math32001 - group theory

available at jtang.dev/resources

(1) revision of subgroups and cosets

group: $(G, *)$ where $G \neq \emptyset$ and
$(G1)$ $\forall a, b \in G, a * b \in G$
$(G2)$ $\forall a, b, c \in G, (ab)c = a(bc)$
$(G3)$ $\exists 1_G \in G, 1_G a = a = a 1_G, \forall a \in G$
$(G4)$ $\forall a \in G, \exists a^{-1} \in G, aa^{-1} = 1_G = a^{-1}a$

subgroup criterion: suppose G is a group and $H \subseteq G$
$H \leq G \iff H \neq \emptyset$ and $\forall a, b \in H$, $ab^{-1} \in H$

right coset: suppose G a group, $H \leq G$ and $a \in G$
$Ha = \{ha \mid h \in H\} \subseteq G$

theorem: suppose G is a group and $H \leq G$
(1) if $g \in G$, then $g \in Hg$
(2) let $a, b \in G$, $Ha = Hb \iff ab^{-1} \in H$
(3) let $a, b \in G$, either $Ha = Hb$ or $Ha \cap Hb = \emptyset$
(4) G is the disjoint union of right cosets of H
(5) if $g \in G$, then $|H| = |Hg|$

theorem: suppose G is a finite group and $H \leq G$
(1) langrange's theorem: $|G| = [G : H]|H|$
(2) if $K \leq G$ and $K \subseteq H$, then $[G : K] = [G : H][H : K]$

theorem: $(S_n, *)$ is a group and $|S_n| = n!$

disjoint cycles: $(\alpha_1, \alpha_2, \ldots, \alpha_r)$, $(\beta_1, \beta_2, \ldots, \beta_s)$ with $\{\alpha_1, \alpha_2, \ldots, \alpha_r\} \cap \{\beta_1, \beta_2, \ldots, \beta_s\} = \emptyset$

theorem: any permutation in S_n can be written as a product of pairwise disjoint cycles

(2) more examples of groups

direct product: suppose $(H, *)$ and $(K, \odot)$ are groups. let $h, h' \in H$ and $k, k' \in K$ and define
$(h, k)(h', k') = (h * h', k \odot k') \in H \times K$

lemma: $|GL_n(q)| = (q^n - 1)(q^n - q)(q^n - q^2) \ldots (q^n - q^{n-1})$

transposition: a two-cycle (α_1, α_2) with $\alpha_1, \alpha_2 \in \Omega$

lemma: for $n \geq 2$, every permutation in S_n can be written as a product of transpositions

even permutation: $\sigma \in S_n, n \geq 2$, where σ can be written as a product of an even number of transpositions
odd permutation: $\sigma \in S_n, n \geq 2$, where σ can be written as a product of an odd number of transpositions

$c(\sigma)$ = number of cycles when σ is written as a product of pairwise disjoint cycles (including cycles of length 1)

lemma: for $n \geq 2$, let $\sigma, \tau \in S_n$, τ be a transposition, then $c(\sigma\tau) = c(\sigma) \pm 1$

$s(\sigma) = (-1)^{n - c(\sigma)}$ which has values ± 1

(2) even more examples of groups

lemma: let $n \geq 2$, if $\sigma \in S_n$ can be written as a product of r transpositions, then $s(\sigma) = (-1)^r$

corollary: let $n \geq 2$, if $\sigma \in S_n$ can be written as a product of r_1, r_2 transpositions, then r_1 and r_2 have the same parity

remark: $(\alpha_1 \alpha_2 \ldots \alpha_r)$ is even (odd) if r is odd (even)

