

3.4 Permutations and Cycle Notation

Shuffle three cards, then shuffle them again. Two shuffles in a row are a shuffle, every shuffle can be undone, and the order of the two shuffles matters. This is the group of bijections of a finite set (Example (Groups) (c)), and it is the one group of this chapter studied in detail, because every determinant in linear algebra is built from it. This section gives it a compact notation, cycle notation, learns to multiply in it, counts its elements, and proves that every permutation breaks into independent loops: **follow the orbit, then peel it off**.

3.4.1 Permutations and two-line notation

Section 3.1 showed that the bijections of a set form a group under composition. On the set $\{1, \dots, n\}$ they are the rearrangements of n objects, and they get a name of their own.

A permutation is a rearrangement: a bijection of a set to itself.

Definition 3.4.1. Permutations and the Symmetric Group

Let X be a set. A **permutation** of X is a bijection $X \rightarrow X$. The permutations of X , with the operation $\sigma\tau := \sigma \circ \tau$, form the group S_X of Example (Groups) (c). For $n \in \mathbb{N}$, the **symmetric group** is

$$S_n := S_{\{1, \dots, n\}},$$

where $\{1, \dots, n\}$ is empty for $n = 0$. The **support** of $\sigma \in S_X$ is the set of points it moves,

$$\text{supp } \sigma := \{x \in X : \sigma(x) \neq x\}.$$

In words: S_X is not a new group. It is the group of bijections of X , with the product written as juxtaposition. Its identity is id_X , written id when X is clear, and the inverse of σ is the inverse function σ^{-1} (Sets, Relations, and Cardinality, Definition 1.5.2). The support of id is empty, and the support is empty only for id : if $\sigma(x) = x$ for every x , then $\sigma = \text{id}_X$ (Sets, Relations, and Cardinality, Proposition 1.4.1).

The product is read right to left. In S_X the product $\sigma\tau$ is the composite $\sigma \circ \tau$: **first apply τ , then σ** , exactly as $g \circ f$ applies f first (Sets, Relations, and Cardinality, Definition 1.4.2). So $(\sigma\tau)(x) = \sigma(\tau(x))$, and a longer product $\sigma_1\sigma_2 \cdots \sigma_r$ applies σ_r first and σ_1 last.

Two-line notation. A permutation $\sigma \in S_n$ is given by its values, and we write them under the points:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

This array is a **table** of values, not a matrix. For example, $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \in S_4$ sends $1 \mapsto 3$, $2 \mapsto 1$, $3 \mapsto 2$ and fixes 4; its support is $\{1, 2, 3\}$. The bottom row of a permutation lists each of $1, \dots, n$ exactly once: once at least, because σ is surjective, and at most once, because it is injective.

The smallest symmetric groups. S_0 has one element, the empty function $\emptyset \rightarrow \emptyset$ (Sets, Relations, and Cardinality, Proposition 1.4.2 (a)), which is a bijection because there is nothing to check; it is the trivial group. S_1 has one element, id , since the only function $\{1\} \rightarrow \{1\}$ sends $1 \mapsto 1$. S_2 has two elements, id and the permutation swapping 1 and 2: a bijection of $\{1, 2\}$ either fixes 1, and then also 2, or sends $1 \mapsto 2$, and then $2 \mapsto 1$. These degenerate cases are

where inductions on n start, here and in Section 3.5.

3.4.2 Cycles

Two-line notation lists every value, even the values of points that do not move. Most permutations met in practice move a few points around a loop and leave the rest alone, and a notation that records only the loop is shorter and shows more.

A cycle moves a list of distinct points one step along the list, the last back to the first, and fixes everything else.

Definition 3.4.2. Cycle, Transposition

Let $n \in \mathbb{N}$ and $k \geq 2$, and let $i_1, \dots, i_k \in \{1, \dots, n\}$ be **distinct**. The k -**cycle** $(i_1 \ i_2 \ \dots \ i_k) \in S_n$ is the permutation γ with

$$\gamma(i_j) := i_{j+1} \quad \text{for } 1 \leq j < k, \quad \gamma(i_k) := i_1,$$

and $\gamma(x) := x$ for every $x \in \{1, \dots, n\}$ not among $i_1, \dots, i_k$. A 2-cycle $(i \ j)$ is a **transposition**. Two cycles are **disjoint** if their supports are disjoint.

In words: $i_1 \mapsto i_2 \mapsto \dots \mapsto i_k \mapsto i_1$, and the points off the list stay put. A transposition $(i \ j)$ swaps i and j .

Well-definedness. Because the entries are distinct, each point of $\{1, \dots, n\}$ receives exactly one value from the rule, so γ is a function. It is a bijection: the cycle $(i_k \ \dots \ i_2 \ i_1)$, the list read backwards, undoes it point by point ($i_{j+1} \mapsto i_j$ and $i_1 \mapsto i_k$, and the other points are fixed by both), so it is a two-sided inverse and Sets, Relations, and Cardinality, Theorem 1.5.4 applies. Hence

$$(i_1 \ i_2 \ \dots \ i_k)^{-1} = (i_k \ \dots \ i_2 \ i_1).$$

Every entry is moved, since $i_{j+1} \neq i_j$ and $i_1 \neq i_k$ by distinctness and $k \geq 2$; so $\text{supp}(i_1 \ \dots \ i_k) = \{i_1, \dots, i_k\}$. A transposition is its own inverse: $(i \ j)(i \ j) = \text{id}$.

Examples. In S_4 , $(1 \ 2 \ 3)$ sends $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$ and fixes 4; in two-line notation it is $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$. The same cycle may be written starting at any of its entries: $(1 \ 2 \ 3) = (2 \ 3 \ 1) = (3 \ 1 \ 2)$, since all three describe the loop $1 \mapsto 2 \mapsto 3 \mapsto 1$. But $(1 \ 3 \ 2)$ is a different permutation: it sends $1 \mapsto 3$. The cycles $(1 \ 2)$ and $(3 \ 4)$ are disjoint; $(1 \ 2)$ and $(2 \ 3)$ are not.

🕒 **Second reading** · Why a cycle has at least two entries

The identity is not a cycle. The definition asks for $k \geq 2$: a “1-cycle” (i) would be the identity, and so would every one of them, so the notation would not be telling us anything. The identity is instead the empty product of cycles (Definition 3.1.2), and that is how it will appear in the decomposition theorem below.

