8.9 Table

D_3	ι	ρ	ρ^2	μ	$\mu\rho$	$\mu\rho^2$
ι	ι	ρ	ρ^2	μ	$\mu\rho$	$\mu\rho^2$
ρ	ρ	ρ^2	ι	$\mu\rho^2$	μ	$\mu\rho$
ρ^2	ρ^2	ι	ρ	$\mu\rho$	$\mu\rho^2$	μ
μ	μ	$\mu\rho$	$\mu\rho^2$	ι	ρ	ρ^2
$\mu\rho$	$\mu\rho$	$\mu\rho^2$	μ	ρ^2	ι	ρ
$\mu\rho^2$	$\mu\rho^2$	μ	$\mu\rho$	ρ	ρ^2	ι

All that remains to prove Cayley's Theorem, at least when the group is finite, is to check that the permutations obtained from the group table form a group isomorphism with the original group. Let λ_x be the permutation of the elements of G given by the x row of the table for G. Then for any $g \in G$, $\lambda_x(g)$ is the entry in the x row and g column of the group table. In other words, $\lambda_x(g) = xg$, which is perfectly valid in the case of an infinite as well as a finite group. We formalize this connection between G and permutations on G in Definition 8.10.

8.10 Definition Let G be a group. The function $\phi : G \to S_G$ given by $\phi(x) = \lambda_x$ where $\lambda_x(g) = xg$ for all $g \in G$ is called the **left regular representation** of G. ■

In order to be sure that λ_x is a permutation, it should be verified that λ_x is both one-to-one and onto. We see that λ_x is one-to-one since if $\lambda_x(a) = \lambda_x(b)$, $xa = xb$ and cancellation gives $a = b$. Also, λ_x maps onto G because for any $b \in G$, $\lambda_x(x^{-1}b)) = b$. We are now ready to prove Cayley's Theorem.

8.11 Theorem **(Cayley's Theorem)** Every group is isomorphic to a group of permutations.

Proof Let G be a group. The left regular representation provides a map $\phi : G \to S_G$ defined by $\phi(x) = \lambda_x$. We must verify that ϕ is a group homomorphism and that ϕ is one-to-one. Then $\phi[G]$ is a subgroup of S_G by Theorem 8.5 and $\phi : G \to \phi[G]$ is an isomorphism.

We first show that ϕ is one-to-one. Suppose that $a, b \in G$ and $\phi(a) = \phi(b)$. Then the permutations λ_a and λ_b are the same, so $\lambda_a(e) = \lambda_b(e)$. Thus $ae = be$ and $a = b$. So ϕ is one-to-one.

We now need to show that ϕ is a group homomorphism. Let $a, b \in G$. Then $\phi(ab) = \lambda_{ab}$ and $\phi_a\phi_b = \lambda_a\lambda_b$. We must show that the two permutations λ_{ab} and $\lambda_a\lambda_b$ are the same. Let $g \in G$.

$$\lambda_{ab}(g) = (ab)g = a(bg) = \lambda_a(bg) = \lambda_a(\lambda_b(g)) = (\lambda_a\lambda_b)(g).$$

Thus $\lambda_{ab} = \lambda_a\lambda_b$, which implies that $\phi(ab) = \phi(a)\phi(b)$. So ϕ is a one-to-one homomorphism, which completes the proof. ◆

8.12 Example The proof of Cayley's Theorem shows that any group G is isomorphic with a subgroup of S_G, but this is typically not the smallest symmetric group that has a subgroup isomorphic with G. For example, D_n is isomorphic with a subgroup of $S_{\mathbb{Z}_n}$ while the proof of Cayley's Theorem gives a subgroup of S_{D_n} and D_n has $2n$ elements while $\mathbb{Z}_n$ has only n elements. On the surface, it may seem that $\mathbb{Z}_6$ cannot be isomorphic with a subgroup of S_n for $n < 6$, but $(1, 2, 3)(4, 5) \in S_5$ generates a subgroup isomorphic with $\mathbb{Z}_6$. ▲

We defined the left regular representation in Definition 8.10. We now define the right regular representation. Instead of λ_x representing the row for x in the group table, we use σ_x to represent the column with head x. Instead of using ϕ for the function that sends x to λ_x, we use τ, which sends x to $\sigma_{x^{-1}}$.

Historical Note

Arthur Cayley (1821–1895) gave an abstract-sounding definition of a group in a paper of 1854: "A set of symbols, $1, \alpha, \beta, \cdots$, all of them different and such that the product of any two of them (no matter in what order) or the product of any one of them into itself, belongs to the set, is said to be a group." He then proceeded to define a group table and note that every line and column of the table "will contain all the symbols $1, \alpha, \beta, \cdots$." Cayley's symbols, however, always represented operations on sets; it does not seem that he was aware of any other kind of group. He noted, for instance, that the four matrix operations $1, \alpha =$ inversion, $\beta =$ transposition, and $\gamma = \alpha\beta$, form, abstractly, the non-cyclic group of four elements. In any case, his definition went unnoticed for a quarter of a century.

