

1. GROUP THEORY: BASIC CONCEPTS

1. GROUP HOMOMORPHISMS

- 1.1. Definition $\phi : G \rightarrow G'$, $\phi(xy) = \phi(x)\phi(y)$, $\forall x, y \in G$.
- 1.2. Properties: $\phi(e) = e'$, $\phi(x^{-1}) = (\phi(x))^{-1}$.
- 1.3. Group isomorphism: homomorphism AND bijective.

2. CYCLIC GROUPS

- 2.1. $C_\infty = (\mathbb{Z}, +)$, $C_n = \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\} \subset (\mathbb{C}^\times, \cdot)$ Note: $|C_n| = n$, $1 \leq n \leq \infty$. Concrete examples.
- 2.2. Definition $G = \langle x \rangle$, $\text{ord}(x)$. $x^k = e$ iff $\text{ord}(x) | k$. $|G| = \text{ord}(x)$.
- 2.3. $G = \langle x \rangle \simeq C_n$, where $n = |G| = \text{ord}(x)$. Construct a map: well-defined, bijective, group homomorphism.

3. PERMUTATION GROUPS

- 3.1. Set A , $|A| = n$. $S(A) = \{f : A \rightarrow A \text{ bijective function}\}$. $(S(A), \cdot, id_A)$ group.
- 3.2. $S(A) \simeq S_n =: S(\{1, 2, \dots, n\})$. $|S_n| = n!$.
- 3.3. (Highly) non-commutative.

4. SUBGROUPS

- 4.1. Notation. $H \leq G$. Closed under group operations. Note: $e \in H$.
- 4.2. Cosets: $gH \subset G$, $g \in G$. Example: $eH = H$.
- 4.3. Note: $|gH| = |H|$, $\forall g \in G$. Proof: bijective map $l_g : H \rightarrow gH$.
- 4.4. Important property: given $x, y \in G$, either $xH = yH$ OR $xH \cap yH = \emptyset$. Note: $xH = H$ iff $x \in H$, and $xH = yH$ iff $y^{-1}x \in H$.
- 4.5. Example: $G = \mathbb{Z}$, $H = 2\mathbb{Z}$.
- 4.6. $G = \sqcup_{j=1}^k g_j H$ (disjoint union). $|H| |G|$.
- 4.7. A group with 20 elements cannot have a subgroup with 7 elements.
- 4.8. Lagrange: $x^n = e$, $\forall x \in G$.
- 4.9. Example: shuffling cards.

5. QUOTIENT SPACE

- 5.1. $G/H = \{g_j H, j = 1, \dots, k\} = \{\hat{g}_1, \dots, \hat{g}_k\}$. $|G/H| = |G|/|H|$.
- 5.2. Equivalence relation: $x \sim_H y \Leftrightarrow xH = yH \Leftrightarrow y^{-1}x \in H$. Then $G/H = G/\sim_H$.
- 5.3. Example: $\mathbb{Z}/2\mathbb{Z} = \{\text{Even}, \text{Odd}\}$.

6. GROUP STRUCTURE

- 6.1. G/H has group structure $xH \cdot yH = xyH$ iff $H \trianglelefteq G$. Notation: $\bar{x} = xH$.
- 6.2. $\mathbb{Z}/2\mathbb{Z} \simeq C_2$, $\bar{2} = \text{Even}$, even+odd=odd etc.
- 6.3. Group homomorphism $p_H : G \rightarrow G/H$, $x \mapsto \bar{x}$.

7. NORMAL SUBGROUPS

- 7.1. A subgroup of an abelian group is automatically normal.
- 7.2. A group can have abelian, non-normal groups.
- 7.3. Example of non-normal subgroup in $SL_2(\mathbb{R})$.
- 7.4. Definition simple group (non-abelian).

