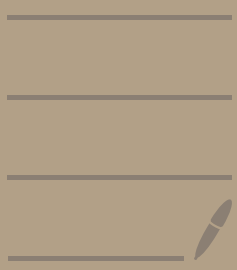
MA419

Basic Algebra

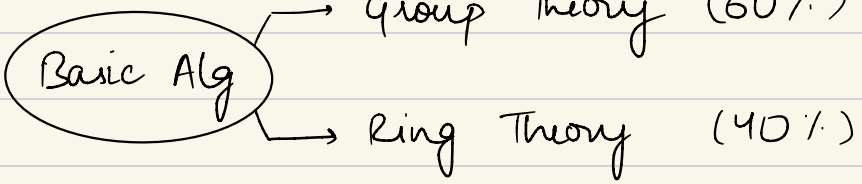


Instructor: Prof. Sudarshan Gurjar

References:
1. Lang Algebra
2. Lang Undergraduate Algebra
3. Dummit & Foote
4. Gallian
5. Artin
6. Hungerford

Grading: Midsem (40%)
Endsem (60%)

Attendance: Not compulsory



- Gp : A gp. is a set G with binary op
$* : G \times G \to G$

1. $*$ is assoc
$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$

2. $\exists\, e \in G$ called identity s.t $g * e = e * g = g$

3. Given $g \in G$, $\exists\, g^{-1} \in G$ s.t $g * g^{-1} = g^{-1} * g = e$

If in add^n, $g_1 * g_2 = g_2 * g_1 \quad \forall\, g_1, g_2 \in G$
then we say G is commutative (abelian)

- Identity & inverses are unique

if e & e' are id., then $e = ee' = e'$

if g_1, g_2 are inv. of g,

$$g_1 = g_1 e = g_1 g g_2 = e g_2 = g_2$$

Not^n: $g^n = \underbrace{g \cdot g \cdot \ldots g}_{n \text{ times}}$, $n \in \mathbb{N}$

$$g^{-n} = (g^{-1})^n$$

- Subgroup: A subset $H \subset G$ is a s.g ($H < G$) if

1. $e \in H$
2. $g_1, g_2 \in H \Rightarrow g_1 g_2 \in H$
3. $g \in H \Rightarrow g^{-1} \in H$

- gp. Homomorphism: $(G, *)$ & $(G', *)$ are gps.

$\varphi : G \to G'$ s.t $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$

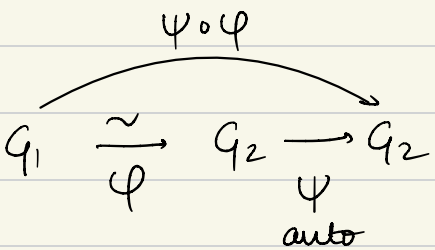
A homomp with an inv. is a gp. isomorphism. (bijective g.h)

- homomp maps id. to id & inv to inv

$$\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e) \Rightarrow \varphi(e) = e'$$
$$\varphi(e) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1}) \Rightarrow \varphi(g^{-1}) = \varphi(g)^{-1}$$

- An isomp. $G \to G$ is called an automorphism of G

- There are as many gi $G_1 \to G_2$ as there are autoмp of G_2



So, $\exists$ bij. b/w $Aut(G_2)$ & $Isom(G_1, G_2)$ if G_1 & G_2 are isomp.

- Kernel: $\varphi : (G, *) \to (G', *)$

$$Ker(\varphi) := \{ g \in G \mid \varphi(g) = e' \}$$

Clearly, $Ker(\varphi) < G$

- Image : $\varphi(G_1) \subset G_2$ is called image of φ.

Clearly, $\varphi(G_1) < G_2$

Examples

1. Trivial gp : G is a one pt. set
$G = \{e\}$

2. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ under add^n

3. Cyclic gp :

- Infinite : $(\mathbb{Z}, +)$
- finite : $(\mathbb{Z}/n\mathbb{Z}, +)$ for $n \in \mathbb{N}$
$= \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$

4. $(\mathbb{Z}/n\mathbb{Z})^* = \{ \bar{a} : a \in \mathbb{N} \ \& \ \underbrace{(a,n) = 1}_{\text{coprime}} \}$

under multip^n

$\exists\ p, q \in \mathbb{Z}$ s.t

$$ap + nq = 1$$
$$\Rightarrow \bar{a}\bar{p} + \bar{n}\bar{q} = \bar{1}$$
$$\Rightarrow \underline{\bar{a}\bar{p} = \bar{1}} \Rightarrow \bar{p} = \bar{a}^{-1}$$

5. Fix a set S & gp. G

Def $\mathrm{Mor}(S, G)$ to be collection of maps $S \to G$

$f_1, f_2 : S \to G$

$f_1 * f_2 (s) = f_1(s) * f_2(s)$

Nt: In math, structure of a space Y is reflected in set of maps $X \to Y$

Id - $f : S \to G$, $s \mapsto e$ $\qquad$ Inv - $f^{-1}(s) = (f(s))^{-1}$

6. Product of gps.

$$G_1 \times G_2 = \{ (g_1, g_2) \mid g_1 \in G_1 \ \& \ g_2 \in G_2 \}$$

Op - Component-wise op

$$(g_1, g_2) * (g_1', g_2') = (g_1 * g_1', \ g_2 * g_2)$$

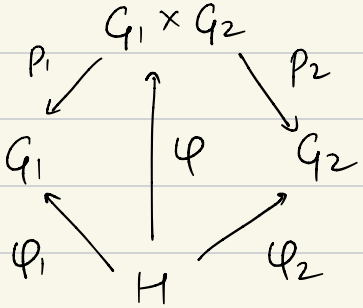
Id - (e_1, e_2)

Inv - $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$

Similarly one can define any finite/infinite product of gps.

- Universal ppt : For any gp. H & homomps.

$\varphi_1 : H \to G_1$, $\varphi_2 : H \to G_2$ $\Rightarrow \exists!$ (unique) $\varphi : H \to G_1 \times G_2$ s.t $p_1 \circ \varphi = \varphi_1$ & $p_2 \circ \varphi = \varphi_2$



$$\varphi(h) = (\varphi_1(h), \varphi_2(h))$$

$G_1 \times G_2$ is the only gp. (upto isomp.) that satisfies the ppt.

7. Boolean operation

For a set S, consider $\mathcal{P}(S)$.

Def. gp. op. on $\mathcal{P}(S)$ by

$$A_1 * A_2 = (A_1 - A_2) \cup (A_2 - A_1)$$

Id: $e = \emptyset$ Inv: $A^{-1} = A$

8. Permutation gp.

For a set S, def. $\text{Perm}(S)$ as the set of all bij $f: S \longleftrightarrow S$ wrt composition

Id: id map Inv: inv map

If S is finite, $|S| = n$, we denote $\text{Perm}(S)$ by S_n.

$|S_n| = n!$

Elem. of S_n are called permutations.
Perms which fix $(n-2)$ elems. & interchange the remaining 2 are called transpositions.

Every perm. is a product (comp.) of transp.
The parity of the no. of transp. is well-defined.

Notⁿ: $\sigma : S \to S$

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ \sigma(x_1) & \sigma(x_2) & \cdots & \sigma(x_n) \end{pmatrix}$$

Def. sign of perm $\operatorname{sgn}(\sigma)$ to be 1 if parity is even, -1 otherwise.

$$\begin{aligned} \operatorname{sgn}: S_n &\longrightarrow \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z} \\ \sigma &\longmapsto \operatorname{sgn}(\sigma) \end{aligned}$$

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$$

The kernel is denoted by A_n called alternating gp.

Fix a transpn, say $(1\ 2)$

$$\varphi : S_n \longrightarrow S_n$$
$$\sigma \longmapsto \sigma(1\ 2)$$

Parity of σ & $\sigma(12)$ is opp.

φ is a bij. $\Rightarrow$ There are equal no. of perms. with sgn $= 1$ & sgn $= -1$

So, $|A_n| = n!/2$

Cayley's Thm: Every gp. embeds inside a perm. gp.

Pf: For a gp. G, consider

$$\varphi : G \longrightarrow \mathrm{Perm}(G)$$
$$g \longmapsto l_g$$

where $l_g : G \longrightarrow G$
$$h \longmapsto gh$$

l_g is a bij. (with $l_g^{-1} = l_{g^{-1}}$)

$l_{gg'} = l_g l_{g'}$ ($\because gg'h = g(g'h)$)

$\Rightarrow \varphi$ is a homomp.

$\because \varphi$ is inj. $\begin{cases} l_g = l_{g'} \\ \Rightarrow l_g(e) = l_{g'}(e) \Rightarrow ge = g'e \\ \Rightarrow g = g' \end{cases}$

$\Rightarrow \varphi : G \hookrightarrow \mathrm{Perm}(G)$

Spl. Case: If $|G| = n$, $G \hookrightarrow S_n$

9. Matrix gps

$M_n(\mathbb{R})$: all $n \times n$ real matrices

$M_n(\mathbb{R}) \simeq \mathbb{R}^{n^2}$

$GL_n(\mathbb{R})$: invertible $n \times n$ matrices

$SL_n(\mathbb{R})$: inv. $n \times n$ mat. of det $= 1$

$O(n)$: orthogonal gp.

$\{ A \in M_n(\mathbb{R}) : AA^T = I \}$

In particular $O(n) \subset GL_n(\mathbb{R})$

$SO(n) = O(n) \cap SL_n(\mathbb{R})$

$SO(n) \subset SL_n(\mathbb{R}) \subset GL_n(\mathbb{R}) \subset M_n(\mathbb{R})$

$SO(n) \subset O(n)$

(subgp) (subgp) (not a subgp.)

$$\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$$
$$A \longmapsto \det(A)$$

$$\ker(\det) = SL_n(\mathbb{R})$$

Heisenberg gp : $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$, $a, b, c \in \mathbb{R}$

is a s.g. of $SL_3(\mathbb{R})$

$SL_n(\mathbb{Z}) \subset SL_n(\mathbb{R})$ is a 'discrete s.g.'

All these matrix gps. are examples of 'Lie Groups'

10. Isometries of $\mathbb{R}^n$

A mapping $T: \mathbb{R}^n \to \mathbb{R}^n$ is called an isometry if

$$d(x, y) = d(Tx, Ty)$$

↑ euclidean metric

- Any isometry is inj.

Thm: Any isometry of $\mathbb{R}^n$, is an orthogonal transformation followed by a translation.

In particular if isometry fixes the origin, it is given by an ortho. transf^n.

Pf: $\langle u, v\rangle = \frac{1}{2}\left[\langle u, u\rangle + \langle v, v\rangle + \langle u-v, u-v\rangle\right]$

$$\langle Tu, Tv\rangle = \frac{1}{2}\left[\langle Tu, Tu\rangle + \langle Tv, Tv\rangle + \langle T(u-v), T(u-v)\rangle\right]$$

$\because\ d(x, x) = d(Tx, Tx)$

$\Rightarrow\quad \langle x, x\rangle = \langle Tx, Tx\rangle$

$\Rightarrow\quad \langle u, v\rangle = \langle Tu, Tv\rangle \rightarrow T$ is orthogonal

11. Quaternion gp

Consider symbols $\pm i, \pm j, \pm k$.
Then $\{\pm i, \pm j, \pm k\}$ forms a gp under

$1 \cdot i = i \;,\; 1 \cdot j = j \;,\; 1 \cdot k = k$
$i^2 = j^2 = k^2 = ijk = -1$

12. Quaternions

$$H = \mathbb{R} \oplus \mathbb{R}_i \oplus \mathbb{R}_j \oplus \mathbb{R}_k$$

Extend the gp. op. in 11. using $\mathbb{R}$-linearity.

$$(a+bi+cj+dk)(a-bi-cj-dk) = a^2+b^2+c^2+d^2$$

$$\Rightarrow (a+bi+cj+dk)^{-1} = \frac{(a-bi-cj-dk)}{a^2+b^2+c^2+d^2} \;;\; a,b,c,d \in \mathbb{R}$$

Representation: A real/complex rep. of gp. G is a homomorphism

$$\rho : G \to GL(V)$$ for some real/complex vector space V

13. G, G' : abelian gps.

$\mathrm{Hom}(G, G')$: set of all gp. homomps. $G \to G'$

is a gp. under $(f+g)(x) = f(x) + g(x)$

Nt : Op. on abelian gps. is denoted by $+$ rather than $*$

eg - $\mathrm{Hom}(\mathbb{Z}, G) \simeq G$

$\varphi \mapsto \varphi(1)$

$\varphi : \mathbb{Z} \to G$

$1 \mapsto \varphi(1)$

$n \mapsto \varphi(1)^n$

$\therefore$ 1 generates $\mathbb{Z}$

$\therefore$ $\varphi(1)$ uniquely determines φ

$$\mathrm{Hom}(\mathbb{Z}/d_1, \mathbb{Z}/d_2) \simeq \{0\}, \quad (d_1, d_2) = 1$$

$$\bar{1} \mapsto \varphi(\bar{1})$$

$$\bar{0} = \bar{d}_1 \mapsto \varphi(\bar{1})^{d_1} = \bar{0}$$

$md_1 + nd_2 = 1 \Rightarrow \varphi(\bar{1})^{md_1 + nd_2} = \varphi(\bar{1})$

$\Rightarrow (\varphi(\bar{1})^{d_1})^m (\varphi(\bar{1})^{d_2})^n = \varphi(\bar{1})$

$\Rightarrow \varphi(\bar{1}) = \bar{0}$ $\quad [\because \varphi(\bar{1})^{d_2} = \bar{0}]$

$\Rightarrow \varphi$ maps all elems. to $\bar{0}$

14. Free Groups

For a set S, def. free gp. on S as follows

An elem. of the form

$$w = x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} \cdots x_{i_r}^{\epsilon_r} \quad \text{where } x_{i_j} \in S, \ \epsilon_i = \pm 1$$

called 'word' of length 'r'.

Def: eq. rel^n : $w \sim w'$ if w' can be obtained from w by deleting or inserting words of the form xx^{-1} for any $x \in S$

eg - $S = \{x_1, x_2, x_3\}$

$w = x_1^{-1} x_2 x_1 x_3$

$w' = x_1^{-1} x_2 x_1 x_2 x_2^{-1} x_3$

, $w \sim w'$

A word is said to be reduced if it cannot be shortened i.e it has smallest length in its eq. class.

The eq. classes of words together with elem e (identity of zero length) form a group under concatenation.

$w = x_1 x_3^{-1}$

$w' = x_3 x_2$

$ww' = [x_1 x_2^{-1} x_2 x_3]$

$= [x_1 x_3]$ ← eq. class.

Op: Concatenation

Inv: $w = [x_{i_1}^{\epsilon_1} x_{i_2}^{\epsilon_2} \dots x_{i_1}^{\epsilon_1}]$

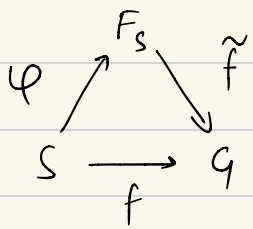
$w' = [x_{i_1}^{-\epsilon_1} \dots x_{i_2}^{-\epsilon_2} x_{i_1}^{-\epsilon_1}]$

Notⁿ : F_S

There is a natural inj. map

$$\varphi : S \hookrightarrow F_S$$
$$x_i \mapsto [x_i]$$

F_S has an inj. universal ppt.
Given any gp. G & a set map $f : S \to G$,
$\exists!\ \tilde{f} : F_S \to G$ s.t the diagram commutes



Generator : For a subset T of a gp. G, we say T generates G if every elem. in G equals a word in elems. of T.

