II.B. Permutation groups

Let X be a set; recall that (if finite) its order $|X|$ is the number of elements. A *transformation* of X is a map

$$\tau\colon X \to X\,;$$

if τ is bijective (or equivalently, invertible), it is called a **permutation**. Let

$$\begin{aligned} \mathfrak{T}_X &:= \text{ set of all transformations of } X, \\ \text{and}\quad \mathfrak{S}_X &:= \text{ set of all permutations of } X. \end{aligned}$$

The binary operation "composition of maps" makes $\mathfrak{T}_X$ into a monoid and $\mathfrak{S}_X$ into a group, the **symmetric group** on X.

II.B.1. PROPOSITION. *If $|X| = n < \infty$, we have $|\mathfrak{T}_X| = n^n$ and $|\mathfrak{S}_X| = n!$.*

PROOF. For each $x \in X$, there are n choices for $\tau(x)$; but if τ is to be bijective, each choice removes an option for the next. $\square$

Say $X = \{x_1, \ldots, x_n\}$. A useful notation is $\tau = \begin{pmatrix} x_1 & \cdots & x_n \\ \tau(x_1) & \cdots & \tau(x_n) \end{pmatrix}$.

II.B.2. EXAMPLE. Let $X = \{A, B\}$. We have

$$\begin{aligned} \mathfrak{T}_X &= \left\{ \begin{pmatrix} A & B \\ A & B \end{pmatrix}, \begin{pmatrix} A & B \\ B & A \end{pmatrix}, \begin{pmatrix} A & B \\ A & A \end{pmatrix}, \begin{pmatrix} A & B \\ B & B \end{pmatrix} \right\} \\ \text{and}\quad \mathfrak{S}_X &= \left\{ \begin{pmatrix} A & B \\ A & B \end{pmatrix}, \begin{pmatrix} A & B \\ B & A \end{pmatrix} \right\}, \end{aligned}$$

where the identity transformation is written first in each set. To remove reference to X and think of $\mathfrak{T}_X$ as an "abstract monoid", write $\{1, \alpha, \beta, \gamma\}$ for its 4 elements (in the same order) and produce a table

	1	α	$\boxed{\beta}$	γ
1	1	α	β	γ
$\boxed{\alpha}$	α	1	$\boxed{\gamma}$	β
β	β	β	β	β
γ	γ	γ	γ	γ

which displays the abstract binary operation corresponding to the compositions of these transformations. For instance, $\alpha\beta = \gamma$ (shown in the table) means, on the level of the transformations, that β followed by α gives γ.

You can make such a table for any (finite order) group or monoid; but conversely, given an arbitrary table of the form

	1	α	β	γ
1	1	α	β	γ
α	α			
β	β		?	
γ	γ			

it need not yield a monoid: associativity *does* impose constraints.

Define the $\mathbf{n^{th}}$ **symmetric group** by

$$\mathfrak{S}_n := \mathfrak{S}_{\{1,\ldots,n\}}.$$

II.B.3. PROPOSITION. *Any $\alpha \in \mathfrak{S}_n$ has, up to order, a unique complete*[3] *factorization into* ***disjoint cycles*** (*which commute*).

II.B.4. EXAMPLE. In $\mathfrak{S}_9$, an example of a *cycle* is (3789), which sends $3 \mapsto 7 \mapsto 8 \mapsto 9 \mapsto 3$. (It is a 4-cycle because it involves 4 elements.) This is *disjoint* from (24) because the subsets of $\{1, 2, \ldots, 9\}$

[3] Here, "complete" means that we formally include the 1-cycles (k) that do nothing, except to say that α sends k to itself, so that each element of $\{1, \ldots, n\}$ appears exactly once in the product of cycles. (A 1-cycle is really just a way of writing the identity element.)

involved are disjoint (which makes them commute). An example of a (complete) factorization of a permutation into disjoint cycles is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 \end{pmatrix} = (16)(24)(3789)(5).$$

PROOF OF II.B.3. The idea is to induce on the number of elements in $\{1, 2, \ldots, n\}$ that α moves. Say it moves the element i_1, viz.

$$i_1 \underset{\alpha}{\mapsto} i_2 \underset{\alpha}{\mapsto} i_3 \underset{\alpha}{\mapsto} \cdots \underset{\alpha}{\mapsto} i_r,$$

where r is the smallest integer for which $i_r \in \{i_1, \ldots, i_{r-1}\}$. (Clearly $2 \leq r \leq n+1$.)

In fact, we must have $i_r = i_1$. (Otherwise, for some $2 \leq j \leq r-1$ we have $\alpha(i_{r-1}) = i_j = \alpha(i_{j-1})$, and α is not injective, a contradiction.) Hence α moves $i_1, \ldots, i_{r-1}$ in a cycle, and $\beta := \alpha \cdot (i_1 \cdots i_{r-1})^{-1}$ (which fixes each of them) moves $r-1$ fewer elements than α. We may view β as a permutation of[4] $\{1, \ldots, n\} \setminus \{i_1, \ldots, i_{r-1}\}$ and apply induction to get a complete factorization into cycles. Throwing in $(i_1 \cdots i_{r-1})$ then gives the desired factorization of α.

