

5.4 Permutations and Iteration

Sections 5.1–5.3 built new functions from old ones: by cutting a domain down, by gluing pieces together, by passing to a quotient, and by combining two functions with an operation. This section does the simplest thing that can be done with a function whose codomain is its own domain: it applies the function again, and again. For a bijection, going forwards and backwards sorts the set into orbits, and on a finite set each orbit is a cycle. We prove that a bijection of a finite set, repeated often enough, gives back the identity, and we say after how many steps. Then we see what is left of this when the map is not a bijection.

5.4.1 Shuffling twelve cards

Lay twelve cards in a row and number the positions $0, 1, \dots, 11$. Cut the row into three piles of four: positions 0–3, positions 4–7, positions 8–11. Now deal them back: take the first card of each pile in turn, then the second card of each pile, and so on. The new row holds the cards from the old positions

$$0, 4, 8, 1, 5, 9, 2, 6, 10, 3, 7, 11,$$

in that order. So the card that was at position 4 is now at position 1, and the card that was at position 1 is now at position 3.

The card at old position i moves to the new position $\sigma(i)$, where

$$\sigma(i) = \begin{cases} 3i & \text{if } 0 \leq i \leq 3, \\ 3i - 11 & \text{if } 4 \leq i \leq 7, \\ 3i - 22 & \text{if } 8 \leq i \leq 11. \end{cases}$$

Check one card from each pile: card 2 lands at 6, card 5 at $15 - 11 = 4$, card 10 at $30 - 22 = 8$, as the row above says. The three pieces $\{0, \dots, 3\}$, $\{4, \dots, 7\}$, $\{8, \dots, 11\}$ are disjoint and cover the positions, so σ is a gluing with nothing to check on overlaps (Example (Method: define a function by gluing)).

Now shuffle again by the same rule. After two shuffles the card from position i is at $\sigma(\sigma(i))$. Follow card 1 through the shuffles: it goes to 3, then 9, then $27 - 22 = 5$, then $15 - 11 = 4$, then $12 - 11 = 1$. Card 2 goes to 6, 7, 10, 8, and back to 2. Cards 0 and 11 never move. These are $1 + 1 + 5 + 5 = 12$ cards, every card of the deck, and each is back in its place after five shuffles. The deck is in its starting order.

Was that luck? Three questions organize the section. Does **every** shuffle of a finite deck, repeated, bring the deck back? After how many shuffles? And what is left of the answer when the rule is not a shuffle, for instance when it sends two positions to one?

5.4.2 Permutations and iterates

A shuffle sends every position to a position, sends no two positions to the same one, and fills every position. That is a bijection from the set of positions to itself.

Definition 5.4.1. Permutation

Let X be a set. A **permutation** of X is a bijection $\sigma: X \rightarrow X$. The set of all permutations of X is written S_X ; it is a subset of X^X , the set of all functions $X \rightarrow X$.

For a finite set, a function $X \rightarrow X$ can be written as a **two-line table**: the elements of X in the top row, and under each element its image. For instance,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

is the function on $\{1, 2, 3\}$ with $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$. It is a table, not a matrix: nothing is multiplied. Such a function is a permutation exactly when its bottom row lists every element of X once: “every element appears” is surjectivity, and “no element twice” is injectivity. The hook’s shuffle is the table with top row $0, \dots, 11$ and bottom row $0, 3, 6, 9, 1, 4, 7, 10, 2, 5, 8, 11$. The two permutations of $\{1, 2\}$ are the identity and the swap $1 \mapsto 2$, $2 \mapsto 1$.

Section 5.3 made composition an operation on X^X (Proposition 5.3.5). The permutations are closed under it, and they keep everything that operation has.

Proposition 5.4.1. Permutations under Composition

Let X be a set.

- (a) If $\sigma, \tau \in S_X$, then $\sigma \circ \tau \in S_X$.
- (b) $\text{id}_X \in S_X$.
- (c) If $\sigma \in S_X$, then $\sigma^{-1} \in S_X$, and $\sigma \circ \sigma^{-1} = \text{id}_X = \sigma^{-1} \circ \sigma$.

Hence S_X is closed under $\circ$, and $\circ$ is an associative operation on S_X with identity id_X , in which every element σ is invertible, with inverse σ^{-1} .

Proof.

- (a) is Theorem 1.5.4 (c). (b) $\text{id}_X \circ \text{id}_X = \text{id}_X$, so id_X is a two-sided inverse of itself, and it is bijective by Theorem 1.6.4. (c) Since σ is bijective, it has the inverse σ^{-1} with $\sigma^{-1} \circ \sigma = \text{id}_X$ and $\sigma \circ \sigma^{-1} = \text{id}_X$ (Theorem 1.6.4, Definition 1.6.2). Read the other way round, the same two equations say that σ is a two-sided inverse of σ^{-1} , so σ^{-1} is bijective by Theorem 1.6.4.

By (a), S_X is closed under $\circ$, so $\circ$ restricted to $S_X \times S_X$ is an operation on S_X (Definition 5.3.1). Associativity holds on all of X^X (Proposition 5.3.5), so in particular on S_X ; id_X lies in S_X by (b) and is an identity there; and by (c) each $\sigma \in S_X$ has an inverse σ^{-1} that lies in S_X . ■

So everything Section 5.3 proved for an associative operation with an identity applies to S_X . For instance, Proposition 5.3.3 (c) gives $(\sigma \circ \tau)^{-1} = \tau^{-1} \circ \sigma^{-1}$: undo the second shuffle first.

Composing a function with itself needs only that its codomain is its domain; bijectivity is not needed. Shuffling twice is $\sigma \circ \sigma$, and “apply f a total of n times” is a definition by recursion.

Definition 5.4.2. Iterates

Let X be a set and $f: X \rightarrow X$. The **iterates** $f^n: X \rightarrow X$, for $n \in \mathbb{N}$, are defined by

$$f^0 := \text{id}_X, \quad f^{n+1} := f \circ f^n.$$

For $\sigma \in S_X$ and $n \in \mathbb{N}$, we also set $\sigma^{-n} := (\sigma^{-1})^n$.

The definition is an instance of Theorem 2.3.1, applied to the set X^X with the starting value id_X and the step $g: \mathbb{N} \times X^X \rightarrow X^X$, $g(n, h) := f \circ h$: there is exactly one sequence $n \mapsto f^n$ in X^X with these two properties. Unwinding, $f^1 = f \circ \text{id}_X = f$, $f^2 = f \circ f$, $f^3 = f \circ (f \circ f)$, and $f^n(x)$ is “apply f to x , n times”. For a permutation the two clauses do not clash: $\sigma^{-0} = (\sigma^{-1})^0 = \text{id}_X = \sigma^0$, and $(\sigma^{-1})^1 = \sigma^{-1}$ is the inverse function. So σ^k has one meaning for every $k \in \mathbb{Z}$. As Section 5.3 warned, f^n is always an iterate in this book, never the pointwise power $x \mapsto f(x)^n$.

The definition adds one f at a time, on the left. The first thing to prove is that blocks of f ’s can be moved around as the notation suggests.

Proposition 5.4.2. Laws of Iterates

Let X be a set, $f: X \rightarrow X$, and $m, n \in \mathbb{N}$.

- (a) $f^{m+n} = f^m \circ f^n$.
- (b) $(f^m)^n = f^{mn}$.
- (c) If $\sigma \in S_X$, then $\sigma^k \in S_X$ for every $k \in \mathbb{Z}$; $\sigma^n \circ \sigma^{-n} = \text{id}_X = \sigma^{-n} \circ \sigma^n$; and $\sigma^{k+l} = \sigma^k \circ \sigma^l$ for all $k, l \in \mathbb{Z}$.

