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

Lecture Notes 6

September 22, 2010

1 More Groups

- Reading: Gallian Ch. 1,2
- Symmetric Group $Sym(S)$
  - Terminology
    - Injection = one-to-one function
    - Surjection = onto function
    - Bijection = one-to-one and onto function
    - Permutation = bijection from a set to itself
  - $Sym(S)$ is the set of all permutations $\pi : S \to S$ under composition. $\pi \circ \tau$ is the permutation defined by $(\pi \circ \tau)(x) = \pi(\tau(x))$.
  - $S_n = Sym(\{1, \ldots, n\})$.
  - **Example:** S_3
  - **Q:** $|S_n| =?$
- Dihedral Group D_n
  - "Symmetries" of regular n-gon, $n \geq 3$.
  - D_n is the set of distance-preserving transformations T of the plane such that $T(n\text{-gon}) = n\text{-gon}$.
  - Elements of D_n
    - If we label vertices $0, 1, \ldots, n-1$ (representing points in $\mathbb{R}^2$) clockwise, then each element $T \in D_n$ is determined by $T(0)$ and $T(1)$.
    - $\text{Rot}_k(i) = k + i \bmod n$: Clockwise rotation by $(k/n)360°$.
    - $\text{Ref}_k(i) = k - i \bmod n$: Reflection through line at $(k/n)180°$ clockwise from line through vertex 0.
  - Generalizes to define symmetries of other geometric objects, eg of tilings, of molecules, and of crystals (cf. Gallian Chs 27–28).

2 Subgroups

- Gallian Chapter 3.
- **Def:** The *order* of a group G, denoted $|G|$, is the number of elements in G (possibly ∞).
- **Def:** For a group G and $g \in G$, the *order* of g, denoted $|g|$, is the smallest positive integer n such that $g^n = e$ (or ∞ if no such n exists).
  Example: Orders in S_3

  Example: Orders in $\mathbb{Q}^*$

- **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⇒4:

  Other implications: in book

- **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 S_3, $\mathbb{Z}_{12}^*$