AM 106: Applied Algebra	**Salil Vadhan**

Lecture Notes 7

September 25, 2017

1 Subgroups

- Gallian Chapter 3.
- **Def:** A subset H of G is called a *subgroup* of G (denoted $H \leq G$) iff H is a group under the operation of G.
- **Example:** $\{0\} \leq \{\text{even integers}\} \leq \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ under addition.
- **Thms 3.1–3.3 (Subgroup Tests)**: For a subset H of a group G, the following are equivalent (TFAE):

  1. $H \leq G$.
  2. H is nonempty, and for all $a, b \in H$, we have $ab \in H$ and $a^{-1} \in H$.
  3. H is nonempty, and for all $a, b \in H$, we have $ab^{-1} \in H$.

  In case H is finite, the following condition is also equivalent to the above:

  4. H nonempty and for all $a, b \in H$, we have $ab \in H$.

  Proof:

  2⇒1:

  4⇒2:

  Other implications: in book

- **Example:** Subgroup lattice of $\mathbb{Z}_{12}$

- **Example:** Subgroup lattice of S_3

- **Example:** Subgroup lattice of $\mathbb{Z}_{12}^*$

- **Def:** For a group G and $g \in G$, the *(cyclic) subgroup generated by* g is $\langle g \rangle = \{g^n : n \in \mathbb{Z}\} = \{\ldots, g^{-2}, g^{-1}, g^0 = e, g^1 = g, g^2, \ldots\}$.

- **Examples:**
  - $\langle 3/2 \rangle$ in $\mathbb{R}^*$.
  - Cyclic subgroups of $\mathbb{Z}_1 2$, S_3, $\mathbb{Z}_{12}^*$

2 Cyclic Groups

- Reading: Gallian Chapter 4.

- **Def:** A group G is *cyclic* if $G = \langle g \rangle$ for some $g \in G$. Such an element g is called a *generator* of G.

- **Examples:**
  1. $\mathbb{Z}$?
  2. $\mathbb{Z}_n$?
  3. S_3?
  4. $\mathbb{Z}_{12}^*$?
  5. $\mathbb{Z}_{13}^*$?

- **Fact:** for every prime p, $\mathbb{Z}_p^*$ is cyclic. More generally, $\mathbb{Z}_n^*$ is cyclic if and only if $n = 4$ or n is of the form p^k or $2p^k$ for an odd prime p and $k \in \mathbb{N}$.
  (We will not prove this fact but you may use it throughout the course.)

- **Thm 4.1 (Classification of cyclic groups):** Let $G = \langle g \rangle$ be a cyclic group.
  1. If g has infinite order, then G is "like $\mathbb{Z}$ in the exponent": $\ldots, g^{-2}, g^{-1}, g^0 = e, g^1, g^2, \ldots$ are all distinct and $g^i \cdot g^j = g^{i+j}$.
  2. If g has finite order n, then G is "like $\mathbb{Z}_n$ in the exponent":

- $g^0, g^1, \ldots, g^{n-1}$ are all of the distinct elements of G.
- For an arbitrary integer k, $g^k = g^{k \bmod n}$, and thus $g^i \cdot g^j = g^{(i+j) \bmod n}$.

- **Example:** Arithmetic in $\mathbb{Z}_{13}^*$ and subgroup lattice of $\mathbb{Z}_{13}^*$

- **Proof of Thm 4.1, Item 2:**

- **Corollary:** $|\langle g \rangle| = |g|$.