9.17.2025: Math 122 Lecture 5 Notes

Vasily Krylov

Lecture 5

Last time: classified cyclic subgroups.

Main Proposition

Proposition 1. *Let G be a group and $x \in G$. Then*

$$\langle x \rangle_G = \{x^k \mid k \in \mathbb{Z}\}.$$

Cases

Case 1:

$$\langle x \rangle_G = \{1, x, x^2, \ldots, x^{n-1}\},$$

all distinct. This corresponds to multiplication in $\mathbb{Z}/n\mathbb{Z}$, identifying $x^k \leftrightarrow k$. Define

$$\operatorname{ord}(x) = \#\langle x \rangle_G = n.$$

Case 2:

$$\langle x \rangle_G = \{\ldots, x^{-1}, 1, x, x^2, \ldots\},$$

all distinct. This corresponds to multiplication in $\mathbb{Z}$. Then

$$\operatorname{ord}(x) = \infty.$$

Examples

Example 1. *In S_3, let $x = (123)$. Then*

$$\langle x \rangle = \{1, (123), (132)\},$$

so $\operatorname{ord}(x) = 3$.

If $y = (12)$, then

$$\langle y \rangle = \{1, (12)\},$$

so $\operatorname{ord}(y) = 2$.

Example 2. *In $(\mathbb{Z}/6\mathbb{Z}, +)$:*

$$\begin{aligned}
\langle 1 \rangle &= \mathbb{Z}/6\mathbb{Z}, & \operatorname{ord}(1) &= 6,\\
\langle 2 \rangle &= \{0, 2, 4\}, & \operatorname{ord}(2) &= 3,\\
\langle 3 \rangle &= \{0, 3\}, & \operatorname{ord}(3) &= 2,\\
\langle 4 \rangle &= \{0, 2, 4\}, & \operatorname{ord}(4) &= 3,\\
\langle 5 \rangle &= \{0, 1, 2, 3, 4, 5\}, & \operatorname{ord}(5) &= 6.
\end{aligned}$$

Questions and More Examples

Question: take $m \in \mathbb{Z}/n\mathbb{Z}$, what is $\mathrm{ord}(m)$?

Example 3. *In* $(\mathbb{Q}, +)$, $\frac{2}{3} \in \mathbb{Q}$ *has order* ∞.

Example 4. *In* $(\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$, *every nonidentity element has order* 2.

Exercise 1. *If* S *is a group with* ≤ 3 *elements, then* S *is cyclic.*

Exercise 2. $(\mathbb{Z}/12\mathbb{Z})^\times = \langle a, b \mid a^2 = b^2 = (ab)^2 = 1 \rangle$.

Isomorphisms

Question: in what sense are two cyclic groups of order n the same?
Answer: they are isomorphic.

Homomorphisms

Let G, G' be two groups. A *homomorphism* is a map

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

such that

$$\varphi(ab) = \varphi(a)\varphi(b).$$

An isomorphism is a bijective homomorphism.

There is a notion of *antihomomorphism*. This is a map $\psi : G \to G'$ such that $\psi(ab) = \psi(b)\psi(a)$. Check that a map $G \to G$ given by $g \mapsto g^{-1}$ is an example of an antihomomorphism.

Examples of homomorphisms

- $G \to G'$, $g \mapsto e_{G'}$: trivial homomorphism (not an iso in general).
- $G \to G$, $g \mapsto g$: identity, an iso.
- $\mathbb{Z} \to \mathbb{Z}$, $m \mapsto 2m$: not an iso.
- $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $m \mapsto m \bmod n$: not an iso.
- $(\mathbb{R}, +) \to (\mathbb{R}^\times_{>0}, \cdot)$, $t \mapsto 2^t$: isomorphism, where $\mathbb{R}^\times_{>0}$ is the group of *positive* real numbers.