applied to the element g^{-1} . This proves (b). In particular,

$$(g^{-1})^p = g^{-p} \quad \text{for every } p \in \mathbb{Z}. \quad (*)$$

(a) in general. We first show, for $m, k \in \mathbb{N}$,

$$g^m g^{-k} = g^{m-k}. \quad (**)$$

By (b), $g^{-k} = (g^{-1})^k$, and $g^k(g^{-1})^k = e$ (shown in (b)). If $m \geq k$, then $m - k \in \mathbb{N}$ and $g^m = g^{m-k} g^k$ by (a) on $\mathbb{N}$, so $g^m(g^{-1})^k = g^{m-k} g^k(g^{-1})^k = g^{m-k}$. If $m < k$, then $k - m \in \mathbb{N}$, and $(g^{-1})^k = (g^{-1})^m (g^{-1})^{k-m}$ by (a) on $\mathbb{N}$ for the element g^{-1} ; since $g^m(g^{-1})^m = e$, we get $g^m(g^{-1})^k = (g^{-1})^{k-m} = g^{-(k-m)} = g^{m-k}$, by (*).

Now let $m, n \in \mathbb{Z}$, and write $u := g^{-1}$, so that $g^p = u^{-p}$ for every $p \in \mathbb{Z}$ by (*) and $(g^{-1})^{-1} = g$. There are four cases. If $m, n \geq 0$, this is (a) on $\mathbb{N}$. If $m \geq 0 > n$, write $n = -k$; this is (**). If $m < 0 \leq n$, write $m = -j$; then $g^m g^n = u^j u^{-n} = u^{j-n} = g^{n-j} = g^{m+n}$, by (**) for u and then (*). If $m, n < 0$, write $m = -j$, $n = -k$; then $g^m g^n = u^j u^k = u^{j+k} = g^{-(j+k)} = g^{m+n}$, by (a) on $\mathbb{N}$ for u and (*). The identities between exponents used here, such as $n - j = m + n$, are ring arithmetic in $\mathbb{Z}$ (Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Theorem 2.3.1).

(c). For $n \in \mathbb{N}$, by Logic and Proof, Axiom 4.2.1 on n : $(g^m)^0 = e = g^0$, and $(g^m)^{n+1} = (g^m)^n g^m = g^{mn} g^m = g^{mn+m} = g^{m(n+1)}$, by the definition, the hypothesis, (a), and (F9) in $\mathbb{Z}$. For $n < 0$, write $n = -k$; then

$$(g^m)^n = ((g^m)^{-1})^k = (g^{-m})^k = g^{(-m)k} = g^{m(-k)} = g^{mn},$$

by the definition, (b), the case $k \in \mathbb{N}$ for the exponent $-m$, and Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Proposition 2.3.2 (c).

(d). Suppose $gh = hg$. First, $gh^n = h^n g$ for $n \in \mathbb{N}$, by Logic and Proof, Axiom 4.2.1: for $n = 0$ both sides are g , and $gh^{n+1} = (gh^n)h = h^n gh = h^n hg = h^{n+1}g$. Next, $(gh)^n = g^n h^n$ for $n \in \mathbb{N}$, again by induction: for $n = 0$ both sides are e , and

$$(gh)^{n+1} = (gh)^n gh = g^n h^n gh = g^n gh^n h = g^{n+1} h^{n+1},$$

using $h^n g = gh^n$ and (a). For $n < 0$, write $n = -k$. Taking inverses in $gh = hg$ gives $h^{-1}g^{-1} = g^{-1}h^{-1}$ (Theorem 3.1.1 (3)), so g^{-1} and h^{-1} commute too. Hence

$$(gh)^n = ((gh)^{-1})^k = (h^{-1}g^{-1})^k = (g^{-1}h^{-1})^k = (g^{-1})^k (h^{-1})^k = g^n h^n,$$

by the definition, Theorem 3.1.1 (3), the commuting just shown, the case $k \in \mathbb{N}$ for the commuting pair g^{-1}, h^{-1} , and the definition again.

