Cayley's Theorem

Recall the Cayley (Group) Table for $\mathbb{Z}/4\mathbb{Z}$ you saw in Section 5:

$\cdot$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

What do you notice about each column in this table? About each row? Each column/row contains all of the values $0-4$ rearranged, or permuted, in some way. So, each row corresponds to some permutation of our group elements and we can use this idea to define a map from G to S_G, the group of all permutations of G.

Thus it should be clear that every *finite* group is isomorphic to a subgroup of some symmetric group (using the method presented above), but in fact something much stronger holds. Cayley's theorem states that this property holds not only for finite groups, but for every group (regardless of order).

This is a classic result in group theory and a very intriguing one – with this in hand, if we can fully understand the structure and properties of S_n and its subgroups, then we will automatically understand the structure and properties of *every* group! However, due to the sheer size of S_n this becomes problematic. For instance, a refinement of Cayley's theorem states that any group G is isomorphic to a subgroup of $S_{|G|}$, but the size of $S_{|G|}$ is $|G|!$, so trying to use $S_{|G|}$ to answer any question you might have about G means working with a group that factorially larger (note, factorial growth is faster than exponential growth!).

Definition
Let $f : A \to B$ be a function and let $H \subseteq A$. The **image of H under f** is $\{f(h) : h \in H\}$ and is denoted by $f[H]$.

Note, a more standard notation for the image is $f(H)$.

Lemma 8.15
Let G and G' be groups and let $\phi : G \to G'$ be an injective function such that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$. Then $\phi[G]$ is a subgroup of G' and ϕ provides an isomorphism of G with $\phi[G]$.

Note, a function $\phi : G \to G'$ between two groups satisfying $\phi(xy) = \phi(x)\phi(y)$ is called a **homomorphism**. You may have briefly seen this in Section 3 when you were discussing isomorphisms (an isomorphism is a bijective homomorphism) and you will explore their properties more in Section 13.

Further, something much more general actually holds. The injectivity requirement can be removed to give an isomorphism between a subgroup of G and $\phi[G]$, which is known as the First Isomorphism Theorem (for groups); which will be seen in Section 32.

Proof. To show that $\phi[G] \leq G'$ we need to show that $\phi[G]$ is closed and contains inverses and the identity element.

First, let $x', y' \in \phi[G] \subseteq G'$, then by definition there exist some $x, y \in G$ such that $\phi(x) = x'$ and $\phi(y) = y'$. Using this and the homomorphism property, we see that

$$x'y' = \phi(x)\phi(y) = \phi(xy),$$

and thus $x'y' \in \phi[G]$, so $\phi[G]$ is closed.

Now, let e, e' be the identity elements in G, G', respectively, then we see

$$e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e),$$

again using the homomorphism property. Now, since G' is a group we have right-cancellation implying $e' = \phi(e)$, and thus $e' \in \phi[G]$.

Finally, let $x' \in \phi[G]$ with $x' = \phi(x)$. We have

$$e' = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = x'\phi(x^{-1}),$$

which gives $(x')^{-1} = \phi(x^{-1}) \in \phi[G]$.

Therefore, we have that $\phi[G] \leq G'$. The fact that $G \cong \phi[G]$ is trivial since, by assumption, ϕ is injective and satisfies the homomorphism property, and surjectivity follows from the definition of $\phi[G]$.

□

Cayley's Theorem
Every group is isomorphic to a group of permutations.

Proof. Let G be a group, since any subgroup of a symmetric group is a group of permutations, if we can define an injective homomorphism $\phi : G \to S_G$ then by Lemma 8.15 the result will follow.

Recall the map $\ell_g : G \to G$ defined by $\ell_g(x) = gx$ for all $x \in G$ defined last class (this is the left-multiplication by g map), which we saw to be bijective and provide a permutation of the elements of G.

Define a map $\phi : G \to S_G$ by $\phi(g) = \ell_g$. We want to show that ϕ is an injective homomorphism.

First, suppose that $\phi(g) = \phi(g')$, then $\ell_g = \ell_{g'}$ as functions mapping G to G. For functions to be equal they must equal at every point, and hence $\ell_g(e) = \ell_{g'}(e)$ implying $g = ge = g'e = g'$; and hence ϕ is injective.

Now, let $g, g' \in G$, then we see, for any $x \in G$,

$$\phi(gg')(x) = \ell_{gg'}(x) = gg'x = g(g'x) = \ell_g(g'(x)) = \ell_g(\ell_{g'}(x)) = \phi(g)(\phi(g')(x)) = \phi(g)\phi(g')(x).$$

Thus, ϕ is a homomorphism.

Since ϕ is an injective homomorphism Lemma 8.14 tells us that $G \cong \phi[G] \leq S_G$ and so G is isomorphic to a group of permutations.

□

Alternatively, we could have used the right-multiplication by g map, r_g, to induce another subgroup of S_G isomorphic to G with one subtle difference. Rather than defining a map $\mu(g) = r_g$ we instead define μ to be $\mu(g) = r_{g^{-1}}$.

Note, the map $\mu(g) = r_g$ actually fails to be a homomorphism:

$$\mu(gg')(x) = r_{gg'}(x) = xgg' = r_{g'}(xg) = r_{g'}(r_g(x)) = r_{g'}r_g(x) = \mu(g')\mu(g)(x) \neq \mu(g)\mu(g')(x).$$

Defining $\mu(g) = r_{g^{-1}}$ solves this 'commutativity' problem and defines a homomorphism.

Definition
The maps ϕ and μ defined above are the **left regular representation** and **right regular representation** of G, respectively.

Note, the left regular representation corresponds to the rows in a Cayley table, while the right regular representation corresponds to the columns (being careful to choose the correct column since $\mu(g) = r_{g^{-1}}$!). For example, using the Cayley table for $\mathbb{Z}/4\mathbb{Z}$ above we see

$$\phi(0) = \ell_0 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{pmatrix}, \qquad \phi(1) = \ell_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix}, \qquad \dots$$

9 Orbits, Cycles, and the Alternating Groups

In your homework you learned about the **orbits** of a permutation. Recall that if A is a set and $\sigma \in S_A$, then the orbit of a under σ is given by

$$\mathcal{O}_{a,\sigma} = \{\sigma^n(a) : n \in \mathbb{Z}\}.$$

The orbits of a permutation naturally determine an equivalence relation on a set, namely, if $a, b \in A$ then $a \sim b$ if and only if $b = \sigma^n(a)$ for some n, i.e., $a \sim b$ iff a and b lie in the same orbit.

Example
Find the orbits of the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} \in S_8.$$

Solution. To find the orbit of 1, we repeatedly apply σ to find

$$1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} \cdots.$$

Hence, the σ-orbit of 1 is $\{1, 3, 6\}$. What would the orbit of 3 be? Of 6? What if we picked a value not in the orbit of 1? Continuing this we can see the σ-orbits are

$$\{1, 3, 6\}, \quad \{2, 8\}, \quad \{4, 5, 7\}.$$

We can graphically represent these orbits in the following way: Each individual cycle above defines a permutation itself! For example the first cycle corresponds to the permutation

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 & 8 \end{pmatrix}.$$

We see that τ has one three-element orbit, $\{1, 3, 6\}$, and five one-element orbits, $\{2\}, \{4\}, \{5\}, \{7\}, \{8\}$. The orbits written in this way lead to a new (and much simplified) notation (called **cycle notation**) representing a permutation, namely,

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 4 & 5 & 1 & 7 & 8 \end{pmatrix} = (1\ 3\ 6)(2)(4)(5)(7)(8) = (1\ 3\ 6).$$