AM 106: Applied Algebra		Salil Vadhan
	Lecture Notes 10	
		October 8, 2018

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:

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

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

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

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

- **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 $\sigma \mapsto \pi \circ \sigma \circ \pi^{-1}$ ("*conjugation* by π")

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

  - Important special case: $A = B$. Then for each permutation π of A, conjugation by π is isomorphism of $Sym(A)$ with itself — an *automorphism* of $Sym(A)$. In general, for any element π of a group G, $\sigma \mapsto \pi \circ \pi^{-1}$ is an automorphism of G.

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

     $\vdots$

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