11-4-1993

Automorphism groups.

Definition. An **automorphism** of a group G is an isomorphism $G \to G$. The set of automorphisms of G is denoted $\operatorname{Aut} G$.

Examples.

1. The identity map $\mathrm{id} : G \to G$ is an automorphism. $\square$

2. There are two automorphisms of $\mathbb{Z}$: the identity map and the map $\mu : \mathbb{Z} \to \mathbb{Z}$ given by $\mu(x) = -x$. For $\mathbb{Z}$ is cyclic, and an isomorphism $\mathbb{Z} \to \mathbb{Z}$ must carry a generator to a generator. Since the only generators of $\mathbb{Z}$ are 1 and -1, the only automorphisms are the maps sending $1 \mapsto 1$ and $1 \mapsto -1$. $\square$

The inverse map which appeared in the last example is a special case of the following result.

Lemma. Let G be an abelian group. The map $\mu : G \to G$ given by $\mu(x) = -x$ is an automorphism.

Proof. μ is a homomorphism, since

$$\mu(x + y) = -(x + y) = -x - y = \mu(x) + \mu(y).$$

Clearly, $\mu \cdot \mu(x) = x$, so μ is its own inverse. Since μ is an invertible homomorphism, it's an isomorphism. $\square$

Remark. Note that if G is not abelian,

$$\mu(xy) = y^{-1}x^{-1} \neq x^{-1}y^{-1} = \mu(x)\mu(y). \ \square$$

Lemma. Let G be a group, and let $g \in G$. The map $i_g : G \to G$ given by

$$i_g(x) = gxg^{-1}$$

is an automorphism of G. (It is called **conjugation** by g, or the **inner automorphism** corresponding to g.)

Proof. i_g is a homomorphism, since

$$i_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = i_g(x)i_g(y).$$

The inner automorphism $i_{g^{-1}}(x) = g^{-1}xg$ clearly inverts i_g. Since i_g is an invertible homomorphism, it's an automorphism. $\square$

Notation. The set of inner automorphisms of G is denoted $\operatorname{Inn} G$. $\square$

Remark. If G is abelian, then

$$i_g(x) = gxg^{-1} = gg^{-1}x = x = \mathrm{id}(x).$$

That is, in an abelian group the inner automorphisms are trivial.
More generally, $i_g = \mathrm{id}$ if and only if $g \in Z(G)$. $\square$

Proposition. $\operatorname{Aut} G$ is a group under function composition.

Proof. The composite of homomorphisms is a homomorphism, and the composite of bijections is a bijection. Therefore, the composite of isomorphisms is an isomorphism, and in particular, the composite of automorphisms is an automorphism. Hence, composition is a well-defined binary operation on $\operatorname{Aut} G$.

Composition of functions is always associative. The identity map is an automorphism of G. Finally, an isomorphism has an inverse which is an isomorphism, so the inverse of an automorphism of G exists and is an automorphism of G. $\square$

Example. From an earlier example, $\operatorname{Aut}\mathbb{Z}$ has order 2. Since there is only one group of order 2, $\operatorname{Aut}\mathbb{Z} \approx \mathbb{Z}_2$. $\square$

Lemma. $\operatorname{Inn} G \lhd \operatorname{Aut} G$.

Proof. First, I need to show that $\operatorname{Inn} G$ is a subgroup. Since $\mathrm{id} = i_1 \in \operatorname{Inn} G$, $\operatorname{Inn} G \neq \emptyset$.

Now suppose $i_g, i_h \in \operatorname{Inn} G$. Then $(i_h)^{-1} = i_{h^{-1}}$, so

$$i_g(i_h)^{-1}(x) = i_g\left(i_{h^{-1}}(x)\right) = g\left(i_{h^{-1}}(x)\right)g^{-1} = gh^{-1}xhg^{-1} = i_{gh^{-1}}(x).$$

Therefore, $i_g(i_h)^{-1} = i_{gh^{-1}} \in \operatorname{Inn} G$, so $\operatorname{Inn} G < \operatorname{Aut} G$.