Idea. Each law is an equation between iterates, and the definition only tells us how to peel one f off the left. So we induct on the exponent that appears first, peel one f , and use the induction hypothesis on what is left. For (c) the new feature is the sign: σ^{-n} undoes σ^n , and a mixed sum $k + l$ is handled by canceling the overlap.

Proof.

- (a) Fix n and induct on m (Logic and Proof, Axiom 4.2.1). For $m = 0$, $f^{0+n} = f^n = \text{id}_X \circ f^n = f^0 \circ f^n$ by Proposition 1.5.3. Suppose $f^{m+n} = f^m \circ f^n$. Then, by Definition 5.4.2, the induction hypothesis and Proposition 1.5.3,

$$f^{(m+1)+n} = f \circ f^{m+n} = f \circ (f^m \circ f^n) = (f \circ f^m) \circ f^n = f^{m+1} \circ f^n.$$

- (b) Induct on n . For $n = 0$, $(f^m)^0 = \text{id}_X = f^0 = f^{m \cdot 0}$. If $(f^m)^n = f^{mn}$, then $(f^m)^{n+1} = f^m \circ (f^m)^n = f^m \circ f^{mn} = f^{m+mn}$ by (a), and $m + mn = m(n+1)$.
- (c) First, $\sigma^n \in S_X$ for $n \in \mathbb{N}$, by induction: $\sigma^0 = \text{id}_X \in S_X$, and $\sigma^{n+1} = \sigma \circ \sigma^n \in S_X$ by Proposition 5.4.1 (a). Since $\sigma^{-1} \in S_X$ (Proposition 5.4.1 (c)), the same induction gives $\sigma^{-n} = (\sigma^{-1})^n \in S_X$. So $\sigma^k \in S_X$ for every $k \in \mathbb{Z}$.

Next, $\sigma^n \circ \sigma^{-n} = \text{id}_X$, by induction on n . For $n = 0$ both factors are id_X . If it holds for n , then $\sigma^{n+1} = \sigma^n \circ \sigma$ by (a) with the exponents n and 1, and $\sigma^{-(n+1)} = \sigma^{-1} \circ \sigma^{-n}$ by Definition 5.4.2, so

$$\sigma^{n+1} \circ \sigma^{-(n+1)} = \sigma^n \circ (\sigma \circ \sigma^{-1}) \circ \sigma^{-n} = \sigma^n \circ \sigma^{-n} = \text{id}_X,$$

by Proposition 1.5.3 and Proposition 5.4.1 (c). The equation $\sigma^{-n} \circ \sigma^n = \text{id}_X$ is the same induction with the roles of σ and σ^{-1} exchanged.

Finally, $\sigma^{k+l} = \sigma^k \circ \sigma^l$. When $k, l \geq 0$ this is (a). When $k, l \leq 0$, it is (a) for the map σ^{-1}

with the exponents $-k$ and $-l$. The cases with k and l of opposite signs reduce to these two by canceling, as the second reading below shows. ■

☞ **Second reading** • *The mixed signs in (c)*

Let k and l have opposite signs. All equalities below use Proposition 1.5.3, the cases of (c) already proved, and $\sigma^n \circ \sigma^{-n} = \text{id}_X = \sigma^{-n} \circ \sigma^n$ for $n \in \mathbb{N}$.

Case $k \geq 0, l = -b$ with $b > 0$. If $k \geq b$, then $\sigma^k = \sigma^{k-b} \circ \sigma^b$ by (a), so $\sigma^k \circ \sigma^{-b} = \sigma^{k-b} \circ (\sigma^b \circ \sigma^{-b}) = \sigma^{k-b}$. If $k < b$, then $\sigma^{-b} = \sigma^{-k} \circ \sigma^{-(b-k)}$ by (a) for σ^{-1} , so $\sigma^k \circ \sigma^{-b} = (\sigma^k \circ \sigma^{-k}) \circ \sigma^{-(b-k)} = \sigma^{k-b}$. In both cases $\sigma^k \circ \sigma^l = \sigma^{k+l}$.

Case $k = -a$ with $a > 0, l \geq 0$. If $l \geq a$, then $\sigma^l = \sigma^a \circ \sigma^{l-a}$ by (a), so $\sigma^{-a} \circ \sigma^l = (\sigma^{-a} \circ \sigma^a) \circ \sigma^{l-a} = \sigma^{l-a}$. If $l < a$, then $\sigma^{-a} = \sigma^{-(a-l)} \circ \sigma^{-l}$ by (a) for σ^{-1} , so $\sigma^{-a} \circ \sigma^l = \sigma^{-(a-l)} \circ (\sigma^{-l} \circ \sigma^l) = \sigma^{l-a}$. Again $\sigma^k \circ \sigma^l = \sigma^{k+l}$.

In particular σ^{-n} is the inverse of σ^n , by the middle clause of (c) and Definition 1.6.2: shuffling backwards n times undoes shuffling forwards n times.

Quick check. For $f: \mathbb{R} \rightarrow \mathbb{R}, f(x) = x + 3$, find f^n and prove your answer.

Solution. $f^n(x) = x + 3n$. By induction on n : $f^0(x) = x = x + 3 \cdot 0$; and if $f^n(x) = x + 3n$, then $f^{n+1}(x) = f(f^n(x)) = (x + 3n) + 3 = x + 3(n+1)$ by Definition 5.4.2. Here f^n is not the power $(x+3)^n$.

5.4.3 Orbits

In the hook, the cards fell into sets that move among themselves: $\{1, 3, 9, 5, 4\}$, $\{2, 6, 7, 10, 8\}$, $\{0\}$ and $\{11\}$. The natural guess for “in the same set” is “one card reaches the other”: $y = f^n(x)$ for some $n \in \mathbb{N}$. This relation is reflexive ($n = 0$) and transitive (add the exponents, Proposition 5.4.2 (a)). It is not symmetric. For $f: \mathbb{N} \rightarrow \mathbb{N}, f(n) = n + 1$, the point 0 reaches $1 = f(0)$, but 1 never reaches 0, since $f^n(1) = 1 + n \geq 1$. So reachability does not cut a set into pieces. For a permutation the repair is to allow negative exponents: walk backwards as well as forwards.

The orbit of a point is everywhere a permutation can take it, forwards or backwards.

Definition 5.4.3. Orbit, Forward Orbit, Fixed Point

Let X be a set and $\sigma \in S_X$. For $x, y \in X$, let $x \sim_\sigma y$ mean that $y = \sigma^k(x)$ for **some** $k \in \mathbb{Z}$. The **orbit** of x under σ is

$$O_\sigma(x) := \{\sigma^k(x) : k \in \mathbb{Z}\}.$$

For an arbitrary function $f: X \rightarrow X$, the **forward orbit** of x is $\{f^n(x) : n \in \mathbb{N}\}$. A **fixed**

point of f is an $x \in X$ with $f(x) = x$.

In words: the orbit collects every point reached from x by applying σ or σ^{-1} any number of times; the forward orbit uses f only, so it makes sense for every self-map. For a permutation, the forward orbit of x is contained in $O_\sigma(x)$, since $\mathbb{N} \subseteq \mathbb{Z}$; on a finite set the two are equal, as the next subsection proves. A fixed point is a point the map does not move, the sense in which Section 3.4 called 0 a fixed point of a bijection. For the hook's shuffle, $O_\sigma(1) = \{1, 3, 9, 5, 4\}$: since $\sigma^5(1) = 1$, the negative powers give nothing new ($\sigma^{-1}(1) = \sigma^4(1)$, and so on; [Proposition 5.4.4](#) proves this in general), and 0 and 11 are the fixed points.

