Math 417 – Sixteenth Day

Bruce Reznick
University of Illinois at Urbana-Champaign

September 30, 2020

Today a few more comments about automorphisms and then another nice group.

Recall that if G is a group, then an automorphism Φ is a bijection from G to itself that preserves the operation: for $g, h \in G$,

$$\Phi(gh) = \Phi(g)\Phi(h)$$

I talked about the automorphisms of V, and now I'd like to be precise. We have $V = \{I, X, Y, Z\}$, where I is the identity and $X^2 = Y^2 = Z^2 = I$ and $XY = YX = Z$, $XZ = ZX = Y$ and $YZ = ZY = X$.

If Φ is an automorphism, then it has to take the identity to the identity, so $\Phi(I) = I$. Suppose π is any permutation of $\{X, Y, Z\}$; that is, $\{\pi(X), \pi(Y), \pi(Z)\} = \{X, Y, Z\}$, then the map defined by

$$\Phi(I) = I, \quad \Phi(X) = \pi(X), \quad \Phi(Y) = \pi(Y), \quad \Phi(Z) = \pi(Z)$$

is an automorphism.

From its definition, Φ is a bijection of $\{I, X, Y, Z\}$ to itself. Now we have to check the operation: $\Phi(uv) = \Phi(u)\Phi(v)$ for all choices of $u, v \in V$.

Since $\Phi(I) = I$, this is automatic when one of u, v equals I. Otherwise, suppose $u = v \in \{X, Y, Z\}$. Then

$$\Phi(u^2) = \Phi(I) = I; \quad \Phi(u)\Phi(u) = (\pi(u))^2 \in \{X^2, Y^2, Z^2\} = \{I\},$$

so $\Phi(u^2) = (\Phi(u))^2$ as we wanted. Finally, suppose $u \neq v$, $u, v \in \{X, Y, Z\}$. If we write w as the third element, so that $\{u, v, w\} = \{X, Y, Z\}$, then $w = uv$, and we need to show that

$$\pi(w) = \Phi(w) = \Phi(uv) = \Phi(u)\Phi(v) = \pi(u)\pi(v).$$

But $\{\pi(X), \pi(Y), \pi(Z)\} = \{X, Y, Z\}$, so no matter which π we choose, this equation will be correct.

Now I would like to talk generally about automorphisms. Fix a group G.

LEMMA If Φ is an automorphism of G, then so is Φ^{-1}.

PROOF Since $\Phi : G \to G$, its inverse is defined: $\Phi^{-1} : G \to G$. We need to check the operation. This is just "symbol-pushing". We need to show that, for every $g_1, g_2 \in G$,

$$\Phi^{-1}(g_1 g_2) = \Phi^{-1}(g_1)\Phi^{-1}(g_2).$$

To prove this, write $h_1 = \Phi^{-1}(g_1)$ and $h_2 = \Phi^{-1}(g_2)$ (we can do this because Φ is surjective.) Then what we need to prove is that

$$\Phi^{-1}(\Phi(h_1)\Phi(h_2)) = \Phi^{-1}(\Phi(h_1))\Phi^{-1}(\Phi(h_2)) = h_1 h_2.$$

But Φ is an automorphism, so $\Phi(h_1)\Phi(h_2) = \Phi(h_1 h_2)$, and this becomes

$$\Phi^{-1}(\Phi(h_1 h_2)) = h_1 h_2,$$

which is true by definition. $\square$.

Suppose now that Φ_1 and Φ_2 are two automorphisms of G. Then we can compose them. For $g \in G$, let

$$\Phi(g) = \Phi_1(\Phi_2(g))$$

THEOREM The composition map Φ is also an automorphism of G.

PROOF Since Φ_1 and Φ_2 are bijections, their composition is also a bijection. Here's a quick proof. First, injection

$$\Phi(g) = \Phi(h) \iff \Phi_1(\Phi_2(g)) = \Phi_1(\Phi_2(h))$$
$$\iff \Phi_2(g) = \Phi_2(h) \iff g = h.$$

(This uses the facts that Φ_1 and Φ_2 are both injective.)

For surjectivity, suppose $g_0 \in G$. Then by the surjectivity of Φ_1 and Φ_2, there exists $g_1 \in G$ so that $\Phi_1(g_1) = g_0$ and there exists $g_2 \in G$ so that $\Phi_2(g_2) = g_1$, hence

$$\Phi(g_2) = \Phi_1(\Phi_2(g_2)) = \Phi_1(g_1) = g_0.$$

That is, Φ is surjective and so it's a bijection.