For normality, suppose $g \in G$ and $\phi \in \operatorname{Aut} G$. Then

$$\phi i_g \phi^{-1}(x) = \phi\left(g\phi^{-1}(x)g^{-1}\right) = \phi(g)x\phi(g^{-1}) = \phi(g)x\phi(g)^{-1} = i_{\phi(g)}(x).$$

Since $\phi i_g \phi^{-1} = i_{\phi(g)} \in \operatorname{Inn} G$, it follows that $\operatorname{Inn} G$ is normal. $\square$

Proposition. The map $\phi : G \to \operatorname{Aut} G$ given by $\phi(g) = i_g$ is a homomorphism onto the subgroup of inner automorphisms of G.

Proof. Obviously, ϕ maps onto $\operatorname{Inn} G$. I must verify that it is a homomorphism.

$$\phi(g)\phi(h)(x) = i_g i_h(x) = i_g\left(hxh^{-1}\right) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = i_{gh}(x) = \phi(gh)(x). \square$$

Corollary. $G/Z(G) \approx \operatorname{Inn} G$.

Proof. The preceding proposition gives a surjective map $\phi : G \to \operatorname{Inn} G$. I only need to verify that $\ker\ \phi = Z(G)$.

First, suppose $g \in Z(G)$. Then

$$\phi(g)(x) = i_g(x) = gxg^{-1} = gg^{-1}x = x = \mathrm{id}(x).$$

Since $\phi(g) = \mathrm{id}$, $g \in \ker\ \phi$.

Conversely, suppose $g \in \ker\ \phi$. Then $\phi(g) = \mathrm{id}$, so $i_g = \mathrm{id}$. Applying both sides to $x \in G$,

$$i_g(x) = x, \quad gxg^{-1} = x, \quad \text{or} \quad gx = xg.$$

Since x was arbitrary, g commutes with everything, so $g \in Z(G)$. Hence, $\ker\ \phi = Z(G)$ as claimed.

Finally, $G/Z(G) \approx \operatorname{Inn} G$ by the First Isomorphism Theorem. $\square$

Examples.

1. If G is abelian, $G = Z(G)$, so $\operatorname{Inn} G = \{1\}$, as noted earlier. $\square$

2. Let $G = S_3$. $Z(S_3) = \{\mathrm{id}\}$, so $|S_3/Z(S_3)| = 6$. Thus, there are 6 inner automorphisms of S_3: different elements of S_3 give rise to distinct inner automorphisms.

You can verify that

$$i_{(1\ 3)}i_{(1\ 2)}(1\ 2) = (2\ 3) \text{ and } i_{(1\ 2)}i_{(1\ 3)}(1\ 2) = (1\ 3).$$

That is, $i_{(1\ 3)}i_{(1\ 2)} \neq i_{(1\ 2)}i_{(1\ 3)}$. It follows that $\operatorname{Inn} S_3$ is a nonabelian group of order 6. Therefore, $\operatorname{Inn} S_3 \approx S_3$. $\square$

Proposition. Let $G = \langle a \rangle$.

1. If $\phi : G \to G$ is an automorphism, then $\phi(a)$ is a generator of G.
2. If b is a generator of G, there is a unique automorphism $\phi : G \to G$ such that $\phi(a) = b$.

Proof.

1. Let $\phi : G \to G$ be an automorphism, and let $g \in G$. Since $\phi^{-1}(g) \in G = \langle a \rangle$, it follows that $\phi^{-1}(g) = a^n$ for some $n \in \mathbb{Z}$. Then $g = \phi(a^n) = \phi(a)^n$. Since every element of G can be expressed as a power of $\phi(a)$, $\phi(a)$ generates G.

2. Suppose b generates G. Define $\phi : G \to G$ by $\phi(a^n) = b^n$ for all $n \in \mathbb{Z}$.

I want to cite an earlier result that says a homomorphism out of a cyclic group is determined by sending a generator somewhere. If G is infinite cyclic, I may send the generator wherever I please, and so ϕ is a well defined homomorphism.

