Groups IA Mich

1 Groups and Homomorphisms

- Definitions of group: group axioms; abelian, finite, order of a group
- Subgroup: subset forms a group under same operation. 'Efficient subgroup test'
- Direct product of two groups forms a new group
- Some important groups: $k\mathbb{Z}$ (multiples of $k \in \mathbb{Z}$), D_{2n} (dihedral group, isometries of regular n-gon), C_n (n-th roots of unity)
- Permutation (invertible $X \to X$), $\mathrm{Sym}(X)$: all permutations of X, S_n: symmetric group, all permutation of the set $\{1, 2, ..., n\}$
- Homomorphisms: a mapping $\phi : H \to G$ (both groups) such that $\forall a, b \in H, \phi(a \cdot_H b) = \phi(a) \cdot_G \phi(b)$ (preserves some relationship)
- Isomorphism = invertible homomorphism (same structure)
  - Image and kernel of a homomorphism: $\mathrm{Im}(\phi) \leq G, \mathrm{Ker}(\phi) \leq H$
  - A homomorphism ϕ is an isomorphism $\iff$ $\mathrm{Im}(\phi) = G, \mathrm{Ker}(\phi) = \{e_H\}$
    (bijective $\iff$ surjective + injective)
  - Inverse of isomorphism is also an isomorphism
- Cyclic group, generator, (every element $= a^k, k \in \mathbb{Z}$)
  - Every cyclic group $\cong C_n$, for some $n = 1, 2, 3, ..., \infty$, with $C_\infty = (\mathbb{Z}, +, 0)$
  - Order of an element: $\mathrm{ord}(g)$ = smallest $k \in \mathbb{Z}_+$for which $g^k = e$, or $\mathrm{ord}(g) = \infty$ if $g^k \neq e$ for all $k \neq 0$
  - $\langle g \rangle = \{g^k : k \in \mathbb{Z}\} \leq G$ and $\langle g \rangle \cong C_n$, where $n = \mathrm{ord}(g)$

2 Cosets and Lagrange's Theorem

- Coset $gH = gh : h \in H$
- Lagrange's Theorem: $H \leq G \implies |H|$ divides $|G|$
- Fermat-Euler Theorem: let U_n be the group of invertible integers (units) in $\mathbb{Z}_n$, then $\forall x \in \mathrm{U}_n : |\langle x \rangle|$ divides $|\mathrm{U}_n| = \phi(n) \implies x^{\phi(n)} = 1$

3 Group Actions

- Group action $*: G \times X \to X$ (left action), axioms
- Examples of group action: regular action (on itself), act on cosets, conjugation action on itself, act on the set of all subgroup by conjugation
- Action of a group G on the set X gives a homomorphism $\rho : G \to \mathrm{Sym}(X)$, called the permutation representation of the action ($\rho(g)$ is a permutation on X that $\forall\, x : \rho(g)(x) = g * x$)
- Cayley's Theorem: every group G is isomorphic to a subgroup of some symmetric group
  (Action group G on the set G, have homomorphism $\rho : G \to \mathrm{Sym}(G)$, and $\mathrm{Im}(\rho) \leq \mathrm{Sym}(G), \mathrm{Ker}(\rho) = \{e\}$, so $G \cong \mathrm{Im}(\rho) \leq \mathrm{Sym}(G)$.)
- Orbit, stabiliser, kernel, faithful, transitive action, collection of orbits
- The set of orbits partitions X, the stabiliser of each element is a subgroup of G
- Orbit-stabiliser Theorem, Cauchy's Theorem

4 Möbius Group

- Functions defined on the extended complex numbers ($\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$) of the form $f(z) = \frac{ax+b}{cz+d}$, $a, b, c, d \in \mathbb{C}$
- Stereographic projection (wait till later)
- Form a group $\mathcal{M}$ under composition, generated by scaling/rotation, translation (and inversion)
- Classify transformations by fixed points:
  - 3 fixed points $\implies$ identity (max number of roots)
  - 2 fixed points: conjugate to scaling
  - 1 fixed point: conjugate to $z + 1$
- $\exists$ a Möbius transformation mapping any 3 points to any 3 points
- Cross ratio $[z_1, z_2, z_3, z_4] = \frac{(z_4-z_1)(z_2-z_3)}{(z_4-z_3)(z_2-z_1)}$

- Circles in $\hat{\mathbb{C}}$: set of z satisfying

$$Az\bar{z} + B\bar{z} + \bar{B}z + C = 0$$

with $A \in \mathbb{R}$, $B, C \in \mathbb{C}$, $B\bar{B} - AC > 0$, which are lines (union with ∞) or circles

- Circles are preserved under Möbius transformation, and $[z_1, z_2, z_3, z_4] \in \mathbb{R} \iff$ the four points lie on a circle

5 Finite Groups

- Quaternions: one element (-1) of order 2; 6 elements $(\pm i, \pm j, \pm k)$ of order 4, all square to -1, $ij = k$ etc.

$$Q_8 = \langle i, j \mid i^4 = 1, i^2 = j^2, ij = ji^{-1} \rangle$$

- Direct Product Theorem: homomorphism, surjective, injective
- Small order groups:
  - Order prime: cyclic C_p
  - All non-identity elements have order 2: $C_2 \times C_2 \times \cdots \times C_2$
  - Order 2: C_2
  - Order 4: $C_2 \times C_2$, C_4
  - Order 6: C_6 or D_6
  - Order 8: $C_2 \times C_2 \times C_2$, $C_4 \times C_2$, C_8, D_8, Q_8

6 Quotient Groups

- Normal subgroup, quotient map, operation on set of cosets
- Check for normal subgroup: find a homomorphism with the subgroup as kernel
- Isomorphism Theorem
- Simple Groups

7 Matrix Groups

- General linear group and special linear group: $\mathrm{GL}_n(\mathbb{F}), \mathrm{SL}_n(\mathbb{F})$
- Determinant as a surjective homomorphism $\det : \mathrm{GL}_n\mathbb{F} \to \mathbb{F}\backslash\{0\}$ with kernel $\mathrm{SL}_n(\mathbb{F})$
- Change of bases is a conjugation action of $\mathrm{GL}_n(\mathbb{F})$ on $M_n(\mathbb{F})$
- Möbius transformation as matrix multiplication
- Orthogonal and special orthogonal group $\mathrm{O}(n), \mathrm{SO}(n)$
- A matrix is orthogonal if and only if it preserve inner products
- In $\mathbb{R}^2$, $\mathrm{O}(n) = \{$ all matrices of det $1 =$ rotation and reflection $\}$
- Every element in $\mathrm{O}(2)$ is a composition of at most 2 reflections

8 Permutation

- Cycle notation
- Disjoint cycles commute, cycling of elements within each cycle
- S_n is generated by transpositions
- Disjoint cycle decomposition, uniqueness
- Sign of permutation
- Alternating group $A_n = \mathrm{Ker}(\mathrm{sgn})$
- Conjugation: in S_n and A_n: splitting of conjugacy classes if centraliser has no odd elements
- A_5 (and onwards) is simple