

3.5 Transpositions Generate the Symmetric Group

Section 3.4 wrote permutations in cycle notation and showed that every permutation breaks into disjoint cycles (Theorem 3.4.4). One small computation there, $(1\ 3)(1\ 2) = (1\ 2\ 3)$ in Example (Computing with Cycles), says more than it seems to: a 3-cycle is two swaps. This section shows that every permutation of $\{1, \dots, n\}$, for $n \geq 2$, is a product of swaps of two points. The determinant of linear algebra is built on exactly this fact, and so is the sign of a permutation, which later volumes define.

Throughout, $n \in \mathbb{N}$, products of permutations are read **right to left** (Definition 3.4.1: $\sigma\tau = \sigma \circ \tau$ applies τ first), and a product $\tau_1\tau_2 \cdots \tau_r$ is the product of a list in the group S_n (Definition 3.1.2), so brackets may be dropped (Proposition 3.1.2 (b)).

3.5.1 Cycles as products of transpositions

Recall from Definition 3.4.2 that a **transposition** is a 2-cycle $(a\ b)$, with $a \neq b$: it swaps a and b and fixes every other point. Two facts about it are used constantly below.

- $(a\ b) = (b\ a)$, since both swap a and b and fix the rest (Sets, Relations, and Cardinality, Proposition 1.4.1).
- A transposition is its own inverse: $(a\ b)(a\ b) = \text{id}$. Indeed $a \mapsto b \mapsto a$, $b \mapsto a \mapsto b$, and every other point is fixed twice. Equivalently, the inverse of $(a\ b)$ is $(b\ a) = (a\ b)$ (Definition 3.4.2).

The computation $(1\ 3)(1\ 2) = (1\ 2\ 3)$ has a pattern: both transpositions contain the first entry 1 of the cycle, and the one applied **first** is $(1\ 2)$, which sends 1 to the next entry. Longer cycles follow the same pattern.

Proposition 3.5.1. A Cycle Is a Product of Transpositions

Let $k \geq 2$, and let $i_1, i_2, \dots, i_k \in \{1, \dots, n\}$ be **distinct**. Then

$$(i_1\ i_2\ \cdots\ i_k) = (i_1\ i_k)(i_1\ i_{k-1}) \cdots (i_1\ i_2),$$

a product of $k - 1$ transpositions.

Read right to left, the factors are $(i_1\ i_2)$, then $(i_1\ i_3)$, and so on up to $(i_1\ i_k)$. For $k = 4$: $(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2)$. Follow 2: the first factor $(1\ 2)$ sends it to 1, the second sends 1 to 3, and the third fixes 3; so $2 \mapsto 3$, as the cycle requires.

Idea. Induct on the length. To pass from $(i_1\ \cdots\ i_k)$ to $(i_1\ \cdots\ i_k\ i_{k+1})$, the only change is that i_k must now go to i_{k+1} instead of back to i_1 , and i_{k+1} must go to i_1 . One more swap of i_1 and i_{k+1} , applied **after** the shorter cycle, makes exactly this change.

Proof. We prove, by Sets, Relations, and Cardinality, Theorem 2.2.1 with base 2 (read on ω by Number Systems: From $\mathbb{N}$ to $\mathbb{R}$), Corollary 1.7.3 (b)), the statement $P(k)$: “for every list $(i_1, \dots, i_k)$ of distinct points of $\{1, \dots, n\}$, the displayed equation holds”.

Base, $k = 2$. The right-hand side is the list of one factor $(i_1 \ i_2)$, whose product is $(i_1 \ i_2)$ (Definition 3.1.2), and this is the left-hand side.

Step. Let $k \geq 2$, suppose $P(k)$, and let $i_1, \dots, i_{k+1}$ be distinct. Put $\gamma := (i_1 \ \dots \ i_k)$ and $\tau := (i_1 \ i_{k+1})$. We claim $\tau\gamma = (i_1 \ \dots \ i_{k+1})$, and check it point by point (Sets, Relations, and Cardinality, Proposition 1.4.1).

- For $1 \leq j < k$: $\gamma(i_j) = i_{j+1}$, which is neither i_1 (as $j + 1 \geq 2$) nor i_{k+1} (as $j + 1 \leq k$), the entries being distinct; so τ fixes it: $\tau\gamma(i_j) = i_{j+1}$.
- $\gamma(i_k) = i_1$ and $\tau(i_1) = i_{k+1}$: so $\tau\gamma(i_k) = i_{k+1}$.
- i_{k+1} is not among $i_1, \dots, i_k$, so γ fixes it, and $\tau(i_{k+1}) = i_1$: so $\tau\gamma(i_{k+1}) = i_1$.
- Every other point x is fixed by γ and by τ .

These are the values of the $(k + 1)$ -cycle (Definition 3.4.2), which proves the claim. By $P(k)$ and the concatenation law Proposition 3.1.2 (a), applied to the list (τ) and the list $((i_1 \ i_k), \dots, (i_1 \ i_2))$,

$$(i_1 \ \dots \ i_{k+1}) = \tau\gamma = (i_1 \ i_{k+1})(i_1 \ i_k) \cdots (i_1 \ i_2),$$

which is $P(k + 1)$. This proves the proposition. ■

The proof never used that the cycle starts at its smallest entry, so the formula may be applied to any way of writing the cycle. Writing $(1 \ 2 \ 3)$ as $(2 \ 3 \ 1)$ gives $(2 \ 1)(2 \ 3) = (1 \ 2)(2 \ 3)$, a second word for the same permutation; we return to this below.

Quick check. Write $(2 \ 5 \ 3)$ as a product of transpositions, and check your answer point by point.

Solution. By Proposition 3.5.1 with $i_1 = 2$, $i_2 = 5$, $i_3 = 3$: $(2 \ 5 \ 3) = (2 \ 3)(2 \ 5)$. Check, applying $(2 \ 5)$ first: $2 \mapsto 5 \mapsto 5$, $5 \mapsto 2 \mapsto 3$, $3 \mapsto 3 \mapsto 2$, and every other point is fixed. So $2 \mapsto 5$, $5 \mapsto 3$, $3 \mapsto 2$, which is $(2 \ 5 \ 3)$.

3.5.2 Every permutation is a product of transpositions

We say that $\sigma \in S_n$ is a **product of transpositions** if $\sigma = \tau_1\tau_2 \cdots \tau_r$ for some $r \geq 1$ and transpositions $\tau_1, \dots, \tau_r \in S_n$. The words “ $r \geq 1$ ” matter for one permutation only: the identity is always the empty product (Definition 3.1.2), but it is a product of **at least one** transposition only when a transposition exists, that is, when $n \geq 2$. Then $\text{id} = (1 \ 2)(1 \ 2)$. More generally, for a set $T \subseteq S_n$, σ is a **product of elements of T** if $\sigma = t_1t_2 \cdots t_r$ for some $r \geq 1$ and $t_1, \dots, t_r \in T$, and T **generates** S_n if every $\sigma \in S_n$ is a product of elements of T . The theorem below says that the transpositions generate S_n for $n \geq 2$, and its corollary says the same for the adjacent transpositions.

Theorem 3.5.2. Transpositions Generate S_n

Let $n \geq 2$. Every $\sigma \in S_n$ is a product of transpositions.

Try it first (ten minutes): write $(1\ 2\ 3\ 4)$ and $(1\ 3)(2\ 4)$ as products of transpositions. Then let $\sigma \in S_4$ with $\sigma(4) \neq 4$: which single transposition τ makes $\tau\sigma$ fix 4?

Idea. The two examples are easy: the first is $(1\ 4)(1\ 3)(1\ 2)$ by Proposition 3.5.1, and the second is already a product of two transpositions. They suggest a route through Theorem 3.4.4, and that route works (the remark after the proof). But it hides where the transpositions come from. The second question points to a route that needs no cycles at all: induction on n . What is the smaller object inside a permutation of $n+1$ points? If σ fixes $n+1$, it is really a permutation of $\{1, \dots, n\}$, and Lemma 3.4.1 makes that precise. If not, say $\sigma(n+1) = k$, one swap repairs it: $\tau := (k\ n+1)$ sends k back to $n+1$, so $\tau\sigma$ fixes $n+1$. Apply the first case to $\tau\sigma$, then undo the swap. In one phrase: **fix one point, then induct.**

Before reading on: why does $\tau\sigma$ fix $n+1$, and why is that the right thing to aim for?

Proof. We use Sets, Relations, and Cardinality, Theorem 2.2.1 with base 2 (read on ω by Number Systems: From $\setminus(\setminus n \setminus)$ to $\setminus(\setminus n \mathbb{R} \setminus)$, Corollary 1.7.3 (b)) on $n \geq 2$.

Base, $n = 2$. Let $\sigma \in S_2$. If $\sigma(1) = 1$, then $\sigma(2) \neq 1$ since σ is injective, so $\sigma(2) = 2$ and $\sigma = \text{id}$ (Sets, Relations, and Cardinality, Proposition 1.4.1). If $\sigma(1) = 2$, then $\sigma(2) = 1$ in the same way, and $\sigma = (1\ 2)$. So $S_2 = \{\text{id}, (1\ 2)\}$. Here $(1\ 2)$ is one transposition and $\text{id} = (1\ 2)(1\ 2)$ is two.

Step. Let $n \geq 2$, suppose that every element of S_n is a product of transpositions, and let $\sigma \in S_{n+1}$. For $\rho \in S_n$, write $\bar{\rho} \in S_{n+1}$ for its extension, $\bar{\rho}(i) = \rho(i)$ for $i \leq n$ and $\bar{\rho}(n+1) = n+1$. By Lemma 3.4.1, $\rho \mapsto \bar{\rho}$ is the inverse of the isomorphism $\sigma \mapsto \sigma'$ from $S' := \{\sigma \in S_{n+1} : \sigma(n+1) = n+1\}$ onto S_n ; so it is an isomorphism $S_n \rightarrow S'$ (Proposition 3.3.2 (b)), and $\overline{\rho\pi} = \bar{\rho}\bar{\pi}$ for all $\rho, \pi \in S_n$, the product on the right being taken in S' , that is, in S_{n+1} .

We record two facts about the extension.

1. *It carries list products to list products:* $\overline{\tau_1 \cdots \tau_r} = \bar{\tau}_1 \cdots \bar{\tau}_r$ for every $r \geq 1$ and $\tau_1, \dots, \tau_r \in S_n$. For $r = 1$ both sides are $\bar{\tau}_1$. If it holds for r , then by the recursion of Definition 3.1.2 and the homomorphism property,

$$\overline{\tau_1 \cdots \tau_{r+1}} = \overline{(\tau_1 \cdots \tau_r)\tau_{r+1}} = \overline{\tau_1 \cdots \tau_r} \bar{\tau}_{r+1} = \bar{\tau}_1 \cdots \bar{\tau}_{r+1},$$

so it holds for $r+1$ (Sets, Relations, and Cardinality, Theorem 2.2.1 with base 1).

2. *It carries transpositions to transpositions:* for distinct $a, b \leq n$, $\overline{(a\ b)}$ swaps a and b and fixes every other point of $\{1, \dots, n+1\}$, including $n+1$; so it is the transposition $(a\ b)$ of S_{n+1} .

Case 1: $\sigma(n+1) = n+1$. Then $\sigma \in S'$, and its restriction σ' lies in S_n (Lemma 3.4.1). By the induction hypothesis, $\sigma' = \tau_1 \cdots \tau_r$ with $r \geq 1$ and transpositions $\tau_j \in S_n$. Since the two maps of the lemma are mutually inverse, $\sigma = \sigma'$, and by facts 1 and 2,

$$\sigma = \sigma' = \overline{\tau_1 \cdots \tau_r} = \bar{\tau}_1 \cdots \bar{\tau}_r,$$

a product of r transpositions of S_{n+1} .

Case 2: $\sigma(n+1) = k \neq n+1$. Then $k \in \{1, \dots, n\}$, and $\tau := (k \ n+1)$ is a transposition of S_{n+1} . Now

$$(\tau\sigma)(n+1) = \tau(\sigma(n+1)) = \tau(k) = n+1,$$

so Case 1 applies to $\tau\sigma$: $\tau\sigma = \tau_1 \cdots \tau_r$ with $r \geq 1$ and transpositions $\tau_j \in S_{n+1}$. Multiply on the left by τ , using $\tau\tau = \text{id}$, (G1), (G2) and the concatenation law Proposition 3.1.2 (a):

$$\sigma = (\tau\tau)\sigma = \tau(\tau\sigma) = \tau(\tau_1 \cdots \tau_r) = \tau\tau_1 \cdots \tau_r,$$

a product of $r+1$ transpositions.

In both cases σ is a product of transpositions. This completes the induction and proves the theorem. ■

The answer to the prompt. The transposition $\tau = (k \ n+1)$ was chosen so that it sends $k = \sigma(n+1)$ back to $n+1$; that is the whole computation in Case 2. Fixing $n+1$ is the right aim because it is exactly the hypothesis of Lemma 3.4.1: a permutation of $n+1$ points that fixes the last one **is** a permutation of n points, and only there does the induction hypothesis speak. Case 1 also needs the restriction σ' to be **onto** $\{1, \dots, n\}$, and the lemma proves this directly from $\sigma(n+1) = n+1$, with no counting.