If G is cyclic of order n, then I must be careful to map the generator a to an element that is killed by n. But b is a generator, so it has order n as Again, the result applies to show that ϕ is a well defined homomorphism.

In both cases, the earlier result says that the map ϕ is unique.

Next, observe that ϕ is invertible. In fact, the map $\psi(b^n) = a^n$ clearly inverts ϕ, and it is well-defined by the same argument which showed that ϕ was well-defined. Since ϕ is an invertible homomorphism from G onto G, it is an automorphism of G. $\square$

This result gives us a way of computing $\operatorname{Aut} \mathbb{Z}_n$: Simply fix a generator and count the number of places where it could go.

Definition. Let $n \geq 1$ be an integer. The **Euler phi-function** $\phi(n)$ is the number of elements in $\{1, \ldots, n\}$ which are relatively prime to n.

Example. $\phi(12) = 4$. $\phi(25) = 20$. $\square$

Corollary. $|\operatorname{Aut} \mathbb{Z}_n| = \phi(n)$.

Proof. By an earlier result, the order of $m \in \mathbb{Z}_n$ is $\dfrac{n}{(m,n)}$. A generator of $\mathbb{Z}_n$ must have order n, and this evidently occurs exactly when $(m,n) = 1$. Now $1 \in \mathbb{Z}_n$ always generates, and the Proposition I just proved implies there is exactly one automorphism of $\mathbb{Z}_n$ for each generator (i.e. for each possible target for 1 under an automorphism). $\square$

How do you compute $\phi(n)$? Next on the agenda is a formula for $\phi(n)$ in terms of the prime factors of n.

Lemma. If p is prime, then $\phi(p) = p - 1$.

Proof. The numbers $\{1, \ldots, p-1\}$ are relatively prime to p. $\square$

Lemma. Let p be prime, and let $n \geq 1$. Then $\phi(p^n) = p^n - p^{n-1}$.

Proof. The numbers in $\{1, \ldots, p^n\}$ which are *not* relatively prime to p^n are exactly the numbers divisible by p. These are

$$p \cdot 1, p \cdot 2, \ldots, p \cdot p^{n-1}.$$

There are p^{n-1} numbers which are *not* relatively prime to p^n, so there are $p^n - p^{n-1}$ which are. $\square$

Example. $\phi(9) = 9 - 3 = 6$. Therefore, $|\operatorname{Aut} \mathbb{Z}_9 = 6$. $\square$

Theorem. If $m, n > 0$ and $(m,n) = 1$, then

$$\phi(mn) = \phi(m)\phi(n).$$

Proof. Write down the integers from 1 to mn:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \dots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \dots & (n-1)m+2 \\ 3 & m+3 & 2m+3 & \dots & (n-1)m+3 \\ \vdots & \vdots & \vdots & & \vdots \\ m & 2m & 3m & \dots & mn \end{array}$$

I'm going to find the numbers which are relatively prime to mn.

First, I only need to look in rows whose row numbers are relatively prime to m. For suppose row i has $(m, i) = k > 1$. Since $k \mid m$ and $k \mid i$, it follows that $k \mid am + i$ (a general element of the i-th row). Since $k \mid m \mid mn$, $k \mid (am + i, mn)$, so $(am + i, mn) \neq 1$.

Therefore, look at rows i for which $(i, m) = 1$. Note that there are $\phi(m)$ such rows.

First, observe $am + i \neq bm + i \bmod n$. Assume without loss of generality that $a > b$. Then

$$(am + i) - (bm + i) = (a - b)m.$$

Now if $n \mid (a - b)m$, then $n \mid (a - b)$, since $(m, n) = 1$. However, $a - b < n$, so this is impossible $\times$.

It follows that the elements of a row are distinct mod n. However, each row has n elements, so mod n each row reduces to $\{0, 1, \dots, n - 1\}$. Hence, exactly $\phi(n)$ elements in each row are relatively prime to n.

