Lecture 4.6: Automorphisms

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra
Basic concepts

Definition

An **automorphism** is an isomorphism from a group to itself.

The set of all automorphisms of $G$ forms a group, called the **automorphism group** of $G$, and denoted $\text{Aut}(G)$.

Remarks.

- An automorphism is determined by where it sends the generators.
- An automorphism $\phi$ must send generators to generators. In particular, if $G$ is cyclic, then it determines a permutation of the set of (all possible) generators.

Examples

1. There are two automorphisms of $\mathbb{Z}$: the identity, and the mapping $n \mapsto -n$. Thus, $\text{Aut}(\mathbb{Z}) \cong C_2$.

2. There is an automorphism $\phi : \mathbb{Z}_5 \to \mathbb{Z}_5$ for each choice of $\phi(1) \in \{1, 2, 3, 4\}$. Thus, $\text{Aut}(\mathbb{Z}_5) \cong C_4$ or $V_4$. (Which one?)

3. An automorphism $\phi$ of $V_4 = \langle h, v \rangle$ is determined by the image of $h$ and $v$. There are 3 choices for $\phi(h)$, and then 2 choices for $\phi(v)$. Thus, $|\text{Aut}(V_4)| = 6$, so it is either $C_6 \cong C_2 \times C_3$, or $S_3$. (Which one?)
Automorphism groups of $\mathbb{Z}_n$

**Definition**

The multiplicative group of integers modulo $n$, denoted $\mathbb{Z}_n^*$ or $U(n)$, is the group

$$U(n) := \{ k \in \mathbb{Z}_n \mid \gcd(n, k) = 1 \}$$

where the binary operation is multiplication, modulo $n$.

**Proposition (homework)**

The automorphism group of $\mathbb{Z}_n$ is $\text{Aut}(\mathbb{Z}_n) = \{ \sigma_a \mid a \in U(n) \} \cong U(n)$, where

$$\sigma_a : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n , \quad \sigma_a(1) = a .$$
Automorphisms of $D_3$

Let's find all automorphisms of $D_3 = \langle r, f \rangle$. We'll see a very similar example to this when we study Galois theory.

Clearly, every automorphism $\phi$ is completely determined by $\phi(r)$ and $\phi(f)$.

Since automorphisms preserve order, if $\phi \in \text{Aut}(D_3)$, then

\[
\phi(e) = e, \quad \phi(r) = r \text{ or } r^2, \quad \phi(f) = f, rf, \text{ or } r^2f.
\]

2 choices

Thus, there are at most $2 \cdot 3 = 6$ automorphisms of $D_3$.

Let's try to define two maps, (i) $\alpha: D_3 \to D_3$ fixing $r$, and (ii) $\beta: D_3 \to D_3$ fixing $f$:

\[
\left\{ \begin{align*}
\alpha(r) &= r \\
\alpha(f) &= rf
\end{align*} \right. \quad \quad \left\{ \begin{align*}
\beta(r) &= r^2 \\
\beta(f) &= f
\end{align*} \right.
\]

I claim that:

- these both define automorphisms (check this!)
- these generate six different automorphisms, and thus $\langle \alpha, \beta \rangle \cong \text{Aut}(D_3)$.

To determine what group this is isomorphic to, find these six automorphisms, and make a group presentation and/or multiplication table. Is it abelian?
Automorphisms of $D_3$

An automorphism can be thought of as a re-wiring of the Cayley diagram.

\[ r \xrightarrow{id} r \]
\[ f \xrightarrow{\alpha} rf \]
\[ r \xrightarrow{\alpha^2} r \]
\[ f \xrightarrow{\alpha^2} r^2 f \]
\[ r \xrightarrow{\beta} r^2 \]
\[ f \xrightarrow{\alpha \beta} r^2 f \]
Automorphisms of $D_3$

Here is the multiplication table and Cayley diagram of $\text{Aut}(D_3) = \langle \alpha, \beta \rangle$.