Quick check. Which of these are equal in S_4 : $(2\ 4\ 1)$, $(1\ 2\ 4)$, $(1\ 4\ 2)$? Write the one that differs in two-line notation.

Solution. $(2\ 4\ 1)$ is the loop $2 \mapsto 4 \mapsto 1 \mapsto 2$, and $(1\ 2\ 4)$ is the same loop started at 1: both send $1 \mapsto 2$, $2 \mapsto 4$, $4 \mapsto 1$ and fix 3. So they are equal. $(1\ 4\ 2)$ runs the loop backwards: it sends $1 \mapsto 4$, $4 \mapsto 2$, $2 \mapsto 1$, so it differs from the other two at 1. In two-line notation it is $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$; it is the inverse of the other two.

Products of cycles are computed by following each point through the factors, **from right to left**.

Example. Computing with Cycles

In S_3 , compute $(1\ 3)(1\ 2)$ and $(1\ 2)(1\ 3)$. In S_5 , write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$$

as a product of cycles.

Solution. For $(1\ 3)(1\ 2)$, follow each point through $(1\ 2)$ first, then $(1\ 3)$: $1 \mapsto 2 \mapsto 2$, $2 \mapsto 1 \mapsto 3$, $3 \mapsto 3 \mapsto 1$. So $(1\ 3)(1\ 2) = (1\ 2\ 3)$. For $(1\ 2)(1\ 3)$: $1 \mapsto 3 \mapsto 3$, $3 \mapsto 1 \mapsto 2$, $2 \mapsto 2 \mapsto 1$. So $(1\ 2)(1\ 3) = (1\ 3\ 2)$. The two products differ, so S_3 is not abelian. For every $n \geq 3$, the same two transpositions lie in S_n , the same computation applies at 1, 2, 3, and both products fix every point ≥ 4 ; so S_n is not abelian for every $n \geq 3$.

For σ , start at 1 and follow: $1 \mapsto 3 \mapsto 1$, a loop $(1\ 3)$. The smallest point not yet used is 2: $2 \mapsto 5 \mapsto 4 \mapsto 2$, a loop $(2\ 5\ 4)$. Every point is now used, so $\sigma = (1\ 3)(2\ 5\ 4)$. To check, follow each point through $(2\ 5\ 4)$ first, then $(1\ 3)$: $1 \mapsto 1 \mapsto 3$, $2 \mapsto 5 \mapsto 5$, $3 \mapsto 3 \mapsto 1$, $4 \mapsto 2 \mapsto 2$, $5 \mapsto 4 \mapsto 4$, which is the bottom row 3, 5, 1, 2, 4. The two cycles move disjoint sets of points, and the product in the other order, $(2\ 5\ 4)(1\ 3)$, is also σ , as the same check shows.

🔄 **Second reading** • *The small symmetric groups are abelian*

For S_n with $n \leq 2$ the situation is different: S_0 , S_1 and S_2 have at most two elements, and any two of their elements commute, since one of them is id or both are equal. So S_n is abelian exactly when $n \leq 2$.

Warning. Mind the order. $\sigma\tau$ applies τ first, as $g \circ f$ applies f first. Reading a product of cycles from left to right gives a wrong answer: read that way, $(1\ 3)(1\ 2)$ would send $1 \mapsto 3 \mapsto 3$, $3 \mapsto 1 \mapsto 2$, $2 \mapsto 2 \mapsto 1$, that is, “ $(1\ 3\ 2)$ ”; but the example computed

$(1\ 3)(1\ 2) = (1\ 2\ 3)$. The left-to-right reading computes the product in the other order.

Section 3.1 noted that the power law $(gh)^n = g^n h^n$ of Proposition 3.1.3 (d) needs $gh = hg$. In S_3 it fails without that hypothesis.

Warning. $(\sigma\tau)^2 = \sigma^2\tau^2$ is false in general. Take $\sigma = (1\ 2)$ and $\tau = (1\ 3)$. By the example, $\sigma\tau = (1\ 3\ 2)$, and $(1\ 3\ 2)(1\ 3\ 2)$ sends $1 \mapsto 3 \mapsto 2$, $2 \mapsto 1 \mapsto 3$, $3 \mapsto 2 \mapsto 1$, so $(\sigma\tau)^2 = (1\ 2\ 3)$. But transpositions are their own inverses, so $\sigma^2\tau^2 = \text{id} \cdot \text{id} = \text{id}$. Here $\sigma\tau \neq \tau\sigma$, and the law fails.

Quick check. Compute $(1\ 2\ 3)(1\ 2)$ in S_3 .

Solution. Apply $(1\ 2)$ first: $1 \mapsto 2 \mapsto 3$, $2 \mapsto 1 \mapsto 2$, $3 \mapsto 3 \mapsto 1$. So 1 and 3 are swapped and 2 is fixed: $(1\ 2\ 3)(1\ 2) = (1\ 3)$.

3.4.3 Counting permutations

How many permutations does S_n have? There are n choices for $\sigma(1)$, then $n - 1$ for $\sigma(2)$, and so on, which suggests $n!$. We make this precise by induction on n , and the induction needs one structural fact: the permutations of $\{1, \dots, n + 1\}$ that fix the last point are, in effect, the permutations of $\{1, \dots, n\}$. Section 3.5 uses the same fact for a different induction.

Lemma 3.4.1. Permutations Fixing the Last Point

Let $n \in \mathbb{N}$, and let $S' := \{\sigma \in S_{n+1} : \sigma(n+1) = n+1\}$, a subgroup of S_{n+1} .

- (a) For $\sigma \in S'$, the restriction σ' of σ to $\{1, \dots, n\}$, with codomain $\{1, \dots, n\}$, is a permutation of $\{1, \dots, n\}$.
- (b) The map $S' \rightarrow S_n$, $\sigma \mapsto \sigma'$, is an isomorphism. Its inverse sends $\rho \in S_n$ to its **extension** $\bar{\rho} \in S'$, defined by $\bar{\rho}(i) := \rho(i)$ for $i \leq n$ and $\bar{\rho}(n+1) := n+1$.

That S' is a subgroup is Example (Subgroups) (e), with $X = \{1, \dots, n+1\}$ and the chosen point $n+1$.

