2.2 PERMUTATIONS

In high school mathematics, the words *permutation* and *arrangement* are used interchangeably, if the word *arrangement* is used at all. We draw a distinction between them.

Definition. A ***permutation*** of a set X is a bijection $\alpha\colon X \to X$. If X is a finite set and $|X| = n$, then an ***arrangement*** of X is a list $x_1, x_2, \ldots, x_n$ with no repetitions of all the elements of X.

Given an arrangement $x_1, x_2, \ldots, x_n$, define $f\colon \{1, 2, \ldots, n\} \to X$ by $f(i) = x_i$; thus, the list $x_1, x_2, \ldots, x_n$ displays the values of f. That there are no repetitions on the list says that f is injective, for $i \neq j$ implies $x_i = f(i) \neq f(j) = x_j$; that every $x \in X$ occurs on the list says that f is surjective. Thus, an arrangement of X defines a bijection $f\colon \{1, 2, \ldots, n\} \to X$.

For example, there are six arrangements of $X = \{a, b, c\}$:

$$abc; \quad acb; \quad bac; \quad bca; \quad cab; \quad cba.$$

All we can do with such lists is count their number, and there are exactly $n!$ arrangements of an n-element set X.

If $X = \{1, 2, \ldots, n\}$, then a permutation $\alpha\colon X \to X$ gives the list $\alpha(1) = i_1, \alpha(2) = i_2, \ldots, \alpha(n) = i_n$. We can use a two-rowed notation to denote this permutation: if $\alpha(j)$ is the jth item on the list, then

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & j & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(j) & \ldots & \alpha(n) \end{pmatrix}.$$

Informally, arrangements (lists) and permutations (bijections) are simply different ways of describing the same thing. The advantage of viewing permutations as bijections, rather than as lists, is that they can now be composed and, by Exercise 2.13(ii) on page 102, their composite is also a permutation.

The results in this section first appeared in an article of Cauchy in 1815.

Definition. The family of all the permutations of a set X, denoted by S_X, is called the ***symmetric group*** on X. When $X = \{1, 2, \ldots, n\}$, S_X is usually denoted by S_n, and it is called the ***symmetric group on*** n ***letters***.

Notice that composition in S_3 is not commutative. If

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \text{and} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

then their composites[3] are

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \text{and} \qquad \beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

so that $\alpha \circ \beta \neq \beta \circ \alpha$ [for example, $\alpha \circ \beta$: $1 \mapsto \alpha(\beta(1)) = \alpha(2) = 3$ while $\beta \circ \alpha$: $1 \mapsto 2 \mapsto 1$].

On the other hand, some permutations do commute; for example,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

commute, as the reader may check.

Composition in S_X satisfies the ***cancellation law***:

$$\text{if } \gamma \circ \alpha = \gamma \circ \beta, \text{ then } \alpha = \beta.$$

To see this,

$$\begin{aligned} \alpha &= 1_X \circ \alpha \\ &= (\gamma^{-1} \circ \gamma) \circ \alpha \\ &= \gamma^{-1} \circ (\gamma \circ \alpha) \\ &= \gamma^{-1} \circ (\gamma \circ \beta) \\ &= (\gamma^{-1} \circ \gamma) \circ \beta \\ &= 1_X \circ \beta = \beta. \end{aligned}$$

A similar argument shows that

$$\alpha \circ \gamma = \beta \circ \gamma \text{ implies } \alpha = \beta.$$

Aside from being cumbersome, there is a major problem with the two-rowed notation for permutations. It hides the answers to elementary questions such as: is the square of a permutation the identity? what is the smallest positive integer m so that the mth power of a permutation is the identity? can one factor a permutation into simpler permutations? The special permutations introduced below will remedy this defect.

Let us first simplify notation by writing $\beta\alpha$ instead of $\beta \circ \alpha$ and (1) instead of 1_X.

[3]There are authors who multiply permutations differently, so that their $\alpha \circ \beta$ is our $\beta \circ \alpha$. This is a consequence of their putting "functions on the right:" instead of writing $\alpha(i)$ as we do, they write $(i)\alpha$. Consider the composite of permutations α and β in which we first apply β and then apply α. We write $i \mapsto \beta(i) \mapsto \alpha(\beta(i))$. In the right-sided notation, $i \mapsto (i)\beta \mapsto ((i)\beta)\alpha$. Thus, the notational switch causes a switch in the order of multiplication.

Definition. If $\alpha \in S_n$ and $i \in \{1, 2, \ldots, n\}$, then α ***fixes*** i if $\alpha(i) = i$, and α ***moves*** i if $\alpha(i) \neq i$.

Definition. Let $i_1, i_2, \ldots, i_r$ be distinct integers in $\{1, 2, \ldots, n\}$. If $\alpha \in S_n$ fixes the other integers (if any) and if

$$\alpha(i_1) = i_2, \quad \alpha(i_2) = i_3, \quad \ldots, \quad \alpha(i_{r-1}) = i_r, \quad \alpha(i_r) = i_1,$$

then α is called an ***r-cycle***. One also says that α is a cycle of ***length*** r.

A 2-cycle interchanges i_1 and i_2 and fixes everything else; 2-cycles are also called ***transpositions***. A 1-cycle is the identity, for it fixes every i; thus, all 1-cycles are equal: $(i) = (1)$ for all i.

Consider the permutation

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

The two-rowed notation does not help us recognize that α is, in fact, a 5-cycle: $\alpha(1) = 4$, $\alpha(4) = 5$, $\alpha(5) = 2$, $\alpha(2) = 3$, and $\alpha(3) = 1$. We now introduce new notation: an r-cycle α, as in the definition, shall be denoted by

$$\alpha = (i_1\ i_2\ \ldots\ i_r).$$

For example, the 5-cycle α above will be written $\alpha = (1\ 4\ 5\ 2\ 3)$. The reader may check that

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\ 2\ 3\ 4),$$

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

and

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = (1\ 2\ 3).$$

Notice that

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

is not a cycle; in fact, $\beta = (1\ 2)(3\ 4)$. The term *cycle* comes from the Greek word for circle. One can picture the cycle $(i_1\ i_2\ \ldots\ i_r)$ as a clockwise rotation of the circle (see Figure 2.8). Any i_j can be taken as the "starting point," and so there are r different cycle notations for any r-cycle:

$$(i_1\ i_2\ \ldots\ i_r) = (i_2\ i_3\ \ldots\ i_r\ i_1) = \cdots = (i_r\ i_1\ i_2\ \ldots\ i_{r-1}).$$

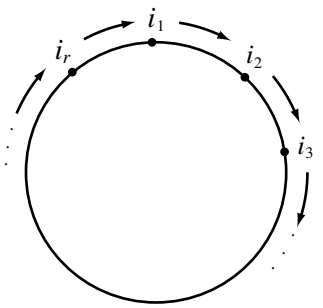

Figure 2.8 A Cycle as a Rotation

Figure 2.9 is a page from Cauchy's 1815 paper in which he introduces the calculus of permutations. Notice that his notation for a cycle is a circle.

