8 Transpositions and the Alternating Group

Recall that a 2-cycle in S_n is called a *transposition*. We have seen that every element of S_n can be written uniquely as a product of disjoint cycles. We will now see that every element can be written as a product of transpositions (so the transpositions generate S_n), but this representation is in no way unique. Nonetheless, we will see that no matter how you express a given element as a product of transpositions, the parity of the number of transpositions in the expression is always the same.

Proposition 8.1 *Every element of $S_n, n \geq 2$, may be written as a product of transpositions.*

Proof. It suffices to show that this is true for cycles of length at least 2. Observe that if $r > 1$, then $(a_1 a_2 \cdots a_r) = (a_1 a_r)(a_1 a_{r-1}) \cdots (a_1 a_2)$.

Definition 8.2 *A permutation $\sigma \in S_n$ is* even *if σ has a factorization as a product of an even number of transpositions, and* odd *if it has a factorization as an odd number of transpositions.*

It is not a priori clear that σ cannot be simultaneously even and odd. Read the book proof (§3.5 of Dummit and Foote) – it is the "standard" proof. Below is an alternate proof.

Definition 8.3 *Let $\sigma = \rho_1 \rho_2 \cdots \rho_t$ be a factorization of σ into disjoint cycles in S_n, and let $\Sigma = \sum_{i=1}^{t} \mathit{length}(\rho_i)$. Observe $\Sigma - t$ depends only on σ, even if some 1-cycles are included in the representation of σ as a product of disjoint cycles. Define the* sign function $\operatorname{sgn} : S_n \to \{\pm 1\}$ *by* $\operatorname{sgn}(\sigma) = (-1)^{\Sigma - t}$. *Observe that* $\operatorname{sgn}(1) = 1$ *and* $\operatorname{sgn}(\tau) = -1$ *for any transposition τ.*

Lemma 8.4 *If $\sigma \in S_n, \tau$ a transposition, then* $\operatorname{sgn}(\tau\sigma) = -\operatorname{sgn}(\sigma)$.

Proof. Let $\sigma = \rho_1 \rho_2 \cdots \rho_t$ be a product of disjoint cycles in which $\Sigma = n$ (adding 1-cycles if necessary), so each $i, 1 \leq i \leq n$ occurs in exactly one ρ_j. Let $\tau = (ab)$. If a, b occur in the same ρ_j, say $\rho_j = (a c_1 \cdots c_k b d_1 \cdots d_m)$, then check that $\tau \rho_j = (b d_1 \cdots d_m)(a c_1 \cdots c_k)$, and τ commutes with the other ρ_n's, so $\operatorname{sgn}(\tau\sigma) = (-1)^{n-(t+1)} = -\operatorname{sgn}(\sigma)$. If a, b occur in different cycles, say $\rho_i = (a c_1 \cdots c_k), \rho_j = (b d_1 \cdots d_m)$, then τ commutes with all the other cycles, and $\tau \rho_i \rho_j = (a c_1 \cdots c_k b d_1 \cdots d_m)$, so $\operatorname{sgn}(\tau\sigma) = (-1)^{n-(t-1)} = -\operatorname{sgn}(\sigma)$.

Proposition 8.5 *The map* $\operatorname{sgn} : S_n \to \{\pm 1\}$ *is a homomorphism.*

Proof. Let $\sigma \in S_n, \sigma = \tau_1\tau_2\cdots\tau_m$ a factorization into transpositions with m minimal. We prove by induction on m that $\operatorname{sgn}(\sigma\rho) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\rho)$ for all $\rho \in S_n$. If $m = 1$, this is just the previous lemma. If $m > 1$, notice that $\tau_2\cdots\tau_m$ is a minimal representation for $\tau_1\sigma$. Then

$$\begin{aligned}
\operatorname{sgn}(\sigma\rho) &= \operatorname{sgn}(\tau_1\cdots\tau_m\rho) \\
&= -\operatorname{sgn}(\tau_2\cdots\tau_m\rho) \text{ (by lemma)} \\
&= -\operatorname{sgn}(\tau_2\cdots\tau_m)\operatorname{sgn}(\rho) \text{ (inductive hypothesis)} \\
&= \operatorname{sgn}(\tau_1\cdots\tau_m)\operatorname{sgn}(\rho) \text{ (by lemma)} \\
&= \operatorname{sgn}(\sigma)\operatorname{sgn}(\rho).
\end{aligned}$$

Corollary 8.6 *The permutation* $\sigma \in S_n$ *is even if and only if* $\operatorname{sgn}(\sigma) = 1$ *and is odd if and only if* $\operatorname{sgn}(\sigma) = -1$. *The number of factors occuring in any factorization of* σ *into a product of transpositions is either always even or always odd.*

Definition 8.7 *The* alternating group A_n *of degree* n *is the subgroup of* S_n *consisting of all even permutations. For* $n \geq 2$, *it is a normal subgroup of index* 2, *as it is the kernel of the surjective homomorphism* $\operatorname{sgn} : S_n \to \{\pm 1\}$.