\[
\begin{array}{cccccc}
\text{id} & \alpha & \alpha^2 & \beta & \alpha \beta & \alpha^2 \beta \\
\hline
\text{id} & \text{id} & \alpha & \alpha^2 & \beta & \alpha \beta & \alpha^2 \beta \\
\alpha & \alpha & \alpha^2 & \text{id} & \alpha \beta & \alpha^2 \beta & \beta \\
\alpha^2 & \alpha^2 & \text{id} & \alpha & \alpha \beta & \beta & \alpha \beta \\
\beta & \beta & \alpha \beta & \alpha^2 \beta & \text{id} & \alpha^2 & \alpha \\
\alpha \beta & \alpha \beta & \beta & \alpha^2 \beta & \alpha & \text{id} & \alpha^2 \\
\alpha^2 \beta & \alpha^2 \beta & \alpha \beta & \beta & \alpha & \text{id} & \alpha
\end{array}
\]

It is purely coincidence that $\text{Aut}(D_3) \cong D_3$. For example, we’ve already seen that

\[
\text{Aut}(\mathbb{Z}_5) \cong U(5) \cong C_4, \quad \text{Aut}(\mathbb{Z}_6) \cong U(6) \cong C_2, \quad \text{Aut}(\mathbb{Z}_8) \cong U(8) \cong C_2 \times C_2.
\]
Automorphisms of $V_4 = \langle h, v \rangle$

The following permutations are both automorphisms:

$\alpha : h \xrightarrow{v} v \xrightarrow{hv} hv$ and $\beta : h \xrightarrow{v} hv$

\begin{align*}
    h \xmapsto{\text{id}} & \quad h \\
    v \xmapsto{} & \quad \nu \\
    hv \xmapsto{} & \quad hv \\

    h \xmapsto{\alpha} & \quad v \\
    v \xmapsto{} & \quad hv \\
    hv \xmapsto{} & \quad v \\

    h \xmapsto{\alpha^2} & \quad hv \\
    v \xmapsto{} & \quad h \\
    hv \xmapsto{} & \quad v \\
\end{align*}
Automorphisms of $V_4 = \langle h, v \rangle$

Here is the multiplication table and Cayley diagram of $\text{Aut}(V_4) = \langle \alpha, \beta \rangle \cong S_3 \cong D_3$.

<table>
<thead>
<tr>
<th></th>
<th>id</th>
<th>$\alpha$</th>
<th>$\alpha^2$</th>
<th>$\beta$</th>
<th>$\alpha \beta$</th>
<th>$\alpha^2 \beta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>id</td>
<td>$\alpha$</td>
<td>$\alpha^2$</td>
<td>$\beta$</td>
<td>$\alpha \beta$</td>
<td>$\alpha^2 \beta$</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>$\alpha$</td>
<td>id</td>
<td>$\alpha \beta$</td>
<td>$\alpha^2 \beta$</td>
<td>$\beta$</td>
<td></td>
</tr>
<tr>
<td>$\alpha^2$</td>
<td>$\alpha^2$</td>
<td>id</td>
<td>$\alpha$</td>
<td>$\alpha \beta$</td>
<td>$\beta$</td>
<td>$\alpha \beta$</td>
</tr>
<tr>
<td>$\beta$</td>
<td>$\beta$</td>
<td>$\alpha \beta$</td>
<td>$\alpha \beta$</td>
<td>id</td>
<td>$\alpha^2$</td>
<td>$\alpha$</td>
</tr>
<tr>
<td>$\alpha \beta$</td>
<td>$\alpha \beta$</td>
<td>$\alpha \beta$</td>
<td>$\alpha$</td>
<td>id</td>
<td>$\alpha^2$</td>
<td></td>
</tr>
<tr>
<td>$\alpha^2 \beta$</td>
<td>$\alpha^2 \beta$</td>
<td>$\alpha \beta$</td>
<td>$\beta$</td>
<td>$\alpha^2$</td>
<td>id</td>
<td></td>
</tr>
</tbody>
</table>

Recall that $\alpha$ and $\beta$ can be thought of as the permutations $h$, $v$, $hv$ and so $\text{Aut}(G) \hookrightarrow \text{Perm}(G) \cong S_n$ always holds.