Math 350, Sections 01,03, Fall 2021

Optional Handout: Group Automorphisms

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

Clearly the identity function $\mathrm{id}_G : G \to G$, given by $\mathrm{id}_G(g) = g$, 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 $\psi : G \to G$ by $\psi(g) = g^{-1}$. Then ϕ is an automorphism of G. If G has at least one element that is not its own inverse, then ϕ is a nontrivial automorphism.

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

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

where we used abelian-ness in the middle.

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

Finally, ψ 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 $\mathrm{id}_{\mathbb{Z}}$ and the above function ψ.

Here's a sketch of that proof: first, show that if G is a cyclic group, $a \in G$ is a generator, and ϕ 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 $\phi : G \to H$ is completely determined by $\phi(a)$. (That is, if H is any group and $\phi_1, \phi_2 : G \to H$ are homomorphisms with $\phi_1(a) = \phi_2(a)$, then $\phi_1 = \phi_2$.)

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

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 $\psi_k : G \to G$ 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 ψ_k is an automorphism.

Note that $\psi_1 = \mathrm{id}_G$, and that ψ_{-1} is the map ψ 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 ψ_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 ψ_k and ψ_ℓ are the same function if and only if $k \equiv \ell \bmod n$. So the full set of automorphisms is the set of ψ_k's where $\gcd(k, n) = 1$ and $1 \leq k \leq n$.

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 $\phi_a : G \to G$ by

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

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

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

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

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

Please note that

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

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

Proof (sketch). Both $\mathrm{Inn}(G)$ and $\mathrm{Aut}(G)$ contain id_G. (Note that $a = e$ makes $\phi_e = \mathrm{id}_G$).

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

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

For example, our discussion above shows that

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

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

$$\Psi : U_n \to \mathrm{Aut}(C_n) \qquad \text{by} \qquad \Psi(k) = \psi_k,$$

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 Ψ is bijective, so that $\mathrm{Aut}(C_n) \cong U_n$.

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

Example. Let $G = V_4 = \{e, a, b, c\}$, the Klein 4-group. Again, $\mathrm{Inn}(V_4)$ is trivial because V_4 is abelian. However, it's not difficult to show that any permutation σ 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 $\mathrm{Aut}(V_4) \cong S_3$.

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 $\phi : S_n \to S_n$ 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` entry on "Outer automorphism group".]

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

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

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 $n \ge 2$ has the same number of 2-cycles as some other conjugacy class of permutations.) It turns out that $\mathrm{Inn}(S_6)$ has index 2 in $\mathrm{Aut}(S_6)$.

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 $\operatorname{Inn}(A_n) \cong A_n$.

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 ϕ_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

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

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

In all of the above examples, we either had $\operatorname{Aut}(G) = \operatorname{Inn}(G)$ or $\operatorname{Inn}(G) = \{\mathrm{id}_G\}$ 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 $\operatorname{Inn}(D_4) \cong D_4/\langle f^2 \rangle \cong V_4$.

Meanwhile, $|\operatorname{Aut}(D_4)| = 8$. 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 $\operatorname{Aut}(D_4) \cong D_4$.)

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

Theorem. Let G be a group. Then $\operatorname{Inn}(G) \lhd \operatorname{Aut}(G)$.

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

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

The Theorem will then following immediately.

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

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

QED

Thus, we can form the quotient group $\operatorname{Out}(G) = \operatorname{Aut}(G)/\operatorname{Inn}(G)$ of **outer automorphisms**.

Please note that an element of $\operatorname{Out}(G)$ is not itself an automorphism; rather, it is a coset of automorphisms for the subgroup $\operatorname{Inn}(G)$ of inner automorphisms.

[However, we sometimes abuse language and call an element of $\operatorname{Aut}(G)$ which is not in $\operatorname{Inn}(G)$ an outer automorphism. For example, it can be shown that $\operatorname{Out}(S_6) \cong C_2$. 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.]