GROUPS AND SYMMETRY: LECTURE 23

LEO GOLDMAKHER

Recall the following result from our previous lecture:

Theorem 1 (1st Isomorphism Theorem)**.** *Given any two groups* Γ *and* H *and a homomorphism* $\varphi : \Gamma \to H$*, we have*

- im $\varphi \leq H$
- ker $\varphi \trianglelefteq \Gamma$
- $\Gamma/$ker $\varphi \simeq$ im φ

As before,

$$\text{im}\,\varphi := \{\varphi(g) : g \in \Gamma\} \qquad \text{and} \qquad \text{ker}\,\varphi := \{g \in \Gamma : \varphi(g) = e\}.$$

Last time, we saw an application: the theorem allowed us to realize the complicated-looking group $\mathbb{C}^\times/\mathbb{R}_{>0}$ was simply the unit circle (up to isomorphism). More generally, one can understand any quotient Γ/N this way: just rig up a homomorphism out of Γ whose kernel is N, then find the image!

We spent the first half of today's lecture proving this theorem. We proved the three claims separately.

$\boxed{\text{im}\,\varphi \leq H}$

Proof. The image of φ is a subset of H by definition, so it remains only to check that it's a group under the operation of H:

(0) *Closure*

If $a, b \in$ im φ, then exist $x, y \in \Gamma$ such that $\varphi(x) = a$ and $\varphi(y) = b$. It follows that

$$ab = \varphi(x)\varphi(y) = \varphi(xy) \in \text{im}\,\varphi.$$

(1) *Associativity*

im φ is automatically associative, since it's a subset of H.

(2) *Identity*

Recall that homomorphisms map the identity to the identity. It follows that

$$e = \varphi(e) \in \text{im}\,\varphi.$$

(3) *Inverses*

Given any $a \in$ im φ, there exists $x \in \Gamma$ such that $\varphi(x) = a$. Since φ is a homomorphism, we have

$$a^{-1} = \varphi(x)^{-1} = \varphi(x^{-1}) \in \text{im}\,\varphi.$$

□

Date: November 29, 2013.

$\boxed{\text{ker}\,\varphi \trianglelefteq \Gamma}$

Proof. This requires showing two things: that ker $\varphi \leq \Gamma$, and that it's normal. We left the former as an exercise and focused on the latter. First, we observed that it suffices to prove

$$g^{-1}(\text{ker}\,\varphi)g \subseteq \text{ker}\,\varphi \qquad\qquad \forall g \in \Gamma. \tag{1}$$

Why? In your problem set you showed that the above was equivalent to $g^{-1}(\text{ker}\,\varphi)g = \text{ker}\,\varphi$ for all $g \in \Gamma$, which we know (from lecture) is equivalent to ker φ being normal in Γ. (Note that all of this is merely a convenient way of *checking* that ker φ is normal in Γ; what normality actually *means* is that $\Gamma/\text{ker}\,\varphi$ is a group.)

We now verify that the normality criterion (1) is satisfied. Pick any $g \in \Gamma$ and $k \in \text{ker}\,\varphi$. We have

$$\varphi(g^{-1}kg) = \varphi(g^{-1})\varphi(k)\varphi(g) = \varphi(g)^{-1}e\varphi(g) = e$$

It follows that $g^{-1}kg \in \text{ker}\,\varphi$. Since g and k were arbitrary, (1) follows. □

$\boxed{\Gamma/\text{ker}\,\varphi \simeq \text{im}\,\varphi}$

Proof. We started by drawing a diagram of all the groups we're dealing with, and the connections between them.

$$\begin{tikzcd}
\Gamma \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \text{im}\,\varphi \leq H \\
\Gamma/\text{ker}\,\varphi \arrow[ur, dashed, "\Delta"'] &
\end{tikzcd} \tag{2}$$

The function $\pi : \Gamma \to \Gamma/\text{ker}\,\varphi$ is the natural projection map defined by $\pi(g) = [g]$. Note that φ maps Γ surjectively onto im φ, and π maps Γ surjectively onto $\Gamma/\text{ker}\,\varphi$. The dotted line is the isomorphism we wish to find between $\Gamma/\text{ker}\,\varphi$ and im φ. Actually, it's not obvious how to find any such map, isomorphism or otherwise. Dan suggested the following:

$$\begin{aligned} \Delta : \Gamma/\text{ker}\,\varphi &\longrightarrow \text{im}\,\varphi \\ [g] &\longmapsto \varphi(g) \end{aligned}$$

