9.22.2025: Math 122 Lecture 6 Notes

Vasily Krylov

Last Time

Last time we discussed homomorphism and isomorphism. A mapping

$$\varphi : G \to G'$$

is a homomorphism if $\varphi(ab) = \varphi(a)\varphi(b)$. If φ is also bijective, then it will be an isomorphism. For example;

$$G \to G', g \to e_{G'}$$

is trivial, and;

$$G \to G, g \to g$$

is the identity. Also consider;

$$\mathbb{Z} \to^a \mathbb{Z}; \ m \to am$$

where a is any integer. Another example is;

$$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \ m \to m \bmod n$$

as well as;

$$(\mathbb{R}, +) \to (\mathbb{R}^\times, \cdot), \ t \to 2^t$$

1 Properties of Homomorphisms

Proposition: Let $\varphi : G \to G'$ be a homomorphism.

1. If $a_1, \cdots, a_k \in G$, then $\varphi(a_1, \cdots a_k) = \varphi(a_1) \cdots \varphi(a_k)$

2. We have that $\varphi(e_G) = e_{G'}$

3. We have that $\varphi(a^{-1}) = \varphi(a)^{-1}$

Proof of (1) - Exercise (Use induction, with $a_1 \cdots a_n = (a_1 \cdots a_{n-1}) \cdot (a_n)$). Sketch;

$$\varphi(a_1 \cdots a_n) = \varphi((a_1 \cdots a_{n-1}) \cdot (a_n)) = \varphi(a_1 \cdots a_{n-1}) \cdot \varphi(a_n)$$

Induction

$$= (\varphi(a_1) \cdots \varphi(a_n)) \cdot (\varphi(a_n)) = \varphi(a_1) \cdots \varphi(a_n)$$

Proof of (2) - Want to check that $\varphi(e_G) = e_{G'}$. We know that $e_G \cdot e_G = e_G$. Applying the homomorphism then yields;

$$\varphi(e_G \cdot e_G) = \varphi(e_G)$$

$$\implies \varphi(e_G) \cdot \varphi(e_G) = \varphi(e_G) \implies \varphi(e_G) = e_{G'}$$

Proof of (c) - Want $\varphi(a^{-1}) = \varphi(a)^{-1}$. Need to check:

$$\varphi(a^{-1}) \cdot \varphi(a) = e_{G'} = \varphi(a) \cdot \varphi(a^{-1})$$

For the left side, we have $\varphi(a^{-1}) \cdot \varphi(a) = \varphi(a^{-1} \cdot a) = \varphi(e_G) = e_{G'}$, and on the right side we have $\varphi(a) \cdot \varphi(a^{-1}) = \varphi(a \cdot a^{-1}) = \varphi(e_G) = e_{G'}$.

2 Isomorphisms

Recall that $\varphi : G \to G'$ is an isomorphism if φ is a homomorphism, as well as bijective.

Lemma - If $\varphi : G \to G'$ is an isomorphism, then $\varphi^{-1} : G' \to G$ is an isomorphism.

Proof: Need to check that $\varphi^{-1}(xy) = \varphi^{-1}(x)\varphi^{-1}(y)$ $\forall x, y \in G'$, and xy is multiplication in G', and $\varphi^{-1}(x)\varphi^{-1}(y)$ is multiplication in G.

Set $a := \varphi^{-1}(x)$; $b := \varphi^{-1}(y)$; $c := \varphi^{-1}(xy)$. Then we want to check that $c = ab$. Since φ is bijective, it is enough to check;

$$\varphi(c) = \varphi(ab)$$

Indeed:

$$\varphi(ab) = \varphi(a)\varphi(b) = xy = \varphi(c)$$

Two groups G, G' are isomorphic if $\exists \varphi : G \to G'$ where φ is an isomorphism. We will write $G \cong G'$.

WARNING: Isomorphisms are NOT unique in general.

3 Examples of Isomorphisms

The groups;

$$(\mathbb{Z}^\times, \cdot) = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$$

Where $1 \to 0$ and $-1 \to 1$.

For another example, consider the group $\langle (123) \rangle \subset S_3$ (where this is the subgroup of S_3 generated by (123)). We have that;

$$\langle (123) \rangle \cong \mathbb{Z}/3\mathbb{Z}$$

Where $1 \to 0$, $(123) \to 1$, and $(132) \to 2$.