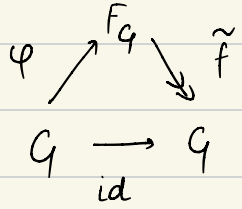
The word $x_{i_1}^{\epsilon_1} \dots x_{i_r}^{\epsilon_r}$ is identified with
$x_{i_1}^{\epsilon_1} * x_{i_2}^{\epsilon_2} \dots * x_{i_r}^{\epsilon_r} \in G$

eg - i. $G = \mathbb{Z}$, $T = \{1\}$

ii $G = \mathbb{Z} \oplus \mathbb{Z}$, $T = \{(1,0), (0,1)\}$

iii $G = S_n$, $T =$ set of transpositions

By universal ppt., for $S = G$



$\varphi \circ \tilde{f} = id$

$\because$ id is surj.

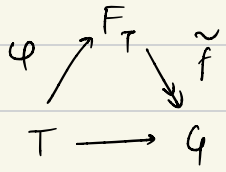
$\therefore$ $\tilde{f}$ is surj.

Hence, free gp. surjects onto every gp.

Notⁿ: Free gp. on n-elems. is denoted by F_n.

eg - $\mathbb{Z} \simeq F_1 = \{\ldots, x^{-1}, e, x^1, \ldots\}$

Now, if T generates G



$\tilde{f}$ is surj as its image contains set of generators of G

Properties of free gps

1. $F_S \simeq F_{S'}$ iff $|S| = |S'|$

2. Any subgp of a free gp. is free.

3. S: coun. inf set
   F_S is denoted by F_∞

   F_∞ embeds in F_2

$$F_\infty = \langle x_1, x_2, \dots \rangle$$
$$F_2 = \langle a, b \rangle$$

$$\varphi : F_\infty \hookrightarrow F_2$$
$$x_k \longmapsto b^k a b^{-k}$$

Let $x_{i_1}^{\epsilon_1} \dots x_{i_l}^{\epsilon_l}$ be a reduced word mapped to e

$$\varphi(x_{i_1}^{\epsilon_1} \cdots x_{i_r}^{\epsilon_r}) = (b^{i_1} a^{\epsilon_1} b^{-i_1}) \cdots (b^{i_r} a^{\epsilon_r} b^{-i_r})$$

Since word is reduced,
either $x_{i_l} \neq x_{i_{l+1}}$ or if $x_{i_l} = x_{i_{l+1}}$ but $\epsilon_l + \epsilon_{l+1} \neq 0$

So, the segment $(b^{-i_l} a^{\epsilon_l} b^{i_l})(b^{-i_{l+1}} a^{\epsilon_{l+1}} b^{i_{l+1}})$ can be reduced i.e it defines a non-trivial element in the word $\varphi(x_{i_1}^{\epsilon_1} \cdots x_{i_r}^{\epsilon_r})$

From this, we conclude $x_{i_1}^{\epsilon_1} \cdots x_{i_r}^{\epsilon_r} \neq e$
and the map is injective

Homomp. eg :

1. abelian G, $\quad G \to G$, $\quad x \mapsto x^n$

2. Conjugation : For $g \in G$, $\quad G \to G$, $\quad h \mapsto ghg^{-1}$

This defines an eq. rel^n on G & eq. classes are called conjugacy classes

3. $G \xrightarrow{\sim} \mathbb{R}$

$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \longmapsto a$

$a \in \mathbb{R}$

4. set S, gp G

for $s \in S$, $\quad ev_s : Mor(S, S) \to G$

evaluation map ↑ $\quad f \longmapsto f(s)$

5. For $a \in \mathbb{R}$

$$(\mathcal{C}(\mathbb{R}), +) \longrightarrow \mathbb{R}$$

$$f \longmapsto f(a)$$

f: cont. fun on $\mathbb{R}$

6. $\det : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$

Let $H, K < G$

$$HK := \{ hk : h \in H, k \in K \}$$

Lem: HK is a subgp. of G iff $HK = KH$

Pf: ($\Rightarrow$) For $h \in H$, $k \in K$, $hk \in HK$

$\because HK < G \Rightarrow (hk)^{-1} \in HK$

$\Rightarrow k^{-1}h^{-1} \in HK$

But, $k^{-1}h^{-1} \in KH \Rightarrow (hk)^{-1} \in KH \Rightarrow hk \in KH$

So $HK \subset KH$

By symmetry of the argument, $KH \subset HK$

$\Rightarrow HK = KH$

($\Leftarrow$) If $HK = KH$,

$$\begin{aligned}(h_1k_1)(h_2k_2) &= (h_1h_3)(k_3k_2) \\ &= hk \in HK\end{aligned} \qquad \left\{\begin{array}{l}\because k_1h_2 \in KH = HK \\ \Rightarrow k_1h_2 = h_3k_3\end{array}\right.$$

$$(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$$

Hence HK is a subgp.

Internal product: If $HK = G$ & $H \cap K = \{e\}$

$$\begin{aligned} H \times K &\xrightarrow{\sim} G \\ (h, k) &\longmapsto hk \end{aligned}$$

Coset: $H < G$.

left (or right) coset of H in G is the subset of the form gH (or Hg) for some $g \in G$

- Left and right cosets are either identical or disjoint, have the same cardinality & their union is G.

Pf: 1. If $aH \cap bH \neq \emptyset$

Consider $\exists\ h_1, h_2$ s.t $ah_1 = bh_2$

$$\Rightarrow a = bh_2h_1^{-1}$$

$$\Rightarrow aH = bh_2h_1^{-1}H = bH$$

2. Fix $g \in G$. $g \in gH$

Hence union of cosets is G.

Lagrange's Thm: For a finite gp. G, $H < G$,

$|H|$ divides $|G|$.

Pf: $G = \bigcup_{g \in G} gH$

bij: $H \longleftrightarrow gH$
$h \longmapsto gh$

$\Rightarrow |H| = |gH|$ $\Rightarrow |G| = \left(\begin{matrix}\text{no. of} \\ \text{distinct} \\ \text{cosets}\end{matrix}\right) |H|$

$\Rightarrow |H|$ divides $|G|$

There is a bij. b/w set of left & right cosets. Its cardinality is called the index of H in G

$$gH \longmapsto Hg^{-1}$$

Note $(gh)H = gH$

$$gH = (gh)H \longmapsto H(gh)^{-1}$$
$$= Hh^{-1}g$$
$$= Hg$$

This shows the map is well-defined.

$$|G| = |H| \text{ (index of } H \text{ in } G)$$
$$= |H|\,(G:H)$$

Remark: $gH \longmapsto Hg$ is not well defined as $gH = (gh)H \longmapsto H(gh) \neq Hg$

Ex: $|HK| = \dfrac{|H||K|}{|H \cap K|}$

Pf: Consider $f : H \times K \to HK$

$(h,k) \mapsto hk$

This map is surj. & fibers $f^{-1}(y)$ partition $H \times K$ into $|HK|$ disjoint sets.

Fix $y \in HK$. Every elem. in $H \times K$ can be written as (hu, vk) for some $u \in H$, $v \in K$.

$$f(hu, vk) = hk \iff huvk = hk \implies uv = 1$$

$$\implies u = v^{-1}$$

$$\implies f^{-1}(y) = \{(hu, u^{-1}k) : u \in H \cap K\}$$

So, $|f^{-1}(y)| = |H \cap K|$

Hence, $\underbrace{|H \times K|}_{|H||K|} = |HK|\,|f^{-1}(y)|$

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

Application

Group of prime order is (finite) cyclic

Pf: For gp. G, let $|G| = p$ (prime)

Consider $g \in G$, $g \neq e$.

$\langle g \rangle < G \Rightarrow |\langle g \rangle|$ divides $|G|$

$\Rightarrow |\langle g \rangle| = 1, p$

$\langle g \rangle \neq 1$ since $g \neq e$

$\Rightarrow |\langle g \rangle| = p \Rightarrow \langle g \rangle = G$

For $n \in \mathbb{N}$, $\varphi(n)$ = no. of natural nos. $\leq n$ which are coprime to n.

Euler's Thm: If $(a, n) = 1$,

$$a^{\varphi(n)} \equiv 1 \mod n$$

Pf: For $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, consider $H = \langle \bar{a} \rangle$

$|H|$ = smallest ℓ s.t $\bar{a}^{\ell} = e$ ($\ell = O(\bar{a})$ order of $\bar{a}$)

By LT, $|H|$ divides $|\mathbb{Z}/n\mathbb{Z}^*|$

$= \varphi(n)$

$\Rightarrow \ell \mid \varphi(n)$

$\Rightarrow \bar{a}^{\varphi(n)} = e$

$\Rightarrow a^{\varphi(n)} \equiv 1 \mod n$

- Special case: (Fermat's little Thm)
If p is prime, $\varphi(p) = p - 1$

$\Rightarrow a^{p-1} \equiv 1 \mod p$

Normal subgp: For $H < G$, the following are equivalent.

1. $gHg^{-1} \subset H \quad \forall\, g \in G$
2. $gHg^{-1} = H \quad \forall\, g \in G$
3. $gH = Hg \quad \forall\, g \in G$

H is normal if it satisfies any of these.

Pf: $1 \Rightarrow 2$. For $h \in H$, $g^{-1}hg \in H$ (by 1.)

$$\Rightarrow \underbrace{g(g^{-1}hg)g^{-1}}_{h} \in gHg^{-1}$$

$$\Rightarrow H \subset gHg^{-1}$$

$$\Rightarrow H = gHg^{-1}$$

$2 \Rightarrow 3$. Trivial $\quad gh_1g^{-1} = h_2 \Rightarrow gh_1 = h_2g$

$3 \Rightarrow 1$. For $h_1, h_2 \in H$, $\quad gh_1 = h_2g$

$$\Rightarrow gh_1g^{-1} = h_2 \in H$$

$$\Rightarrow gHg^{-1} \subset H$$

eg -

1. G: abelian gp. H: any subgp. } H is normal in G.

2. $\varphi : G \to G'$ be a homomp.

$K = \ker(\varphi)$ is normal in G.

$\because$ for $k \in K$, $g \in G$,

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1}$$
$$= e$$

$$\Rightarrow gkg^{-1} \in K \Rightarrow gKg^{-1} \subset K$$

$$k = g(g^{-1}kg)g^{-1} = gk'g^{-1} \in gKg^{-1} \Rightarrow K \subset gKg^{-1}$$

$$\Rightarrow gKg^{-1} = K$$

3. Index 2 subgps. are normal.

Let $H < G$ be an index 2 subgp.

For $a \in G$, s.t $a \notin H$, aH & Ha are the only other left & right cosets.

$$G = H \amalg aH = H \amalg Ha \Rightarrow aH = Ha$$

eg – 3.1 $A_n < S_n$

3.2 $SO(n) < O(n)$

4. For a gp. G, let $Aut(G)$ denote the automp. gp. of G.

$$c : G \to Aut(G)$$
$$g \mapsto c_g$$

$$c_g : G \leftrightarrow G$$
$$h \mapsto ghg^{-1}$$

{ conjugation by g

Claim: c is a homomp.

- c_g is automp.

$$G \xrightarrow{c_g} G \xrightarrow{c_{g^{-1}}} G$$
$$h \longmapsto ghg^{-1} \longmapsto g^{-1}(ghg^{-1})g = h$$

$\therefore$ $c_{g^{-1}}$ is inv. of c_g

Hence, c_g is automp.

- $c_{g'g} = c_{g'} c_g$

$$G \xrightarrow{c_g} G \xrightarrow{c_{g'}} G$$
$$h \longmapsto ghg^{-1} \longmapsto g'(ghg^{-1})g'^{-1}$$
$$= (g'g)\,h\,(g'g)^{-1}$$

$$G \xrightarrow{c_{g'g}} G$$
$$h \longmapsto (g'g)\,h\,(g'g)^{-1}$$

Hence c is a homomp.

The image of c is a normal subgp.

Consider $\varphi \in \mathrm{Aut}(G)$

$$\begin{aligned}
\varphi c_g \varphi^{-1}(h) &= \varphi\left(g \varphi^{-1}(h) g^{-1}\right) \\
&= \varphi(g)\, \varphi(\varphi^{-1}(h))\, \varphi(g^{-1}) \\
&= \varphi(g)\, h\, \varphi(g^{-1}) \\
&= \varphi(g)\, h\, \varphi(g)^{-1} \\
&= c_{\varphi(g)}(h)
\end{aligned}$$

The image of c are called the inner automp. of G.

5. For a gp. G, define center of G to be

$$Z(G) = \{ g \in G : hg = gh \ \forall \ h \in G \}$$

$Z(G)$ is a normal subgp. of G.

Let $g \in Z(G)$, $h \in G$.

$$\begin{aligned} hgh^{-1} &= hh^{-1}g && [\because gh^{-1} = hg^{-1}] \\ &= g && [\because gh = hg] \\ &\in G \end{aligned}$$

Note, $Z(G) = \ker(C)$ from the above example.

Rem: Arbitrary intersection of normal subgroups is normal

Quotient gp.

For a normal subgp. $H \subset G$, let G/H be the set of left cosets of H in G.

Def a gp. structure on G/H as

$$(g_1H) * (g_2H) := g_1g_2H$$

Suppose $aH = a'H$ & $bH = b'H$.

$\Rightarrow a' = ah_1$, $b' = bh_2$

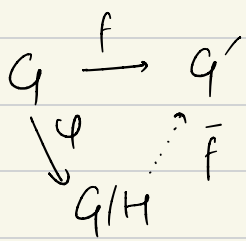
$$\begin{aligned}(a'H) * (b'H) &= a'b'H \\ &= ah_1bh_2H \\ &= ab\underbrace{(b^{-1}h_1b)}_{h_3}h_2H = abh_3h_2H \\ &= abH\end{aligned}$$

Hence the map is well-defined.

Canonical homomp. $\varphi : G \to G/H$

$g \mapsto gH$

φ has the ppt. that given any homomp. $f : G \to G'$ s.t H is a normal subgp. of G with $H \subset \ker(f)$, f factors uniquely through a homomp. $\bar{f} : G/H \to G'$ i.e the diagram commutes



$\bar{f}(gH) = f(g)$

Suppose $aH = a'H \Rightarrow a' = ah$

$\bar{f}(a'H) = f(a') = f(ah) = f(a)f(h)$

$= f(a) = \bar{f}(aH)$ $\quad [\because h \in H \subset \ker(f)]$

Commutator subgp.

Let subgp. $H \subset G$ be generated by finite products of the kind $aba^{-1}b^{-1}$, $a, b \in G$

This is called the commutator subgp. and is denoted by $[G, G]$

$[G, G]$ is a normal subgp.

Let $g \in G$, $c \in [G, G]$

By def^n $gcg^{-1}c^{-1} \in [G, G]$. But $c^{-1} \in [G, G]$

$\Rightarrow gcg^{-1} \in [G, G]$

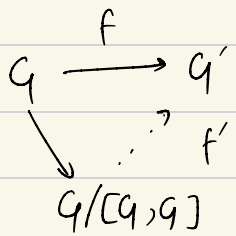
Hence, $[G, G]$ is normal.

$G/[G, G]$ is abelian

$\because \bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1} = \bar{e} \Rightarrow \bar{x}\bar{y} = \bar{y}\bar{x}$

$(\because \bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1} \in [G, G])$

Infact, given any abelian gp. G' and a homomp $f: G \to G'$, $\exists!$ homomp. $f': G/[G,G] \to G'$ s.t diagram commutes

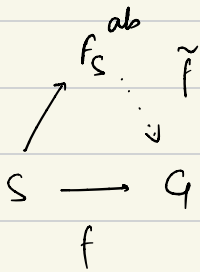


$$f'(a[G,G]) = f(a)$$

For a set S, consider F_S (free group on S)

Let F_S^{ab} denote $F_S/[F_S, F_S]$
(free abelian group on S)

It has the universal ppt., given a gp G & a set map $f: S \to G$, $\exists!$ homomp $\tilde{f}: F_S^{ab} \to G$ s.t the diagram commutes



Suppose, S is a finite set with n-elements.
Then $F_S^{ab} \simeq \mathbb{Z}^n$

Isomorphism Thms

First isomp. thm

Let $f: G \to G'$ be a surjective homomp.
Let K be $\ker(f)$. Then $G/K \simeq G'$

Pf: Define $f': G/K \to G'$ as

$$f'(aK) = f(a)$$

Well defined: $aK = a'K \Rightarrow a' = ak$, $k \in K$

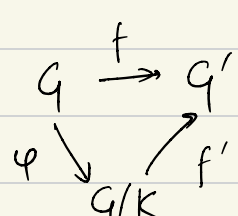
$$\Rightarrow f'(a'K) = f(a') = f(ak) = f(a) = f'(aK)$$

Inj: $f'(aK) = e \Rightarrow f(a) = e \Rightarrow a \in K$

$$\Rightarrow aK = K$$

Surj: follows from surj of f.