The other part is showing that Φ is a homomorphism, but we just proved last week that the composition of two homomorphisms is a homomorphism last week, except that we had one from G to H and another one from H to K. Apply that result, but assume $K = H = G$. □

The set of automorphisms of a group G is denoted $Aut(G)$, and called the *automorphism group* of G.

THEOREM Under the operation of composition:

$$(\Phi_1 * \Phi_2)(g) := \Phi_1(\Phi_2(g)) \quad \text{for } g \in G,$$

$Aut(G)$ is a group.

PROOF We have just shown that if $\Phi_1, \Phi_2 \in Aut(G)$ implies that $\Phi_1 * \Phi_2 \in Aut(G)$, so $*$ is a binary operation.

The identity map $\Phi_0(g) = g$ is the trivial automorphism, and so is in $Aut(G)$. It also has the pleasant composition property that $\Phi * \Phi_0 = \Phi_0 * \Phi = \Phi$ for $\Phi \in Aut(G)$, so it is the identity element.

By the lemma, $\Phi \in Aut(G)$, then $\Phi^{-1} \in Aut(G)$ and by the definition of the operation,

$$(\Phi * \Phi^{-1})(g) = \Phi(\Phi^{-1}(g)) = g = \Phi_0(g),$$

so the functional inverse is the inverse in $Aut(G)$.

Finally, we need to check associativity. As usual, for any $\Phi_j \in Aut(G)$ and $g \in G$,

$$((\Phi_1 * \Phi_2) * \Phi_3)(g) = (\Phi_1 * \Phi_2)(\Phi_3(g)) = \Phi_1(\Phi_2(\Phi_3(g)))$$
$$(\Phi_1 * (\Phi_2 * \Phi_3))(g) = \Phi_1(\Phi_2(\Phi_3(g))) = ((\Phi_1 * \Phi_2) * \Phi_3)(g).$$

Thus, Aut(G) is a group. □

We can combine a lot of what we've done this semester into one theorem.

THEOREM Let $G = C_n$. Then $Aut(G)$ is isomorphic to $((\mathbb{Z}/n\mathbb{Z})^*, \odot)$, so

$$|Aut(C_n)| = \phi(n),$$

where ϕ is the Euler phi-function.

PROOF Write $G = \langle a \rangle, a^n = e$. If $\Phi \in Aut(G)$, then $\Phi(e) = e$. Since $\Phi(a) \in G$, we have $\Phi(a) = a^k$ for some $k \in \{0, \ldots, n-1\}$. We know that for every k, Φ is a homomorphism defined by

$$\Phi_k(a^r) = a^{kr}$$

(Take our result about homomorphisms from C_n to C_m with $m = n$; we need k to be divisible by $n/gcd(n,n) = n/n = 1$, which is no condition at all.)

What we need to check is whether Φ_k is a bijection. If Φ_k is a bijection, then there exists $g = a^s \in C_n$ so that $a = \Phi_k(a^s) = a^{ks}$. This implies that $ks \equiv 1 \mod n$, which implies that $gcd(k,n) = 1$, and s is just the inverse of k mod n. And if $gcd(k,n) = 1$, such an s exists.

So far, we've shown that there is $g \in C_n$ so that $\Phi_k(g) = a$ if and only if $gcd(k,n) = 1$. But if $\Phi_k(g) = a$, then $\Phi_k(g^i) = \Phi_k(a^{si}) = a^i$. To expand that out a bit:

$$\Phi_k(a^{si}) = a^{ski} = (a^{sk})^i = a^i.$$

Therefore,

$$Aut(C_n) = \{\Phi_k \mid gcd(k,n) = 1\}$$

How do these combine? Suppose $\Phi_j, \Phi_k \in Aut(C_n)$. Then

$$(\Phi_j * \Phi_k)(a) = \Phi_j(\Phi_k(a)) = \Phi_j(a^k) = (a^k)^j = a^{jk} = \Phi_{jk}(a).$$

That is, $\Phi_j * \Phi_k = \Phi_{jk}$, and $gcd(j,n) = gcd(k,n) = 1$.