8. HOMOMORPHISM REVISITED

- 8.1. $\phi : G \rightarrow G'$. Then $\ker \phi \trianglelefteq G$, and $\text{Im } \phi \leq G'$.
- 8.2. Every normal subgroup occurs in this manner: $p : G \rightarrow G/H$.
- 8.3. Theorem. $G/\text{Ker } \phi \simeq \text{Im } \phi \rightarrow 1$. Notation: $1 \rightarrow \ker \phi \rightarrow G \rightarrow \text{Im } \phi$.
- 8.4. Cyclic groups revisited. $\phi : \mathbb{Z} \rightarrow \langle x \rangle$ onto, so $\langle x \rangle \simeq \mathbb{Z}/\ker \phi$. Subgroups of \mathbb{Z} ? Theorem: a subgroup of a cyclic group is cyclic.
- 8.5. Corollary. $\mathbb{Z}/n\mathbb{Z} \simeq C_n$: new realization of cyclic group.
- 8.6. $\text{sgn} : S_n \rightarrow C_2$. Define $A_n = \ker \text{sgn} \trianglelefteq S_n$. Then $|A_n| = n!/2$. Example $S_3, A_3 =$ cyclic permutations.
- 8.7. Notation: $\phi : G \hookrightarrow G'$ etc.

9. PRODUCT OF GROUPS

- 9.1. $|G_1 \times G_2| = |G_1| \cdot |G_2|$.
- 9.2. $\mathbb{Z}^n = n$ -dimensional lattice.
- 9.3. Compare $C_2 \times C_2$ and C_4 : look at elements of order 4.

10. CAYLEY

- 10.1. Theorem. If $|G| = n$, then $G \hookrightarrow S_n$.
- 10.2. Group of automorphisms: $\text{Inn}(G) \subset \text{Aut}(G)$. $\alpha_g(x) = gxg^{-1}$, $\alpha : G \rightarrow \text{Aut}(G)$.
- 10.3. G abelian $\Leftrightarrow \text{Inn}(G) = e$.
- 10.4. Example of an outer automorphism: $\phi : \mathbb{R} \rightarrow \mathbb{R}$, $\phi(x) = 2x$.
- 10.5. $\text{Aut}(\mathbb{Z}), \text{Aut}(\mathbb{Z}^2)$.

11. GROUP ACTION

- 11.1. $X = \text{set}$, $\alpha : G \times X \rightarrow X$ map. Notation: $\alpha(g, x) = g \cdot x$. $e \cdot x = x, \forall x; g \cdot (h \cdot x) = gh \cdot x$. $g \in G$ induces: $\alpha(g, \cdot) = g : X \rightarrow X$
- 11.2. $\alpha_g : X \rightarrow X$ is injective.
- 11.3. We say that the set X carries an action of G .
- 11.4. Definition: transitive action.
- 11.5. Theorem. X admits a transitive action of G , then there exists a bijection (of sets) $G/H \rightarrow X$, $H = \text{Stab}_G(x_0)$, for some fixed base point x_0 .
- 11.6. Examples:
 - 1. $S_n/S_{n-1} = \{1, 2, \dots, n\}$
 - 2. Linear action: $GL_2(\mathbb{R})/B \simeq \mathbb{R}^2 - 0$, $GL_n(\mathbb{R})/P = \mathbb{R}^n - 0$, $SO(n)/SO(n-1) = S^{n-1}$.
 - 3. Not linear (Möbius transforms): $SL_2(\mathbb{R})/SO(2) = \mathbb{H}$. Thus $\Gamma \backslash SL(2, \mathbb{R})/K = \Sigma_g, g \geq 2$.
- 11.7. Counting orbits: $X = \sqcup_{j=1}^k O_{x_j} \Rightarrow |X| = |\text{Fix}_G(X)| + \sum_{j=1}^k \frac{|G|}{|\text{Stab}(x_j)|}$ (class equation).
- 11.8. Conjugacy action: $X = G$: $|G| = |Z(G)| + \sum_{j=1}^k |C_j|$, $|C_j| = |G|/|G_{g_j}| > 1$.

11.9. Corollary. $|G| = p \Rightarrow G \simeq C_p$.

11.10. Corollary. $|G| = p^n \Rightarrow p \mid |Z(G)| \Rightarrow \exists g \in Z(G) \leq G$ such that $g^p = 1$.

11.11. Theorem (Cauchy, Sylow): $p \mid |G| \rightarrow$ there exists an element of order p . Group action of $\mathbb{Z}/p\mathbb{Z}$ on $X := \{(g_1, \dots, g_p) : g_1 \dots g_p = 1\}$. Then

$$|G|^{p-1} = |X| = |Fix_{\mathbb{Z}/p\mathbb{Z}}(X)| + p + \dots + p \equiv |Fix| \pmod{p}$$

Since $(e, e, \dots, e) \in Fix \Rightarrow |Fix| \geq p$, i.e. there exists an element $g \in G$ such that $g^p = e$.

Question: the formula suggests there are at least $p - 1$ elements with this property.