A_n = set of all even permutations $(n \geq 2)$

lemma: let $n \geq 2$, then $A_n \leq S_n$

remark: $|A_n| = \frac{1}{2} n!$

(3) subgroups

suppose G is a group, $g \in G$, $A, B \subseteq G$, $\emptyset \neq S \subseteq G$, then
(1) conjugate of A by g, $A^g = \{g^{-1}ag \mid a \in A\}$
(2) setwise product of A and B, $AB = \{ab \mid a \in A, b \in B\}$
(3) $A^- = \{a^{-1} \mid a \in A\}$
(4) $C_G(S) = \{g \in G \mid xg = gx, \forall x \in S\}$
(5) $N_G(S) = \{g \in G \mid S^g = S\}$
(6) $\langle S \rangle = \{x_1 x_2 \ldots x_n \mid x_i \in S \cup S^-, n \in \mathbb{N}\}$

remarks
(1) $C_G(S) \subseteq N_G(S)$
(2) if $\emptyset \neq S \leq G$, then $S \subseteq N_G(S)$
(3) $S \cup S^- \subseteq \langle S \rangle$, and if $R \subseteq S$, then $\langle R \rangle \leq \langle S \rangle$
(4) if $S = \{x\}$, then $C_G(S) = C_G(x)$ and $\langle S \rangle = \langle x \rangle$

lemma: suppose G is a group, $\emptyset \neq S \subseteq G$, then $C_G(S), N_G(S)$ and $\langle S \rangle$ are all subgroups of G

remark: $C_G(S) \leq N_G(S) \leq G$

$Z(G) = \{g \in G \mid gx = xg, \forall x \in G\}$

lemma: since $Z(G) = C_G(G)$, we have $Z(G) \leq G$

lemma: suppose G is a group, $H, K \leq G$, then
$HK \leq G \iff HK = KH$

remark: let G be a group with $H, K \leq G$, then

$$HK = \bigcup_{k \in K} Hk = \bigcup_{h \in H} hK$$

so HK is the union of certain right cosets of H

lemma: suppose G is a finite group, $H, K \leq G$, then

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

corollary: suppose G is a finite group, $H, K \leq G$
if $|G| = \frac{|H||K|}{|H \cap K|}$, then $G = HK$

(4) conjugacy and class equation

suppose G is a group, $\emptyset \neq S \subseteq G$, $g \in G$
conjugate of S: $S^g = \{g^{-1}xg \mid x \in S\}$

remarks: suppose G is a group, $\emptyset \neq S \subseteq G$
(1) let $g \in G$, then $|S| = |S^g|$
(2) let $g \in G$, if $S \leq G$ then $S^g \leq G$
(3) if $x, y \in G$, x and y are conjugate (i.e. $x = g^{-1}yg$), then x and y have the same order
(4) $1^G = \{g^{-1}1g \mid g \in G\} = \{1\}$
(5) $x^G = \{x\} \iff x \in Z(G)$

lemma: let G be a group, then G is a disjoint union of its conjugacy classes

lemma: suppose G is a group and $\emptyset \neq S \subseteq G$ and set $N = N_G(S)$. let $\{g_i \mid i \in I\}$ be a complete set of representatives for the right cosets of N in G. then, the set of conjugates in S are $\{s^{g_i} \mid i \in I\}$ and $S^{g_i} = S^{g_j} \iff g_i = g_j$. in particular, if G if finite, then the number of conjugates of S is equal to $[G : N] = \frac{|G|}{|N|}$

remark: if G if a finite group and $\emptyset \neq S \subseteq G$, then the number of conjugates of S divides $|G|$

lemma: suppose G is a group, $x \in G$ and $C = C_G(x)$. let $\{g_i \mid i \in I\}$ be a complete set of representatives for the right cosets of C in G. then, the conjugacy classes of x are $x^G = \{x^{g_i} \mid i \in I\}$ and $x^{g_i} = x^{g_j} \iff g_i = g_j$. in particular, if G is finite then $|x^G| = [G : C] = \frac{|G|}{|C|}$ and so $|x^G| \big| |G|$