Let us now give an ***algorithm*** to factor a permutation into a product of cycles. For example, take

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 \end{pmatrix}.$$

Begin by writing "(1." Now $\alpha\colon 1 \mapsto 6$, so write "(1 6." Next, $\alpha\colon 6 \mapsto 1$, and so the parentheses close: α begins "(1 6)." The first number not having appeared is 2, and so we write "(1 6)(2." Now $\alpha\colon 2 \mapsto 4$, so we write "(1 6)(2 4." Since $\alpha\colon 4 \mapsto 2$, the parentheses close once again, and we write "(1 6)(2 4)." The smallest remaining number is 3; now $3 \mapsto 7$, $7 \mapsto 8$, $8 \mapsto 9$, and $9 \mapsto 3$; this gives the 4-cycle (3 7 8 9). Finally, $\alpha(5) = 5$; we claim that

$$\alpha = (1\ 6)(2\ 4)(3\ 7\ 8\ 9)(5).$$

Since multiplication in S_n is composition of functions, our claim is that

$$\alpha(i) = [(1\ 6)(2\ 4)(3\ 7\ 8\ 9)(5)](i)$$

for every i between 1 and n (after all, two functions f and g are equal if and only if $f(i) = g(i)$ for every i in their common domain). The right side is the composite $\beta\gamma\delta$, where $\beta = (1\ 6)$, $\gamma = (2\ 4)$, and $\delta = (3\ 7\ 8\ 9)$ (actually, there is also the 1-cycle (5), which we may ignore when we are evaluating, for (5) is the identity function). Now $\alpha(1) = 6$; multiplication of permutations views the permutations as functions and then takes their composite. For example, if $i = 1$,

QU'UNE FONCTION PEUT ACQUÉRIR, ETC. 79

Nous observerons d'abord que, si dans la substitution $\begin{pmatrix} A_s \\ A_t \end{pmatrix}$ formée par deux permutations prises à volonté dans la suite

$$A_1, \quad A_2, \quad A_3, \quad \ldots, \quad A_N,$$

les deux termes A_s, A_t renferment des indices correspondants qui soient respectivement égaux, on pourra, sans inconvénient, supprimer les mêmes indices pour ne conserver que ceux des indices correspondants qui sont respectivement inégaux. Ainsi, par exemple, si l'on fait $n = 5$, les deux substitutions

$$\begin{pmatrix} 1.2.3.4.5 \\ 2.3.1.4.5 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1.2.3 \\ 2.3.1 \end{pmatrix}$$

seront équivalentes entre elles. Je dirai qu'une substitution aura été réduite à sa plus simple expression lorsqu'on aura supprimé, dans les deux termes, tous les indices correspondants égaux.

Soient maintenant $\alpha, \beta, \gamma, \ldots, \zeta, \eta$ plusieurs des indices $1, 2, 3, \ldots, n$ en nombre égal à p, et supposons que la substitution $\begin{pmatrix} A_s \\ A_t \end{pmatrix}$ réduite à sa plus simple expression prenne la forme

$$\begin{pmatrix} \alpha & \beta & \gamma & \ldots & \zeta & \eta \\ \beta & \gamma & \delta & \ldots & \eta & \alpha \end{pmatrix},$$

en sorte que, pour déduire le second terme du premier, il suffise de ranger en cercle, ou plutôt en polygone régulier, les indices α, β, γ, $\delta, \ldots, \zeta, \eta$ de la manière suivante :

et de remplacer ensuite chaque indice par celui qui, le premier, vient prendre sa place lorsqu'on fait tourner d'orient en occident le polygone

Figure 2.9

A. Cauchy, M´emoire sur le nombre des valeurs qu'une fonction peut acqu´erir lorsqu'on y permute de toutes les manieères possibles les quantit´es qu'elle renferme
J. de l'École Poly., XVII^e Cahier, Tome X (1815), pp. 1–28
From: *Oeuvres Completes d'Augustin Cauchy*, II Serie, Tome I, Gauthier-Villars, Paris, 1905.

then

$$\begin{aligned}\beta\gamma\delta(1) &= \beta(\gamma(\delta(1))) \\ &= \beta(\gamma(1)) \qquad \delta \text{ fixes } 1 \\ &= \beta(1) \qquad\quad \gamma \text{ fixes } 1 \\ &= 6.\end{aligned}$$

In Proposition 2.24, we will give a more satisfactory proof that α has been factored as a product of cycles.

Factorizations into cycles are very convenient for multiplication of permutations. For example, in S_5, let us simplify the product

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

by displaying the "partial outputs" of the algorithm: $\sigma\colon 1 \mapsto 3 \mapsto 4 \mapsto 4$, so that σ begins (1 4. Next, $\sigma\colon 4 \mapsto 4 \mapsto 2 \mapsto 1$; hence, σ begins (1 4). The smallest number not yet considered is 2, and $\sigma\colon 2 \mapsto 5 \mapsto 1 \mapsto 2$; thus, σ fixes 2, and σ begins (1 4)(2). The smallest number not yet considered is 3, and $\sigma\colon 3 \mapsto 2 \mapsto 5 \mapsto 5$. Finally, $\sigma\colon 5 \mapsto 1 \mapsto 3 \mapsto 3$, and we conclude that

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

In the factorization of a permutation into cycles, given by the algorithm above, one notes that the family of cycles is *disjoint* in the following sense.

Definition. Two permutations $\alpha, \beta \in S_n$ are ***disjoint*** if every i moved by one is fixed by the other: if $\alpha(i) \neq i$, then $\beta(i) = i$, and if $\beta(j) \neq j$, then $\alpha(j) = j$. A family $\beta_1 \ldots, \beta_t$ of permutations is ***disjoint*** if each pair of them is disjoint.