Remark. Alternatively, Theorem 3.4.4 writes $\sigma = \gamma_1 \cdots \gamma_s$ with disjoint cycles γ_j . If $s = 0$, then $\sigma = \text{id} = (1 \ 2)(1 \ 2)$, using $n \geq 2$. Otherwise Proposition 3.5.1 writes each γ_j as a product of transpositions, and the concatenation law Proposition 3.1.2 (a) joins the words. For $\sigma = (1 \ 3)(2 \ 5 \ 4)$ of Example (Computing with Cycles) this gives $(1 \ 3)(2 \ 4)(2 \ 5)$.

3.5.3 The word is not unique

A product $\tau_1 \cdots \tau_r$ equal to σ is a **word** for σ . A permutation has many words. For the 3-cycle of the opening,

$$(1 \ 2 \ 3) = (1 \ 3)(1 \ 2) = (1 \ 2)(2 \ 3) = (1 \ 3)(1 \ 2)(1 \ 2)(1 \ 2).$$

The first word is Example (Computing with Cycles). The second is Proposition 3.5.1 applied to $(2 \ 3 \ 1)$, as above; directly, applying $(2 \ 3)$ first, $1 \mapsto 1 \mapsto 2$, $2 \mapsto 3 \mapsto 3$, $3 \mapsto 2 \mapsto 1$. The third inserts $(1 \ 2)(1 \ 2) = \text{id}$ after the first word.

Warning. “The transpositions of σ ” means nothing, and neither does “ σ is a product of r transpositions, so r is determined by σ ”. The three words for $(1 \ 2 \ 3)$ above have lengths 2, 2 and 4, and the first two consist of different transpositions. A word must also be read **right to left**, like every product of permutations: reversing the word $(1 \ 3)(1 \ 2)$ gives $(1 \ 2)(1 \ 3) = (1 \ 3 \ 2)$ (Example (Computing with Cycles)), a different permutation.

Something does survive. The three lengths 2, 2, 4 above are all even. That every word for a given permutation has a length of the same parity is true, but it is not proved here: it is the theorem on the **sign** of a permutation, proved in the chapter “Determinants” of the linear algebra volume *Determinants and the Structure of Operators* and in the chapter “Symmetric Groups and the Sign of a Permutation” of *Groups*. Nothing in this chapter uses it.

⌚ **Second reading** · *A minimal change: 3-cycles do not generate*

Not every kind of cycle generates S_n . Change “transpositions” to “3-cycles” in the theorem, with $n = 3$. By Definition 3.4.2, a 3-cycle of S_3 is $(i_1 i_2 i_3)$ with $\{i_1, i_2, i_3\} = \{1, 2, 3\}$, and rotating the written cycle shows that there are only two of them: $(1 2 3) = (2 3 1) = (3 1 2)$ and $(1 3 2) = (3 2 1) = (2 1 3)$. Let $H := \{\text{id}, (1 2 3), (1 3 2)\}$. Computing right to left as in Example (Computing with Cycles),

$$\begin{aligned} (1 2 3)(1 2 3) &= (1 3 2), & (1 3 2)(1 3 2) &= (1 2 3), \\ (1 2 3)(1 3 2) &= \text{id}, & (1 3 2)(1 2 3) &= \text{id}, \end{aligned}$$

and id times anything is that thing; so H is closed under products. By induction on the length $r \geq 1$, using the recursion of Definition 3.1.2, every product of r 3-cycles lies in H . But $(1 2) \notin H$. So the 3-cycles do **not** generate S_3 , and the theorem depends on the kind of cycle it names.

3.5.4 Adjacent transpositions

Linear algebra often sorts a list by swapping **neighbors**, positions i and $i+1$. The transpositions $(i i+1)$, $1 \leq i < n$, are the **adjacent** transpositions, and they are enough.

Corollary 3.5.3. Adjacent Transpositions Generate S_n

Let $n \geq 2$. Every $\sigma \in S_n$ is a product of adjacent transpositions $(i i+1)$, $1 \leq i < n$.

Idea. By Theorem 3.5.2 it is enough to write one transposition $(i j)$, $i < j$, with adjacent ones. Conjugating by a neighbor swap moves an endpoint one step: $(i i+1)(i+1 j)(i i+1) = (i j)$. So the gap $j - i$ shrinks by one, and an induction on the gap finishes.

Proof. First let $1 \leq i < j \leq n$ with $j - i \geq 2$, and put $s := (i i+1)$, $t := (i+1 j)$; here $i+1 < j$, so t is a transposition. We check $sts = (i j)$ point by point, applying the right-hand s first:

$$\begin{aligned} i &\mapsto i+1 \mapsto j \mapsto j, & j &\mapsto j \mapsto i+1 \mapsto i, \\ i+1 &\mapsto i \mapsto i \mapsto i+1, \end{aligned}$$

and every other point is fixed by s , t and s . So

$$(i j) = (i i+1)(i+1 j)(i i+1). \quad (*)$$

Next we prove, by Sets, Relations, and Cardinality, Theorem 2.2.1 with base 1 on d , the statement $Q(d)$: “for every $i \geq 1$ with $i + d \leq n$, $(i i+d)$ is a product of adjacent transpositions”. $Q(1)$ holds, since $(i i+1)$ is one. Suppose $Q(d)$, and let $i + d + 1 \leq n$. By $(*)$ with $j = i + d + 1$, $(i i+d+1) = (i i+1)(i+1 i+1+d)(i i+1)$, and the middle factor is a product of adjacent transpositions by $Q(d)$, applied at $i+1$. Joining the three words by Proposition 3.1.2 (a) gives $Q(d+1)$.

Finally let $\sigma \in S_n$. By Theorem 3.5.2, $\sigma = \tau_1 \cdots \tau_r$ with $r \geq 1$. Each τ_j is $(a b) = (b a)$ with $a \neq b$, so it can be written as $(i i+d)$ with i the smaller entry and $d \geq 1$ the difference; by

$Q(d)$ it is a product of adjacent transpositions. Joining these r words by Proposition 3.1.2 (a) proves the corollary. ■

The words this proof produces are long. Unwinding $(*)$ twice, $(1\ 4) = (1\ 2)(2\ 4)(1\ 2)$ and $(2\ 4) = (2\ 3)(3\ 4)(2\ 3)$, so

$$(1\ 4) = (1\ 2)(2\ 3)(3\ 4)(2\ 3)(1\ 2).$$

The corollary only promises that some word exists; it says nothing about the shortest one.

Quick check. Find a second word of adjacent transpositions for $(1\ 4)$ in S_4 , different from the one above, and check it point by point.