class equation: suppose G is a finite group and let $x_1, x_2, \ldots, x_k \in G$ be chosen, one from each of the k conjugacy classes of G. set $n_i = |x_i|$. assume our notation is chosen such that $n_1 = n_2 = \cdots = n_l = 1$ and $n_i > 1$ for $i \geq l$, then
(1) $|G| = \sum_{i=1}^{k} n_i = \sum_{i=1}^{k} [G : C_G(x_i)]$
(2) $|G| = |Z(G)| + \sum_{i=l+1}^{k} n_i$
(3) $|G| = |Z(G)| + \sum_{i=l+1}^{k} [G : C_G(x_i)]$

p**-group**: a group G with $|G| = p^a$ for some prime p and $a \in \mathbb{N} \cup \{0\}$

lemma: if G is a p-group, $G \neq \{1_G\} \implies Z(G) \neq \{1_G\}$

(5) group actions

suppose G is a group and $\Omega \neq \emptyset$. we say that G **acts on** Ω (or Ω is a G**-set**) if for each $g \in G$ and each $\alpha \in \Omega$
(A1) $\forall \alpha \in \Omega, \forall g_1, g_2 \in G, \alpha(g_1 g_2) = (\alpha g_1) g_2$
(A2) $\forall \alpha \in \Omega, \alpha 1_G = \alpha$

G**-orbit of** α: $\alpha^G = \{\alpha g \mid g \in G\} \subseteq \Omega$

lemma: suppose Ω is a G-set, then Ω is the disjoint union of its G-orbits

stabilizer of α: $G_\alpha = \{g \in G \mid \alpha g = \alpha\}$

(5) group actions

lemma: suppose Ω is a G-set and $\alpha \in \Omega$, then $G_\alpha \leq G$

lemma: suppose G is a finite group which acts on Ω and let Δ be a G-orbit of Ω, then
(1) for any $\alpha \in \Delta$, $|\Delta| = [G : G_\alpha] = \frac{|G|}{|G_\alpha|}$
(2) for any $\alpha, \beta \in \Delta$, $g \in G$ with $\alpha g = b$, we have $G_\alpha^g = G_\beta$

theorem: suppose G is a finite group which acts on Ω
(1) Ω is the disjoint union of its G-orbits
(2) for any $\alpha \in \Omega$, $G_\alpha \leq G$
(3) let $\Delta_1, \ldots, \Delta_m$ be the G-orbits of Ω.
if $\alpha_i \in \Delta_i$ for $i = 1, \ldots, m$, then

$$|\Omega| = \sum_{i=1}^{m} |\Delta_i| = \sum_{i=1}^{m} [G : G_{\alpha_i}]$$

and each $|\Delta_i| \big| |G|$

cauchy's theorem: suppose G is a finite group and p is a prime. if $p \big| |G|$, then G contains at least one element of order p

transitively: suppose Ω is a G-set. we say that G acts transitively on Ω if Ω is a G-orbit. in symbols, $\forall \alpha \in \Omega, \alpha^G = \{\alpha g \mid g \in G\} = \Omega$

$fix_\Omega(g) = \{\alpha \in \Omega \mid \alpha g = \alpha\}$ (Ω a finite G-set, $g \in G$)

burnside's theorem: suppose G is a finite group which acts on a finite set Ω. if G has t orbits of Ω, then

$$t = \frac{1}{|G|} \sum_{g \in G} |fix_\Omega(g)|$$

(6) finitely generated abelian groups (fgag)

finitely generated: a group G such that $\langle S \rangle = G$ for a finite subset $S \subseteq G$
abbreviation: fgag for finitely generated abelian group

lemma: let $n, m \in \mathbb{N}$. $\mathbb{Z}_n \times \mathbb{Z}_m \iff hcf(n, m) = 1$

classification theorem for fgag: any fgag G is isomorphic to a direct product of cyclic groups