This definition is problematic, as Dickson pointed out: $[g]$ is a set, whereas $\varphi(g)$ is a function of the single element g. Why is this a problem? Suppose $a \in [g]$. Then $[a] = [g]$. So how do we define $\Delta([g])$ – as $\varphi(g)$ or as $\varphi(a)$? In other words, is Δ well-defined?

Turns out it is, as Dan demonstrated. His argument went as follows. Recall that $[x] = x(\text{ker}\,\varphi)$. Applying the homomorphism φ to the set (i.e. to each element of the set), we find that

$$\varphi([x]) = \varphi\Big(x(\text{ker}\,\varphi)\Big) = \varphi(x)\varphi(\text{ker}\,\varphi) = \{\varphi(x)\}.$$

Note that $\varphi([x])$ is a set, since we are applying a function to a set; the above calculation shows that this set has only one element in it! It follows that

$$\begin{aligned} [x] = [y] &\Longrightarrow \varphi([x]) = \varphi([y]) \\ &\Longrightarrow \{\varphi(x)\} = \{\varphi(y)\} \\ &\Longrightarrow \varphi(x) = \varphi(y) \\ &\Longrightarrow \Delta([x]) = \Delta([y]) \end{aligned}$$

Thus Δ is well-defined after all.

Now we've come up with a function from $\Gamma/\ker\varphi$ to $\mathrm{im}\,\varphi$. What we're really after, though, is an isomorphism between these two. Is Δ an isomorphism? To check this, we need to check whether it's a bijection and a homomorphism. We verify this now. As usual, rather than checking directly that Δ is a bijection, we verify separately that it's injective and surjective.

Δ is injective.

Suppose $\Delta([x]) = \Delta([y])$. Then $\varphi(x) = \varphi(y)$, whence $\varphi(x^{-1}y) = e$. It follows that $x^{-1}y \in \ker\varphi$, or in other words that $y \in [x]$. Thus the sets $[x]$ and $[y]$ are not disjoint, whence $[x] = [y]$.

Δ is surjective.

Suppose $y \in \mathrm{im}\,\varphi$. Then by definition, there exists $x \in \Gamma$ such that $y = \varphi(x)$. It immediately follows that $\Delta([x]) = \varphi(x) = y$.

Δ is a homomorphism.

Given any elements $[x], [y] \in \Gamma/\ker\varphi$, we have

$$\Delta([x][y]) = \Delta([xy]) = \varphi(xy) = \varphi(x)\varphi(y) = \Delta([x])\Delta([y]).$$

Thus, we've proved that Dan's map Δ is an isomorphism. The theorem follows. □

The diagram (2) is helpful for visualizing the proof. It's called a *commutative diagram*, because you can get from Γ to $\mathrm{im}\,\varphi$ in two different ways – directly by applying φ, or indirectly by first applying π and then applying Δ – and each way gives the same result. In other words: $\varphi = \Delta \circ \pi$. In fact, our whole proof boils down to finding a function Δ which makes this hold (i.e. which makes the diagram commute.)

The above proof is yet another illustration of a general principle: the most natural map between two isomorphic groups usually turns out to be an isomorphism. So if you're ever trying to prove that two groups are isomorphic, just construct any map you can from one to the other. Chances are, it will be an isomorphism.

From here, we moved on to another cool theorem. In your homework, you've seen that if the order of a group is a multiple of 3, then the group contains an element of order 3. This generalizes rather nicely.

Theorem 2 (Cauchy's theorem)**.** *Suppose Γ is a finite abelian group. If a prime $p \mid |\Gamma|$, then Γ has an element of order p.*

Note that the theorem is true even without the hypothesis that Γ is abelian. In fact, the proof outlined on your homework can be generalized to prove this. Here we'll follow a totally different approach which illustrates the utility of the tools we've developed. The drawback of the approach we present here is that it only proves the theorem for abelian groups.