Solution. Shrink the gap from the other end: $(1\ 4) = (3\ 4)(1\ 3)(3\ 4)$ and $(1\ 3) = (2\ 3)(1\ 2)(2\ 3)$, so $(1\ 4) = (3\ 4)(2\ 3)(1\ 2)(2\ 3)(3\ 4)$. Check, applying the right-most factor first: $1 \mapsto 1 \mapsto 1 \mapsto 2 \mapsto 3 \mapsto 4$; $4 \mapsto 3 \mapsto 2 \mapsto 1 \mapsto 1 \mapsto 1$; $2 \mapsto 2 \mapsto 3 \mapsto 3 \mapsto 2 \mapsto 2$; $3 \mapsto 4 \mapsto 4 \mapsto 4 \mapsto 4 \mapsto 3$. So $1 \leftrightarrow 4$ with 2, 3 fixed, which is $(1\ 4)$. (The first step is the mirror image of $(*)$: $(i\ j) = (j-1\ j)(i\ j-1)(j-1\ j)$ for $j-i \geq 2$, checked in the same way.)

3.5.5 Exercises

3.5.5.1 A. Check your understanding

Exercise. A1

- Where in Theorem 3.5.2 is the hypothesis $n \geq 2$ used? What goes wrong for $n = 1$?
- Run the proof of Theorem 3.5.2 on $\sigma := (1\ 3\ 4\ 2) \in S_4$: at each stage name the case, the transposition τ chosen, and the permutation passed down to the smaller symmetric group. Write down the word for σ the run produces, and check it.
- Where does the proof use Lemma 3.4.1, and for what?
- State the idea of the proof in two sentences.

Solution.

- In the base case. The induction starts at $n = 2$, where $\text{id} = (1\ 2)(1\ 2)$ needs a transposition to exist. For $n = 1$, $S_1 = \{\text{id}\}$ has no transposition at all (a transposition needs two distinct points), so id is a product of transpositions only as the empty product, which the definition of “product of transpositions” ($r \geq 1$) excludes.
- First stage, in S_4 .* $\sigma(4) = 2 \neq 4$: Case 2, with $k = 2$ and $\tau = (2\ 4)$. Then $\tau\sigma$, applying σ first: $1 \mapsto 3 \mapsto 3$, $3 \mapsto 4 \mapsto 2$, $2 \mapsto 1 \mapsto 1$, $4 \mapsto 2 \mapsto 4$. So $\tau\sigma = (1\ 3\ 2)$, which fixes 4, and Case 1 passes its restriction, the permutation $(1\ 3\ 2)$ of $\{1, 2, 3\}$, down to S_3 .
Second stage, in S_3 . $\sigma' := (1\ 3\ 2)$ has $\sigma'(3) = 2 \neq 3$: Case 2 again, with $\tau' = (2\ 3)$. Then $\tau'\sigma'$: $1 \mapsto 3 \mapsto 2$, $2 \mapsto 1 \mapsto 1$, $3 \mapsto 2 \mapsto 3$. So $\tau'\sigma' = (1\ 2)$, which fixes 3; Case 1 passes $(1\ 2) \in S_2$ down.
Base, in S_2 . $(1\ 2)$ is one transposition.

Back up. $\tau'\sigma' = (1\ 2)$ gives $\sigma' = \tau'(1\ 2) = (2\ 3)(1\ 2)$, and then $\sigma = \tau(\tau\sigma) = (2\ 4)(2\ 3)(1\ 2)$, each transposition read in S_4 by fact 2 of the proof. Check, applying $(1\ 2)$ first: $1 \mapsto 2 \mapsto 3 \mapsto 3$, $3 \mapsto 3 \mapsto 2 \mapsto 4$, $4 \mapsto 4 \mapsto 4 \mapsto 2$, $2 \mapsto 1 \mapsto 1 \mapsto 1$. So $1 \mapsto 3 \mapsto 4 \mapsto 2 \mapsto 1$, which is $(1\ 3\ 4\ 2)$.

The second route of the remark after the theorem gives another word: by [Proposition 3.5.1](#), $(1\ 3\ 4\ 2) = (1\ 2)(1\ 4)(1\ 3)$ (check: $1 \mapsto 3 \mapsto 3 \mapsto 3$, $3 \mapsto 1 \mapsto 4 \mapsto 4$, $4 \mapsto 4 \mapsto 1 \mapsto 2$, $2 \mapsto 2 \mapsto 2 \mapsto 1$). That is a correct word, but it is not the run asked for. Neither is $(2\ 4)(1\ 2)(1\ 3)$, which applies one Case-2 step and then the cycle formula to $\tau\sigma = (1\ 3\ 2)$; it is a third valid word.

- (c) In two places. In the paragraph opening the Step, part (b) of the lemma says that $\rho \mapsto \bar{\rho}$ is the inverse of the isomorphism $\sigma \mapsto \sigma'$ from S' onto S_n ; so, by [Proposition 3.3.2 \(b\)](#), the extension is a homomorphism, the product of extensions being taken in S_{n+1} . Fact 1 rests on this. In Case 1, part (a) says that a permutation σ of $\{1, \dots, n+1\}$ fixing $n+1$ restricts to a permutation σ' of $\{1, \dots, n\}$, to which the induction hypothesis applies, and part (b) says that extending σ' back gives σ , so that the extension carries the word for σ' to a word for σ .
- (d) Induct on n : a permutation that fixes the last point is a permutation of one point fewer, so the induction hypothesis writes it as transpositions. A permutation that moves the last point is brought to that case by one transposition, which is then undone.

3.5.5.2 B. Practice

Exercise. B1

Write $(1\ 2\ 3\ 4\ 5)$ and $(1\ 5)(2\ 4)$ as products of transpositions, and then as products of adjacent transpositions. Check one of your adjacent words point by point.

Solution. Transpositions. By [Proposition 3.5.1](#), $(1\ 2\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$. The permutation $(1\ 5)(2\ 4)$ is already a product of two transpositions.

Adjacent transpositions. A word of neighbor swaps for the 5-cycle can be checked directly:

$$(1\ 2\ 3\ 4\ 5) = (1\ 2)(2\ 3)(3\ 4)(4\ 5).$$

Check, applying $(4\ 5)$ first: $1 \mapsto 1 \mapsto 1 \mapsto 1 \mapsto 2$; $2 \mapsto 2 \mapsto 2 \mapsto 3 \mapsto 3$; $3 \mapsto 3 \mapsto 4 \mapsto 4 \mapsto 4$; $4 \mapsto 5 \mapsto 5 \mapsto 5 \mapsto 5$; $5 \mapsto 4 \mapsto 3 \mapsto 2 \mapsto 1$. So $1 \mapsto 2 \mapsto 3 \mapsto 4 \mapsto 5 \mapsto 1$, as required.