(e). For $n \in \mathbb{N}$, both multiples are given by the same two clauses, $0 \cdot a = 0$ and $(n+1) \cdot a = n \cdot a + a$, so they are the same function $\mathbb{N} \rightarrow R$ by the uniqueness in Sets, Relations, and Cardinality, Theorem 2.3.1. In $\mathbb{Z}$, Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Section 2.3 shows $n \cdot a = na$ for $n \in \mathbb{N}$ (the paragraph “Multiples”, before Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Proposition 2.3.5). For $n = -m$ with $m \in \mathbb{N}$, $(-m) \cdot a = m \cdot (-a) = m(-a) = (-m)a$, by Definition 3.1.3, the case $n \in \mathbb{N}$, and Number Systems: From $\backslash(\backslash\mathbb{N}\backslash)$ to $\backslash(\backslash\mathbb{N}\mathbb{R}\backslash)$, Proposition 2.3.2 (c). This proves the proposition. ■

Part (d) needs $gh = hg$: without it the law fails, and Section 3.4 exhibits a failure with two permutations of $\{1, 2, 3\}$.

🕒 **Second reading** · *Multiples in Chapters 2 and 3 agree*

Remark. For $n = -m < 0$, part (b) in additive notation reads $m \cdot (-a) = -(m \cdot a)$, so the multiple $(-m) \cdot a = m \cdot (-a)$ of [Definition 3.1.3](#) equals $-(m \cdot a)$. That is how Section 2.5 defines $n \cdot a$ for $n < 0$ in a commutative ring. So “ $n \cdot a$ ” means the same thing in Chapters 2 and 3 for every $n \in \mathbb{Z}$, and the identities of Lemma 2.5.1 apply to the multiples of the group $(R, +)$. No proof in this chapter rests on this comparison; Exercise R1 of Section 3.5 needs only part (e).

3.1.5 The units of a commutative ring form a group

Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Section 3.5 found the units of a commutative ring R , the elements u with $uv = 1$ for some $v \in R$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.5.1), and showed in the paragraph after the definition that 1 is a unit, that products and inverses of units are units, and that the inverse u^{-1} is unique. In the language of this section:

Proposition 3.1.4. The Units Form a Group

Let R be a commutative ring. Then $R^\times$, the set of units of R , is an abelian group under the multiplication of R , with identity 1, and the inverse of u in this group is u^{-1} .

Proof. By the paragraph after Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.5.1, a product of two units is a unit, so multiplication restricts to a binary operation on $R^\times$. (G1) holds by (F5) of Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 2.3.1. For (G2), 1 is a unit since $1 \cdot 1 = 1$, and $u \cdot 1 = 1 \cdot u = u$ by (F7) and (F6). For (G3), let $u \in R^\times$. Then $uu^{-1} = u^{-1}u = 1$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.5.1 and (F6), and u^{-1} is itself a unit, by the same paragraph. The group is abelian by (F6). This proves the proposition. ■

So the third situation at the start of the section was the group $(\mathbb{Z}/12\mathbb{Z})^\times$. More examples:

- $\mathbb{Z}^\times = \{1, -1\}$ (the examples after Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Definition 3.5.1), a group with two elements.
- $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] : \gcd(a, n) = 1\}$ for $n \in \mathbb{Z}_{>0}$, by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 3.5.1. For $n = 8$ it is $\{[1], [3], [5], [7]\}$, and every element is its own inverse: $[3][3] = [9] = [1]$, $[5][5] = [25] = [1]$, $[7][7] = [49] = [1]$.
- $F^\times = F \setminus \{0\}$ for a field F : every non-zero element is a unit by (F8), and 0 is not, since $0 \cdot v = 0 \neq 1$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.2 (b)). So the group of [Example \(Groups\)](#) (b) is $F^\times$.

Quick check. In $(\mathbb{Z}/7\mathbb{Z})^\times$, find $[3]^{-1}$ and $[3]^{-2}$.

Solution. $[3]^{-1} = [5]$, since $3 \cdot 5 = 15 = 2 \cdot 7 + 1$, so $[3][5] = [1]$. By [Definition 3.1.3](#), $[3]^{-2} = ([3]^{-1})^2 = [5][5] = [25] = [4]$, since $25 = 3 \cdot 7 + 4$. Check: $[3]^2[4] = [9][4] = [36] = [1]$, as $36 = 5 \cdot 7 + 1$.