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \mathbb{Z}_{n_k} \times \mathbb{Z}^s$$

where $s > 0$ and $n_i \mid n_{i+1}$ for $i = 1, \ldots, k-1$

rank of G: the value s above
torsion coefficients of G: the values $n_1, \ldots, n_k$ as above

corollary: any finite abelian group G is isomorphic to $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \mathbb{Z}_{n_k}$ where $n_i \mid n_{i+1}$ for $i = 1, \ldots, k-1$. in addition, $|G| = n_1 n_2 \ldots n_k$

corollary: any fgag which has no elements of finite order (apart from 1) is isomorphic to $\mathbb{Z}^s$ for some $s \geq 0$

(6) finitely generated abelian groups (fgag)

theorem
let $G_1 = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \mathbb{Z}_{m_k} \times \mathbb{Z}^s \quad (s > 0, m_i \mid m_{i+1})$
and $G_2 = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \mathbb{Z}_{n_l} \times \mathbb{Z}^t \quad (t > 0, n_i \mid n_{i+1})$
then $G_1 \cong G_2 \iff s = t, k = l, m_i = n_i$ for $i = 1, \dots, k$

(7) normal subgroups and factor groups

normal subgroup: $N \leq G$ such that $\forall g \in G, N^g = N$
notation: $N \trianglelefteq G$ if N is a normal subgroup of G

lemma: suppose G is a group, $N \leq G$, then $N \trianglelefteq G$ is equivalent to the following statements:
(1) $N_G(N) = G$
(2) the conjugates of N are $\{N\}$
(3) $\forall g \in G, \forall n \in N, n^g = g^{-1}ng \in N$
(4) $\forall g \in G, Ng = gN$
(5) N is the union of some conjugacy classes of G

lemma: suppose G is a group, $H \leq G$. if $[G : H] = 2$, then $H \trianglelefteq G$

notation: for $g \in G, Ng = \overline{g}$
factor group of G by N: $G/N = \{Ng \mid g \in G\}$ with binary operation $\overline{x} \cdot \overline{y} = \overline{xy}$

remarks
(1) the elements of G/N are right cosets of N in G
(2) $1_{G/N} = \overline{1} = N$ and for $\overline{x} \in G/N, \overline{x}^{-1} = \overline{x^{-1}}$
(3) if G is a finite group, then $|G/N| = [G : N] = \frac{|G|}{|N|}$
(4) the order of $\overline{x}$ in G/N is the smallest $n \in \mathbb{N}$, $x^n \in N$

lemma: if $G/Z(G)$ is a cyclic group, then G is abelian

lemma: if G is a group and $|G| = p^2$ for some prime p, then G is abelian

lemma: every subgroup of G/N is of the form H/N where $N \leq H \leq G$. also $H/N \trianglelefteq G/N \iff H \trianglelefteq G$

homomorphism from G to K: $\theta : G \to K$, such that $\forall g_1, g_2 \in G, \theta(g_1 g_2) = \theta(g_1)\theta(g_2)$
$Im(\theta) = \{\theta(g) \mid g \in G\} \subseteq K$
$ker(\theta) = \{g \in G \mid \theta(g) = 1_K\} \subseteq G$

lemma: suppose θ is a group-homomorphism, $\theta : G \to K$
(1) $\theta(1_G) = 1_K$
(2) $\forall g \in G, \theta(g^{-1}) = \theta(g)^{-1}$
(3) $Im(\theta) \leq K$
(4) $ker(\theta) \trianglelefteq G$

first isomorphism theorem: suppose G and K are groups and $\theta : G \to K$ is a homomorphism. then

$$G/ker(\theta) \cong Im(\theta)$$

second isomorphism theorem: suppose G is a group, $H \leq G$, and $N \trianglelefteq G$

$$H/(H \cap N) \cong NH/N$$

(7) normal subgroups and factor groups

third isomorphism theorem: suppose G is a group, $N \leq M \leq G$ and $N, M \trianglelefteq G$