Idea. A permutation fixing $n+1$ cannot send any other point to $n+1$, since that value is taken; so it maps $\{1, \dots, n\}$ into itself. It also reaches every point there, because whatever reaches $j \leq n$ cannot be $n+1$. Restricting and extending undo each other, and restriction respects composition.

Proof.

- (a) Let $\sigma \in S'$ and $i \in \{1, \dots, n\}$. If $\sigma(i) = n+1 = \sigma(n+1)$, then $i = n+1$ by injectivity, which is false; so $\sigma(i) \in \{1, \dots, n\}$, and $\sigma': \{1, \dots, n\} \rightarrow \{1, \dots, n\}$, $\sigma'(i) := \sigma(i)$, is

a function. It is injective because σ is. It is surjective: for $j \in \{1, \dots, n\}$ there is $i \in \{1, \dots, n+1\}$ with $\sigma(i) = j$, since σ is surjective, and $i \neq n+1$, since $\sigma(n+1) = n+1 \neq j$. So $\sigma' \in S_n$.

(b) Write $R(\sigma) := \sigma'$ and $E(\rho) := \bar{\rho}$.

E maps into S' . The extension $\bar{\rho}$ is a function on $\{1, \dots, n+1\}$ with values in that set, and $\bar{\rho}^{-1}$ undoes it point by point: for $i \leq n$, $\bar{\rho}^{-1}(\bar{\rho}(i)) = \rho^{-1}(\rho(i)) = i$, and both fix $n+1$; the other composite is the same with ρ and ρ^{-1} exchanged. So $\bar{\rho}$ is a bijection (Sets, Relations, and Cardinality, Theorem 1.5.4) fixing $n+1$.

R and E are mutually inverse. For $\sigma \in S'$, $\bar{\sigma}'$ agrees with σ at every $i \leq n$ and at $n+1$, so $E(R(\sigma)) = \sigma$ (Sets, Relations, and Cardinality, Proposition 1.4.1). For $\rho \in S_n$, $(\bar{\rho})'$ agrees with ρ at every $i \leq n$, so $R(E(\rho)) = \rho$. Hence R is a bijection with inverse E (Sets, Relations, and Cardinality, Definition 1.5.2, Sets, Relations, and Cardinality, Theorem 1.5.4).

R is a homomorphism. Let $\sigma, \tau \in S'$ and $i \leq n$. By (a), $\tau(i) \leq n$, so

$$(\sigma\tau)'(i) = \sigma(\tau(i)) = \sigma'(\tau'(i)) = (\sigma'\tau')(i).$$

So $(\sigma\tau)' = \sigma'\tau'$, and R is an isomorphism. Its inverse E is an isomorphism by Proposition 3.3.2 (b). This proves the lemma. ■

So inside S_{n+1} sits a copy of S_n , the permutations that leave the last point alone. The factorial $n!$ is that of Sets, Relations, and Cardinality, Definition 2.3.1, read in $\mathbb{N}$: $0! = 1$ and $(n+1)! = n!(n+1)$.

Proposition 3.4.2. The Symmetric Group Has $n!$ Elements

For every $n \in \mathbb{N}$, S_n is finite and has $n!$ elements: $|S_n| = n!$.

Idea. Sort the permutations of $\{1, \dots, n+1\}$ by where they send the last point. Those sending it to $n+1$ are a copy of S_n , by the lemma. Those sending it to $k \leq n$ are matched with the first kind by composing with the swap $(k \ n+1)$. So there are $n+1$ classes of $n!$ permutations each.

Proof. We use induction on n (Logic and Proof, Axiom 4.2.1). For $n = 0$, S_0 has exactly one element, the empty function (Sets, Relations, and Cardinality, Proposition 1.4.2 (a)), and $0! = 1$.

Suppose S_n has $n!$ elements. For $k \in \{1, \dots, n+1\}$ let

$$A_k := \{\sigma \in S_{n+1} : \sigma(n+1) = k\}.$$

Every $\sigma \in S_{n+1}$ lies in exactly one A_k , namely for $k = \sigma(n+1)$. So the sets $A_1, \dots, A_{n+1}$ are pairwise disjoint and their union is S_{n+1} .

The class A_{n+1} . A_{n+1} is the subgroup S' of Lemma 3.4.1. By the induction hypothesis there is a bijection $\{1, \dots, n!\} \rightarrow S_n$ (Sets, Relations, and Cardinality, Definition 3.1.2);

composing it with the bijection $S_n \rightarrow S'$ of the lemma gives a bijection $\{1, \dots, n!\} \rightarrow A_{n+1}$ (Sets, Relations, and Cardinality, Theorem 1.4.4 (c)). So A_{n+1} has $n!$ elements.

The classes A_k , $k \leq n$. Let $\tau := (k \ n+1)$, a transposition with $\tau\tau = \text{id}$. If $\sigma \in A_k$, then $(\tau\sigma)(n+1) = \tau(k) = n+1$, so $\tau\sigma \in A_{n+1}$; if $\rho \in A_{n+1}$, then $(\tau\rho)(n+1) = \tau(n+1) = k$, so $\tau\rho \in A_k$. The maps $A_k \rightarrow A_{n+1}$, $\sigma \mapsto \tau\sigma$, and $A_{n+1} \rightarrow A_k$, $\rho \mapsto \tau\rho$, are mutually inverse, since $\tau(\tau\sigma) = (\tau\tau)\sigma = \sigma$ by (G1), $\tau\tau = \text{id}$ and (G2), and likewise for ρ . So $\sigma \mapsto \tau\sigma$ is a bijection $A_k \rightarrow A_{n+1}$ (Sets, Relations, and Cardinality, Theorem 1.5.4), and composing as before, A_k has $n!$ elements.