3.1.6 Exercises

3.1.6.1 A. Check your understanding

Exercise. A1

- State the axioms (G1)–(G3), and say where in the definition of a group closure is required.
- Is $\mathbb{Z}$ with $a * b := a + b + 1$ a group? Justify your answer.
- True or false: in every group, $(ab)^{-1} = a^{-1}b^{-1}$. Justify your answer.
- Compute $3 \cdot [5]$ and $(-2) \cdot [5]$ in the group $(\mathbb{Z}/7\mathbb{Z}, +)$.

Solution.

- (G1) $(ab)c = a(bc)$ for all $a, b, c \in G$; (G2) there is $e \in G$ with $ea = ae = a$ for every $a \in G$; (G3) for every $a \in G$ there is $b \in G$ with $ab = ba = e$. Closure is not an axiom of its own: it is required by “binary operation”, a function $G \times G \rightarrow G$, whose values lie in G .
- Yes. The rule is a function $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$. (G1): both $(a * b) * c = (a + b + 1) + c + 1$ and $a * (b * c) = a + (b + c + 1) + 1$ equal $a + b + c + 2$, by (F1) and (F2). (G2): $e = -1$ works, since $a * (-1) = a + (-1) + 1 = a$ and $(-1) * a = a$ likewise. (G3): the inverse of a is $-a - 2$, since $a * (-a - 2) = a - a - 2 + 1 = -1$, and the other order gives the same by (F1). It is abelian, since $a + b + 1 = b + a + 1$.
- False. Let f and g be the bijections of $\{1, 2, 3\}$ with f swapping 1, 2 and g swapping 2, 3, each fixing the third point; each is its own inverse. Then $f \circ g$ sends $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$ (for instance $(f \circ g)(2) = f(3) = 3$), so its inverse sends $1 \mapsto 3$. But $f^{-1} \circ g^{-1} = f \circ g$ sends $1 \mapsto 2$. So $(f \circ g)^{-1} \neq f^{-1} \circ g^{-1}$. The correct rule is $(ab)^{-1} = b^{-1}a^{-1}$ ([Theorem 3.1.1](#) (3)); in an abelian group $b^{-1}a^{-1} = a^{-1}b^{-1}$, so there the statement is true.
- By [Definition 3.1.3](#), $3 \cdot [5] = [5] + [5] + [5] = [15] = [1]$, since $15 = 2 \cdot 7 + 1$. Next $-[5] = [-5] = [2]$, so $(-2) \cdot [5] = 2 \cdot [2] = [4]$.

3.1.6.2 B. Practice

Exercise. B1: Groups or not

Determine which of the following are groups. Justify your answer.

- $\mathbb{Q}_{>0}$ under multiplication.

- (b) $\{1, -1\} \subseteq \mathbb{Z}$ under multiplication.
- (c) The odd integers under addition.
- (d) $\{[1], [3], [5], [7]\} \subseteq \mathbb{Z}/8\mathbb{Z}$ under multiplication.
- (e) $\mathbb{Z}/6\mathbb{Z} \setminus \{[0]\}$ under multiplication.

Solution.

- (a) A group. $\mathbb{Q}$ is an ordered field (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Theorem 2.5.1), so a product of positive rationals is positive by (O4), and multiplication is a binary operation on $\mathbb{Q}_{>0}$. Associativity is (F5), and $1 > 0$ (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.5 (e)) is an identity. For $x > 0$, x^{-1} exists since $x \neq 0$, and $x^{-1} > 0$ by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.5.2 (a). So the inverse stays in $\mathbb{Q}_{>0}$.
- (b) A group: it is $\mathbb{Z}^\times$, a group by Proposition 3.1.4.
- (c) Not a group: addition is not a binary operation on the odd integers, since $1 + 1 = 2$ is even and so not odd (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Corollary 3.1.3 (a)).
- (d) A group: it is $(\mathbb{Z}/8\mathbb{Z})^\times$ (the examples after Proposition 3.1.4), and every element is its own inverse.
- (e) Not a group: $[2][3] = [0]$, so multiplication is not a binary operation on the set (Example (Not Groups)).

