THE SYMMETRIC GROUP

HAROLD COOPER

1. Permutations

Definition 1.1. A *permutation* of a finite set S is a bijection $\sigma\colon S \to S$.

Lemma 1.1. *There are exactly* $n!$ *permutations of an* n*-element set.*

Proof. For an n-element set $S = \{x_1, \ldots, x_n\}$, we can construct a permutation σ on S as follows:

(1) Assign one of the n elements of S to $\sigma(x_1)$.
(2) Assign one of the $n-1$ elements of $S - \{\sigma(x_1)\}$ to $\sigma(x_2)$.
$\vdots$
(n) Assign the 1 remaining element to $\sigma(x_n)$.

This method can generate $n(n-1)\cdots 1 = n!$ different permutations of S. Furthermore, it should be reasonably clear that these permutations are distinct, and that any permutation can be generated in this way, and thus we know that there are exactly $n!$ permutations of an n-element set.

$\square$

Definition 1.2. For a set S, $\mathrm{Perm}(S)$ is the set of all permutations on S. Multiplication of two elements $\sigma, \tau \in \mathrm{Perm}(S)$ is simply their composition $\sigma\tau = \sigma \circ \tau$.

Note that the composition of two bijections $\sigma, \tau\colon S \to S$ is itself a bijection $\sigma \circ \tau\colon S \to S$. Thus multiplication in $\mathrm{Perm}(S)$ is closed. It is also associative, and has identity and inverse, since function composition is associative and has identity and inverse (and the identity function is of course a bijection and the inverse of a bijection is a bijection). So $\mathrm{Perm}(S)$ satisfies the axioms of a group.

Definition 1.3. The *symmetric group* S_n is the group $\mathrm{Perm}(\{1, \ldots, n\})$ of all permutations on the first n integers.

Lemma 1.2. *If* $|S| = n$ *then* $\mathrm{Perm}(S) \approx S_n$.

Proof. Since S has n elements, we can index them $S = \{x_1, \ldots, x_n\}$.
Then our isomorphism $\phi\colon S_n \to \mathrm{Perm}(S)$ operates simply as $\phi(\sigma)(x_i) = x_{\sigma(i)}$, which is clearly a homomorphism and clearly bijective.

$\square$

2. Group Operations

Definition 2.1. Given a group G and a set S, a *group operation* by G on S is a product mapping (written like multiplication) from $G \times S$ to S, with the property that the identity of G fixes every element in S, and for all $g, g' \in G$ and $s \in S$, $g(g's) = (gg')s$.

Lemma 2.1. *Given an operation by G on S, every $g \in G$ permutes S.*

Proof. Let us denote the *function* corresponding to a given element $g \in G$ under a certain operation on S as $g_*\colon S \to S$ defined by $g_*(s) = gs$ for all $s \in S$.
G is a group, so g has an inverse g^{-1}, which itself has a corresponding function $g_*^{-1}\colon S \to S$ under the given operation. We have for any $s \in S$ that $g_*^{-1}(g_*(s)) = g^{-1}(gs) = (g^{-1}g)s = s$ and $g_*(g_*^{-1}(s)) = g(g^{-1}s) = (gg^{-1})s = s$.
So g_* is a function with an inverse, so it must be bijective, and since it maps S to S it is thus by definition a permutation.
Thus the function corresponding to every group element under any group operation on a set S is a permutation of S, i.e. for all $g \in G$, $g_* \in \mathrm{Perm}(S)$.

$\square$

Thus given a group operation we can define a homomorphism $\phi\colon G \to \mathrm{Perm}(S)$ simply by $\phi(g) = g_*$ (with g_* defined as above). (It is left as a [dull] exercise to show that this is indeed a homomorphism.)

3

Theorem 3.1 (Cayley's Theorem)**.** *Every group of order n is isomorphic to a subgroup of S_n.*

Proof. Suppose G a group of order n.
Let G operate on itself by left multiplication. Then by our lemma on group operations we have a homomorphism $\phi\colon G \to \mathrm{Perm}(G)$. If $gg' = g'$ then $g = 1$, so the only element acting as the trivial permutation is the identity, i.e. $\phi(g) = 1 \iff g = 1$ so ϕ is injective.
But then by the First Isomorphism Theorem, $\operatorname{im}\phi \approx G/\ker\phi = G/\{1\} \approx G$.
So $G \approx \operatorname{im}\phi \subset \mathrm{Perm}(G)$ is a subgroup of $\mathrm{Perm}(G)$, but of course $\mathrm{Perm}(G) \approx S_n$, so G is isomorphic to a subgroup of S_n.

$\square$

Theorem 3.2. $GL_2(\mathbb{F}_2) \approx S_3$

Proof. Let $G = GL_2(\mathbb{F}_2)$.

For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, $\det A = ad - bc \neq 0 \Rightarrow ad \neq bc$ which can happen in 6 ways, so $|GL_2(\mathbb{F}_2)| = 6$. And we know from above that $|S_3| = 3! = 6$.

Let $S = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$ be operated on by G simply by left matrix multiplication. As shown above this gives a homomorphism $\phi \colon G \to \mathrm{Perm}(S)$.

For $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S$, $A \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix}$, while $A \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} b \\ d \end{pmatrix}$. Thus both $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are only fixed by the identity. In other words, every nontrivial element of G acts on S in a nontrivial way, i.e. $\phi(g) = 1 \iff g = 1$, or ϕ is injective.
And we can compose this homomorphism with the isomorphism between $\mathrm{Perm}(S)$ and S_3 (since $|S| = 3$) to get an injective homomorphism $\psi \colon G \to S_3$, which since $|G| = |S_3| = 3$ must be an isomorphism.

$\square$