For $(1\ 5)(2\ 4)$, use $(*)$ of the corollary's proof repeatedly: $(1\ 5) = (1\ 2)(2\ 5)(1\ 2)$, $(2\ 5) = (2\ 3)(3\ 5)(2\ 3)$, $(3\ 5) = (3\ 4)(4\ 5)(3\ 4)$, and $(2\ 4) = (2\ 3)(3\ 4)(2\ 3)$. Joining the words ([Proposition 3.1.2 \(a\)](#)),

$$\begin{aligned} (1\ 5)(2\ 4) &= (1\ 2)(2\ 3)(3\ 4)(4\ 5)(3\ 4)(2\ 3)(1\ 2) \\ &\quad \cdot (2\ 3)(3\ 4)(2\ 3), \end{aligned}$$

a word of ten adjacent transpositions.

Exercise. B2

Let $n \geq 2$ and $\rho := (1\ 2\ \dots\ n) \in S_n$ (for $n = 2$, $\rho = (1\ 2)$).

- (a) Prove that $\sigma(a b)\sigma^{-1} = (\sigma(a) \sigma(b))$ for every $\sigma \in S_n$ and every transposition $(a b) \in S_n$.
- (b) Prove that $\rho^{i-1}(1 \ 2)\rho^{-(i-1)} = (i \ i+1)$ for $1 \leq i \leq n-1$.
- (c) Deduce that every $\sigma \in S_n$ is a product of factors each equal to $(1 \ 2)$, ρ or ρ^{-1} .

Solution.

- (a) The points $\sigma(a)$, $\sigma(b)$ are distinct, since σ is injective, so the right-hand side is a transposition. Check point by point, applying σ^{-1} first. For $x = \sigma(a)$: $\sigma^{-1}(x) = a \mapsto b \mapsto \sigma(b)$. For $x = \sigma(b)$: $\sigma^{-1}(x) = b \mapsto a \mapsto \sigma(a)$. For any other x : $\sigma^{-1}(x) \notin \{a, b\}$ (otherwise $x = \sigma(\sigma^{-1}(x))$ would be $\sigma(a)$ or $\sigma(b)$), so $(a b)$ fixes it, and $\sigma(\sigma^{-1}(x)) = x$. These are the values of $(\sigma(a) \sigma(b))$ (Sets, Relations, and Cardinality, Proposition 1.4.1).
- (b) First, $\rho^m(j) = j + m$ whenever $m \in \mathbb{N}$, $j \geq 1$ and $j + m \leq n$. By induction on m : $\rho^0 = \text{id}$; and if it holds for m and $j + m + 1 \leq n$, then $\rho^{m+1} = \rho^m \rho$ (Definition 3.1.3), so $\rho^{m+1}(j) = \rho^m(j + 1) = j + 1 + m$, using $\rho(j) = j + 1$ for $j < n$ (Definition 3.4.2). Now let $1 \leq i \leq n-1$ and $\sigma := \rho^{i-1}$. Then $\sigma(1) = i$ and $\sigma(2) = i + 1$, since $2 + (i-1) \leq n$, and $\sigma^{-1} = \rho^{-(i-1)}$ by Proposition 3.1.3 (b). By (a), $\rho^{i-1}(1 \ 2)\rho^{-(i-1)} = (i \ i+1)$.
- (c) By Corollary 3.5.3, σ is a product of adjacent transpositions. By (b), each $(i \ i+1)$ equals $\rho^{i-1}(1 \ 2)\rho^{-(i-1)}$, where ρ^{i-1} is the product of $i-1$ factors ρ and $\rho^{-(i-1)} = (\rho^{-1})^{i-1}$ the product of $i-1$ factors ρ^{-1} (Definition 3.1.3, Proposition 3.1.3 (b)). Joining all these words by Proposition 3.1.2 (a) writes σ as required.

3.5.5.3 C. Going deeper

Exercise. C1: Exit check: transpositions generate

Let $n \geq 2$. State and prove that every $\sigma \in S_n$ is a product of transpositions.

Solution. Statement. For $n \geq 2$, every $\sigma \in S_n$ is $\tau_1 \cdots \tau_r$ for some $r \geq 1$ and transpositions $\tau_j \in S_n$ (Theorem 3.5.2).

Proof. Induction on $n \geq 2$ (Sets, Relations, and Cardinality, Theorem 2.2.1 with base 2). For $n = 2$, a bijection σ of $\{1, 2\}$ has $\sigma(1) = 1$, and then $\sigma(2) = 2$ by injectivity, or $\sigma(1) = 2$ and $\sigma(2) = 1$; so $S_2 = \{\text{id}, (1 \ 2)\}$, and $\text{id} = (1 \ 2)(1 \ 2)$.

Suppose the statement for $n \geq 2$, and let $\sigma \in S_{n+1}$.

If $\sigma(n+1) = n+1$, then $\sigma(i) \neq n+1$ for $i \leq n$ by injectivity, so σ restricts to an injective map $\sigma': \{1, \dots, n\} \rightarrow \{1, \dots, n\}$. It is onto: for $j \leq n$, $j = \sigma(i)$ for some i , and $i \neq n+1$ because $\sigma(n+1) = n+1 \neq j$. So $\sigma' \in S_n$ (Lemma 3.4.1), and $\sigma' = \tau_1 \cdots \tau_r$ by the hypothesis. Extending each permutation of $\{1, \dots, n\}$ by $n+1 \mapsto n+1$ is the inverse of the restriction isomorphism of Lemma 3.4.1 (b), so it is a homomorphism (Proposition 3.3.2 (b)). By induction on r , using the recursion of Definition 3.1.2 (fact 1 in the proof of Theorem 3.5.2), it carries this word to the word $\bar{\tau}_1 \cdots \bar{\tau}_r$ in S_{n+1} , each $\bar{\tau}_j$ the transposition of the same two points; and it carries σ' to σ . Hence $\sigma = \bar{\tau}_1 \cdots \bar{\tau}_r$.

If $\sigma(n+1) = k \neq n+1$, let $\tau := (k \ n+1)$. Then $(\tau\sigma)(n+1) = \tau(k) = n+1$, so by the first case $\tau\sigma = \tau_1 \cdots \tau_r$ with transpositions in S_{n+1} . Since $\tau\tau = \text{id}$, $\sigma = \tau(\tau\sigma) = \tau\tau_1 \cdots \tau_r$. This completes the induction.