Warning. Forward orbits need not cut a set into pieces. For $f(n) = n + 1$ on $\mathbb{N}$, the forward orbit of 0 is $\mathbb{N}$ and that of 1 is $\{n \in \mathbb{N} : n \geq 1\}$: they overlap and are not equal. Only orbits of a **permutation**, with k running over $\mathbb{Z}$, are guaranteed to be disjoint or equal.

The guarantee is the next theorem: $\sim_\sigma$ is an equivalence relation, and the orbits are its classes.

Theorem 5.4.3. The Orbits of a Permutation Partition the Set

Let X be a set and $\sigma \in S_X$. Then $\sim_\sigma$ is an equivalence relation on X , and the class of each $x \in X$ is $O_\sigma(x)$. Hence the orbits of σ form a partition of X . Moreover, x is a fixed point of σ if and only if $O_\sigma(x) = \{x\}$.

Proof. We check (Eq1)–(Eq3) of Definition 4.2.1, using [Proposition 5.4.2](#) (c) throughout. (Eq1): $x = \sigma^0(x)$, so $x \sim_\sigma x$. (Eq2): if $y = \sigma^k(x)$, then $\sigma^{-k}(y) = \sigma^{-k}(\sigma^k(x)) = \sigma^{-k+k}(x) = \sigma^0(x) = x$, so $y \sim_\sigma x$. (Eq3): if $y = \sigma^k(x)$ and $z = \sigma^l(y)$, then $z = \sigma^l(\sigma^k(x)) = \sigma^{l+k}(x)$ and $l + k \in \mathbb{Z}$, so $x \sim_\sigma z$.

The class of x is $\{y \in X : y \sim_\sigma x\}$ (Definition 4.2.2), which by (Eq2) is $\{y \in X : x \sim_\sigma y\} = \{\sigma^k(x) : k \in \mathbb{Z}\} = O_\sigma(x)$. By Theorem 4.2.1 (d), the classes form a partition of X .

If $O_\sigma(x) = \{x\}$, then $\sigma(x) = \sigma^1(x) \in O_\sigma(x)$, so $\sigma(x) = x$. Conversely, let $\sigma(x) = x$. Then $\sigma^n(x) = x$ for every $n \in \mathbb{N}$, by induction: $\sigma^{n+1}(x) = \sigma(\sigma^n(x)) = \sigma(x) = x$. Also $\sigma^{-1}(x) = \sigma^{-1}(\sigma(x)) = x$, so x is a fixed point of σ^{-1} , and the same induction gives $\sigma^{-n}(x) = (\sigma^{-1})^n(x) = x$. Hence $\sigma^k(x) = x$ for every $k \in \mathbb{Z}$, and $O_\sigma(x) = \{x\}$. ■

The theorem answers the hook's first observation: the cards always fall into sets that move among themselves, because the orbits are the classes of an equivalence relation, and each card lies in exactly one class.

Quick check. Find the orbits of $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$.

Solution. From 1: $1 \mapsto 3 \mapsto 1$, so $O_\sigma(1) = \{1, 3\}$ (going backwards, $\sigma^{-1}(1) = 3$, gives nothing new). From 2: $2 \mapsto 5 \mapsto 4 \mapsto 2$, so $O_\sigma(2) = \{2, 5, 4\}$. These two orbits are disjoint and cover

$\{1, \dots, 5\}$, as [Theorem 5.4.3](#) says they must; σ has no fixed point.

5.4.4 Following an orbit

In the hook, card 1 came back after five shuffles and card 0 after one. On a finite set this always happens, and the first return controls everything else about the orbit.

Proposition 5.4.4. Following an Orbit

Let X be a finite set, $\sigma \in S_X$, and $x \in X$. Then there is a **least** integer $k \geq 1$ with $\sigma^k(x) = x$. For this k :

- (a) the points $x, \sigma(x), \dots, \sigma^{k-1}(x)$ are distinct;
- (b) $O_\sigma(x) = \{x, \sigma(x), \dots, \sigma^{k-1}(x)\}$, so $O_\sigma(x)$ has exactly k elements;
- (c) for every $m \in \mathbb{Z}$, $\sigma^m(x) = x$ if and only if $k \mid m$.

The number k is the **length** of the orbit $O_\sigma(x)$.

Idea (Scratch work). The set is finite and the forward orbit $x, \sigma(x), \sigma^2(x), \dots$ is an infinite list, so the list must repeat. A repeat is not yet a return to x : we need to cancel the front of it, and that is where injectivity comes in.

Givens	Goal
X has n elements; σ bijective	some $k \geq 1$ with $\sigma^k(x) = x$
the $n + 1$ points $\sigma^0(x), \dots, \sigma^n(x)$	two of them equal: $m \mapsto \sigma^{m-1}(x)$ on $\{1, \dots, n + 1\}$ is not injective (Corollary 2.5.3 (a))
$\sigma^i(x) = \sigma^j(x)$ with $0 \leq i < j \leq n$;	cancel σ^i , which is injective
$\sigma^j = \sigma^i \circ \sigma^{j-i}$	(Proposition 5.4.2 (c)): $k = j - i$ works
a non-empty set of such k	a least one (Theorem 2.1.3)

Once there is a least return time, (a) is minimality again, and (c) is division with remainder: m full rounds plus a part of a round.

Proof. Let X have n elements. The set $\{1, \dots, n + 1\}$ has $n + 1$ elements, so the function $\{1, \dots, n + 1\} \rightarrow X$, $m \mapsto \sigma^{m-1}(x)$, is not injective (Corollary 2.5.3 (a)). So there are integers $0 \leq i < j \leq n$ with $\sigma^i(x) = \sigma^j(x)$. By [Proposition 5.4.2](#) (c), $\sigma^j = \sigma^i \circ \sigma^{j-i}$, so $\sigma^i(\sigma^{j-i}(x)) = \sigma^i(x)$, and since $\sigma^i \in S_X$ is injective, $\sigma^{j-i}(x) = x$. Hence the set $K := \{k \in \mathbb{N} : k \geq 1 \text{ and } \sigma^k(x) = x\}$ contains $j - i$, and by Theorem 2.1.3 it has a least element k .

- (a) Suppose $\sigma^i(x) = \sigma^j(x)$ with $0 \leq i < j < k$. As above, $\sigma^{j-i}(x) = x$, with $1 \leq j - i < k$, so $j - i \in K$, against the choice of k . So the k points are distinct.
- (b) First, $\sigma^{qk}(x) = x$ for every $q \in \mathbb{Z}$. For $q \geq 0$, by induction on q : $\sigma^0(x) = x$, and $\sigma^{(q+1)k}(x) = \sigma^k(\sigma^{qk}(x)) = \sigma^k(x) = x$ by [Proposition 5.4.2](#) (c). For $q < 0$, $-q > 0$, so $\sigma^{-qk}(x) = x$ by the case just proved, and $\sigma^{qk}(x) = \sigma^{qk}(\sigma^{-qk}(x)) = \sigma^0(x) = x$. Now let

$m \in \mathbb{Z}$, and write $m = qk + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < k$ (Theorem 2.2.3). Then

$$\sigma^m(x) = \sigma^r(\sigma^{qk}(x)) = \sigma^r(x).$$

If $r = 0$, this is x . If $1 \leq r < k$, then $\sigma^r(x) \neq x$, since otherwise $r \in K$ and $r < k$. So $\sigma^m(x) = x$ if and only if $r = 0$. By the uniqueness in Theorem 2.2.3, $r = 0$ holds exactly when $m = q'k$ for some $q' \in \mathbb{Z}$, that is, when $k \mid m$.

