THE ALTERNATING GROUP IS SIMPLE

1. Some Properties of the Symmetric Group

Let $n \in \mathbb{Z}_{>0}$ be a a positive integer, and let S_n denote the group of permutations of n letters.

The fact that every element of S_n can be written (nonuniquely) as a product of transpositions (2-cycles) is self-evident.

The fact that every element of S_n can be written as a product of an even number of transpositions, or as an odd number of transpositions, but *not both* is not at all self-evident. See Gallian for a short elementary proof. However, granting the fact, the identity (composing from right to left, as seems to be the practice in introductory texts)

$$(1\,2\,3\,\cdots\,k) = (1\,k)\cdots(1\,3)(1\,2)$$

shows that that *a k-cycle is even if and only if k is odd.*

The subgroup of even permutations in S_n is the *alternating* group A_n. Its name comes from the fact that if its elements are viewed as even permutations of the symbols $r_1, \ldots, r_n$ then they preserve the polynomial expression

$$\prod_{i<j}(r_i - r_j),$$

whereas the odd permutations negate the expression.

An element of S_n can also be written

$$\tau = \begin{pmatrix} x_1 & \cdots & x_n \\ y_1 & \cdots & y_n \end{pmatrix},$$

where $\{x_1, \ldots, x_n\} = \{y_1, \ldots, y_n\} = \{1, \ldots, n\}$ and typically $x_1 = 1, \ldots, x_n = n$ or similarly for the y-values. And an element of S_n can be written as a product of disjoint cycles,

$$\sigma = (a_1 \cdots a_k)(b_1 \cdots b_\ell)\cdots, \qquad \{a_i\} \sqcup \{b_j\} \sqcup \cdots = \{1, \ldots, n\}.$$

Clearly the order of σ is the least common multiple of the lengths of its cycles.

Proposition 1.1. *The conjugation-action of S_n on itself restricts to the subset of elements having each particular cycle-structure, and the action is transitive on each such subset.*

Proof. If

$$\sigma = (a_1\,\cdots\,a_k)(b_1\,\cdots\,b_\ell)\cdots$$

and

$$\tau = \begin{pmatrix} \alpha_1 & \cdots & \alpha_k & \beta_1 & \cdots & \beta_\ell & \cdots \\ a_1 & \cdots & a_k & b_1 & \cdots & b_\ell & \cdots \end{pmatrix}$$

then (composing right-to-left)

$$\tau^{-1}\sigma\tau = (\alpha_1\,\cdots\,\alpha_k)(\beta_1\,\cdots\,\beta_\ell)\cdots.$$

□

2. Simplicity of the Alternating Group

Let G be a group. Recall that a subgroup of G is *normal* if its normalizer is all of G, or equivalently, if it is the kernel of a homomorphism out of G. Every subgroup of an abelian group is normal.

Since the alternating group A_n is the kernel of the homomorphism

$$S_n \longrightarrow \mathbb{Z}/2\mathbb{Z}, \quad \sigma \longmapsto \text{parity of } \sigma,$$

it follows that A_n is a normal subgroup of S_n. We wonder about normal subgroups of A_n in turn. For $n = 4$, the Klein four-group

$$V = \{e,\ (1\,2)(3,\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\}$$

is normal in A_4 because conjugation preserves cycle-structure. However, the Klein four-group turns out to be the only example.

Definition 2.1. *A group G is* **simple** *if it has no nontrivial normal subgroups.*

As discussed in Gallian, the problem of classifying all finite simple groups has been a long, titanic mathematical endeavor. Our aim here is more modest.

Proposition 2.2. *The alternating group A_n is simple for $n \neq 4$.*

Proof. Since $A_1 \approx A_2 \approx \{\cdot\}$ and $A_3 \approx \mathbb{Z}/3\mathbb{Z}$, we may take $n \geq 5$. The equalities

$$(a\,b)(c\,d) = (a\,c\,b)(a\,c\,d), \qquad (a\,b)(b\,c) = (a\,b\,c)$$

show that A_n is generated by the set of its 3-cycles. Also, beyond Proposition 1.1, all 3-cycles are conjugate in A_n. Indeed, each $(a_1\,a_2\,a_3)$ takes the form $\tau^{-1}(1\,2\,3)\tau$ for some $\tau \in S_n$; if τ is even then we are done, and if τ is odd then also $(a_1\,a_2\,a_3) = \tau^{-1}(4\,5)(1\,2\,3)(4\,5)\tau$ with $(4\,5)\tau$ even. This argument uses the condition $n \geq 5$, but it does not assume that $(4\,5)$ and τ are disjoint. The upshot is that given a normal subgroup $N \neq \{e\}$ of A_n where $n \geq 5$, we need only to show that N contains a 3-cycle. Now reason as follows.

- If N contains an element $\sigma = (1\,\cdots\,r)\tau$ where $r \geq 4$, then let $\delta = (1\,2\,3)$ and compute
$$\sigma^{-1} \cdot \delta^{-1}\sigma\delta = (r\,\cdots\,1)(1\,3\,2)(1\,\cdots\,r)(1\,2\,3) = (2\,3\,r).$$
Thus N contains a 3-cycle as desired. The same argument holds for any $\sigma = (a_1\,\cdots\,a_r)\tau$, using $\delta = (a_1\,a_2\,a_3)$. We use this same idea for notational ease without comment from now on.
- If N contains an element $\sigma = (1\,2\,3)(4\,5\,6)\tau$, then let $\delta = (1\,2\,4)$ and compute that we are done by the previous bullet,
$$\sigma^{-1} \cdot \delta^{-1}\sigma\delta = (1\,3\,2)(4\,6\,5)(1\,4\,2)(1\,2\,3)(4\,5\,6)(1\,2\,4) = (1\,2\,4\,3\,6).$$
- If N contains an element $\sigma = (1\,2\,3)\tau$ where τ is a product of 2-cycles, then $\sigma^2 = (1\,3\,2)$ and we are done.
- If N contains an element $\sigma = (1\,2)(3\,4)\tau$ where τ is a product of 2-cycles, then let $\delta = (1\,2\,3)$ so that $\sigma^{-1}\delta^{-1}\sigma\delta = (1\,4)(2\,3)$. Next (using $n \geq 5$ here),
$$(1\,5\,2)(1\,4)(2\,3)(1\,2\,5) = (1\,3)(4\,5),$$
and then we are done by the first bullet,
$$(1\,4)(2\,3)(1\,3)(4\,5) = (1\,2\,3\,4\,5).$$

This completes the proof. ∎