Marking scheme. (10 points)

- 2: sets up induction on n with base $n = 2$, and handles S_2 , including id as a product of transpositions.
- 3: Case $\sigma(n+1) = n+1$: reduces to S_n , with the restriction shown to be a permutation of $\{1, \dots, n\}$ (surjectivity justified, or Lemma 3.4.1 cited).
- 3: Case $\sigma(n+1) = k \neq n+1$: chooses a transposition τ with $\tau\sigma$ fixing $n+1$, and computes $(\tau\sigma)(n+1) = n+1$.
- 1: undoes τ , using $\tau^{-1} = \tau$.
- 1: says why transpositions of S_n , extended, are transpositions of S_{n+1} and the extended word still equals σ .

Fatal errors (0 for the step): using “ σ is a product of transpositions in S_{n+1} ” inside its own proof (circular); assuming the cycle decomposition or the cycle formula without citing it as proved.

Second route (accepted, 10 points).

- 3: cites Theorem 3.4.4 as proved, writing σ as a product of disjoint cycles.
- 3: writes each cycle as transpositions by [Proposition 3.5.1](#), cited or proved, with the factors in the right (right-to-left) order.
- 2: handles $\sigma = \text{id}$ as $(1\ 2)(1\ 2)$, using $n \geq 2$.
- 2: joins the words into one product of transpositions (Proposition 3.1.2 (a)).

Third route (accepted, 10 points): strong induction on $|\text{supp } \sigma|$ (finite, as a subset of $\{1, \dots, n\}$).

- 2: sets up the induction and handles the base $\text{supp } \sigma = \emptyset$, that is, $\sigma = \text{id} = (1\ 2)(1\ 2)$, using $n \geq 2$.
- 3: for $\sigma \neq \text{id}$, picks i with $j := \sigma(i) \neq i$ and $\tau := (i\ j)$, and shows that $\tau\sigma$ fixes i and every point that σ fixes (such a point is neither i nor j , by injectivity).
- 3: concludes $\text{supp}(\tau\sigma) \subseteq \text{supp } \sigma \setminus \{i\}$, so the hypothesis applies to $\tau\sigma$ (or $\tau\sigma = \text{id}$, and $\sigma = \tau$).
- 1: undoes τ , using $\tau^{-1} = \tau$.
- 1: joins the words (Proposition 3.1.2 (a)).

Exercise. C2: Find the error

Here is an argument.

Claim. Every cycle is a product of transpositions.

Proof. (1) Let $\gamma = (i_1\ i_2\ \dots\ i_k)$ with $k \geq 2$ and distinct entries. (2) The cycle sends i_1 to i_2 , then i_2 to i_3 , and so on, up to i_k , which it sends back to i_1 . (3) The swap $(i_1\ i_2)$ takes i_1 to i_2 ; the swap $(i_1\ i_3)$ is next; and so on. (4) Hence $\gamma = (i_1\ i_2)(i_1\ i_3) \dots (i_1\ i_k)$. (5) So γ is a product of $k - 1$ transpositions.

Is the claim true? Does the argument prove it? Name the line that fails and the reason, give a counterexample to the illegal step, and repair the argument.

Solution. The claim is true: it is [Proposition 3.5.1](#). The argument does not prove it.

Line (4) fails, on the strength of line (3). Line (3) lists the transpositions in the order in which they should act, and line (4) writes them left to right in that order. But a product of

permutations acts right to left (Definition 3.4.1): in $(i_1 i_2)(i_1 i_3) \cdots (i_1 i_k)$ the factor $(i_1 i_k)$ acts first. The equation of line (4) is an unproved “fact”, and a false one: entry (N9) of Logic and Proof, Example (What is not allowed). Lines (1), (2) and (5) are correct.

Counterexample to the step. For $k = 3$ and $\gamma = (1 2 3)$, line (4) claims $(1 2 3) = (1 2)(1 3)$. But $(1 2)(1 3) = (1 3 2)$ (Example (Computing with Cycles)), and $(1 3 2) \neq (1 2 3)$, since the first sends 1 to 3 and the second sends 1 to 2. There is no counterexample to the conclusion.

In fact the product in line (4) is γ^{-1} : by Proposition 3.1.2 (c), the inverse of $(i_1 i_k) \cdots (i_1 i_2) = \gamma$ is the reversed product of the inverses, and each transposition is its own inverse.

Repair. Reverse the order of the factors: $\gamma = (i_1 i_k)(i_1 i_{k-1}) \cdots (i_1 i_2)$, and prove it as in Proposition 3.5.1, by induction on k with a point-by-point check of $(i_1 i_{k+1})(i_1 \cdots i_k) = (i_1 \cdots i_{k+1})$.

Marking scheme. (10 points)

- 2: says the claim is true and the argument does not prove it.
- 3: names line (4) (or lines (3)–(4) together) and the reason: the factors are written in the order they should act, but products act right to left.
- 2: a counterexample to the step, such as $(1 2)(1 3) = (1 3 2) \neq (1 2 3)$.
- 3: gives a correct formula for γ as a product of transpositions and justifies it. For the reversed product $(i_1 i_k) \cdots (i_1 i_2)$, the induction or a citation of Proposition 3.5.1 is enough. For another word, such as $(i_1 i_2)(i_2 i_3) \cdots (i_{k-1} i_k)$, the reader must prove it, by induction on k or by a point-by-point check for general k .

Fatal errors (0 for the step): a counterexample to the conclusion (there is none); a “repair” that keeps line (4)’s product and silently replaces γ by another cycle (such as γ^{-1}).

Exercise. C3

- Let $\sigma \in S_n$ and let $(i_1 \cdots i_k) \in S_n$ be a cycle. Prove that $\sigma(i_1 \cdots i_k)\sigma^{-1} = (\sigma(i_1) \cdots \sigma(i_k))$.
- Deduce that any two transpositions of S_n are conjugate: for transpositions τ, τ' there is $\pi \in S_n$ with $\tau' = \pi\tau\pi^{-1}$.

Solution.

- Write $\gamma := (i_1 \cdots i_k)$, and read indices so that i_{k+1} means i_1 . The points $\sigma(i_1), \dots, \sigma(i_k)$ are distinct, since σ is injective, so the right-hand side is a k -cycle. For $x = \sigma(i_j)$: $\sigma^{-1}(x) = i_j \mapsto i_{j+1} \mapsto \sigma(i_{j+1})$. For x not among the $\sigma(i_j)$: $\sigma^{-1}(x)$ is not among the i_j , so γ fixes it, and $\sigma\gamma\sigma^{-1}(x) = x$. These are the values of $(\sigma(i_1) \cdots \sigma(i_k))$.
- Here $n \geq 2$, since a transposition exists. First, every transposition $(a b)$, written with $a < b$, is conjugate to $(1 2)$: by (a) it suffices to find π with $\pi(1) = a$, $\pi(2) = b$. If $(a, b) = (1, 2)$, take $\pi = \text{id}$. If $a = 1$ and $b \geq 3$, take $\pi = (2 b)$. If $a \geq 2$, then $b \geq 3$; take $\pi = (1 a)(2 b)$: applying $(2 b)$ first, $1 \mapsto 1 \mapsto a$, and $2 \mapsto b \mapsto b$, since $b \neq 1$ and $b \neq a$. Now let $\tau = \pi(1 2)\pi^{-1}$ and $\tau' = \pi'(1 2)\pi'^{-1}$. Then $(1 2) = \pi^{-1}\tau\pi$, and

$$\tau' = \pi'\pi^{-1}\tau\pi\pi'^{-1} = (\pi'\pi^{-1})\tau(\pi'\pi^{-1})^{-1},$$

by Proposition 3.1.2 (c) and Theorem 3.1.1 (3). Conjugacy in S_n is studied in the

chapter “Symmetric Groups and the Sign of a Permutation” of *Groups*.