Before writing down the formal proof, let me sketch the idea. Suppose Γ has a nontrivial proper subgroup $N \leq \Gamma$ (i.e. $\{e\} \neq N \neq \Gamma$). By Lagrange's theorem, we know $|N| \mid |\Gamma|$. It follows that if p divides $|\Gamma|$, then p either divides $|N|$ or $|\Gamma|/|N|$. Either way, we've reduced the original question to the same question about a *smaller group* (either N or Γ/N); induction! The one hitch is that Γ/N and Γ are totally different groups – if we find an element of order p in Γ/N, it's not obvious how to translate that into an element of order p in Γ itself. To accomplish this we'll have to be a little clever, but don't let this distract you from the big picture of the proof – a reduction from a big group to a smaller one.

But enough talk – let's do some math.

Proof. We proceed by induction on the order of Γ. If $|\Gamma| = 2$, the theorem clearly holds. Now suppose Γ is some group of order at least 3, and that the theorem holds for all groups of order less than $|\Gamma|$. Our aim is to prove that Γ contains an element of order p for every prime $p \,\big|\, |\Gamma|$.

First, observe that if the only subgroups of Γ are the trivial ones ($\{e\}$ and Γ), then Γ must have prime order (this is a problem in your latest problem set), and Cauchy's theorem holds immediately. Thus, we may assume that there exists a subgroup $N \leq \Gamma$ such that $\{e\} \neq N \neq \Gamma$. In particular, we have

$$1 < |N| < |\Gamma|.$$

By induction, Cauchy's theorem holds for N: for every $p \,\big|\, |N|$, the group N contains an element of order p. Since $N \subseteq \Gamma$, we conclude that Γ must contain an element of order p for every prime $p \,\big|\, |N|$.

We may thus restrict our attention to primes $p \,\big|\, |\Gamma|$ which do *not* divide $|N|$. Fix any such p. By Lagrange's theorem, we know that $|N| \,\big|\, |\Gamma|$, whence

$$p \,\big|\, |\Gamma/N|.$$

Once again, Γ/N is a strictly smaller group than Γ, so by induction we know that Γ/N contains an element of order p; say this element is $[x]$, where $x \in \Gamma$. The fact that $[x]$ has order p in Γ/N means that

$$[x]^p = [e] \qquad \text{but} \qquad [x]^k \neq [e] \quad \forall k \in \{1, 2, \ldots, p-1\}.$$

Recall that what we really want is an element of Γ of order p. Unfortunately, the above does not guarantee that x has order p in Γ; the most we can deduce is that

$$x^p \in N \qquad \text{but} \qquad x^k \notin N \quad \forall k \in \{1, 2, \ldots, p-1\}.$$

However, as Dan pointed out, this does tell us that

$$(x^p)^{|N|} = e.$$

Right away, we see that

$$(x^{|N|})^p = e,$$

which is suggestive – is it possible that the element $x^{|N|} \in \Gamma$ has order p?

Suppose $(x^{|N|})^k = e$ for some positive integer k. Then in the group Γ/N we would have

$$[x]^{k|N|} = [e]. \tag{3}$$

On the other hand, we know that $[x]$ has order p in Γ/N. The following lemma is immediately applicable.

Lemma 3. *If K is a group and $a^m = e$ for some $a \in K$, then $|a| \,\big|\, m$.*

Taking the lemma on faith for the moment, we deduce from (3) that

$$p \,\big|\, k|N|.$$

Since we are assuming that p doesn't divide $|N|$ (otherwise the proof would have already been over!), we conclude that $p \mid k$. But this means that $k \geq p$. In other words, we have shown that

$$(x^{|N|})^k \neq e$$

for $k \in \{1, 2, \ldots, p-1\}$. Combined with the fact that $(x^{|N|})^p = e$, we conclude that $x^{|N|}$ has order p in Γ. The theorem is proved! □

A few questions remain about the proof. First, where did we use the hypothesis that Γ is abelian? And second, how does one prove that lemma? These are both exercises for you!

WWW.MATH.TORONTO.EDU/LGOLDMAK/C01F13/
E-mail address: lgoldmak@math.toronto.edu