Section 9: Orbits, Cycles, and Alternating Groups

We will start by proving Cayley's Theorem, from last time.

Definition 0.1. Let $f : A \to B$ be a function and let H be a subset of A. The **image** of H under f is the set $f[H] = \{f(h) \mid h \in H\}$.

Definition 0.2. Let G and G' be groups. A **homomorphism** is a function $\phi : G \to G'$ such that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$.

In the context of what we already know, an *isomorphism* is a homomorphism that is also one-to-one and onto.

Lemma 0.3. *Let G and G' be a groups and let $\phi : G \to G'$ be a homomorphism. Then, $\phi[G]$ is a subgroup of G'.*

Proof. First, we show that $\phi[G]$ is a subgroup. Let $x', y' \in \phi[G]$. By definition of $\phi[G]$, there exist $x, y \in G$ such that $\phi(x) = x'$ and $\phi(y) = y'$. By the homomorphism condition, $\phi(xy) = \phi(x)\phi(y) = x'y'$, so $x'y' \in \phi[G]$ so $\phi[G]$ is closed. It contains the identity because $\phi(e) = e$ and contains inverses because $\phi(x^{-1}) = \phi(x)^{-1}$. Therefore, it is a subgroup of G'. □

Lemma 0.4. *Let G and G' be a groups and let $\phi : G \to G'$ be a homomorphism that is one-to-one. Then, G is isomorphic to $\phi[G]$.*

Proof. Consider ϕ as a function $\phi : G \to \phi[G]$. By definition of ϕ, it is one-to-one and satisfies the homomorphism property. By definition of $\phi[G]$, $\phi : G \to \phi[G]$ is onto. Therefore, ϕ is an isomorphism. □

Using all of this, we can prove the theorem.

Theorem 0.5 (Cayley's Theorem)**.** *Every group is isomorphic to a subgroup of a permutation group.*

Proof. Let G be a group. We will show that G is isomorphic to a subgroup of S_G. By the previous lemmas, we just need to define a one-to-one homomorphism $\phi : G \to S_G$. For any $g \in G$, we can define a permutation $\lambda_g : G \to G$ by $\lambda_g(x) = gx$ for any $x \in G$. To show this is a permutation, we must show that it is onto and one-to-one. For any element $h \in G$, the equation $gx = h$ has a unique solution $x = g^{-1}h$, so $\lambda_g(g^{-1}h) = gg^{-1}h = h$, so λ_g is onto. If $\lambda_g(x) = \lambda_g(y)$, this implies $gx = gy$ which, by cancellation, implies $x = y$. Therefore, λ_g is one-to-one. Therefore, λ_g is a permutation.

With this definition, we can define the function $\phi : G \to S_G$ by $\phi(g) = \lambda_g$. We must check that this is one-to-one and satisfies the homomorphism condition. To see it is one-to-one, suppose $\lambda_g = \lambda_h$. Then, $\lambda_g(e) = \lambda_h(e)$, so $ge = he$, so $g = h$. Hence, ϕ is one-to-one. To check the homomorphism condition, we must check that $\phi(gh) = \phi(g)\phi(h)$. But, $\phi_(gh)$ is the function $\phi(gh) = \lambda_{gh}$, and $\phi(g)\phi(h) = \lambda_g \circ \lambda_h$. For any $x \in G$, $\lambda_{gh}(x) = ghx$ and $\lambda_g \circ \lambda_h(x) = g(h(x))$, so $\lambda_{gh} = \lambda_g \circ \lambda_h$. Therefore, ϕ is a one-to-one homomorphism so G is isomorphic to $\phi[G] \leq S_G$. □

For the rest of today, we will talk about *cycles*.

Example 0.6. Consider the permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 6 & 1 & 3 \end{pmatrix}$. We can describe this is another way by looking at how the numbers cycle amongst themselves.

Starting with 1, we see that $1 \mapsto 2$ and then $2 \mapsto 5$ and then $5 \mapsto 1$, so the permutation gives a *cycle* $1 \mapsto 2 \mapsto 5 \mapsto 1$. Similarly, we see that $3 \mapsto 4 \mapsto 6 \mapsto 3$, so we can view this permutation as two cycles. We will denote this by $(125)(346)$.

We will call (125) the *orbit* of 1 (or 2, or 5) and (346) the *orbit* of 3 (or 4, or 6).

In general, there are many ways to describe permutations. This method is called **cycle notation**.

In cycle notation, we express each permutation in terms of elements that eventually cycle back to themselves. Every element $1, \ldots, n$ can appear at most once in your cycle, and we conventionally write cycles left to right starting with the smallest number. If any elements are left out in cycle notation, they are defined to be fixed (not changed) by the permutation. This is easiest to see with examples.

Example 0.7. Let's consider permutations in S_5. Let's write the permutation $\sigma = (124)(35)$ in the notation we used on Monday. $(124)(35)$ should be interpreted as two cycles: $1 \to 2$, $2 \to 4$, and $4 \to 1$, and then $3 \to 5$ and $5 \to 3$. So, this says $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$

If $\tau = (124)$, then $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$