We will now sketch an elementary but tricky proof of the simplicity of A_n for $n \neq 4$. Another clever proof using group actions and the class equation will be given later.

Theorem 8.8 A_n *is simple if and only if* $n \neq 4$.

Proof. First, observe that this is clear for $n = 1, 2, 3$, as the orders of the alternating groups are $1, 1, 3$ respectively. For $n > 4$, the idea is to assume that we have a nontrivial normal subgroup $N \lhd A_n$, and take a nonidentity element $\sigma \in N$. We then conjugate this element by some $\delta \in A_n$ which changes it in a small way. This gives a "small" permutation $\sigma^{-1}\delta\sigma\delta^{-1} \in N$. We show this forces N to be equal to all of A_n. We begin with two important lemmas.

Lemma 8.9 *Let* i, j *be any two fixed, distinct elements of* $\{1, 2, \ldots, n\}$. *Then for* $n \geq 3$, A_n *is generated by the set of* 3*-cycles* $T := \{(ijk) \mid 1 \leq k \leq n, k \neq i, j\}$.

Proof of Lemma. We may assume $n \geq 4$. Nonidentity elements of A_n are products of terms of the form $(ab)(cd)$ or $(ab)(ac)$ for distinct $a, b, c, d \in \{1, 2, \ldots, n\}$. Then $(ab)(cd) = (acb)(acd), (ab)(ac) = (acb)$, so A_n is generated by the set of all 3-cycles. All 3-cycles are of the form $(ija), (iaj), (iab), (jab)$, or (abc), with $a, b, c \neq i, j$. Now (ija) is in T, and $(iaj) = (ija)^2 \in \langle T \rangle$. Also $(iab) = (ijb)(ija)^2 \in \langle T \rangle$, and $(jab) = (ijb)^2(ija) \in \langle T \rangle$. Finally, $(abc) = (ija)^2(ijc)(ijb)^2(ija) \in \langle T \rangle$. Thus T generates all 3-cycles, and hence generates A_n.

Lemma 8.10 *Assume $N \lhd A_n$. If N contains a 3-cycle, then $N = A_n$.*

Proof of Lemma. We may assume $n \geq 4$. Suppose $(ija) \in N$. Choose $k \neq i, j, a$. Then

$$(ijk) = (ij)(ak)(ija)^2(ak)(ij) = [(ij)(ak)](ija)^2[(ij)(ak)]^{-1} \in N.$$

Proof of Theorem. To see that A_4 is not simple, observe that the subgroup $N := \{1, (12)(34), (13)(24), (14)(23)\}$ is normal in A_4. (In fact, it is a normal subgroup of S_4, with $S_4/N \cong S_3$ and $A_4/N \cong \boldsymbol{Z}/3\boldsymbol{Z}$.)

Now let $n \geq 5$. Assume $N \lhd A_n, N \neq \{1\}$.

(1). If N contains a 3-cycle, we are done by the preceding lemma.

(2). Assume N contains an element σ, which when written as a product of disjoing cycles has a factor $(i_1 \ldots i_r), r \geq 4$. Let $\delta = (i_1 i_2 i_3)$. Then $\sigma^{-1}\delta\sigma\delta^{-1} \in N$ by normalcy. Check that $\sigma^{-1}\delta\sigma\delta^{-1} = (i_1 i_3 i_r)$. Thus N contains a 3-cycle, so $N = A_n$.

(3). Assume now that N contains an element σ which, when written as a product of disjoint cycles, has at least two factors of length 3, say $(i_1 i_2 i_3)(i_4 i_5 i_6)$. Let $\delta = (i_1 i_2 i_4)$. Then $\sigma^{-1}\delta\sigma\delta^{-1} = (i_1 i_4 i_2 i_6 i_3) \in N$, and we are done by the previous case.

(4). Then assume that N contains an element σ which is a product of a 3-cycle with disjoint 2-cycles: $\sigma = (i_1 i_2 i_3)\tau$, where $\tau^2 = 1$. Then $\sigma^2 = (i_1 i_2 i_3)\tau(i_i i_2 i_3)\tau = (i_1 i_2 i_3)^2 = (i_1 i_3 i_2) \in N$, so N contains a 3-cycle and we are done by (1).

(5). Suppose N contains an element which can be written as a product of an even number of disjoint 2-cycles: $\sigma = (i_1 i_2)(i_3 i_4)\tau$, where $\tau^2 = 1$. Let $\delta = (i_1 i_2 i_3)$. Then $\sigma^{-1}\delta\sigma\delta^{-1} = (i_1 i_3)(i_2 i_4) \in N$. Choose i_5 distinct from i_1, i_2, i_3, i_4. (This is where the proof fails for $n = 4$.) Let $\gamma = (i_1 i_3 i_5)$. Then $(i_1 i_3)(i_2 i_4)\gamma(i_1 i_3)(i_2 i_4)\gamma^{-1} = \gamma \in N$, and we are again done by (1).

Since if N is nontrivial, at least one of the situations in (1) - (5) above must occur, it follows that N contains a 3-cycle and hence that $N = A_n$.