$\left(\because f = \varphi \circ f' \Rightarrow f' \text{ is surj} \right)$



Prop: For homomp. $f: G \to G'$

1. If $H < G$, then $f(H) < G'$

2. If H is normal in G & f is onto, then $f(H)$ is normal in G'

3. If $H' < G'$, then $f^{-1}(H') < G$

4. If H' is normal in G', then $f^{-1}(H')$ is normal in G.

5. In addn if f is onto, $G/f^{-1}(H') \simeq G'/H'$

Pf: 2. Consider $g' \in G'$. So, $g' = f(g)$ for some $g \in G$ ($\because f$ is onto)

$$g' f(H) g'^{-1} = f(g) f(H) f(g^{-1})$$
$$= f(gHg^{-1}) = f(H)$$

4. $G \xrightarrow{f} G' \xrightarrow{\varphi} G'/H'$

$f^{-1}(H')$ is inv. of H' in G'

$\Rightarrow$ $f^{-1}(H')$ is inv. of e in G'/H'

i.e kernel of $\varphi \circ f$

Hence $f^{-1}(H')$ is normal.

5. Let $H = f^{-1}(H')$

Def. $G/H \xrightarrow{\tilde{f}} G'/H'$ as

$$\tilde{f}(aH) = f(a)H'$$

Well defined :

Inj : $f(a)H' = eH' \Rightarrow f(a) \in H'$

$\Rightarrow a \in H$

$\Rightarrow aH = H$

Surj :

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow & \tilde{} & \downarrow \\ G/H & \xrightarrow{\tilde{f}} & G'/H' \end{array}$$

Second isomp. thm

For normal subgps. $H, K < G$ s.t $K < H$, then H/K is normal in G/K &

$$(G/K)/(H/K) \simeq G/H$$

Pf: $G \twoheadrightarrow G/K$

$\because$ normal $H < G$

$\therefore$ By prev. PP^{n}, image of H is a normal subgp. & equals H/K

By 1st isomp. thm., $G/H \simeq (G/K)/(H/K)$

Third isomp thm

Let $H, K < G$, s.t normal $K < G$,
then $K \cap H$ is normal in H &

$$H/H\cap K \simeq HK/K$$

Pf: $\because$ normal $K < G$, $HK = KH$
& hence $HK < G$
Also, normal $K < HK$. So HK/K is well-defined

$\because$ normal $K < G$, $H \cap K$ is normal in H
(by prev. ppn under the inclusion map)

Def: $f: H/H\cap K \longrightarrow HK/K$

$$g\,H\cap K \longmapsto gK$$

Elements of finite order are called torsion elements.

If G is abelian, this is a subgp. of G and is denoted by G_{tor}.

G is called torsion-free if there is no non-identity elem. of finite order.

eg - $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

If every elem. of G has finite order, we say G is a torsion gp.

eg - 1. Finite gps.
2. $\mathbb{Q}/\mathbb{Z}$

Rem: $\mathrm{Hom}(G, G') = e$

torsion gp. ↑ ↑ torsion-free

$\because$ If $g \in G$ s.t $O(g) = n \Rightarrow \varphi : G \to G'$

$O(\varphi(g)) \mid n$

Normalizer: For $H<G$, def. normalizer of H in G as

$$N_G(H) = \{ g \in G : gHg^{-1} = H \}$$

Centralizer: For $x \in G$, def. centralizer of x in G as

$$C_G(x) = \{ g \in G : gx = xg \}$$

Group Action

Let gp. G & set S.

Left action of G on S, refers to a map $\alpha : G \times S \to S$ satisfying

1. $\alpha(e, s) = s \quad \forall\, s \in S$
2. $\alpha(g, \alpha(h, s)) = \alpha(gh, s) \quad \forall\, g, h \in G$ & $s \in S$

Fix $g \in G$. Consider $\alpha_g : S \to S$

$$s \longmapsto \alpha(g, s)$$

α_g is a bij.

(inj.)

$\because$ if $\alpha(g, s) = \alpha(g, s')$

$\Rightarrow \alpha(g^{-1}, \alpha(g, s)) = \alpha(g^{-1}, \alpha(g, s'))$

$\Rightarrow \alpha(gg^{-1}, s) = \alpha(gg^{-1}, s')$

$\Rightarrow \alpha(e, s) = \alpha(e, s') \Rightarrow s = s'$

(sur.)

Fix $s \in S$. $\because$ $\alpha(g^{-1}, s) \in S$ s.t

$$\alpha(g, \alpha(g^{-1}, s)) = \alpha(gg^{-1}, s) = \alpha(e, s)$$
$$= s$$

$\Rightarrow s \in \text{Img}(\alpha_g)$

Not^{n}: From now, $\alpha(g, s)$ will be denoted gs.

Each α_g acts as a permutation of S.

Thus we get a map.

$$\varphi_\alpha : G \longrightarrow \mathrm{Perm}(S)$$
$$g \longmapsto \alpha_g$$

φ_α is a gp. homomp.
(by 2nd ppt. of gp. action)

Conversely, given a homomp. $\varphi : G \to \mathrm{Perm}(S)$, we get a left action by G on S by

$$\alpha : G \times S \longrightarrow S$$

$$\alpha(g, s) = \varphi(g)(s)$$

↑ img. of s under $\varphi(g)$

eg: 1. Trivial action

$$\alpha : G \times S \to S$$

$$\alpha(g, s) = s$$

2. $G = S_n$

$S = \{1, 2, \ldots, n\}$

$$\alpha(\sigma, i) = \sigma(i)$$

This induces an action of G on $\mathbb{R}[x_1, \ldots, x_n]$

$$\sigma(f(x_1, \ldots, x_n)) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$

Consider $P_1 = \sum_{i=1}^{n} x_i$, $P_2 = \sum_{i<j} x_i x_j$, $P_3 = \sum_{i<j<k} x_i x_j x_k$

$\ldots$ $P_n = x_1 \cdots x_n$

These polynomials are invariant under the action of S_n.

Thm: Any polynomial in $x_1, \dots, x_n$ which is invariant under action of S_n is a polynomial in $P_1, \dots, P_n$.

3. $G = GL_n(\mathbb{R})$ $\quad \alpha(g, v) = gv$
$S = \mathbb{R}^n$

4. $G =$ isometries of $\mathbb{R}^n$
$S = \mathbb{R}^n$

5. $S = G$
G acts on itself by left translation
$\alpha(g, h) = gh$

6. $S = G$
G acts on itself by conjugation
$\alpha(g, h) = ghg^{-1}$

7. Let G be a group acting on set S.
Then G acts on set of all maps $S \to S'$ for any set S'

$$\alpha(g, f(s)) = f(\alpha(g^{-1}, s))$$

or

$$gf(s) = f(g^{-1}s)$$

Rem: homomp. $\varphi : G \to G'$, $\alpha' : G' \times S \to S$

If G' acts on S, we get an induced action of G on S

$$\alpha(g, s) = \alpha'(\varphi(g), s)$$

Stabilizer: Let G act on S.

Def. The stabilizer at a pt. $s \in S$ to be

$$G_s = \{ g \in G : gs = s \}$$

Orbit: Let G act on S. (denoted by $S^{/G}$)

Fix $s \in S$. We get an induced map.

$$\varphi : G \to S$$
$$g \mapsto gs$$

This is called the orbit map. The image of φ is called the orbit of s & is denoted by $\alpha(G, s)$ or Gs or $Orb(s)$

Rem: $G_{gs} = g G_s g^{-1}$

The orbit map $\varphi_s : G \longrightarrow S$ descends to

$$g \longmapsto gs$$

a bij. $\tilde{\varphi}_s : G/G_s \longleftrightarrow Gs$

$$gG_s \longmapsto gs$$

(inj.) $\tilde{\varphi}_s(\bar{g}_1) = \tilde{\varphi}_2(\bar{g}_2) \Rightarrow g_1 s = g_2 s$

$\Rightarrow g_1^{-1} g_2 s = s$

$\Rightarrow g_1^{-1} g_2 \in G_s$

$\Rightarrow \bar{g}_1 = \bar{g}_2$

(surj.) Follows from Gs being image of φ_s

Transitive : A gp. action is said to be transitive if given $s_1, s_2 \in S$, $\exists\ g \in G$ s.t $gs_1 = s_2$

OR there is exactly one orbit for G-action

Faithful : A gp. action is said to be faithful if given $g \in G$, $(g \neq e)$ $\exists\ s \in S$ s.t $gs \neq s$

OR

The kernel of the associated mapping $\varphi : G \to \text{Perm}(S)$ is trivial

Free : The action is said to be free if $gs = s$ for some elem. $\Rightarrow g = e$

OR

$G_s = e \quad \forall\ s \in S$

Note : A faithful action moves at least one elem. of S for every elem. of G.

A free action moves all elems. of S.

So, free $\Rightarrow$ faithful

In prev. eg.)

1. Trivial action – Not faithful.
   Not transitive

2. Action of S_n – faithful but <u>not</u> free
   Transitive

3. Action of GL_n – faithful but <u>not</u> free
   Not transitive

4. Isometries of $\mathbb{R}^n$ – faithful but <u>not</u> free
   Transitive

5. $G \overset{G}{\curvearrowright}$ by translations – Free
   Transitive

6. $G \overset{G}{\curvearrowright}$ by conjugation – Not faithful in general
   Not transitive

   ∵ conj. by center fixes all elem. of group
   ∵ can never conj. by any elem. to obtain e.

Rem: S^G $\quad s_1, s_2 \in S$

If $\quad Orb(s_1) \cap Orb(s_2) \neq \emptyset \Rightarrow Orb(s_1) = Orb(s_2)$

$\because \quad g_1 s_1 = g_2 s_2 \Rightarrow s_1 = g_1^{-1} g_2 s_2 \Rightarrow hs_1 = (hg_1^{-1}g_2)s_2$

$\Rightarrow Orb(s_1) \subseteq Orb(s_2)$

Sim., $\quad hs_2 = (hg_2^{-1}g_1)s_1 \Rightarrow Orb(s_2) \subseteq Orb(s_1)$

Hence, $\quad Orb(s_1) = Orb(s_2)$

So, $\quad S = \coprod_{s_i: \text{ representatives of orbits}} Orb(s_i)$

which is in bij with $\coprod G/G_{s_i}$

$\Rightarrow \quad |S| = \sum_{s_i} |Orb(s_i)|$

$= \sum_{s_i} [G : G_{s_i}]$

Consider $G \curvearrowright^{G}$ by conj.

For $h \in G$, $\quad G_h = \{ g \in G : ghg^{-1} = h \} = C_G(h)$

For finite gp. G, # conjugates of $h \in G$ = index of centralizer

(# elems. in orbit of h) (# elems. in $G/C_G(h)$)

Sim. if for subgp. $H < G$, if G acts on S: conjugates of H by conj.

conjugates of H in G = index of the normalizer of H in G

(# elems. in orbit of H i.e entire S) (# elems. in $G/N_G(H)$)

Let finite gp. G & $G \curvearrowright^{g} G$ by conj.

$$G = Z(G) \amalg c(g_i) \longrightarrow \text{conj. class. of } g_i$$

g_i : representatives of conjugacy classes not in centre

$\therefore$ conj. class of elem. of $Z(G)$ is itself.

$$\Rightarrow |G| = |Z(G)| + \sum_{i=1}^{n} |C(g_i)|$$

$$= |Z(G)| + \sum_{i=1}^{n} [G : C_G(g_i)]$$

This is called Class Equation

Lem: (p groups)
Let gp. G with $|G| = p^e$ for a prime p.
Then $Z(G) \neq e$

Pf: $$\underbrace{|G|}_{\text{div. by } p} = |Z(G)| + \underbrace{\sum_{i=1}^{r} [G : C_G(g_i)]}_{\text{div. by } p}$$

$\Rightarrow$ $|Z(G)|$ is div. by p
$\Rightarrow$ $Z(G)$ has at least p elems.

Lem: Any group of order p^2 is abelian (for prime p).

Pf: Suppose G is not-abelian.
$\Rightarrow$ $Z(G)$ is proper s.g. of G.

By prev. lem., $|Z(G)| > 1 \Rightarrow |Z(G)| = p$

Let $g \in G$ s.t $g \notin Z(G)$. Consider $C_G(g)$.

In general $Z(G) \subseteq C_G(g)$

But, $g \in C_G(g)$ & $g \notin Z(G) \Rightarrow Z(G) \subsetneq C_G(g)$

$\Rightarrow |C_G(g)| = p^2 \quad (\because |C_G(g)| > |Z(G)|)$

$\Rightarrow C_G(g) = G$

$\Rightarrow g \in Z(G) \rightarrow$ Contd^n

Hence, G is abelian

Rem: If $|G| = p^3$, $|Z(G)| \neq e$

If $Z(G) \neq G$ & $Z(G) = p^2 \Rightarrow G/Z(G)$ is cyclic (order p)
& G is abelian
$\rightarrow$ Contd^n

Hence, $|Z(G)| = p^3, p$

Lem: Let G be a finite gp. & let p be a prime dividing $|G|$. Then G has an elem. of order p.

Pf: Ind^n on G

Case 1: G is abelian.
Suppose $\exists\ H<G$ s.t $p \mid |H|$, then we're done.
Suppose **not**, consider a proper subgp. $H<G$

$$G \longrightarrow G/H$$

$\because\ p \mid |G/H| \Rightarrow$ by ind^n, G/H has an elem. of order p say $\bar{x}$

$\Rightarrow\ x^p \in H \quad (\because \bar{x}^p = e \text{ in } G/H)$

Let $|H| = l$ with $(l, p) = 1$

$\Rightarrow\ x^{pl} = e$

Claim : $x^l \neq e$

Suppose $x^l = e \Rightarrow \bar{x}^l = e$ in G/H

But $\bar{x}^p = e$ & $(p, l) = 1 \Rightarrow \exists\, a, b$ s.t $ap + bl = 1$

$\Rightarrow \bar{x}^{ap+bl} = \bar{x}^1 \Rightarrow \bar{x} = e \rightarrow$ Contd^n $\because O(\bar{x}) = p$

Thus, x^l has order p as desired.

Case 2 : General G

By ind^n we are reduced to the case where every proper subgp. has order coprime to p.

$$|G| = |Z(G)| + \sum [G : C_G(g_i)]$$

$|G|$: divisible by p

$\sum [G : C_G(g_i)]$: divisible by p $\left(\because p \nmid C_G(g_i) \;\&\; p \mid G \Rightarrow p \mid [G : C_G(g_i)]\right)$

$\Rightarrow p \mid |Z(G)| \rightarrow$ Contd^n

p-Sylow gp:

Let G be a gp & p be a prime.
Let $|G| = p^n \cdot m$ with $(p, m) = 1$

A subgp $H < G$ of order p^l for some $l \in \mathbb{N}$ is called a p-gp. If $l = n$, we say H is a p-Sylow gp.

Thm: For finite gp G & a prime p dividing $|G|$. Then G has a p-Sylow subgp.

Pf: Let $|G| = p^n \cdot m$, $(p, m) = 1$

By ind^n, if G has a proper subgp div. by p^n, we are done.

Assume that for every proper subgp. $H < G$, $p^n \nmid |H|$.
$\Rightarrow$ p divides index of every proper subgp.