To see the uniqueness, let $\gamma_1 \cdots \gamma_s = \alpha = \beta_1 \cdots \beta_t$ be two complete factorizations. Since disjoint cycles commute, we may without loss of generality assume that β_1 and γ_1 contain i_1 (and that no other cycles in the two products do). Applying α repeatedly, we get

$$\begin{cases} \gamma_1(i_1) & = & i_2 & = & \beta_1(i_1) \\ & & \vdots & & \\ \gamma_1(i_r) & = & i_1 & = & \beta_1(i_{r-1}) \end{cases}$$

and so $\beta_1 = \gamma_1$. Cancel them and proceed inductively. $\square$

A **transposition** is a 2-cycle (ij); it sends $i \mapsto j \mapsto i$ and fixes all other elements.

II.B.5. PROPOSITION. *Any $\alpha \in \mathfrak{S}_n$ factors (nonuniquely) into a product of (not necessarily disjoint) transpositions.*

[4]Given sets $T \subset S$, $S \setminus T$ denotes the set-theoretic complement (the elements of S that aren't in T). You can view this β as an element of $\mathfrak{S}_{n-r+1}$, or (as we do here) an element of $\mathfrak{S}_n$ that fixes $i_1, \ldots, i_{r-1}$.

PROOF. Factor α into disjoint cycles, then (for example) factor the cycles via the formula $(123\cdots r) = (1r)(1\,r{-}1)\cdots(13)(12)$. $\square$

For each permutation $\alpha \in \mathfrak{S}_n$, write $c(\alpha)$ for the number of disjoint cycles in its complete factorization,[5] and define the **sign**

$$\mathrm{sgn}(\alpha) := (-1)^{n-c(\alpha)}.$$

Viewing $\{1, -1\}$ as a group under multiplication, we have the

II.B.6. THEOREM. *The map* $\mathrm{sgn}\colon \mathfrak{S}_n \to \{1,-1\}$ *is a homomorphism of groups. That is,* $\mathrm{sgn}(\alpha\beta) = \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta)$.

PROOF. First observe that there are $n-1$ cycles in the complete factorization of a transposition τ; e.g., $(12) = (12)(3)(4)\cdots(n)$. So $\mathrm{sgn}(\tau) = -1$.

Writing $\beta = \sigma_1 \cdots \sigma_{c(\beta)}$ for a complete factorization, consider $(ab)\beta$. Without loss of generality, *either* (i) a, b occur in σ_1 or (ii) a occurs in σ_1 and β in σ_2. Using

$$(ab)\underbrace{(ac_1\cdots c_k bd_1\cdots d_\ell)}_{\sigma_1}\sigma_2\cdots\sigma_{c(\beta)} = (ac_1\cdots c_k)(bd_1\cdots d_\ell)\sigma_2\cdots\sigma_{c(\beta)}$$

in case (i) and

$$(ab)\underbrace{(ac_1\cdots c_k)}_{\sigma_1}\underbrace{(bd_1\cdots d_\ell)}_{\sigma_2}\sigma_3\cdots\sigma_{c(\beta)} = (ac_1\cdots c_k bd_1\cdots d_\ell)\sigma_3\cdots\sigma_{c(\beta)}$$

in case (ii), we either gain or lose a cycle in the complete factorization of $(ab)\beta$. So for any transposition τ, we have $\mathrm{sgn}(\tau\beta) = -\mathrm{sgn}(\beta)$.

Finally, writing $\alpha = \tau_1\cdots\tau_m$ by II.B.5, we have

$$\begin{aligned}\mathrm{sgn}(\alpha\beta) &= \mathrm{sgn}(\tau_1\cdot\tau_2\cdots\tau_m\beta) = \\ &\quad -\mathrm{sgn}(\tau_2\cdots\tau_m\beta) = \cdots = (-1)^m\mathrm{sgn}(\beta), \quad \text{and}\end{aligned}$$

$$\begin{aligned}\mathrm{sgn}(\alpha)\mathrm{sgn}(\beta) &= \mathrm{sgn}(\tau_1\cdot\tau_2\cdots\tau_m)\mathrm{sgn}(\beta) = \\ &\quad -\mathrm{sgn}(\tau_2\cdots\tau_m)\mathrm{sgn}(\beta) = \cdots = (-1)^m\mathrm{sgn}(\beta),\end{aligned}$$

which completes the proof. $\square$

[5] It is essential to include the 1-cycles in this count!

II.B.7. COROLLARY. *The "number of transpositions" in* $\alpha \in \mathfrak{S}_n$ *is well-defined mod* 2.

PROOF. $\mathrm{sgn}(\alpha) = \mathrm{sgn}(\tau_1 \cdots \tau_m) = (-1)^m$, and we know $\mathrm{sgn}(\alpha)$ is well-defined. So m is well-defined mod 2. $\square$

The upshot is that we can unambiguously call α "even" or "odd" according to whether it can be written as a product of an even or odd number of transpositions. (To see which is the case, one instead writes the complete factorization into disjoint cycles and computes $\mathrm{sgn}(\alpha)$.)