Now for an example of two groups that are not isomorphic, consider;

$$(\mathbb{Z}/12\mathbb{Z})^{\times} \not\cong \mathbb{Z}/4\mathbb{Z}$$

Every element of $(\mathbb{Z}/12\mathbb{Z})^{\times}$ has order ≤ 2, but $\mathbb{Z}/4\mathbb{Z}$ has an element of order 4 (note that both groups contain four elements).

For another example, consider that $x \in G$, $\operatorname{ord}(x) = n$ implies;

$$\{1, x, \cdots, x^{n-1} = \langle x \rangle_G \cong \mathbb{Z}/n\mathbb{Z}$$

where $x^k \to k$.

For $x \in G$, where $\operatorname{ord}(x) = \infty$, we have that;

$$\langle x \rangle_G \cong \mathbb{Z}$$

We see that two isomorphic groups are "the same" and we do not want to distinguish them. The groups isomorphic to a given group G forms what is called an **isomorphism class** of G.

Lemma: If $G_1 \cong G_2; G_2 \cong G_3$, then $G_1 \cong G_3$ (That is, any two groups in the isomorphism class are isomorphic).

Proof: Follows from the claim:
If $\varphi : G \to H; \psi : H \to S$ where φ, ψ are homomorphisms of groups, then $\psi \circ \varphi$ is a homomorphism.

Proof:

$$(\psi \circ \varphi)(ab) = \psi(\varphi(ab)) = \psi(\varphi(a)\varphi(b)) = \psi(\varphi(a))\psi(\varphi(b)) = (\psi \circ \varphi)(a) \cdot (\psi \circ \varphi)(b)$$

Classifying all groups (describing their isomorphism classes) is very complicated and too hard. We will see that every group of order p (where p is prime) is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Question: Can you describe all groups of order 4?

4 More Examples

Clearly $G \to G$ via $g \to g$ is the identity isomorphism. Interestingly, in general, there are many ways to identify G with itself. An isomorphism $G \to G$ is called an **automorphism**.

An example of an automorphism. Consider $S_3 = \langle x = (123), y = (12) \rangle$, with $x^3 = 1, y^2 = 1, yx = x^2 y$, which can be written as $\{1, x, x^2, y, xy, x^2 y$.

Exercise: $x \xrightarrow{\varphi} x^2$ and $y \xrightarrow{\varphi} y$ extends to the automorphism of S_3.

Explictly, we have;

$$\begin{cases} 1 \to 1 \\ x \to x^2 \\ x^2 \to x \\ y \to y \\ xy \to x^2 y \\ x^2 y \to xy \end{cases}$$

To solve this exercise, we need to check that the relations are preserved;

$$\begin{cases} x^3 = 1 \to (x^2)^3 = x^6 = 1 \checkmark \\ y^2 = 1 \to y^2 = 1 \checkmark \\ yx = x^2 y \to yx^2 = ? x^4 y \end{cases}$$

Want:

$$yx^2 = x^4 y \implies yx^2 = xy \implies x^2 = yxy \implies x^2 y = yx \checkmark$$

Where we first used $x^3 = 1$, then left multiplied by y, and finally right multiplied by y.

In general: If $G = \langle x_1, \cdots x_k \rangle / \text{relations}$ then to define a homomorphism:

$$\varphi : G \to S$$

Need to:

1. define φ on generators;

$$\begin{cases} x_1 \xrightarrow{\varphi} y_1 \\ \vdots \\ x_k \to y_k \end{cases}$$

2. Check that relations are preserved:

$$x_1^{q_1} \cdots x_k^{q_k} = 1 \implies y_1^{q_1} \cdots y_k^{q_k} = 1$$

   where the left side is equality in G, and the right side is equality in S

The automorphism $\varphi : S_3 \to S_3$ that we constructed is a particular case of a very general construction: Exercise: For G a group, and $g \in G$ is any element;

$$G \xrightarrow{\varphi_g} G, h \xrightarrow{\varphi_g} ghg^{-1}$$

then φ_g is an automorphism of G, where ghg^{-1} is the conjugate of h by g.

Example: $\varphi : S_3 \to S_3$ corresponds to $g = y = (12)$. Indeed, $y \to yyy^{-1} = y$ and;

$$x = (123) \to (12)(123)(12) = (132) = x^2$$

4