- (c) The display shows that every point $\sigma^m(x)$ of the orbit is one of $\sigma^0(x), \dots, \sigma^{k-1}(x)$; conversely each of these lies in the orbit. By (a), $\{1, \dots, k\} \rightarrow O_\sigma(x)$, $j \mapsto \sigma^{j-1}(x)$, is injective, and it is onto by what was just shown; so $O_\sigma(x)$ has k elements (Definition 2.5.2).

■

Two things to take from the proof. The forward orbit already contains $x, \sigma(x), \dots, \sigma^{k-1}(x)$, so on a finite set it equals the orbit: walking forwards reaches every point that walking backwards does. And in the existence of a return, the hypothesis “ σ is a permutation” was used once, in the cancellation of σ^i ; the rest of the proof needs negative powers only because the orbit is defined with them. The last subsection shows what goes wrong without it. The argument is a method in its own right.

Example. Method: follow an orbit

Template. (1) List the forward orbit $x, f(x), f^2(x), \dots$ (2) On a finite set of n elements, two of the first $n+1$ terms are equal (Corollary 2.5.3). (3) Take the first repeat, or the least return time (Theorem 2.1.3). (4) Carry the repeat with the map’s structure: cancel if the map is injective; push forward with $f^{l+1} = f \circ f^l$ always.

When to use it. Repeated application of one map on a finite set: shuffles, the tick of a clock, maps on $\mathbb{Z}/n$.

The usual failure. Speaking of “the first repeat” without proving that a repeat exists; canceling a map that is not injective, which forgets the tail before the cycle.

Now the hook, in full.

Example. The three-pile shuffle

Let σ be the shuffle of twelve cards in three piles of four. Show that σ is a permutation of $\{0, \dots, 11\}$, find its orbits and their lengths, and find the least $N \geq 1$ with $\sigma^N = \text{id}$.

Solution. A formula. Write $i = 4p + r$ with $0 \leq r < 4$ (Theorem 2.2.3); for $0 \leq i \leq 11$, $p \in \{0, 1, 2\}$ is the pile and r the place in it. The card is dealt in round r (counting from 0), after the p cards of that round from the earlier piles, so $\sigma(i) = 3r + p$; the three cases of the hook are $p = 0, 1, 2$.

A permutation. Every $j \in \{0, \dots, 11\}$ is $3r + p$ for exactly one pair with $0 \leq p < 3$, by Theorem 2.2.3, and then $0 \leq r \leq 3$, because $-3 < j - p = 3r \leq 11$. So $3r + p \mapsto 4p + r$ is a function $\{0, \dots, 11\} \rightarrow \{0, \dots, 11\}$, and it undoes σ on both sides. By Theorem 1.6.4, $\sigma \in S_X$ for $X = \{0, \dots, 11\}$.

Arithmetic modulo 11. $3i - \sigma(i) = 12p + 3r - 3r - p = 11p$, so $\sigma(i) \equiv 3i \pmod{11}$. For $i \leq 10$, $\sigma(i) \neq 11$, since $3r + p = 11$ forces $r = 3$, $p = 2$, that is $i = 11$. So for $i \leq 10$, $3i = 11p + \sigma(i)$ with $0 \leq \sigma(i) < 11$, and $\sigma(i)$ is the remainder of $3i$ on division by 11 by the uniqueness in Theorem 2.2.3; and $\sigma(11) = 11$.

Orbits. Follow each orbit (Example (Method: follow an orbit)), reducing modulo 11:

$$\begin{aligned} 1 &\mapsto 3 \mapsto 9 \mapsto 5 \mapsto 4 \mapsto 1 & (27 \equiv 5, 15 \equiv 4, 12 \equiv 1), \\ 2 &\mapsto 6 \mapsto 7 \mapsto 10 \mapsto 8 \mapsto 2 & (18 \equiv 7, 21 \equiv 10, 30 \equiv 8, 24 \equiv 2), \end{aligned}$$

and 0, 11 are fixed. The orbits are $\{0\}$, $\{11\}$, $\{1, 3, 9, 5, 4\}$, $\{2, 6, 7, 10, 8\}$, of lengths 1, 1, 5, 5.

The return. Each length divides 5, so $\sigma^5(x) = x$ for every x by Proposition 5.4.4 (c), and $\sigma^5 = \text{id}$ by Proposition 1.5.1. For $1 \leq N < 5$, $5 \nmid N$, so $\sigma^N(1) \neq 1$ by the same part (c). Hence $N = 5$. The arithmetic agrees: $3^5 = 243 = 22 \cdot 11 + 1$, so five shuffles multiply every position below 11 by 1 modulo 11.

Quick check. Let $t: \mathbb{Z}/12 \rightarrow \mathbb{Z}/12$, $[a] \mapsto [a + 1]$, be the tick of Example (Maps out of the clock). What is the length of the orbit of $[1]$ under t ? And under $[a] \mapsto [a + 3]$?

Solution. By induction, $t^m([1]) = [1 + m]$ for $m \in \mathbb{N}$, and $[1 + m] = [1]$ exactly when $12 \mid m$ (Theorem 4.2.1 (b), Definition 4.2.5). The least $m \geq 1$ is 12: the orbit is all of $\mathbb{Z}/12$, of length 12. The map $[a] \mapsto [a + 3]$ is well defined as the tick is $((a + 3) - (a' + 3) = a - a')$, and is a permutation with inverse $[a] \mapsto [a - 3]$. From $[1]$: $[1], [4], [7], [10], [13] = [1]$. The orbit is $\{[1], [4], [7], [10]\}$, of length 4.

5.4.5 Cycles

The hook's shuffle moves 1, 3, 9, 5, 4 round in a ring, moves 2, 6, 7, 10, 8 round in another ring, and leaves everything else alone. A permutation that moves one ring and nothing else deserves a name and a notation.

Definition 5.4.4. Cycle

Let X be a set, $k \geq 2$, and $x_1, \dots, x_k \in X$ **distinct**. The **cycle** $(x_1 x_2 \cdots x_k)$ is the function $X \rightarrow X$ that sends $x_j \mapsto x_{j+1}$ for $1 \leq j < k$, sends $x_k \mapsto x_1$, and sends every other point of X to itself. Two cycles are **disjoint** if their sets of entries are disjoint.

The cycle is defined by gluing (Example (Method: define a function by gluing)): the pieces $\{x_1, \dots, x_k\}$ and its complement are disjoint and cover X , so there are no overlaps to check. On the first piece the rule reads the index j of a point, and distinctness makes that index unique. On the second piece the rule is the identity. A cycle is a permutation: $(x_k \cdots x_2 x_1)$ sends $x_{j+1} \mapsto x_j$ and $x_1 \mapsto x_k$, so composing it with $(x_1 \cdots x_k)$ in either order fixes each x_j , and it fixes each point off the entries since both factors do. By Theorem 1.6.4 the cycle is bijective, with inverse the reversed cycle. The same cycle has k names: $(1\ 3\ 9\ 5\ 4) = (3\ 9\ 5\ 4\ 1)$, since both send each entry to the next one round the ring.

The theorem below says that every permutation of a finite set is built from its orbits in this way: one cycle for each orbit with at least two points. Before stating it, note that such orbits are finitely many. Let X have n elements via a bijection $\varphi: \{1, \dots, n\} \rightarrow X$. Send each orbit O to the least i with $\varphi(i) \in O$ (Theorem 2.1.3). Distinct orbits are disjoint (Theorem 5.4.3), so they get distinct indices, and the orbits are in bijection with a subset of $\{1, \dots, n\}$, which is finite (Proposition 2.5.6).

