

### Optional Handout: Group Automorphisms

Let  $G$  be a group. Recall that, as Saracino defines on page 110, an **automorphism** of  $G$  is an isomorphism  $\phi : G \rightarrow G$ ; that is,  $\phi$  is a one-to-one and onto homomorphism from  $G$  to itself.

Clearly the identity function  $\text{id}_G : G \rightarrow G$ , given by  $\text{id}_G(g) = g$ , is an automorphism; any other automorphism is called a **nontrivial automorphism**.

**Example.** If  $G = \mathbb{Z}$ , then the function  $\psi(n) = -n$  is a nontrivial automorphism of  $\mathbb{Z}$ .

More generally:

**Theorem.** Let  $G$  be an **abelian** group. Define  $\psi : G \rightarrow G$  by  $\psi(g) = g^{-1}$ . Then  $\psi$  is an automorphism of  $G$ . If  $G$  has at least one element that is not its own inverse, then  $\psi$  is a nontrivial automorphism.

**Proof.** For any  $g, h \in G$ , we have

$$\psi(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = \psi(g)\psi(h),$$

where we used abelian-ness in the middle.

Moreover,  $\psi$  is one-to-one because for all  $g, h \in G$ , if  $g^{-1} = h^{-1}$ , then  $g = h$ .

Finally,  $\psi$  is onto because for any  $g \in G$ , we have  $\psi(g^{-1}) = g$ .

QED

In fact, one can also prove that the only two automorphisms of  $\mathbb{Z}$  are  $\text{id}_{\mathbb{Z}}$  and the above function  $\psi$ .

Here's a sketch of that proof: first, show that if  $G$  is a cyclic group,  $a \in G$  is a generator, and  $\phi$  is an automorphism of  $G$ , then  $\phi(a)$  is also a generator of  $G$ .

Second, show that if  $G$  is cyclic with generator  $a$ , then **any** homomorphism  $\phi : G \rightarrow H$  is completely determined by  $\phi(a)$ . (That is, if  $H$  is any group and  $\phi_1, \phi_2 : G \rightarrow H$  are homomorphisms with  $\phi_1(a) = \phi_2(a)$ , then  $\phi_1 = \phi_2$ .)

Finally, observe that  $\pm 1$  are the only generators of  $\mathbb{Z}$ , so there is (at most) one automorphism mapping 1 to 1 (namely  $\text{id}_{\mathbb{Z}}$ ), and (at most) one mapping 1 to  $-1$  (namely  $\psi$ ).

**Example.** You'll see on the homework that if  $G$  is an **abelian** group and  $k \in \mathbb{Z}$  is an integer, then the function  $\psi_k : G \rightarrow G$  given by  $\psi_k(g) = g^k$  is a homomorphism.

It turns out that if  $G$  is **finite and abelian**, and if  $\gcd(|G|, k) = 1$ , then  $\psi_k$  is an automorphism.

Note that  $\psi_1 = \text{id}_G$ , and that  $\psi_{-1}$  is the map  $\psi$  in the "Theorem" of the previous example.

For the case that  $G = C_n$ , the cyclic group of order  $n$ , one can show, conversely, that every automorphism of  $C_n$  is one of the functions  $\psi_k$ , where  $k \in \mathbb{Z}$  is relatively prime to  $n$ .

[Again, the proof uses the fact that an automorphism of  $C_n$  must map the generator 1 to a generator, and the automorphism is completely determined by this generator. The result follows, with a little more work, from the fact that the generators of  $C_n$  are precisely those integers in  $C_n$  that are relatively prime to  $n$ .]

Also for  $C_n$ , the functions  $\psi_k$  and  $\psi_\ell$  are the same function if and only if  $k \equiv \ell \pmod n$ . So the full set of automorphisms is the set of  $\psi_k$ 's where  $\gcd(k, n) = 1$  and  $1 \leq k \leq n$ .

More on the automorphisms of  $C_n$  in an example on the next page. . .

---

**Example.** Let  $G$  be **any** group (probably non-abelian, in fact, if what we're about to do isn't going to be totally boring), and fix an element  $a \in G$ .

Define a function  $\phi_a : G \rightarrow G$  by

$$\phi_a(g) = aga^{-1}.$$

It's not hard to show that  $\phi_a$  is an automorphism of  $G$ . (This is Exercise 12.22.)

Moreover,  $\phi_a = \text{id}_G$  if and only if  $a \in Z(G)$ . (In particular, we always get the identity map if  $G$  is abelian.)

Any automorphism  $\phi$  of  $G$  which is equal to  $\phi_a$  for some  $a \in G$  is called an **inner automorphism** of  $G$ .

