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

Lecture Notes 9

October 4, 2010

Reading: Gallian Chapter 6

# 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:

$$\begin{array}{c|cc} \circ & x & y \\ \hline x & y & x \\ y & x & y \end{array}.$$

  - 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. $\varphi$ 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**
  - $S_4 \cong D_8$?

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

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

- **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. order$(\varphi(g)) =$ 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 $\varphi(G') \stackrel{\text{def}}{=} \{\varphi(g) : g \in G'\} \leq H$.

  $\vdots$

## 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 $\phi_a$ 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 $n \neq 6$.