Adding up. We prove, by Sets, Relations, and Cardinality, Theorem 2.2.1 with base 1 (read on ω by Number Systems: From $\setminus(\setminus\mathbb{N}\setminus)$ to $\setminus(\setminus\mathbb{R}\setminus)$, Corollary 1.7.3 (b)), the statement $P(j)$: “if $j \leq n+1$, the union $A_1 \cup \dots \cup A_j$ has $j n!$ elements”. For $j = 1$ this is the count of A_1 , and the step adds the $n!$ elements of A_{j+1} , disjoint from $A_1 \cup \dots \cup A_j$, by Sets, Relations, and Cardinality, Proposition 3.1.5, with $j n! + n! = (j+1) n!$. For $j = n+1$, S_{n+1} has $(n+1) n! = (n+1)!$ elements. This completes the induction and proves the proposition. ■

So S_3 has 6 elements, S_4 has 24, and S_{10} already has 3628800. For S_3 all six can be listed: id , the three transpositions $(1\ 2)$, $(1\ 3)$, $(2\ 3)$, and the two 3-cycles $(1\ 2\ 3)$, $(1\ 3\ 2)$. These are six different permutations, so by the proposition they are all of S_3 : a proper subset of a 6-element set has fewer elements (Sets, Relations, and Cardinality, Proposition 3.1.6, Sets, Relations, and Cardinality, Corollary 3.1.4).

3.4.4 Disjoint cycles and the decomposition theorem

In [Example \(Computing with Cycles\)](#), σ came apart into the loops $(1\ 3)$ and $(2\ 5\ 4)$, which move disjoint sets of points, and the order of the two factors did not matter. Both observations hold in general. We start with the second: permutations moving disjoint sets of points do not interfere with each other.

Proposition 3.4.3. Disjoint Permutations Commute

Let $n \in \mathbb{N}$ and $\sigma, \tau \in S_n$ with $\text{supp } \sigma \cap \text{supp } \tau = \emptyset$. Then $\sigma\tau = \tau\sigma$. Moreover, every permutation σ maps $\text{supp } \sigma$ onto itself: $\sigma(\text{supp } \sigma) = \text{supp } \sigma$.

In particular, disjoint cycles commute.

Idea. A point moved by σ is fixed by τ , and so is its image under σ , because σ keeps its moved points among its moved points. So on $\text{supp } \sigma$ only σ acts, on $\text{supp } \tau$ only τ , and elsewhere neither: the order of application cannot matter.

Proof. σ maps its support onto itself. Let $i \in \text{supp } \sigma$. If $\sigma(i) \notin \text{supp } \sigma$, then $\sigma(\sigma(i)) = \sigma(i)$, and injectivity gives $\sigma(i) = i$, against $i \in \text{supp } \sigma$. So $\sigma(\text{supp } \sigma) \subseteq \text{supp } \sigma$. Conversely, let $j \in \text{supp } \sigma$ and $i := \sigma^{-1}(j)$. If $i \notin \text{supp } \sigma$, then $j = \sigma(i) = i \notin \text{supp } \sigma$, a contradiction; so $i \in \text{supp } \sigma$ and $j = \sigma(i) \in \sigma(\text{supp } \sigma)$. Hence $\sigma(\text{supp } \sigma) = \text{supp } \sigma$.

Commuting. Let $i \in \{1, \dots, n\}$. There are three cases, since i lies in at most one of the disjoint supports.

Case 1: $i \in \text{supp } \sigma$. Then $i \notin \text{supp } \tau$, so $\tau(i) = i$. Also $\sigma(i) \in \text{supp } \sigma$ by the first part, so $\sigma(i) \notin \text{supp } \tau$ and $\tau(\sigma(i)) = \sigma(i)$. Hence $(\sigma\tau)(i) = \sigma(i) = (\tau\sigma)(i)$.

Case 2: $i \in \text{supp } \tau$. The same argument with σ and τ exchanged gives $(\tau\sigma)(i) = \tau(i) = (\sigma\tau)(i)$.

Case 3: i lies in neither support. Then $\sigma(i) = i = \tau(i)$, and both products send i to i .

So $\sigma\tau$ and $\tau\sigma$ agree at every point, and $\sigma\tau = \tau\sigma$ (Sets, Relations, and Cardinality, Proposition 1.4.1). This proves the proposition. ■

The hypothesis “disjoint” cannot be dropped: $(1\ 2)$ and $(1\ 3)$ share the point 1, and [Example \(Computing with Cycles\)](#) shows that they do not commute. Exercise C1 looks at the dropped hypothesis more closely.

Now the main theorem. To break a permutation into loops, start at a point it moves and follow it until it comes back. The loop found is a cycle; remove it, and fewer points are moved, so induction finishes the job.

Theorem 3.4.4. Disjoint Cycle Decomposition

Let $n \in \mathbb{N}$. Every $\sigma \in S_n$ is a product $\sigma = \gamma_1\gamma_2 \cdots \gamma_s$, $s \in \mathbb{N}$, of pairwise disjoint cycles, each with support contained in $\text{supp } \sigma$. For $\sigma = \text{id}$ the product is empty ($s = 0$).

The clause about supports is part of the statement because the induction needs it: it is what makes the new cycle disjoint from the old ones. The theorem says nothing about uniqueness; that the decomposition is unique up to the order of the factors is proved in *Groups*, the chapter “Symmetric Groups and the Sign of a Permutation”.

Idea. Induction on the number m of points that σ moves. ① Pick a moved point i and follow its orbit $i, \sigma(i), \sigma^2(i), \dots$. There are only n points, so the orbit repeats, and it repeats first at i itself. ② The points before the return form a cycle γ on which σ acts exactly as γ does. ③ Peel it off: $\rho := \gamma^{-1}\sigma$ fixes the orbit and everything σ fixes, so it moves fewer points, and the induction hypothesis decomposes it. Then $\sigma = \gamma\rho$.

Before reading on: why must the orbit of i return to i itself, and not to some later point?

Proof. We use strong induction (Logic and Proof, Theorem 4.2.2) on $m \in \mathbb{N}$, for the statement: every $\sigma \in S_n$ whose support has m elements is a product of pairwise disjoint cycles with supports in $\text{supp } \sigma$. Every support is a subset of $\{1, \dots, n\}$, which has n elements, so it is finite (Sets, Relations, and Cardinality, Proposition 3.1.6), and every σ is covered by the statement for some m .

Let $\sigma \in S_n$, let $\text{supp } \sigma$ have m elements, and suppose the statement holds for every smaller number. If $m = 0$, then $\text{supp } \sigma = \emptyset$, so $\sigma = \text{id}$, the empty product (Definition 3.1.2). Let $m \geq 1$ and choose $i \in \text{supp } \sigma$.