This looks a great deal like $((\mathbb{Z}/n\mathbb{Z})^*, \odot)$! To make this precise, define $\Psi : Aut(C_n) \to ((\mathbb{Z}/n\mathbb{Z})^*, \odot)$ in the only reasonable way:

$$\Psi(\Phi_k) = [k]_n.$$

The previous discussions have hopefully made it clear that Ψ is a bijection: $\Phi_k \in Aut(C_n)$ if and only if $[k]_n \in (\mathbb{Z}/n\mathbb{Z})^*$, so all we have to check is the operation, and

$$\Psi(\Phi_j * \Phi_k) = \Psi(\Phi_{jk}) = [jk]_n = [j]_n[k]_n = \Psi(\Phi_j) \odot \Psi(\Phi_k).$$

Thus, Ψ is the desired isomorphism.

Since $(\mathbb{Z}/n\mathbb{Z})^*$ has $\phi(n)$ elements, where ϕ is the Euler phi function, if follows that $|Aut(C_n)| = |(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$. □

As a remark, lots of times, isomorphisms are easy to check, once you understand the groups involved.

Let's do a few examples here, for $n = 11$ and $n = 12$.

First, since 11 is prime, $\phi(11) = 11 - 1 = 10$ and all possible nontrivial homomorphisms from $C_{11} = \langle a \rangle, a^{11} = e$ to itself are automorphisms:

$$\Phi_k(a) = a^k, \qquad a \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

As we have seen, $[2]_{11}$ is a generator of $((\mathbb{Z}/11\mathbb{Z})^*, \odot)$; that is, the powers of $[2]_{11}$ give the entire group. I list $[2^i]_{11}$ below:

$$[1]_{11}, [2]_{11}, [4]_{11}, [8]_{11}, [5]_{11}, [10]_{11}, [9]_{11}, [7]_{11}, [3]_{11}, [6]_{11}.$$

By the isomorphism, the powers of Φ_2 generate $Aut(C_{11})$:

$$\Phi_1, \Phi_2, \Phi_4, \Phi_8, \Phi_5, \Phi_{10}, \Phi_9, \Phi_7, \Phi_3, \Phi_6.$$

Powers here mean under composition, so $\Phi_8 = \Phi_2^3$ means that

$$\Phi_2(\Phi_2(\Phi_2(a))) = \Phi_2(\Phi_2(a^2)) = \Phi_2(a^4) = a^8 = \Phi_8(a).$$

On the other hand, we saw about a month ago that $\phi(12) = 4$ and $((\mathbb{Z}/12\mathbb{Z})^*, \odot)$ is isomorphic to V. To be specific, the elements of $(\mathbb{Z}/12\mathbb{Z})^*$ are:

$$[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}.$$

What does $Aut(C_{12})$ look like?

$$\Phi_k(a) = a^k, \qquad a \in \{1, 5, 7, 11\}.$$

As a review, the reason that, say $\Phi_{10} \notin Aut(C_{12})$ is that the image of Φ_{10}, that is, $\{\Phi_{10}(a^k)\}$, consists of

$$\{e, a^{10}, a^8, a^6, a^4, a^2\}$$

Since $a \notin Im(\Phi_{10})$, the map Φ_{10} is not a surjection, and can't be an automorphism.

A check that $Aut(C_{12}) \approx V$: since $\Phi_j * \Phi_k = \Phi_{jk} = \Phi_{(jk \mod 12)}$,

$$\Phi_1 * \Phi_k = \Phi_k * \Phi_1 = \Phi_k,$$
$$(\Phi_5)^2 = \Phi_{25} = \Phi_1,$$
$$(\Phi_7)^2 = \Phi_{49} = \Phi_1,$$
$$(\Phi_{11})^2 = \Phi_{121} = \Phi_1,$$
$$\Phi_5 * \Phi_7 = \Phi_7 * \Phi_5 = \Phi_{35} = \Phi_{11},$$
$$\Phi_5 * \Phi_{11} = \Phi_{11} * \Phi_5 = \Phi_{55} = \Phi_7,$$
$$\Phi_7 * \Phi_{11} = \Phi_{11} * \Phi_7 = \Phi_{77} = \Phi_5.$$

The final topic for today is another interesting group, the generalization of V to "three dimensions". For our purposes, let $C_2 = (\mathbb{Z}/2\mathbb{Z}, \oplus)$, so the components are $[0]_2$ or $[1]_2$

$$C_2 \times C_2 \times C_2 = \{([i]_2, [j]_2, [k]_2)\}, \qquad i, j, k \in \{0, 1\}.$$