Theorem 5.4.5. Cycle Decomposition

Let X be a finite set and $\sigma \in S_X$. Let $O_1, \dots, O_r$ be the distinct orbits of σ with at least two elements, choose $x_i \in O_i$, let k_i be the number of elements of O_i (so $|O_i| = k_i$), and let

$$\gamma_i := (x_i \ \sigma(x_i) \ \dots \ \sigma^{k_i-1}(x_i)).$$

Then $\gamma_1, \dots, \gamma_r$ are pairwise disjoint cycles, $\gamma_i \circ \gamma_j = \gamma_j \circ \gamma_i$ for all i, j , and

$$\sigma = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_r,$$

bracketed from the left; if $r = 0$, this says $\sigma = \text{id}_X$.

Idea. Both sides are functions on X , so we compare values (Proposition 1.5.1). A point of O_i is moved by γ_i exactly as σ moves it, and is left alone by every other γ_j . So composing the cycles one at a time, the composite agrees with σ on more and more orbits; an induction on the number of cycles composed makes that precise.

Proof. By Proposition 5.4.4, $O_i = \{x_i, \sigma(x_i), \dots, \sigma^{k_i-1}(x_i)\}$ and these $k_i \geq 2$ points are distinct, so γ_i is a cycle whose set of entries is O_i . Distinct orbits are disjoint (Theorem 5.4.3), so the cycles are pairwise disjoint.

The key value. Let $y \in O_i$, say $y = \sigma^m(x_i)$ with $0 \leq m < k_i$. If $m < k_i - 1$, then $\gamma_i(y) = \sigma^{m+1}(x_i) = \sigma(y)$ by Definition 5.4.2. If $m = k_i - 1$, then $\gamma_i(y) = x_i = \sigma^{k_i}(x_i) = \sigma(y)$. So $\gamma_i(y) = \sigma(y)$ for every $y \in O_i$; and $\sigma(y) = \sigma^{m+1}(x_i) \in O_i$. For $j \neq i$, γ_j fixes every point of O_i , since $O_i \cap O_j = \emptyset$.

Define $\delta^{(0)} := \text{id}_X$ and $\delta^{(j)} := \delta^{(j-1)} \circ \gamma_j$ for $1 \leq j \leq r$, by recursion (Theorem 2.3.1, with $\gamma_j := \text{id}_X$ for $j > r$). So $\delta^{(r)}$ is the composite of the theorem, bracketed from the left. Let $U_j := O_1 \cup \dots \cup O_j$. We prove by induction on $j \leq r$:

$$\delta^{(j)}(y) = \sigma(y) \text{ for } y \in U_j, \quad \delta^{(j)}(y) = y \text{ for } y \in X \setminus U_j.$$

For $j = 0$, $U_0 = \emptyset$ and $\delta^{(0)} = \text{id}_X$. Suppose the claim holds for $j-1$, and let $y \in X$. If $y \in O_j$, then $\gamma_j(y) = \sigma(y) \in O_j$, and O_j is disjoint from U_{j-1} , so $\delta^{(j)}(y) = \delta^{(j-1)}(\sigma(y)) = \sigma(y)$. If $y \notin O_j$, then $\gamma_j(y) = y$, so $\delta^{(j)}(y) = \delta^{(j-1)}(y)$; and since $y \notin O_j$, $y \in U_{j-1}$ exactly when $y \in U_{j-1}$. In both cases the claim holds for j .

For $j = r$: a point y outside U_r lies in an orbit with fewer than two elements, so $O_\sigma(y) = \{y\}$ and $\sigma(y) = y$ (Theorem 5.4.3). Hence $\delta^{(r)}(y) = \sigma(y)$ for every $y \in X$, and $\delta^{(r)} = \sigma$ by Proposition 1.5.1. That disjoint cycles commute is a check of values at a point of O_i , of O_j , and of neither, which the second reading below carries out.

■

○ **Second reading** · *Disjoint cycles commute*

Let $i \neq j$ and $y \in X$. If $y \in O_i$, then $\gamma_j(y) = y$, so $\gamma_i(\gamma_j(y)) = \gamma_i(y) = \sigma(y)$; and $\gamma_i(y) = \sigma(y) \in O_i$ is fixed by γ_j , so $\gamma_j(\gamma_i(y)) = \sigma(y)$. If $y \in O_j$, the same two lines with i and j exchanged give $\sigma(y)$ on both sides. If y lies in neither, both cycles fix it, and both composites give y . So $\gamma_i \circ \gamma_j = \gamma_j \circ \gamma_i$ by Proposition 1.5.1. For $i = j$ there is nothing to prove.

From now on we write $\gamma\delta$ for $\gamma \circ \delta$, the right factor applied first, the convention of *Algebraic Preliminaries*, Chapter 2. Two examples. The three-pile shuffle of [Example \(The three-pile shuffle\)](#) is

$$\sigma = (1\ 3\ 9\ 5\ 4)(2\ 6\ 7\ 10\ 8),$$

and the two factors may be written in either order. The tick of Example (Maps out of the clock) has one orbit, all of $\mathbb{Z}/12$, with $t^m([0]) = [m]$, so it is the single cycle $([0]\ [1]\ \cdots\ [11])$.

The decomposition answers the hook's second question. A permutation of a finite set comes back to the identity, and the orbit lengths say when.

Corollary 5.4.6. Some Power Is the Identity

Let X be a finite set and $\sigma \in S_X$. For an integer $N \geq 1$, $\sigma^N = \text{id}_X$ if and only if the length of every orbit of σ divides N . There is such an N .

Proof. By Proposition 1.5.1, $\sigma^N = \text{id}_X$ means $\sigma^N(x) = x$ for every $x \in X$, and by [Proposition 5.4.4](#) (c) that holds exactly when the length k_x of $O_\sigma(x)$ divides N for every x . This proves the equivalence.

For existence, let X have n elements, and let $\varphi: \{1, \dots, n\} \rightarrow X$ be a bijection (Definition 2.5.2), and let $N := \prod_{i=1}^n k_{\varphi(i)}$ (Definition 2.3.1). Each factor is an integer ≥ 1 , so N is an integer ≥ 1 . Write $P_j := \prod_{i=1}^j k_{\varphi(i)}$. For a fixed $i \leq n$, $k_{\varphi(i)} \mid P_j$ for every j with $i \leq j \leq n$, by induction on j : $P_i = P_{i-1} k_{\varphi(i)}$, and $P_j \mid P_{j+1} = P_j k_{\varphi(j+1)}$, so Proposition 1.1.1 carries the divisibility from P_j to P_{j+1} . Hence $k_x \mid P_n = N$ for every $x = \varphi(i) \in X$, and $\sigma^N = \text{id}_X$ by the first part. ■

The **least** such N is the least positive common multiple of the orbit lengths: by the corollary, N works exactly when it is a common multiple of all of them. For two distinct lengths a and b , that least common multiple is the one found in Example (The supremum under divisibility is the least common multiple). For the three-pile shuffle the lengths are 1, 1, 5, 5, and the answer is 5, as the hook found by hand.

Quick check. Decompose $[a] \mapsto [5a]$ on $\mathbb{Z}/12$ into disjoint cycles.

Solution. The map is well defined by Proposition 4.2.5. Applying it twice gives $[25a] = [a]$, since $25 \equiv 1 \pmod{12}$, so it is its own inverse and a permutation. Following orbits: $[1] \mapsto [5] \mapsto [25] = [1]$; $[2] \mapsto [10] \mapsto [50] = [2]$; $[4] \mapsto [20] = [8] \mapsto [40] = [4]$; $[7] \mapsto [35] = [11] \mapsto [55] = [7]$; and $[0], [3], [6], [9]$ are fixed ($15 \equiv 3, 30 \equiv 6, 45 \equiv 9$). So the map is $([1] [5])([2] [10])([4] [8])([7] [11])$.