Consider the special case of cycles. If $\alpha = (i_1\ i_2\ \ldots\ i_r)$ and $\beta = (j_1\ j_2\ \ldots\ j_s)$, then any k in the intersection $\{i_1, i_2, \ldots, i_r\} \cap \{j_1, j_2, \ldots, j_s\}$ is moved by both α and β. Thus, it is easy to see that two cycles are disjoint if and only if $\{i_1, i_2, \ldots, i_r\} \cap \{j_1, j_2, \ldots, j_s\} = \varnothing$; that is, $\{i_1, i_2, \ldots, i_r\}$ and $\{j_1, j_2, \ldots, j_s\}$ are disjoint sets.

When permutations α and β are disjoint, there are exactly three distinct possibilities for a number i: it is moved by α, it is moved by β, or it is moved by neither (that is, it is fixed by both).

Lemma 2.22. *Disjoint permutations $\alpha, \beta \in S_n$ commute.*

Proof. It suffices to prove that if $1 \leq i \leq n$, then $\alpha\beta(i) = \beta\alpha(i)$. If β moves i, say, $\beta(i) = j \neq i$, then β also moves j [otherwise, $\beta(j) = j$ and $\beta(i) = j$ contradicts β's being an injection]; since α and β are disjoint, $\alpha(i) = i$ and $\alpha(j) = j$. Hence $\beta\alpha(i) = j = \alpha\beta(i)$. A similar argument shows that $\alpha\beta(i) = \beta\alpha(i)$ if α moves i. The last possibility is that neither α nor β moves i; in this case, $\alpha\beta(i) = i = \beta\alpha(i)$. Therefore, $\alpha\beta = \beta\alpha$, by Proposition 2.2. •

In particular, disjoint cycles commute.

It is possible for permutations that are not disjoint to commute; for example, the reader may check that (1 2 3)(4 5) and (1 3 2)(6 7) do commute. An even simpler example arises from a permutation commuting with its powers: $\alpha\alpha^2 = \alpha^2\alpha$.

Lemma 2.23. *Let $X = \{1, 2, \ldots, n\}$, let $\alpha \in S_X = S_n$, and, if $i_1 \in X$, define i_j for all $j \geq 1$ by induction: $i_{j+1} = \alpha(i_j)$. Write $Y = \{i_j : j \geq 1\}$, and let Y' be the complement of Y.*

(i) *If α moves i_1, then there is $r > 1$ with $i_1, \ldots, i_r$ all distinct and with $i_{r+1} = \alpha(i_r) = i_1$.*

(ii) *$\alpha(Y) = Y$ and $\alpha(Y') = Y'$.*

Proof.
(i) Since X is finite, there is a smallest $r > 1$ with $i_1, \ldots, i_r$ all distinct, but with $i_{r+1} = \alpha(i_r) \in \{i_1, \ldots, i_r\}$; that is, $\alpha(i_r) = i_j$ for $1 \leq j \leq r$. If $j > 1$, then $\alpha(i_r) = i_j = \alpha(i_{j-1})$. But α is an injection, so that $i_r = i_{j-1}$, contradicting $i_1, \ldots, i_r$ all being distinct. Therefore, $\alpha(i_r) = i_1$.
(ii) It is obvious that $\alpha(Y) \subseteq Y$, for if $i_j \in Y$, then $\alpha(i_j) = i_{j+1} \in Y$. If $k \in Y'$, then either $\alpha(k) \in Y$ or $\alpha(k) \in Y'$, for Y' is the complement of Y, and so $X = Y \cup Y'$. If $\alpha(k) \in Y$, then $\alpha(k) = i_j = \alpha(i_{j-1})$ for some j (by part (i), this is even true for $i_j = i_1$). Since α is injective, $k = i_{j-1} \in Y$, contradicting $Y \cap Y' = \varnothing$. Therefore, $\alpha(Y') \subseteq Y'$.

We now show that the inclusions $\alpha(Y) \subseteq Y$ and $\alpha(Y') \subseteq Y'$ are actually equalities. Now $\alpha(X) = \alpha(Y \cup Y') = \alpha(Y) \cup \alpha(Y')$, and this is a disjoint union because α is an injection. But $\alpha(Y) \subseteq Y$ gives $|\alpha(Y)| \leq |Y|$, and $\alpha(Y') \subseteq Y'$ gives $|\alpha(Y')| \leq |Y'|$. If either of these inequalities is strict, then $|\alpha(X)| < |X|$. But $\alpha(X) = X$, because α is a surjection, and this is a contradiction. •

The argument in the proof of Lemma 2.23(i) will be used again.

Proposition 2.24. *Every permutation $\alpha \in S_n$ is either a cycle or a product of disjoint cycles.*

Proof. The proof is by induction on the number $k \geq 0$ of points moved by α. The base step $k = 0$ is true, for α is now the identity, which is a 1-cycle.

If $k > 0$, let i_1 be a point moved by α. As in Lemma 2.23, define $Y = \{i_1, \ldots, i_r\}$, where $i_1, \ldots, i_r$ are all distinct, $\alpha(i_j) = i_{j+1}$ for $j < r$, and $\alpha(i_r) = i_1$. Let $\sigma \in S_X$ be the r-cycle $(i_1\ i_2\ i_3\ \ldots\ i_r)$, so that σ fixes each point, if any, in the complement Y' of Y. If $r = n$, then $\alpha = \sigma$. If $r < n$, then $\alpha(Y') = Y'$, as in the lemma. Define $\alpha' = \alpha\sigma^{-1}$; we claim that α' and σ are disjoint. If σ moves i, then $i = i_j \in Y$. But $\alpha'(i_j) = \alpha\sigma^{-1}(i_j) = \alpha(i_{j-1}) = i_j$; that is, α'

fixes i_j. Suppose that α' moves k. We have just seen that $k \notin Y$, so that we may assume that $k \in Y'$; but, by definition, σ fixes every $k \in Y'$. Therefore, $\alpha = \alpha'\sigma$ is a factorization into disjoint permutations. The number of points moved by α' is $k - r < k$, and so the inductive hypothesis gives $\alpha' = \beta_1 \cdots \beta_t$, where $\beta_1, \ldots, \beta_t$ are disjoint cycles. Therefore, $\alpha = \alpha'\sigma = \beta_1 \cdots \beta_t\sigma$ is a product of disjoint cycles, as desired. •

We have just proved that the output of the algorithm on page 106 is always a product of disjoint cycles.

Usually one suppresses the 1-cycles in this factorization [for 1-cycles equal the identity (1)]. However, a factorization of α containing one 1-cycle for each i fixed by α, if any, will arise several times in the sequel.

Definition. A ***complete factorization*** of a permutation α is a factorization of α into disjoint cycles that contains one 1-cycle (i) for every i fixed by α.

