Math 417 – Fifteenth Day – Class

Bruce Reznick
University of Illinois at Urbana-Champaign

September 28, 2020

I got some very good questions after Sunday night's talk, and I'd like to give you all the answers I gave your classmates when they wrote. If you have follow-ups, it's hard for me to see you all on screen-share, so put it into the Chat.

First: what's going on with "well-defined"? What are we checking?

What we're doing is that sometimes on a map f from G to H, the same object in G might have different names. (This applies whether G is a group or another kind of object.) For example $[1]_6 = [7]_6$, or you could have $aK = bK$ for a subgroup K. What mathematicians mean by a "well-defined" map f is that, however you name the object, the image under f is the same.

Second: When we talk about a homomorphism becoming an isomorphism and that $Ker(\phi) = \{eH\}$ and $Im(\phi) = H$, does $Ker(\phi) = \{eH\}$ tell us that the relationship is injective and $Im(\phi) = H$ tell us that the map is surjective?

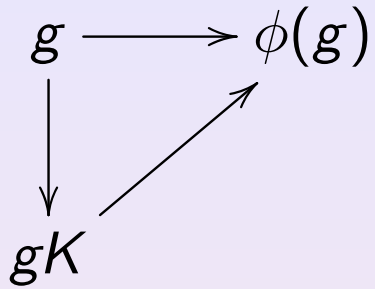
Exactly!

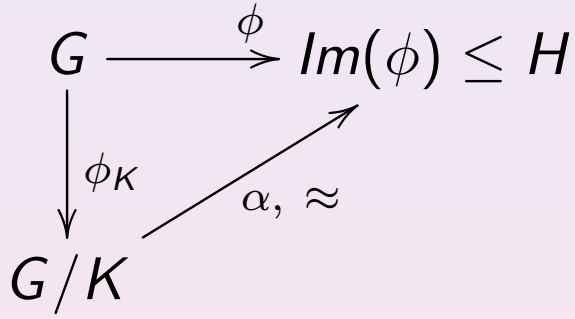
Third: Why did we look at $6/3 = 2$ or $6/2 = 3$ in the context of cosets and S_3?

There are three parameters: the order of a group, the order of a subgroup, and the number of cosets, and these are related by the equation $|G| = |H| \cdot [G : H]$, so if you know two of them, you know the third.

Fourth: Could you also go over exactly was the Fundamental Homomorphism Theorem is?

There are two things about it. One is that any homomorphism ϕ from $G \to H$ can be split up into a composition of two maps. The other is that one of the maps is an isomorphism. I put some diagrams on the next frame.





If you've ever seen diagrams like these in a classroom when you walk in, that's all they mean. Lots of mathematicians use diagrams like these in their research. I don't, and I had to google how to write them in LaTeX.

The other question had to do with automorphisms and inner automorphisms, and that fit in well with the material I had already planned to present.

Recall that an automorphism Φ of G is an isomorphism of G to itself and this means that it is a homomorphism of $G \to G$ which is injective and surjective. An automorphism can be thought of as an "internal symmetry" of a group.

One trivial automorphism of any group G is the identity map: $\Phi(g) = g$, but since any group has it, it's not very illuminating. Here's another example

THEOREM If G is an abelian group, then $\Phi(g) = g^{-1}$ is an automorphism.

PROOF. It's easily shown to be injective and surjective (check if you don't see these!) and $\phi(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1}$ $= \phi(g)\phi(h)$, where the key step in the middle comes from the assumption that G is abelian. $\square$.

For example, if $G = \mathbb{Z}/n\mathbb{Z}$, then $\phi([a]_n) = [-a]_n = [n-a]_n$ is an automorphism.

As noted yesterday, a general class of automorphisms comes from conjugation. If G is any group and $g \in G$ is fixed, define a map $i_g : G \to G$ by

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

We saw that it is an isomorphism, but it isn't interesting for an abelian group, because then $i_g(x) = x$ for every x and i_g is the identity map.

An automorphism that is defined in this way is called an "inner" automorphism; every other automorphism is an "outer" automorphism. So the map $x \to x^{-1}$ in an abelian group is an outer automorphism.

What happens with our favorite non-abelian group S_3? Here's a start. What is i_{ρ_0}? Well, ρ_0 is the identity, so $\rho_0 x \rho_0^{-1} = x$. This is just the identity.

Here is i_{ρ_1}, noting that $\rho_1^{-1} = \rho_2$

$$
\begin{aligned}
i_{\rho_1}(\rho_0) &= \rho_1\rho_0\rho_2 = \rho_0, \\
i_{\rho_1}(\rho_1) &= \rho_1\rho_1\rho_2 = \rho_1, \\
i_{\rho_1}(\rho_2) &= \rho_1\rho_2\rho_2 = \rho_2, \\
i_{\rho_1}(\mu_1) &= \rho_1\mu_1\rho_2 = \rho_1\mu_3 = \mu_2, \\
i_{\rho_1}(\mu_2) &= \rho_1\mu_2\rho_2 = \rho_1\mu_1 = \mu_3, \\
i_{\rho_1}(\mu_3) &= \rho_1\mu_3\rho_2 = \rho_1\mu_2 = \mu_1
\end{aligned}
$$

So what happens here is this: ρ_0, ρ_1, ρ_2 don't change under i_{ρ_1}, but the flips are cycled: $\mu_1 \mapsto \mu_2 \mapsto \mu_3 \mapsto \mu_1$.

