

# Math 55a Review part 2 - Group theory

(1)

- Lec. 1 • A group  $(G, \circ)$  is a set with an operation  $\circ : G \times G \rightarrow G$  st. (1)  $\exists e \in G$  identity s.t.  $eg = ge = g \forall g \in G$ ,  
 Artin ch. 2 (2)  $\forall g \in G \exists$  inverse  $g^{-1} \in G$  st.  $gg^{-1} = g^{-1}g = e$ , (3) associativity  $(ab)c = a(bc) \forall a, b, c \in G$ .

- A group is abelian if  $\circ$  is commutative ( $ab = ba \forall a, b \in G$ )

- Ex:  $(\mathbb{Z}, +)$ ,  $(\mathbb{Z}/n, +)$ ,  $(\mathbb{C}^*, \times)$ , symmetric group  $S_n$ ;  $GL_n(\mathbb{R})$  etc.; products  $G \times H$ ,  $\mathbb{Z}^n$ , ...

- like sets, groups can be finite  $(\mathbb{Z}/n, S_n, \dots)$ , countable  $(\mathbb{Z}, \mathbb{Z}^n, \mathbb{Q}, \dots)$ , uncountable  $(\mathbb{R}, \dots)$

- $H \subset G$  is a subgroup if  $e \in H$ ,  $a \in H \Rightarrow a^{-1} \in H$ ,  $a, b \in H \Rightarrow ab \in H$ .  $|H|$  divides  $|G|$ .  
 $H, H'$  subgroups of  $G \Rightarrow H \cap H'$  is a subgroup of  $G$ .

All subgroups of  $(\mathbb{Z}, +)$  are  $\mathbb{Z}n = \{mn / m \in \mathbb{Z}\}$  for some  $n \geq 0$ .

- A homomorphism  $\varphi: G \rightarrow H$  is a map st.  $\varphi(ab) = \varphi(a)\varphi(b) \forall a, b \in G$ . ( $\Rightarrow \varphi(a^{-1}) = \varphi(a)^{-1}$ )  
 isomorphism = bijective homomorphism, automorphism = isom.  $G \cong G$ .  $(\text{Aut}(G), \circ)$  is a group.

- The kernel of  $\varphi: G \rightarrow H$ :  $\ker(\varphi) = \{g \in G / \varphi(g) = e_H\}$  subgroup of  $G$ .  $\varphi$  injective  $\Leftrightarrow \ker \varphi = \{e\}$   
 The image of  $\varphi$ :  $\text{Im}(\varphi) = \{\varphi(g) / g \in G\} \subset H$  subgroup of  $H$ .  $\varphi$  surjective  $\Leftrightarrow \text{Im } \varphi = H$ .

- Given  $a \in G$ ,  $\varphi: \mathbb{Z} \rightarrow G$   $k \mapsto a^k$  is a homomorphism with  $\text{im}(\varphi) = \langle a \rangle$  subgp generated by  $a$ .

$\ker(\varphi) = \mathbb{Z}_n$  where  $n = \text{order of } a = \min \{n > 0 \text{ st. } a^n = e\}$ .

Hence the cyclic group  $\langle a \rangle$  is  $\cong \mathbb{Z}/n$  if  $a$  has order  $n$ ,  $\cong \mathbb{Z}$  if infinite order.

$(a_1, \dots, a_k)$  generate  $G$  if every element of  $G$  is a product of  $a_i$  and their inverses).

- Lec. 3 • A subgroup  $H \subset G$  determines an equivalence relation (axioms:  $a \sim a$ ;  $a \sim b \Leftrightarrow b \sim a$ ;  $\{a \sim b\} \cap \{b \sim c\} = \{a \sim c\}$ )  
 $a \sim b$  iff  $a^{-1}b \in H$ , whose equivalence classes are the (left) cosets  $aH = \{ah / h \in H\}$ .

The quotient set:  $G/H = \{\text{cosets } aH\}$ . The index of  $H$ :  $(G:H) = |G/H| = \frac{|G|}{|H|}$  if finite.

- Lec. 4 • If  $G$  is finite:  $H \subset G$  subgroup  $\Rightarrow |H|$  divides  $|G|$ ;  $a \in G \Rightarrow \text{ord}(a) | |G|$ ;  $|G| = p$  prime  $\Rightarrow G \cong \mathbb{Z}/p$ .
- A subgroup  $H \subset G$  is normal  $\Leftrightarrow aH = Ha \quad \forall a \in G \Leftrightarrow aHa^{-1} = H \quad \forall a \in G$ .  
 (left cosets = right cosets) (conjugate subgroups)

- The operation  $(aH)(bH) = abH$  makes  $G/H$  a group iff  $H$  is a normal subgroup.