Follow the orbit. Powers are taken in the group S_n (Definition 3.1.3). The map $\{0, 1, \dots, n\} \rightarrow \{1, \dots, n\}$, $c \mapsto \sigma^c(i)$, goes from a set of $n + 1$ elements to a set of n elements, so it is not injective (Sets, Relations, and Cardinality, Corollary 3.1.3 (a)): $\sigma^a(i) = \sigma^b(i)$ for some $0 \leq a < b \leq n$. Apply σ^{-a} to both sides. By Proposition 3.1.3 (a), $\sigma^{-a}\sigma^a = \sigma^0 = \text{id}$ and $\sigma^{-a}\sigma^b = \sigma^{b-a}$, so

$$i = \sigma^{b-a}(i), \quad b - a \geq 1.$$

So the set of $c \in \mathbb{Z}_{>0}$ with $\sigma^c(i) = i$ is non-empty and bounded below by 0, and it has a least element r (Number Systems: From $\mathbb{N}$ to $\mathbb{R}$, Proposition 2.3.6). Since $\sigma(i) \neq i$, $r \geq 2$.

The points $i, \sigma(i), \dots, \sigma^{r-1}(i)$ are distinct. Indeed, if $\sigma^c(i) = \sigma^d(i)$ with $0 \leq c < d \leq r - 1$, the argument just given yields $\sigma^{d-c}(i) = i$ with $0 < d - c < r$, against the minimality of r . Let

$$O := \{\sigma^c(i) : 0 \leq c \leq r - 1\}, \quad \gamma := (i \ \sigma(i) \ \dots \ \sigma^{r-1}(i)),$$

an r -cycle (Definition 3.4.2) with $\text{supp } \gamma = O$.

σ acts on O as γ does. For $0 \leq c < r - 1$, $\gamma(\sigma^c(i)) = \sigma^{c+1}(i) = \sigma(\sigma^c(i))$, where $\sigma^{c+1} = \sigma\sigma^c$ by Proposition 3.1.3 (a). For $c = r - 1$, $\gamma(\sigma^{r-1}(i)) = i = \sigma^r(i) = \sigma(\sigma^{r-1}(i))$. So $\sigma(x) = \gamma(x)$ for every $x \in O$. In particular σ moves every point of O , since γ does, and $O \subseteq \text{supp } \sigma$.

Peel it off. Let $\rho := \gamma^{-1}\sigma$. For $x \in O$, $\rho(x) = \gamma^{-1}(\sigma(x)) = \gamma^{-1}(\gamma(x)) = x$. For $x \notin \text{supp } \sigma$, we have $x \notin O$, so $\gamma(x) = x$ and hence $\gamma^{-1}(x) = x$; then $\rho(x) = \gamma^{-1}(x) = x$. So ρ fixes every point of O and every point outside $\text{supp } \sigma$:

$$\text{supp } \rho \subseteq \text{supp } \sigma \setminus O.$$

Since $i \in O$, the set $\text{supp } \sigma \setminus O$ is a proper subset of $\text{supp } \sigma$, so it has fewer than m elements, and so does its subset $\text{supp } \rho$ (Sets, Relations, and Cardinality, Proposition 3.1.6, twice). By the induction hypothesis, $\rho = \gamma_1 \cdots \gamma_s$ with pairwise disjoint cycles γ_j and $\text{supp } \gamma_j \subseteq \text{supp } \rho \subseteq \text{supp } \sigma \setminus O$. Each γ_j is therefore disjoint from γ , whose support is O .

Finally, $\gamma\rho = \gamma\gamma^{-1}\sigma = \sigma$, so by Proposition 3.1.2 (a)

$$\sigma = \gamma\gamma_1 \cdots \gamma_s,$$

a product of pairwise disjoint cycles, with $\text{supp } \gamma = O \subseteq \text{supp } \sigma$ and $\text{supp } \gamma_j \subseteq \text{supp } \sigma$. This completes the induction and proves the theorem. ■

The answer to the prompt. The orbit returns to i itself because σ is injective; in the proof, that is the step “apply σ^{-a} ”. If the first repetition were $\sigma^b(i) = \sigma^a(i)$ with $a \geq 1$, applying σ^{-1} would give the earlier repetition $\sigma^{b-1}(i) = \sigma^{a-1}(i)$. For a function that is not injective this fails: $f: \{1, 2\} \rightarrow \{1, 2\}$ with $f(1) = f(2) = 2$ has the orbit $1, 2, 2, 2, \dots$, which never comes back to 1.

The proof is an algorithm. Here it is run on one permutation.

A worked run. Let $\sigma \in S_6$ send $1 \mapsto 4$, $2 \mapsto 6$, $3 \mapsto 3$, $4 \mapsto 1$, $5 \mapsto 2$, $6 \mapsto 5$. Its support is $\{1, 2, 4, 5, 6\}$. Start at 1: $1 \mapsto 4 \mapsto 1$, so $r = 2$ and $\gamma = (1 \ 4)$. Peel it off: $\rho = (1 \ 4)^{-1}\sigma = (1 \ 4)\sigma$ fixes 1 and 4 and agrees with σ elsewhere, with support $\{2, 5, 6\}$. Start again at 2: $2 \mapsto 6 \mapsto 5 \mapsto 2$, so $r = 3$ and the next cycle is $(2 \ 6 \ 5)$. Peeling it off leaves the identity, and the point 3, fixed by σ , never enters. So

$$\sigma = (1 \ 4)(2 \ 6 \ 5).$$

Quick check. Decompose $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 4 & 1 & 2 \end{pmatrix} \in S_6$ into disjoint cycles.

Solution. Start at 1: $1 \mapsto 3 \mapsto 5 \mapsto 1$, the cycle $(1\ 3\ 5)$. The next moved point is 2: $2 \mapsto 6 \mapsto 2$, the cycle $(2\ 6)$. The point 4 is fixed. So the permutation is $(1\ 3\ 5)(2\ 6)$, and by [Proposition 3.4.3](#) also $(2\ 6)(1\ 3\ 5)$.

By [Proposition 3.4.3](#), two neighboring factors of a disjoint cycle decomposition may be exchanged; for instance $(1\ 3\ 5)(2\ 6) = (2\ 6)(1\ 3\ 5)$. The next section breaks each cycle further, into transpositions.