The elements relatively prime to mn are therefore the $\phi(n)$ elements in the $\phi(m)$ rows whose row numbers are relatively prime to m. Hence, $\phi(mn) = \phi(m)\phi(n)$. $\square$

Corollary. Let $n = p_1^{e_1} \cdots p_m^{e_m}$ be the prime factorization of n. Then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$

Proof. If $m = 1$, the result says $\phi(p^n) = p^n\left(1 - \dfrac{1}{p}\right)$, which follows from an earlier result.

Let $m > 1$, and assume the result is true when n is divisible by fewer than m primes. Suppose that $n = p_1^{e_1} \cdots p_m^{e_m}$ is the prime factorization of n. Then

$$\phi(n) = \phi\left(p_1^{e_1} \cdots p_{m-1}^{e_{m-1}}\right)\phi(p_m^{e_m}) = \left(\prod_{i=1}^{m-1} p_i^{e_i}\right)\left(\prod_{i=1}^{m-1}\left(1 - \frac{1}{p_i}\right)\right)\left(p^m\left(1 - \frac{1}{p_m}\right)\right) = n\prod_{i=1}^{m}\left(1 - \frac{1}{p_i}\right).$$

This establishes the result by induction. $\square$

Example. $|\operatorname{Aut} \mathbb{Z}_{11}| = 10$. In fact, there are two groups of order 10: $\mathbb{Z}_{10}$ and D_5, the group of symmetries of the regular pentagon.

I'll digress a little here and prove part of this claim: namely, that an *abelian* group of order 10 is isomorphic to $\mathbb{Z}_{10}$.

As in most extended proofs of this sort, you should try to get a feel for the *kinds* of techniques involved. Each classification problem of this kind presents its own difficulties, so there is not question of "memorizing" some kind of general method: there isn't any!

Suppose then that G is abelian. I claim G is cyclic. Suppose not. Then every element of G has order 2 or order 5.

I claim that there is an element of order 5 and an element of order 2. First, suppose every element besides 0 has order 2. Consider distinct elements a and b, $a, b \neq 0$. Look at the subgroup $\langle a, b\rangle$. I'll show that

$$\langle a, b\rangle = \{0, a, b, a + b\}.$$

Since $2a = 2b = 0$, it is easy to see by checking cases that this set is closed. However, a subset of a finite group closed under the operation is a subgroup.

Now I have a contradiction, since this putative subgroup has order 4, which does not divide 10. It follows that there must be an element of order 5.

On the other hand, could G contain *only* elements of order 5? Let a have order 5, and let b be an element of order 5 which is not in $\langle a \rangle$. Since $|\langle a \rangle \cap \langle b \rangle|$ divides $|\langle a \rangle| = 5$, it must be either 1 or 5. If it is 5, then $\langle a \rangle = \langle b \rangle$, which is impossible (since $b \notin \langle a \rangle$) $\times$. Therefore, $|\langle a \rangle \cap \langle b \rangle| = 1$, and so $\langle a \rangle \cap \langle b \rangle = \{0\}$. This accounts for $4 + 4 + 1 = 9$ elements of G. The remaining element must generate a subgroup of order 5, which (by the preceding argument) intersect $\langle a \rangle$ and $\langle b \rangle$ in exactly $\{0\}$. We now have at least 13 elements in G $\times$.

The preceding arguments show that G must contain an element a of order 2 and an element b of order 5. I will now show that G is the internal direct product of $\langle a \rangle$ and $\langle b \rangle$.

Since $|\langle a \rangle \cap \langle b \rangle|$ must divide both 2 and 5, it can only be 1. Therefore, $\langle a \rangle \cap \langle b \rangle = \{0\}$.

Since G is abelian, $\langle a \rangle$ and $\langle b \rangle$ are automatically normal.

