MA2202 Chapter 1

(1) Group : set, identity, inverse, associativity (If abelian, then its commutative)

(2) $\{e\}$ trivial group.

(3) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ additive., $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$, $\mathbb{Z}^\times = \{\pm 1\}$ are multiplicative

(4) Permutation Groups $\text{Perm}(\Omega \text{ (set)}) = \{\text{All bijections from } \Omega \to \Omega\}$.

(5) Symmetric Groups $S_n = \text{Perm}(\{1,2,\dots,n\})$; $|S_n| = n!$

(6) Matrix Groups : $GL_n(F) = \{A \in Mat_{n\times n}(F) \mid \det(A) \neq 0\}$.

(7) Quaternion Group: $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ $1 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $i = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$, $j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $k = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$

(8) Cyclic Decomposition of $\sigma \in S_n$ (Just know)

- 8.1 t-cycle: cycle of length t
- 8.2 Cycles disjoint $\iff$ no numbers in common and hence can commute.
- 8.3 σ^{-1} : just reverse order in cycle

(9) Dihedral groups $D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}$ (reflection; rotation)

↳ Each element can be written as $s^k r^i$, $k \in \{0,1\}$, $i \in \{0,1,\dots,n-1\}$.

↳ $r^n = s^2 = 1$, $rs = sr^{-1}$

(10) Generators and Relations
- S_n generated by all cycles in S_n.
- $(\mathbb{Z}, +)$ generated by $+1$; Q_8 generated by $\{i,j\}/\{j,k\}/\{i,k\}$.
- $\mathbb{R}$ generated by $[0,1]$; D_{2n} generated by $\{r,s\}$.

(11) Homomorphisms $\varphi: G \to H$: $\varphi(xy) = \varphi(x)\varphi(y)$; $\varphi(1_G) = 1_H$; $\varphi(x^{-1}) = [\varphi(x)]^{-1}$

(12) ψ, ϕ are hom. $\psi \circ \phi$ and $\phi \circ \psi$ are hom.

(13) Weird hom. $1 \to G$, $G \to 1$

(14) Isomorphism: Bijective Homomorphisms.

(15) $G \cong H$; G is isomorphic to H, $\cong$ is an equivalence relation.

- If ψ is isom. $\exists$ ϕ hom. such that $\psi\circ\phi = id_H$ and $\phi\circ\psi = id_G$

(16) $D_6 \cong S_3$

(17) For sets Δ and Ω, if $|\Delta| = |\Omega|$, then $S_\Delta \cong S_\Omega$

Tutorial Qns

(1) $x \in G$. If $x^2 = 1 \iff |x| = 1$ or 2.

(2) $|x| = |x^{-1}|$

(3) $|x| = |gxg^{-1}|$ $\forall$ $x, g \in G$

(4) Commuting elements: $(ab)^n = a^n b^n$.

(5) $x^2 = 1$ $\forall x \in G \Rightarrow G$ abelian

(6) $(a,b) \in A \times B$, $|(a,b)| = \text{lcm}(|a|, |b|)$

(7) $|G| < \infty$ and even order, $\exists\, x \in G$ s.t $x^2 = 1$

(8) $\sigma = (1\ 2\ 3 \cdots m)$, σ^i is m-cycle $\iff \gcd(i,m) = 1$

(9) For D_{2n}, n=even, r^k is element of order 2 which commutes all of D_{2n}. (and the only one)

(10) If $\varphi: G \to H$ isom. then $|\varphi(x)| = |x| \ \forall x \in G$.

(11) If $\varphi: G \to H$, G abelian $\iff$ H abelian.

(12) $\mathbb{R} - \{0\}$ not isom. to $\mathbb{C} - \{0\}$

(13) $\mathbb{R}$ not isom. $\mathbb{Q}$

(14) $\mathbb{Z}$ not isom. $\mathbb{Q}$

(15) D_8 not isom. Q_8.

(16) If $G = A \times B$, $H = B \times C$, $G \times C \cong A \times H$

(17) $\varphi: g \to g^{-1}$ hom. $\iff$ G is abelian $\iff \phi: g \to g^2$ too.
$G \to G$

(18) $\varphi: \mathbb{C} \to \mathbb{C}$ $(z \longmapsto z^k)$ is surjective hom.

(19) Aut(G) : All isom. of G as a set. Group under f^n composition.

(20) $q \longmapsto kq$ is an automorphism of $\mathbb{Q}$

(21) ~~Chapter 2~~

(1) Subgroup H of G, denoted $H \leq G$ s.t $x, y \in H$, $xy \in H$, $1_G \in H$ and $x^{-1} \in H$.

(2) $\tau: H \to G$: the canonical inclusion hom. $(h \longmapsto h)$

(3) Proper subgroup: $H < G \iff H \leq G$ and $H \neq G$

(4) Subgroup Criterion: $H \leq G \iff H \neq \emptyset$ and $\forall x, y \in H$, $xy^{-1} \in H$.

(5) (FINITE) Subgroup Criterion: $H \leq G \iff H \neq \emptyset$ and $\forall x, y \in H$, $xy \in H$.