5.4.6 Maps that are not permutations

The last question of the hook: what if the rule sends two positions to one? Then there is no inverse, orbits in the sense of Definition 5.4.3 are not defined, and Proposition 5.4.4's cancellation is not available. Forward orbits still exist, and on a finite set they still repeat. What changes is that the repeat need not involve the starting point.

Proposition 5.4.7. Forward Orbits of a Self-Map of a Finite Set

Let X be a set with n elements, $f: X \rightarrow X$, and $x \in X$. There are integers $m \geq 0$ and $p \geq 1$ with $m + p \leq n$ such that

$$f^{l+p}(x) = f^l(x) \quad \text{for every integer } l \geq m.$$

Idea. This is Example (Method: follow an orbit) with step (4) done without canceling: the pigeonhole repeat $f^i(x) = f^j(x)$ cannot be pulled back to x , but it can be pushed forward, one application of f at a time.

Proof. As in the proof of Proposition 5.4.4, Corollary 2.5.3 (a) gives integers $0 \leq i < j \leq n$ with $f^i(x) = f^j(x)$. Let $m := i$ and $p := j - i \geq 1$; then $m + p = j \leq n$. We prove $f^{l+p}(x) = f^l(x)$ by induction on $l \geq m$ (Theorem 2.2.1). For $l = m$ it is $f^j(x) = f^i(x)$. If it holds for l , then by Definition 5.4.2

$$f^{l+1+p}(x) = f(f^{l+p}(x)) = f(f^l(x)) = f^{l+1}(x).$$

■

The forward orbit of x is thus a **tail** $x, f(x), \dots, f^{m-1}(x)$ followed by a **cycle** that repeats with period p . For a permutation the tail can be taken empty: $m = 0$ and $p = k$, the length of $O_\sigma(x)$, work, by Proposition 5.4.4 (c). Without injectivity it need not be.

Example. Squaring on an eleven-hour clock

Let $s: \mathbb{Z}/11 \rightarrow \mathbb{Z}/11$, $s([a]) := [a^2]$. Show that s is well defined, follow the forward orbit of $[2]$, and find m and p . Does $[2]$ ever come back?

Solution. Well defined. If $a \equiv a' \pmod{11}$, then $a \cdot a \equiv a' \cdot a'$ by the product clause of Proposition 4.2.5: the rule $a \mapsto [a^2]$ is constant on classes (Example (Method: define a

function on a quotient)).

The orbit. Squaring and reducing modulo 11:

$$[2] \mapsto [4] \mapsto [16] = [5] \mapsto [25] = [3] \mapsto [9] \mapsto [81] = [4],$$

using $16 - 11 = 5$, $25 - 22 = 3$, $81 - 77 = 4$. So $s^5([2]) = [4] = s^1([2])$, with $s^1([2]), \dots, s^4([2])$ distinct: the tail is $[2]$, and the cycle is $[4], [5], [3], [9]$, so $m = 1$ and $p = 4$.

No return. The set $C = \{[4], [5], [3], [9]\}$ contains $s([2]) = [4]$, and the computation above shows that s maps C into C ($[4] \mapsto [5] \mapsto [3] \mapsto [9] \mapsto [4]$). So by induction on $l \geq 1$ (Theorem 2.2.1, Definition 5.4.2), every $s^l([2])$ with $l \geq 1$ lies in C , and none of them is $[2]$. This is the tail-and-cycle shape that Proposition 5.4.7 predicts. The reason is the failure of injectivity: $s([2]) = [4] = s([9])$, with $[2] \neq [9]$. The point $[4]$ has two arrows coming in, from $[2]$ and from $[9]$; the cycle comes back to $[4]$ through $[9]$, and never needs $[2]$ again.

The example is the usual failure of Example (Method: follow an orbit) in action: from $s([2]) = s([9])$ one may not cancel s to conclude $[2] = [9]$.

Quick check. Follow the forward orbit of $[0]$ under $[a] \mapsto [a^2 + 1]$ on $\mathbb{Z}/7$, and find m and p .

Solution. $[0] \mapsto [1] \mapsto [2] \mapsto [5] \mapsto [26] = [5]$, since $26 - 21 = 5$. The tail is $[0], [1], [2]$, so $m = 3$, and $[5]$ is a fixed point, so $p = 1$.

Remark (Looking ahead). *Algebraic Preliminaries*, Chapter 2 gives a name, group, to a set with an associative operation that has an identity and inverses, as $\circ$ on S_X does by Proposition 5.4.1, and studies S_X among its examples.

5.4.7 Exercises

5.4.7.1 A. Check your understanding

Exercise. A1

- For $\sigma = (1\ 4)(2\ 3\ 5)$ on $\{1, \dots, 5\}$, write the two-line tables of σ , σ^{-1} and σ^2 .
- Let $f: \{1, \dots, 5\} \rightarrow \{1, \dots, 5\}$ send $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 4$, $4 \mapsto 2$, $5 \mapsto 5$. Find m and p as in Proposition 5.4.7 for $x = 1$, with m as small as possible.
- How many fixed points has the three-pile shuffle of twelve cards?

Solution.

- Applying the right factor first, σ sends $1 \mapsto 4$, $2 \mapsto 3$, $3 \mapsto 5$, $4 \mapsto 1$, $5 \mapsto 2$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}, \quad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix}, \quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}.$$

The table of σ^{-1} is that of σ read from bottom to top; $\sigma^{-1} = (1\ 4)(2\ 5\ 3)$ and $\sigma^2 = (2\ 5\ 3)$, since the swap $(1\ 4)$ applied twice is the identity.

- (b) The forward orbit is $1, 2, 3, 4, 2, \dots$: $f^4(1) = 2 = f^1(1)$, with $f^0(1), \dots, f^3(1)$ distinct. So $m = 1$, $p = 3$ work. And $m = 0$ is impossible: f maps $\{2, 3, 4\}$ into itself and $f(1) = 2$, so by induction $f^l(1) \in \{2, 3, 4\}$ for every $l \geq 1$, and $f^p(1) \neq 1 = f^0(1)$ for every $p \geq 1$.
- (c) Two: positions 0 and 11 ([Example \(The three-pile shuffle\)](#)).

5.4.7.2 B. Practice

Exercise. B1: Doubling on nine hours

Let $d: \mathbb{Z}/9 \rightarrow \mathbb{Z}/9$, $d([a]) := [2a]$. Show that d is a permutation, decompose it into disjoint cycles, and find the least $N \geq 1$ with $d^N = \text{id}$.

Solution. d is well defined by Proposition 4.2.5, and so is $e([a]) := [5a]$. Since $10 \equiv 1 \pmod{9}$, $e(d([a])) = [10a] = [a]$ and $d(e([a])) = [a]$, so d is bijective with inverse e (Theorem 1.6.4). Following orbits ([Example \(Method: follow an orbit\)](#)):

$$[1] \mapsto [2] \mapsto [4] \mapsto [8] \mapsto [16] = [7] \mapsto [14] = [5] \mapsto [10] = [1],$$

$[3] \mapsto [6] \mapsto [12] = [3]$, and $[0]$ is fixed. So

$$d = ([1\ 2\ 4\ 8\ 7\ 5])([3\ 6]),$$

with orbit lengths 6, 2, 1. By [Corollary 5.4.6](#), $d^N = \text{id}$ exactly when $6 \mid N$, $2 \mid N$ and $1 \mid N$, that is, when $6 \mid N$ (since $2 \mid 6$, Proposition 1.1.1). The least such $N \geq 1$ is 6.