Marking scheme. (10 points)

- 2: notes that the $\sigma(i_j)$ are distinct (σ injective), so the right side of (a) is a k -cycle.
- 2: checks $\sigma\gamma\sigma^{-1}(\sigma(i_j)) = \sigma(i_{j+1})$, including the wrap-around $j = k$.
- 2: checks that every x outside $\{\sigma(i_1), \dots, \sigma(i_k)\}$ is fixed.
- 3: for transpositions $(a\ b), (c\ d)$, exhibits a permutation π with $\{\pi(a), \pi(b)\} = \{c, d\}$, covering every case of overlap between $\{a, b\}$ and $\{c, d\}$; directly or through $(1\ 2)$.
- 1: applies (a) with $k = 2$ to conclude $\tau' = \pi\tau\pi^{-1}$, or composes the two conjugations by $(1\ 2)$ using $(\pi'\pi^{-1})^{-1} = \pi\pi'^{-1}$.

Fatal errors (0 for the step): a proof of (a) that only asserts the formula (0 for the three (a) items); π is not a bijection, or is built only for disjoint (or only for overlapping) pairs. Part (b) may use (a) even where (a) was not proved.

3.5.5.4 R. Review

Exercise. R1

Let F be a field. Show that $\varphi(k) := k \cdot 1_F$ defines a homomorphism $(\mathbb{Z}, +) \rightarrow (F, +)$, that $\ker \varphi = m\mathbb{Z}$ for exactly one $m \in \mathbb{N}$, and that this m is 0 or a prime.

Solution. Homomorphism. In additive notation, Proposition 3.1.3 (a) says $(k + l) \cdot 1_F = k \cdot 1_F + l \cdot 1_F$ for all $k, l \in \mathbb{Z}$, the multiples being those of the group $(F, +)$ (Definition 3.1.3). That is $\varphi(k + l) = \varphi(k) + \varphi(l)$. By Proposition 3.1.3 (e), for $k \in \mathbb{N}$ these group multiples are the multiples of *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Section 2.3, which are the multiples of Lemma 2.5.1; that lemma is applied below only to natural numbers.

Kernel. $\ker \varphi$ is a subgroup of $\mathbb{Z}$ (Theorem 3.3.1 (c)), so $\ker \varphi = m\mathbb{Z}$ for exactly one $m \in \mathbb{N}$ (Theorem 3.2.4): $m = 0$ if the kernel is $\{0\}$, and otherwise m is its least positive element.

m is 0 or prime. $m \neq 1$: $1 \cdot 1_F = 1_F$ (Definition 3.1.3), and $1_F \neq 0_F$ in a field (*Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Definition 2.3.1), so $1 \notin \ker \varphi$. Suppose $m \geq 2$ were not prime. By *Sets, Relations, and Cardinality*, Definition 2.2.2 it has a positive divisor $a \notin \{1, m\}$; write $m = ab$ with $b \in \mathbb{Z}$. Then $b > 0$, as $a, m > 0$; $a \leq m$ and $b \leq m$ by *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Proposition 3.1.1 (e); and $b \neq m$, since $b = m$ would give $a = 1$ (cancel $m \neq 0$ in $\mathbb{Z}$). So $0 < a < m$ and $0 < b < m$. By Lemma 2.5.1 (b),

$$(a \cdot 1_F)(b \cdot 1_F) = (ab) \cdot 1_F = m \cdot 1_F = 0_F.$$

But $a \notin m\mathbb{Z}$: if $m \mid a$ with $a > 0$, then $m \leq a$ by *Number Systems: From $\mathbb{N}$ to $\mathbb{R}$* , Proposition 3.1.1 (e), against $a < m$. So $a \cdot 1_F \neq 0_F$, and in the same way $b \cdot 1_F \neq 0_F$. A field has no zero divisors (Theorem 2.1.1 (f)): a contradiction. So m is 0 or prime.

This is a group-theoretic route to Chapter 2’s characteristic. The number m is $\text{char } F$ (Definition 2.5.1): if $m > 0$ it is the least positive n with $n \cdot 1_F = 0_F$, and $m = 0$ exactly when there is none. The result is Theorem 2.5.3, whose proof there runs the same argument without the language of kernels.

Exercise. R2

Show that $(\mathbb{Z}/6\mathbb{Z}, +) \cong ((\mathbb{Z}/7\mathbb{Z})^\times, \cdot)$, and that $(\mathbb{Z}/6\mathbb{Z}, +) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Solution. The first isomorphism. By Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Theorem 3.5.2, $\mathbb{Z}/7\mathbb{Z}$ is a field, so every non-zero class is a unit, while $[0]$ is not ($[0][x] = [0] \neq [1]$). So the units are the six classes $[1], \dots, [6]$, distinct by Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Theorem 3.4.3 (b), and they form a group by Proposition 3.1.4. Compute the powers of $[3]$:

$$[3]^0, [3]^1, \dots, [3]^5 = [1], [3], [2], [6], [4], [5],$$

from $3 \cdot 3 = 9 = 7 + 2$, $2 \cdot 3 = 6$, $6 \cdot 3 = 18 = 14 + 4$, $4 \cdot 3 = 12 = 7 + 5$, and then $[3]^6 = [5][3] = [15] = [1]$.

Define $f([k]) := [3]^k$. *Well defined:* if $[k] = [k']$ in $\mathbb{Z}/6\mathbb{Z}$, then $k' = k + 6q$ with $q \in \mathbb{Z}$, and by Proposition 3.1.3 (a), (c),

$$[3]^{k'} = [3]^k([3]^6)^q = [3]^k[1]^q = [3]^k,$$

since every power of the identity is the identity (Definition 3.1.3, by induction on $q \in \mathbb{N}$, and for $q < 0$ because $[1]^{-1} = [1]$). *A homomorphism:* $f([k] + [l]) = f([k + l]) = [3]^{k+l} = [3]^k[3]^l = f([k])f([l])$, by Proposition 3.1.3 (a). *Bijective:* the six classes $[0], \dots, [5]$ of $\mathbb{Z}/6\mathbb{Z}$ (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Theorem 3.4.3 (b)) go to the six distinct units listed above, which are all of $(\mathbb{Z}/7\mathbb{Z})^\times$. So f is an isomorphism (Definition 3.3.1).