(6) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ (under $+$) ; $\underset{\{\pm 1\}}{\mathbb{Z}^\times} \leq \mathbb{Q}^\times \leq \mathbb{R}^\times \leq \mathbb{C}^\times$ (under $\times$)

(7) $n\mathbb{Z} = \{a \in \mathbb{Z} \mid \exists k \in \mathbb{Z} \text{ s.t } a = nk\}$
$= \{nk \in \mathbb{Z} \mid k \in \mathbb{Z}\}. \leq \mathbb{Z}$

(8) For any $H \leq \mathbb{Z}$, $\exists n \in \mathbb{Z}_{\geq 0}$ s.t $H = n\mathbb{Z}$ (Theorem)

E.g $\varphi: S_2 \to S_3$

$S_2 \to 1 \to S_3$ $\ker(\varphi) = S_2$
$1 \gg 1 \to (1)$ $\operatorname{im}(\varphi) = 1_{S_3}$.
a

(9) Suppose $\varphi: G \to H$ is a hom. $\ker(\varphi)$ and $\operatorname{Im}(\varphi) \leq H$
$\leq G$

(10) $g \in G$, $a \in G$, gag^{-1} is <u>g-conjugate of a</u>

(11) G-conjugacy class of $a = \{\text{conjugates of } a \text{ in } G\} = \{sas^{-1} \mid s \in G\}$.

(12) $C_G(a) := \{g \in G \mid gag^{-1} = a\}$ (centraliser)

(13) $N_G(A) := \{g \in G \mid gAg^{-1} = A\}$ (normaliser)

(14) $Z(G) := \{g \in G \mid \forall a \in G \ gag^{-1} = a\}$ (center) — contains elements that commutes everyone.

(15) For $a \in G$: $C_G(a) = N_G(\{a\})$

(16) $A \subseteq G$: $C_G(A) = \bigcap_{a \in A} C_G(a)$ and $C_G(A) \subseteq N_G(A)$

(17) $Z(G) = C_G(G)$; $N_G(G) = G \Leftarrow gGg^{-1} = G$

(18) $C_G(1_G) = N_G(\{1_G\}) = G$.

(19) $G = Z(G) \iff G$ is abelian $\iff C_G(a) = G \ \forall a \in G \iff C_G(A) = N_G(A) = G \ \forall A \subseteq G$

(20) $C_G(A) \leq G$; $N_G(A) \leq G$

(21) $G = D_8$, $A = \{1, r, r^2, r^3\}$; $C_{D_8}(A) = A$; $N_{D_8}(A) = D_8$

(22) Centerless: $Z(G) = \{1_G\}$

(23) Let $x \in G$, Cyclic group $= \langle x \rangle = \{ x^n \mid n \in \mathbb{Z} \}$ (x) or $\{ nx \mid n \in \mathbb{Z} \}$ (+)

(24) If $H = \langle x \rangle$, x generates H

(25) $H = \langle x \rangle$, then $H = \langle x^{-1} \rangle$

(26) G is cyclic $\iff \exists\, g \in G$ s.t $G = \langle g \rangle$

(27) $\mathbb{Z}$ is cyclic generated by $\{\pm 1\}$

(28) $\mathbb{Z}/n\mathbb{Z}$ is cyclic generated by $\bar{a}$, but must have $\gcd(a, n) = 1$

(29) Universal Property of $\mathbb{Z}$: For any G and $x \in G$, $\exists!\ \varphi : \mathbb{Z} \to G$ s.t $\varphi(1_{\mathbb{Z}}) = x$

(30) Hom. is injective if $\ker(\varphi) = \{1\}$
surjective $\operatorname{Im}(\varphi) = H$
for $\varphi : G \to H$.

(31) Let $\varphi : \mathbb{Z} \to G$ be unique hom. such that $\varphi(1_{\mathbb{Z}}) = x$, $\operatorname{im}(\varphi) = \langle x \rangle$

(32) If $|X| < \infty$, then if $|X| = n$, $|\langle x \rangle| = n$ too.

(33) If $|X| = \infty$, then $\langle x \rangle$ is infinite cyclic

$\ker(\varphi) = \begin{cases} 0 & \text{if } |x| = \infty \\ n\mathbb{Z} & \text{if } |x| = n. \end{cases}$

(34) Any 2 infinite, cyclic groups are isomorphic. ($\mathbb{Z} \cong G$)

(35) Universal Property of $\mathbb{Z}/n\mathbb{Z}$: For any G and any $x \in G$: $\exists!\ \varphi : \mathbb{Z}/n\mathbb{Z} \to G$ where $\varphi(\bar{1}) = x$.

(36) Any 2 finite, cyclic group of the same order, are isomorphic. ($\mathbb{Z}/n\mathbb{Z} \cong G$)

(37) $H \leq \mathbb{Z}$, $\exists\, n \in \mathbb{Z}_{\neq 0}$ s.t $H = n\mathbb{Z}$, H is cyclic and $n \in \mathbb{Z}^+$ is char. as smallest elem. of $H \cap \mathbb{Z}^+$

(38) Let $\varphi : G \to H$ be hom. $\varphi^{-1}(H_0) = \{ g \in G \mid \exists\, h \in H_0 \text{ s.t } \varphi(g) = h \} \leq G$.
If $H_0 \leq H$; $G_0 \leq G$ $\varphi^{adj}(G_0) = \{ \varphi(g) \mid g \in G_0 \} \leq H$

(39) For any $a \in \mathbb{Z}_{\neq 0}$: $\pi(a\mathbb{Z}) = \langle \bar{d} \rangle = d\mathbb{Z}/n\mathbb{Z}$ where $d := \gcd(a, n)$.
If $a \mid n$, then $d = a$ and $\pi(a\mathbb{Z}) = \langle \bar{a} \rangle$.

(40) For any $H \leq \mathbb{Z}/n\mathbb{Z}$, $\exists!\, a \in \mathbb{Z}^+$ s.t $a|n$, $H = \pi(a\mathbb{Z}) = \langle \bar{a} \rangle$
H is also cyclic, $a \in \mathbb{Z}^+$ char. by smallest int s.t $\bar{a} \in H$.

(41) If G is cyclic, (1) Every subgrp is cyclic.
(2) If G is infinite, then $n \mapsto \langle x^n \rangle$ is a bijection.
(3) If G is finite, then $a \to \langle x^a \rangle$ is a bijection.

(42) $\mathbb{Z} = \langle a \rangle \iff a = \pm 1$.

(43) $\mathbb{Z}/n\mathbb{Z} = \langle \bar{a} \rangle \iff \gcd(a,n) = 1$

(44) If G is cyclic and $G = \langle x \rangle$, if $|G| = \infty$, then $G = \langle x^a \rangle \iff a = \pm 1$.
if $|G| < \infty$, then $G = \langle x^a \rangle \iff \gcd(a,n) = 1$.

(45) For any $d, n \in \mathbb{Z}_{\geq 0}$, $n\mathbb{Z} \subseteq d\mathbb{Z} \iff d|n$. in $\mathbb{Z}$.

(46) For any $a, b \in \mathbb{Z}^+$ dividing n, $\langle \bar{a} \rangle \subseteq \langle \bar{b} \rangle \iff b|a$ in $\mathbb{Z}$.

(47) Lattices:

Order 2: $\mathbb{Z}/2\mathbb{Z}$ / $2\mathbb{Z}/2\mathbb{Z}$

order 4: $\mathbb{Z}/4\mathbb{Z}$ / $2\mathbb{Z}/4\mathbb{Z}$ / $4\mathbb{Z}/4\mathbb{Z}$

or

$V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$\langle (1,0) \rangle$ $\langle (1,1) \rangle$ $\langle (0,1) \rangle$

$\langle (0,0) \rangle$

order 6:

$\mathbb{Z}/6\mathbb{Z}$

$2\mathbb{Z}/6\mathbb{Z}$ $3\mathbb{Z}/6\mathbb{Z}$

$6\mathbb{Z}/6\mathbb{Z}$

or

$S_3 \cong D_6$

$\langle (123) \rangle$ ← normal

$\langle (12) \rangle$ $\langle (13) \rangle$ $\langle (23) \rangle$

1.

Some order 8:

$D_8 = \langle r, s \rangle$

$\langle s, r^2 \rangle$ $\langle r \rangle$ $\langle rs, r^2 \rangle$

$\langle s \rangle$ $\langle r^2 s \rangle$ $\langle r^2 \rangle$ $\langle rs \rangle$ $\langle r^3 s \rangle$

1

Q_8

$\langle i \rangle$ $\langle j \rangle$ $\langle k \rangle$

$\langle -1 \rangle$

1.

Tutorial Results

(1) Torsion subgroup of $G := \{ g \in G \mid |g| < \infty \}$

(2) $H \cup K$ subgroup $\iff H \subseteq K$ OR $K \subseteq H$

(3) $H \leq \mathbb{Q}$ s.t $\frac{1}{x} \in H$ $\forall x \in H \setminus \{0\}$, then $H = 0$ or $H = \mathbb{Q}$.

(4) $C_G(Z(G)) = G$ and $N_G(Z(G)) = G$.

(5) $A, B \subseteq G$, $A \subseteq B$, then $C_G(B) \leq C_G(A)$

(6) $H \leq G$, then $H \leq N_G(H)$ and $H \leq C_G(H)$

$\Updownarrow$ H abelian.

(7) $n \geq 3$, $Z(D_{2n}) = \{1\}$ if n odd

$Z(D_{2n}) = \{1, r^k\}$ if $n = 2k$ (even)

(8) $|H| = 2$ and $H \leq G$, $N_G(H) = C_G(H)$. If $N_G(H) = G \Rightarrow H \leq Z(G)$

(9) Suppose $|X| = n$, $|\langle x \rangle| = |g\langle x \rangle g^{-1}| = n$ and $g\langle x \rangle g^{-1} = \langle x \rangle$

(10) $H \leq G \Rightarrow H = \langle H - \{1\} \rangle$

(11) $\mathbb{Q}^{\times}_{>0} = \left\langle \left\{ \frac{1}{p} \mid p \text{ is prime} \right\} \right\rangle$

(12) Finitely generated: H is finitely generated if $\exists A$ s.t $|A| < \infty$ and $H = \langle A \rangle$.

(13) Finite grp is finitely generated.

(14) $\mathbb{Z}$ is finitely generated.

(15) $\mathbb{Q}$ is not finitely generated, but every finitely generated subgroup of $\mathbb{Q}$ is cyclic.

(16) Maximal subgroup M of $G \Rightarrow M \neq G$ and only $M, G \leq G$.

(17) Divisibly: A is divisible if $\forall a \in A$ and $\forall k \in \mathbb{Z}^{\#}_{>0}$, $\exists x \in A$ s.t $x^k = a$. (x) or $kx = a$ (+)

(18) No finite abelian group is divisible, but $\mathbb{Q}$ under + is divisible.

Chapter 3

(1) Left g-coset of H: gH, right g-coset of H: Hg

(2) $G/H = \{ gH \mid \forall g \in G \}$. $G\backslash H = \{ Hg \mid \forall g \in G \}$.

(3) $\pi : G \to G/H$ is a surjective map.

(4) $g_1, g_2 \in G$, then TFAE: $g_1H = g_2H \leq G/H \Leftrightarrow g_1H \subseteq g_2H \Leftrightarrow g_1 \in g_2H \Leftrightarrow g_2^{-1}g_1 \in H$

(5) $\sim$: $g_2^{-1}g_1 \in H \Leftrightarrow g_1 \sim g_2 \Leftrightarrow \sim$ is an equivalence relation.

(6) For the H in (5): $\pi : G \to G/H$ is the quotient hom. ($g \mapsto gH$) and it is surjective.

(7) Set of left cosets of H in G partition G.

(8) Index of H in G: $[G:H] := |G/H|$ (cardinality of G/H)

(9) Lagrange's Theorem: $|G| = [G:H]|H|$

(10) If G finite ①: $\forall H \leq G$, $|H| \mid |G|$

②: $\forall x \in G$: $|\langle x \rangle| \mid |G|$

③ $x^{|G|} = 1_G$.

(11) If $G = (\mathbb{Z}/n\mathbb{Z})^{\times}$, then $|G| = \varphi(n) =$ # of positive integers $a \leq n$ s.t $\gcd(a,n) = 1$.

(12) Yields Euler's Theorem: $x^{\varphi(n)} \equiv 1 \pmod{n}$ if $\gcd(x,n) = 1$ by (10. ③) $x^{|G|} = 1_G$

(13) If $n =$ prime @ $G = (\mathbb{Z}/p\mathbb{Z})^{\times}$, then $\varphi(n) = p-1$, so $x^{p-1} = 1 \pmod{p}$

(14) $|G| < \infty$ and $|G| = p$ prime, $G \cong \mathbb{Z}/p\mathbb{Z}$ and is cyclic.

(15) $N \trianglelefteq G \iff \forall g \in G \; gNg^{-1} = N \iff N_G(N) = G \iff gNg^{-1} \subseteq N \iff gN = Ng$.

(16) If G is abelian, then $\forall H \leq G$, $H \trianglelefteq G$. (Every subgroup is normal)

(17) If $H \leq Z(G)$, then H is normal in G. Moreover, $Z(G) \trianglelefteq G$.

(18) $\langle (123) \rangle$ is the only normal subgroup of S_3

(19) $\langle r \rangle$ is normal subgroup of D_8; $\langle r^2 \rangle$ also normal, but $Z(D_8) = \langle r^2 \rangle$

(20) $AB = \{ab \in G : a \in A, b \in B\}$; $A^{-1} = \{a^{-1} G G : a \in A\}$.

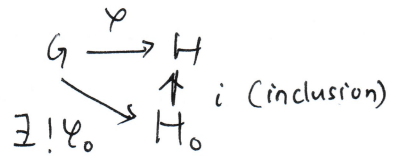
(21) $HH = H$ (obv.), $(gH)^{-1} = H^{-1}g^{-1} = Hg^{-1}$

(22) If $N \trianglelefteq G$, then $(g_1N)(g_2N) = g_1g_2N$, $(gN)^{-1} = g^{-1}N$.

(23) Quotient Group Modulo N: $N \trianglelefteq G$, G/N is quotient group.

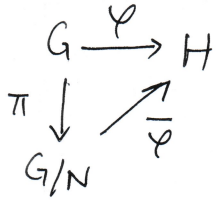
(24) If $H \trianglelefteq G$. $G/H \times G/H \to G/H \iff H \trianglelefteq G$.

(25) Universal Property of Subgroup: $\varphi : G \to H$ s.t $\text{im}(\varphi) \subseteq H_0$.
$\exists ! \, \varphi_0 : G \to H_0$ s.t $\varphi = i \circ \varphi_0$



(26) $\pi : G \to G/N$ is a surjective hom. $(g \to gN)$
$\ker(\pi) = N$

(27) Universal Property of Quotient Group:
Let $\varphi : G \to H$ s.t $N \subseteq \ker(\varphi)$
$\exists ! \, \overline{\varphi} : G/N \to H$ s.t $\varphi = \overline{\varphi} \circ \pi$



(28) First Isomorphism Theorem:

Let $\varphi : G \to H$, Decompose $\varphi = i \circ \tilde{\varphi} \circ \pi$ where $\begin{cases} \pi \text{ is quotient hom.} \\ i \text{ is inclusion hom.} \end{cases}$
and. $\tilde{\varphi} : G/\ker(\varphi) \to \text{im}(\varphi)$ is isom. induced by φ.

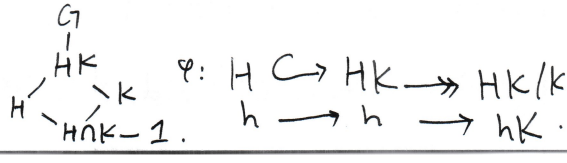
(29) For any $\varphi : G \to H$, $\ker(\varphi) \trianglelefteq G$.

(30) Conversely: any $N \trianglelefteq G$ is the kernel of some hom. $\varphi : G \to H$ for some H.

(31) $\varphi : G \to H$ hom. $|\text{im}(\varphi)| = |G : \ker(\varphi)|$
If G is finite $|\text{im}(\varphi)|$ is finite and divides $|G|$
If H is finite $|\text{im}(\varphi)|$ divides $|H|$ as well. Since $\text{im}(\varphi) \leq H$.

(32) No non-trivial hom $\varphi : G \to H$ where $\gcd(|H|, |G|) = 1$.

(33) Second Isomorphism Theorem:
Let G be group, $H \leq G$, $K \trianglelefteq G$, then $HK \leq G$, $H \subseteq HK$, $K \trianglelefteq HK$, $H \cap K \trianglelefteq H$.
and $H / H \cap K \cong HK/K$



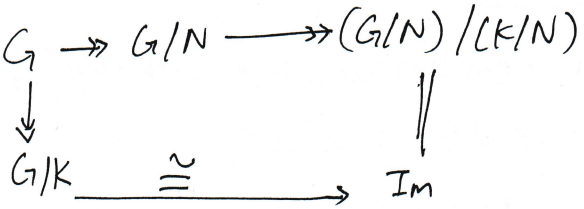
(34) **Third Isomorphism Theorem**

Let G be group, $N, K \trianglelefteq G$ and $N \subseteq K$.

① $K/N \trianglelefteq G/N$

② $G \twoheadrightarrow G/N \twoheadrightarrow (G/N)/(K/N)$

induces isom. $G/K \cong (G/N)/(G/K)$



(35) **Lattice Isomorphism Theorem**

Let $N \trianglelefteq G$ and $\pi : G \to G/N$ be a quotient hom.

$\left\{ \begin{matrix} \text{Subgroups of } G \text{ where} \\ N \trianglelefteq G \ (\text{contain } N) \end{matrix} \right\} \longrightarrow \left\{ \begin{matrix} \text{subgroups of} \\ G/N \end{matrix} \right\}$ are inclusion-preserving bijections. normality-preserving

(36) Transposition: A 2-cycle.

(37) S_n is generated by all the transpositions.

$S_n = \langle T \rangle$ where $T := \{ (i\ j) \in S_n : 1 \le i < j \le n \}$

$\Rightarrow$ Every element of S_n can be written as a product of transpositions.

(38) $(a_1\ a_2 \cdots a_m) = (a_1\ a_m)(a_1\ a_{m-1}) \cdots (a_1\ a_3)(a_1\ a_2)$

(39) S_n generated by $(1\ 2), (1\ 3), \cdots, (1\ n-1)$

(40) S_n is also generated by adjacent transpositions $(1\ 2)(2\ 3) \cdots (n-1\ n)$

(41) Tricks: $(a\ b) = (1\ b)(1\ a)(1\ b)$; $(1\ b+1) = (b\ b+1)(1\ b)(b\ b+1)$.

(42) S_n also generated by $(1\ 2)$ and $(1\ 2\ 3 \cdots n)$

(43) Reversal of σ is (a, b) with $a, b \in \{1, 2, \cdots, n\}$ s.t $a < b$ and $\sigma(a) > \sigma(b)$

(44) Sign hom. of S_n : $\epsilon : S_n \to \{\pm 1\}$. and is surjective.

$$\epsilon(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ has even reversals (transpositions)} \\ -1 & \text{if } \sigma \text{ has odd reversals (transpositions)} \end{cases}$$

(45) $\epsilon((a_1\ a_2 \cdots a_m)) = (-1)^{m-1}$ since $(a_1\ a_2 \cdots a_m)$ is m-cycle and it can be written as a product of $m-1$ transpositions. by (40)

(46) $A_n := \ker(\epsilon) \trianglelefteq S_n$, the alternating group is kernel of ϵ ; $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$

(47) A_4 has no order 6 subgroup.

(48) For any finite group G, if $H \le G$ and $[G:H] = 2$, H is normal in G.

Tutorial Questions

(1) If n is the smallest integer such that $g^n \in N$, then $|gN| = n$ in G/N.

(2) If $H, K \leq G$, $H \cap K \trianglelefteq G$

(3) $N \leq G$. $gNg^{-1} \subseteq N \iff gNg^{-1} = N$

(4) $N \leq G$ and assume $N = \langle S \rangle$, then $gSg^{-1} \subseteq N \iff gNg^{-1} = N$.

(5) Suppose $N \leq G$ and $N = \langle S \rangle$, $G = \langle T \rangle$. $N \trianglelefteq G \iff tSt^{-1} \subseteq N \ \forall t \in T$.

(6) $N \leq G$, $gN = Ng \iff g \in N_G(N)$

(7) $H \leq G$ and $N \trianglelefteq H$, then $H \leq N_G(N)$.
$N_G(N)$ is largest subgroup of G containing a normal N

(8) $G = D_{2n}$, $\langle r^k \rangle \trianglelefteq D_{2n}$ and $D_{2n}/\langle r^k \rangle \cong D_{2k}$.

(9) $G/Z(G)$ is cyclic $\Rightarrow$ G is abelian.

(10) $H, K \trianglelefteq G$ and $H \cap K = 1$, then $xy = yx \ \forall x \in H, y \in K$

(11) $N \trianglelefteq G$ and $\gcd(|N|, |G:N|) = 1$, then N is unique subgroup of order $|N|$

Chapter 4

(1) Action map G on A : $\alpha : G \times A \to A$, $(g, a) \mapsto g \cdot a$
$\updownarrow$ Bijective

(2) Action hom. $G \to S_A = \mathrm{Perm}(A)$

(3) Suppose $\alpha : G \times A \to A$, any $g \in G$, σ_g be map. $\sigma_g : A \to A$, $a \mapsto \sigma_g(a)$

(4) Suppose $\varphi : G \to S_A$, $g \cdot a = \varphi(g)(a)$, $\alpha_g : G \times A \to A$, $(g, a) \to g \cdot a = \varphi(g)(a)$
$g \in S_A$

} map and hom. inducing each other.

(5) Trivial Action : G on A

hom : $G \to S_A$, $g \mapsto id_A$

map : $G \times A \to A$, $(g, a) \mapsto a$.

(6) Tautological Action : S_A act on A.

id. action hom : $S_A \to S_A$, $g \mapsto g$

tautological action map. $S_A \times A \to A$, $(g, a) \mapsto g(a)$

(7) S_n acts tautologically on $\{1, 2, \ldots, n\}$.

(8) Group ACTING ON ITSELF by left multiplication

$\alpha : G \times G \to G$, $(g, a) \mapsto g \cdot a = ga$.

$\varphi : G \to \mathrm{Perm}(G)$, $(g)_a \mapsto (a \mapsto ga)$

$\ker(\varphi) := \{1\}$

So By 1st Isom. Theorem: $G \cong \mathrm{im}(\varphi) \leq \mathrm{Perm}(G)$

(9) Cayley's Theorem: Every group is isom. to a subgroup of some permutation grp.
If $|G| = n$, then $G \cong H \leq S_n$. (9)

(10) Group ACTING ON ITSELF by conjugation.

$\alpha: G \times G \to G$ i.e $(g, a) \to gag^{-1}$

$\varphi: G \to \mathrm{Aut}(G) \subseteq \mathrm{Perm}(G)$ since ~~gag^{-1}~~ $g \mapsto gag^{-1}$ is an isom.

$\ker(\varphi) := Z(G)$

(11) Inner automorphism of G is $\sigma \in \mathrm{Aut}(G)$ s.t $\exists\, g \in G$ s.t $\sigma = (a \mapsto gag^{-1})$

(12)
$$\begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(G) \subseteq \mathrm{Perm}(G) \\ \downarrow & & \uparrow \\ G/Z(G) & \xrightarrow{\cong} & \mathrm{Inn}(G) \end{array}$$

(13) New actions by composition
Say we have action hom. $G \to S_A$ and $\exists\ \varphi: G_0 \to G$
By composition $G_0 \to G \to \mathrm{Perm}(G) \geq \mathrm{Aut}(G)$
New action map, $G_0 \to \mathrm{Perm}(A)$

(14) Map $\mathrm{Perm}(A) \xrightarrow{\text{Yes}} \mathrm{Perm}(\mathcal{P}(A))$ is a well-defined hom.
$\sigma \mapsto \mathcal{P}(\sigma)$

(15) New Actions by Powering
~~old~~: $G \to \underbrace{\mathrm{Perm}(A)}_{\text{old}} \xrightarrow{\varphi} \underbrace{\mathrm{Perm}(P(A))}_{\text{new}}$

(16) Lemma: $A_0 \subseteq A$. $\mathrm{Perm}(A)_{A_0} = \{\sigma \in \mathrm{Perm}(A) \mid \sigma(A_0) = A_0\} \leq \mathrm{Perm}(A)$
and $\mathrm{Perm}(A)_{A_0} \to \mathrm{Perm}(A_0)$ is a well-defined hom.
$\sigma \mapsto \sigma|_{A_0}$

(17) Stable: $A_0 \subseteq A$ is stable under action of G on $A \iff \sigma_g(A_0) \subseteq A_0 \iff \sigma_g(A_0) = A_0 \iff G \to \mathrm{Perm}(A)_{A_0} \to \mathrm{Perm}(A_0)$ } $\forall g \in G$.
defines action of G on A_0 induced by action ~~of~~ on A

(18) New Actions using Maps
$G \to \mathrm{Perm}(A)$, $g \mapsto \sigma_g$
$G \to \mathrm{Perm}(B)$, $g \mapsto \tau_g$
G action on $\mathrm{Maps}(A,B)$: $\varphi: G \times \mathrm{Maps}(A,B) \to \mathrm{Maps}(A,B)$
$(g, f) \to \tau_g \circ f \circ \sigma_g^{-1}$

(19) Let $A = \{1, 2, \dots, n\}$; B be any set.
$\alpha: S_n \times B^n \to B^n$, $(\sigma, (b_1, b_2, \dots, b_n)) \mapsto (b_{\sigma^{-1}(1)}, b_{\sigma^{-1}(2)}, \dots, b_{\sigma^{-1}(n)})$
You get new actions by Permutating Components

(20) More generally $G \times B^n \to B^n$, $(g, (b_1, b_2, \dots, b_n)) \mapsto (gb_1, gb_2, \dots, gb_n)$
is called the diagonal action

(21) G-orbit of $a \in A := \{ b \in A : \exists\ g \in G \text{ s.t } g \overset{\text{act}}{\cdot} a = b \}$

$:= \{ g \cdot a \in A : g \in G \}$.

$:= G \cdot a$. "The effect of G on a"

(22) G-orbits of A form a partition of A and is an equivalence relationship.

(23) Action of G on A is transitive $\iff$ only 1 orbit $\iff G \cdot a = A$ $\exists$ ~~any~~ $a \in A$

(24) $G_a := \{ g \in G : ga = a \}$ is called the Stabiliser of a.

(25) Trivial Action of G on A.

$G \cdot a = \{a\}$; $G_a = G$

(26) Tautological action of $\text{Perm}(A)$ on A

$G \cdot a = A$ (transitive)

Stabiliser $G_a := \text{Perm}(A)_{\{a\}}$ where a is stable.

(27) Left Multiplication Action of G on itself.

$G \cdot a = G$ (transitive)

$G_a = \{1_G\}$

(28) Left Multiplication Action of G on coset space G/H

$G \cdot a = G/H$; $G_{1H} = H$; $G_{xH} = xHx^{-1}$ → why diff? $gxH = xH$ if $g \in G_{xH}$.

$\Rightarrow x^{-1}gxH = H$

$\Rightarrow x^{-1}gx \in H$

$\Rightarrow g \in xHx^{-1}$.

(29) Conjugation action of G on itself.

$G \cdot 1 = \{1_G\}$ → not transitive unless $|G| = 1$.

$G \cdot a = \{ gag^{-1} \mid \forall g \in G \} = \{ \text{conjugates of } a \}$

$G_a = \{ g \in G \mid gag^{-1} = a \} = C_G(a)$

(30) Conjugation action of G on subsets of G.

$A \subseteq G$. $G \cdot A = \{ gAg^{-1} : g \in G \}$

$G_A = \{ g \in G \mid gAg^{-1} = A \} = N_G(A)$

(31) Let G be ~~the~~ some finite group. p is the smallest prime dividing $|G|$.

$\Rightarrow$ Any subgroup of G of index p is normal. (Corollary)

Consider lect: Left Mult. action of G on G/H where $H \leq G$ s.t $[G:H] = p$.

(32) Basic Result: $G/G_a \to G \cdot a$, $gG_a \to g \cdot a$ is a well-defined bijection.

Thus Orbit Stabiliser Theorem $|G| = |G \cdot a|\,|G_a| = |\text{Stab}(a)|\,|\text{Orb}(a)|$

And $|G \cdot a| = [G : G_a]$ index.

(33) # of conjugates of S, $|G : N_G(S)|$

(34) # of conjugates of s, $|G : C_G(s)|$

(35) Orbit Decomposition: Let $a_i \in A$ be reps. of distinct G-orbits in A.

$$A = \bigsqcup_{i=1} G \cdot a_i \cong \bigsqcup_{i=1} G/G_{a_i}$$

(36) Fixed point: $a \in A$ s.t $\forall g \in G$ $g \overset{\text{action}}{\cdot} a = a$

↳ $G.a = \{a\}$; $G_a = G$

↳ Denoted as a set of fixed points as $A^G \subseteq A$.

(37) Let $a_1, a_2, \dots, a_r \in A$ be choice repr. of distinct, non-trivial orbits.

$$|A| = |A^H| + \sum_{i=1}^{r} [G : G_{a_i}]$$

(38) Another variant known as the class Eqn for conjugacy classes

$$|G| = |G^H| = \sum_{i=1}^{r} [G : G_{a_i}]$$

Since $G^H = \{ g \in G \text{ s.t } \forall g' \in G,\ g'gg'^{-1} = g \} = Z(G)$

$G_{a_i} = \{ g \in G \text{ s.t } g' a_i g'^{-1} = a_i \} = C_G(a_i)$

So $|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(a_i)]$

(39) Cauchy's Theorem: Let G be finite group. $p \mid |G|$, then $\exists x \in G$ s.t $\text{ord}(x) = p$.

(40) Sylow's Theorems

Let G be a finite group of order $p^\alpha m$, $\alpha \geq 1$, $p \nmid m$.

(1) Sylow p-groups of G exist

(1)' For $0 \leq k \leq \alpha$, $\exists$ an order p^k subgroup of G.

(2): Any 2 Sylow-p groups, P, Q are conjugate i.e $gPg^{-1} = Q$ for some $g \in G$.

(2)' $\text{Syl}_p(G)$ transitive under conjugation action of G

(3) $n_p(G) \mid |G|$ and $n_p(G) \equiv 1 \pmod p$.

(41) p-group: finite group of order p^α

(42) Sylow p-subgroup is a p-subgroup of index prime to p. i.e if $|G| = p^\alpha m$, $p \nmid m$, $P \in \text{Syl}_p(G)$ would be $|P| = p^\alpha$

(43) $n_p(G) := |\text{Syl}_p(G)|$

(44) Basic Lemma: If H is a p-group acting on finite set A, then $|A^H| \equiv |A| \pmod p$.

(45) If H is a p-subgroup of a finite group G, then $[N_G(H) : H] \equiv [G : H] \pmod p$.

(46) Lemma: $P \in \text{Syl}_p(G)$, For any p-subgroup Q of G. $Q \cap N_G(P) = Q \cap P$.

(47) A simple group is a group G with $|G| > 1$ s.t only normal subgroups are 1 and G.

(48) If $|G| =$ prime p, $G \cong \mathbb{Z}/p\mathbb{Z}$, which means abelian and simple.

(49) Conversely, if G is abelian and simple, $\exists$ p prime s.t $G \cong \mathbb{Z}/p\mathbb{Z}$.

(50) **Classification Theorem (of finite, simple groups)**

- 18 infinite families of finite simple groups
- 26 sporadic finite simple groups

] Every finite simple group $\cong$ to exactly one of the groups in list.

(51) 1 group is $\{\mathbb{Z}/p\mathbb{Z} : p \text{ prime}\}$

(52) 2nd family $\{A_n : n \geq 5\}$ non-abelian finite simple groups.

(53) **Theorem**: P is p-group of order p^α, $\alpha \geq 1$, $Z(P) \neq 1$, non-trivial center.

Pf: Use Basic Lemma: $|Z(P)| \equiv |P| \bmod p$.

$1_P \in Z(P)$, so $|Z(P)| \geq 1$ and divides p, so $\geq p > 1$ ⊗

(54) p-group of order p^α, $\alpha \geq 2$ is <u>not</u> simple.

(55) If $|G| = pq$, $p < q$, both primes, then G has a normal Sylow q-subgroup.

(56) Finite group of order pq, where p, q are primes is <u>not</u> simple

(57) More general: $|G| = p^\alpha q^\beta$, $p \neq q$ primes, $\alpha, \beta \geq 1$

If $p, p^2, \ldots, p^\alpha$ all $\not\equiv 1 \pmod q$

Then G has a normal Sylow q-subgroup, and thus G is not simple.

(58) **Classical Result**: A non-abelian simple group is of order ≥ 60.

A finite group of order 60 is either abelian simple and hence $|G| = p$ and $G \cong \mathbb{Z}/p\mathbb{Z}$ or not simple.

(59) If $|G| = pqr$, $p < q < r$ primes, then G has a normal Sylow subgroup.

(60) Cool result: If $\exists\, H \subsetneq G$ where $[G:H]! < |G|$, then G has a nontrivial normal subgroup contained in H (which is also proper)

(61) (Burnside) $|G| = p^\alpha q^\beta$, p, q prime, $\alpha, \beta \geq 1$, G is not simple.

(62) (Feit-Thompson) Finite simple group of odd order is $\cong \mathbb{Z}/p\mathbb{Z}$ with p odd prime.

(63) Conjugacy in S_n.

(63.1) cycle-type of σ is partition $n_1 \leq n_2 \leq \ldots \leq n_r$ of n s.t $\sum_{i=1}^{r} n_i = n$ where $\sigma = \pi$ disjoint cycles (pairwise) of length n_i for 1 to r.

E.g. $(1\,2)(3\,4\,5)(6\,7\,8\,9)$ has cycle type 2, 3, 4 in S_9

$(1\,3\,5\,7)(2\,4\,6\,8)$ has cycle type 1, 4, 4 in S_9

(64) Proposition Impt: For any $\sigma, \tau \in S_n$ and any $i, j \in \{1, 2, \ldots, n\}$

- $\sigma(i) = j \Rightarrow \tau\sigma\tau^{-1}$ maps $\tau(i)$ to $\tau(j)$
- Thus if i, j appears in cycle decomp. of σ, then $\tau(i), \tau(j)$ appears similarly for $\tau\sigma\tau^{-1}$
- AND $\sigma := (a_1\, a_2 \cdots a_{k_1})(b_1\, b_2, \ldots b_{k_2})$, then $\tau\sigma\tau^{-1} := (\tau(a_1)\,\tau(a_2) \ldots \tau(a_{k_1}))(\tau(b_1) \ldots \tau(b_{k_2}))$
- AND cycle type of σ and $\tau\sigma\tau^{-1}$ are the same.

(65) If $\sigma_1, \sigma_2 \in S_n$ have the same cycle type $\Leftrightarrow \sigma_1, \sigma_2$ are conjugate in S_n.

(66) map $\{$conjugacy classes of $S_n\} \longrightarrow \{$partitions of $n\}$ is a well-defined bijection.

↳ # of conjugacy classes of S_n
= # of partitions of n.

(67) Crazy Result: Let $m_1, m_2, \dots, m_s$ be distinct integers in cycle type of σ, $k_1, k_2, \dots, k_s$ be respective multiplicities, condition $\sum_{i=1}^{s} k_i m_i = n$

$$\#\text{ of conjugates of } \sigma = \frac{n!}{(k_1! m_1^{k_1})(k_2! m_2^{k_2}) \cdots (k_s! m_s^{k_s})} = \frac{n!}{\prod_{i=1}^{s} (k_i! m_i^{k_i})}$$

(68) If $\sigma \in S_n$ is m-cycle, then

$$\#\text{ of } m\text{-cycles} = \frac{n(n-1)(n-2)\cdots(n-m+1)}{m}.$$

(69) Implication of Sylow(2)

If $K \trianglelefteq G$, then if K contains a Sylow p-subgroup of G, it contains All Sylow p-subgroups of G.

If $K \trianglelefteq G$, then if K is contained in a Sylow p-subgroup of G, then it is contained in all Sylow p-subgroups of G.

(70) If G is finite simple of order 60, $A_5 \cong G$.

Tutorial Results (Discussed)

(1) If G is a transitive permutation group on A,

Block: B is a block if $B \subseteq A$ and $\forall \sigma \in G$, either $\sigma(B) = B$ or $\sigma(B) \cap B = \phi$.

(2) $\sigma_1(B), \sigma_2(B), \dots, \sigma_n(B)$ are partitions of A

(3) Transitive group is primitive if only blocks in A are 1 an itself.

(4) Transitive group is primitive iff $\forall a \in A$, subgroups are G_a and G.

(5) Group (Perm. Grp) is doubly transitive if $\forall a \in A$, G_a is transitive on $A - \{a\}$.

(6) Doubly Transitive group is primitive.

(7) If $[G:H] = n$, $\exists\ K \trianglelefteq G$ s.t $K \leq H$ and $[G:K] \leq n!$

(8) $Z(S_n) = 1$ for $n \geq 3$.

(9) G is odd order, then x, non identity $\in G$, x and x^{-1} are not conjugate in G.