10.06.2025: Math 122 Lecture 10 Notes

Vasily Krylov

1 Last Time

Recall from last time that $H \subset G$ is normal if and only if G/H is a group. In general, G/H is a set. For G finite, then $[G : H] := |G/H|$. We also have a bijection $aH \xrightarrow{a^{-1}} H$.

Corollary: If G is finite, then;

$$|G| = |H| \cdot [G : H]$$

Proof: We have $G = \bigsqcup aH$, the the number of cosets being $|G/H|$, $|aH| = |H|$. Then;

$$|G| = \sum_{|G/H|} |H| = |G/H| \cdot |H|$$

completing the proof.

Lagrange's Theorem: Let $H \subset G$ be a subgroup. The order of H divides the order of G.

Corollary: The order of an element of a finite group divides the order of the group.

Proof: Take $a \in G$, where $\langle a \rangle \subset G$. Recall that $\mathrm{ord}(a) = |\langle a \rangle|$ divides $|G|$ by Lagrange's theorem applied to $H = \langle a \rangle$.

Corollary: Suppose G has prime order. Then $G \cong \mathbb{Z}/p\mathbb{Z}$ or $G = \{1\}$.

Proof: Assume $G \neq \{1\}$. Take $a \in G \setminus \{1\}$, $\mathrm{ord}(a) > 1$, $\mathrm{ord}(a)|p \implies \mathrm{ord}(a) = p$. It follows that $\langle a \rangle = G$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Corollary: If G is finite and $a \in G$, then $a^{|G|} = 1$.

Proof: $a^{\mathrm{ord}(a)} = 1$, $\mathrm{ord}(a)||G|$,

$$a^{|G|} = \left(a^{\mathrm{ord}(a)}\right)^{\frac{|G|}{\mathrm{ord}(a)}} = 1$$

2 Applications of Lagrange's Theorem

1. If $H, K \subset G$ are finite subgroups of G, and $\gcd(|H|, |K|) = 1$, then $H \cap K = \{1\}$.
Proof: $|H \cap K|\Big||H|$ and $|H \cap K|\Big||G|$ implies that $|H \cap K| = 1$ (using the fact that $\gcd(|H|, |K|) = 1$.

2. Let G be finite, and abelian of order $2n$ with n odd. Show that G contains a unique element of order 2.
Proof: First, pair elements $g \to g^{-1}$. Element 1 will be paired with itself, which implies there exists another element g such that $g^{-1} = g \implies g^2 = 1$. Now it remains to show that this g is unique.

Consider $H := \langle g \rangle \subset G$ a normal subgroup. Take G/H to be a group of odd order. If $x \in G$ has order 2, this implies $x^2 = 1 \implies (xH)^2 = 1 \implies xH = H \implies x \in \{1, g\}$, and so $x = g$.
Important Comment: Lagrange's theorem tells us that if $\text{ord}(a)\Big||G|$ for $a \in G$. However, the converse is NOT true.

For example, take $\mathbb{Z}/12\mathbb{Z})^\times$. This group has order four, but no element is of order 4.
However, the converse is true for prime divisors of $|G|$.

Cauchy's Theorem (to be proven later): Take G a finite group, with $p\Big||G|$, where p is prime. Then $\exists a \in G$ such that $\text{ord}(a) = p$. Try to prove this theorem for G commutative.

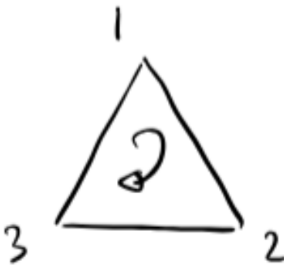
3 Dihedral Groups

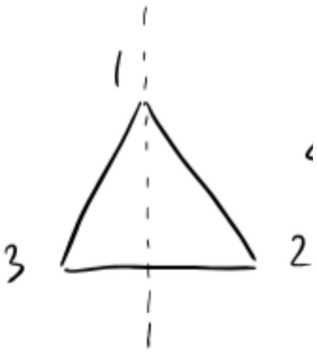
An important family of examples of groups is the class of groups whose elements are symmetries of geometric objects. The simplest subclass are symmetries of regular planar figures.

Definition: For $n \geq 3$, let D_{2n} be the set of symmetries of a regular n-gon. Each symmetry can be described uniquely by the corresponding permutation of $\{1, 2, \cdots, n\}$. In other words, we have an embedding;

$$D_{2n} \hookrightarrow S_n$$

For example, consider $n = 3$. A rotation by $\frac{2\pi}{3}$ corresponds to $(123) \in S_3$, and a reflection corresponds to $(23) \in S_3$. S_3 is generated by $(123), (23)$, so this implies $D_6 \cong S_3$.


1
3
2


1
3
2