| | |
|---|---|
| **AM 106/206: Applied Algebra** | **Prof. Salil Vadhan** |

Lecture Notes 12

October 20, 2010

- Reading: Gallian Chapters 9 & 10

# 1 Normal Subgroups

- Motivation:
  - Recall that the cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ ($a+n\mathbb{Z}$) are the same as the congruence classes modulo $n$ ($[a]_n$)
  - These form a group under addition, isomorphic to $\mathbb{Z}_n^*$: $[a+b]_n = [a+b \bmod n]_n$ depends only on $[a]_n$ and $[b]_n$ (and not on the particular choice of coset representatives $a$ and $b$), so we can define $[a]_n + [b]_n = [a+b]_n$.
  - **Q:** under what conditions on $H \leq G$ do the left-cosets of $H$ form a group under the operation of $G$?
- **Def:** A subgroup $H$ of $G$ is *normal* iff for every $a \in G$, $aH = Ha$. If this holds, we write $H \lhd G$.
- **Proposition:** For $H \leq G$, the following are equivalent:
  - $H \lhd G$
  - for every $a \in G$, $aHa^{-1} = H$
  - for every $a \in G$, $h \in H$, $aha^{-1} \in H$. That is, if $h \in H$, then all *conjugates* of $h$ are also in $H$.
- **Examples:**
  - Which subgroups of an abelian group are normal?
  - Which subgroups of $S_4$ are normal?

  - $A_n \lhd S_n$

## 2 Factor Groups

- **Thm 9.2:** If $H \lhd G$, then the operation $(aH)(bH) = abH$ on the left-cosets of $H$ is well-defined (does not depend on the choice of coset representatives $a, b$) and forms a group, denoted $G/H$ (called a *factor group*, the *quotient* of $G$ by $H$, or "$G$ mod $H$").
- **Proof:**

- **Examples:**
  - $\mathbb{Z}/n\mathbb{Z}$
  - $S_n/A_n$
  - $(\mathbb{Z}_3 \times \mathbb{Z}_5)/(\mathbb{Z}_3 \times \{0\})$
  - $S_4/H$ where $H$ is the normal subgroup of size 4.
  - $\mathbb{Z}_n/\langle a \rangle$
  - $\mathbb{R}/\mathbb{Z}$

## 3 Homomorphisms

- **Def:** For groups $G$, $H$, and mapping $\varphi : G \to H$ is a *homomorphism* if for all $a, b \in G$, we have $\varphi(ab) = \varphi(a)\varphi(b)$.
  - Note: we don't require that $\varphi$ is one-to-one or onto!
- **Def:** For a homomorphism $\varphi : G \to H$,
  - the *image* of $\varphi$ is $\mathrm{Im}(\varphi) = \varphi(G) = \{\varphi(g) : g \in G\} \leq H$.
  - the *kernel* of $\varphi$ is $\mathrm{Ker}(\varphi) = \{g \in G : \varphi(g) = \varepsilon\} \lhd G$.
- **Thm 10.3:** If $\varphi : G \to H$ is a homomorphism, then $G/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$.
  **Picture:**

- **Examples:**

| Domain | Range | Mapping | Homo.? | Image | Kernel |
|---|---|---|---|---|---|
| $\mathbb{Z}$ | $\mathbb{Z}_n$ | $x \mapsto x \bmod n$ | | | |
| $\mathbb{Z}_n$ | $\mathbb{Z}_d$ | $x \mapsto x \bmod d$ | | | |
| $\mathbb{R}^n$ | $\mathbb{R}^n$ | $x \mapsto Mx$, $M$ a matrix | | | |
| $\mathbb{Z} \times \mathbb{Z}$ | $\mathbb{Z}$ | $(x, y) \mapsto xy$ | | | |
| $S_n$ | $\{\pm 1\}$ | $\sigma \mapsto \text{sign}(\sigma)$ | | | |
| $\mathbb{R}$ | $\mathbb{C}^*$ | $x \mapsto e^{2\pi i x}$ | | | |
| $\mathbb{Z}_3 \times \mathbb{Z}_5$ | $\mathbb{Z}_3$ | $(x, y) \mapsto x$ | | | |
| $G$ | $G/N$, where $N \lhd G$ | $g \mapsto gN$ | | | |

- **Properties of Homomorphisms:**

  1. $\varphi(\varepsilon_G) = \varepsilon_H$.
  2. $\varphi(a^{-1}) = \varphi(a)^{-1}$.
  3. order($\varphi(a)$) divides order($a$).

- **Properties of Images:**

  1. $\varphi(G)$ is a subgroup of $H$.
  2. $G$ cyclic $\Rightarrow \varphi(G)$ cyclic.
  3. $G$ abelian $\Rightarrow \varphi(G)$ abelian.

- **Properties of Kernels:**

  1. Ker($\varphi$) is *normal* subgroup of $G$.
     - Can prove that $K$ is normal by finding a homomorphism $\varphi$ s.t. Ker($\varphi$) $= K$.
  2. $\varphi(a) = \varphi(b) \Leftrightarrow b^{-1}a \in \text{Ker}(\varphi) \Leftrightarrow a\text{Ker}(\varphi) = b\text{Ker}(\varphi)$.
  3. $\varphi$ injective (one-to-one) if and only if Ker($\varphi$) $= \{\varepsilon\}$.

- **Proof of Thm 10.3 ($G/\text{Ker}(\varphi) \cong \text{Im}(\varphi)$):**