---

**Definition.** Let  $G$  be a group. Define  $\text{Aut}(G)$  to be the set of all automorphisms of the group  $G$ , and  $\text{Inn}(G)$  to be the set of all inner automorphisms of  $G$ .

Please note that

$$\text{Inn}(G) \subseteq \text{Aut}(G) \subseteq S_G,$$

where (as on pages 63–64 of Saracino)  $S_G$  denotes the set of all bijective functions from  $G$  to itself (homomorphisms or not).

**Theorem.**  $\text{Inn}(G)$  and  $\text{Aut}(G)$  are subgroups of  $S_G$ . That is, they each form groups under composition.

**Proof (sketch).** Both  $\text{Inn}(G)$  and  $\text{Aut}(G)$  contain  $\text{id}_G$ . (Note that  $a = e$  makes  $\phi_e = \text{id}_G$ .) It's easy to verify that the composition of two automorphisms is an automorphism (see Theorem 12.1(ii) in Saracino). It's also easy to check that  $\phi_a \circ \phi_b = \phi_{ab}$ , so that  $\text{Inn}(G)$  is also closed under composition.

Similarly, the inverse of an automorphism is an automorphism (Theorem 12.1(iii)), and it's easy to check that  $(\phi_a)^{-1} = \phi_{(a^{-1})}$ . QED

---

By the way, we can define a function  $\Phi : G \rightarrow \text{Inn}(G)$  by  $\Phi(a) = \phi_a$ . The fact that  $\phi_a \circ \phi_b = \phi_{ab}$  means that  $\Phi$  is a homomorphism. It's easy to see that  $\Phi$  is onto. Also,  $\Phi(a) = \text{id}_G$  if and only if  $a \in Z(G)$ ; so it will follow from an upcoming result (the First Isomorphism Theorem, Theorem 13.2) that  $\text{Inn}(G) \cong G/Z(G)$ .

---

**Example.** If  $G$  is abelian, then  $\text{Inn}(G) = \{\text{id}_G\}$  is the trivial group. However,  $\text{Aut}(G)$  is generally much larger.

For example, our discussion above shows that

$$\text{Aut}(C_n) = \{\psi_k : 1 \leq k \leq n \text{ and } (k, n) = 1\}.$$

In fact,  $\psi_k \circ \psi_\ell = \psi_{k\ell}$ , which means that there is a homomorphism

$$\Psi : U_n \rightarrow \text{Aut}(C_n) \quad \text{by} \quad \Psi(k) = \psi_k,$$

where  $U_n$  is the group of integers between 1 and  $n$  relatively prime to  $n$  under multiplication modulo  $n$ .

It's easy to check that  $\Psi$  is bijective, so that  $\text{Aut}(C_n) \cong U_n$ .

Meanwhile, we also said that  $\text{Aut}(\mathbb{Z}) = \{\text{id}_g, \psi_{-1}\}$ , so that  $\text{Aut}(\mathbb{Z}) \cong C_2$ .

---

**Example.** Let  $G = V_4 = \{e, a, b, c\}$ , the Klein 4-group. Again,  $\text{Inn}(V_4)$  is trivial because  $V_4$  is abelian. However, it's not difficult to show that any permutation  $\sigma$  of  $\{e, a, b, c\}$  that leaves  $e$  fixed (i.e., such that  $\sigma(e) = e$ ) is an automorphism of  $V_4$ . For example, the transposition function  $\sigma = (a, b)$  (i.e., the function from  $V_4$  to itself that exchanges  $a$  and  $b$  but has  $\sigma(e) = e$  and  $\sigma(c) = c$ ) is an automorphism of  $V_4$ . From that, it's not too difficult to show that  $\text{Aut}(V_4) \cong S_3$ .

---

**Example.** Let  $G = S_n$ , with  $n \neq 6$ . Then it can be shown that every automorphism of  $S_n$  is an inner automorphism. That is, if  $\phi : S_n \rightarrow S_n$  is an automorphism, then there is some  $\sigma \in S_n$  such that  $\phi = \phi_\sigma$ . [This is not at all obvious. If you are curious about how this proof goes, ask me about it. You might also take a look at the [wikipedia.org](https://en.wikipedia.org/wiki/Outer_automorphism_group) entry on "Outer automorphism group".]