By Class Eq^n, $|G| = |Z(G)| + \sum [G : C_G(g_i)]$

($|G|$: div. by p; $\sum [G : C_G(g_i)]$: div. by p)

$\Rightarrow p \mid |Z(G)|$

By prev. lem., $Z(G)$ has a subgp. H of order p & $H \lhd G$ (H is normal $\because$ every subgp. of $Z(G)$ is normal)

$$G \xrightarrow{\varphi} G/H \text{ - order } p^{n-1} \cdot m$$

$\cup$

P' (p-Sylow subgp.)

$|P'| = p^{n-1}$

Let $P = \varphi^{-1}(P')$

Then $P/H \simeq P'$ (by 1st isomp. thm)

$\Rightarrow |P| = p^n$

Hence, P is the p-Sylow subgp. of G.

Fixed pt: Let G act on set S. A fixed pt. for the action is an element $s \in S$ s.t

$gs = s \quad \forall\, g \in G$

Lem: Let H be a p-gp acting on finite set S.

1. $\#$ fixed pts. of $S \equiv \#S \pmod p$

2. If the action has only 1 fixed pt.,
   $\#S \equiv 1 \pmod p$

3. If p divides $\#S$
   $\#$ fixed pts. $\equiv 0 \pmod p$

Pf: $S = \coprod \mathrm{Orb}(s_i)$

$\#\,\mathrm{Orb}(s_i) = [G : G_{s_i}]$

for a fixed pt., $\mathrm{Orb}(s_i) = \{s_i\}$

$\Rightarrow$ S = fixed pts $\amalg$ Orbits with ≥ 2 elem.

div. by p ($\because$ each $G_{s_i} < G$ (p-gp) $\Rightarrow p \mid [G : G_{s_i}]$)

$\Rightarrow$ $\#S \equiv \#$ fixed pts. $(\text{mod } p)$

Sylow Thm

Let G be a gp. of order $p^n m$, $(m, p) = 1$ where p is prime

1. G has a p-Sylow subgp.

2. Every p-subgp. is contained in a p-Sylow subgp.

3. All p-Sylow subgps. are conjugates

4. $\#p$-Sylow subgps. $\equiv 1 \ (\text{mod } p)$ & divides $|G|$.

Pf. We have already proved 1.

2. We first show if H is a p-subgp. contained in the normalizer of a p-Sylow subgp. $Q < G$, then $H < Q$

Suppose $H < N_G(Q)$

$\because$ $Q \lhd N_G(Q)$

So, $HQ < N_G(Q)$ & $[HQ : Q] = [H : H \cap Q]$

(by 3rd isomp. thm.)

Suppose $H \not\subseteq Q$, then $Q \subsetneq HQ$

$\Rightarrow [HQ : Q] > 1$

$\because [H : H \cap Q]$ is div. by p.

$\Rightarrow p \mid [HQ : Q]$

$\Rightarrow |HQ| = p^{\#} |Q|$ $\rightarrow$ Contd^{n}

$\because Q$ was p-Sylow subgp.

Now, fix a p-Sylow subgp. Q.
Let S be the set of conjugates of Q.

G acts on S by conj.

$$g \circ (g_1 Q g_1^{-1}) = g g_1 Q g_1^{-1} g^{-1}$$

$$\#S = [G : N_G(Q)]$$

$\because$ Q is p-Sylow subgp. $\Rightarrow$ $[G : N_G(Q)]$ is coprime to p

$\Rightarrow$ $\#S \not\equiv 0 \pmod{p}$

Consider the action of H on S.
By prev. lem., H has a fixed pt. on S.
say Q'

$\Rightarrow$ $H \subset N_G(Q')$ where Q' is conj. of Q.
$\Rightarrow$ $H \subset Q'$ (by prev. part of the proof)

3. Let R be a p-Sylow subgp.
Taking $H = R$ in the earlier argument,

$$R < N_G(Q') \Rightarrow R < Q' \Rightarrow R = Q' \quad (\because |R| = |Q'|)$$

So, R is conj. of Q

4. Consider the conj. action of Q on S.

Q is the only fixed pt. in S for this action

By prev. lemma, $\#S \equiv 1 \pmod p$

$\Rightarrow$ #p-Sylow subgps $\equiv 1 \pmod p$

$\because \#S = [G : N_G(Q)] \Rightarrow \#S \mid |G|$

$\Rightarrow$ #p-Sylow subgps. $\mid |G|$

Applications of Sylow Thm

Thm: Let p, q be primes with $p < q$ & $p \nmid (q-1)$. Then any group of order pq is cyclic.

Pf: By 4. of Sylow thms, $\exists$ a unique p-Sylow subgp. Sim. $\exists$ a unique q-Sylow subgp.

Let H & K be the unique cyclic subgp. of order p & q resp.

$H \cap K = \{e\}$

$\because$ H & K are normal in G

$\therefore$ $HK < G$

$$|HK| = \frac{|H||K|}{|H \cap K|} = pq \quad \Rightarrow \quad HK = G$$

So, $H \times K \longrightarrow HK \ (= G)$ is isomp.

$(h, k) \longmapsto hk$

($\because$ elems. of H & K commute

for $h \in H$, $k \in K$,

$hkh^{-1}k^{-1} \in H$ and $hkh^{-1}k^{-1} \in K$ $\Rightarrow$ $hkh^{-1}k^{-1} = e$ $\Rightarrow$ $hk = kh$)

If x & y are generators of H & K resp.

$O(x) = p$ & $O(y) = q \Rightarrow O(xy) = \text{lcm}(p,q) = pq$

$\Rightarrow \langle xy \rangle = HK = G$

Hence, G is cyclic.

$$\begin{array}{ccc} H \times K & \simeq & G \\ \downarrow\wr & \downarrow\wr & \downarrow\wr \\ \mathbb{Z}_p \times \mathbb{Z}_q & \simeq & \mathbb{Z}_{pq} \end{array}$$

$\because (\bar{1}, \bar{1})$ has order pq

Rem: If $p \mid (q-1)$, then $\exists!$ non-abelian gp. of order pq.

Imp. Example

$G = GL(\mathbb{Z}_p)$

$|G| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$

p-Sylow subgp. of G is given by

$$U = \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

(U: unipotent)

$$|U| = p^{\frac{n(n-1)}{2}}$$

For any gp. G with $|G| = n$

$$G \hookrightarrow S_n \hookrightarrow U$$

Every p-Sylow subgp. of G is the intersection of a conj. of U in $GL_n(\mathbb{Z}_p)$ with G.

Thm: Let G be a p-gp. $|G| = p^n$.
Then $\exists$ a filteration of G by subgps.
$e < G_1 < G_2 < \dots < G_{n-1} < G$ s.t $G_i \triangleleft G$ &
G_i/G_{i-1} has order p.

Pf: $e \neq Z(G) < G$

Let H be the cyclic subgp. of order p contained in $Z(G)$

If $H = G$, we're done.
Else, consider G/H. By ind^n, this has a filteration of the desired kind.

$$G \longrightarrow G/H$$

Hence, H along with pre-images of filteration of G/H under this map gives us the req. filteration.

$$e < \underbrace{f^{-1}(\bar{e})}_{H} < \underbrace{f^{-1}(\bar{G}_1)}_{G_1} < \dots < \underbrace{f^{-1}(\bar{G}_{n-1})}_{G_{n-1}} < G$$

Since,

Normality - $G' \triangleleft G/H \Rightarrow f^{-1}(G') \triangleleft G$

Ratio - $f^{-1}(G_1) < f^{-1}(G_2) < G$

$\downarrow f \qquad \downarrow f \qquad \downarrow f$

$G_1 < G_2 < G/H$

$\Rightarrow f^{-1}(G_2)/f^{-1}(G_1) \simeq G_2/G_1$

So, $|f^{-1}(G_2)|/|f^{-1}(G_1)| = |G_2|/|G_1| = p$

Thm: Let G be a finite gp. & p be the smallest prime dividing $|G|$. Then any subgp. $H \subset G$ of index p is normal.

Pf: Consider $N_G(H)$

If $N_G(H) = G$, we're done.
Else $N_G(H) = H$.

Since, if $H \subsetneq N_G(H)$
$[G : N_G(H)] < [G : H] = p$ & p is the smallest prime dividing $|G|$ $\longrightarrow$ Contd^{n}

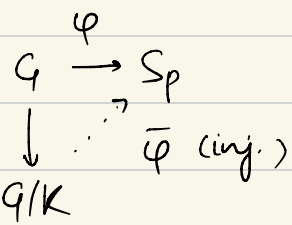
Consider the conj. action of G on H.
Then H has p conjugates $(\because [G : N_G(H)] = p)$

This defines a homomp.

$$\varphi : G \longrightarrow S_p \qquad \left(\begin{array}{l}\text{Elem. of } G \text{ permute} \\ \text{conj. of } H\end{array}\right)$$

Let $K = \ker(\varphi)$

Then $K \subset H$



Claim: $K = H$

$$[G:K] = [G:H][H:K]$$

$[G:K]$ divides $p!$; $[G:H]$ is p

$\Rightarrow [H:K]$ divides $(p-1)!$

$G/K \simeq Sp/\varphi(K)$

$\Rightarrow |G/K|$ divides $|Sp| = p!$

If $K \subsetneq H$,

$[H:K] > 1 \Rightarrow G$ will be divisible by a prime smaller than $p \rightarrow$ Contd^{n}

Thm: Let G be a group of order 56, then G has a proper normal subgp.

Pf: $56 = 2^3 \cdot 7$

G has a 2-Sylow subgp. of order 8 & a 7-Sylow subgp. of order 7.

If, the 7-Sylow subgp. is unique, we're done.
Else, number of 7-Sylow subgps. is 8.

$\therefore$ Intersection of any 7-Sylow subgps. is $\{e\}$
(as intersection would be a subgp. of both)

$\therefore$ They account for $8 \times (7-1) = 48$ elems. besides e.

The complement comprises of $56 - 48 = 8$ elems.
which form the unique 2-Sylow subgp of order 8.
$\Rightarrow$ 2-Sylow subgp. is normal

Simple gp : A gp. G is said to be simple if it has no proper, non-identity, normal subgps.

eg : 1. A_n, $n \geq 5$

$A_\infty = \bigcup_{n=5}^{\infty} A_n$

2. S_n is not simple

3. $PSL_n(\mathbb{R}/\mathbb{C}) = SL_n(\mathbb{R}/\mathbb{C})$ / scalar matrices

Thm : There is a classification of simple finite groups. There are 18 infinite families -

- $\mathbb{Z}_p$, p: prime
- A_n, $n \geq 5$
- 16 ∞ families called 'groups of Lie type'

There are 26 other 'sporadic gps' which are not part of any ∞ family.

The largest of these sporadic groups called the 'Monster group.' Its order is $\sim 10^{53}$.

20 out of these 26 are subquotients of Monster gp.

- The order of any simple gp other than $\mathbb{Z}_p$ is divisible by atleast 3 distinct primes.

Thm : (Wilson)

If p is a prime, $(p-1)! \equiv -1 \pmod{p}$

Pf : 1. $G = \mathbb{Z}_p^\times$

Consider the prod. of all non-zero elems. in G

$\bar{N} = \bar{1} \cdot \bar{2} \cdots \overline{(p-1)}$

Then, $\bar{N}$ is prod. of all elems $\bar{x} \in \mathbb{Z}_p$ s.t

$\bar{x} = \bar{x}^{-1} \Rightarrow \bar{x}^2 = 1$

only 2 elems satisfy this - $\bar{1}$ & $-\bar{1} = \overline{p-1}$

$\bar{N} = \bar{1} \cdot \bar{2} \cdots \overline{(p-1)} = \bar{1} \cdot -\bar{1} = -\bar{1}$

$\Rightarrow \overline{(p-1)!} = -\bar{1}$

$\Rightarrow (p-1)! \equiv -1 \pmod{p}$

2. $G = S_p$, $|G| = p$

Any p-Sylow subgp. of S_p has p elems. & they form a p-cycle.

There are $(p-1)!$ elems. of order p.
Each of them define a p-Sylow subgp.

$\because$ Sylow subgps. intersect trivially
$\therefore$ Each p-Sylow subgp. contributes $(p-1)$ non-identity elems. to this coll.

$$\Rightarrow \#\text{p-Sylow subgp.} = \frac{(p-1)!}{(p-1)} = (p-2)!$$

Also, $\#\text{p-Sylow subgp} \equiv 1 \pmod p$

$$\Rightarrow (p-2)! \equiv 1 \pmod p$$

$$\Rightarrow (p-1)! \equiv (p-1) \equiv -1 \pmod p$$

Groups of order pq (p, q: prime, $p < q$)

We showed that if $p \nmid (q-1)$, any gp. of order pq is cyclic.

Suppose $p \mid (q-1)$. Then $\exists$ a non-ab. gp. of order pq.

x, y: symbols

Consider free gp. on x & y.

Consider the following rel^n $x^p = e$, $y^q = e$,

$$xyx^{-1} = y^r$$

where $r \not\equiv 1 \pmod q$ & $r^p \equiv 1 \pmod q$

$\mathbb{Z}_q^*$ cyclic of order $q-1$ has such an elem. $\bar{r}$ s.t $\bar{r}^p \equiv 1 \pmod q$

H be the subgp. of $\langle x, y \rangle$ (free gp. generated by x & y) generated by x^p, y^q, xyx^{-1}

$$xyx^{-1} = y^r$$

$$\underbrace{x^p y x^{-p}}_{y} = \underbrace{x^{p-1} y^r x^{-(p-1)}}_{y} \quad \rightarrow \text{ So, the rel}^{n}\text{s are well-defined}$$

Consider $\dfrac{\langle x, y \rangle}{x^p = e,\ y^q = e,\ xy^r x = y^r}$

It has elems. $e, x, \ldots, x^{p-1}$

$y, yx, \ldots, yx^{p-1}$

$\vdots$

$y^{q-1}, y^{q-1}x, \ldots, y^{q-1}x^{p-1}$

} pq elems.

In this group, $\bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1} = \bar{y}^{r-1} \neq e$

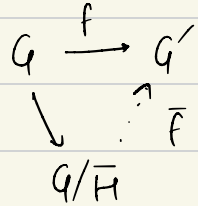
$\Rightarrow$ $\bar{x}$ & $\bar{y}$ don't commute

Normal closure :

Let G gp. & $H < G$. The normal closure of H is the intersection of all normal s.g containing H.

This is the smallest normal s.g. containing H & is denoted by $\bar{H}$.

This has the universal ppt that if $f: G \to G'$ is a gp. homomp. s.t $f(H) = e$, then f factors uniquely through at homomp. $\bar{f}: G/\bar{H} \to G'$



Since, $\bar{H} \subset \ker(f)$

eg: $\frac{\langle x_1, \ldots, x_n \rangle}{\overline{(\lambda_1, \ldots, \lambda_k)}}$, $\frac{\langle x, y \rangle}{\overline{(x)}}$

Dihedral gp: Fix $n \in \mathbb{N}$. Consider the regular polygon with $2n$ sides. We consider isometries of $\mathbb{R}^2$ which preserve this polygon (fixing origin)

This permutes the vertices & hence defines a perm. of the vertices & hence defines an elem. of S_n.

The positions of vertices 1 & 2 completely determine the isometry.

This gp. is generated by clockwise rotations of multiples of π/n & reflections about a line joining 0 with a vertex. It is denoted by D_{2n}.

Label the vertices from 1 to $2n$. Let r denote the clockwise rot^n by $\pi/4$ & s denote reflection about the line joining 0 & vertex 1.

(before any perm.)

$1, r, \ldots, r^{2n-1}, s, sr, \ldots, sr^{2n-1}$ are all distinct.

Also, $rs = sr^{-1}$

Thus, the dihedral gp. is defined by $\dfrac{\langle r, s \rangle}{\langle r^{2n}, s^2, rs = sr^{-1} \rangle}$

Thm: Any gp. of order 8 is isomp. to either

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_8$, Q_8, D_4

Semi-direct product

G : gp. $\quad H, K < G$ s.t $H \trianglelefteq G$

Then $HK < G$ is a subgp.