3.4.5 Exercises

3.4.5.1 A. Check your understanding

Exercise. A1

- (a) Compute $(1\ 2\ 3\ 4)(2\ 4)$ and $(2\ 4)(1\ 2\ 3\ 4)$ in S_4 , as products of disjoint cycles.
- (b) Find the inverse of $(1\ 5\ 2\ 7)$ in S_7 , written as a cycle starting at 1.
- (c) Run the proof of [Theorem 3.4.4](#) on

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \in S_5,$$

starting at $i = 1$: give the orbit of 1, the number r , the cycle γ , and $\rho = \gamma^{-1}\sigma$; then finish the run. Which step of the proof uses that σ is injective?

- (d) Compute $((1\ 2)(2\ 3))^2$ and $(1\ 2)^2(2\ 3)^2$ in S_3 .

Solution.

- (a) For $(1\ 2\ 3\ 4)(2\ 4)$, apply $(2\ 4)$ first: $1 \mapsto 1 \mapsto 2$, $2 \mapsto 4 \mapsto 1$, $3 \mapsto 3 \mapsto 4$, $4 \mapsto 2 \mapsto 3$. So the product is $(1\ 2)(3\ 4)$. For $(2\ 4)(1\ 2\ 3\ 4)$, apply $(1\ 2\ 3\ 4)$ first: $1 \mapsto 2 \mapsto 4$, $4 \mapsto 1 \mapsto 1$, $2 \mapsto 3 \mapsto 3$, $3 \mapsto 4 \mapsto 2$. So the product is $(1\ 4)(2\ 3)$. The two orders give different permutations.
- (b) By the inverse formula after [Definition 3.4.2](#), $(1\ 5\ 2\ 7)^{-1} = (7\ 2\ 5\ 1)$, which, started at 1, is $(1\ 7\ 2\ 5)$.
- (c) The orbit of 1 is $1 \mapsto 2 \mapsto 5 \mapsto 1$, so $r = 3$ and $\gamma = (1\ 2\ 5)$, with $\gamma^{-1} = (5\ 2\ 1) = (1\ 5\ 2)$. Then $\rho = \gamma^{-1}\sigma$ sends $1 \mapsto 2 \mapsto 1$, $2 \mapsto 5 \mapsto 2$, $5 \mapsto 1 \mapsto 5$, $3 \mapsto 4 \mapsto 4$, $4 \mapsto 3 \mapsto 3$: $\rho = (3\ 4)$. Running the proof on ρ , starting at 3: $3 \mapsto 4 \mapsto 3$, so the cycle is $(3\ 4)$, and peeling it off leaves id. Hence $\sigma = (1\ 2\ 5)(3\ 4)$. Injectivity is used where the orbit is shown to return to i itself: the step that applies σ^{-a} to $\sigma^a(i) = \sigma^b(i)$.
- (d) $(1\ 2)(2\ 3)$: $1 \mapsto 1 \mapsto 2$, $2 \mapsto 3 \mapsto 3$, $3 \mapsto 2 \mapsto 1$, so it is $(1\ 2\ 3)$, and its square sends $1 \mapsto 2 \mapsto 3$, $3 \mapsto 1 \mapsto 2$, $2 \mapsto 3 \mapsto 1$: $((1\ 2)(2\ 3))^2 = (1\ 3\ 2)$. On the other hand $(1\ 2)^2(2\ 3)^2 = \text{id}$, since transpositions are their own inverses. A second instance of the warning on $(\sigma\tau)^2$.

3.4.5.2 B. Practice

Exercise. B1: The table of S_3

List the six elements of S_3 in cycle notation and write out the table whose entry in row x and column y is xy . Hence find all $x \in S_3$ with $x^2 = \text{id}$, and all x that commute with every element of S_3 .

Solution. By the list after [Proposition 3.4.2](#), the elements are $\text{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)$. Computing each product right to left, as in [Example \(Computing with Cycles\)](#), the entry in row x , column y is xy :

xy	id	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
id	id	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$(1\ 2)$	$(1\ 2)$	id	$(1\ 3\ 2)$	$(1\ 2\ 3)$	$(2\ 3)$	$(1\ 3)$
$(1\ 3)$	$(1\ 3)$	$(1\ 2\ 3)$	id	$(1\ 3\ 2)$	$(1\ 2)$	$(2\ 3)$
$(2\ 3)$	$(2\ 3)$	$(1\ 3\ 2)$	$(1\ 2\ 3)$	id	$(1\ 3)$	$(1\ 2)$
$(1\ 2\ 3)$	$(1\ 2\ 3)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3\ 2)$	id
$(1\ 3\ 2)$	$(1\ 3\ 2)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3)$	id	$(1\ 2\ 3)$

For example, the entry in row $(1\ 2)$, column $(2\ 3)$ is $(1\ 2)(2\ 3)$: $1 \mapsto 1 \mapsto 2$, $2 \mapsto 3 \mapsto 3$, $3 \mapsto 2 \mapsto 1$, which is $(1\ 2\ 3)$.

Reading the diagonal, $x^2 = \text{id}$ exactly for $x = \text{id}, (1\ 2), (1\ 3), (2\ 3)$. An element x commutes with every element exactly when row x equals column x . This holds for id . It fails for every other element: $(1\ 2)(1\ 3) = (1\ 3\ 2) \neq (1\ 2\ 3) = (1\ 3)(1\ 2)$ handles $(1\ 2)$ and $(1\ 3)$; $(2\ 3)(1\ 2) = (1\ 3\ 2) \neq (1\ 2\ 3) = (1\ 2)(2\ 3)$ handles $(2\ 3)$; and $(1\ 2\ 3)(1\ 2) = (1\ 3) \neq (2\ 3) = (1\ 2)(1\ 2\ 3)$ handles $(1\ 2\ 3)$, while $(1\ 3\ 2)(1\ 2) = (2\ 3) \neq (1\ 3) = (1\ 2)(1\ 3\ 2)$ handles $(1\ 3\ 2)$. Hence only id commutes with everything.

Exercise. B2: Counting cycles

Let $n \in \mathbb{N}$ and $2 \leq k \leq n$. Show that S_n contains exactly

$$\frac{n!}{(n-k)!k}$$

k -cycles. Check the formula for $n = 4$ by listing the cycles of S_4 .

Solution. We use one counting fact: *if a finite set is the union of N pairwise disjoint subsets with q elements each, it has Nq elements.* This is Sets, Relations, and Cardinality, Proposition 3.1.5 applied $N - 1$ times, by induction on N , as in the proof of [Proposition 3.4.2](#).