Finally, I claim that $G = \langle a \rangle + \langle b \rangle$. To see this, I need only show that the right side has order 10. This will be true if the following elements are distinct:

$$S = \{ma + nb \mid 0 \le m \le 1,\ 0 \le n \le 4\}.$$

Suppose then that $pa + qb = ra + sb$, where $0 \le p, r \le 1$ and $0 \le q, s \le 1$. Then

$$(p - r)a = (q - s)b \in \langle a \rangle \cap \langle b \rangle = \{0\}.$$

Therefore, $2 \mid p - r$ and $5 \mid q - s$, which (given the ranges for these parameters) force $p = r$ and $q = s$.

It follows that the elements of S are distinct, so

$$10 = |S| \le |\langle a \rangle + \langle b \rangle|.$$

Obviously, this forces $G = \langle a \rangle + \langle b \rangle$.

Therefore, $G \approx \langle a \rangle \times \langle b \rangle$, and $G \approx \mathbb{Z}_{10}$. □

The group of automorphisms $\operatorname{Aut} G$ is an important group which is contructed from a given group. In case $G = \mathbb{Z}_n$, there's another one, which turns out to be related to $\operatorname{Aut} \mathbb{Z}_n$.

Definition. $U(n)$ is the set of numbers in $\{1, \ldots, n\}$ relatively prime to n.

Example. $U(9) = \{1, 2, 4, 5, 7, 8\}$. □

Lemma. $U(n)$ is a group under multiplication mod n.

Proof. If x and y are relatively prime to n, then $(x, n) = 1$ and $(y, n) = 1$. Therefore, there are numbers a, b, c, d such that

$$1 = ax + bn, \qquad 1 = cy + dn.$$

Multiply the two equations:

$$1 = ac(xy) + (axd + bcy + bdn)n.$$

It follows that $(xy, n) = 1$, so the product of two elements of $U(n)$ is again an element of $U(n)$.

Multiplication of integers mod n is associative, and since 1 is relatively prime to n, it will serve as the identity.

Finally, suppose $(x, n) = 1$. Write $ax + bn = 1$. Reducing the equation mod n, I get $ax = 1 \bmod n$. Therefore, x has a multiplicative inverse mod n, namely a (possibly reduced mod n to lie in $U(n)$).

This shows that $U(n)$ is a group under multiplication mod n. □

Clearly, $|U(n)| = \phi(n)$. But $|\operatorname{Aut} \mathbb{Z}_n| = \phi(n)$. The answer to the obvious question is: "Yes".

Theorem. $\operatorname{Aut} \mathbb{Z}_n \approx U(n)$.

Proof. Define $\phi : U(n) \to \operatorname{Aut} \mathbb{Z}_n$ by

$$\phi(a) = \tau_a,$$

where τ_a is the unique automorphism of $\mathbb{Z}_n$ which maps 1 to a. I showed earlier that this *does* indeed give rise to a unique automorphism, and that every automorphism of $\mathbb{Z}_n$ arises in this way. It follows that ϕ is a well-defined one-to-one correspondence. I need only show that ϕ is a homomorphism.

Let $a, b \in U(n)$. Then $\phi(ab) = \tau_{ab}$, where τ_{ab} is the map sending 1 to ab. I must show that this is the same as $\phi(a)\phi(b) = \tau_a\tau_b$.

To do this, consider the effect of the two maps on $m \in \mathbb{Z}_n$. $\tau_{ab}(m) = mab$, since τ_{ab} sends 1 to ab and τ_{ab} is a homomorphism.

On the other hand,

$$\tau_a\tau_b(m) = \tau_a(mb) = mba,$$

since τ_b sends 1 to b and τ_a sends 1 to a, and since they're both homomorphisms. Therefore, the maps are equal, and ϕ is a homomorphism — hence, an isomorphism. $\square$

Example. $\operatorname{Aut}\mathbb{Z}_{10} \approx U(10) = \{1, 3, 7, 9\}$

There are only two groups of order 4: $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. Notice that $3^2 = 9 \bmod 10$. Since 3 does not have order 2, it follows that $\operatorname{Aut}\mathbb{Z}_{10} \not\approx \mathbb{Z}_2 \times \mathbb{Z}_2$. Therefore, $\operatorname{Aut}\mathbb{Z}_{10} \approx \mathbb{Z}_4$. $\square$