Notice, $h_1 k_1 h_2 k_2 = h_1 \underbrace{k_1 h_2 k_1^{-1}}_{\in H} k_1 k_2$

Motivated by action of K on H by conj., we def. the semidirect prod.

Let H, K be gp.

Let $\varphi : K \to \mathrm{Aut}(H)$ be a homomp.

Def. a gp on $H \times K$ by

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 \varphi(k_1) h_2, \; k_1 k_2)$$

Not^n: We will denote $\varphi(k)h$ by $k \cdot h$.

Thm:

1. This defines a gp. operation

We denote this gp. by $H \rtimes K$ & call it the semidirect prod. of H & K.

2. The inclusion $H \to H \rtimes K$, $h \mapsto (h, 1)$ & $K \to H \rtimes K$, $k \mapsto (1, k)$ are gp. homomp.

3. $H \cap K = e$

4. $H \trianglelefteq H \rtimes K$

5. $\forall\ h \in H,\ k \in K,\quad k \cdot h = khk^{-1}$

Pf: 1. Consider

$$[(h_1,k_1)\cdot(h_2,k_2)]\cdot(h_3,k_3) = (h_1(k_1\cdot h_2),k_1k_2)\cdot(h_3,k_3)$$
$$= (h_1\,(k_1\cdot h_2)\,\underbrace{(k_1k_2\cdot h_3)}_{k_1\cdot(k_2\cdot h_3)},\,k_1k_2k_3)$$
$$= (h_1\,k_1\cdot(h_2(k_2\cdot h_3)),\,k_1k_2k_3)$$
$$= (h_1,k_1)\cdot(h_2(k_2\cdot h_3),\,k_2k_3)$$
$$= (h_1,k_1)\cdot[(h_2,k_2)\cdot(h_3,k_3)]$$

$(1,1)$ is the identity elem.

Claim: $(h,k)^{-1} = (k^{-1}\cdot h^{-1},\,k^{-1})$

$$(h,k)\cdot(k^{-1}\cdot h^{-1},k^{-1}) = (h\,\underbrace{k\cdot(k^{-1}\cdot h^{-1})}_{h^{-1}},\,kk^{-1})$$
$$= (1,1)$$

4. Let $(g_1,g_2)\in G = H\rtimes K$

$$(g_1,g_2)\cdot(h_1,1)\cdot(g_2^{-1}\cdot g_1,\,g_2^{-1})$$
$$= (g_1(g_2\cdot h),g_2)\cdot(g_2^{-1}\cdot g_1,g_2^{-1})$$
$$= (\underbrace{g_1(g_2\cdot h)\,g_2\cdot(g_2^{-1}\cdot g_1)}_{\in H},\,1)\in H$$

5. $G = HK$

$(h_1, k_1) \cdot (h_2, k_2) = (h_1 k_1 \cdot h_2, k_1 k_2)$
$= (h_1 k_1 h_2 k_1^{-1}, k_1 k_2)$

Equating LHS, $k_1 \cdot h_2 = k_1 h_2 k_1^{-1}$

Ppn: H, K gps. $\varphi : K \to Aut(H)$ homomp.
The following are eq.

1. The identity map $H \rtimes K \to H \times K$ is a homomp. & hence an isomp.

2. φ is the trivial homomp.

3. $K \lhd H \rtimes K$

Pf: 1. $\Rightarrow$ 2.

$f((h_1,k_1)\cdot(h_2,k_2)) = f((h_1,k_1))\, f((h_2,k_2))$

$\Rightarrow f((h_1 k_1 \cdot h_2, k_1 k_2) = (h_1,k_1)\cdot(h_2,k_2) \quad \in H\times K$

$\Rightarrow (h_1 k_1 \cdot h_2, k_1 k_2) = (h_1 h_2, k_1 k_2)$

$\Rightarrow k_1 \cdot h_2 = h_2 \quad \forall\ k_1 \in K,\ h_2 \in H$

$\Rightarrow \varphi$ is trivial.

2 $\Rightarrow$ 3 $\quad \varphi$ is trivial $\Rightarrow \underbrace{\varphi(k)\,h}_{khk^{-1}} = h \Rightarrow kh = hk$

$\Rightarrow$ Elems in H & K commute.

In particular, H normalizes K.

$\because$ K normalizes K trivially

$\Rightarrow H \rtimes K = HK$ normalizes K

i.e $K \trianglelefteq H \rtimes K$

3 → 1 $\underbrace{(h_1 k_1) \cdot (h_2 k_2)}_{} = (h_1 h_2, k_1 k_2)$ in $H \times K$

$(h_1 k_1 \cdot h_2, k_1 k_2)$

$= (h_1 k_1 h_2 k_1^{-1}, k_1 k_2)$

$= (h_1 k_1 k_1^{-1} h_2, k_1 k_2)$

$= (h_1 h_2, k_1 k_2)$

in $H \times K$

[Elems in H & K commute $\because H \lhd H \times K$]

$hkh^{-1}k^{-1} \in K, H$

$\Rightarrow hkh^{-1}k^{-1} = e$

$\Rightarrow hk = kh$

Thm: Let gp. G, $H, K < G$ s.t

1. $H \lhd G$
2. $H \cap K = e$
3. $G = HK$

Then $G \simeq H \times_\varphi K$, where $\varphi : K \to Aut(H)$

$k \mapsto \underbrace{[h \mapsto khk^{-1}]}_{C_k}$

Pf: Define $f : H \times_\varphi K \to G$

$(h, k) \mapsto hk$

We check that f is a homomp.

$f(h_1, k_1) \cdot f(h_2, k_2) = h_1 k_1 h_2 k_2$

$\Rightarrow f(h_1 \underbrace{k_1 \cdot h_2}_{k_1 h_2 k_1^{-1}}, k_1 k_2) = h_1 k_1 h_2 k_2$

$\Rightarrow h_1 k_1 h_2 k_1^{-1} k_1 k_2 = h_1 k_1 h_2 k_2$

$\Rightarrow h_1 k_1 h_2 k_2 = h_1 k_1 h_2 k_2$

$H \cap K = e$ imply inj. & $G = HK$ imply surj.

Hence, f is an isomp.

eg :

1. $H = (\mathbb{R}, +)$, $K = (\mathbb{R}^*, \cdot)$

$$\varphi : K \to \mathrm{Aut}(H)$$
$$y \mapsto [x \mapsto yx]$$

$H \rtimes K$

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 + y_1 x_2, y_1 y_2)$$

$$\begin{pmatrix} y_1 & x_1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} y_2 & x_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} y_1 y_2 & x_1 + y_1 x_2 \\ 0 & 1 \end{pmatrix}$$

$H \rtimes K$ is isomp. to the gp. of affine transformations (isometries) of the plane.

2. $G = S_n$

$H = A_n$

$K = \{1, \tau\}$ where τ is a transposition τ

By thm proved above, $G = HK$

3. $G = GL_n(\mathbb{R})$

$H = SL_n(\mathbb{R})$

$K = \begin{pmatrix} \alpha & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix}$

Clearly, $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$ & $H \cap K = e$

$A \in GL_n(\mathbb{R})$, $A = (a_{ij})$

$$= \underbrace{\begin{pmatrix} \frac{a_{11}}{\det(A)} & \cdots & a_{11} \\ \vdots & & \vdots \\ \frac{a_{n1}}{\det(A)} & \cdots & a_{nn} \end{pmatrix}}_{\in SL_n(\mathbb{R})} \underbrace{\begin{pmatrix} \det(A) & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix}}_{\in K}$$

So, $G = HK$

By thm proved above, $G = H \rtimes K$

$$\Rightarrow GL_n(\mathbb{R}) = SL_n(\mathbb{R}) \rtimes K$$

Note, the conj. action of K on $SL_n(\mathbb{R})$ is non-trivial.

Also, $K \simeq \mathbb{R}^*$

Suppose n is odd.

$$Z = \begin{pmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix}, \quad \lambda \in \mathbb{R}^*$$

$$Z \subset GL_n(\mathbb{R})$$

$$Z \cap SL_n(\mathbb{R}) = e, \quad \left(\because \lambda^n = 1 \text{ for odd } n \Rightarrow \lambda = 1 \right)$$

Claim : $GL_n(\mathbb{R}) \simeq SL_n(\mathbb{R}) \rtimes \mathbb{Z}$

$A \in GL_n(\mathbb{R})$

$$A = \underbrace{\left[A \begin{pmatrix} \det(A)^{1/n} & & \\ & \ddots & \\ & & \det(A)^{1/n} \end{pmatrix}^{-1} \right]}_{\in SL_n(\mathbb{R})} \underbrace{\begin{pmatrix} \det(A)^{1/n} & & \\ & \ddots & \\ & & \det(A)^{1/n} \end{pmatrix}}_{\in \mathbb{Z}}$$

So, $GL_n(\mathbb{R}) = SL_n(\mathbb{R}) \times \mathbb{Z}$

$\because SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$ & $\mathbb{Z} \lhd GL_n(\mathbb{R})$
& $SL_n(\mathbb{R}) \cap \mathbb{Z} = e$

Hence, the identity map $SL_n(\mathbb{R}) \rtimes \mathbb{Z} \to SL_n(\mathbb{R}) \times \mathbb{Z}$ is an isomp.

$\Rightarrow GL_n(\mathbb{R}) \simeq SL_n(\mathbb{R}) \times \mathbb{R}^*$

4. Gps. of order pq

p, q primes, $p < q$, $p \nmid (q-1)$

Let G be a gp. of order pq.

H: subgp. of order q (normal)
K: subgp. of order p (normal)

$\because G = HK$
$\therefore G \cong H \rtimes K$

$$\underbrace{K}_{\mathbb{Z}_p} \longrightarrow \underbrace{\mathrm{Aut}(H)}_{\underbrace{\mathbb{Z}_q}_{\mathbb{Z}_{q-1}}}$$

$\mathbb{Z}_p$ has no proper subgp. So map is inj.
However, image of $\mathbb{Z}_p$ must be a subgp. of $\mathbb{Z}_{q-1}$ which isn't possible as $p \nmid q-1$

$\therefore$ No such non-tvl. homomp. exists.

So, the map is trivial & hence $G \cong H \times K \cong \mathbb{Z}_{pq}$

Hence, $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q \simeq \mathbb{Z}_{pq} \quad \forall\ \varphi$

Suppose $p \mid (q-1)$

$$\mathrm{Aut}(\mathbb{Z}_q) \simeq \mathbb{Z}_{q-1}$$

This has a unique subgp. of order p, generated by γ

Def. $\varphi : \mathbb{Z}_p \to \mathbb{Z}_{q-1} = \mathrm{Aut}(\mathbb{Z}_q)$

$\bar{1} \mapsto \gamma$

This def. a semi-direct prod. $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$

Check this gp. is non-abelian.

<u>Claim</u>: This is the unique non-ab. gp. of order pq.

Lem: H, K gps. $\varphi : K \to \mathrm{Aut}(H)$

Let $G = H \rtimes_\varphi K$

Let $f : K \to K$ be an automorphism

Let $\varphi' = \varphi \circ f : K \to \mathrm{Aut}(H)$

Then $H \rtimes_{\varphi'} K = H \rtimes_\varphi K$

Pf: (uniqueness)

Let $\varphi' : \mathbb{Z}_p \to \mathbb{Z}_{q-1}$

$\bar{1} \mapsto \gamma^i$, $1 \le i \le p-1$

Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$

$1 \mapsto i$

Then $\varphi' = \varphi \circ f$

By above lemma, $H \rtimes_{\varphi'} K \simeq H \rtimes_\varphi K$

5. Dihedral gp

$$D_{2n} = \langle r, s \mid r^{2n} = 1,\ s^2 = 1,\ sr = r^{-1}s \rangle$$

Thus, D_{2n} has a cyclic subgp. of order $2n$ i.e $\langle r \rangle$ & index 2 (hence normal)

Also, $\langle s \rangle$ is a gp. of order 2.

Hence, by thm stated earlier, $D_{2n} \cong \underbrace{\mathbb{Z}_{2n}}_{\langle r \rangle} \rtimes_\varphi \underbrace{\mathbb{Z}_2}_{\langle s \rangle}$

$$\varphi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_{2n})$$
$$\bar{1} \mapsto [r \mapsto -r]$$

Solvability

A gp. G is said to be solvable if $\exists$ a tower of subgps. s.t

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n = e \quad \text{s.t} \quad G_{i+1} \lhd G_i$$
& G_i/G_{i+1} is abelian.

eg: 1. Abelian gp.
$G > e$

2. S_n is solvable if $n \leq 4$

$S_2 \simeq \mathbb{Z}_2$
$S_3 > A_3 > e$
$S_4 > A_4 > \text{Klein's 4-gp} > e$
$\simeq$
$\mathbb{Z}_2 \times \mathbb{Z}_2$
$(1,0) \longmapsto (12)(34)$
$(0,1) \longmapsto (13)(24)$

Thm: S_n is not solvable if $n \geq 5$

3. G : gp, $H \triangleleft G$

G is solvable iff H & G/H are solvable

Pf: ($\Rightarrow$) Suppose G is solvable

$$G \supsetneq G_1 \supsetneq G_2 \cdots \supsetneq G_n = e$$

$$\Rightarrow G \cap H > G_1 \cap H > G_2 \cap H \cdots > G_{n-1} \cap H > e$$

& remove the repetitions.

$$\begin{array}{ccc} G_2 & \triangleleft & G_1 \\ i \uparrow & & \uparrow i \\ i^{-1}(G_2) = G_2 \cap H & \triangleleft & G_1 \cap H \end{array}$$

So, $$\frac{G_1 \cap H}{G_2 \cap H} = G_1/G_2$$

Sim. , $G \trianglerighteq G_1 \trianglerighteq G_2 \cdots \trianglerighteq G_n = e$

$\Rightarrow$ $G/H > G_1/H > G_2/H \cdots > G_{n-1}/H \trianglerighteq e$

& remove the repetitions.

$$\begin{array}{ccc} G_2 & \triangleleft & G_1 \\ \downarrow & & \downarrow \\ G_2/H & \triangleleft & G_1/H \end{array} \qquad (\because \text{map is surjective})$$

$$G_i \xrightarrow{\varphi} G_i/H \to \bar{G}_i/\bar{G}_{i+1}$$

$(= \bar{G}_i \text{ say})$

Thus φ induces a surj. homomp.

$$G_i/G_{i+1} \longrightarrow \bar{G}_i/\bar{G}_{i+1}$$

(abelian) $\therefore$ (abelian)

($\Leftarrow$) Conversely, suppose H & G/H are solvable

The tower of H along with the pre-image of tower of G/H under the map $G \to G/H$ together constitute the tower for G.

$$H = H_0 \supsetneq H_1 \supsetneq \dots \supsetneq H_m = e$$

&

$$G/H = \bar{K}_0 \supsetneq \bar{K}_1 \supsetneq \dots \supsetneq \bar{K}_s = \bar{e}$$

So,

$$G = K_0 \supsetneq K_1 \supsetneq \dots \supsetneq K_s = H = H_0 \supsetneq H_1 \supsetneq \dots \supsetneq H_m = e$$

Check that this is an abelian tower

Thm: (Feit-Thompson Thm)
Every gp. of odd order is solvable

eg: p, q distinct primes $(p<q)$
Any gp. of order pq is solvable

Pf: Let H be the q-Sylow subgp.
Then H is normal & solvable $(\simeq \mathbb{Z}_q)$
$G/H \simeq \mathbb{Z}_p$ Hence solvable. Hence G is solvable

Non-examples:
S_n is not solvable if $n \geq 5$

Pf: Fix 5 distinct integers i, j, k, ℓ, s.
Def. $\sigma = (i\ j\ k)$, $\tau = (\ell\ s)$

One computes $\sigma\tau\sigma^{-1}\tau^{-1} = (\ell\ k\ i)$

Suppose S_n is solvable
$S_n = H_0 \supsetneq H_1 \supsetneq \cdots \supsetneq H_m = e$ be an abelian tower

H_0/H_1 is abelian

$$\overline{(1\,k\,i)} = \overline{\sigma\tau\sigma^{-1}\tau^{-1}} = \bar{e} \quad \Rightarrow \quad \overline{(1\,k\,i)} \in H_1$$

$(\because aba^{-1}b^{-1}$ is e in abelian gp.$)$

This shows that if H_i contains a 3-cycle, then H_{i+1} also contains it. By ind^n, $\overline{(1\,k\,i)} \in H_m = e$

→ Contd^n

finitely generated abelian gps.