The factorization algorithm always yields a complete factorization. For example, if

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

then the algorithm gives $\alpha = (1)(2\ 3\ 4)(5)$, which is a complete factorization. However, if one suppresses 1-cycles, the factorizations

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

are not complete factorizations. In a complete factorization $\alpha = \beta_1 \cdots \beta_t$, every symbol i between 1 and n occurs in exactly one of the β's.

There is a relation between an r-cycle β and its ***powers*** β^k, where β^k denotes the composite of β with itself k times. We modify notation a bit for the next observation; write $\beta = (i_0\ i_1\ \ldots\ i_{r-1})$. Note that $i_1 = \beta(i_0)$, $i_2 = \beta(i_1) = \beta(\beta(i_0)) = \beta^2(i_0)$, $i_3 = \beta(i_2) = \beta(\beta^2(i_0)) = \beta^3(i_0)$, and, for all $k \leq r - 1$,

$$i_k = \beta^k(i_0). \tag{1}$$

Since $\beta(i_{r-1}) = i_0$, it is easy to see that the equation $i_k = \beta^k(i_0)$ holds if subscripts j in the notation i_j are taken mod r.

Lemma 2.25.

(i) *Let $\alpha = \beta\delta$ be a factorization into disjoint permutations. If β moves i, then $\alpha^k(i) = \beta^k(i)$ for all $k \geq 1$.*

(ii) *If β and γ are cycles both of which move $i = i_0$, and if $\beta^k(i) = \gamma^k(i)$ for all $k \geq 1$, then $\beta = \gamma$.*

Remark. The hypothesis in (ii) does not assume that the cycles β and γ have the same length, but this is part of the conclusion. ◀

Proof.
(i) Since β moves i, disjointness implies that δ fixes i; indeed, every power of δ fixes i. Now β and δ commute, by Lemma 2.22, and so Exercise 2.27(i) on page 121 gives $(\beta\delta)^k(i) = \beta^k(\delta^k(i)) = \beta^k(i)$, as desired.
(ii) By Eq. (1), if $\beta = (i_0\ i_1\ \ldots\ i_{r-1})$, then $i_k = \beta^k(i_0)$ for all $k < r-1$. Similarly, if $\gamma = (i_0\ j_1 \ldots j_{s-1})$, then $j_k = \gamma^k(i_0)$ for $k < s-1$. We may assume that $r \leq s$, so that $i_1 = j_1, \ldots, i_{r-1} = j_{r-1}$. Since $j_r = \gamma^r(i_0) = \beta^r(i_0) = i_0$, it follows that $s-1 = r-1$ and $j_k = i_k$ for all k. Therefore, $\beta = (i_0\ i_1\ \ldots\ i_{r-1}) = \gamma$. •

The next theorem is an analog of the fundamental theorem of arithmetic.

Theorem 2.26. *Let $\alpha \in S_n$ and let $\alpha = \beta_1 \cdots \beta_t$ be a complete factorization into disjoint cycles. This factorization is unique except for the order in which the cycles occur.*

Proof. Let $\alpha = \gamma_1 \cdots \gamma_s$ be a second complete factorization of α into disjoint cycles. Since every complete factorization of α has exactly one 1-cycle for each i fixed by α, it suffices to prove, by induction on ℓ, the larger of t and s, that the cycles of length > 1 are uniquely determined by α.

The base step is true, for when $\ell = 1$, the hypothesis is $\beta_1 = \alpha = \gamma_1$.

To prove the inductive step, note first that if β_t moves $i = i_0$, then $\beta_t^k(i_0) = \alpha^k(i_0)$ for all $k \geq 1$, by Lemma 2.25(i). Now some γ_j must move i_0; since disjoint cycles commute, we may re-index so that γ_s moves i_0. As in the first paragraph, $\gamma_s^k(i_0) = \alpha^k(i_0)$ for all k. It follows from Lemma 2.25(ii) that $\beta_t = \gamma_s$, and the cancellation law on page 104 gives $\beta_1 \cdots \beta_{t-1} = \gamma_1 \cdots \gamma_{s-1}$. By the inductive hypothesis, $s = t$ and the γ's can be reindexed so that $\gamma_1 = \beta_1, \ldots, \gamma_{t-1} = \beta_{t-1}$. •

Every permutation is a bijection; how do we find its inverse? In Figure 2.8, the pictorial representation of a cycle β as a clockwise rotation of a circle, the inverse β^{-1} is just a counterclockwise rotation.

Proposition 2.27.

(i) *The inverse of the cycle $\alpha = (i_1\ i_2\ \ldots\ i_r)$ is the cycle $(i_r\ i_{r-1} \ldots\ i_1)$:*

$$(i_1\ i_2\ \ldots\ i_r)^{-1} = (i_r\ i_{r-1} \ldots\ i_1).$$

(ii) *If $\gamma \in S_n$ and $\gamma = \beta_1 \cdots \beta_k$, then*

$$\gamma^{-1} = \beta_k^{-1} \cdots \beta_1^{-1}$$

(*note that the order of the factors in γ^{-1} has been reversed*).

Proof.
(i) If $\alpha \in S_n$, we show that both composites are equal to (1). Now the composite $(i_1\ i_2\ \dots\ i_r)(i_r\ i_{r-1}\dots\ i_1)$ fixes each integer between 1 and n, if any, other than $i_1, \dots, i_r$. The composite also sends $i_1 \mapsto i_r \mapsto i_1$ while it acts on i_j, for $j \geq 2$, by $i_j \mapsto i_{j-1} \mapsto i_j$. Thus, each integer between 1 and n is fixed by the composite, and so it is (1). A similar argument proves that the composite in the other order is also equal to (1), from which it follows that

$$(i_1\ i_2\ \dots\ i_r)^{-1} = (i_r\ i_{r-1}\dots\ i_1).$$

(ii) The proof is by induction on $k \geq 2$. For the base step $k = 2$, we have

$$(\beta_1\beta_2)(\beta_2^{-1}\beta_1^{-1}) = \beta_1(\beta_2\beta_2^{-1})\beta_1^{-1} = \beta_1\beta_1^{-1} = (1).$$

Similarly, $(\beta_2^{-1}\beta_1^{-1})(\beta_1\beta_2) = (1)$.