- $\forall \varphi: G \rightarrow H$  homomorphism,  $\ker(\varphi) = K$  is a normal subgroup of  $G$ , and  $\text{Im}(\varphi) \cong G/K$ .

If  $\varphi$  is surjective, we have an exact sequence  $\{1\} \rightarrow K \xrightarrow{i} G \xrightarrow{\varphi} H \rightarrow \{1\}$   $\text{Im}(i) = \ker(\varphi)$ .  
 injective surjective

Ex:  $\{1\} \rightarrow H \subset G \rightarrow G/H \rightarrow \{1\}$ ;  $0 \rightarrow \mathbb{Z}/m \rightarrow \mathbb{Z}/mn \rightarrow \mathbb{Z}/n \rightarrow 0$  ( $\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n$  iff  $\text{gcd}(m, n) = 1$ )

$$\{e\} \rightarrow \mathbb{Z}/3 \rightarrow S_3 \xrightarrow{\text{sign}} \mathbb{Z}/2 \rightarrow \{e\}$$

A homomorphism  $G \xrightarrow{\varphi} H$  factors through  $G \rightarrow G/K \xrightarrow{\bar{\varphi}} H$  iff  $K \subset \ker \varphi$

- $G$  is simple if its only normal subgroups are  $\{e\}$  and itself. Ex:  $\mathbb{Z}/p$  p prime;  $A_n$ ,  $n \geq 5$ .

- Ex: the center  $Z(G) = \{z \in G / zg = gz \forall g \in G\}$  is a normal subgroup (abelian:  $zz' = z'z$ )

- Lec. 5 • Ex: the commutator subgroup  $[G, G] = \bigcap_{\text{finite}} \{[a_i, b_i]\}$ , where  $[a, b] = aba^{-1}b^{-1}$ , is normal, and  
 $G/[G, G] = \text{Ab}(G)$  (abelianization) largest abelian quotient of  $G$ .  $\forall G \xrightarrow{\varphi} H$ ,  $H$  abelian  
 factors  $G \rightarrow \text{Ab}(G) \xrightarrow{\bar{\varphi}} H$ .

- Lec. 19 • Every finitely generated abelian group is  $\cong \mathbb{Z}^r \times \mathbb{Z}/n_1 \times \dots \times \mathbb{Z}/n_k$  for some  $r, n_1, \dots, n_k$ .

Artin 14.7

- Group actions:  $G$ -action on set  $S$ :  $G \times S \rightarrow S$  st.  $e.s = s \quad \forall s \in S$  ( $\Leftrightarrow$  homom.  $\rho: G \rightarrow \text{Perm}(S)$ ) (2)
  $(g, s) \mapsto g \cdot s \quad (gh).s = g(h \cdot s)$   
faithful if  $\rho$  injective; transitive if  $\forall s, t \in S \exists g \in G$  st.  $g \cdot s = t$  (ie: 1 orbit)

Lec. 20

- The orbit of  $s \in S$  is  $O_s = G \cdot s = \{g \cdot s \mid g \in G\}$ . These form a partition  $S = \sqcup$  orbits.
- The stabilizer of  $s$  is  $\text{Stab}(s) = \{g \in G \mid g \cdot s = s\}$  subgroup of  $G$ .
- Elements in same orbit have conjugate stabilizer subgroups  $\text{Stab}(g \cdot s) = g \text{Stab}(s) g^{-1} \subset G$ .
- Orbit-stabilizer: if  $H = \text{Stab}(s)$ , then  $G/H \cong O_s$  bijection, in particular  $|O_s| \cdot |\text{Stab}(s)| = |G|$ .

