

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 ϕ 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. Every map $\phi: \mathbb{Z}_5 \rightarrow \mathbb{Z}_5$ where $\phi(1) \in \{1, 2, 3, 4\}$ is an automorphism. Thus, $|\text{Aut}(\mathbb{Z}_5)| \cong C_4$ or V_4 . (Which one?)
3. An automorphism ϕ 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 .

$$U(5) = \{1, 2, 3, 4\} \cong C_4$$

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$$U(8) = \{1, 3, 5, 7\} \cong C_2 \times C_2$$

$$U(6) = \{1, 5\} \cong C_2$$

	1	5
1	1	5
5	5	1

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

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 ϕ is completely determined by $\phi(r)$ and $\phi(f)$.

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

$$\phi(e) = e, \quad \phi(r) = \underbrace{r \text{ or } r^2}_{2 \text{ choices}}, \quad \phi(f) = \underbrace{f, rf, \text{ or } r^2f}_{3 \text{ choices}}.$$

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

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

$$\begin{cases} \alpha(r) = r \\ \alpha(f) = rf \end{cases} \quad \begin{cases} \beta(r) = r^2 \\ \beta(f) = f \end{cases}$$

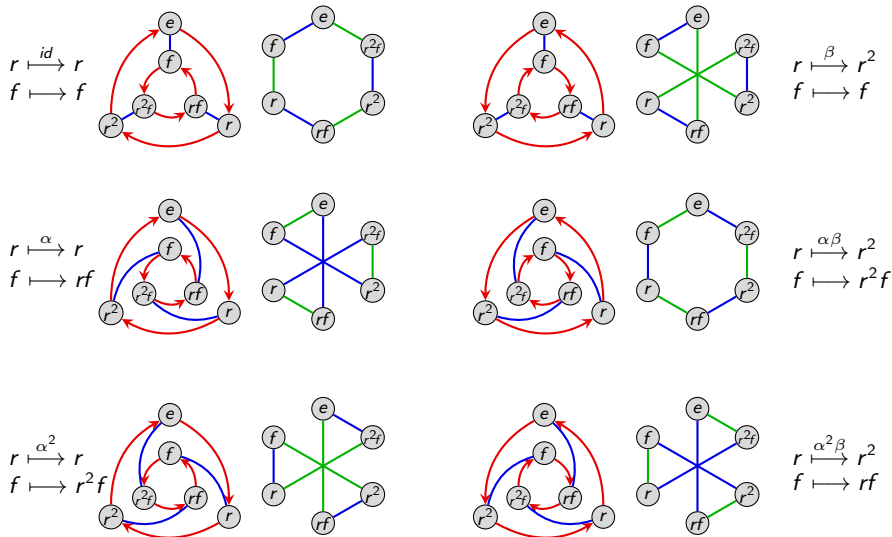
I claim that:

- 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

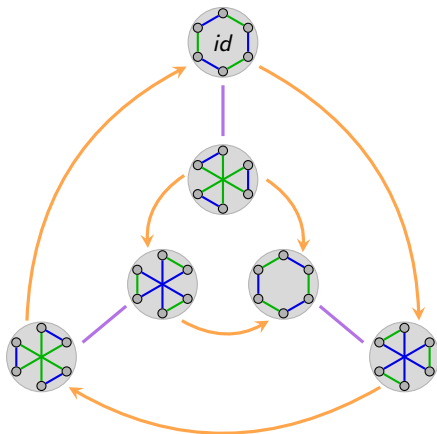
An automorphism can be thought of as a **re-wiring** of the Cayley diagram.



Automorphisms of D_3

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

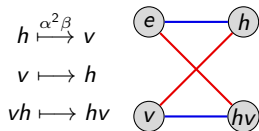
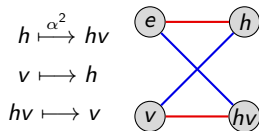
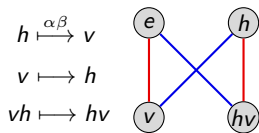
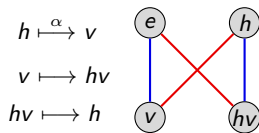
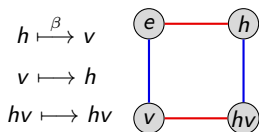
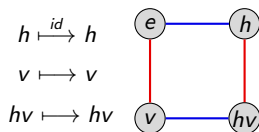
	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
id	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
α	α	α^2	id	$\alpha\beta$	$\alpha^2\beta$	β
α^2	α^2	id	α	$\alpha^2\beta$	β	$\alpha\beta$
β	β	$\alpha^2\beta$	$\alpha\beta$	id	α^2	α
$\alpha\beta$	$\alpha\beta$	β	$\alpha^2\beta$	α	id	α^2
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	β	α^2	α	id



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

$$\text{Aut}(\mathbb{Z}_5) \cong U(5) \cong C_4, \quad \text{Aut}(\mathbb{Z}_6) \cong U(5) \cong C_4, \quad \text{Aut}(\mathbb{Z}_8) \cong U(5) \cong C_2 \times C_2.$$

Automorphisms of V_4

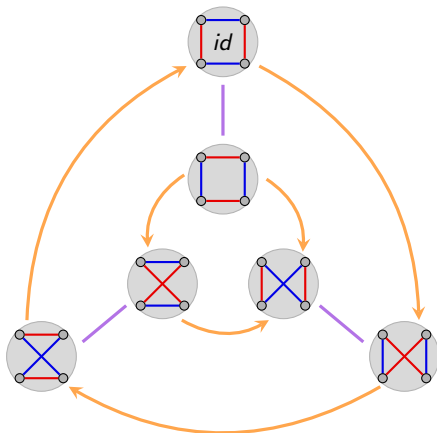


Notice that α is the permutation $h \xrightarrow{v} hv$ and β is the permutation $h \xrightarrow{v} hv$

Automorphisms of V_4

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

	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
id	id	α	α^2	β	$\alpha\beta$	$\alpha^2\beta$
α	α	α^2	id	$\alpha\beta$	$\alpha^2\beta$	β
α^2	α^2	id	α	$\alpha^2\beta$	β	$\alpha\beta$
β	β	$\alpha^2\beta$	$\alpha\beta$	id	α^2	α
$\alpha\beta$	$\alpha\beta$	β	$\alpha^2\beta$	α	id	α^2
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	β	α^2	α	id



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