For the inductive step, let $\delta = \beta_1 \cdots \beta_k$, so that $\beta_1 \cdots \beta_k\beta_{k+1} = \delta\beta_{k+1}$. Then

$$\begin{aligned}(\beta_1 \cdots \beta_k\beta_{k+1})^{-1} &= (\delta\beta_{k+1})^{-1}\\ &= \beta_{k+1}^{-1}\delta^{-1}\\ &= \beta_{k+1}^{-1}(\beta_1 \cdots \beta_k)^{-1}\\ &= \beta_{k+1}^{-1}\beta_k^{-1} \cdots \beta_1^{-1}. \quad \bullet\end{aligned}$$

Thus, $(1\ 2\ 3\ 4)^{-1} = (4\ 3\ 2\ 1) = (1\ 4\ 3\ 2)$ and $(1\ 2)^{-1} = (2\ 1) = (1\ 2)$ (every transposition is equal to its own inverse).

Example 2.28.
The result in Proposition 2.27 holds, in particular, if the factors are disjoint cycles (in which case the reversal of the order of the factors is unnecessary because they commute with one another, by Lemma 2.22). Thus, if

$$\alpha = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3\end{pmatrix},$$

then $\alpha = (1\ 6)(2\ 4)(3\ 7\ 8\ 9)(5)$ and

$$\begin{aligned}\alpha^{-1} &= (5)(9\ 8\ 7\ 3)(4\ 2)(6\ 1)\\ &= (1\ 6)(2\ 4)(3\ 9\ 8\ 7). \quad \blacktriangleleft\end{aligned}$$

Definition. Two permutations $\alpha, \beta \in S_n$ have the ***same cycle structure*** if their complete factorizations have the same number of r-cycles for each $r \geq 1$.

According to Exercise 2.21 on page 120, there are

$$(1/r)[n(n-1)\cdots(n-r+1)]$$

r-cycles in S_n. This formula can be used to count the number of permutations having any given cycle structure if one is careful about factorizations having several cycles of the same length. For example, the number of permutations in S_4 with cycle structure $(a\ b)(c\ d)$ is

$$\tfrac{1}{2}\left[\tfrac{1}{2}(4\times 3)\right]\times[\tfrac{1}{2}(2\times 1)]=3,$$

the extra factor $\frac{1}{2}$ occurring so that we do not count $(a\ b)(c\ d)=(c\ d)(a\ b)$ twice. Similarly, the number of permutations in S_n of the form $(a\ b)(c\ d)(e\ f)$ is

$$\frac{1}{3!2^3}[n(n-1)(n-2)(n-3)(n-4)(n-5)]$$

(see Exercise 2.21 on page 120).

Example 2.29.

Cycle Structure	Number
(1)	1
(1 2)	6
(1 2 3)	8
(1 2 3 4)	6
(1 2)(3 4)	3
	24

Table 2.1. Permutations in S_4 ◀

Example 2.30.

Cycle Structure	Number
(1)	1
(1 2)	10
(1 2 3)	20
(1 2 3 4)	30
(1 2 3 4 5)	24
(1 2)(3 4 5)	20
(1 2)(3 4)	15
	120

Table 2.2. Permutations in S_5 ◀

After a lemma, we present a computational aid.

Lemma 2.31. *Let $\alpha, \gamma \in S_n$. For all i, if $\gamma: i \to j$, then $\alpha\gamma\alpha^{-1}: \alpha(i) \to \alpha(j)$.*

Proof.
$$\alpha\gamma\alpha^{-1}(\alpha(i)) = \alpha\gamma(i) = \alpha(j). \quad \bullet$$

Proposition 2.32. *If $\gamma, \alpha \in S_n$, then $\alpha\gamma\alpha^{-1}$ has the same cycle structure as γ. In more detail, if the complete factorization of γ is*

$$\gamma = \beta_1\beta_2 \cdots (i\ j\ \ldots) \cdots \beta_t,$$

then $\alpha\gamma\alpha^{-1}$ is the permutation σ which is obtained from γ by applying α to the symbols in the cycles of γ.

Remark. For example, if $\gamma = (1\ 3)(2\ 4\ 7)(5)(6)$ and $\alpha = (2\ 5\ 6)(1\ 4\ 3)$, then

$$\alpha\gamma\alpha^{-1} = (\alpha 1\ \alpha 3)(\alpha 2\ \alpha 4\ \alpha 7)(\alpha 5)(\alpha 6) = (4\ 1)(5\ 3\ 7)(6)(2). \quad \blacktriangleleft$$

Proof. If γ fixes i, then Lemma 2.31 shows that σ fixes $\alpha(i)$. Assume that γ moves a symbol i, say, $\gamma(i) = j$, so that one of the cycles in the complete factorization of γ is

$$(i\ j\ \ldots).$$

By the definition of σ, one of its cycles is

$$(\alpha(i)\ \alpha(j)\ \ldots);$$

that is, $\sigma: \alpha(i) \mapsto \alpha(j)$. But Lemma 2.31 says that $\alpha\gamma\alpha^{-1}: \alpha(i) \mapsto \alpha(j)$, so that σ and $\alpha\gamma\alpha^{-1}$ agree on all numbers of the form $\alpha(i)$. But every $k \in X$ has the form $k = \alpha(i)$, because $\alpha: X \to X$ is a surjection, and so $\sigma = \alpha\gamma\alpha^{-1}$. $\bullet$

Proposition 2.33. *If $\gamma, \gamma' \in S_n$, then γ and γ' have the same cycle structure if and only only if there exists $\alpha \in S_n$ with $\gamma' = \alpha\gamma\alpha^{-1}$.*

Proof. Sufficiency has just been proved, in Proposition 2.32.

Conversely, assume that γ and γ' have the same cycle structure; that is, $\gamma = \beta_1 \cdots \beta_t$ and $\gamma' = \sigma_1 \cdots \sigma_t$ are complete factorizations with β_λ and σ_λ having the same length for all $\lambda \le t$. Let $\beta_\lambda = (i_1^\lambda, \ldots, i_{r(\lambda)}^\lambda)$ and $\sigma_\lambda = (j_1^\lambda, \ldots, j_{r(\lambda)}^\lambda)$. Define

$$\alpha(i_1^\lambda) = j_1^\lambda, \quad \alpha(i_2^\lambda) = j_2^\lambda, \quad \ldots, \quad \alpha(i_{r(\lambda)}^\lambda) = j_{r(\lambda)}^\lambda,$$

for all λ. Since $\beta_1 \cdots \beta_t$ is a complete factorization, every $i \in X = \{1, \ldots, n\}$ occurs in exactly one β_λ; hence, $\alpha(i)$ is defined for every $i \in X$, and $\alpha: X \to X$

is a (single-valued) function. Since every $j \in X$ occurs in some σ_λ, because $\sigma_1 \cdots \sigma_t$ is a complete factorization, it follows that α is surjective. By Exercise 2.12 on page 102, α is a bijection, and so $\alpha \in S_n$. Proposition 2.32 says that $\alpha\gamma\alpha^{-1}$ has the same cycle structure as γ and the λth cycle, for each λ, is

$$\big(\alpha(i_1^\lambda)\ \ \alpha(i_2^\lambda)\ \ \ldots\ \alpha(i_{r(\lambda)}^\lambda)\big) = \sigma_\lambda.$$