Artin ch. 7

- Burnside's lemma ( $G, S$  finite): let  $S^g = \{s \in S \mid gs = s\}$  fixed points of  $g \in G$ , then #orbits =  $\frac{1}{|G|} \sum_{g \in G} |S^g|$
- $G$  acts on itself by left multiplication. This gives  $G \hookrightarrow \text{Perm}(G)$ , hence:  
 every finite group  $G$  is isomorphic to a subgroup of  $S_n$ ,  $n = |G|$ .
- $G$  acts on itself by conjugation:  $g$  acts by  $h \mapsto ghg^{-1}$ .
- orbits = conjugacy classes;  $\text{Stab}(h) = \{g \in G \mid gh = hg\} = Z(h)$  centralizer of  $h$ .
- Hence  $|G| = \sum_{\text{conj. classes}} |C_h|$ , where for each conj. class  $|C_h| = \frac{|G|}{|\text{Z}(h)|}$  divides  $|G|$ . (class eqn of  $G$ )
- For  $p$ -groups ( $|G| = p^k$ ), the class equation  $\Rightarrow |Z(G)| \geq p$  (number of conj. classes of size 1)  
 Hence  $\therefore |G| = p^2$ ,  $p$  prime  $\Rightarrow G$  is abelian ( $\cong \mathbb{Z}/p \times \mathbb{Z}/p$  or  $\mathbb{Z}/p^2$ )  
 • 5 isom. classes of groups of order 8:  $\mathbb{Z}/8, \mathbb{Z}/4 \times \mathbb{Z}/2, (\mathbb{Z}/2)^3, D_4$ , quaternion group.

Lec. 21:

- $G \subset SO(3)$  finite subgp  $\Rightarrow$  by considering the action of  $G$  on its poles (unit vectors along rotation axes),  
 $G \cong$  one of  $\mathbb{Z}/n$ ,  $D_n$  (regular  $n$ -gon),  $A_4$  (tetrahedron),  $S_4$  (cube),  $A_5$  (dodecahedron/icosahedron)

Lec. 22:

- The symmetric group  $S_n$  is generated by transpositions  $(ij)$ , in fact by  $s_i = (i \ i+1)$ .
- $\forall \sigma \in S_n \ \exists$  unique decomp of  $\sigma$  as product of disjoint cycles  $(a_1 \dots a_{k_1})$ .
- $\sigma, \tau \in S_n$  are in same conjugacy class iff they have the same cycle lengths.

- the alternating group  $A_n = \ker(\text{sign}: S_n \rightarrow \mathbb{Z}/2) = \{\text{products of even # of transpositions}\}$

Lec. 23:

- A conjugacy class in  $S_n$  which consists of even permutations is either 1 or 2 conj. classes in  $A_n$ ;  
 it splits into 2 iff the centralizer  $Z(\sigma) \subset A_n$  ( $\Leftrightarrow$  cycle lengths of  $\sigma$  are all odd & distinct).
- $A_n$  is simple for  $n \geq 5$  ( $A_4$  isn't:  $\{\text{id}, (ij)(kl)\} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$  is normal in  $A_4$  and  $S_4$ ).

Lec. 24:

- Sylow theorems:  $|G| = p^e m$ ,  $p \nmid m \Rightarrow$  a Sylow  $p$ -subgroup of  $G$  is a subgp. of order  $p^e$ .

Thm 1:  $\forall p$  prime  $|G|$ ,  $G$  contains a Sylow  $p$ -subgroup. ( $\rightarrow$  consequence:  $G$  contains an elt of order  $p$ )

Thm 2: all Sylow  $p$ -subgroups of  $G$  are conjugates of each other, and every subgroup of order  $p^k$  ( $k \leq e$ ) is contained in a Sylow subgroup.

Thm 3: the number  $s_p$  of Sylow  $p$ -subgroups satisfies  $s_p \equiv 1 \pmod{p}$  and  $s_p \mid m = \frac{|G|}{p^e}$ .

- If  $G$  contains subgroups  $N, H$  st.  $N \cap H = \{e\}$  (eg because  $\gcd(|N|, |H|) = 1$ ) and  $|G| = |N| \cdot |H|$ , then  $\forall g \in G \ \exists$  unique  $n \in N, h \in H$  st.  $g = nh$ .

If  $N$  and  $H$  are both normal in  $G$  then  $G \cong N \times H$ . If  $N$  is normal but not  $H$ , we have a semidirect product  $N \rtimes_{\varphi} H$ ,  $\varphi: H \rightarrow \text{Aut}(N)$  given by conjugation inside  $G$ .