Exercise. B2: An element equal to its square

Let G be a group and $g \in G$ with $gg = g$. Prove that $g = e$.

The first step is given: by (G2), $gg = g = ge$.

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

Solution. The move is **multiply by the inverse**: g appears on the left of both sides, so multiply both sides on the left by g^{-1} and regroup.

Completion: from $gg = ge$, cancellation (Theorem 3.1.1 (4)) gives $g = e$. Written out, $g = (g^{-1}g)g = g^{-1}(gg) = g^{-1}(ge) = (g^{-1}g)e = e$.

Exercise. B3: Powers of a conjugate

Let G be a group and $g, h \in G$. Prove that $(ghg^{-1})^n = gh^n g^{-1}$ for every $n \in \mathbb{Z}$.

Solution. For $n \in \mathbb{N}$, by Logic and Proof, Axiom 4.2.1 on n . For $n = 0$, both sides are e , since $geg^{-1} = gg^{-1} = e$. Suppose $(ghg^{-1})^n = gh^n g^{-1}$. Then, dropping brackets (Proposition 3.1.2 (b)),

$$(ghg^{-1})^{n+1} = (ghg^{-1})^n ghg^{-1} = gh^n g^{-1} ghg^{-1} = gh^n hg^{-1} = gh^{n+1} g^{-1},$$

by Definition 3.1.3, the hypothesis, $g^{-1}g = e$, and Definition 3.1.3 again.

For $n < 0$, write $n = -k$ with $k \in \mathbb{N}$. By Proposition 3.1.3 (b), the case just proved, and Proposition 3.1.2 (c),

$$(ghg^{-1})^n = ((ghg^{-1})^k)^{-1} = (gh^k g^{-1})^{-1} = (g^{-1})^{-1} (h^k)^{-1} g^{-1} = gh^{-k} g^{-1},$$

where the last step uses Theorem 3.1.1 (3) and Proposition 3.1.3 (b). This proves the identity for every $n \in \mathbb{Z}$.

3.1.6.3 C. Going deeper

Exercise. C1: Exit check: the basic laws of a group

Prove parts (1)–(3) of Theorem 3.1.1 from (G1)–(G3) only: the identity is unique; the inverse of each element is unique; and $(a^{-1})^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$.

Solution (Hint 1). For uniqueness, take two candidates and compute one expression in two ways.

Solution (Hint 2). For inverses, let b and b' both be inverses of a , and start from $b = be$.

Solution. The proof of (1)–(3) in Theorem 3.1.1 is a complete answer. In outline: two identities e, e' give $e = ee' = e'$; two inverses b, b' of a give $b = be = b(ab') = (ba)b' = eb' = b'$; a is an inverse of a^{-1} , so $(a^{-1})^{-1} = a$ by uniqueness; and $(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1} = (a(bb^{-1}))a^{-1} = e$ and $(b^{-1}a^{-1})(ab) = ((b^{-1}a^{-1})a)b = (b^{-1}(a^{-1}a))b = e$, so $(ab)^{-1} = b^{-1}a^{-1}$ by uniqueness.

Marking scheme. (10 points) - 2: uniqueness of the identity, with each of the two identity properties named where it is used. - 3: uniqueness of inverses, by inserting $e = ab'$ (or an equivalent use of (G2) and (G3)) and regrouping, with each step named. - 1: $(a^{-1})^{-1} = a$, by reading $aa^{-1} = a^{-1}a = e$ as “ a is an inverse of a^{-1} ” and citing uniqueness. - 3: $(ab)(b^{-1}a^{-1}) = e$, with (G1) named, **and** $(b^{-1}a^{-1})(ab) = e$. - 1: the conclusion $(ab)^{-1} = b^{-1}a^{-1}$, citing uniqueness of inverses. Fatal errors (0 for the step): using commutativity; “dividing” by an element. Checking only one product earns 1 of those 3 points (not fatal), or all 4 points for $(ab)^{-1}$ with a proof from (G1)–(G3) that a one-sided inverse is the inverse ($xy = e$ or $yx = e$ implies $y = x^{-1}$). A proof of uniqueness of inverses through cancellation earns the 3 points only if cancellation is itself proved from (G1)–(G3).