Exercise. B2: Iterates commute

Let $f, g: X \rightarrow X$. Prove that $f^{n+1} = f^n \circ f$ for every $n \in \mathbb{N}$, and that if $f \circ g = g \circ f$, then $f^n \circ g = g \circ f^n$ for every $n \in \mathbb{N}$.

Solution. The first equation is [Proposition 5.4.2](#) (a) with the exponents n and 1, since $f^1 = f$. For the second, induct on n . For $n = 0$, $\text{id}_X \circ g = g = g \circ \text{id}_X$ (Proposition 1.5.3). If $f^n \circ g = g \circ f^n$, then, by [Definition 5.4.2](#) and Proposition 1.5.3,

$$f^{n+1} \circ g = f \circ (f^n \circ g) = f \circ (g \circ f^n) = (f \circ g) \circ f^n = (g \circ f) \circ f^n = g \circ f^{n+1}.$$

Exercise. B3: Orbits are invariant

Let $\sigma \in S_X$ and $x \in X$. Prove that $\sigma(O_\sigma(x)) = O_\sigma(x)$.

Solution. ($\subseteq$) A point of $\sigma(O_\sigma(x))$ is $\sigma(\sigma^k(x)) = \sigma^{k+1}(x)$ for some $k \in \mathbb{Z}$ (Definition 1.7.1, [Proposition 5.4.2](#) (c)), and $k+1 \in \mathbb{Z}$. ($\supseteq$) For $k \in \mathbb{Z}$, $\sigma^k(x) = \sigma(\sigma^{k-1}(x))$ by [Proposition 5.4.2](#)

(c), and $\sigma^{k-1}(x) \in O_\sigma(x)$.

Exercise. B4: Prove or disprove

Prove or disprove each statement.

- (a) If X is finite and $f: X \rightarrow X$ is injective, then every $x \in X$ has $f^k(x) = x$ for some $k \geq 1$.
- (b) If $f: X \rightarrow X$ and $f^N = \text{id}_X$ for some $N \geq 1$, then f is a permutation.
- (c) Every function from a finite non-empty set to itself has a fixed point.
- (d) Every orbit of a permutation is finite.
- (e) If X is finite and every orbit of $\sigma \in S_X$ has length 1 or 2, then $\sigma \circ \sigma = \text{id}_X$.

Solution.

- (a) True. The proof of [Proposition 5.4.4](#) used only that σ^i is injective. Here f^i is injective for every $i \in \mathbb{N}$, by induction with Theorem 1.5.4 (a) ($f^0 = \text{id}_X$, $f^{i+1} = f \circ f^i$). So pigeonhole gives $f^i(x) = f^j(x)$ with $i < j$; by [Proposition 5.4.2](#) (a), $f^j = f^i \circ f^{j-i}$, and canceling f^i gives $f^{j-i}(x) = x$, with $j - i \geq 1$.
- (b) True. By [Proposition 5.4.2](#) (a), $f \circ f^{N-1} = f^N = \text{id}_X$ and $f^{N-1} \circ f = f^{(N-1)+1} = \text{id}_X$. So f^{N-1} is a two-sided inverse of f , and f is bijective by Theorem 1.6.4.
- (c) False. The swap of $\{0, 1\}$, $0 \mapsto 1$, $1 \mapsto 0$, moves both points.
- (d) False. $\sigma: \mathbb{Z} \rightarrow \mathbb{Z}$, $\sigma(n) = n + 1$, is a permutation with inverse $n \mapsto n - 1$, and $\sigma^k(0) = k$ for every $k \in \mathbb{Z}$ (induction in each direction), so $O_\sigma(0) = \mathbb{Z}$. This is not finite: it contains $\mathbb{N}$, which is infinite (Example (Hilbert's Hotel), Proposition 2.5.6).
- (e) True. Each orbit length k_x divides 2, so $\sigma^2(x) = x$ by [Proposition 5.4.4](#) (c), for every x ; and $\sigma^2 = \sigma \circ \sigma$ by [Definition 5.4.2](#). So $\sigma \circ \sigma = \text{id}_X$ by Proposition 1.5.1.

5.4.7.3 C. Going deeper

Exercise. C1: Exit check: fifteen cards

Fifteen cards lie at positions $0, \dots, 14$. Cut them into three piles of five and deal them back in turn, as in the hook, so that

$$\sigma(i) = \begin{cases} 3i & \text{if } 0 \leq i \leq 4, \\ 3i - 14 & \text{if } 5 \leq i \leq 9, \\ 3i - 28 & \text{if } 10 \leq i \leq 14. \end{cases}$$

Show that σ is a permutation, decompose it into disjoint cycles, and find the least $N \geq 1$ with $\sigma^N = \text{id}$.

Solution. A permutation. The three pieces have images $\{0, 3, 6, 9, 12\}$, $\{1, 4, 7, 10, 13\}$ and $\{2, 5, 8, 11, 14\}$: the positions with remainder 0, 1, 2 on division by 3. Each piece is injective ($3i - c = 3i' - c$ gives $i = i'$), and the images are disjoint and cover $\{0, \dots, 14\}$ by Theorem 2.2.3. So two different cards in one piece land in different places, two cards in

different pieces land in different images, and every position is hit: σ is bijective. (This is the cross-piece check of Example (Method: define a function by gluing).)

Arithmetic modulo 14. Write $i = 5p + r$ with $0 \leq r < 5$; the card lands at $\sigma(i) = 3r + p$, and $3i - \sigma(i) = 15p - p = 14p$, so $\sigma(i) \equiv 3i \pmod{14}$. Since $3r + p = 14$ only for $r = 4, p = 2$, that is $i = 14$, σ maps $\{0, \dots, 13\}$ into itself, with $\sigma(i)$ the remainder of $3i$ on division by 14, and $\sigma(14) = 14$. By induction and Proposition 4.2.5, $\sigma^k(i) \equiv 3^k i \pmod{14}$ for $i \leq 13$.

Cycles. 0, 7 ($21 \equiv 7$) and 14 are fixed. Following orbits (Example (Method: follow an orbit)):

$$\begin{aligned} 1 &\mapsto 3 \mapsto 9 \mapsto 13 \mapsto 11 \mapsto 5 \mapsto 1 \quad (27 \equiv 13, 39 \equiv 11, 33 \equiv 5, 15 \equiv 1), \\ 2 &\mapsto 6 \mapsto 4 \mapsto 12 \mapsto 8 \mapsto 10 \mapsto 2 \quad (18 \equiv 4, 36 \equiv 8, 24 \equiv 10, 30 \equiv 2). \end{aligned}$$

These account for $3 + 6 + 6 = 15$ positions, so $\sigma = (1\ 3\ 9\ 13\ 11\ 5)(2\ 6\ 4\ 12\ 8\ 10)$ by Theorem 5.4.5.

The return. The orbit lengths are 1, 1, 1, 6, 6. By Corollary 5.4.6, $\sigma^N = \text{id}$ exactly when $6 \mid N$; the least $N \geq 1$ is 6. Check: $3^6 = 729 = 52 \cdot 14 + 1$, so six shuffles multiply every position below 14 by 1 modulo 14.

Marking scheme. (10 points) - 2: proves σ bijective, including the check across pieces (or by an explicit inverse). - 2: reduces σ to multiplication by 3 modulo 14 on $\{0, \dots, 13\}$ with 14 fixed, or follows the orbits directly from the three formulas. - 3: finds the two 6-cycles and the fixed points 0, 7, 14, with the arithmetic shown. - 3: concludes $N = 6$ and shows that no smaller N works, either from the orbit lengths by Corollary 5.4.6 or directly ($3^6 \equiv 1 \pmod{14}$ and $\sigma^k(1) \neq 1$ for $1 \leq k \leq 5$). Fatal errors (0 for the step): claiming bijectivity from injectivity of each piece alone; taking N as the sum, rather than a common multiple, of the orbit lengths.