A : ab. gp.

A is said to be finitely generated if $\exists$ elements $x_1, \dots, x_n \in A$ s.t every element $x \in A$ can be written as $x = \sum_{i=1}^{n} n_i x_i$, $n_i \in \mathbb{Z}$

OR

$\exists$ surjection $\mathbb{Z}^n \to A$

$(1, \dots, 0) \mapsto x_1$

Examples :

1. $\mathbb{Z}^n$ generated by $(1, 0 \dots, 0), (0, 1, \dots, 0), \dots, (0, \dots, 1)$

2. $\mathbb{Z}_n$ generated by $\bar{1}$

3. Any finite direct sum of fin. gen. ab. gps. is fin. gen.

Non-example :

1. Any uncountable ab. gp.
2. $\mathbb{Q}$, $\mathbb{Q}/\mathbb{Z}$

Suppose $\mathbb{Q}$ is finitely generated by $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots, \frac{p_1}{q_1}$

Let p be a prime <u>not</u> dividing any q_i.

Suppose $\frac{1}{p} = \sum n_i \frac{p_i}{q_i} = \frac{N}{\prod q_i}$ for some integer N

$\rightarrow$ Contdⁿ $\because p \nmid q_i$

3. $\bigoplus_{k=1}^{\infty} \mathbb{Z}$

<u>Free</u> : We say fin. gen ab. gp. A is free if $\exists$ elems. $x_1, \ldots, x_r$ s.t any elem. $x \in A$ can be written <u>uniquely</u> as a linear combination $x = \sum_{n_i \in \mathbb{Z}} n_i x_i$

<u>OR</u>

$\exists$ isomp. of gps. $A \simeq \mathbb{Z}^r$ for some r.

Ppⁿ: Let A be fin. gen. ab. gp. Let $f: A \twoheadrightarrow A'$ be a surjection of gps. s.t A' is free. Let K be the kernel of f. Then $\exists$ a subgp. $B < A$ s.t $f|_B : B \xrightarrow{\sim} A'$ is an isomp., $B \cap K = 0$ & $A = B \oplus K$

(identity)

$$\begin{array}{ccc} K < A & \xrightarrow{f} & A' \\ \cup & \nearrow_{\sim} f|_B & \\ B & & \end{array}$$

Pf: Let $x_1, x_2, \dots, x_r$ be the generators of A'.
Let $y_1, y_2, \dots, y_n$ be the elems. in A s.t $f(y_i) = x_i$

Let B be subgp. of A generated by $y_1, \dots, y_r$.
Clearly, $f|_B : B \to A'$

$$y_i \mapsto x_i$$

inj.: If $y = \sum n_i y_i$ s.t $f(y) = \sum n_i x_i = 0$

$$\Rightarrow n_i = 0 \quad \forall i$$

$$\Rightarrow y = 0$$

$$\Rightarrow B \cap K = 0$$

Let $a \in A$.

Let $f(a) = \sum_{i=1}^{r} n_i x_i$

$$f\left(a - \sum_{i=1}^{r} n_i y_i\right) = f(a) - \sum_{i=1}^{r} n_i x_i = 0$$

$$\Rightarrow \quad a - \sum_{i=1}^{r} n_i y_i \in K$$

$$\Rightarrow \quad a = b + k \quad , \quad b \in B, \; k \in K$$

So, $A = B \oplus K$

Thm: Let A be a fin. gen. free ab. gp. of rank r. Let $B < A$ be a subgp. Then B is also free of rank $\leq r$.

(Rank: If A is a fin. gen. free ab. gp. Then the no. of generators is called the rank
i.e $A \simeq \mathbb{Z}^r$, $r = rk\, A$)

Rem: If $A' < A$ s.t $rk\, A = rk\, A'$, then A/A' is finite.

eg: $A' = 2\mathbb{Z}$, $A = \mathbb{Z}$

Pf: $A \simeq \mathbb{Z}^r$

The proof is by ind^n on r.

If $r = 1$, $A \simeq \mathbb{Z}$ any non-empty subgps. of $\mathbb{Z}$ is isomp. to $n\mathbb{Z}$, hence free.

Consider the homomp.

$$\begin{aligned} pr_r : A &\to \mathbb{Z} \\ (a_1, \dots, a_r) &\mapsto a_r \end{aligned}$$

Consider the restricted homomp. $pr_r|_B : B \to \mathbb{Z}$

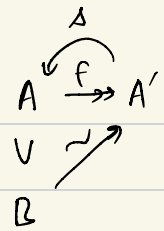
The kernel of this map is a subgp. of $\mathbb{Z}^{r-1}$ & hence by ind^n free of $rk \leq r-1$

So, by the last pp^n,

$$B \simeq \underbrace{Ker(pr|_B)}_{\text{free by ind}^n} \oplus \underbrace{Img(pr|_B)}_{\text{free since s.g. of } \mathbb{Z}}$$

Hence, B is free.

Rem :



By composing the isomp. $A' \to B$ with the inclusion map $B \subset A$, we obtain the map $s : A' \to A$ s.t $s \circ f = Id_A$.

Such a map is called a splitting

Well-definedness of rk

$$\mathbb{Z}^r \simeq \mathbb{Z}^s$$

$$\Rightarrow \quad \frac{\mathbb{Z}^r}{(p\mathbb{Z}^r)} \simeq \frac{\mathbb{Z}^s}{(p\mathbb{Z}^s)}$$

$$\| \qquad\qquad \|$$

$$(\mathbb{Z}_p)^r \qquad (\mathbb{Z}_p)^s$$

Different cardinalities

Cor: Subgp. of a fin. gen. ab. gp is f.g.

Pf: Let A be a fin. gen. ab. gp.
Then $\exists$ surj. $\mathbb{Z}^r \xrightarrow{\varphi} A$ for some r.

Let $A' < A$ be a subgp.

$$\begin{array}{ccc} \mathbb{Z}^r & \twoheadrightarrow & A \\ \cup & & \cup \\ \varphi^{-1}(A') & \twoheadrightarrow & A' \end{array}$$

$\varphi^{-1}(A')$ is a subgp. of $\mathbb{Z}^r$ & hence free of $rk \leq r$

Hence, A' is also f.g, since $\varphi^{-1}(A') \twoheadrightarrow A'$ is a surj.

Rem: Subgp. of f.g gp. is **not** f.g in general

$$F_\infty \hookrightarrow F_2$$

However, s.g. of a free gp. is free.

Torsion subgp.:

A : ab. gp.

Def A_{tor} to be the set $\{x \in A : nx = 0 \text{ for some } n \in \mathbb{Z}\}$

$A_{tor} < A$ (requires abelianness)

We say A is a torsion gp. if $A = A_{tor}$

If A is f.g & a torsion gp. then A is finite

In general, A/A_{tor} is torsion free.

$$n\bar{x} = 0 \Rightarrow nx \in A_{tor} \Rightarrow m(nx) = 0$$
$$\Rightarrow (mn)x = 0$$
$$\Rightarrow x \in A_{tor}$$
$$\Rightarrow \bar{x} = \bar{0}$$

Thm: Let A be a f.g torsion-free ab. gp. Then A is free.

Pf: Let $x_1, x_2, \dots, x_r$ be the maximal set of elems. in A s.t whenever $\sum_{i=1}^{r} n_i x_i = 0$, each $n_i = 0$

Since A is torsion free, $r \geq 1$

span of $x_1, \dots, x_r$ define a free subgp. of A of rk r.

Let $x \in A$ be outside the span of $x_1, \dots, x_r$
Then $\exists$ a non-trvl linear comb.

$$mx + \sum_{i=1}^{r} n_i x_i = 0$$

$\because$ A is finitely generated, $\exists\, M \in \mathbb{N}$ s.t for any $y \in A$, $My \in \text{span}\langle x_1, \dots, x_r \rangle$

$$\begin{array}{ccc} A & \xhookrightarrow{\cdot M} & A \\ a & \longmapsto & Ma \end{array}$$

The map is inj. & its image is a s.g of free gp. generated by $x_1, \ldots, x_n$.

$\therefore$ $\mathrm{Img}(\cdot M)$ is free.
Since it is inj., A is free.

A : f.g. ab. gp.
A/A_{tor} : torsion-free hence free

$$A \twoheadrightarrow A/A_{tor} \simeq \mathbb{Z}^r$$

By prev. thm, $A \simeq A_{tor} \oplus \mathbb{Z}^r$

A_{tor} is f.g & hence finite

Claim: f.g. torsion gps. are finite

Suppose B is f.g & torsion. Let $x_1, \ldots, x_n$ be set of generators of order $m_1, \ldots, m_n$ resp.

Then every elem. in B can be written as

$$y = \sum_{i=1}^{n} a_i x_i \quad , \quad 0 \le a_i \le m_i$$

(finite choices)

So, f.g torsion gp is the same as finite abs. gp.

A : finite abs. gp.

For any prime p, def.

$$A(p) = \{ x \in A : p^n x = 0 \text{ for some } n \}$$

Thm : $\exists$ isomp. $\bigoplus_{\text{finite}} A(p) \to A$

Pf : $\exists$ a homomp. of the above kind

$$(a_1, \dots, a_r) \to \sum a_i$$

inj. : Suppose $\sum a_i = 0$, $a_i \in A(p_i)$

$$\Rightarrow a_1 = \underbrace{-a_2}_{\text{annihilated by } p_2^{N_2}} - a_3 \dots \underbrace{- a_n}_{\text{annihilated by } p_n^{N_n}}$$

$\Rightarrow \exists N$ s.t $(p_2 \cdots p_n)^N a_1 = 0$

But $p_1^M a_1 = 0$ for some M.

But $(p_1^M, (p_2 \cdots p_n)^N) = 1 \Rightarrow 1 \cdot a_1 = 0 \Rightarrow a_1 = 0$

Sim., we can show $a_i = 0 \quad \forall\ i = 1, \cdots, n$

Hence, the map is inj.

surj: For any $m \in \mathbb{Z}_{>0}$, def. A_m to be the kernel of the map. $A \xrightarrow{m} A$, $x \mapsto mx$

Claim: If m & n are coprime, $A_{mn} = A_m \oplus A_n$

$(m, n) = 1 \Rightarrow \mu m + \nu n = 1$ for some $\mu, \nu \in \mathbb{Z}$

Let $x \in A_{mn}$. $\Rightarrow x = \underbrace{\mu m x}_{\in A_n} + \underbrace{\nu n x}_{\in A_m}$

Clearly, $A_m \cap A_n = \{0\} \Rightarrow A_{mn} = A_m \oplus A_n$

Inductively, $m = \prod_{i=1}^{k} p_i^{n_i}$, p_i : distinct primes

$$A_m = \bigoplus_{i=1}^{k} A_{p_i^{n_i}}$$

fix $x \in A$.

$\exists n \in \mathbb{Z}_{>0}$ s.t $nx = 0$. $\quad n = p_1^{k_1} \cdots p_n^{k_n}$

$$x \in A_n = \bigoplus_{i=1}^{k} A_{p_i^{n_i}}$$

$A_{p_i^{n_i}} \subset A(p_i)$

$\Rightarrow x \in \bigoplus_{\text{finite}} A(p_i)$

Hence, the map is surj.

$$A \simeq \bigoplus_{\substack{p\text{-prime} \\ \text{(finite)}}} A(p)$$

Let us understand $A(p)$ for a prime p.

An ab. gp for which $A = A(p)$ is called a p-gp.

eg: $\mathbb{Z}_{p^n}$, $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^m}$

Thm: Every finite p-gp is isomp. to

$$\mathbb{Z}_{p^{\lambda_1}} \oplus \mathbb{Z}_{p^{\lambda_2}} \oplus \dots \oplus \mathbb{Z}_{p^{\lambda_k}}$$

The integer $(\lambda_1, \dots, \lambda_k)$ can be chosen uniquely s.t $\lambda_1 \geq \dots \geq \lambda_k$

We call A to be of the type $(p^{\lambda_1}, \dots, p^{\lambda_k})$

Lem: Let A be a p-gp. Let a be an elem. of maximal order in A, say p^{λ_1}. Let A_1 be the subgp. of A generated by a. If A/A_1 has an elem. of order p^{λ}, for some λ, then A has an elem. of order p^{λ}.

Pf:

A

$\cup$

$A_1 = \langle a \rangle$

Let $\bar{b} \in A/A_1$ be an elem. of order p^{λ}.
Let b be a lift of $\bar{b}$ to A ($b \in A$)

$$p^{\lambda}\bar{b} = \bar{0} \Rightarrow p^{\lambda}b \in A_1$$
$$\Rightarrow p^{\lambda}b = na$$

Order of $\bar{b} \leq$ order of b

If $n=0$, order of $b = p^{\lambda}$ & we're done
In general, write $n = p^k\mu$ with $(p,\mu) = 1$

$\because (p,\mu) = 1 \Rightarrow a^{\mu}$ is also a generator of A_1
& hence with order p^{λ_1}

We can assume $k \leq \lambda_1$ ($\because p^{\lambda_1}$ is the max order)

Then, $\underbrace{p^k \mu a}_{na} = p^\lambda b$ has order $p^{\lambda_1 - k}$ clearly

$\Rightarrow$ Order of $b = p^{\lambda_1 - k + \lambda}$

Hence, $\lambda_1 - k + \lambda \leq \lambda_1 \Rightarrow \lambda \leq k$

So, $p^\lambda b = p^k \mu a \quad (\lambda \leq k)$

$\Rightarrow \exists\, c \in A_1 \;\; s.t \;\; p^\lambda b = p^\lambda c \Rightarrow p^\lambda (b-c) = 0$

$(p^{k-\lambda} \mu a)$

$\Rightarrow \bar{c} = 0 \Rightarrow \overline{b-c} = \bar{b}$

Hence, we have found a lift of $\bar{b}$ in A of order p^λ, namely $b-c$.

Thm: Every finite ab. p-gp A is a direct sum of cyclic gps. i.e.

$$A \simeq A_1 \oplus A_2 \oplus \cdots \oplus A_n$$
$$\text{order } p^{\lambda_1} \quad p^{\lambda_2} \quad p^{\lambda_n}$$

Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n \geq 1$

Then the tuple $(\lambda_1, \ldots, \lambda_n)$ is unique.

Pf: Use ind^n on the order of the gp.

Let it be true for any gp. with order less than $n = \text{ord}(A)$

Choose $a_1 \in A$, which has maximal order.

Also, A is not cyclic, so $\text{ord}(a_1) = p^k$ for some $k < \lambda$

Consider the quotient gp. A/A_1, $\text{ord}(A) = p^\lambda$

So, $\text{ord}(A/A_1) = p^{\lambda - k}$ $\quad \text{ord}(A_1) = p^k$, $A_1 = \langle a_1 \rangle$

By ind^n hyp., $A/A_1 \overset{\varphi}{\simeq} A_2 \oplus A_3 \cdots \oplus A_n$

Take any $x \in A$. Then $\bar{x} \in A/A_1$

$$\bar{x} = m_2 a_2 + \dots + m_n a_n \quad \text{where}$$

$a_2, a_3, \dots, a_n$ are the generators for the cyclic gps. $A_2, A_3, \dots, A_n$.