This paper of 1854 was one of about 300 written during the 14 years Cayley was practicing law, being unable to find a suitable teaching post. In 1863, he finally became a professor at Cambridge. In 1878, he returned to the theory of groups by publishing four papers, in one of which he stated Theorem 8.11 of this text; his "proof" was simply to notice from the group table that multiplication by any group element permuted the group elements. However, he wrote, "this does not in any wise show that the best or the easiest mode of treating the general problem [of finding all groups of a given order] is thus to regard it as a problem of [permutations]. It seems clear that the better course is to consider the general problem in itself."

The papers of 1878, unlike the earlier one, found a receptive audience; in fact, they were an important influence on Walther von Dyck's 1882 axiomatic definition of an abstract group, the definition that led to the development of abstract group theory.

8.13 Definition Let G be a group. The map $\tau : G \to S_G$ given by $\tau(x) = \sigma_{x^{-1}}$ where $\sigma_x(g) = gx$ is called the **right regular representation** of G. ■

We could have used the right regular representation to prove Cayley's Theorem instead of the left regular representation. Exercise 54 asks for the details of the proof.

Even and Odd Permutations

It seems reasonable that every reordering of the sequence $1, 2, \ldots, n$ can be achieved by repeated interchange of positions of pairs of numbers. We discuss this a bit more formally.

8.14 Definition A cycle of length 2 is a **transposition**. ■

Thus a transposition leaves all elements but two fixed, and maps each of these onto the other. A computation shows that

$$(a_1, a_2, \cdots, a_n) = (a_1, a_n)(a_1, a_{n-1}) \cdots (a_1, a_3)(a_1, a_2).$$

Therefore any cycle of length n can be written as a product of $n - 1$ transpositions. Since any permutation of a finite set can be written as a product of cycles, we have the following.

8.15 Theorem Any permutation of a finite set containing at least two elements is a product of transpositions. ♦

Naively, this theorem just states that any rearrangement of n objects can be achieved by successively interchanging pairs of them.

8.16 Example Following the remarks prior to the theorem, we see that (1, 6) (2, 5, 3) is the product (1, 6) (2, 3) (2, 5) of transpositions. ▲

8.17 Example In S_n for $n \geq 2$, the identity permutation is the product (1, 2) (1, 2) of transpositions. ▲

We have seen that every permutation of a finite set with at least two elements is a product of transpositions. The transpositions may not be disjoint, and a representation of the permutation in this way is not unique. For example, we can always insert at the beginning the transposition (1, 2) twice, because (1, 2) (1, 2) is the identity permutation. What is true is that the number of transpositions used to represent a given permutation must either always be even or always be odd. This is an important fact. The proof involves counting orbits and was suggested by David M. Bloom.

Let $\sigma \in S_A$ and $a \in A$. We let the **orbit** of a be the set $\{\sigma^k(a) \mid k \in \mathbb{Z}\}$. In the case of $\sigma \in S_n$, a simple way to think of the orbit of a is to think of the elements in the cycle containing a in the disjoint cycle representation of σ.

8.18 Example Let $\sigma = (1, 2, 6)(3, 5) \in S_6$. Then the orbit of 1 is the set $\{1, 2, 6\}$, which is also the orbit of 2 and the orbit of 6. The set $\{3, 5\}$ is the orbit of 3 and the orbit of 5. What about the orbit of 4? Recall that if we include 1-cycles, $\sigma = (1, 2, 6)(3, 5)(4)$, which says the orbit of 4 is $\{4\}$. ▲

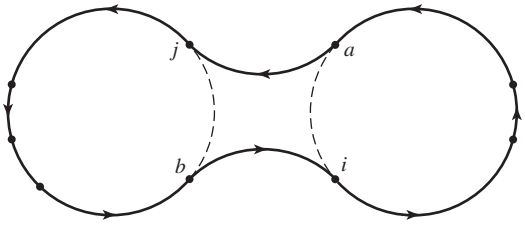
8.19 Theorem No permutation in S_n can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

Proof Let $\sigma \in S_n$ and let $\tau = (i, j)$ be a transposition in S_n. We claim that the number of orbits of σ and of $\tau\sigma$ differ by 1.

Case I Suppose i and j are in different orbits of σ. Write σ as a product of disjoint cycles, the first of which contains j and the second of which contains i, symbolized by the two circles in Fig. 8.20. We may write the product of these two cycles symbolically as

$$(b, j, \times, \times, \times)(a, i, \times, \times)$$

where the symbols $\times$ denote possible other elements in these orbits.



8.20 Figure

Computing the product of the first three cycles in $\tau\sigma = (i, j)\sigma$, we obtain

$$(i, j)(b, j, \times, \times, \times)(a, i, \times, \times) = (a, j, \times, \times, \times, b, i, \times, \times).$$

The original 2 orbits have been joined to form just one in $\tau\sigma$ as symbolized in Fig. 8.20. Exercise 42 asks us to repeat the computation to show that the same thing happens if either one or both of i and j should be the only element of their orbit in σ.

Case II Suppose i and j are in the same orbit of σ. We can then write σ as a product of disjoint cycles with the first cycle of the form

$$(a, i, \times, \times, \times, b, j, \times, \times)$$