The second isomorphism. $1 = 3 \cdot 1 + 2 \cdot (-1)$, so 2 and 3 are coprime (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Corollary 3.2.2). By Example (Homomorphisms) (e), which rests on Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Theorem 3.5.3 (b), $[x]_6 \mapsto ([x]_2, [x]_3)$ is an isomorphism of additive groups $\mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

The method is that of Example (Isomorphic and Non-Isomorphic Small Groups) (b), where $[2]$ played the role of $[3]$ modulo 5.

Exercise. R3

Let X be a set. Show that the permutations $\sigma \in S_X$ with $\text{supp } \sigma$ finite form a subgroup of S_X .

Solution. Let $H := \{\sigma \in S_X : \text{supp } \sigma \text{ is finite}\}$. We use Theorem 3.2.1. $H \neq \emptyset$: $\text{supp id}_X = \emptyset$, which has 0 elements (Sets, Relations, and Cardinality, Definition 3.1.2).

Let $\sigma, \tau \in H$. If $x \notin \text{supp } \sigma \cup \text{supp } \tau$, then $\tau(x) = x$, so $\tau^{-1}(x) = x$, and $\sigma(x) = x$; hence $\sigma\tau^{-1}(x) = x$. So

$$\text{supp}(\sigma\tau^{-1}) \subseteq \text{supp } \sigma \cup \text{supp } \tau = \text{supp } \sigma \cup (\text{supp } \tau \setminus \text{supp } \sigma).$$

The set $\text{supp } \tau \setminus \text{supp } \sigma$ is finite, as a subset of the finite set $\text{supp } \tau$ (Sets, Relations, and Cardinality, Proposition 3.1.6); it is disjoint from $\text{supp } \sigma$, so the union is finite (Sets, Relations, and Cardinality, Proposition 3.1.5); and $\text{supp}(\sigma\tau^{-1})$, a subset of it, is finite (Sets, Relations, and Cardinality, Proposition 3.1.6). So $\sigma\tau^{-1} \in H$, and H is a subgroup.

For an infinite X the subgroup can be proper. On $X = \mathbb{Z}$, the translation $\sigma(x) := x + 1$ is a bijection (its inverse is $x \mapsto x - 1$) that moves every point, since $x + 1 \neq x$. Its support $\mathbb{Z}$ is not finite: $x \mapsto 2x$ is a bijection from $\mathbb{Z}$ onto $2\mathbb{Z}$ (injective by cancellation, Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 2.3.5 (f)), and $2\mathbb{Z} \neq \mathbb{Z}$ since $1 \notin 2\mathbb{Z}$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 3.1.1 (g)), which a finite set does not allow (Sets, Relations, and Cardinality, Theorem 3.1.9).

Exercise. R4

Let G be a finite group with an even number of elements. Prove that some $g \in G$ with $g \neq e$ has $g^2 = e$.

Solution. The tool is to pair each element with its inverse. Define $g \sim h$ on G by $h \in \{g, g^{-1}\}$. It is an equivalence relation (Sets, Relations, and Cardinality, Definition 2.5.1): reflexive since $g \in \{g, g^{-1}\}$; symmetric since $h = g^{-1}$ gives $g = h^{-1}$ (Theorem 3.1.1 (3)); transitive since $h \in \{g, g^{-1}\}$ and $k \in \{h, h^{-1}\}$ give $k \in \{g, g^{-1}, (g^{-1})^{-1}\} = \{g, g^{-1}\}$. The class of g is $\{g, g^{-1}\}$, and the classes partition G (Sets, Relations, and Cardinality, Theorem 2.5.1).

A class has one element exactly when $g = g^{-1}$, that is, when $g^2 = e$: if $g = g^{-1}$, then $g^2 = gg^{-1} = e$; if $g^2 = e$, then g is an inverse of g , so $g = g^{-1}$ by uniqueness of inverses (Theorem 3.1.1 (2)). Let $T := \{g \in G : g^2 = e\}$, the union of the one-element classes, and $U := G \setminus T$, the union of the two-element classes; both are finite, as subsets of G (Sets, Relations, and Cardinality, Proposition 3.1.6).

$|U|$ is even. We show, by Logic and Proof, Theorem 4.2.2 on j , that every subset $V \subseteq U$ with j elements that contains g^{-1} whenever it contains g has an even number of elements. If $j = 0$, this holds. If $j \geq 1$, pick $g \in V$; then $g^{-1} \in V$ and $g^{-1} \neq g$ (as $g \notin T$), so $\{g, g^{-1}\}$ has 2 elements, and $V' := V \setminus \{g, g^{-1}\}$ again contains the inverse of each of its elements: if $h \in V'$, then $h^{-1} \in V$, and $h^{-1} \notin \{g, g^{-1}\}$, since otherwise $h = (h^{-1})^{-1} \in \{g^{-1}, g\}$ by Theorem 3.1.1 (3). As V is the disjoint union of V' and $\{g, g^{-1}\}$, $j = |V'| + 2$ (Sets, Relations, and Cardinality, Proposition 3.1.5 with Sets, Relations, and Cardinality, Corollary 3.1.4), so V' has $j - 2 < j$ elements; that number is even by the hypothesis, so j is even. Apply this to $V = U$.

Conclusion. $G = T \cup U$ is a disjoint union, so $|G| = |T| + |U|$ (Sets, Relations, and Cardinality, Proposition 3.1.5). With $|G|$ and $|U|$ even, $|T| = |G| - |U|$ is even. Since $e \in T$, $|T| \geq 1$, so $|T| \geq 2$: an even number cannot be 1, as $2 \nmid 1$ (Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Proposition 3.1.1 (g)). So T contains some $g \neq e$, and $g^2 = e$.

Look-alikes. Lagrange's theorem (the chapter "Cosets and Lagrange's Theorem" of *Groups*) and Cauchy's theorem (the chapter "Group Actions, the Orbit-Stabilizer Theorem, and the Class Equation" of *Groups*) would give this, but neither is available here. "Pick $g \neq e$ and square it" does not work: in $(\mathbb{Z}/6\mathbb{Z}, +)$, where the condition reads $2 \cdot g = [0]$, the element $g = [1]$ has $2 \cdot [1] = [2] \neq [0]$; the element that works there is $[3]$, and the pairing argument shows that such an element exists without searching for it.