Therefore, $\alpha\gamma\alpha^{-1} = \gamma'$. •

Example 2.34.
If

$$\gamma = (1\ 2\ 3)(4\ 5)(6) \quad \text{and} \quad \gamma' = (2\ 5\ 6)(3\ 1)(4),$$

then $\gamma' = \alpha\gamma\alpha^{-1}$, where

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 3 & 1 & 4 \end{pmatrix} = (1\ 2\ 5)(3\ 6\ 4).$$

Note that there are other choices for α as well. ◀

Here is another useful factorization of a permutation.

Proposition 2.35. *If $n \geq 2$, then every $\alpha \in S_n$ is a product of transpositions.*

Proof. Of course, $(1) = (1\ 2)(1\ 2)$ is a product of transpositions, as is every transposition: $(i\ j) = (i\ j)(1\ 2)(1\ 2)$. By Proposition 2.24, it suffices to factor an r-cycle β into a product of transpositions. This is done as follows. If $r = 1$, then β is the identity, and $\beta = (1\ 2)(1\ 2)$. If $r \geq 2$, then

$$\beta = (1\ 2\ \ldots\ r) = (1\ r)(1\ r-1)\cdots(1\ 3)(1\ 2).$$

[One checks that this is an equality by evaluating each side. For example, the left side β sends $1 \mapsto 2$; each of $(1\ r), (1\ r-1), \ldots, (1\ 3)$ fixes 2, and so the right side also sends $1 \mapsto 2$.] •

Every permutation can thus be realized as a sequence of interchanges. Such a factorization is not as nice as the factorization into disjoint cycles. First of all, the transpositions occurring need not commute: $(1\ 2\ 3) = (1\ 3)(1\ 2) \neq (1\ 2)(1\ 3)$; second, neither the factors themselves nor the number of factors are uniquely determined. For example, here are some factorizations of $(1\ 2\ 3)$ in S_4:

$$\begin{aligned}(1\ 2\ 3) &= (1\ 3)(1\ 2)\\ &= (2\ 3)(1\ 3)\\ &= (1\ 3)(4\ 2)(1\ 2)(1\ 4)\\ &= (1\ 3)(4\ 2)(1\ 2)(1\ 4)(2\ 3)(2\ 3).\end{aligned}$$

Is there any uniqueness at all in such a factorization? We now prove that the *parity* of the number of factors is the same for all factorizations of a permutation α; that is, the number of transpositions is always even or always odd [as is suggested by the factorizations of $\alpha = (1\ 2\ 3)$ displayed above].

Example 2.36.
The ***15-puzzle*** consists of a ***starting position***, which is a 4×4 array of the numbers between 1 and 15 and a symbol # (which we interpret as "blank"), and *simple moves*. For example, consider the starting position shown below.

3	15	4	12
10	11	1	8
2	5	13	9
6	7	14	#

A ***simple move*** interchanges the blank with a symbol adjacent to it; for example, there are two beginning simple moves for this starting position: either interchange # and 14 or interchange # and 9. One wins the game if, after a sequence of simple moves, the starting position is transformed into the standard array 1, 2, 3, . . ., 15, #.

To analyze this game, note that the given array is really a permutation α of $\{1, 2, \ldots, 15, \#\}$; that is, $\alpha \in S_{16}$. More precisely, if the spaces are labeled 1 through 15, #, then $\alpha(i)$ is the symbol occupying the ith square. For example, the starting position given above is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & \# \\ 3 & 15 & 4 & 12 & 10 & 11 & 1 & 8 & 2 & 5 & 13 & 9 & 6 & 7 & 14 & \# \end{pmatrix}.$$

Each simple move is a special kind of transposition, namely, one that moves #. Moreover, performing a simple move (corresponding to a special transposition τ) from a position (corresponding to a permutation β) yields a new position corresponding to the permutation $\tau\beta$. For example, if α is the position above and τ is the transposition interchanging 14 and #, then $\tau\alpha(\#) = \tau(\#) = 14$ and $\tau\alpha(15) = \tau(14) = \#$, while $\tau\alpha(i) = i$ for all other i. That is, the new configuration has all the numbers in their original positions except for 14 and # being interchanged. Therefore, to win the game, one needs special transpositions $\tau_1, \tau_2, \ldots, \tau_m$ so that

$$\tau_m \cdots \tau_2 \tau_1 \alpha = (1).$$

It turns out that there are some choices of α for which the game can be won, but there are others for which it cannot be won, as we shall see in Example 2.42. ◀

The following discussion will enable us to analyze the 15-game.

Lemma 2.37. *If $k, \ell \geq 0$ and the letters a, b, c_i, d_j are all distinct, then*

$$(a\ b)(a\ c_1\ \ldots\ c_k\ b\ d_1\ \ldots\ d_\ell) = (a\ c_1\ \ldots\ c_k)(b\ d_1\ \ldots\ d_\ell)$$

and

$$(a\ b)(a\ c_1\ \ldots\ c_k)(b\ d_1\ \ldots\ d_\ell) = (a\ c_1\ \ldots\ c_k\ b\ d_1\ \ldots\ d_\ell).$$

Proof. The left side of the first asserted equation sends

$$\begin{aligned}
a &\mapsto c_1 \mapsto c_1;\\
c_i &\mapsto c_{i+1} \mapsto c_{i+1} \text{ if } i < k;\\
c_k &\mapsto b \mapsto a;\\
b &\mapsto d_1 \mapsto d_1;\\
d_j &\mapsto d_{j+1} \mapsto d_{j+1} \text{ if } j < \ell;\\
d_\ell &\mapsto a \mapsto b.
\end{aligned}$$

Similar evaluation of the right side shows that both permutations agree on a, b, and all c_i, d_j. Since each side fixes all other numbers in $\{1, 2, \ldots, n\}$, if any, both sides are equal.

