9.24.2025: Math 122 Lecture 7 Notes

Vasily Krylov

Last Time

We discussed *automorphisms* $\varphi : G \xrightarrow{\sim} G$, where φ is defined as an *isomorphism* from a group to itself. We also discussed one nontrivial example of an automorphism:

$$S_3 \xrightarrow{\varphi} S_3$$

where $x = (123) \mapsto (132) = x^2$ and $y = (12) \mapsto (12) = y$. Note that φ is *uniquely* determined by where it maps x, y. This example is a particular case of a when we take $g \in G$ such that $\varphi_g : G \xrightarrow{\sim} G$; $h \mapsto ghg^{-1}$. So for $G = S_3$, $g = (12)$ gets φ as above.

Question:

For which groups are automorphisms φ_g all equal to id?

Answer:

For *commutative* groups ($ghg^{-1} = gg^{-1}h = h$). In general, $\varphi_g = \text{id}$ if and only if $ghg^{-1} = h$ $\forall h \in G$. (Note this is equivalent to $gh = hg$.) So g commutes with every element of G. Such g are called *central*.

Why are automorphisms important?

They allow us to identify different elements of the group.

Proposition 1. *Claim if $\varphi : G \xrightarrow{\sim} G'$ is an automorphism, then for $g \in G$, $g' := \varphi(g)$ we have $ord(g) = ord(g')$.*

Proof. If $g^n = 1$, then $\varphi(g^n) = \varphi(1) = 1$. Note $\varphi(g^n) = \varphi(g)^n = (g')^n$.

If $(g')^m = 1$ then $(\varphi^{-1})(g'^m) = \varphi^{-1}(1) = 1$, so $g^m = \varphi^{-1}(g')^m$. So $g^n = 1$ if and only if $(g')^m = 1$, which means that $\text{ord}(g) = \text{ord}(g')$. □

Corollary 1. *If $x, x' \in G$ are conjugate, i.e. $\exists g \in G$ such that $x' = gxg^{-1}$, then $ord(x) = ord(x')$.*

This means that, for example, $(12), (123) \in S_3$ are *not* conjugate.

Exercise 1. *Cycles $(k_1, \ldots, k_n), (p_1, \ldots, p_m) \in S_N$ are conjugate if and only if $n = m$.*

Example 1. $(1423) = (243)(1234)(234)$, *where we note that* $(234) = (243)^{-1}$.

So in general:

$$\sigma \cdot (p_1 \ldots, p_m) \cdot \sigma^{-1} = (\sigma(p_1) \ldots \sigma(p_m)).$$

Work this out!

Back to homomorphisms

An isomorphism is *bijective*. A homormorphism is in general neither *injective* nor *surjective*. Given homomorphism $\varphi : G \to G$, how do we "make" it surjective?

Replace G' by the *image* of φ.

Proposition 2. *im* $\varphi = \{\varphi(g) \mid g \in G\}$, *where this is a subgroup of* G'.

Proof. As an exercise, let's check that im $\varphi \subset G'$ is closed under multiplication.

$$\varphi(g_1) \cdot \varphi(g_2) = \varphi(g_1 g_2) \in \text{im } \varphi,$$

so it is closed. □

Example 2. $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}$, $n \mapsto 2n$. *Then* $im(\varphi) = 2\mathbb{Z}$. *Similarly, take* $(\mathbb{R}, +) \xrightarrow{\varphi} (\mathbb{R}^\times, \cdot)$. *If* $t \mapsto 2^t$, *then* $im(\varphi) = \mathbb{R}_{>0}$, *i.e. the positive real numbers.*

So if $\varphi : G \to G'$, then we can replace G' by $\text{im}(\varphi) =: S$ and write $\varphi : G \to S$. Note that φ is still *not* an isomorphism in general: although it is *surjective*, it can fail to be *injective*.

How do we "measure" the non-injectivity of homormophism $\varphi : G \in \mathcal{S}$?