Exercise. C2: Find the error

Here is a claim and a proof.

Claim. For every function f from a finite set X to itself and every $x \in X$, there is $k \geq 1$ with $f^k(x) = x$.

Proof. By pigeonhole, $f^i(x) = f^j(x)$ for some $i < j$. Apply f^{-i} to both sides: $x = f^{j-i}(x)$. Take $k = j - i$.

Is the claim true? Find the line that fails, say why, and state what the argument does prove.

Solution. The claim is false. The line that fails is “apply f^{-i} ”: f^{-i} is defined only for a permutation (Definition 5.4.2), and the claim is about every self-map. A counterexample to that step, and to the claim, is Example (Squaring on an eleven-hour clock) with $x = [2]$: $s^1([2]) = s^5([2]) = [4]$, but no $s^k([2])$ with $k \geq 1$ is $[2]$. The correct conclusion from the pigeonhole repeat is Proposition 5.4.7: after a tail, the forward orbit is periodic. For a permutation, or more generally an injective f (B4 (a)), the cancellation is legitimate and the claim holds.

Marking scheme. (10 points) - 3: says the claim is false, with a counterexample. - 4: names the failing line, “apply f^{-i} ”, and the reason: f need not be invertible, or even injective. - 3: states the correct conclusion (tail then cycle, Proposition 5.4.7), or the extra hypothesis

under which the proof is right. Fatal errors (0 for the step): accepting the proof because the claim holds for permutations; objecting to the pigeonhole step, which is correct.

Exercise. C3: Each point, its own clock

Let X be a finite set and $\sigma \in S_X$. Show that the length of $O_\sigma(x)$ is the same for all points x of one orbit. Show also that if σ has exactly two orbits, then the number of elements of X is the sum of their lengths.

Solution. Let $y \in O_\sigma(x)$. Then $x \sim_\sigma y$, so $O_\sigma(y) = O_\sigma(x)$ by Theorem 5.4.3 and Theorem 4.2.1 (b). By Proposition 5.4.4 (b), the length of an orbit is its number of elements, so the length at y is the number of elements of $O_\sigma(y) = O_\sigma(x)$, which is the length at x .

If σ has exactly two orbits O and O' , they are disjoint and their union is X (Theorem 5.4.3, Definition 4.2.3). By Proposition 5.4.4 (b), O and O' have as many elements as their lengths k and k' , so $X = O \cup O'$ has $k + k'$ elements by Proposition 2.5.5.

5.4.7.4 R. Review

Exercise. R1

On $\mathbb{R}$, let $x \sim y$ mean $x - y \in \mathbb{Z}$. Show that $[x] \mapsto [2x]$ is a well-defined surjection $\mathbb{R}/\sim \rightarrow \mathbb{R}/\sim$ that is not injective.

Solution. Here $\sim$ is the equivalence relation of Example (The reals modulo the integers). Let $g: \mathbb{R} \rightarrow \mathbb{R}/\sim$, $g(x) := [2x]$. If $x \sim x'$, then $2x - 2x' = 2(x - x') \in \mathbb{Z}$, so g is constant on classes, and Theorem 5.2.3 (a) gives the function $[x] \mapsto [2x]$ (Example (Method: define a function on a quotient)). It is onto: every class $[y]$ is the image of $[y/2]$. It is not injective: $[0] \mapsto [0]$ and $[\frac{1}{2}] \mapsto [1] = [0]$, while $[0] \neq [\frac{1}{2}]$ by Example (The reals modulo the integers). The method is the well-definedness check of Section 4.2 (Example (Method: checking that a definition on classes is well defined)).

Exercise. R2

Let $\varphi: X \rightarrow Y$ be a bijection. Show that $\sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$ is a bijection from S_X to S_Y , and that x is a fixed point of σ if and only if $\varphi(x)$ is a fixed point of $\varphi \circ \sigma \circ \varphi^{-1}$.

Solution. For $\sigma \in S_X$, $\varphi \circ \sigma \circ \varphi^{-1}: Y \rightarrow Y$ is a composite of bijections (φ^{-1} is bijective by Theorem 1.6.4, since φ is a two-sided inverse of it, Definition 1.6.2), so it lies in S_Y (Theorem 1.5.4 (c)); so the rule is a function $c: S_X \rightarrow S_Y$. In the same way $d(\tau) := \varphi^{-1} \circ \tau \circ \varphi$ defines $d: S_Y \rightarrow S_X$. By Proposition 1.5.3 and $\varphi^{-1} \circ \varphi = \text{id}_X$, $\varphi \circ \varphi^{-1} = \text{id}_Y$ (Definition 1.6.2),

$$d(c(\sigma)) = \varphi^{-1} \circ ((\varphi \circ \sigma) \circ \varphi^{-1}) \circ \varphi = (\varphi^{-1} \circ (\varphi \circ \sigma)) \circ (\varphi^{-1} \circ \varphi) = ((\varphi^{-1} \circ \varphi) \circ \sigma) \circ \text{id}_X = \sigma,$$

with Proposition 1.5.3 at each regrouping, and likewise $c(d(\tau)) = \tau$. So c has a two-sided

inverse and is bijective (Theorem 1.6.4). For the fixed points,

$$c(\sigma)(\varphi(x)) = \varphi(\sigma(\varphi^{-1}(\varphi(x)))) = \varphi(\sigma(x)),$$

which equals $\varphi(x)$ if and only if $\sigma(x) = x$, since φ is injective. The tools are the composites and inverses of Sections 1.5 and 1.6. (Section 3.3's Exercise (C2: Permutations of the naturals) used bijections of $\mathbb{N}$ for a different purpose.)

Exercise. R3

Let $f: \mathbb{R} \rightarrow \mathbb{R}$, $f(x) = 2x + 1$. Prove that $f^n(x) = 2^n x + 2^n - 1$ for every $n \in \mathbb{N}$ and $x \in \mathbb{R}$.

Solution. By induction on n (Logic and Proof, Axiom 4.2.1), with the powers of Definition 2.3.2. For $n = 0$: $f^0(x) = x = 1 \cdot x + 1 - 1$. If $f^n(x) = 2^n x + 2^n - 1$, then by Definition 5.4.2

$$f^{n+1}(x) = 2(2^n x + 2^n - 1) + 1 = 2^{n+1} x + 2^{n+1} - 1,$$

since $2 \cdot 2^n = 2^n \cdot 2 = 2^{n+1}$. The method is the induction of Section 2.2 on a sequence defined by recursion (Theorem 2.3.1).

Exercise. R4

Let $f: X \rightarrow Y$, $A \subseteq X$ and $B \subseteq Y$. Show that $(f|_A)^{-1}(B) = A \cap f^{-1}(B)$.

Solution. For every a , by Definition 1.7.2 applied to $f|_A: A \rightarrow Y$ and to f , and $f|_A(a) = f(a)$ for $a \in A$ (Definition 5.1.1),

$$a \in (f|_A)^{-1}(B) \iff a \in A \wedge f(a) \in B \iff a \in A \cap f^{-1}(B),$$

where the second step uses $A \subseteq X$. The two sets have the same elements, so they are equal. This is the element-chasing of Section 1.7 applied to a function built in Section 5.1. The tool is the preimage definition (Definition 1.7.2), tested pointwise. The look-alike tools fail: image rules such as Proposition 5.1.1 compare images, not preimages, and $f(A \cap C)$ can be strictly smaller than $f(A) \cap f(C)$; and $(f|_A)^{-1}$ here is a preimage, not an inverse function, which $f|_A$ need not have.