Moreover, for  $n \geq 3$ , the center  $Z(S_n)$  is trivial, so that for  $n \geq 3$  with  $n \neq 6$ , we have

$$\text{Aut}(S_n) = \text{Inn}(S_n) \cong S_n/Z(S_n) = S_n/\{e\} \cong S_n.$$

On the other hand, if  $n = 6$ , it turns out that there are automorphisms of  $S_6$  that are not inner automorphisms. [This is *really* not obvious.] Essentially, the reason this is possible is that  $S_6$  has exactly 15 permutations of the form  $(x_1, x_2)(x_3, x_4)(x_5, x_6)$  (i.e., three disjoint 2-cycles), and exactly 15 2-cycles, which opens the door for automorphisms that exchange these two conjugacy classes. (No other  $S_n$  for  $n \geq 2$  has the same number of 2-cycles as some other conjugacy class of permutations.) It turns out that  $\text{Inn}(S_6)$  has index 2 in  $\text{Aut}(S_6)$ .

---

**Example.** The alternating group  $A_n$  has trivial center  $Z(A_n) = \{e\}$  (at least for  $n \geq 4$ ; note that  $A_2 = \{e\}$  and  $A_3 \cong C_3$  are abelian), so that  $\text{Inn}(A_n) \cong A_n$ .

However,  $A_n$  has other automorphisms coming from the fact that  $A_n$  is itself a normal subgroup of  $S_n$ . That is, if  $f \in S_n$  is an **odd** permutation and if  $\sigma \in A_n$ , then  $f\sigma f^{-1} \in A_n$ . Thus, the inner (for  $S_n$ ) automorphism  $\phi_f$  of  $S_n$ , when restricted to the smaller domain  $A_n$ , gives a **non-inner** (for  $A_n$ ) automorphism  $\phi_f|_{A_n}$  of  $A_n$ .

So for  $n \geq 4$ ,  $A_n$  has

$$\text{Aut}(A_n) \supsetneq \text{Inn}(A_n) \cong A_n.$$

(And  $\text{Aut}(A_3) \cong \text{Aut}(C_3) \cong U_3 \cong C_2$ , since  $A_3 \cong C_3$ .)

In all of the above examples, we either had  $\text{Aut}(G) = \text{Inn}(G)$  or  $\text{Inn}(G) = \{\text{id}_G\}$  or  $Z(G) = \{e\}$ . However, “most” of the time, none of these equalities holds; they are usually all proper containments of sets.

**Example.** Let  $G = D_4$ . Then  $Z(D_4) = \langle f^2 \rangle = \{e, f^2\}$ , so that  $\text{Inn}(D_4) \cong D_4/\langle f^2 \rangle \cong V_4$ .

Meanwhile,  $|\text{Aut}(D_4)| = 8$ . In fact,  $f$  can be mapped to either  $f$  or  $f^{-1}$ , and  $g$  can be mapped to any of the four elements  $f^i g$  by an automorphism. That is, for each of the  $2 \cdot 4$  choices of where to map  $f$  and  $g$  just described, there is exactly one such automorphism of  $D_4$ . (In fact, it can be shown that  $\text{Aut}(D_4) \cong D_4$ .)

So  $\text{Aut}(D_4) \supsetneq \text{Inn}(D_4)$ , and  $\text{Inn}(D_4) \supsetneq \{\text{id}_G\}$ , and  $Z(D_4) \supsetneq \{e\}$ .

**Theorem.** Let  $G$  be a group. Then  $\text{Inn}(G) \triangleleft \text{Aut}(G)$ .

**Proof.** Given  $\phi \in \text{Inn}(G)$  and  $\psi \in \text{Aut}(G)$ . Then there is some  $a \in G$  such that  $\phi = \phi_a$ . We claim that

$$\psi \circ \phi \circ \psi^{-1} = \phi_b, \quad \text{where } b = \psi(a).$$

The Theorem will then follow immediately.

For any  $x \in G$ , noting that  $a = \psi^{-1}(b)$ , we compute:

$$\psi \circ \phi \circ \psi^{-1}(x) = \psi(a\psi^{-1}(x)a^{-1}) = \psi\left(\psi^{-1}(b)\psi^{-1}(x)\psi^{-1}(b^{-1})\right) = \psi(\psi^{-1}(bxb^{-1})) = bxb^{-1}.$$

QED

Thus, we can form the quotient group  $\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)$  of **outer automorphisms**. Please note that an element of  $\text{Out}(G)$  is not itself an automorphism; rather, it is a coset of automorphisms for the subgroup  $\text{Inn}(G)$  of inner automorphisms.

[However, we sometimes abuse language and call an element of  $\text{Aut}(G)$  which is not in  $\text{Inn}(G)$  an outer automorphism. For example, it can be shown that  $\text{Out}(S_6) \cong C_2$ . That is, technically speaking, there is exactly one nontrivial **coset** of outer automorphisms of  $S_6$ . But mathematicians will often refer to “the” nontrivial outer automorphism of  $S_6$ , though of course they know that they really mean a whole coset worth of non-inner automorphisms.]