The answer is that the non-injectivity of φ is "controlled" by $\ker \varphi = \{g \in G \mid \varphi(g) = 1_S\}$. Namely, φ is injective if and only if $\ker \varphi = \{1_G\}$, which we will prove.

Example 3. $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/n\mathbb{Z}, m \mapsto m \mod n$. *Then* $\ker \varphi = n\mathbb{Z}$, *a subgroup of* $\mathbb{Z}$.

In general:

Proposition 3. $\ker \varphi$ *is a subgroup of* G.

Proof. Let's prove that $\ker \varphi$ is closed under multiplication. $a, b \in \ker \varphi$ means that $\varphi(a) = \varphi(b) = 1$. We want $ab \in \ker \varphi$: and

$$\varphi(ab) = \varphi(a)\varphi(b) = 1 \cdot 1 = 1,$$

as desired. □

Proposition 4. $\varphi : G \to G'$ *is a homomorphism,* $a, b \in G$. *The following conditions are equivalent:*

1. $\varphi(a) = \varphi(b)$.
2. $a^{-1}b \in \ker \varphi$.

Proof. (1) → (2) if $\varphi(a) = \varphi(b)$ then $\varphi(a)\varphi(b)^{-1} = 1 = \varphi(ab^{-1})$. Then $ab^{-1} \in \ker \varphi$, as desired.

(2) → (1) if $\varphi(ab^{-1}) = 1$ then $\varphi(a)\varphi(b)^{-1} = 1$, so $\varphi(a) = \varphi(b)$. □

Corollary 2. φ *is injective if and only if* $\ker \varphi = \{1_G\}$.

Proof. If φ is injective, then $|\varphi^{-1}(\{1\})| \leq 1$. The kernel must contain 1_G, so then $\ker \varphi = \{1_G\}$. Now if $\ker \varphi = \{1\}$, we want to check that if $\varphi(a) = \varphi(b)$ then $a = b$. We know that $\varphi(a) = \varphi(b)$ if and only if $a^{-1}b \in k = \{1\}$, so $a^{-1}b = 1$ and $a = b$, as desired. □

Corollary 3. *Take $\varphi : G \mapsto S$, a surjective homomorphism. Then $\forall x \in S$, $\varphi^{-1}(x) \cong \ker \varphi$, which are isomorphic as sets (i.e. there exists a bijective map between them). In particular,*

$$G = \bigcup_{x \in S} \varphi^{-1}(x),$$

which is a disjoint decomposition into sets of the same size.

Proof. We want to identify $\varphi^{-1}(x) \cong \ker \varphi$. Pick any $a \in G$ such that $\varphi(a) = x$. Then $b \in \varphi^{-1}(x)$ if and only if $\varphi(b) = x = \varphi(a)$ which is true if and only if $a^{-1}b \in \ker \varphi$ by the earlier proposition. So (left) multiplication by a^{-1} defines the identification

$$\varphi^{-1}(x) \xrightarrow{\sim} \ker \phi.$$

□

Question: Who is the inverse?

Answer: Left multiplication by a! In particular

$$\ker \varphi \xrightarrow{\sim, a\cdot} \varphi^{-1}(x)$$

Important corollary

Corollary 4. *If $\varphi : G \to G'$ is some arbitrary homomorphism of finite groups, then $\#G = \#im(\varphi) = \#\ker \varphi$. We will use this corollary next time to describe the kernel of some interesting morphism.*

Proof. $G \to \mathrm{im}(\varphi)$ is a surjective homomorphism. So by the corollary above,

$$G = \bigcup_{x \in \mathrm{im}(\varphi)} \varphi^{-1}(x),$$

where all have the same number of elements equal to $\#\ker \varphi$. Then

$$\#G = \sum_{x \in \mathrm{im}(\varphi)} \#\varphi^{-1}(x) = \sum_{x \in \mathrm{im}(\varphi)} \#\ker \varphi = \#\ker \phi \cdot \#\mathrm{im}(\varphi).$$

□