Let's write $([i]_2, [j]_2, [k]_2)$ as ijk, so the $8 = 2^3$ elements are:

$$000, \quad 001, \quad 010, \quad 011, \quad 100, \quad 101, \quad 110, \quad 111.$$

Addition is component-wise mod 2 and commutative, so for example, $011 + 101 = 112 = 110$. The identity is 000, and

$$([i]_2, [j]_2, [k]_2) + ([i]_2, [j]_2, [k]_2) =$$
$$([2i]_2, [2j]_2, [2k]_2) = ([0]_2, [0]_2, [0]_2),$$

so every element has order two.

The order of this group is 8, so subgroups might have order 1,2,4 or 8, and proper subgroups would have order 2 or 4. Any subgroup of order 2 would have to look like $\{000, ijk\}$ and there are $7 = 2^3 - 1$ ways to pick ijk, so there are 7 subgroups of order 2.

Let's write $000 = e$, because it's the identity, and suppose H is a subgroup of order 4. Suppose $e, x, y \in H$ are different. Then we have to have $x + y \in H$, but then we actually get a subgroup: $x + (x + y) = (x + y) + x = y$, etc.,

$$H = \{e, x, y, x + y\},$$

which you won't be shocked to learn is isomorphic to V.

How many different subgroups of order 4 are there? At first glance, you might count them this way: there are 7 choices for x (not e) and then 6 choices for y (not e or x), so you might think there are $7 \cdot 6 = 42$ subgroups, but that is over-counting! For example, $\{e, x, y, x+y\}$ gives you the same set as $\{e, y, x, y+x\}$.

If you started with $x+y$ and y you'd get $(x+y)+y = x$. In fact, each subgroup arises in six different ways, and there are seven different subgroups, presented with an "external" definition.

$$H_1 = \{000,\ 001,\ 010,\ 011\} = \{ijk \mid i = 0\}$$
$$H_2 = \{000,\ 001,\ 100,\ 101\} = \{ijk \mid j = 0\}$$
$$H_3 = \{000,\ 001,\ 110,\ 111\} = \{ijk \mid i = j\}$$
$$H_4 = \{000,\ 010,\ 100,\ 110\} = \{ijk \mid k = 0\}$$
$$H_5 = \{000,\ 010,\ 101,\ 111\} = \{ijk \mid i = k\}$$
$$H_6 = \{000,\ 011,\ 100,\ 111\} = \{ijk \mid j = k\}$$
$$H_7 = \{000,\ 011,\ 101,\ 110\} = \{ijk \mid i + j + k \equiv 0 \mod 2\}.$$

A couple of final remarks. If you think of $\{ijk\}$ as the point $(i, j, k) \in \mathbb{R}^3$, then C_2^3 can be thought of as the vertices of a unit cube, and six of these subgroups are the intersections of the cube with a plane that passes through the origin: $x = 0$, $y = 0$, $x = y$, $z = 0$, $x = z$, $y = z$.

If you draw it out, the vertices of H_7 don't lie in the plane, but they form a regular tetrahedron, taken from alternate vertices of the cube.

The other thing I want to say is that we can look at the H_i's and take out 000 and just look at these as seven sets, and for convenience, I'll look at the remaining numbers as if they were in binary, so, for example, $101 \to 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 5$.

$$S_1 = \{001,\ 010,\ 011\} = \{1, 2, 3\}$$
$$S_2 = \{001,\ 100,\ 101\} = \{1, 4, 5\}$$
$$S_3 = \{001,\ 110,\ 111\} = \{1, 6, 7\}$$
$$S_4 = \{010,\ 100,\ 110\} = \{2, 4, 6\}$$
$$S_5 = \{010,\ 101,\ 111\} = \{2, 5, 7\}$$
$$S_6 = \{011,\ 100,\ 111\} = \{3, 4, 7\}$$
$$S_7 = \{011,\ 101,\ 110\} = \{3, 5, 6\}$$

Notice that each number is in three sets and each set has three numbers. Every pair of numbers is in exactly one set, and any two sets contain exactly one number in common.

You can think of each S_j as a "line" and each number as a "point". There is exactly one line containing any two points and any two lines intersect in exactly one point.

It is called the *Fano plane* and is a finite projective plane "of order 2". You won't see these terms again in this class this semester!