Then, $x - m_2 a_2 - \dots - m_n a_n$ lies in A_1

$$\Rightarrow x - m_2 a_2 - \dots - m_n a_n = m_1 a_1$$

$$\Rightarrow x = m_1 a_1 + \dots + m_n a_n$$

$$\Rightarrow A = A_1 + \dots + A_n$$

Taking image of x in A/A_1 we get

$$\bar{x} = 0 + m_2 \bar{a}_2 + \dots + m_n \bar{a}_n$$

This shows that, $A \simeq \bigoplus A_i$, $\text{ord}(A_i) = p^{\alpha_i}$

for uniqueness, we again induct on order.

Suppose A has 2 decompositions $(r_1 \geq r_2 \cdots \geq r_k \geq 1)$ & $(m_1 \geq m_2 \geq \cdots \geq m_s \geq 1)$

Consider the subgp.

$$pA = \{ pa : a \in A \}$$

We know that,

$$pA \simeq pA_1 \oplus pA_2 \oplus \cdots \oplus pA_k$$
$$pA \simeq pB_1 \oplus pB_2 \oplus \cdots \oplus pB_s$$

Decomposing, we get

$$(p^{r_1-1}, p^{r_2-1}, \cdots, p^{r_k-1}) = (p^{m_1-1}, p^{m_2-1}, \cdots, p^{m_s-1})$$

We get $r_i - 1 = m_j - 1 \Rightarrow r_i = m_j$

Now, $A = (p^{r_1}, p^{r_2}, \cdots, p^{r_k}, \underbrace{p, p, \cdots, p}_{\mu})$

$$= (p^{m_1}, p^{m_2}, \cdots, p^{m_s}, \underbrace{p, p, \cdots, p}_{l})$$

Total no. of elems. $= p^{r_1 + \cdots + r_k + \mu} = p^{m_1 + \cdots + m_s + l}$

$\Rightarrow \mu = l$

$\therefore$ The tuple $(r_1, \ldots, r_k)$ is unique.

Ring Theory

Commutative Ring with identity is a set R together with two operations $+ : R \times R \to R$, $\cdot : R \times R \to R$ s.t

1. $(R, +)$ is an abelian gp.
   Denote its identity by 0.

2. $(\cdot)$ is associative : $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, $\forall a, b, c \in R$

3. $(\cdot)$ is commutative $a \cdot b = b \cdot a \quad \forall a, b \in R$

4. $a \cdot (b + c) = a \cdot b + a \cdot c$

5. $\exists 1 \in R$ s.t $a \cdot 1 = a \quad \forall a \in R$

Ring Homomorphism : Let R, S be rings.
A map $f: R \to S$ is called a ring homomorphism if

1. f is a homomp. of ab. gp. wrt add^n operation on R & S.

$$f(a+b) = f(a) + f(b)$$

(add^n in R on the left; add^n in S on the right)

2. $f(a \cdot b) = f(a) \cdot f(b)$
3. $f(1_R) = 1_S$

Ring isomorphism : A ring homomp. with a 2-sided inverse is called a ring isomp. i.e f is a bijective ring homomp.

Subring: Let R be a ring. A subring of R is a subset $R' \subseteq R$ s.t

1. $(R', +)$ is an ab. subgp. of $(R, +)$
2. $1 \in R$
3. $a \cdot b \in R'$ whenever $a, b \in R'$

If $f: R \to S$ is a ring homomp., then $f(R)$ is a subring of S.

Unit: R – ring

The set $\{x \in R : \exists\, y \in R \text{ s.t } x \cdot y = 1\}$ are called units of R.

(y is called the multiplicative inverse of x)

Units of R denoted $U(R)$ form a gp. with 1 as an identity elem.

If $x, y \in U(R)$,

$$(xy)(y^{-1}x^{-1}) = x(y \cdot y^{-1})x^{-1} = x \cdot 1 \cdot x^{-1} = x \cdot x^{-1} = 1$$

So, $xy \in U(R)$

Examples:

1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$

2. $(\mathbb{Z}_n, +, \cdot)$

$$\overline{a+b} = \bar{a} + \bar{b}$$
$$\overline{a \cdot b} = \bar{a} \cdot \bar{b}$$

$\mathbb{Z} \to \mathbb{Z}_n$ is a ring homomp.

3. Polynomial Rings

Fix a ring R.
Let S be a set. For each elem. $i \in S$, introduce a variable x_i. Let T be a coll. of all poly. in $\{X_i\}_{i \in S}$ with coefficients in R.

Then T is a ring with usual add^n & multip^n of poly.

$$T = R[X_i]_{i \in S}$$

eg: $S = \{1, 2, 3, 4\}$
$T = \mathbb{Z}[X_1, X_2, X_3, X_4]$, 1_T = const. poly.

4. Power series

As before, we could consider the set of all power series in variables $\{X_i\}_{i \in S}$

$$T = R[[X_i]]_{i \in S}$$

eg: $R = \mathbb{Z}$, $S = \{1, 2, 3, 4, \dots\}$

$T = \mathbb{Z}[[X_1, X_2, \dots]]$, coeffs. from $R = \mathbb{Z}$

$$2 + 3X_1 + 4X_2X_3X_5^3 + \dots \in T$$

5. Convergent power series in $\mathbb{R}[[X_1, X_2, \dots, X_n]]$ for all the values of $x_1, \dots, x_n$. It is denoted by $\mathbb{R}\{\{X_1, \dots, X_n\}\}$

eg: $\mathbb{R}\{\{X\}\}$

$$1 + X + \frac{X^2}{2!} + \dots \to e^X$$

6. Fix an ab. gp. G. Fix a ring R.
Denote by $R[G]$, the coll. of all formal sums of the type $\sum a_g \cdot g$ where $a_g \in R$, $g \in G$.

$R[G]$ is called the group ring, $g \in G$

0 elem : elem. all whose coeffs are zero.
1 elem : $1_R \cdot e$

Gp operation : $(a_g \cdot g)(b_h \cdot h) = (a_g \cdot b_h)(g \cdot h)$

multipn in R ↑ multipn in G ↑

Extend by linearity.

7. Fix a set S and a ring R. Let $Mor(S,R)$ be the coll. of all set maps from S to R.

Then $Mor(S,R)$ has a ring structure

$$(f+g)(s) = f(s) + g(s),$$
$$(f \cdot g)(s) = f(s) \cdot g(s)$$

8. X: any metric sp.

Let $\mathcal{C}(X)$ be the set of all cont. maps from X to $\mathbb{R}$.

This is a ring as before:

$$(f+g)(s) = f(s) + g(s)$$
$$(f \cdot g)(s) = f(s) \cdot g(s)$$

Sum & prod. of cont. maps is cont.

9. Let $f, g \in L^1(\mathbb{R})$ i.e $\int_{\mathbb{R}} |f| \, dx$ exists.

Define a ring op. on this coll. whereby add^n is the usual add^n & multip^n defined by convolution

$$f * g = \int_{\mathbb{R}} f(x_0 - y) \, g(y) \, dy$$

10. $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$

11. Product of rings

$(R, +, \cdot)$ & $(S, \bar{+}, \bar{\cdot})$

$R \times S$ has a ring structure wrt componentwise add^n & multip^n.

Add^n id : $(0_R, 0_S)$

Multip^n id : $(1_R, 1_S)$

Rem : $M_n(K)$ is an important non-commutative ring

Examples of Ring Homomp.

1. $\mathbb{Z} \to \mathbb{Z}_n$

2. R: any ring

$$R[X_1, \dots, X_n] \to R[Y_1, \dots, Y_n]$$
$$X_i \mapsto f_i(Y_1, \dots, Y_n) \quad \text{for some } f_i$$

3. complex conj.

$$\mathbb{C} \to \mathbb{C}$$
$$z \mapsto \bar{z}$$

$$\overline{z+w} = \bar{z} + \bar{w}$$
$$\overline{zw} = \bar{z}\,\bar{w}$$
$$\bar{1} = 1$$

4. Evaluation map

X : metric sp.

$\mathcal{C}(X)$: cont. real valued fn^{n}s

$p \in X$

$$\begin{array}{ccc} \mathcal{C}(X) & \longrightarrow & \mathbb{R} \\ f & \overset{ev_p}{\longmapsto} & f(p) \end{array}$$

$$ev_p(f+g) = (f+g)(p) = f(p) + g(p) = ev_p(f) + ev_p(g)$$

5. Any ring automp. of $\mathbb{Q}$ is identity

Let $f : \mathbb{Q} \to \mathbb{Q}$ be a ring automp.

Then $f(n) = n \quad \forall\, n \in \mathbb{Z} \qquad (\because f(1) = 1)$

Let $1 = p/q$.

$$f(\underbrace{p/q + p/q \cdots + p/q}_{q\text{-times}}) = q\, f(p/q)$$

$$\Rightarrow \frac{f(p)}{q} = f(p/q) \quad \Rightarrow \quad f(p/q) = p/q$$

Ex: Show that a ring automs. of $\mathbb{R}$ is identity.

Integral domain: A ring R is called an integral domain if whenever $a \cdot b = 0$ for $a, b \in R$, $a = 0$ or $b = 0$

Field: A ring R is said to be a field if every elem. $x \neq 0 \in R$ has an inverse i.e $\exists\, x^{-1} \in R$ s.t $x \cdot x^{-1} = 1$

Note: Field $\Rightarrow$ Integral domain

R: field

Let $x, y \in R$ s.t $x, y \neq 0$

Suppose $x \cdot y = 0 \Rightarrow x^{-1} \cdot (x \cdot y) = 0$

$\Rightarrow (x^{-1} \cdot x) \cdot y = 0$

$\Rightarrow y = 0 \rightarrow$ Contdn

Converse is true only if field is finite.

So, a finite integral domain is a field.

R: finite integral domain

Let $x \in R$ with $x \neq 0$

Let $R = \{x_1, \ldots, x_n\}$ with $x = x_1$, say

Consider the set $\{xx_1, \ldots, xx_n\}$

Claim: These all are distinct.

If $xx_i = xx_j \Rightarrow x \cdot (x_i - x_j) = 0$

$\because x \neq 0 \Rightarrow x_i - x_j = 0 \Rightarrow x_i = x_j$

In particular, $\exists\ 1 \leq j \leq n$ s.t $x \cdot x_j = 1$

$\Rightarrow x_j = x^{-1}$

Examples

1. $\mathbb{Z}_n$ is an integral domain (hence field) iff n is prime.

($\Rightarrow$) If $n = a \cdot b$, with both $a, b \neq 1$.

$\Rightarrow \bar{a} \cdot \bar{b} = 0$ in $\mathbb{Z}_n$ even though neither $\bar{a}$ nor $\bar{b}$ is zero.

($\Leftarrow$) If p is a prime, $\mathbb{Z}_p$ is a domain

$\bar{a} \cdot \bar{b} = 0$ in $\mathbb{Z}_p$

$\Rightarrow a \cdot b$ is divisible by p

$\Rightarrow p \mid a$ or $p \mid b$

$\Rightarrow \bar{a} = 0$ or $\bar{b} = 0$

How to find inverse?

$\bar{a} \in \mathbb{Z}_p \Rightarrow a \in \mathbb{Z}$ s.t. $(a, p) = 1$

$(\bar{a} \neq 0) \Rightarrow \mu a + \nu p = 1$

$\Rightarrow \bar{\mu}\bar{a} = \bar{1}$ in $\mathbb{Z}_p$

2. $\mathbb{Z}$ is an integral domain which is not a field

3. If R is an integral domain, $R[X_1, \ldots, X_n]$ is also an integral domain.
(Use ind^n & show R is a domain $\Rightarrow R[X]$ is a domain)

Quotient field: Let R be an integral domain. Construct a field $Q(R)$ as follows.

Consider set of all pairs (p, q) with $q \neq 0$.
Def. an eq. rel^n whereby $(p, q) \sim (p', q')$ if $pq' = p'q$

Suppose $(p, q) \sim (p', q')$ & $(p', q') \sim (p'', q'')$

$\Rightarrow pq' = p'q$ $\quad\quad$ $\Rightarrow p'q'' = p''q'$

$\Rightarrow qp'q'' = qp''q'$

$\Rightarrow p'qq'' = q'qp''$

$\Rightarrow pq'q'' = q'qp''$

$\Rightarrow q'(pq'' - p''q) = 0$

$\Rightarrow pq'' = p''q$

$\Rightarrow (p, q) \sim (p'', q'')$

Denote eq. classes by $[\ ]$.

Add^n: $[p,q]+[p',q'] = [pq'+qp', qq']$

Multip^n: $[p,q]\cdot[p',q'] = [pp', qq']$

One checks that these are well defined.

This defines a ring structure on $Q(R)$

$\exists$ inj. homomp. $\quad R \hookrightarrow Q(R)$

$x \mapsto [x,1]$

In particular, id. elem. of $Q(R)$ is $[1,1]$

Inverse: $[p,q]^{-1} = [q,p]$ (if $p \neq 0$)

universal ppt.

Given a field F & an inj. homomp. $\varphi : R \to F$, $\exists!$ ring homomp. $Q(R) \xrightarrow{\bar{\varphi}} F$ s.t the diagram commutes

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & F \\ \downarrow & \nearrow_{\bar{\varphi}} & \\ Q(R) & & \end{array}$$

Def: $\bar{\varphi}[p,q] = \dfrac{\varphi(p)}{\varphi(q)}$

Rem: 1. $Q(R)$ is the smallest field containing R.

2. If R is a field, $\exists$ a natural isomp.
$R \simeq Q(R)$

$\because [p,q] \in Q(R)$

$[p,q] \sim [p/q, 1] \in R$

$\Rightarrow$ Map is surj.

eg: 1. $Q(R[X]) = \left\{ \frac{f(x)}{g(x)} \; ; \quad f(x), g(x) \in R[X] \;\&\; g(x) \neq 0 \right\}$

2. $\mathbb{Z} \subset R \subset \mathbb{Q}$

$R = \left\{ \frac{a}{2^n} \; ; \quad a \in \mathbb{Z}, \; n \in \mathbb{Z}_{>0} \right\}$

$Q(\mathbb{Z}) = Q(R) = Q(\mathbb{Q}) = \mathbb{Q}$

3. $R[X,Y] \subset Q(R[X])[Y] \subset Q(R[X,Y])$

Ideal : R - ring

An ideal in R is a subset $I \subset R$ s.t.

1. I is a subgp. of $(R,+)$
2. Given $x \in I$, $y \in R$, $xy \in I$

1 may not belong to I.

Examples

1. R: any ring
   $\{0\}$ is an ideal
   R is an ideal

2. $R = \mathbb{Z}$
   For any $n \in \mathbb{Z}$, $n\mathbb{Z}$ defines an ideal.

Converse is also true.
Let $I \subset \mathbb{Z}$ be an ideal.
Let $n \in \mathbb{Z}_{\geq 0}$ be the smallest natural no. in I.

Claim: $I = (n) = n\mathbb{Z}$
(generated by n)

$\therefore$ any subgp. of $\mathbb{Z}$ is of the form $n\mathbb{Z}$.

3. Let R be any ring. But S be any subset.

Consider the ideal I_S to be the coll. of elems. in R of the type

$$I_S = \sum_{\text{finite}} a_i x_i \quad , \quad a_i \in R, \; x_i \in S$$

$$\underbrace{y}_{\in R} \cdot \underbrace{\sum a_i x_i}_{\in I_S} = \underbrace{\sum (y \cdot a_i)\, x_i}_{\in I_S}$$

Given any ideal $I \subset R$, taking $I = S$, it follows that $I_S = I$

Hence, every ideal is generated this way.

4. Let $f: R \to R$ be a ring homomp.
Then $\ker(f) = \{a \in R : f(a) = 0\}$ is an ideal in R.

Pf: Clearly $\ker(f)$ is a subgp. of $(R, +)$

Let $x \in \ker(f)$, $a \in R$

$$f(ax) = f(a)\underbrace{f(x)}_{0} = 0$$

$ax \in \ker(f)$

Every ideal arises from kernel of some ring homomp.