Lists. Let T_k be the set of lists $(i_1, \dots, i_k)$ of **distinct** elements of $\{1, \dots, n\}$. Then T_k has $n(n-1) \cdots (n-k+1)$ elements, by induction on k : T_0 has one element, the empty list, and T_{j+1} is the disjoint union, over the lists $t \in T_j$, of the sets of lists extending t by a point x of the complement C of its entry set E . Here E has j elements, since the entries are distinct, so $j + |C| = n$ (Sets, Relations, and Cardinality, Proposition 3.1.6, Sets, Relations,

and Cardinality, Proposition 3.1.5, Sets, Relations, and Cardinality, Corollary 3.1.4) and C has $n - j$ elements. By the counting fact, T_{j+1} has $(n - j)$ times as many elements as T_j . Since $n(n - 1) \cdots (n - k + 1) \cdot (n - k)! = n!$, this number is $n!/(n - k)!$.

Lists to cycles. Each list in T_k defines the k -cycle $(i_1 \cdots i_k)$, and every k -cycle arises this way. Two lists give the same cycle exactly when one is a rotation of the other. Indeed, rotations give the same cycle (the remark after Definition 3.4.2). Conversely, if $(i_1 \cdots i_k) = (j_1 \cdots j_k) = \gamma$, then j_1 lies in the support $\{i_1, \dots, i_k\}$, say $j_1 = i_c$, and then $j_2 = \gamma(j_1) = i_{c+1}$, and so on around the loop: the second list is the first rotated to start at i_c . The k rotations of a list are k different lists, since their first entries differ. So the lists fall into pairwise disjoint classes of k elements, one class per k -cycle, and by the counting fact, with N_k the number of k -cycles,

$$k N_k = \frac{n!}{(n - k)!}.$$

Dividing by k gives the formula.

Check, $n = 4$. Transpositions: $4!/(2! \cdot 2) = 6$, namely $(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$. 3-cycles: $4!/(1! \cdot 3) = 8$, two for each of the four sets of three points: $(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)$. 4-cycles: $4!/(0! \cdot 4) = 6$, starting at 1 with the other three points in any of their $3! = 6$ orders: $(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)$.

Exercise. B3: The rotations of a square

Label the corners of a square 1, 2, 3, 4 in order around it. The quarter turn moves each label to the next corner, which is the permutation $\rho = (1\ 2\ 3\ 4) \in S_4$ (Example (Groups) (e)).

- (a) Compute ρ^2 and ρ^3 as products of disjoint cycles, and show $\rho^4 = \text{id}$.
- (b) Show that $\langle \rho \rangle = \{\text{id}, \rho, \rho^2, \rho^3\}$.
- (c) Show that $[k] \mapsto \rho^k$ is a well-defined isomorphism $(\mathbb{Z}/4\mathbb{Z}, +) \rightarrow \langle \rho \rangle$.

Solution.

- (a) $\rho^2 = \rho\rho$ sends $1 \mapsto 2 \mapsto 3, 3 \mapsto 4 \mapsto 1, 2 \mapsto 3 \mapsto 4, 4 \mapsto 1 \mapsto 2$: $\rho^2 = (1\ 3)(2\ 4)$. Then $\rho^3 = \rho^2\rho$ sends $1 \mapsto 2 \mapsto 4, 4 \mapsto 1 \mapsto 3, 3 \mapsto 4 \mapsto 2, 2 \mapsto 3 \mapsto 1$: $\rho^3 = (1\ 4\ 3\ 2)$. Finally $\rho^4 = \rho^3\rho$ sends $1 \mapsto 2 \mapsto 1, 2 \mapsto 3 \mapsto 2, 3 \mapsto 4 \mapsto 3, 4 \mapsto 1 \mapsto 4$: $\rho^4 = \text{id}$.
- (b) By Definition 3.2.2, $\langle \rho \rangle = \{\rho^k : k \in \mathbb{Z}\}$. For $k \in \mathbb{Z}$, divide by 4: $k = 4q + r$ with $0 \leq r < 4$ (Number Systems: From $\setminus(\setminus n\mathbb{N}\setminus)$ to $\setminus(\setminus n\mathbb{R}\setminus)$, Theorem 3.1.2 (a)). By Proposition 3.1.3 (a) and (c),

$$\rho^k = (\rho^4)^q \rho^r = \text{id}^q \rho^r = \rho^r,$$

where $\text{id}^q = (\rho^0)^q = \rho^0 = \text{id}$, again by (c). So every ρ^k is one of $\rho^0 = \text{id}, \rho, \rho^2, \rho^3$, and all four lie in $\langle \rho \rangle$.

- (c) *Well defined.* If $[k] = [k']$ in $\mathbb{Z}/4\mathbb{Z}$, then $k' - k \in 4\mathbb{Z}$ (Number Systems: From $\setminus(\setminus n\mathbb{N}\setminus)$ to $\setminus(\setminus n\mathbb{R}\setminus)$, Definition 3.4.2), so $k' = k + 4q$ for some $q \in \mathbb{Z}$, and $\rho^{k'} = \rho^k(\rho^4)^q = \rho^k$ as in (b). *Homomorphism.* $[k] + [l] = [k + l] \mapsto \rho^{k+l} = \rho^k \rho^l$ by Proposition 3.1.3 (a). *Bijective.* The four distinct classes $[0], [1], [2], [3]$, which are all of $\mathbb{Z}/4\mathbb{Z}$ (Number Systems: From $\setminus(\setminus n\mathbb{N}\setminus)$ to $\setminus(\setminus n\mathbb{R}\setminus)$, Theorem 3.4.3 (b)), go to $\text{id}, \rho, \rho^2, \rho^3$, which are four different permutations by (a) (they differ at the point 1: 1, 2, 3, 4) and are all of

$\langle \rho \rangle$ by (b). So the map is a bijection, hence an isomorphism, and the four rotations of the square form a copy of $\mathbb{Z}/4\mathbb{Z}$, as Section 3.1 announced.

3.4.5.3 C. Going deeper

Exercise. C1: Dropping “disjoint”

Proposition 3.4.3 assumes that the supports are disjoint.

- (a) Find two transpositions that share exactly one point and do not commute.
- (b) Find two cycles in S_3 with the **same** support that do commute.
- (c) In the proof of **Proposition 3.4.3**, which step fails for the pair of (a)?

Solution.