For the second equation, reverse the first equation,

$$(a\ c_1\ \ldots\ c_k)(b\ d_1\ \ldots\ d_\ell) = (a\ b)(a\ c_1\ \ldots\ c_k\ b\ d_1\ \ldots\ d_\ell),$$

and multiply both sides on the left by $(a\ b)$:

$$\begin{aligned}
(a\ b)(a\ c_1\ \ldots\ c_k)(b\ d_1\ \ldots\ d_\ell) &= (a\ b)(a\ b))(a\ c_1\ \ldots\ c_k\ b\ d_1\ \ldots\ d_\ell)\\
&= (a\ c_1\ \ldots\ c_k\ b\ d_1\ \ldots\ d_\ell). \quad \bullet
\end{aligned}$$

An illustration of the lemma is

$$(1\ 2)(1\ 3\ 4\ 2\ 5\ 6\ 7) = (1\ 3\ 4)(2\ 5\ 6\ 7).$$

Definition. If $\alpha \in S_n$ and $\alpha = \beta_1 \cdots \beta_t$ is a complete factorization into disjoint cycles, then ***signum***[4] α is defined by

$$\operatorname{sgn}(\alpha) = (-1)^{n-t}.$$

Theorem 2.26 shows that sgn is a (single-valued) function, for the number t is uniquely determined by α. If ε is a 1-cycle, then $\operatorname{sgn}(\varepsilon) = 1$, for $t = n$ and $(-1)^0 = 1$. If τ is a transposition, then it moves two numbers, and it fixes each of the $n - 2$ other numbers; therefore, $t = 1 + (n - 2) = n - 1$, and so $\operatorname{sgn}(\tau) = (-1)^{n-(n-1)} = -1$.

[4] *Signum* is the Latin word for "mark" or "token"; of course, it has become the word *sign*.

Lemma 2.38. *If $\alpha, \tau \in S_n$, where τ is a transposition, then*

$$\operatorname{sgn}(\tau\alpha) = -\operatorname{sgn}(\alpha).$$

Proof. Let $\alpha = \beta_1 \cdots \beta_t$ be a complete factorization of α into disjoint cycles, and let $\tau = (a\ b)$. If a and b occur in the same β, say, in β_1, then $\beta_1 = (a\ c_1 \dots c_k\ b\ d_1 \dots d_\ell)$, where $k, \ell \geq 0$. By Lemma 2.37,

$$\tau\beta_1 = (a\ c_1 \dots c_k)(b\ d_1 \dots d_\ell).$$

This is a complete factorization of $\tau\alpha = (\tau\beta_1)\beta_2 \cdots \beta_t$, for the cycles in it are pairwise disjoint and every number in $\{1, 2, \dots, n\}$ occurs in exactly one cycle. Thus, $\tau\beta$ has $t + 1$ cycles, for $\tau\beta_1$ splits into two disjoint cycles. Therefore, $\operatorname{sgn}(\tau\alpha) = (-1)^{n-(t+1)} = -\operatorname{sgn}(\alpha)$.

The other possibility is that a and b occur in different cycles, say, $\beta_1 = (a\ c_1 \dots c_k)$ and $\beta_2 = (b\ d_1 \dots d_\ell)$, where $k, \ell \geq 0$. But $\tau\alpha = (\tau\beta_1\beta_2)\beta_3 \cdots \beta_t$, and Lemma 2.37 gives

$$\tau\beta_1\beta_2 = (a\ c_1 \dots c_k\ b\ d_1 \dots d_\ell).$$

Therefore $\tau\alpha$ has a complete factorization with $t - 1$ cycles, and so $\operatorname{sgn}(\tau\alpha) = (-1)^{n-(t-1)} = -\operatorname{sgn}(\alpha)$, as desired. •

Theorem 2.39. *For all $\alpha, \beta \in S_n$,*

$$\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta).$$

Proof. Assume that $\alpha \in S_n$ is given and that α has a factorization as a product of m transpositions: $\alpha = \tau_1 \cdots \tau_m$. We prove, by induction on m, that $\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)$ for every $\beta \in S_n$. The base step $m = 1$ is precisely Lemma 2.38, for $m = 1$ says that α is a transposition. If $m > 1$, then the inductive hypothesis applies to $\tau_2 \cdots \tau_m$, and so

$$\begin{aligned}
\operatorname{sgn}(\alpha\beta) &= \operatorname{sgn}(\tau_1 \cdots \tau_m\beta) \\
&= -\operatorname{sgn}(\tau_2 \cdots \tau_m\beta) && \text{(Lemma 2.38)} \\
&= -\operatorname{sgn}(\tau_2 \cdots \tau_m)\operatorname{sgn}(\beta) && \text{(by induction)} \\
&= \operatorname{sgn}(\tau_1 \cdots \tau_m)\operatorname{sgn}(\beta) && \text{(Lemma 2.38)} \\
&= \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta). \quad \bullet
\end{aligned}$$

It follows by induction on $k \geq 2$ that

$$\operatorname{sgn}(\alpha_1\alpha_2 \cdots \alpha_k) = \operatorname{sgn}(\alpha_1)\operatorname{sgn}(\alpha_2) \cdots \operatorname{sgn}(\alpha_k).$$

Definition. A permutation $\alpha \in S_n$ is ***even*** if $\text{sgn}(\alpha) = 1$, and α is ***odd*** if $\text{sgn}(\alpha) = -1$. We say that α and β have the ***same parity*** if both are even or both are odd.

Let us return to factorizations of a permutation into a product of transpositions. We saw on page 116 that there are many such factorizations of a permutation, and the only common feature of these different factorizations appeared to be the parity of the number of factors. To prove this apparent statement, one must show that a permutation cannot be a product of an even number of transpositions as well as a product of an odd number of transpositions.

Theorem 2.40.

(i) *Let $\alpha \in S_n$. If α is even, then α is a product of an even number of transpositions, and if α is odd, then α is a product of an odd number of transpositions.*

(ii) *If $\alpha = \tau_1 \cdots \tau_q = \tau'_1 \cdots \tau'_p$ are factorizations into transpositions, then q and p have the same parity.*

Proof.
(i) If $\alpha = \tau_1 \cdots \tau_q$ is a factorization of α into transpositions, then Theorem 2.39 gives $\text{sgn}(\alpha) = \text{sgn}(\tau_1) \cdots \text{sgn}(\tau_q) = (-1)^q$, for we know that every transposition is odd. Therefore, if α is even; that is, if $\text{sgn}(\alpha) = 1$, then q is even, while if α is odd; that is, if $\text{sgn}(\alpha) = -1$, then q is odd.
(ii) If there were two factorizations of α, one into an odd number of transpositions and the other into an even number of transpositions, then $\text{sgn}(\alpha)$ would have two different values. •

Corollary 2.41. *Let $\alpha, \beta \in S_n$. If α and β have the same parity, then $\alpha\beta$ is even, while if α and β have distinct parity, then $\alpha\beta$ is odd.*

Proof. If $\text{sgn}(\alpha) = (-1)^q$ and $\text{sgn}(\beta) = (-1)^p$, then Theorem 2.39 gives $\text{sgn}(\alpha\beta) = (-1)^{q+p}$, and the result follows. •

We return to the 15-game.