$$(G/N)/(M/N) \cong G/M$$

(8) simple groups and jordan-hölder theorem

simple group: a group $G \neq \{1\}$ with G and $\{1\}$ as the only normal subgroups

lemma: suppose G is a group, $N \trianglelefteq G$, $g \in G$, $n \in N$. then, $n^{-1}g^{-1}ng \in N$

commutator of n and g: $[n, g] = n^{-1}g^{-1}ng$

lemma: let $n \in \mathbb{N}, n \geq 5$
(1) every element of A_n can be written as a product of 3-cycles
(2) the 3-cycles of A_n are all conjugate in A_n

lemma: A_5 is a simple group

theorem: for $n \geq 5, A_n$ is a simple group

composition series of G: the subgroups $G_1, \dots, G_n$ of a finite group G such that
(1) $G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = \{1\}$
(2) $G/G_1, G_1/G_2, \dots G_{n-1}/G_n$ are all simple groups

composition factors of G: $G/G_1, G_1/G_2, \dots, G_{n-1}/G_n$

remark: none of G_i/G_{i+1} are of order 1

maximal normal subgroup of G: K such that $K \trianglelefteq G$ and whenever $K \trianglelefteq N \trianglelefteq G$, then $K = N$ or $N = G$

remarks
(A) K is a maximal subgroup of G if $K \trianglelefteq G \iff G/K$ is a simple group
(B) $N_1 \trianglelefteq G, N_2 \trianglelefteq G \implies N_1N_2 \trianglelefteq G$
(C) $N_1 \trianglelefteq G, N_2 \trianglelefteq G \implies N_1 \cap N_2 \trianglelefteq G$
(D) $N \trianglelefteq G, H \leq G \implies HN/N \cong H/(H \cap N)$

lemma: any non-trivial finite group G has at least one composition series

jordan-hölder theorem: suppose G is a finite group, $G \neq \{1\}$ with composition series

$$G \trianglerighteq H_1 \trianglerighteq H_2 \cdots \trianglerighteq H_r = \{1\}$$
$$G \trianglerighteq K_1 \trianglerighteq K_2 \cdots \trianglerighteq K_s = \{1\}$$

then $r = s$, and $\{G/H_1, H_1/H_2, \dots, H_{r-1}/H_r\}$ and $\{G/K_1, K_1/K_2, \dots, H_{s-1}/K_s\}$ are the same simple groups up to isomorphism and multiplicity.

(9) sylow's theorems and applications

sylow's theorems: suppose G is a finite group, $|G| = p^r m$ where p is a prime, $r \in \mathbb{Z}, r \geq 0$ and $p \nmid m$.
(1) there exists at least one subgroup P of G with $|P| = p^r$
(2) the subgroups of G of order p^r form a conjugacy class
(3) if $X \leq G$ and X is a p-group, then $X \leq P^g$ for some $g \in G$
(4) if n is the number of subgroups of G of order p^r, then $n \mid m$ and $n \equiv 1 \pmod p$

notation: $Syl_p(G)$ is the set of Sylow p-subgroups and $n_p = |Syl_p(G)|$

remarks
(1) such subgroups of order p^r are called Sylow p-subgroups of G
(2) $P \in Syl_p(G) \implies P \leq G$ and $|P| = p^r$
(3) for $P \in Syl_p(G)$, $n_p = [G : N_G(P)]$, with $n_p \mid m$ and $n_p \equiv 1 \pmod p$

theorem: suppose G is a finite group with $|G| = pq$ where p and q are distinct primes. if $p \nmid q - 1$, then G has a normal Sylow p-subgroup

corollary: suppose G is a finite group with $|G| = pq$, where p and q are distinct primes such that $p < q$ and $p \nmid q - 1$, then G is a cyclic group.

lemma
(1) there are no simple groups of order 200
(2) there are no simple groups of order 50

theorem: if G is a finite group with $|G| = pqr$ where p, q and r are distinct primes, then G is not simple