$$(n, h) \cdot (n', h') = (n \varphi(h)(n'), hh')$$

- Lec. 25
- Given  $H \subset G$  (eg.  $p$ -Sylow), the number of conjugate subgroups  $gHg^{-1} \subset G$  (eg. all  $p$ -Sylows) equals  $|G/N(H)|$ ,  $N(H)$  normalizer  $= \{g \in G \mid gHg^{-1} = H\}$  (largest subgp of  $G$  st.  $H$  is normal inside  $N$ ).
  - Example:  $|G|=15 \Rightarrow$  Sylow subgroups of order 3 and 5 are normal ( $s_3 = s_5 = 1 \Rightarrow G = \mathbb{Z}_3 \times \mathbb{Z}_5$ ).  
 $|G|=21 \Rightarrow s_3 \in \{1, 7\}$ ,  $s_7 = 1$ , so either  $G = \mathbb{Z}_3 \times \mathbb{Z}_7$  or semidirect prod  $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$ .  
 $|G|=12 \Rightarrow$  1 or 3 2-Sylows, one of these is normal  $\Rightarrow$  5 iron-clad classes:  
 1 or 4 3-Sylows  $\mathbb{Z}_4 \times \mathbb{Z}_3, (\mathbb{Z}/2)^2 \times \mathbb{Z}_3, A_4, D_6, \mathbb{Z}_3 \times \mathbb{Z}_4$ .

- Lec. 26
- The free group  $F_n = \langle a_1, \dots, a_n \rangle = \{\text{all reduced words } a_1^{m_1} \dots a_n^{m_k}\}$  (words in  $a_i^{\pm 1}$  never simplify except  $a_i a_i^{-1} = a_i^{-1} a_i = 1$ )
  - Any group  $G$  with  $n$  generators  $g_1, \dots, g_n$  is a quotient of  $F_n$ , via  $\varphi: F_n \xrightarrow{\text{a}_i \mapsto g_i} G$ .  $G$  is finitely presented if  $\text{Ker}(\varphi)$  is generated by a finite set  $r_1, \dots, r_k$  & their conjugates. Write  $G \cong \langle g_1, \dots, g_n \mid r_1, \dots, r_k \rangle = F_n / \langle \text{normal subgp gen'd by conjugates of } r_j \rangle$ .
  - The Cayley graph of  $G$  w/ generators  $g_i$ : vertices = elements of  $G$   
 edges: connect  $g$  to  $g \cdot g_i \quad \forall g \in G, \forall g_i$ .
  - A normal form for elements of  $G = \langle g_1, \dots, g_n \mid r_1, \dots, r_k \rangle$  is a set of words in  $g_1^{\pm 1}, \dots, g_n^{\pm 1}$  st. every element of  $G$  appears exactly once among these.

- Lec. 27
- Ex:  $S_n \cong \langle \sigma_1, \dots, \sigma_{n-1} \mid \sigma_i^2 = 1, \sigma_i \sigma_j = \sigma_j \sigma_i \quad |i-j| \geq 2, \sigma_i \sigma_j \sigma_i = \sigma_j, \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \rangle$ .  
 $SL_2(\mathbb{Z})$  is gen'd by  $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ .  $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z}) / \{\pm I\} = \langle S, T \mid S^2, (ST)^3 \rangle$

- Lec. 28
- A representation of  $G$  is a vector space  $V$  on which  $G$  acts by linear operators; i.e.  $\rho: G \rightarrow GL(V)$ .
  - Artin ch. 10: A subrepresentation is a subspace  $W \subset V$  invariant under  $G$ :  $g(w) = w \quad \forall g \in G$ .  $V$  is irreducible if has no nontrivial subrepresentations.
  - Fulton-Harris ch. 1-2:  $G$  finite,  $V$  finite dim./ $\mathbb{C}$ : each  $g: V \rightarrow V$  has finite order,  $g^n = \text{Id} \Rightarrow$  diagonalizable,  $\lambda_j = e^{\frac{2\pi i k}{n}}$
  - if  $G$  is abelian, all operators  $g: V \rightarrow V$  are simultaneously diagonalizable  $\Rightarrow$  irreduc. rep's are 1-dim!. These correspond to elements of the dual group  $\widehat{G} = \text{Hom}(G, \mathbb{C}^*)$ . (Note  $\widehat{\mathbb{Z}/m}$  is  $\cong \mathbb{Z}/m$ )
  - a homomorphism of representations is a  $G$ -equivariant linear map, i.e.  $\varphi(gv) = g\varphi(v)$ .
  - $V, W$  rep's of  $G \Rightarrow$  so are  $V \oplus W$ ,  $V \otimes W$  ( $g: v \otimes w \mapsto gv \otimes gw$ ),  $V^*$  ( $l \mapsto l \circ g^{-1}$ ),  $V^* \otimes W \cong \text{Hom}(V, W)$  ( $\varphi \mapsto g \circ \varphi \circ g^{-1}$ ). ( $\text{Hom}_G(V, W) = \text{invariant part } \text{Hom}(V, W)^G$ )
  - Any  $\mathbb{C}$ -representation of a finite group  $G$  admits an invariant Hermitian inner product, with respect to which  $G$  acts by unitary operators.

