AM 106/206: Applied Algebra **Madhu Sudan**[1]

Lecture Notes 8

September 27, 2017

Reading: Gallian Chapters 6 and 7

1 Isomorphisms

- **Q:** When are two groups the "same" up to the names of elements?
- **Examples:**
  - $\mathbb{Z}_2$ and the group $G = \{x, y\}$ with the following Cayley table:

$\circ$	x	y
x	y	x
y	x	y

  - Any infinite cyclic group and $\mathbb{Z}$.
  - Any cyclic group of order n and $\mathbb{Z}_n$.
  - n-dimensional real vector space and $\mathbb{R}^n$

- **Def:** For groups G and H, an *isomorphism* from G to H is a mapping $\varphi : G \to H$ such that
  1. φ is a bijection (i.e. one-to-one and onto).
  2. for every $a, b \in G$, $\varphi(ab) = \varphi(a)\varphi(b)$. (Note that ab is computed using the operation of G, and $\varphi(a)\varphi(b)$ using the operation of H.)

  If there exists an isomorphism from G to H, we say that G and H are *isomorphic* and write $G \cong H$.

- Comments
  - Gallian writes $G \approx H$, but $G \cong H$ is more standard notation than $G \approx H$.
  - Isomorphism is an equivalence relation on groups.
- **More Examples**

[1]These notes are copied mostly verbatim from the lecture notes from the Fall 2010 offering, authored by Prof. Salil Vadhan. I will attempt to update them, but apologies if some references to old dates and contents remain.

- $S_4 \cong D_8$?

- $S_4 \cong \mathbb{Z}_{24}$?

- $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$?

- **Thm:** If A and B are the same size (i.e. there is a bijection $\pi : A \to B$), then $Sym(A) \cong Sym(B)$.
  - **Proof:** Consider the map $\varphi : Sym(A) \to Sym(B)$ given by $\sigma \mapsto \pi \circ \sigma \circ \pi^{-1}$.

  - Example: $A = \{1, 2, 3, 4, 5, 6, 7\}$, $B = \{a, b, c, d, e, f, g\}$, $\sigma = (15)(236)(47)$.

- Isomorphisms preserve all "group-theoretic properties" — properties that can be described in terms of the group operation and numbers of elements of the group (but not the specific names of those elements).

- **Examples (from Thms 6.2, 6.3:)** If $\varphi : G \to H$ is an isomorphism, then
  1. $\varphi(e) = e$.
  2. for all $g \in G$, $\varphi(g^{-1}) = \varphi(g)^{-1}$.
  3. $\text{order}(\varphi(g)) = \text{order}(g)$.
  4. if G is abelian, then H is abelian
  5. if G is cyclic, then H is cyclic
  6. if $G' \leq G$, then $\varphi(G') \overset{\text{def}}{=} \{\varphi(g) : g \in G'\} \leq H$.

     $\vdots$

2 Cayley's Theorem

- **Def:** We write $G \lesssim H$ if G is isomorphic to a subgroup of H. (Equivalently, there is a function $\varphi : G \to H$ satisfying all of the properties of an isomorphism except for being *onto*.)

- **Example:** $D_n \lesssim S_n$.

- **Cayley's Theorem:** For every group G, $G \lesssim Sym(G)$.

  - Every group is (isomorphic to) a permutation group!
  - The subgroups of S_n include all finite groups.

- **Proof of Cayley's Thm:**

  - **Example:** $\mathbb{Z}_5 \lesssim Sym(\{0, 1, 2, 3, 4\})$.

3 Automorphisms

- **Def:** An *automorphism* of a group G is an isomorphism from G to itself.
- **Prop:** The set $\mathrm{Aut}(G)$ of automorphisms of G form a group under composition.
  - "group-theoretic symmetries" of G
- **Example:** $\mathrm{Aut}(\mathbb{Z}_n)$.
- **Def:** $x, y \in G$ are *conjugates* if $y = axa^{-1}$ for some $a \in G$. (This is an equivalence relation on elements of G.)
- **Def:** For $a \in G$, the *inner automorphism* of G corresponding to a is the automorphism ϕ_a given by $\phi_a(x) = axa^{-1}$, aka "conjugation by a".
- **Prop:** The set $\mathrm{Inn}(G)$ of inner automorphisms of G form a group under composition.
- **Examples:**
  - $\mathrm{Inn}(Z_n)$
  - $\mathrm{Inn}(GL_n(\mathbb{R}))$
  - $\mathrm{Inn}(S_n)$
- **Note:** For every group G, $\mathrm{Inn}(G) \leq \mathrm{Aut}(G) \leq Sym(G)$.

- **Fact:** $\mathrm{Inn}(S_n) \cong S_n$ when $n \geq 3$.
- **Fact:** $\mathrm{Inn}(S_n) = \mathrm{Aut}(S_n)$ when $n \neq 6$.

4 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 $n\mathbb{Z}$: $[a]_n = a + n\mathbb{Z}$.

5 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!

6 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.
- Defs of $\text{stab}_G(s)$, $\text{orb}_G(s)$ for $G \leq Sym(S)$ and $s \in S$.
- **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: