AM 106: Applied Algebra **Salil Vadhan**

Lecture Notes 11

October 11, 2018

1 Cosets

- **Def:** For a group G, $H \leq G$, and $a \in G$, the *left coset of H containing a* is the set $aH = \{ah : h \in H\}$. Similarly, the *right coset of H containing a* is $Ha = \{ha : h \in H\}$.

- **Examples:**

  - $G = \mathbb{Z}$, $H = 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$. (Note: $3\mathbb{Z}$ is *not* the left coset of $\mathbb{Z}$ containing 3. Why not?)

  - $G = S_3$, $H = \{\varepsilon, (23)\}$.

  - $G = \mathbb{R}^3$, $H = \{(x, y, z) : z = 0\}$.

- **Thm:** If $H \leq G$, then the cosets of H form a partition of G into disjoint subsets, each of size $|H|$.
  Proof:

  1. Every element $a \in G$ is contained in at least one coset:

  2. Every element $a \in G$ is contained in only one coset, i.e. if $a \in bH$, then $aH = bH$.

  3. The size of each coset aH is the same as the size of H.

- A picture:

- **Another View:** define a relation R_H on G by $a \sim b$ iff $a^{-1}b \in H$ ($\Leftrightarrow b \in aH \Leftrightarrow aH = bH$). This is an equivalence relation, whose equivalence classes are exactly the cosets of H. That is, $[a]_{R_H} = aH$.
  - Example: On $\mathbb{Z}$, $a \equiv b \pmod{n}$ iff $a - b \in n\mathbb{Z}$. The congruence classes modulo n are exactly the cosets of $n\mathbb{Z}$: $[a]_n = a + n\mathbb{Z}$.

2 Lagrange's Theorem and Related Results

- **Def:** For a group G and $H \leq G$, the *index of H in G* $[G : H]$ is the number of distinct left cosets of H in G.
- **Corollaries of Theorem above:** For a finite group G:
  - If $H \leq G$, then $[G : H] = |G|/|H|$.
  - (Lagrange's Thm) The order of a subgroup divides the order of the group. That is, if $H \leq G$, then $|H|$ divides $|G|$.
  - The order of an element divides the order of the group. That is, if $a \in G$, then the order of a divides $|G|$.
  - Every group of prime order is cyclic. That is, if $|G|$ is prime, then G is cyclic.
  - $a^{|G|} = e$ for every $a \in G$.
  - (Fermat's Little Thm) $a^p \equiv a \bmod p$ for every $a \in \mathbb{Z}$ and prime p.
    * Starting point for all (randomized and deterministic) polynomial-time primality testing algorithms!

3 Orbits and Stabilizers

- **Def:** For a permutation group $G \leq Sym(S)$ and a point $s \in S$,
  - The *orbit* of s under G is $\text{orb}_G(s) = \{\varphi(s) : \varphi \in G\}$,
  - The *stabilizer* of s in G is $\text{stab}_G(s) = \{\varphi \in G : \varphi(s) = s\}$.
- **Examples:** $G = D_5 \leq Sym(\mathbb{R}^2)$.
  - $s =$ center of pentagon.
  - $s =$ non-center point on vertical axis.
  - $s =$ point $5°$ clockwise from vertical axis.
- **Orbit-Stabilizer Theorem (Thm. 7.3):** $|\text{orb}_G(s)| = [G : \text{stab}_G(s)]$.
- Orbit–Stabilizer Thm follows from:
  Lemma: For $\varphi, \psi \in G$, $\varphi(s) = \psi(s)$ iff $\varphi\text{stab}_G(s) = \psi\text{stab}_G(s)$.
  Thus distinct points $\varphi(s)$ in the orbit are in one-to-one correspondence with distinct cosets $\varphi\text{stab}_G(s)$.

  Proof: