Abstract Algebra: Group Theory.

Yashas.N

0 symbols or terms used

$|$ → divides i.e. $(m, n) \to gcd(m, n)$ $a|b$
implies a divides b.
$|a| \to$ order of element in the group or
$|G| \to$ order of the group.
$\forall \to$ for all.
iff → if and only if.
$H \lll G \to H$ is a subgroup of G.
Basic → in headings indicates easy to
derive properties.

1 Preliminaries

G.C.D

greatest common divisor : $(a, b) = d$ i.e. $gcd(a, b) = d$ if $d|a, d|b$ and if there exist e such that $e|a, e|d$ then $e|d$ (here $a, b, m, e \in \mathbb{Z}^+$)

L.C.M

$lcm(a, b) = c$ then $a|c, b|c$ and if there exist e such that $a|e, b|e$ then $c|e$ (here $a, b, m, e \in \mathbb{Z}^+$)

Euclidean algorithm

if $a, b \in \mathbb{Z}^+$ then

$$\begin{gathered} a = q_0 b + r_0 \\ b = q_1 r_0 + r_1 \\ r_0 = q_2 r_1 + r_2 \\ \vdots \\ r_{n-2} = q_n r_{n-1} + r_n \\ r_{n-1} = q_{n+1} r_n \end{gathered}$$

here r_n is the $gcd(a, b)$

if we reverse the Euclidean algorithm i.e. write $r_n = r_{n-2} - q_n r_{n-1}$ and use the preceding equation for r_{n-2}, r_{n-1} to write r_n in terms of r_{n-3}, r_{n-2} and repeating this process we get

$$ax + by = d = (a, b).$$

for $a, b, x, y, d \in \mathbb{Z}^+$

Euler's φ function

$\varphi(n)$ gives the number of relative primes of n i.e. there are $\varphi(n)$ numbers $< n$ such that their gcd with respect to (w.r.t) n is 1. Properties and derivation of $\varphi(n)$:

■ if p is a prime them $\varphi(p) = p - 1$.
■ $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p - 1)$.
■ if $(a, b) = 1$ then $\varphi(ab) = \varphi(a)\varphi(b)$.

from preceding points we have for $n = p_1^{s_1} p_2^{s_2} .. p_k^{s_k}$ (p_i prime and $s_i \in \mathbb{N}$)

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{s_1} p_2^{s_2} .. p_k^{s_k}), \\ &= \varphi(p_1^{s_1})\varphi(p_2^{s_2}) .. \varphi(p_k^{s_k}), \\ &= p_1^{s_1-1}(p_1 - 1)p_2^{s_2-1}(p_2 - 1) \\ &\quad .. p_k^{s_k-1}(p_k - 1). \end{aligned}$$

2 Groups

2.1 Definitions

Binary operation

function $\star : G \times G \to G$ (for any set G) is a Binary operation.

Group

$(G, \star)$: a set G with an binary operation $\star$ on it is a group if :

■ $\star$ is associative.

■ Inverse : for every $a \in G$ $\exists a^{-1} \in G$ such that $a^{-1} \star a = a \star a^{-1} = e$.

a Group is abelian or commutative if $\star$ is commutative. instead of writing $\star$ it is omitted i.e. we write ab instead of $a \star b$

Order of an element : for $a \in G$ $|a| = n$ is the smallest +ve integer such that $a^n = e$.

(here $a^n = \overbrace{a \star a \star a .. \star a}^{n \text{ times}}$)

Subgroup

a subset S of a group G is a subgroup if S is group under same binary operation as G this is denoted by $S \lll G$.

Maximal subgroup

a proper subgroup $M \lll G$ is maximal in G iff $M \lll H \lll G \implies H = G$ i.e. no other proper subgroup of G contains M.

2.2 Basic Properties of Groups

a^{-1} is unique for every a, $(a^{-1})^{-1} = a$.
$(ab)^{-1} = b^{-1}a^{-1}$.
$ay = b, xa = b$ has a unique solution for every $a, b \in G$ i.e right cancellation and left cancellation laws holds in a group.

for $a, b \in \mathbb{N}$:
$x^a x^b = x^{a+b}$, $(x^a)^b = x^{ab}$, $(x^a)^{-1} = x^{-a}$.

if $|x| = n$, $n = st$ then $|x^s| = t$

Cyclic subgroup

$\langle x \rangle = \{x^n | n \in \mathbb{Z}^+\}$ forms as subgroup

if A, B are groups the $A \times B = \{(a, b) | a \in A, b \in B\}$ with component wise group operations forms a group with $|(a, b)| = \mathrm{lcm}(|a|, |b|)$

H is a subgroup of G ($H \lll G$) then :

■ H is closed under group operations and inverses

■ $ab^{-1} \in H \forall a, b \in H$

Torsion subgroup

if G is an abelian group then $\{g \in G : |g| < \infty\}$ is a subgroup of G (if G is an non-abelian infinite group this may not hold)

if $H, K \lll G$ then :

■ $H \cap K \lll G$.

■ $H \cup K \lll G$ iff $H \subseteq K$ or $K \subseteq H$.

3 Homomorphism and Isomorphisms

Homomorphism

a map $\phi : G \to H$ for groups $(G, \star), (H, \diamond)$ is a homomorphism if
$\phi(a \star b) = \phi(a) \diamond \phi(b)$ $\forall a, b \in G$

Isomorphisms

a map between two groups ϕ is isomorphism if it is homomorphism and bijective (one-one and onto).

3.1 Basic Properties of group related to homo and isomorphisms

if $\phi : G \to H$ is homomorphism then

■ $\phi(x^n) = \phi(x)^n$ $\forall x \in G, \forall n \in \mathbb{Z}$

■ kernel(ϕ) $= ker(\phi)$
$= \{x | \phi(x) = e_H$(identity of H)$\}$ is subgroup of G

■ image under ϕ i.e. $\phi(G)$ is a subgroup of H

■ ϕ is injective iff $ker(\phi) = \{e_G\}$

if $\phi : G \to H$ is isomorphism then
■ $|G| = |H|$
■ G is abelian iff H is abelian
■ $|x| = |\phi(x)|\ \forall x \in G$

The map $\psi : g \to g^{-1}$ in G is homomorphism (isomorphism to be specific) iff G is abelian. (use $\psi((ab)^{-1}) = ab,\ \psi(b^{-1}a^{-1}) = ba$)

The map $\psi : g \to g^2$ in G is homomorphism iff G is abelian.

if A is abelian then the map $\psi : a \to a^k$ is a homomorphism.

4 Automorphism $\mathrm{Aut}(\ )$

$\mathrm{Aut}(G)$ is the set of all isomorphism of a group G onto itself.
$\mathrm{Aut}(G)$ forms a group under function composition.

if there exists an Automorphism ϕ of G such that $\sigma(g) = g \iff g = 1$ (i.e. no fixed points) and $\sigma^2 = I$ (Identity) then G is abelian.

if A, B are groups then $A \times B \cong B \times A$ (isomorphic) (use isomorphic map $\phi : A \times B \to B \times A$ by $(a, b) \to (b, a)$).

5 Group Actions*

Importance is given to group actions as a set 'acting' on another set is the major recurring theme not only in Group Theory but whole of Mathematics, also plays a major role in proofs as it gives lot of information about structures of 'objects' in Mathematics.

A Group Action on of a Group G a set A is a map from $G \times A \to A$ ($g.a$ for $g \in G, a \in A$) satisfying the following properties $\forall a \in A, g_1, g_2 \in G$
■ $g_1.(g_2.a) = (g_1 g_2).a$ (here $g_1 g_2$ is the group G operation on its members g_1, g_2
■ $1.a = a$ (1 is identity in G)
Note : if g is fixed then we see that $g.a$ for varying $a \in A$ acts as a map $\sigma_g : A \to A$ and from that fact that $g \in G$ (group) we have $g^{-1} \in G$ and $(g^{-1}g).a = (gg^{-1}).a = 1.a = a$ thus this map has a left and right inverse so σ_g is bijection map in A

Immediate consequence of the preceding point is that group action of G on A is nothing but a set of permutations (elements of S_A symmetric group in A) $\sigma_g : A \to A$ given by $\sigma_g(a) = g.a$

from preceding point and group actions obey a kind of group properties (G) we get :

the map $g \to \sigma_g \in S_A$ is a
Homomorphism
i.e. Group actions can be summarized as a homomorphism $\phi : G \to S_A$.

Faithful

a group action is faithful if distinct elements in G produce distinct permutations of A i.e. the homomorphic map ϕ of the group action is injective.

Kernel of action

kernel of a group action is the set $\{g \in G | g.a = a\, \forall a \in A\}$.

a Group action is faithful iff its kernel = 1.

Stabiliser

for $a \in A$ Stabiliser of a (for group action G on A) is set $G_a = \{g \in G | g.a = a\}$
■ Kernel of the group action is contained in every Stabiliser.

■ Define a relation $\sim$ on set $\mathbf{A}$ with group action $\mathbf{G}$ on $\mathbf{A}$ as :
■ $\mathbf{a} \sim \mathbf{b}$ iff $\mathbf{a} = \mathbf{g.b}$ for $\mathbf{g} \in \mathbf{G}$
■ then $\sim$ is equivalence relation

Orbit

orbit of $\mathbf{x} \in \mathbf{A}$ under action of $\mathbf{G}$ is the equivalence class of $\mathbf{x}$ under the preceding relation $\sim$ i.e $\mathcal{O}_{\mathbf{x}} = \{\mathbf{y} \in \mathbf{A} | \mathbf{x} = \mathbf{gy} \text{ for } \mathbf{y} \in \mathbf{A}, \mathbf{g} \in \mathbf{G}\}$

Clearly Kernel of an group action (of $\mathbf{G}$) and Stabiliser of an element are subgroups of $\mathbf{G}$.

Number of elements in the orbit or equivalence class of $\mathbf{a}$:

$$|\mathcal{O}_{\mathbf{a}}| = |\mathbf{G} : \mathbf{G}_{\mathbf{a}}|.$$

(use bijective map from $\mathbf{C}_{\mathbf{a}} = \{\mathbf{g.a} | \mathbf{g} \in \mathbf{G}\} \to \{\mathbf{g}\mathbf{G}_{\mathbf{a}}\}$ by $\mathbf{b} = \mathbf{g.a} \to \mathbf{g}\mathbf{G}_{\mathbf{a}}$.)

Transitive

A group action of $\mathbf{G}$ on $\mathbf{A}$ is transitive if there exist only one orbit for the action i.e. $\mathcal{O}_{\mathbf{a}} = \mathbf{A} \forall \mathbf{a} \in \mathbf{G}$.

5.1 Major Group Actions

5.1.1 Conjugation

define a group action (conjugation) : of $\mathbf{G}$ to its power set $\mathbf{P}(\mathbf{G})$ by

$$\mathbf{g} : \mathbf{B} \to \mathbf{g}\mathbf{B}\mathbf{g}^{-1} = \{\mathbf{g}\mathbf{b}\mathbf{g}^{-1} | \mathbf{b} \in \mathbf{B}\}.$$

for $\mathbf{B} \subseteq \mathbf{G}, \mathbf{g} \in \mathbf{G}$

Centralizer

■ centralizer of an element $\mathbf{a} \in \mathbf{G}$ in $\mathbf{G}$ $\mathbf{C}_{\mathbf{G}}(\mathbf{a})$ is the Stabiliser of $\mathbf{a}$ under conjugation i.e. $\mathbf{C}_{\mathbf{G}}(\mathbf{a}) = \mathcal{O}_{\{\mathbf{a}\}} = \{\mathbf{g} \in \mathbf{G} | \mathbf{g}\mathbf{a}\mathbf{g}^{-1} = \mathbf{a}\}$ i.e. all the elements that commute with $\mathbf{a}$.
■ centralizer of a $\mathbf{A} \subset \mathbf{G}$ in $\mathbf{G}$ $\mathbf{C}_{\mathbf{G}}(\mathbf{A})$ is the intersection of all the centralizer of elements of $\mathbf{A}$ in $\mathbf{G}$ i.e. $\mathbf{C}_{\mathbf{G}}(\mathbf{A}) = \bigcap_{\mathbf{a} \in \mathbf{A}} \mathcal{O}_{\{\mathbf{a}\}}$ $= \{\mathbf{g} \in \mathbf{G} | \mathbf{g}\mathbf{a}\mathbf{g}^{-1} = \mathbf{a} \forall \mathbf{a} \in \mathbf{A}\}$ i.e. all the elements of $\mathbf{G}$ that commute with every element of $\mathbf{A}$.

Normalizer

Normalizer of $\mathbf{A} \subset \mathbf{G}$ in $\mathbf{G}$ $\mathbf{N}_{\mathbf{G}}(\mathbf{A})$ is the Stabiliser of $\mathbf{A}$ under conjugation i.e. $\mathbf{N}_{\mathbf{G}}(\mathbf{A}) = \mathbf{G}_{\mathbf{a}} = \{\mathbf{g} \in \mathbf{G} | \mathbf{g}\mathbf{A}\mathbf{g}^{-1} = \mathbf{A}\}$

Center

center of $\mathbf{G}$ denoted by $\mathbf{Z}(\mathbf{G})$ is the kernel of conjugation i.e. elements of $\mathbf{G}$ that commute with every element of $\mathbf{G}$.

Basic properties induced by conjugation :
■ $\mathbf{C}_{\mathbf{G}}(\mathbf{Z}(\mathbf{G})) = \mathbf{N}_{\mathbf{G}}(\mathbf{Z}(\mathbf{G})) = \mathbf{G}$.
■ $\mathbf{Z}(\mathbf{G}) \ll \mathbf{C}_{\mathbf{G}}(\mathbf{A}) \ll \mathbf{N}_{\mathbf{G}}(\mathbf{A}) \ll \mathbf{G}$. for any $\mathbf{A} \subset \mathbf{G}$
■ if $\mathbf{A} \subset \mathbf{B}$ then $\mathbf{C}_{\mathbf{G}}(\mathbf{B}) \ll \mathbf{C}_{\mathbf{G}}(\mathbf{A})$.

Normal

$\mathbf{N} \ll \mathbf{G}$ is said to be normal in $\mathbf{G}$ ($\mathbf{N} \trianglelefteq \mathbf{G}$) if $\mathbf{N}_{\mathbf{G}}(\mathbf{N}) = \mathbf{G}$ i.e. $\mathbf{g}\mathbf{N}\mathbf{g}^{-1} = \mathbf{N} \; \forall \mathbf{g} \in \mathbf{G}$

if $\mathbf{H} \trianglelefteq \mathbf{G}, \mathbf{K} \trianglelefteq \mathbf{G}$ then $\mathbf{H} \cap \mathbf{K} \trianglelefteq \mathbf{G}$

now as $|\mathcal{O}_{\mathbf{a}}| = |\mathbf{G} : \mathbf{G}_{\mathbf{a}}|$ we get :

number of conjugates of a subset $\mathbf{S}$ of $\mathbf{G}$ is
$|\{\mathbf{g}\mathbf{S}\mathbf{g}^{-1}\}| = |\mathbf{G} : \mathbf{N}_{\mathbf{G}}(\mathbf{S})|$.
in particular the number of conjugates of
$\mathbf{a} \in \mathbf{G}$
$|\{\mathbf{g}\mathbf{a}\mathbf{g}^{-1}\}| = |\mathbf{G} : \mathbf{C}_{\mathbf{G}}(\mathbf{a})|$.

two elements $\mathbf{a}, \mathbf{b} \in \mathbf{G}$ are conjugates in $\mathbf{G}$ if $\mathbf{a} = \mathbf{g}\mathbf{b}\mathbf{g}^{-1}$ for some $\mathbf{g} \in \mathbf{G}$.

we can form a group action of $\mathbf{G}$ acting on itself by conjugation i.e. $\mathbf{g} : \mathbf{a} = \mathbf{g}\mathbf{a}\mathbf{g}^{-1}$ for $\mathbf{a}, \mathbf{g} \in \mathbf{G}$ then this forms an equivalence relation defined by preceding point in $\mathbf{G}$ the equivalence classes of this relation is called **conjugacy classes** of $\mathbf{G}$.

■ if a and b belong to same conjugacy class i.e. $a = gbg^{-1}$ then $|a| = |b|$
■ if $2||G|$ and $a \in G$ then $a^2 \notin$ conjugacy class of a
■ if G is of odd order then for non identity element $x \in G$ is not a conjugate of x^{-1} (use : $x \sim x^{-1}$ then as $2 \not|\, |G|$ we have $x \not= x^{-1}$ so similarly we have $x \sim y \implies y \sim y^{-1}$ so conjugacy class of x has an even order.)

if $H \trianglelefteq G$ and H is non trivial (i.e. $H \not= \{1\}, H \not= G$) then for a conjugacy class $\mathfrak{C}$ of $G : \mathfrak{C} \subset H$ or $\mathfrak{C} \cap H = \emptyset$.

5.1.2 Left (right) multiplication

Cosets

a Group can act on its subgroup by left multiplication to produce sets called cosets i.e. for $H \ll G$ define $g.H = gH = \{gh | h \in H\}$ in fact group action can only be produced (well defined) if G acts on the set of cosets (left) of $H \ll G$

Properties of Left Multiplication : if G acts on cosets of $H \ll G$ in G by left multiplication then
■ Left Multiplication is Transitive
■ Stabiliser of $1H = G_H = H$
■ Kernel of this action is $\{g | g.xH = xH \forall x \in G\} = \bigcap_{x \in G} xHx^{-1}$ which is the largest normal subgroup of G contained in H.

now if we take $H = 1 \ll G$ then we get Cayley's Theorem (as one can intrepret this group actions as homomorphism from $G \to S_G$)

number of left cosets of $A \ll G$ is called **index** of A in G and is denoted by $|G : A|$

if G is finite group then for $H \ll G$
$|G : H| = \frac{|G|}{|H|}$ (by Lagrange's Theorem).

if $H, K \ll G$ of finite index in G (possibly an infinite group) i.e. $|G : H| = m,\ |G : K| = n$ then

$$\operatorname{lcm}(m, n) \leq |G : H \cap K| \leq mn.$$

(in particular if $(mn) = 1$ then $|G : H \cap K| = mn$.)

if $H \ll K \ll G$ then

$$|G : H| = |G : K|\,|K : H|.$$

6 Quotient Groups

Fiber : another word for preimage. It can be imagined as a comparison of a cloth to a function and the therads or fibers weaive to make up the cloth i.e. the preimages make up the functions at particular value.

for any $N \ll G$ (group) and $g \in G$ we have $gN = \{gn | n \in N\}$ is called a left coset of N in G and $Ng = \{ng | n \in N\}$ the right coset.

for any homomorphisms $\phi : G \to H$ between two groups with Kernel K then

Quotient Group

let G/K be the set containing the fibers preceding $a \in H$ i.e. $G/K = \{X \subset G | \phi^{-1}(a) = X\}$.

■ left cosets of K in G are equal to right cosets of K in G i.e. $gK = Kg\, \forall g \in G$ i.e. K is normal in G
■ Members of G/K are only the left cosets (or right cosets) of K in G
i.e. if $X \in G/K$ then $X = \phi^{-1}(a) = uK$ for some $u \in G$ i.e. if $u \in X$ then $X = \{uk | k \in K\}$ only.

Now for any $N \ll G$:
■ The set of left cosets (right) of N in G partition G and $uN = nN$ iff $v^{-1}u \in N$.
■ The operations $uN.vN = (uv)N$ is well

defined iff $gng^{-1} \in N \forall g \in G, n \in N$ i.e. iff N is normal in G. By this opeartions (if well defined) the cosets of N in G : $\{gN\}$ forms a group.

Now if $N \trianglelefteq G$ (N normal in G) iff :
■ $gN = Ng \; \forall g \in G$
■ N is a kernel of some homomorphism from G, namely the natural projection homomorphism G onto G/N i.e. $\pi : G \to G/N$ given by $\pi(g) \to gN$ has the kernel N.

Quotient group of Cyclic groups are cyclic.

if $B \lll A$ an abelian group then A/B is abelian.

if $G/Z(G)$ is cyclic then G is abelian

for $N \trianglelefteq G$ xN, yN commute iff $x^{-1}y^{-1}xy \in N$

Commutator subgroup of G : $N = \langle x^{-1}y^{-1}xy | x, y \in G \rangle$ (set generated by these elements) then N is normal in G and G/N is abelian.

if we define $HK = \{hk | h \in H, k \in K\}$ for some $H, K \lll G$ then
■ $HK \lll G$ iff $HK = KH$.
in particular if $H \lll N_G(K)$ then HK is a subgroup.
■ $|HK| = \frac{|H||K|}{|H \cap K|}$.

if $H \trianglelefteq G$ and is of prime index i.e. $|G : H| = p$ then for any $K \lll G$ either
■ $K \lll H$ or
■ $G = HK$ and $|K : H \cap K| = p$
(use $G/H \cong Z_p$ so if $g \in K$ and $g \notin H$ then gH generates G/H so every element of G is of form $g^i h_i$ for some $h_i \in H$ and for index use 2^{nd} isomorphism theorem)

if $A \trianglelefteq G$ and $B \trianglelefteq H$ then $A \times B \trianglelefteq G \times H$ and $(G \times H)/(A \times B) \cong (G/A) \times (H/B)$

if $M, N \trianglelefteq G$ are such that $G = MN$ then $G/(M \cap N) \cong (G/M) \times (G/N)$

7 Cyclic Groups and order

a Group is cyclic if it is generated by a single element i.e. $G = \{x^n | n \in \mathbb{Z}\} = \langle x \rangle$

if $H = \langle x \rangle$ then
■ $|H| = |x|$
■ if $|x| = n < \infty$ then $H = \{1, x, x^2, .., x^{n-1}\}$.
■ if $|x| = \infty$ and if $a, b \in \mathbb{Z}$ are such that $a \neq b$ then $x^a \neq x^b$.
■ if $|x| = \infty$ then for $a, b \in Z$ $\langle x^a \rangle = \langle x^b \rangle$ iff $a = \pm b$.

if for $m, n \in \mathbb{Z}$, $x \in G$ (group) such that $x^n = 1$, $x^m = 1$ then for $d = (m, n)$ we have $x^d = 1$. and in particular $x^m = 1 \implies m||x|$.

Any two cyclic groups of same finite order are isomorphic and a cyclic group of infinite order is isomorphic to $\mathbb{Z}$. So cyclic group of order n an be concidered as $Z_n = \mathbb{Z}/n\mathbb{Z}$.

for $x \in G$ (group) we have
■ if $|x| = \infty$ then $|x^a| = \infty$ for every $a \in \mathbb{Z} - \{0\}$
■ if $|x| = n < \infty$ then

$$|x^a| = \frac{n}{(n,a)}.$$

for $H = \langle x \rangle$:
■ if $|x| = \infty$ then $H = \langle x^a \rangle$ iff $a = \pm 1$
■ if $|x| = n < \infty$ the $H = \langle x^a \rangle$ iff $(n, a) = 1$
so the number of generators of H is $\varphi(n)$.
■ Every subgroup of H is cyclic i.e. if $K \lll H$ then $K = \langle x^k \rangle$
where k is the smallest +ve integer such that $x^k \in K$

■ Clearly every subgroup of finite cyclic group is unique of the given order i.e. for a group G if there exist more than one subgroup for a given order then G is not cyclic
■ if $|H| = n < \infty$ the for each +ve integer a dividing n there exists a unique subgroup of H of order a i.e. $\langle x^d \rangle$ for $d = n/a$ is a unique subgroup of order a in H.
■ from preceding point and as $\langle x^m \rangle = \langle x^{(m,n)} \rangle$ we get the subgroups of H corresponds bijectively to divisor of n where $|H| = n < \infty$.

if $|x| = n, |y| = m$ for $x, y \in G$ and if x, y commute then $|xy| = lcm(n, m)$.

every Automorphism σ_a of $H = \langle x \rangle$ can be characterised by $\sigma_a(x) = x^a$ for some $(n, a) = 1$ from this we get

$$Aut(Z/nZ) \cong (Z/nZ)^*.$$

■ Every Group is union of its cyclic groups (as $a \in G \implies \langle a \rangle \ll G$ so $G = \bigcup_{a \in G} \langle a \rangle$.)
■ So if $|G|$ is infinite then it at-least has infinite subgroups.

8 Direct product

if $G_1, G_2, .., G_n$ are groups with operations $\star_1, \star_2, .., \star_n$ respectively then direct product $G = G_1 \times G_2 \times .. \times G_n = \{(g_1, g_2, .., g_n) | g_i \in G_i\}$ with operation $\star$ such that $(g_1, g_2, .., g_n) \star (h_1, h_2, .., h_n) = (g_1 \star_1 h_2, g_2 \star_2 h_2, .., g_n \star_n h_n)$

let G be a direct product as in preceding point then for $(G, \star)$:
■ G is group of order $|G_1||G_2|..|G_n|$ (if any G_i is infinite the so is G)
■ $G_i \cong \{(1, .., g_i, .., 1) | g_i \in G_i\}$ this subset is a subgroup of G (note g_i is in ith position and 1 in other positions are identities of respective groups)
■ for fixed i $\pi_i : G \to G_i$ by $\pi_i((g_1, .., g_i .., g_n)) = g_i$ is a surjective homomorphism such that $Ker\,\pi = \{(g_1, .., g_{i-1}, 1, g_{i+1} .., g_n)\} \cong G_1 \times .. \times G_{i-1} \times G_{i+1} \times .. \times G_n$ (here 1 is in the ith position.)
■ if $x \in G_i, y \in G_j, i \neq j$ if $\dot{x} = (1, .., x .., 1)$ (for x in ith position) and $\dot{y} = (1, .., y .., 1)$ (for y in jth position) then $\dot{x}\dot{y} = \dot{y}\dot{x}$ i.e. they commute.
■ $Z(G_1 \times G_2 \times .. \times G_n) = Z(G_1) \times Z(G_2) \times .. \times Z(G_n)$ i.e. center of G is the direct product of centers of its products.
■ if $\pi \in S_n$ then:
$G_1 \times G_2 \times .. \times G_n \cong G_{\pi(1)} \times G_{\pi(2)} \times .. \times G_{\pi(n)}$ i.e the order in the products of direct product doesn't make any difference
■ if $I \subset \{1, 2, .., n\}, J = \{1, 2, .., n\} - I$,
$G_I \ll G$ is isomorphic to direct product of G_i for $i \in I$ and
$G_J \ll G$ is isomorphic to direct product of G_j for $j \in J$ then
G_I is normal in G.
$G/G_I \cong G_J$.
$G \cong G_I \times G_J$.

Recognition Theorem of Direct product

If $H, K \trianglelefteq G$ are such that $H \cap K = \emptyset$ then

$$HK \cong H \times K.$$

(use fact that there $|H \cap K|$number of ways of writing elements each element of HK.)

9 Generated subgroups and groups

■ for any subset $A \subseteq G$ define subgroup generated by $A = \langle A \rangle = \bigcap_{\substack{A \subset H \\ H \ll G}} H$
■ if $A = \{a_1, a_2, .. a_n\}$ then
$\langle A \rangle = \{a_1^{i_1} a_2^{i_2} .. a_k^{i_n} | a_j \in A, i_l = \pm 1, k \in \mathbb{Z}^+\}$ (note: a_i can be equal to a_{i+1} and so on to give more powers of an element.)
■ if G is abelian and $A = \{a_1, a_2, .. a_n\}$ then

$\langle A\rangle = \{a_1^{i_1}a_2^{i_2}..a_k^{i_n} | i_j \in Z\}$

Finitely Generated Groups

- A group G is finitely generated if there exist a finite subset of A of G such that $G = \langle A\rangle$
- every finite subgroup of finitely generated group is finitely generate.

10 Simple and solvable Groups

Simple Group

group G is simple iff the only normal subgroups of G are trivial subgroups (i.e. $\{1\}, G$)

Composition series

Composition series of a group for a group G is the set inclusion or a Chain (w.r.t ordering of subgroups) given by

$$\{1\} \trianglelefteq N_0 \trianglelefteq N_1 \trianglelefteq .. \trianglelefteq N_{k-1} \trianglelefteq N_k = G.$$

where N_{i+1}/N_i is a simple group and N_i are called composition factors. (note this doesn't mean all $N_i \trianglelefteq G$ as $H \trianglelefteq K \trianglelefteq G$ doesn't imply $H \trianglelefteq G$.)

every Group has a composition series and if for same group G

$$\{1\} \trianglelefteq N_0 \trianglelefteq N_1 \trianglelefteq .. \trianglelefteq N_{k-1} \trianglelefteq N_k = G.$$
$$\{1\} \trianglelefteq M_0 \trianglelefteq M_1 \trianglelefteq .. \trianglelefteq M_{s-1} \trianglelefteq M_s = G.$$

then $k = s$ and $M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1}$ for some permutation $\pi \in S_k$.

if G is an abelian simple group then $G \cong Z_p$ for some p prime (true even if G is infinite.)
(use the fact that every subgroup of abelian group is normal and cauchys theorem.)

Holders Program

- Classify all finite simple groups
- Find all ways of combining simple groups to form other groups
- Classifying all finite simple groups has been completes in 1970 took more than 5000 Journal pages and a 100 years. Which says that :

There is a list of 18 infinite families of simple groups and 26 simple groups not belonging here (sporadic groups) such that every finite simple group is isomorphic to one of these groups. (for eg $\{Z_p | p$ is a prime$\}$ is one of the infinite families.)

Solvable Groups

a group G is solvable if there is chain of subgroups
$\{1\} \trianglelefteq G_0 \trianglelefteq G_1 \trianglelefteq .. \trianglelefteq G_{s-1} \trianglelefteq G_s = G.$
such that G_{i+1}/G_i is abelian.

if $N(\trianglelefteq G)$ and G/N are solvable then G is solvable

G is finite solvable group with solvable chain $\{1\} \trianglelefteq H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq .. \trianglelefteq H_s = H.$ iff :

- H_{i+1}/H_i **is cyclic**
(use argument that H_{i+1}/H_i is simple abelian group as H_i is maximal normal subgroup of H_{i+1}.)
- all composition factors of G are of prime order.

if G is a finite group in which every proper subgroup is abelian then G is solvable.

11 Major Theorems and properties

Lagrange's Theorem

if G is a finite group and H is a subgroup of G then :

- order of H divides order of G
- and the number of left cosets (right) of H in G i.e index of H in G

$$= |G : H| = \frac{|G|}{|H|}.$$

(can be easily derived by coset theory or respective group action theory)

Consequences of Lagrange's Theorem :

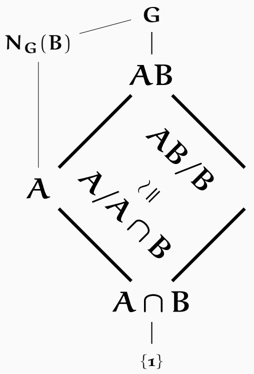
■ if $H, K \ll G$ finite group such that $|H| = n, |K| = m$, and $(m, n) = 1$ then $H \cap K = \{1\}$.
■ if order of group G is a prime (p) then G is cyclic ($G \cong \mathbb{Z}/p\mathbb{Z}$)
■ Fermats little theorem : if p is a prime then $a^p \equiv a \pmod{p}\ \forall a \in \mathbb{Z}$.
(apply Lagrange's theorem on $(\mathbb{Z}/p\mathbb{Z})^*$
■ Euler Theorem (generalized Fermats little theorem) : $a^{\varphi(n)} \equiv 1 \pmod{n}$ for every $(a, n) = 1$. (apply Lagrange's theorem on $(\mathbb{Z}/n\mathbb{Z})^*$

First Isomorphism Theorem (**fundamental**)

if $\phi : G \to H$ is homomorphism of groups then $G/ker\phi \cong \phi(G)$ (easy direct proof)

Second Isomorphism Theorem (**diamond**)

for a group G with subgroups A, B such that $A \ll N_G(B)$ then $AB \ll G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and $AB/B \cong A/A \cap B$.(use homomorphism $\phi : A \to AB/B$ by $\phi(a) = aB$) lattice diagram :



Third Isomorphism Theorem (**quotient of quotient**)

if $H \trianglelefteq G$, $K \trianglelefteq G$ and $H \ll K$ then $K/H \trianglelefteq G/H$ and $(G/H)/(K/H) \cong G/K$.

Fourth Isomorphism Theorem (**lattice**)

let $N \trianglelefteq G$ (group) then there is a bijection from set of subgroups $A \ll G$ containing N to subgroups $\overline{A} = A/N \ll G/N$ i.e. every subgroup of G/N is of from $\overline{A} = A/N$ for some $A \ll G$ containing N and this bijection has the following properties : $\forall A, B \ll G$ with $N \ll A, B$ we have
■ if $A \ll B$ iff $\overline{A} \ll \overline{B}$.
■ if $A \ll B$ then $|B : A| = |\overline{B} : \overline{A}|$.
■ $\overline{A \cap B} = \overline{A} \cap \overline{B}$.
■ $A \trianglelefteq G$ iff $\overline{A} \trianglelefteq \overline{G}$.

Cayley's Theorem

every group is isomorphic to a group of permutations (a subgroup of a symmetric group) in particular if $|G| = n < \infty$ then $G \cong$ a subgroup of S_n (can be derived by left multiplication action of G on its subgroup $\{1\}$).

Consequences of Cayley's theorem

■ if G is a finite group of order n, p is the smallest prime dividing n and if any subgroup is of index p (if exists) in G i.e. $|G : H| = p$ then H is normal.
(use left multiplication action of G on $\{gH\}$ i.e. $\pi_H : G \to S_p$ (permutation representation of the action) whose kernel $K \ll H$ is such that G/K isomorphic to a subgroup of S_p and $|G : K| = |G : H||H : K|$ so $|G : K| = pk$ and $pk|p! \implies k|(p-1)!$ thus $k = 1$ by minimality of $p||G|$ so $K = H$.)
■ Immidieately from preceding point we get **any subgroup of index 2 is necessarily a normal subgroup**.
■ using similar argument as preceding points we get : if H has finite index in G i.e. $|G : H| = n < \infty$ then There exists $K \ll H$ normal in G such that $|G : K| \leq n!$.
■ now if we follow Group action (left multiplication) to find the elements of subgroup of symmetric group that G is isomorphic to then these elements are called **left regular representations** of G.
■ if G is a finite group then for left regular

representation of $\mathbf{G}$ of an element $x \in \mathbf{G}$ of order n in $\mathbf{G}$ is product of m n—cycles only, where $|\mathbf{G}| = nm.$

■ so for $\pi : \mathbf{G} \to S_{\mathbf{G}}$ represents the isomorphism stated in Caleys's theorem (by left regular representation) and $x \in \mathbf{G}$ $\phi(x)$ is an odd permutation iff $|x|$ is even and $\frac{|\mathbf{G}|}{|\langle x \rangle|}$ is odd.(refer symmetric groups)

■ Immediately from preceding point we get in representation of $\mathbf{G}$ if there exists an odd permutation then $\mathbf{G}$ has a subgroup of index $\mathbf{2}.$

■ if $|\mathbf{G}| = 2k$ for k odd then $\mathbf{G}$ has a subgroup of index 2 i.e. $\exists \mathbf{H} \ll \mathbf{G}$ more precisely $\mathbf{H} \trianglelefteq \mathbf{G}$ such that $|\mathbf{G} : \mathbf{H}| = 2$ (use preceding 4 points)

The Class Equation

for $\mathbf{G}$ a finite group if $g_1, g_2, .., g_r$ are representatives of distinct conjugacy classes (equivalence class of $\mathbf{G}$ acting on itself by conjugation) of $\mathbf{G}$ not contained in $\mathbf{Z}(\mathbf{G})$ then

$$|\mathbf{G}| = |\mathbf{Z}(\mathbf{G})| + \sum_{i=1}^{r} |\mathbf{G} : \mathbf{C}_{\mathbf{G}}(g_i)|.$$

(an immediate consequence of conjugacy relation).

Consequences of Class equations :

■ if $\mathbf{P}$ is a group such that $|\mathbf{P}| = p^{\alpha}$ for p prime and $\alpha \geq 1$ then $\mathbf{P}$ has a non trivial center. i.e.
$\mathbf{Z}(\mathbf{P}) \neq 1$ (and by Lagrange theorem $|\mathbf{Z}(\mathbf{P})| \geq p$)

■ now using the preceding point and lattice isomorphism theorem for strong induction on we get :
for p prime if $|\mathbf{G}| = p^{\alpha}$ then there exists a subgroup of order p^{β} in $\mathbf{G}$ for every $0 \leq \beta \leq \alpha.$

■ if $|\mathbf{G}| = p^2$ for p prime then $\mathbf{G}$ is abelian as $\mathbf{P}/\mathbf{Z}(\mathbf{P})$ is cyclic and more precisely $\mathbf{Z} \cong \mathbf{Z}_{p^2}$ or $\mathbf{Z}_p \times \mathbf{Z}_p$

Cauchy's Theorem

if $\mathbf{G}$ is finite group such that $p||\mathbf{G}|$ (prime p) then $\mathbf{G}$ has an element of order $p.$
(use McKay's proof : form p—tupels from elements of $\mathbf{G}$ i.e. $\{(x_1, x_2, .., x_p)\}$ such that $x_1 x_2 .. x_p = 1$ and prove cyclic permutation here forms an equivalence relation , whose equivalence classes can have only orders 1 or p and there exist more than one element whose equivalence class is singleton.)

Consequences of Cauchy's theorem

■ **If $\mathbf{G}$ is finite ablelian group then it has a subgroup of order n for every +ve n dividing $|\mathbf{G}|.$** (use induction : as $\mathbf{G}$ is abelian every subgroup is normal and quotient group is defined.)

■ any group of order $\mathbf{P}^2$ is abelian and is of form $\mathbf{Z}_p \times \mathbf{Z}_p$ (refer direct products) or $\mathbf{Z}_{p^2}$

SYLOW'S Theorem

Definitions : for a prime p, $\mathbf{G}$ group
a group of order p^{α} is called a p-group, subgroups of $\mathbf{G}$ which are p-groups are called p-subgroups.
If $\mathbf{G}$ is group of order $p^{\alpha}m$ where $p \not| m$ (does not divide) then a subgroup of $\mathbf{G}$ or order p^{α} is called a Sylow p-subgroup of $\mathbf{G}.$
The set of all Sylow p-subgroups of $\mathbf{G}$ is denoted by $Syl_p(\mathbf{G})$ and number of Sylow p-subgroups of $\mathbf{G}$ is denoted by $n_p(\mathbf{G})$
Theorem : if $\mathbf{G}$ group has an order $p^{\alpha}m$ for $p \not| m$, prime p then :

■ Sylow p-subgroups of $\mathbf{G}$ exists, i.e. $Syl_p(\mathbf{G}) \neq \emptyset.$

■ if $\mathbf{P}$ is Sylow p-subgroups of $\mathbf{G}$ and $\mathbf{Q}$ is any p-subgroup of $\mathbf{G}$ then $\exists g \in \mathbf{G}$ such that $\mathbf{Q} \ll g\mathbf{P}g^{-1}$ i.e. every p-group of $\mathbf{G}$ is subgroup of conjugate of a Sylow p-subgroups of $\mathbf{G}$, particularly any two Sylow p-subgroups of $\mathbf{G}$ are conjugates in $\mathbf{G}.$

■ $n_p(\mathbf{G}) \equiv 1 \pmod{p}$ i.e. $n_p(\mathbf{G}) = 1 + kp$ and as $n_p(\mathbf{G}) = |\mathbf{G} : \mathbf{N}_{\mathbf{G}}(\mathbf{P})|$ we get $n_p(\mathbf{G})|m.$

Consequences of of Sylow's Theorem

if P is Sylow p-subgroups of G then P is normal in G iff P char G. iff all subgroups generated by elements of p-power order are p-groups (i.e. if $X \subset G$ and $|x|$is a power of p for every $x \in X$ then $\langle X \rangle$ is p-group) iff $n_p(G) = 1$.

11.0.1 Classification of groups using Sylow's theorem

if p, q are distinct primes

group G of order pq

■ if $p < q, Q \in Syl_q(G)$ and $P \in Syl_p(G)$ then $Q \trianglelefteq G$
also if $P \trianglelefteq G$ then $G \cong Z_{pq}$.(use $G/C_G(P) \cong$ a subgroup of $Aut(Z_p)$ and $p, q \not| p - 1$ to prove $C_G(P) = G$)
■ if $p < q$ we have $n_p|q \implies n_p = 1$ or q and as $n_p = 1 + kp \implies$ if $p \not| q - 1$ then $n_p = 1$ so $P \trianglelefteq G$ and $G \cong Z_{pq}$
■ if $p|q - 1$ then this is a unique non Abelian group of order pq

group G of order p^2q

■ if $q < p$ then the Sylow p-subgroup is normal in G (as $n_p = 1$).
■ if $p < q$ then Sylow q-subgroup is normal in G except for when $q = p + 1$ i.e. $p = 2$ i.e. $|G| = 12$ then G has either a Sylow - 2 or a 3 normal subgroup (use $n_q|p^2 \implies q|p+1$).

■ if G is a finite group of order $n = p_1p_2..p_r$ for distinct primes p_i such that $p_i \not| p_j - 1\ \forall i, j$ then G is cyclic.
Converse of preceding point is true i.e. for $n \geq 2$ and if every group of order n is cyclic then $n = p_1..p_r$ for $p_i \not| p_j - 1$.
Generalising preceding points we get
■ Z_n is the only group of order n i.e. number of groups of order n is 1 (cyclic) iff $gcd(n, \phi(n)) = (n, \phi(n)) = 1$
■ Every Group of order n is abelian iff prime factorization of $n = p_1p_2..p_iq_1^2q_2^2..q_j^2$ for and n is relatively prime to $(p_1 - 1)(p_2 - 1)..(p_i - 1)(q_1^2 - 1)(q_2^2 - 1)..(q_j^2 - 1)$. (last two points are not a direct consequence but look into Gallian's papers)

12 Automorphism Theorems

if $H \trianglelefteq G$ (group) then G acts by conjugation on H as automorphism of H i.e. $\sigma_g : H \to gHg^{-1}$ by $\sigma_g(h) = ghg^{-1}$ is an automorphism.

now by properties of conjugate action and preceding point we have :
$\{\sigma_g\} \cong G/C_G(H)$ so $G/C_G(H) \cong$ subgroup of $Aut(H)$ if H is normal in G

clearly $K \trianglelefteq N_G(K)$ so we have
$N_G(K)/C_G(K) \cong$ a subgroup of $Aut(H)$.
Particularly $G/Z(G) \cong$ a subgroup of $Aut(G)$.

the preceding mentioned subgroup of $Aut(G)$ formed by conjugation is called inner automorphism of G denoted by $Inn(G)$.

Characteristic Subgroups

Characteristic Subgroups of G are subgroup of G which remain fixed for every automorphism of G i.e. H char G iff $\sigma(H) = H\ \forall \sigma \in Aut(G)$

Properties of Characteristic Subgroups

■ They are Normal (converse is not true.)
■ if H is unique subgroup of order n in G (only subgroup of order n) then H char G.
■ if K char H and $H \trianglelefteq G$ then $K \trianglelefteq G$.
■ H char K and K char G then H char G.

13 Semi Direct product

Motivation : to Generalise direct product so that not both H and K be normal to make a group HK, this helps in building larger groups which have subgroups isomorphic to both H and K. In this case H is normal and K is necessarily not. let $H \trianglelefteq G$ and $H \cap K = 1$ then there is a unique way of writing elements of HK. If we have $hk \to (h, k)$ using some map then $(h_1, k_1)(h_2, k_2) = (h_1k_1)(h_2k_2) = h_1k1h_2(k_1^{-1}k_1)k_2 = h_1(k_1h_2k_1^{-1})k1k_2 = h_3k_3 = (h_3, k_3)$. so if we understand how $k_1h_2k_1^{-1} \in H$ without the need of G then we can define a larger group HK. This needs us to act K on H (by conjugation) i.e. a homomorphic map from $K \to \mathrm{Aut}(H)$. we then define : if $k.h = khk^{-1}$ then $(h_1k_1)(h_2k_2) = (h_1k_1.h_2)(k_1k_2)$ gets the operation part done for HK

For H,K be groups, $\phi : K \to \mathrm{Aut}(H)$ a homomorphism this defines a left action of K on H say by $.$ then let G be set of ordered pairs $\{(h, k)|h \in H, k \in K\}$ and define operations on it by $(h_1, k_1)(h_2, k_2) = (h_1\,k_1.h_2, k_1k_2)$:

■ this operation makes G into a group (**Semi Direct product**) of order $|G| = |H||K|$

■ for set $\tilde{H} = \{(h, 1)|h \in H\} \ll G$ the map $h \to (h, 1)$ makes $H \cong \tilde{H}$

■ similarly for set $\tilde{K} = \{(1, k)|k \in K\} \ll G$ the map $k \to (1, k)$ makes $K \cong \tilde{K}$

■ and $\tilde{H} \trianglelefteq G$, $\tilde{H} \cap \tilde{K} = \{1\}$, if $\tilde{h} = (h, 1) \in \tilde{H}, \tilde{k} = (1, k) \in \tilde{K}$ then $\tilde{k}\tilde{h}\tilde{k}^{-1} = (k.h, 1) = (\phi(k)(h), 1)$ i.e. action of k on h under ϕ.

The preceding group G can be symbolised (as in case of direct product) as $G = H \rtimes_{\phi} S$ or simply $H \rtimes G$ i.e. read as G semi direct product of H and K (| on the right of $\rtimes$denotes that $H \trianglelefteq G$)

$H \rtimes G = H \times G$

■ iff $\phi : K \to \mathrm{Aut}(H)$ is trivial i.e. $\phi(k) = 1 \, \forall k \in K$.

■ iff $K \trianglelefteq H \rtimes K$.

■ iff $\psi : H \rtimes K \to H \times K$ by $(h, k) \to (h, k)$ (i.e. identity map) is homomorphism (in fact isomorphism.)

Recognition Theorem of Semi Direct product

if $H, K \ll G$ are such that $H \trianglelefteq G$ and $H \cap K = 1$ then by ϕ action of conjugation of K on H in G we have

$$HK \cong H \rtimes K.$$

For $H \ll G$, $K \ll G$ is called **Compliment** of H in G if $H \cap K = 1$ and $G = HK$

13.1 Examples

Group G of order pq for p, q distinct primes: by Sylows theorems we have at least one of the Sylow subgroup is normal, say $p < q$ then $Q = Syl_q(G) \trianglelefteq G$ and $\mathrm{Aut}(Q)$ is cyclic group of order $q - 1$.

case 1 : if $p \not| q - 1$ then $\phi : Syl_p(G) = P \to \mathrm{Aut}(Q)$ is trivial so $G = PQ = P \rtimes Q = P \times Q$ this makes G cyclic as stated earlier.

case 2 : if $p | q - 1$ as $\mathrm{Aut}(Q)$ is cyclic it contains a unique subgroup (cyclic) of order p say $\langle \gamma \rangle$ so any homomorphism $\phi_i : P \to \mathrm{Aut}(Q)$ is given by $\phi_i(x) = \gamma^i$ for $P = \langle x \rangle, 0 \geq i \geq p - 1$. Now ϕ_0 is trivial so goes to case 1. if $i \neq 0$ then each ϕ_i gives raise to non-abelian group $Q \rtimes_{\phi_i} P$, but all these groups are isomorphic as the any non trivial homomorphisms of $|P| = p = |\langle \gamma \rangle|$ maps generators map to generators. Thus all these semi direct product groups are same.

Finally we have there are only two unique groups of order pq one cyclic and other the non trivial semi direct product of its sylow subgroups.

Class equation of non abelian pq order group

now for the unique non-abelian group of order pq for $p|q-1$ we have $n_p = q$ and as each element of sylow p subgroup is transferred to one (non identity) element of other sylow p group by conjugation and as sylow p group $\cong Z_p$ (abelian) we have each element other than e of sylow p subgroup has q elements in conjugacy class i.e. q is repeated $p-1$ times, now as Q = sylow q subgroup is normal and $\cong Z_q$ we have $|Inn(Q)| = |G/C_g(Q)| = |G/Q| = p$ so p elements in one class and number of distinct classes equal to partition of $q-1$ non identity elements of Q into each p element part sets i.e. $q-1/p$ distinct classes. From this we get

$|G| = pq$

$$= 1 + \underbrace{p + p + .. + p}_{\frac{q-1}{p}\text{ times}} + \underbrace{q + q + .. + q}_{p-1\text{ times}}.$$

Group G of order p^3 for p an odd prime : assume G is not cyclic then

if G is not abelian then $|Z(G)| = p$ only by class equation and fact that if $P/Z(P)$ is cyclic then P is abelian.

defining a pth power map $x \to x^p$ gives a homomorphism from $P \to Z(P)$ and with kernel of size only p^3 or if this kernel is p^2 then there is an element of order p^2

case 1 : G has a element x of order p^2

let $H = \langle x \rangle$ then H is prime index in G so $H \trianglelefteq G$, if E is kernel pth power map then $E \cong Z_p \times Z_p$ as every $x \in E$ $x^p = 1$ clearly $E \cap H =< x^p >$.

now if $y \in E - H$ then for $K = \langle y \rangle$ we have $H \cap K = \{1\}$ and $G = H \rtimes K$ thus $G \cong Z_{p^2} \rtimes Z_p$ for some $\phi : K \to Aut(H)$ if ϕ is trivial then $G \cong Z_{p^2} \times Z_p$ which is abelian so for non trivial ϕ there exists a unique non abelian $H \rtimes K$ (the non trivial ones are isomorphic as K is of order p)

case 2 : every non identity element is of order $p.$ so for any subgroup of H if is of order p^2 then $H = Z_p \times Z_p$ and clearly $H \trianglelefteq G$ (as prime index) , if $K = \langle y \rangle$ for some $y \in G - H$ then $|K| = p$ and $H \cap K = \{1\}$ thus $G = H \rtimes K$ i.e. $G \cong (Z_p \times Z_p) \rtimes Z_p$ for some $\phi : K \to Aut(H)$ by similar reasoning if ϕ is trivial then $G \cong Z_p \times Z_p \times Z_p$ which is abelian , only other possibility is a non abelian G

Thus the only groups of order p^3 upto isomorphism are :

abelian : cyclic, $Z_{p^2} \times Z_p$, $Z_p \times Z_p \times Z_p$

and non abelian : $Z_{p^2} \rtimes Z_p$, $(Z_p \times Z_p) \rtimes Z_p$ for some non trivial ϕ homomorphism from Z_p to its complement.

Class equation for group of order p^3

clearly $|Z(G)| = p$ now if $g \notin Z(G)$ then $g \in C_G(g)$ and $Z(G) \ll C_G(g)$ but $C_G(g) \neq G$ so only possibility remaining is $|C_G(g)| = p^2$ so $|G : C_G(g)| = p$ now calculating we get

$$|G| = p^3 = \underbrace{1 + 1 + .. + 1}_{p\text{ times}} + \underbrace{p + p + .. + p}_{p^2-1\text{ times}}.$$

13.2 p-groups and Fundamental theorem of finite abelian groups

a group of order p^α for p prime and $\alpha \geq 1$ is called a p-Group.

for a p-Group of order p^a

■ $Z(P) \neq \{1\}$. i.e. center of P is not trivial

■ for non trivial $H \trianglelefteq P$ then $H \cap Z(P) \neq 1$.

(In particular every normal subgroup of order p of P is contained in $Z(P)$.)

■ for $H \trianglelefteq P$ and if $p^b||H|$ then H contains a group of order p^b which is normal in P (In particular P has a normal subgroup p^b for every $b \in \{0, 1, .., a\}$)

■ if proper $H \ll P$ then proper $H \ll N_P(H)$ i.e. every proper subgroup of P is a proper subgroup of its normaliser in P.

■ Every maximal subgroup of P is of index

p and is normal.

Every finite abelian group is a direct product of its Sylow subgroups
(if finite abelian G is such that $|G| = p_1^{k_1}p_2^{k_2}p_3^{k_3}..p_r^{k_r}$ for distinct primes p_i then $P_1 = Syl_{p_1}(G), P_2 = Syl_{p_2}(G) \trianglelefteq G$ and $P_1 \cap P_2 = \{1\}$ as $p_1 \not| p_2$ thus $P_1P_1 \cong P_1 \times P_2$ now $P_3 = Syl_{p_3}(G) \trianglelefteq G$ and $P_1P_2 \cap P_3 = \{1\}$ as $p3 \not| p2, p3 \not| p1$ thus $P_1P_2P_3 \cong P_1P_2 \times P_3 \cong P_1 \times P_2 \times P_3$ continuing this process till P_r we get by an order argument $G = P_1P_2P_3..P_r \cong P_1 \times P_2 \times P_3 \times .. \times P_r$.)

if G is an abelian p group then for $a \in G$ with maximal order we have

$$G = \langle a \rangle \times K.$$

where K is the complement of $\langle a \rangle$ in G
(use induction : choose $b \notin \langle a \rangle$ of minimal order and prove $\langle a \rangle \cap \langle b \rangle = \{1\}, |\langle b \rangle| = p$, for $G/\langle b \rangle$ if $\bar{}$ represents the corresponding elements in $G/\langle b \rangle$ prove $|\overline{a}| = |a|$ so $\overline{a}$ is maximal order thus $\overline{G} = \overline{a} \times \overline{K}$ pull back $\overline{K}$ to K in G , prove $\langle a \rangle \cap K = \{1\}$ and claim $G = \langle a \rangle \times K$ by order argument .)

an Immediate consequence of preceding point :
Every p-Group is the direct product of its cyclic subgroups.
From Last three points we get a Fundamental theorem of finite abelian Groups :

Fundamental theorem of finite abelian Groups

elementary divisors decomposition form : if G is an abelian group of order $n = p_1^{\alpha_1}p_2^{\alpha_2}..p_k^{\alpha_k}$ then :

■ $G \cong A_1 \times A_2 \times .. \times A_k$ where $|A_i| = p_i^{\alpha_i}$.

■ each $A_i \cong Z_{p_i^{\beta_{i1}}} \times Z_{p_i^{\beta_{i2}}} \times .. \times Z_{p_i^{\beta_{it}}}$ with $\beta_{i1} \geq \beta_{i2} \geq .. \geq \beta_{it}$ and $\beta_{i1} + \beta_{i2} + .. + \beta_{it} = \alpha_i$
(p_{ij}^{β} are called elementary divisors of G)

■ This decomposition is unique (till isomorphism.)

Fundamental theorem of finite abelian Groups

invariant factors decomposition form : Every finite abelian group G is of unique decomposition form (till isomorphism) given by

$$G \cong Z_{n_1} \times Z_{n_2} \times .. \times Z_{n_s}.$$

With $n_j \geq 2 \forall i$ and $n_{i+1}|n_i$ for $1 \leq i \leq s-1$

for $m, n \in \mathbb{Z}^+$

■ $Z_m \times Z_n \cong Z_{mn}$ iff $(m, n) = 1$

■ if $n = p_1^{\alpha_1}p_2^{\alpha_2}..p_k^{\alpha_k}$ then
$Z_n = Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times .. \times Z_{p_k^{\alpha_k}}$.
From this theorem we can Change the forms of a Fundamental theorem of finite abelian Groups.

14 Presentations

A presentation of a group is a compact way of stating the properties of group from which the group it self can be derived

Generators a group G is said to be generated by a subset $A = \{a_1, a_2, .., a_n\}$ if every element of G is a combination of these elements (by group operation) and is denoted by $G = \langle A \rangle = \langle a_1, a_2, .., a_n \rangle$

Every finite group has a finite generating set (consider the group itself)

The properties that these generators holds holds even for the group and the converse is also true the properties possessed by the group is the properties fo these generators too. Thus if we know all the generators and all their properties it is enough to in a sense to know the whole group itself all other properties of the group can be derived from these so if $a_1, a_2, .., a_n$ are generators of G with properties $P_1, P_2, .. P_m$ only then G

can be stated as $\langle a_1, a_2, .., a_n | P_1, P_2, .., P_m \rangle$ and this is called **Presentation** of G in a sense the presentation is 'complete' or is made 'complete' by adding properties i.e. whole of G the group and the corresponding group operation can be derived from the Presentation of **G.**

To denote presentations ('complete') we use $G \mathrel{\overset{\wedge}{\underset{\vee}{\equiv}}} \langle a_1, a_2, .., a_n | P_1, P_2, .., P_m \rangle$

examples

$$Z_n \mathrel{\overset{\wedge}{\underset{\vee}{\equiv}}} \langle x | x^n = 1 \rangle$$
$$D_{2n} \mathrel{\overset{\wedge}{\underset{\vee}{\equiv}}} \langle r, s | r^n = s^2 = 1,\ rs = sr^{-1} \rangle$$
for $d = (m, n)$
$$Z_m \times Z_n \mathrel{\overset{\wedge}{\underset{\vee}{\equiv}}} \langle x, y | x^n = y^m = 1, xy = yx, x^{n/d} = y^{n/d} \rangle$$

15 Major Group examples and their Properties

15.1 Cyclic Group

Cyclic groups can be viewed as quotient groups of $\mathbb{Z}$ formed by $\{kn | k \in \mathbb{Z}\} = n\mathbb{Z} \ll Z$ for $n \in \mathbb{Z}$ i.e. $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, .., \overline{n-1}\}$ where $\bar{s} = \{q \in \mathbb{Z} | q \pmod{n} = s\}$ and $(\mathbb{Z}/nZ, \oplus) \cong Z_n$ where $\oplus$ is modulo addition w.r.t n i.e. $a \oplus b = (a + b) \pmod{n}$. All properties of this group is same as any cyclic group of same finite order.
Infinite cyclic group $\mathbb{Z}$ whose generators are $\{1, -1\}$ only.

15.2 $(\mathbb{Z}/n\mathbb{Z})^*$

Define a group $(\mathbb{Z}/n\mathbb{Z})^*$ subset of $Z/n\mathbb{Z}$ (not subgroup) with operation $\otimes$ i.e. $a \otimes b = (ab) \pmod{n}$ and $(\mathbb{Z}/n\mathbb{Z})^* = \{i < n | (i, n) = 1\}$ i.e. $i < n$ such that i is relative prime to n and $Aut(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^*$

$|(\mathbb{Z}/n\mathbb{Z})^*| = \varphi(n)$

$(\mathbb{Z}/2^n\mathbb{Z})^*$ is not cyclic for $n \geq 3$
(as $(2^n - 1, 2^n) = 1$,$(2^{n-1} - 1, 2^n) = 1$ but $(2^n - 1)^2 \equiv 1 \pmod{2^n}$ and $(2^{n-1} - 1)^2 \equiv 1 \pmod{2^n}$ so $| < 2^{n-1} - 1 > | = | < 2^n - 1 > | = 2$)

for every odd prime p and $n \geq 1$

$(\mathbb{Z}/p^n\mathbb{Z})^*$ is a cyclic group of order $p^{n-1}(p-1)$

(use ring theory.)

15.3 Dihedral Groups

Motivation

given a n-regular (equal sides) polygon the ways in which it can be moved or transformed via rigid motions (no tear or distortions like stretch) to obtain the same figure (symmetric to original position). We call these transformations symmetries, to visualize them we can mark each vertex (corner) with fixed number starting from 1 to n in a clockwise fashion and see how symmetries change the positions of these numbers.
■ for example if r a symmetry that rotates the polygon by $2\pi/n$ degrees clockwise, changes the position of numbers like 1 goes to position where 2 was i.e. $1 \to 2$, similarly $i \to i+1$ for $1 \leq i < n$ and $n \to 1$
■ This motion can be replicated counter-clockwise also and the flip or mirroring of positions via a line of symmetry also constitute such motions.
■ all these motions can be condensed in to just two motions and their combinations:
■ r a rotation clockwise by $2\pi/n$
■ s a flip (change of position from left to right vis-a-vis like a mirror) through the line of symmetry between vertex 1 and centre of the polygon
■ **Group concept** These motions from a group if we regard identity as the one fixed starting position and composition of motions as binary operations.
I.e. for a n-regular polygon the group formed by symmetries (rigid motions) constitute a group under composition

This group is made up of r and s motions and their combinations, Properties and

derivation:
■ $r^n = e$ (Identity), $s^2 = e$.
■ $s \neq r^j$.
■ $sr^j \neq sr^i$ $(i \neq j)$.
■ $(r^i)^{-1} = r^{n-i}$, $s^{-1} = s$.
■ $rs = sr^{-1}$ so by induction

$$r^i s = sr^{-i}.$$

■ from preceding points we get:

Dihedral group of n-regular polygon = D_{2n} = $\{e, r, r^2, .., r^n - 1, s, sr, sr^2, .., sr^{n-1}\}$.

here $2n$ signifies the order of the group

Properties of D_{2n}

■ $\{r^i | 0 \leq i < n\}$, $\{e, s\}$ forms Cyclic subgroups (there are many other cyclic, non cyclic-subgroup).
■ if n is odd only e commutes with every element.
■ if n is even only $e, r^{n/2}$ commutes with every element.
■ if G is any finite group generated by two distinct elements x, y for order of $y = 2$ then $G \cong D_{2n}$ where $n = |xy|$
■ **also if $|G| = 2p$ for a prime p and is non abelian then $G \cong D_{2p}$**

Class equation

for D_{2n} we have
■ if n is even then : $\{e, r^n/2\} = Z(D_{2n})$, for every r^i, $r^j r^i r^{n-j} = r^i$, $sr^i s = r^{-i} = r^{n-1}$ and $sr^j r^i r^{-j} s = r^{-i}$ so for given $n - 2$ r^i variables have a conjugacy class of order 2 so a total of $n - 2/2$ classes , for s, $r^j sr^{-j} = sr^{n-2j}$ now as n is even $n - 2j$ is even so conjugacy class of $s = \{sr^{2i}\}$ and for sr, $r^j srr^{-j} = sr^{n-2j+1}$ so conjugacy class of $sr = \{sr^{2i+1}\}$ from this we get class equation

$$|D_{2n}| = 1 + 1 + \underbrace{2 + 2 + .. + 2}_{\frac{n-2}{2}\text{ times}} + \frac{n}{2} + \frac{n}{2}$$

■ if n is odd most remain same but as $\{e\} = Z(D_{2n})$, $n - 1/2$ conjugacy classes of 2 elements and only one remaining class with n elements (class of s) so we get class equation

$$|D_{2n}| = 1 + \underbrace{2 + 2 + .. + 2}_{\frac{n-1}{2}\text{ times}} + n$$

Semi direct product construction of $D_{2n} = H \rtimes K$

■ clearly $\langle r \rangle$ is of index 2 so normal in D_{2n} so $H = \langle r \rangle = Z_n$ and $K = Z_2$ only possibility left
■ we know $rs = sr^{-1}$ i.e. $srs = r^{-1}$ or $sr^i s = r^{-i}$ so define automorphism $\phi : K \to Aut(H)$ by $x.y = y^{-1}$
■ thus we have $D_2n \cong Z_n \rtimes Z_2$

15.4 Symmetric Groups

Motivation : every element in a finite or countably finite set can be numbered so representing each element with a number makes sense the bijections (maps) of these sets form a group these can be represented as permutations or rearrangements of numbers.

Group concept : for a given set A the bijections (maps) on this set given by S_A forms a group under function composition : identity map acts as identity, clearly composition of two bijections is another bijection, every bijection has an inverse which is a bijection

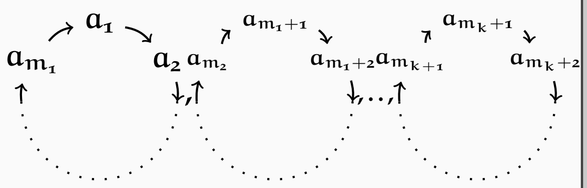
for set $\Omega = \{1, 2, .., n\}$ the bijections on this or Symmetric group of this group is S_n and clearly $|S_n| = n!$

15.4.1 Cycles

each bijection σ of Ω can be represented as the following :

$$\sigma = (a_1, a_2, .., a_{m_1})(a_{m_1+1}, a_{m_1+2}, .., a_{m_2}).. (a_{m_k+1}, a_{m_k+2}, .., a_{m_{k+1}})$$

which can be read as (if → indicates maps to)



where a_i's are distinct elements of Ω

15.4.2 Properties of Cycles and cycle decompositions:

cycles can be composed similar to corresponding bijections and the results in both case are same (note : composition of cycles are simplified right to left).

disjoint cycles commute.

order of a m-cycle (of length m or consisting of m elements) is m

order of a bijection with disjoint cycles representation is the l.c.m of lengths of the cycles in its representation.

Cycle Type : for $\sigma \in S_n$ is a product of $n_1, n_2, .., n_r$ cycles (including 1-cycle) such that $n_1 \geq n_2 \geq .. \geq n_r$ then integers $n_1, n_2, .., n_r$ are called the cycle type of σ

Partition of $n \in \mathbb{N}$ is a non decreasing sequence of +ve integers summing up to n.

a bijection has order p prime iff it is represented as product of commuting p-cycles.

if $\sigma, \tau \in S_n$ and σ has a cycle decomposition $(a_1, a_1, .., a_{k_1})(b_1, b_2, .., b_{k_1}), ..$ then

$$\tau\sigma\tau^{-1} \text{ has cycle decomposition } (\tau(a_1), \tau(a_1), .., \tau(a_{k_1})) (\tau(b_1), \tau(b_2), .., \tau(b_{k_1})), ...$$

(use if $\sigma(i) = j \implies \tau\sigma\tau^{-1}(\tau(i)) = \tau(j)$ thus if i, j appear in $\sigma \implies \tau(i), \tau(j)$ appear in τ's cycle decomposition).

From preceding point we get 2 elements of S_n are conjugates iff they have same cycle type.

and from preceding two point we get the number of conjugacy classes of S_n are equal to the partitions of n. (note here we include even 1-cycles)

if $\sigma \in S_n$ and σ is decomposed into (distinct) $m_1, m_2, .., m_r$ cycles (including 1-cycle) with multiplicity (number of cycles for a fixed length) of $k_1, k_2, .., k_r$ (so $n = \sum_{i=1}^{r} k_i m_i$, σ consists of k_i m_i-cycles which are disjoint) then the number of permutations of cycle type σ or the number of elements in the conjugacy class of σ is equal to

$$\frac{n!}{(k_1!m_1^{k_1})(k_2!m_2^{k_2})..(k_r!m_r^{k_r})} = \frac{n!}{\prod_{i=1}^{r} k_i!m_i^{k_i}}.$$

from preceding point we have, if $\mathcal{K}$ is a transposition conjugacy class of S_n and $\mathcal{K}'$ is any other conjugacy class on an element of order 2 that is not a transposition of S_n then except for $n = 6$ (S_6) $|K| \neq |K'|$ (for S_6 $|K| = 15$ and for class 3 disjoint transposition $|K'| = 15$ only exception).

from preceding two points we have :

$$\mathbf{Aut}(S_n) = \mathbf{Inn}(S_n).$$

with only exception of S_6
where $|\mathbf{Aut}(S_6) : \mathbf{Inn}(S_6)| = 2$
(use if $\sigma \in \mathbf{Aut}(S_n)$ then for a conjugacy class K $\sigma(K)$ is also a conjugacy class, so transpositions are mapped to transpositions except in S_6, $\sigma((1,2)) = (a,b_1), \sigma((1,3)) = (a,b_2),..,\sigma((1,n)) = (a,b_n)$ only , and these permutations generate S_n so $\mathbf{Aut}(S_n)$ has at most $n!$ order= order of $\mathbf{Inn}(S_n)$).

Class equation

from all preceding points we get if $n \geq 3$ (as $S_2 \cong Z_2$)

$$|S_n| = 1 + \sum_{p_i} \left(\frac{n!}{\prod_{i=1}^{r} k_{ij}! m_{ij}^{k_{ij}}} \right).$$

where $p_i's$ are distinct partitions of n such that p_i has disjoint k_{ij} cycles of cycle length m_{ij} i.e $n = \sum_j k_{ij} m_{ij}$

Greatest order element in S_n

■ order of element is equal to the lcm of lengths of disjoint cycles
■ so for given n we need to partition n into primes and multiply the primes in partition to get the order and find a partition of

$n = p_1 + p_2 + .. + p_k = \sum_{i=1}^{k} p_i$ for p_i primes

such that $p_1 p_2 .. p_k = \prod_{i=1}^{k} p_i$ is maximum.
■ by number theory we have the products of parts in partition is maximum if each part tends to e and number of parts tends to n/e so if $g(n)$ represents the greatest order element in S_n then we have

$$g(n) < e^{\frac{n}{e}}.$$

15.4.3 Transpositions and Alternating Group

a two cycle is called a transposition.

Every element of S_n can be made into product of transpositions (not necessarily distinct)
for eg : a cycle

$$(a_1, a_2, .., a_m) = \\ (a_1, a_m)(a_2, a_m)..(a_{m-1}, a_m).$$

let $x_1, x_2, .., x_n$ be n independent variables then we define :

$$\triangle = \prod_{1 \leq i \leq j \leq n} (x_i - x_j),$$

and for $\sigma \in S_n$

$\sigma(\triangle) = \prod_{1 \leq i \leq j \leq n} (x_{\sigma(i)} - x_{\sigma(j)})$. Then we get (by rearranging) $\sigma(\triangle) = \pm\triangle$.

Again we define a function : sign of $\sigma \in S_n$ i.e. $\epsilon : S_n \to \{-1, 1\}$ as

$$\epsilon(\sigma) = \begin{cases} +1, & \text{if } \sigma(\triangle) = \triangle \\ -1, & \text{if } \sigma(\triangle) = -\triangle \end{cases}$$

we call (define) $\sigma \in S_n$ is even permutation if $\epsilon(\sigma) = 1$ or an odd permutation if $\epsilon(\sigma) = 1$

map $\epsilon : S_n \to \{\pm 1\}$ is a homomorphism (if $\{\pm 1\}$ is assumed as multiplicative group)

Alternating Group

so an Alternating group of degree n denoted by A_n is the kernel of this homomorphism (i.e. set of all even permutations in S_n)

Classifying methods :

■ a transposition is an odd permutation
■ every n-cycle can be decomposed as product of $n-1$ transpositions.
■ so a m- cycle is odd permutation iff m is even and
vis-a-v a m- cycle is even permutation iff m is odd
■ from preceding points we get :

a permutation σ is odd iff the number of cycles of even length in its cycle decomposition is odd and vis-a-v for a permutation to be even.

every A_n for $n \geq 5$ is a simple group.

15.5 Quaternion Group

let $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ define group operations as

$$\forall a \in q_8, 1.a = a.1, -1.-1 = 1, -1.a = -a$$
$$i.i = j.j = k.k = -1$$
$$i.j = k, \quad j.i = -k$$
$$j.k = i, \quad k.j = -i$$
$$k.i = j, \quad i.k = -j$$

■ clearly Q_8 is non-ablelian
■ $Z(Q_8) = \{1, -1\}$
■ $\langle i\rangle, \langle j\rangle, \langle k\rangle$ are 3 normal subgroups of order 4 in Q_8

Generalised Quaternion Group

(refer semi-direct product and presentations)
■ let $H = \langle h\rangle \cong Z_{2^n}$, $K = \langle x\rangle \cong Z_4$ the form $H \rtimes K$ by $G = K \rightarrow Aut(H)$ by inversion i.e. $x.h = h^{-1}$ i.e. $xhx^{-1} = h^{-1}$
■ so $x^2 \in Z(G)$ and if $z = h^{2^{n-1}}$ then $\langle z\rangle$ is a unique subgroup of order 2 in H and x inverts this i.e. $xzz^{-1} = z^{-1} = z$ thus x centralizes z so we have $z \in Z(G)$ as z commutes with both x, h. now $x^2 z \in Z(G)$ so we have $\langle x^2 Z\rangle \trianglelefteq G$.
■ Now form the quotient group $\overline{G} = G/\langle x^2 z\rangle$ let bar indicate this transition so we have
$\overline{x}$ inverts $\overline{h}$ (property inherited from G) and $|\overline{G}| = |G|/|\langle x^2 z\rangle| = |G|/2 = 2^{n+1}$
if $n = 2$ we have $x^2 h^2 \in \langle x^2 z\rangle \implies x^2 x^2 h^2 \in x^2\langle x^2 z\rangle$ i.e. $h^2 \in x^2\langle x^2 z\rangle$ so we have $\overline{x}^2 = \overline{h}^2$ which implies $\overline{G} \cong Q_8$
■ Thus the General Quaternion Group is given by the Quotient group $\overline{G}$ and is presented as
$Q_{2^{n+1}} \cong \langle h, x | h^{2^n} = x^4 = 1, xhx^{-1} = h^{-1}, h^{2^{n-1}} = x^2\rangle$.

15.6 Matrix Groups

refer linear algebra and field theory
for each $n \in \mathbb{Z}^+$ let general linear group $GL_n(F)$ be set of $n \times n$ matrices with entries from F a field and with Determinant non-zero then $GL_n(F)$ forms a non-abelin group under matrix multiplication i.e.
$GL(F) = \{A_{n \times n} = [a_{ij}] | a_{ij} \in F, Det(A) \neq 0\}$

if $|F| = q < \infty$ then

$$|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2)..(q^n - q^{n-1})$$

(use the fact that if $det(A) \neq 0$ then its rows are linearly independent so the 1^{st} row r_1 can have $q^n - 1$ choices (as $|F^n| = q^n$ the vector space where the row lies and row is not zero) similarly 2^{nd} row r_2 is any thing but not a multiple of 1^{st} so as there are q elements in F there are q multiples of 1^{st} row and so there are $q^n - q$ choices , similarly for 3^{rd} row r_3 is not a linear combination of the first two hence $r_3 \neq q_1 r_1 + q_2 r_2$ so there are q^2 choices for linear combination thus r_3 has $q^n - q^2$ choices continuing similarly till n rows we get the result)

for each $n \in \mathbb{Z}^+$ let Special linear group $SL_n(F)$ be set of $n \times n$ matrices with entries from F a field and with Determinant $= 1$ then $SL_n(F)$ forms a non-abelin group under matrix multiplication as determinant is a multiplicative function i.e. $det(AB) = det(A)det(B)$ if all matrices involved are square
$SL(F) = \{A_{n \times n} = [a_{ij}] | a_{ij} \in F, Det(A) = 1\}$

if $|F| = q < \infty$ then

$$|SL_n(F)| = \frac{|GL_n(F)|}{q-1}$$

(use the fact that determinant is homomorphism from $GL_n(F) \to F^*$ with kernel $SL_n(F)$ and 1^{st} isomorphism theorem).

For a prime p is V is an abelian group(additive) of order p^n and property $pv = v + .. + v = 0 \ \forall v \in V$ then V is a n dimensional vector space over F_p so automorphisms of V are precisely non singular linear transformations from V to itself i.e. $Aut(V) \cong GL(V) \cong GL_n(F_p)$ so one can say $Aut(\underbrace{Z_p \times Z_p \times .. \times Z_p}_{n \text{ time}}) \cong GL_n(F_p)$ or $|Aut(\underbrace{Z_p \times Z_p \times .. \times Z_p}_{n \text{ time}})| = (p^n - 1)(p^n - p)..(p^n - p^{n-1})$

Semi direct relation and presentation of groups of order p^3

■ from Semi direct products we have a group of order p^3 has only 2 non-abelian groups i.e. $Z_{p^2} \rtimes Z_p$ and $(Z_p \times Z_p) \rtimes Z_p$ now from preceding arguments if $H = Z_p \times Z_p$ them $Aut(H) \cong GL_2(F_p)$ or $|Aut(H)| = (p^2 - 1)(p^2 - p) = p(p-1)(p^2-1)$ thus by cauchy's theorem $Aut(H)$ has an non trivial group of order p

■ we define this automorphism by: if $H = \langle a \rangle \times \langle b \rangle$ and $K = \langle x \rangle$ then define $\phi : K \to Aut(H)$ by $x.a = ab$ and $x.b = b$ in additive sense if we look at H as vector space over F_p then x acts as a non-singular linear transformation of $x(a) = a + b$ and $x(b) = a$ where $\{a, b\}$ forms a basis of H so matrix of $x = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \in GL_2(F_p)$

■ this results in a group with presentation $\langle x, a, b | x^p = a^p = b^p = 1, ab = ba, xax^{-1} = ab, xbx^{-1} = b \rangle$ and this group is called Heisenberg group over Z_p $H(F_p)$ (Heisenberg group $H(F)$ in general has an order p^{3n})

■ for the other group of order p^3 we have $Aut(H) \cong Z_{\phi(p^2) = Z_{p(p-1)}}$ so there is an non-trivial group of order p here too now if $H = \langle y \rangle, K = \langle x \rangle$ we define this automorphism by $x.y = y^{1+p}$ resulting in presentation $\langle x, y | x^p = y^{p^2} = 1, xyx^{-1} = y^{1+p} \rangle$

■ so if G is an non abelian group of order p^3, if it has an element of order p^2 then it is isomorphic to $Z_p^2 \rtimes_\phi Z_p$ $phi : x.y = y^{1+p}$ or if it doesn't have an element of order p^2 then is isomorphic to $H(F_p)$

15.6.1 Heisenberg group $H(F_p)$

$H(F)\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} a, b, c \in F\}$
where F is any field finite of infinite.

Properties

■ $H(F)$ is multiplicative matrix group, a subgroup of $GL_3(F)$

■ It is a **non-abelian** group of order p^3 if $|F| = p$ (can be used as example)

■ every element $h \in H(F)$ is of form $h = I + N$ for I identity and N nilpotent (so $N^3 = 0$). Now if F is characteristic p then $h^p = (I + N)^p$ using binomial theorem (as I and N are commutative)

we have $h^p = I + \sum_{k=1}^{p} \binom{p}{k} N^p \equiv I \pmod{p}$

if $p \neq 2$ so **every element of $H(F)$ for $ch(F) \neq 2$ has order p**

if $ch(F) = 2$ then $\binom{2}{2} = 1$ so order may vary

15.7 Familiar Q, Z, R, C and their quotient Groups properties

Z

let $Z \times Z \times ..Z$ n times be written as Z^n then

■ $Z^n \ncong Z^m$ iff $m \neq n$ (Z^n is generated by a set of cardinality atleast n like basis)

Q

■ every element (except 0) in Q has infinite order.

■ if $0 \neq a, b \in Q$ then there exist $n, m \in Z$ such that $na = mb \neq 0$ this property between elements is called commensurable i.e. any 2 non zero elements of Q are commensurable

■ every finitely generated subgroup of Q is **cyclic**
(use if $H = \langle \frac{m_1}{n_1}, \frac{m_2}{n_2}, .. \frac{m_k}{n_k}, \rangle \ll Q$, if $h \in H$ then $h = a_1 \frac{m_1}{n_1} + a_2 \frac{m_2}{n_2} + .. + a_k \frac{m_k}{n_k} = \frac{u}{n_1 n_1 .. n_k}$ for some $a_i \in Z$ so clearly $h \in \langle \frac{1}{n_1 n_1 .. n_k} \rangle$ so $H \ll \langle \frac{1}{n_1 n_1 .. n_k} \rangle$ and subgroup of cyclic group is cyclic)

■ Q is not finitely generated. (then it would be cyclic by preceding argument)

■ every proper subgroup of Q has infinite index so same goes for Q/Z
(use if $|Q : H| = n < \infty$ then $nq \in H \ \forall q \in Q$ but $q \to nq$ is isomorphism on Q so $Q \subseteq H$)

■ $Q \not\cong Q \times Z$ as $Q \times Z$ has subgroups of finite index like $Q \times 2Z$

■ $Q \not\cong Q \times Q$ as in $Q \times Q$ not every finitely generated subgroup is cyclic (eg: $\langle (0, 1), (1, 0) \rangle$)

■ Diadic rational group $\{a/2^n | n \in Z\}$ is a proper non cyclic group of Q

■ $(Q^*, \times)$ i.e. multiplicative group $Q - \{0\}$ is generated by $\{1/p | p$ is prime in$Z\}$

Q/Z

■ every element of Q/nZ has a finite order
(for $\frac{p}{q} + nZ$ we have $\frac{nqp}{q} + nZ = nZ$ and $nq \leq \infty$)

■ $Q/Z \cong Q/nZ$ (use isomorphism $x + Z \to x + nZ$)

■ every coset of Z in Q contains only one representative $q \in Q$ in the range $0 \leq q < 1$
(use if $0 \leq p, q <$ and $p + Z = q + Z$ then $p \in q + Z$ so $p = q + n$ for $n \in Z$ then clearly only possible n is 0) i.e.
$Q/Z = \{\frac{p}{q} + Z \mid 0 < p < q \in Z\}$.

■ From preceding representation we get that for a given $n \in Z^+$, Q/Z has only finitely many elements of order n precisely $\phi(n)$ elements i.e. $\{\frac{m}{n} + Z \mid 0 < m < n, (m, n) = 1\}$ is the required set.

■ also $\langle \frac{1}{n} + Z \rangle$ is the unique cyclic subgroup of order n in Q/Z. also we have $Q/Z = \cup_{q=1}^{\infty} \langle 1/q + Z \rangle$.

■ Q/Z is the torsion subgroup of R/Q (use if $a + Z \in R/Z$ has finite order then $na \in Z$ so $na = m$ i.e. $a = m/n \in Q$ so $a + Z \in Q/Z$)

■ Q/Z is isomorphic to multiplicative group of roots of unity in C^* (use map : choose the unique representative $0 \leq r/s < 1$ for the coset $r/s + Z$ and map to $r/s \to e^{\frac{2\pi r i}{s}}$)

a useful example Prüfer p-group Z_p'

let $H_k = \{z | z^{p^k} = 1\}$ for a prime p i.e. H_k is the set of p^k th root of unity then

■ H_k is cyclic group under complex multiplication (as generator of n^{th} root of unity is $e^{2\pi i/n}$)

■ $H_k \subset H_m$ iff $k \leq m$

now let $Z_p' = \{z | z^{p^n} = 1, n \in Z^+\}$ then

■ every proper subgroup of Z_p' is of form H_k i.e. every proper subgroup of Z_p' is cyclic

■ Z_p' is not finitely generated

■ to sum things up $Z_p' \ll (C^*, \times)$ such that every proper subgroup is cyclic but Z_p' is not even finitely generated

16 Nilpotent Groups and Commutator subgroups

for any G group define $Z_0(G) = 1, Z_1(G) = Z(G)$ (center of G) and $Z_{i+1}(G)$ as subgroup of G containing $Z_i(G)$ such that $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$ i.e. $Z_{i+1}(G)$ is the complete pre image of center of $G/Z_i(G)$ under natural projection ($Z_i(G) \trianglelefteq G$ by lattice isomorphism theorem.) this gives us a chain of subgroups

$$Z_0(G) \ll Z_1(G) \ll Z_2(G) \ll ..$$

called **upper central series** of G.

A group G is nilpotent if $Z_c(G) = G$ for some $c \in \mathbb{Z}^+$, smallest such c is called nilpotence class of G.

if P is a p-Group of order p^a then P is a nilpotent group of nilpotency class at most $a - 1$ (use fact that for a p-group center is not $\{1\}$ and order argument)

G is nilpotent iff $G/Z(G)$ is nilpotent.
(let $K = G/Z(G)$ then $Z_2(G)/Z_1(G) = Z(G/Z(G)) = Z_1(K)$, $Z_3(G)/Z_2(G) = Z(G/Z_2(G)) = Z((G/Z_1(G))/(Z_2(G)/Z_1(G)))$ by lattice isomorphism theorem so $Z_3(G)/Z_2(G) = Z(G/Z(G)/Z_1(K)) = Z_2(G)/Z_1(G)$ continuing this argument we get $Z_{i+1}(G)/Z_i(G) = Z_i(K)/Z_{i-1}(K)$ $\forall i$ thus if any one of K or G is nilpotent then the ratio described is $= \{1\}$ for some i, so the other is also nilpotent)

A finite group G of and let $p_1, p_2, .., p_s$ be the only distinct primes dividing $|G|$ and if $P_i \in Syl_{p_i}(G)$ then the following are equivalent i.e. $\Longleftrightarrow$

■ G is nilpotent.

■ if proper $H \ll G$ then proper $H \ll G$ i.e. every proper subgroup of G is a proper subgroup of its normaliser in G.

■ $P_i \trianglelefteq G$ i.e. every Sylow subgroup of G is normal.

■ $G \cong P_1 \times P_2 \times .. \times P_s$.

Now from preceding last point and from p-group theory we have:
If G is Finite Group then G is nilpotent iff it has a normal subgroup of each order dividing $|G|$ and is cyclic iff it has a unique subgroup of each order dividing $|G|$.

Frattini's Argument

if G is a finite group , $H \trianglelefteq G$ and P is a Sylow p-subgroup of H then $G = HN_G(P)$ and $|G : H|$ divides $|N_G(P)|$

A finite group is nilpotent iff every maximal subgroup of it is normal.

each group $Z_i(G)$ occurring in upper central series of G is a characteristic group G i.e. $Z_i(G)$ $char$ G

let $[x, y] = x^{-1}y^{-1}xy$ and if $H, K \ll G$ then $[H, K] = \langle [h, k] | h \in H, k \in K \rangle$ i.e. the group generated by these elements. ($G' = \langle [x, y] | x, y \in G \rangle$ is the commutator subgroup as mentioned earlier)

Properties of Commutators and their generated groups :
if $H \ll G$ group, $G' = \langle [x, y] | \forall x, y \in G \rangle$ and $x, y \in G$ then

■ $xy = yx[x, y]$.

■ $H \trianglelefteq G$ iff $[H, G] \ll H$. (as $g^{-1}hg \in H$ iff $h^{-1}g^{-1}hg \in H$)

■ $\sigma[x, y] = [\sigma(a), \sigma(b)]$ for any automorphism $\sigma \in Aut(G)$
so G' Char G.

■ G/G' is the largest abelian quotient group of G i.e. if $H \trianglelefteq G$ and G/H is abelian then $G' \ll H$ and conversely if $G' \ll H$ then $H \trianglelefteq G$ and G/H is abelian.
(use lattice iso thm for $H/G' \trianglelefteq G/G'$.)

■ restating the preceding point :
if $\phi : G \to A$ is a homomorphism of G to an abelian group A then $G' \ll ker(\phi)$

let $G_0 = G, G_1 = [G, G], .., G_{i+1} = [G, G_i]$ then the chain of groups

$$G_0 \gg G_1 \gg G_2 \gg ..$$

is called the **lower central series** of G

If $\phi : G \to H$ is group homomorphism then

$$\phi(G_n) \subseteq K_n$$

Every group occurring in lower central series is a characteristic subgroup of G i.e $G_i\ charG.$

Relation of UCS,LCS and Nilpotency

Group G is nilpotent iff $G_n = 1$ for some $n \geq 0$.
More precisely, G is nilpotent class c iff c is the smallest nonnegative integer such that $G_c = \{1\}$.

Derived Series

For any Group G define $G_{(0)} = G$, $G_{(1)} = [G, G]$ and $G_{(i+1)} = [G_{(i)}, G_{(i)}]$ this series of subgroups are called derived or commutator series of G
every $G_{(I)}\ Char\ G$

Solvablity and Derived series

■ A Group G is Solvable iff $G_{(n)} = 1$ for some $n \geq 1.$
■ if $H \ll G$ then $H_{(i)} \ll G_{(i)}$ thus if G is solvable so is are its subgroups
■ $\phi : G \to K$ is surjective homomorphism then $\phi(G_{(i)}) = K_{(i)}$ thus homomorphic images and quotient groups of Solvable groups are solvable.
■ if $N \trianglelefteq G$, N and G/N are solvable then so is G (use natural projection $\phi : G \to G/N$ so $\phi(G_{(n)}) = (G/N)_{(n)} = 1N$ so $G_{(n)} \ll N$ and as N is solvable this follows)

17 Application in medium order groups

this sections gives ways to find if a group of order < 10000 is not simple i.e. does it always have a non-trivial proper normal subgroup

1. Counting elements

■ if $|G| = pm$ for $p \not| m$ then $P \in Syl_p(G)$ imply that every element of P has order p and by Lagrange theorem different conjugates intersect in identity only so number of elements of order p in G is equal to $n_p(p-1)$
■ now after finding elements of order $p_i's$ if we assume that none of these is simple i.e. $n_{p_i} \neq 1$ then we can add all these elements of prime order, sometimes these number add up to > $|G|$ giving a contradiction that the group is not simple or has some order normal subgroup
■ eg: $|G| = 105 = 3.5.7$ then if we assume that G is simple the we must have $n_3 = 7$, $n_5 = 21$, $n_7 = 15$ so $7.2 = 14$ order 3 elements , $21.4 = 84$ order 5 and $15 * 6 = 90$ order 7 elements so adding up we get 188 elements > $|G|$ so G can never be simple.

2. Exploiting subgroups of small index

■ Now if G has a subgroup H of index k then we can apply group action of G on cosets of H in G to obtain a homomorphism from G to symmetric group S_k whose kernel is the largest normal group of G contained in H

■ Now if we assume that G is simple then this kernel ought to be identity thus G is isomorphic to a subgroup of S_k by 1^{st} iso thm. So we have $|G||k!$

■ now if we have k minimal i.e. no integer less than k satisfies $|G||k!$ then clearly any subgroup of index $< k$ should not exist if G is simple (if so it would mean $G \cong$ subgroup of S_l for $l < k$ contradicting minimality of k.)

■ now if $|G| = p_1^{a_1} p_2^{a_2} \ldots p_s^{a_s}$ for $a_j's \in \{1, 2\}$ and $p_1 < p_2 < \ldots < p_s$ the $k = p_s$

■ Now we can assume G is simple and choose k and some times find a contradiction that there exist a subgroup of G of index $< k$ thus proving G is not simple

■ eg: $|G| = 3393 = 3^2.13.29$, we have $k = 29$ so $G \lll S_{29}$ but we see that $n_3 = 13$ and ifor $P \in Syl_3(G)$ we have $|G : N_G(P)| = 13 < 29$ a contradiction.

3. Permutation representation

■ this method is refinement of preceding we assume that $G \lll S_k$ k minimal.

■ Here we can show some times that within S_k there is no simple group of order n.

■ Ristrictions like following allow preceding point to be in discussion: 1. if G contains an element or subgroup of a particular order so must S_k and
2. if $P \in Syl_p(G)$ and if P is also Sylow $p-$ subgroup of S_k then $|N_G(P)$ must divide $|N_{S_k}(P)$.

■ the 2^{nd} point is use full in case if $k = p$ or $p + 1$ and G has a subgroup of index k

■ if the case is as preceding then $p^2 \nmid k!$ so Sylow $p-$ subgroups of S_k are precisely generated by p cycles only. So counting gives: no. of Sylow $p-$ subgroups of S_k = no. p cycles in S_k / no of p cycles in each Sylow $p-$ subgroups = $n_p = (k(k-1)..(k-(p-1))/p)/p-1$ thus we have for $P \in Syl_p(S_k)$ then $|N_{S_k}(P) = |S_k|/|G : N_{S_k}(P) = k!/n_p = p(p-1)$ if $k = p$ or $p+1$.

■ Now if this is the case sometimes we find that $|N_G(P)| \nmid |N_{S_k}(P)|$ thus leading to contradiction of G being simple.

■ eg : $|G| = 396 = 2^2.3^2.11$ if G is simple we must have $n_11 = 12$ so if $P \in Syl_{11}(G)$ we have $|N_G(P) = |G|/n+11 = 33$ so G has a subgroup of index 12 thus we should have $G \lll S_{12}$ but $n_{11} = 11(11-1) = 110$ in S_12 and $33 \nmid 110$ thus G is not simple.

■ Important proposition to check for even order groups:
1. if G has no subgroup of index 2 and $G \lll S_k$ then $G \lll A_k$
2. If $P \in Syl_p(S_k)$ for odd prime p then $P \in Syl_p(A_k)$ and $|N_{A_k}(P)| = \frac{1}{2}|N_{s_k}(A_k)|$

■ eg: if $|G| = 264 = 2^3.3.11$, if G is simple then $n_{11} = 12$ so we have $G \lll S_{12}$ and by preceding propositions $G \lll A_{12}$ thus if $P \in Syl_{11}(G)$ then $|N_G(P) = 22$ but $|N_{A_{12}}(P) = 11(11-1)/2 = 55$ clearly $22 \nmid 55$ a contradiction.

4. Playing $p-$ subgroups off against each other for different primes p

■ choose primes p, q such that $|G| = pq$ is always cyclic i.e. $p \nmid q - 1$ for $p < q$

■ if G has $Q \in Syl_q(G)$, $|Q| = q$ and $p||N_G(Q)|$ then by Cauchy's Theorem on $N_G(Q)$ gives a group P of order p (P need not be a Sylow p-subgroup of G) normalising Q thus PQ is a group, Now we have chosen p, q as preceding we get PQ abelian so $PQ \lll N_G(P)$ so $q||N_G(P)|$

■ This information is sometimes sufficient to claim that $N_G(P) = G$ i.e. $P \trianglelefteq G$ or make $N_G(P)$ have minimal index smaller than permitted by permutation representation to give a contradiction

■ eg: if $|G| = 1785 = 3.5.7.17$, if G is simple then we must have $n_{17} = 35$ so we get for $Q \in Syl_{17}(G)$ then $N_G(Q) = 3.17$. Now $3||N_G(Q)$ so we have P a Sylow 3-subgroup of $N_G(Q)$ the as $3|17-1$ we have PQ is abelian so we should have that $Q \ll N_G(P)$ as P is also a Sylow 3-subgroup of G i.e. $17||N_G(P)|$ thus we cannot have $17||G : N_G(P)| = n3$ possible values of $n_3 = 7, 5.17, 5, 7, 17$ only and by previous argument $n_3 = 7$ only, this contradicts the fact that minimal index is 17.

5. Studying normalizers of intersections of Syloy p— subgroups

■ Refining the counting argument by opening that restriction that different Sylow p-subgroups intersect in identity i.e. if $P \in Syl_p(G)$ and $|P| = p^a,\ a \geq 2$ we cannot use $n_p(|P|-1)$ counting arguments.

■ Now if $R, P \in Syl_p(G)$ and $R \cap P \neq 1$ then let $P_0 = P \cap Q$ by theorems in p-groups we have $P_0 \ll N_P(P_0)$ and $P_0 \ll N_R(P_0)$ with proper inclusion, Here one can try $N_G(P_0)$ is large enough of has sufficiently small index in G for a contradiction.

■ a special case of preceding argument arises when $|P_0| = p^{a-1}$ the P_0 is of smallest prime index in P, R thus normal in both i.e. $P_0 \trianglelefteq P, R$ thus we can have $|N_G(P_0)| > p^a$ so sometimes leading to a contradiction by only possibility of $N_G(P_0) = G$

$\star$ for a finite group G, $|G| = p^a m$ and if $n_p \not\equiv 1 \pmod{p^2}$ then there are two distinct Sylow p-subgroups of G such that $P \cap R$ is of index p in both P, R i.e. $P \cap R = p^{a-1}$ ■ eg $|G| = 1053 = 3^4.13$ if G was simple then we must have $n_3 = 13$, but $13 \not\equiv 1 \pmod{3^2}$ so there exists $P, R \in Syl_3(G)$ with $P_0 = P \cap R = 3^3$ thus for $N = N_G(P_0)$ we have $N \trianglelefteq P, R$ so $|N| > 3^4$ so only possibility is $N = G$ a contradiction.

17 References

[1] David S. Dummit, Richard M. Foote : Abstract Algebra, John Wailey & sons, 3, (2004).

[2] Joseph A. Gallian : Contemporary Abstract Algebra, Cengage Learning, 9, (2017).