Example 2.42.
An analysis of the 15-puzzle in Example 2.36 shows that if $\alpha \in S_{16}$ is the starting position, then the game can be won if and only if α is an even permutation that fixes #. For a proof of this, we refer the reader to McCoy and Janusz, *Introduction to Modern Algebra*. The proof in one direction is fairly clear, however. The blank # starts in position 16. Each simple move takes # up, down, left, or right. Thus, the total number m of moves is $u+d+l+r$, where u is the number of up moves,

etc. If # is to return home, each one of these must be undone: there must be the same number of up moves as down moves, i.e., $u = d$, and the same number of left moves as right moves, i.e., $r = l$. Thus, the total number of moves is even: $m = 2u + 2r$. That is, if $\tau_m \cdots \tau_1 \alpha = (1)$, then m is even; hence, $\alpha = \tau_1 \cdots \tau_m$ (because $\tau^{-1} = \tau$ for every transposition τ), and so α is an even permutation. Armed with this theorem, one sees that the starting position α in Example 2.36 is, in cycle notation,

$$\alpha = (1\ 3\ 4\ 12\ 9\ 2\ 15\ 14\ 7)(5\ 10)(6\ 11\ 13)(8)(\#),$$

where (8) and (#) are 1-cycles. Now $\operatorname{sgn}(\alpha) = (-1)^{16-5} = -1$, so that α is an odd permutation; therefore, the game starting with α cannot be won. ◀

EXERCISES

***2.19** Find $\operatorname{sgn}(\alpha)$ and α^{-1}, where

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

2.20 If $\sigma \in S_n$ fixes some j, where $1 \leq j \leq n$ (that is, $\sigma(j) = j$), define $\sigma' \in S_X \cong S_{n-1}$ (where $X = \{1, \ldots, \widehat{j}, \ldots, n\}$) by $\sigma'(i) = \sigma(i)$ for all $i \neq j$. Prove that

$$\operatorname{sgn}(\sigma') = \operatorname{sgn}(\sigma).$$

***2.21** **(i)** If $1 < r \leq n$, prove that there are

$$\tfrac{1}{r}[n(n-1)\cdots(n-r+1)]$$

r-cycles in S_n.

(ii) If $kr \leq n$, where $1 < r \leq n$, prove that the number of $\alpha \in S_n$, where α is a product of k disjoint r-cycles, is

$$\tfrac{1}{k!}\tfrac{1}{r^k}[n(n-1)\cdots(n-kr+1).]$$

***2.22** **(i)** If α is an r-cycle, show that $\alpha^r = (1)$.

(ii) If α is an r-cycle, show that r is the smallest positive integer k such that $\alpha^k = (1)$.

2.23 Show that an r-cycle is an even permutation if and only if r is odd.

2.24 Given $X = \{1, 2, \ldots, n\}$, let us call a permutation τ of X an ***adjacency*** if it is a transposition of the form $(i\ i+1)$ for $i < n$. If $i < j$, prove that $(i\ j)$ is a product of an odd number of adjacencies.

***2.25** Define $f : \{0, 1, 2, \ldots, 10\} \to \{0, 1, 2, \ldots, 10\}$ by

$$f(n) = \text{the remainder after dividing } 4n^2 - 3n^7 \text{ by } 11.$$

(i) Show that f is a permutation.

(ii) Compute the parity of f.

(iii) Compute the inverse of f.

2.26 **(i)** A permutation $\alpha \in S_n$ is ***regular*** if either α has no fixed points and it is the product of disjoint cycles of the same length, or $\alpha = (1)$. Prove that α is regular if and only if α is a power of an n-cycle.

(ii) Prove that if α is an r-cycle, then α^k is a product of (r, k) disjoint cycles, each of length $r/(r, k)$.

(iii) If p is a prime, prove that every power of a p-cycle is either a p-cycle or (1).

(iv) How many regular permutations are there in S_5? How many regular permutations are there in S_8?

***2.27** **(i)** Prove that if α and β are (not necessarily disjoint) permutations that commute, then $(\alpha\beta)^k = \alpha^k\beta^k$ for all $k \geq 1$.

(ii) Give an example of two permutations α and β for which $(\alpha\beta)^2 \neq \alpha^2\beta^2$.

***2.28** **(i)** Prove, for all i, that $\alpha \in S_n$ moves i if and only if α^{-1} moves i.

(ii) Prove that if $\alpha, \beta \in S_n$ are disjoint and if $\alpha\beta = (1)$, then $\alpha = (1)$ and $\beta = (1)$.

***2.29** If $n \geq 2$, prove that the number of even permutations in S_n is $\frac{1}{2}n!$.

2.30 Give an example of $\alpha, \beta, \gamma \in S_5$, none of which is the identity (1), with $\alpha\beta = \beta\alpha$ and $\alpha\gamma = \gamma\alpha$, but with $\beta\gamma \neq \gamma\beta$.

***2.31** If $n \geq 3$, show that if $\alpha \in S_n$ commutes with every $\beta \in S_n$, then $\alpha = (1)$.

2.3 GROUPS

Generalizations of the quadratic formula for finding the roots of cubic and quartic polynomials were discovered in the early 1500s. Over the next three centuries, many tried to find analogous formulas for the roots of higher-degree polynomials, but in 1824, N. H. Abel (1802–1829) proved that there is no such formula giving the roots of the general polynomial of degree 5. In 1831, E. Galois (1811–1832) completely solved this problem by finding precisely which polynomials, of arbitrary degree, admit such a formula for their roots. His fundamental idea involved his invention of the idea of *group*. Since Galois's time, groups have arisen in many other areas of mathematics, for they are also the way to describe the notion of symmetry, as we will see later in this section and also in Chapter 6.

The essence of a "product" is that two things are combined to form a third thing of the same kind. For example, ordinary multiplication, addition, and subtraction combine two numbers to give another number, while composition combines two permutations to give another permutation.

Definition. A (binary) ***operation*** on a set G is a function

$$*\colon G \times G \to G.$$