Exercise. C2: Find the error

Here is a statement and an argument for it.

Claim. In every group, $(ab)^{-1} = b^{-1}a^{-1}$.

Argument. (1) By (G1)–(G3), $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$.
 (2) Since $xy = yx$ for all x, y in a group, also $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = e$.
 (3) So $b^{-1}a^{-1}$ is a two-sided inverse of ab , and $(ab)^{-1} = b^{-1}a^{-1}$ by uniqueness of

inverses.

Is the claim true? Does the argument prove it? If not, name the line that fails, explain why, and give a counterexample to the step.

Solution. The claim is **true**: it is [Theorem 3.1.1](#) (3). The argument does **not** prove it.

Lines (1) and (3) are correct. The failing line is (2), and only (2). It rests on the general “fact” that any two elements of a group commute. That is not an axiom, it has not been proved, and it is false, so the line cites nothing: entry (N9) of Logic and Proof, Example (What is not allowed). A counterexample to the step: the bijections f, g of $\{1, 2, 3\}$ in A1 (c), with $(f \circ g)(1) = 2$ and $(g \circ f)(1) = g(2) = 3$, so $f \circ g \neq g \circ f$. There is no counterexample to the conclusion, which is true.

The repair is to compute the second product as the first one was computed, with (G1): $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$. Alternatively, line (1) alone suffices: it says that $b^{-1}a^{-1}$ solves $y(ab) = e$, whose only solution is $e(ab)^{-1} = (ab)^{-1}$ by [Theorem 3.1.1](#) (5).

Exercise. C3: Rearranging in an abelian group

Let G be an abelian group and $(g_1, \dots, g_r)$ a list in G with $r \geq 2$.

- Prove that swapping two adjacent entries g_i, g_{i+1} ($1 \leq i < r$) does not change the product of the list.
- Deduce that the product does not change under any rearrangement obtained by finitely many such adjacent swaps.

Solution.

- By [Proposition 3.1.2](#) (a) and (b), the product of the list is the bracketing

$$(g_1 \cdots g_{i-1})(g_i g_{i+1})(g_{i+2} \cdots g_r),$$

where an empty product is e . The list with g_i and g_{i+1} swapped has, in the same way, the product $(g_1 \cdots g_{i-1})(g_{i+1} g_i)(g_{i+2} \cdots g_r)$. Since G is abelian, $g_i g_{i+1} = g_{i+1} g_i$, so the two products are equal.

- By Logic and Proof, Axiom 4.2.1 on the number k of swaps: for $k = 0$ the list is unchanged, and a rearrangement by $k + 1$ swaps is one swap applied to a rearrangement by k swaps, whose product equals the original product by the hypothesis; the last swap does not change the product, by (a).

Section 3.5 proves that every permutation of $\{1, \dots, r\}$ is a product of adjacent transpositions; read for lists, every rearrangement is obtained by adjacent swaps, and so the product of a list in an abelian group does not depend on the order of the factors.

Marking scheme. (10 points) - 3: (a) brackets both products as $(g_1 \cdots g_{i-1})(\cdot)(g_{i+2} \cdots g_r)$, citing [Proposition 3.1.2](#), with the empty product read as e when $i = 1$ or $i + 1 = r$. - 2: (a) uses $g_i g_{i+1} = g_{i+1} g_i$ (abelian) to conclude that the products agree. - 1: (b) names the induction and its variable, the number of swaps. - 2: (b) base case: zero swaps leave the list

unchanged. - 2: (b) step: writes a rearrangement by $k + 1$ swaps as one swap after k swaps and applies (a) to the intermediate list. Fatal errors (0 for the step): (a) swaps the two entries inside a product written without brackets, with no appeal to the list-product laws; (b) “and so on” in place of an induction.