- (a) $(1\ 2)$ and $(2\ 3)$ share only the point 2. By the table of Exercise B1, $(1\ 2)(2\ 3) = (1\ 2\ 3)$ and $(2\ 3)(1\ 2) = (1\ 3\ 2)$, which differ (at 1: 2 versus 3).
- (b) $(1\ 2\ 3)$ and $(1\ 3\ 2)$ both have support $\{1, 2, 3\}$. They are inverse to each other (the inverse formula after **Definition 3.4.2**), so both products are id: $(1\ 2\ 3)(1\ 3\ 2) = \text{id} = (1\ 3\ 2)(1\ 2\ 3)$. More generally every permutation commutes with its inverse and with its own powers (**Proposition 3.1.3** (a)). So disjointness is sufficient for commuting, not necessary.
- (c) Case 1 at the point $i = 1 \in \text{supp}(1\ 2)$: the proof needs $\sigma(i) = 2 \notin \text{supp}\tau$, so that τ fixes it. Here $\tau = (2\ 3)$ moves 2, so $(\tau\sigma)(1) = \tau(2) = 3$, while $(\sigma\tau)(1) = \sigma(1) = 2$.

Exercise. C2: Powers of disjoint cycles

- (a) Let $\sigma = (i_1 \cdots i_k) \in S_n$ be a k -cycle and $m \in \mathbb{Z}_{>0}$. Prove that $\sigma^m = \text{id}$ if and only if $k \mid m$.
- (b) Let σ be a k -cycle and τ an l -cycle in S_n , disjoint. Prove that, for every $m \in \mathbb{Z}_{>0}$, $(\sigma\tau)^m = \text{id}$ if and only if $k \mid m$ and $l \mid m$.
- (c) Deduce that the least $m \geq 1$ with $(\sigma\tau)^m = \text{id}$ is the least positive common multiple of k and l .
- (d) Find the least $m \geq 1$ with $((1\ 2)(3\ 4\ 5))^m = \text{id}$ in S_5 .

Solution (Hint 1). For (b): a power of τ fixes every point that τ fixes.

Solution (Hint 2). Converse of (b): evaluate $\sigma^m\tau^m = \text{id}$ at a point of $\text{supp}\sigma$.

Solution.

- (a) Read the indices of the entries modulo k : for $j \in \mathbb{Z}$ let $i_j := i_t$, where $t \in \{1, \dots, k\}$ and $j \equiv t \pmod{k}$. Write $j - 1 = kq + s$ with $0 \leq s < k$ (Number Systems: From

$\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Theorem 3.1.2 (a)) and take $t := s + 1$; t is unique because s is. Then $\sigma(i_j) = i_{j+1}$ for every j , which is Definition 3.4.2. By induction on $m \in \mathbb{N}$ (Logic and Proof, Axiom 4.2.1), $\sigma^m(i_j) = i_{j+m}$ for every j : for $m = 0$ both sides are i_j , and $\sigma^{m+1}(i_j) = \sigma(\sigma^m(i_j)) = \sigma(i_{j+m}) = i_{j+m+1}$, using $\sigma^{m+1} = \sigma\sigma^m$ (Proposition 3.1.3 (a)). Every point off the cycle is fixed by σ , hence by σ^m . So $\sigma^m = \text{id}$ if and only if $i_{j+m} = i_j$ for every j . Since the entries $i_1, \dots, i_k$ are distinct, $i_{j+m} = i_j$ holds exactly when $j + m \equiv j \pmod{k}$, that is, when $k \mid m$.

- (b) The supports are disjoint, so $\sigma\tau = \tau\sigma$ (Proposition 3.4.3), and $(\sigma\tau)^m = \sigma^m\tau^m$ by Proposition 3.1.3 (d). If $k \mid m$ and $l \mid m$, then $\sigma^m = \tau^m = \text{id}$ by (a), so $(\sigma\tau)^m = \text{id}$. Conversely, suppose $\sigma^m\tau^m = \text{id}$. Let $x \in \text{supp } \sigma$. Then $x \notin \text{supp } \tau$, so $\tau(x) = x$, and by induction on m (Logic and Proof, Axiom 4.2.1) $\tau^m(x) = x$ (Hint 1). Hence $\sigma^m(x) = \sigma^m(\tau^m(x)) = x$. Also σ^m fixes every $x \notin \text{supp } \sigma$, since σ does. So $\sigma^m = \text{id}$, and then $\tau^m = \sigma^m\tau^m = \text{id}$. By (a), $k \mid m$ and $l \mid m$.
- (c) By (b), the $m \geq 1$ with $(\sigma\tau)^m = \text{id}$ are exactly the positive common multiples of k and l . This set contains kl , and so it has a least element (Number Systems: From $\backslash(\backslash nN\backslash)$ to $\backslash(\backslash nR\backslash)$, Proposition 2.3.6), the least positive common multiple of k and l . By Exercise (C3: Inclusions and intersections), the common multiples of k and l are exactly the multiples of that number.
- (d) (1 2) and (3 4 5) are disjoint, of lengths 2 and 3. The positive common multiples of 2 and 3 start 6, 12, $\dots$ (a common multiple of 2 is even, and $3 \nmid 2, 4$), so the least m is 6.

Marking scheme. (10 points) - 3: (a) the formula $\sigma^m(i_j) = i_{j+m}$ with indices modulo k , proved by induction, and the points off the cycle fixed. - 1: (a) from distinctness of the entries to $k \mid m$, in both directions. - 2: (b) commuting from disjointness, cited, and $(\sigma\tau)^m = \sigma^m\tau^m$ with the reason. - 3: (b) the converse: from $\sigma^m\tau^m = \text{id}$, uses disjointness of the supports to get $\sigma^m = \text{id}$ and $\tau^m = \text{id}$. - 1: (c) and (d), the least element named.

Second route: $\sigma^m = \tau^{-m}$, with $\text{supp } \sigma^m \subseteq \text{supp } \sigma$ and $\text{supp } \tau^{-m} \subseteq \text{supp } \tau$, and these are disjoint, so both are id; this earns the same 3 points if both inclusions are justified.

Fatal errors (0 for the step): $(\sigma\tau)^m = \sigma^m\tau^m$ without using that the cycles commute; “ $\sigma^m\tau^m = \text{id}$ so $\sigma^m = \tau^{-m}$, hence both are id” with no use of disjointness.