- Lec. 29
- $V$  rep. of a finite group (over  $\mathbb{C}$ ),  $W \subset V$  invariant subspace  $\Rightarrow \exists U \subset V$  invariant st.  $V = U \oplus W$ . Hence: any  $\mathbb{C}$ -representation of a finite group decomposes into a direct sum of irreducibles.
  - Schur's lemma:  $V, W$  irred. rep's of  $G \Rightarrow$  any homom.  $\varphi \in \text{Hom}_G(V, W)$  is either zero or an isomorphism; and all iso's of an irred. rep. are multiples of id:  $\text{Hom}_G(V, V) = \mathbb{C} \cdot \text{id}_V$ .
  - Ex: rep's of  $S_n$ : trivial rep  $U = \mathbb{C}$ ,  $\sigma$  acts by id; alternating rep:  $U' = \mathbb{C}$ ,  $\sigma$  acts by  $(-1)^\sigma$ . standard rep. (dim.  $n-1$ ):  $V = \{(z_1, \dots, z_n) \mid \sum z_i = 0\} \subset \mathbb{C}^n$ ,  $\sigma$  acts by permuting coords:  $e_i \mapsto e_{\sigma(i)}$ .  $U, U', V$  are the only irred. rep's of  $S_3$ .

- Lec. 30: • The key tool to study representations is the character  $\chi_V: G \rightarrow \mathbb{C}$ ,  $\chi_V(g) = \text{tr}(g: V \rightarrow V)$  (In terms of eigenvalues,  $\text{tr}(g) = \sum \lambda_i$ , and  $\text{tr}(g^k) = \sum \lambda_i^k$ , so  $\chi_V$  recovers all symmetric polynomial expressions in the  $\lambda_i$ , hence the  $\lambda_i$  as unordered tuple).
- $\chi_V: G \rightarrow \mathbb{C}$  is a class function, ie.  $\chi_V(hgh^{-1}) = \chi_V(g)$ .
- $\chi_{V \oplus W} = \chi_V + \chi_W$ ,  $\chi_{V \otimes W} = \chi_V \chi_W$ ,  $\chi_{V^*} = \overline{\chi_V}$ ,  $\chi_{\text{Hom}(V, W)} = \overline{\chi_V} \chi_W$ .
  - for a permutation rep. ( $G$  acting on  $S \rightsquigarrow G$  acts on  $V$  with basis  $(e_s)_{s \in S}$ ,  $g \cdot e_s = e_{g \cdot s}$ )  $\chi(g) = \#\{s \in S / g \cdot s = s\} = |S^g|$ .

• Character table of  $G$  = list, for each irred. rep.  $V_i$ , the value of  $\chi_{V_i}$  on each conjugacy class.

•  $\varphi = \frac{1}{|G|} \sum_{g \in G} g: V \rightarrow V$  projection onto  $V^G = \{v \in V / gv = v \forall g\}$ , so  $\dim(V^G) = \text{tr}(\varphi) = \frac{1}{|G|} \sum_g \chi_V(g)$

- Lec. 31
- $H(\alpha, \beta) = \frac{1}{|G|} \sum_{g \in G} \overline{\alpha(g)} \beta(g)$  Hermitian inner product on  $\mathbb{C}_{\text{Class}}(G) = \{\text{class functions } G \rightarrow \mathbb{C}\}$   
Then  $\dim \text{Hom}_G(V, W) = H(\chi_V, \chi_W)$ .

- The characters of the irreducible reps of  $G$  are an orthonormal basis of  $(\mathbb{C}_{\text{Class}}(G), H)$ . In particular the number of irred. reps = number of conjugacy classes
- The multiplicities  $a_i$  in the decomposition of a  $G$ -rep.  $W$  into irreducibles  $W \cong \bigoplus_i V_i^{\otimes a_i}$  are given by  $a_i = \dim \text{Hom}_G(V_i, W) = H(\chi_{V_i}, \chi_W)$ . Moreover,  $H(\chi_V, \chi_W) = \sum_i a_i^2$ .
- The regular rep. of  $G$  (=permutation rep. for  $G$  acting on itself by left multiplication) contains each irred. rep.  $V_i$  with multiplicity  $= \dim V_i$ ; therefore  $|G| = \sum_i (\dim V_i)^2$ .

- Lec. 32-33
- These results allow us to find character tables of various groups (eg.  $S_4, A_4, S_5, A_5$ ) by starting from known representations, considering tensor products, and using  $H(\cdot, \cdot)$  pairings and orthogonality to find irreducible pieces & the missing irreducible reps.