5. $\mathbb{R}[X_1, \ldots, X_n]$
$I = (X_1, \ldots, X_n)$ $\quad S = \{x_1, \ldots, x_n\}$

I consists of all poly. whose const. term is 0.

6. X: metric sp. , $p \in X$

$\mathcal{C}(X)$: cont. fn^{n}s on X

$M_p = \{$ all cont. fn^{n}s vanishing at $p \in X\}$

M_p is an ideal.

Quotient

$(R, +, \cdot)$: ring

$I \subset R$: ideal

Consider the quotient ab. gp. R/I

Def. multip^n on R/I by

$$(a+I)\cdot(b+I) = ab + I$$

Well-definedness: Let $a', b' \in I$ s.t $a'-a \in I$ & $b'-b \in I$

$a' = a+x$, $b' = b+y$, $x, y \in I$

$$a'b' = (a+x)(b+y) = ab + \underbrace{ay + bx + xy}_{\in I}$$

$$\Rightarrow \quad ab' - ab \in I$$

The quotient map $R \xrightarrow{\varphi} R/I$ is a ring homomp.

$$a \longmapsto a+I$$

$$a+b \longmapsto a+b+I = (a+I)+(b+I)$$

$$ab \longmapsto ab+I = (a+I)\cdot(b+I)$$

The kernel of φ is clearly I.

Thm: Let $f: R \to R'$ be a surjective ring homomp. with kernel I. Then f factors through an isomp. $\bar{f}: R/I \to R'$ s.t. the following diagram commutes

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ \downarrow & \nearrow_{\bar{f}} & \\ R/I & & \end{array}$$

Pf: Def. $\bar{f}(a+I) = f(a)$

This is well-defined.

$\bar{f}$ is a ring homomp. as f is a ring homomp.

Rem: If $I \subset R$ is an ideal & I contains a unit, then $I = R$.

$\because$ If unit $u \in I \Rightarrow u \cdot u^{-1} \in I \Rightarrow 1 \in I \Rightarrow R = I$

Prime ideal: A proper ideal $I \subset R$ is called a prime ideal if whenever $x, y \in R$ s.t $xy \in I$, $x \in I$ or $y \in I$

Maximal ideal: A proper ideal $I \subset R$ is called a maximal ideal if R does not contain a bigger proper ideal.

Thm: $I \subset R$ ideal. Then

1. I is a prime ideal iff R/I is an integral domain

2. I is a maximal ideal iff R/I is a field.

Pf: 1. Suppose $I \subset R$ is a prime ideal.
Consider R/I. Let $\bar{x}, \bar{y} \in R/I$ s.t $\bar{x} \cdot \bar{y} = 0$

$\Rightarrow x \cdot y \in I \Rightarrow x \in I$ or $y \in I$

$\Rightarrow \bar{x} = 0$ or $\bar{y} = 0$

Sim., converse can be checked.

2. Suppose I is a maximal ideal.
Consider R/I.
Let $\bar{0} \neq \bar{x} \in R/I$ be any elem.
Then $x \notin I$. But I is maximal.

$\Rightarrow I \subsetneq (I, x)$

$\therefore (I, x) = R$ ($\because$ I was maximal)

$\because 1 \in R \Rightarrow \exists\ a \in R,\ y \in I$ s.t $ax + y = 1$

$\Rightarrow \bar{a}\bar{x} = 1$

$\therefore$ R/I is a field

Suppose R/I is a field.

Let $x \in R$ be s.t $x \notin I$

$\because x \notin I \Rightarrow \bar{x} \neq 0$

$\Rightarrow \exists\ \bar{y} \in R/I$ s.t $\bar{x} \cdot \bar{y} = \bar{1}$

$\Rightarrow xy - 1 = a \in I$

$\Rightarrow 1 = xy - a \in (I, x)$

$\because 1 \in (I, x) \Rightarrow (I, x) = R$

$\therefore$ I is maximal

Cor: Every maximal ideal is a prime ideal.

Examples :

1. R is an integral domain iff the (0) ideal is a prime ideal

2. $R = \mathbb{Z}$. Then $n\mathbb{Z}$ is a prime ideal iff $n = 0$ or a prime. It is a maximal ideal iff n is a prime.

By eg. 1, (0) is a prime ideal.
If $n \neq 0$, we have seen, $\mathbb{Z}_n$ is an integral domain iff it is a field iff n is a prime.

$\Rightarrow n\mathbb{Z}$ is prime iff it is maximal iff n is a prime

3. R: field
The only ideal in R are 0 & R.

Any homomp. $\varphi : R \to S$ is inj
(field) (non-zero ring)

$\ker(\varphi) = 0$ or R

But $1 \notin \ker(\varphi) \Rightarrow \ker(\varphi) = 0$

4. $R \xrightarrow{\varphi} R/I$ ring homomp.

$\exists$ bij. correspondence b/w ideals in R/I & ideals in R containing I given by $\varphi^{-1}(J) \leftarrow J \subset R/I$

Moreover its easy to show that if $I' \supset I$ is an ideal in R, $\varphi(I')$ is an ideal in R/I.

Moreover if I' is prime, $\varphi(I')$ is maximal.

$$\begin{array}{ccc} R & \longrightarrow & R/I \\ \cup & & \cup \\ I' & \longrightarrow & \varphi(I') \\ \cup & & \\ I & \longrightarrow & 0 \end{array}$$

$I' = \varphi^{-1}(\varphi(I'))$.

If $\varphi(I') \subsetneq J$, then $I' \subsetneq \varphi^{-1}(J) = R$ ($\because I'$ is maximal)

Algebraically closed field:

A field k is said to be algebraically closed if every non-const. polynomial $f(x) \in k[X]$ has a root in k.

eg: $(\mathbb{C}, +, \cdot)$ - Fundamental Thm of Algebra

Thm: (Weak form of Hilbert's Nullstellensatz)
Let k be an alg. closed field. Then every maximal ideal in $R = k[X_1, \ldots, X_n]$ is of the form $(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$ for some $(a_1, \ldots, a_n) \in k^n$

$$k^n \leftrightarrow \begin{pmatrix} \text{Maximal ideals} \\ \text{in } R \end{pmatrix}$$

Pf: ($\Rightarrow$) Out of scope

($\Leftarrow$) Fix $(a_1, \ldots, a_n) \in k^n$

$$\begin{aligned} k[X_1, \ldots, X_n] &\xrightarrow{\varphi} k \\ x_i &\longmapsto a_i \end{aligned}$$

The kernel of φ is generated by

$(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$

$$R/(x_1 - a_1, \dots, x_n - a_n) \xrightarrow{\sim} k$$

$\Rightarrow (x_1 - a_1, \dots, x_n - a_n)$ is maximal.

eg: Not true for fields which are not algebraically closed

$k = \mathbb{R}$

$I = (1 + x^2)$

$$\mathbb{R}[X] \xrightarrow{\varphi} \mathbb{C}$$

$$\alpha \longmapsto \alpha \qquad \alpha \in \mathbb{R}$$

$$x \longmapsto i$$

$$1 + x^2 \longmapsto 0$$

φ descends to a homomp.

$$\overline{\varphi} : \frac{\mathbb{R}[X]}{(1 + x^2)} \longrightarrow \mathbb{C}$$

Claim: $\bar{\varphi}$ is an isomp.

Any elem. in $\mathbb{R}[X]/(1+x^2)$ is uniquely equiv. to an elem. of the form $a_0 + a_1\bar{x}$ $(\because \bar{x}^2 = -1)$

But, $\bar{\varphi}(a_0 + a_1\bar{x}) = a_0 + a_1 i = 0$ iff $a_0 = a_1 = 0$

So, $(1+x^2)$ is a maximal ideal in $\mathbb{R}[X]$.

Thm: Every ring has a maximal ideal.
If a ring has a unique maximal ideal, we call it a local ring.

5. k : field

$R = k[[X]]$

Units of R are power series of the form

$a_0 + a_1 x + a_2 x^2 + \dots$ with $a_0 \neq 0$.

$= a_0(1+p)$, $p = a_0^{-1}(a_1 x + a_2 x^2 + \dots)$

$$(a_0(1+p))^{-1} = \frac{1}{a_0(1+p)} = a_0^{-1}(1 + p + p^2 + \dots)$$

$\therefore (x)$ is the unique maximal ideal in $k[[X]]$.

Hence, $k[[X]]$ is a local ring. ($\because$ others contain units)

Extension & contraction of Ideals

$\varphi : R \to S$ ring homomorp.

$I \subset R$ ideal

Def. I^e (extended) to be the ideal in S generated by $\varphi(I)$.

Sim., given an ideal $J \subset S$, define J^c (contracted) $= \varphi^{-1}(J) \subset R$

Ex: Prove that $I^{ec} \supseteq I$ & $J^{ce} \subseteq J$

Give examples where these inclusions are strict.

Rem: $k \subset f$ is an inclusion of fields, then f becomes a vector sp. over k.

Principal Ideal Domain :

A ring is called a principal ideal domain (PID) if it is an integral domain in which every ideal is generated by a single elem.

eg :

1. Any field

2. $\mathbb{Z}$ – every ideal is (n)

3. $k[X]$ for a field k.

Let $I \subset k[X]$ be an ideal.
Let $f \in I$ be a poly. of smallest degree

Claim : $I = (f)$

If not, let $g \in I$ s.t $g \notin (f)$
By division algorithm, $g = fh + h'$, where
which is a contd^n to degree $h' <$ degree h
the choice of f.

4. $k[[X]]$

non-eg:

$k[X_1, \dots, X_n]$ if $n \geq 2$ not a PID.

$I = (X_1, \dots, X_n)$ is not principal.

If $I = (f) \Rightarrow f \mid X_i \ \forall i$

$\Rightarrow f \in k^*$ → Contd^n

(generates unit ideal)

Euclidean domain: An int. domain R is called a Euclidean domain if $\exists\, d : R \setminus \{0\} \to \mathbb{Z}$ s.t

1. $d(ab) \geq d(a) \ \forall a, b$
2. Given $a, b \in R$, $\exists\, p, r \in R$ s.t $a = bp + r$ s.t either $r = 0$ or $d(r) < d(b)$

eg: 1. $R = \mathbb{Z}$; $d(a) = |a|$

2. $R = \mathbb{Z} + i\mathbb{Z}$

$d(a + ib) = a^2 + b^2$

Obs: Every ED is a PID.

R : ED

$I \subset R$ ideal

$(f \neq 0)$

Let $f \in I$ be an elem. s.t $d(f)$ is the smallest possible. Then $I = (f)$

Converse is not true i.e ∃ PID which are not ED.

Ppⁿ: In a PID, every non-zero prime ideal is maximal.

Pf: R : PID

P : Prime ideal

$$P \subsetneq M \subsetneq R$$
$$= (a) \quad = (b)$$

$a = bu \quad (\because b \notin P,\ u \in P)$

$\Rightarrow a = b(ax)$

$\Rightarrow bx = 1$

$\Rightarrow (b) = R$

Rem: $k[X, Y]$

(x) is prime, but not maximal

R: int. domain

Irreducible elem.: An elem. $a \in R$ is called reducible if a is not a unit & when $a = bc$, either b is a unit or c is a unit.

p is called prime if whenever $p \mid bc$, either $p \mid b$ or $p \mid c$.

Lem: Prime elem. generates a prime ideal. (& conversely)

Pf: $p \in R$ be prime.

$I = (p)$

If $ab \in I \Rightarrow ab = px \Rightarrow p \mid ab$

$\Rightarrow p \mid a$ or $p \mid b$

If $p \mid a \Rightarrow a \in I$, else $p \mid b \Rightarrow b \in I$

Prime $\Rightarrow$ Irreducible

If $p \in R$ is prime.

Suppose $p = ab \Rightarrow p|a$ or $p|b$

Suppose $p|a$. But $a|p$

In an int. domain, $x|y$ & $y|x \Rightarrow x = y \cdot (\text{unit})$ *

$\therefore$ $p = au$ $(u : \text{unit})$

$\Rightarrow b = u$

$\therefore$ p is irreducible

Converse is <u>not</u> true

* $y = cx$, $x = yd \Rightarrow y = ycd \Rightarrow cd = 1$

$\because$ c & d are units

$\therefore$ $y = x \cdot (\text{unit})$

$R = \mathbb{Z}[\sqrt{-5}] = \{ a + b\sqrt{-5} : a, b \in \mathbb{Z} \}$

$(1+2\sqrt{-5})(1-2\sqrt{-5}) = 21 = 3 \cdot 7$

$\Rightarrow (1+2\sqrt{-5})$ divides 3.7 but <u>not</u> 3 or 7.

Hence <u>not</u> prime.

But, $(1+2\sqrt{-5})$ is irreducible in $\mathbb{Z}[\sqrt{-5}]$

<u>Unique Factorization Domain</u> :

A int. domain R is called a UFD if every elem $a \in R$ can be expressed <u>uniquely</u>* as a prod. of irreducible elems.

$a = a_1 \dots a_r$
$= b_1 \dots b_s$
} product of irreducibles

Then $r = s$ & for each a_i, $\exists\, b_j$ s.t $b_j = a_i \cdot (\text{unit})$

* $a = bc = (bu)(u^{-1}c)$, u : unit

i.e uniqueness upto units

Thm: R : int. domain. Suppose

1. Every elem. $a \in R$ can be written as prod. of irreducibles
2. Irreducible $\Rightarrow$ Prime

Then R is a UFD.

Thm: (E.D $\Rightarrow$ PID) $\Rightarrow$ UFD

In a UFD, every irreducible elem. is prime.

R : UFD, p : irred. elem.

$ab \in (p) \Rightarrow ab = px$

$\Rightarrow \underbrace{(a_1 \cdots a_r)(b_1 \cdots b_s)}_{\text{irred.}} = px$

$\Rightarrow a_i = p\,\#$ or $b_j = p\,\#$

$\Rightarrow a \in (p)$ or $b \in (p)$

Examples:

1. A field is a UFD.

2. If R is a UFD, $R[X]$ is a UFD.

3. $\mathbb{Z}[\sqrt{5}] \simeq \frac{\mathbb{Z}[X]}{(x^2+5)}$ is not a UFD (has an irred. elem. which is not prime)

4. Quotient of a UFD is not necessarily a UFD.
$$\frac{k[X,Y,Z,W]}{(XY-ZW)}$$

$\bar{X}\bar{Y} = \bar{Z}\bar{W}$.

$\bar{X}, \bar{Y}, \bar{Z}, \bar{W}$ are all irred.

Eisenstein's Criterion

R: UFD, $p \in R$: prime elem.

Let $f = a_0 + a_1 x + \dots + a_n x^n \in R[X]$ s.t

$p \mid a_0, p \mid a_1, \dots, p \mid a_{n-1}, p \nmid a_n$ & $p^2 \nmid a_0$.

Then f is irreducible.

Cor: Fix a prime no. p.

$X^n - p \in \mathbb{Z}[X]$ is irreducible. $(n \geq 2)$

Chinese Remainder Thm

R: ring

$I_1, \dots, I_n$ ideals in R s.t $\underbrace{I_i + I_j}_{\text{ideal generated by } I_i \text{ \& } I_j} = R$ for any $1 \leq i \neq j \leq n$

Then $\exists$ isomp., $R/\bigcap_i^n I_i \simeq \prod_i^n R/I_i$

Finite Generation

A ring R is said to be Noetherian if every ideal $I \subset R$ is finitely generated i.e $I = (f_1, \dots, f_k)$

Thm: If R is Noetherian, $R[X]$ is Noetherian (Hilbert Basis Thm)

Quotient of Noetherian is Noetherian.

Thus, if k is any field,

$$\frac{k[X_1, \dots, X_n]}{I} \quad \text{is Noetherian}$$

(finitely generated k-alg.

(Subring of Noetherian is <u>not</u> necessarily Noetherian)