Can this be explained? Let me put the pictures of the rotations of S_3 back up:

$$\rho_0 = \begin{matrix} 1 & 2 \\ 3 & \end{matrix}, \quad \rho_1 = \begin{matrix} 3 & 1 \\ 2 & \end{matrix}, \quad \rho_2 = \begin{matrix} 2 & 3 \\ 1 & \end{matrix};$$

$$\mu_1 = \begin{matrix} 1 & 3 \\ 2 & \end{matrix}, \quad \mu_2 = \begin{matrix} 3 & 2 \\ 1 & \end{matrix}, \quad \mu_3 = \begin{matrix} 2 & 1 \\ 3 & \end{matrix}.$$

Suppose that, rather than acting on the permutations, I acted on the *labels*, and renamed 1 as 2, renamed 2 as 3 and renamed 3 as 1. Call the action F, with the understanding that $F(\rho_0)$ represents the new names.

That should be an automorphism; it's some kind of symmetry on the group S_3.

$$F(\rho_0) = \begin{matrix} 2 & 3 \\ 1 & \end{matrix}, \quad F(\rho_1) = \begin{matrix} 1 & 2 \\ 3 & \end{matrix}, \quad F(\rho_2) = \begin{matrix} 3 & 1 \\ 2 & \end{matrix};$$

$$F(\mu_1) = \begin{matrix} 2 & 1 \\ 3 & \end{matrix}, \quad F(\mu_2) = \begin{matrix} 1 & 3 \\ 2 & \end{matrix}, \quad F(\mu_3) = \begin{matrix} 3 & 2 \\ 1 & \end{matrix}.$$

So what does $F(\rho_1)$ do? What used to be in the 1 position is now in the 2 position, what used to be in the 2 position is now in the 3 position and what used to be in the 3 position is now in the 1 position, so as a permutation, $F(\rho_1) = \rho_1$. Similarly, $F(\rho_2) = \rho_2$.

What about $F(\mu_1)$? What was in the 1 position is now in the 3 position, what was in the 2 position is now in the 2 position and what was in the 3 position is now in the 1 position, so $F(\mu_1) = \mu_2$. Similarly, $F(\mu_2) = \mu_3$ and $F(\mu_3) = \mu_1$.

If you go through everything, you'll discover that $F(x) = i_{\rho_1}(x)$. And notice that ρ_1 takes $1 \to 2 \to 3 \to 1$ too.

WORKSHEET PROBLEM

1. For the group $G = S_3$, compute the conjugation by μ_1. That is, compute

$$i_{\mu_1}(x) = \mu_1 x \mu_1^{-1} = \mu_1 x \mu_1, \quad \text{for } x \in S_3.$$

Give an "interpretation" for this automorphism in terms of labels.

I'll leave the multiplication table up for your convenience, and you can do your work before you go to the breakout rooms, and then talk about it there.

S_3	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

WORKSHEET SOLUTION

Here's what I get:

$$
\begin{aligned}
i_{\mu_1}(\rho_0) &= \mu_1\rho_0\mu_1 = \mu_1\mu_1 = \rho_0,\\
i_{\mu_1}(\rho_1) &= \mu_1\rho_1\mu_1 = \mu_1\mu_3 = \rho_2,\\
i_{\mu_1}(\rho_2) &= \mu_1\rho_2\mu_1 = \mu_1\mu_2 = \rho_1,\\
i_{\mu_1}(\mu_1) &= \mu_1\mu_1\mu_1 = \mu_1\rho_0 = \mu_1,\\
i_{\mu_1}(\mu_2) &= \mu_1\mu_2\mu_1 = \mu_1\rho_2 = \mu_3,\\
i_{\mu_1}(\mu_3) &= \mu_1\mu_3\mu_1 = \mu_1\rho_1 = \mu_2
\end{aligned}
$$

The interpretation is that the label 1 is fixed and the labels 2 and 3 are reversed. Hmm. That's what μ_1 does as well.

THEOREM Suppose $\alpha, \beta \in S_n$, then $i_\beta(\alpha) \in S_n$ is the permutation which takes $\beta(j)$ to $\beta(\alpha(j))$.

PROOF Let's just write it out: $i_\beta(\alpha) = \beta\alpha\beta^{-1}$, so

$$i_\beta(\alpha)(\beta(j)) = \beta(\alpha(\beta^{-1}(\beta(j)))) = \beta(\alpha(j))$$

For example, let $n = 4$ and think of elements in D_4. Let $\alpha = \rho_1 = (1234)$ and $\beta = \mu_1 = (12)(34)$. Then

$$\pi := i_{\mu_1}(\rho_1) = \mu_1\rho_1\mu_1^{-1} = (12)(34)(1234)(12)(34) :$$
$$1 \to 2 \to 3 \to 4, \quad 2 \to 1 \to 2 \to 1,$$
$$3 \to 4 \to 1 \to 2, \quad 4 \to 3 \to 4 \to 3$$
$$= (1432).$$

So $\pi(\beta(j)) = \beta(\alpha(j))$ Can we check this? I'll do it for $j = 1, 2$:

$$\alpha(1) = 2, \ \beta(2) = 1, \quad \beta(1) = 2, \ \pi(2) = 1,$$
$$\alpha(2) = 3, \ \beta(3) = 4, \quad \beta(2) = 1, \ \pi(1) = 4.$$