1. Groups

1.1 Notations

- numbers : $\mathbb{N}$. $\mathbb{Z}$ $\mathbb{Q}$ (rational) $\mathbb{R}$ (real) $\mathbb{C}$ $\mathbb{Z}_n$ (set of int. module n)

- matrices : For $n \in \mathbb{N}$, an $n \times n$ matrix over $\mathbb{R}$. is an $n \times n$ array

$$A = [a_{ij}] = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ a_{n1} & \cdots & & a_{nn} \end{bmatrix} \quad \text{with } a_{ij} \in \mathbb{R}. \quad 1 \le i, j \le n.$$

addition : $A + B = [a_{ij} + b_{ij}]$

multiplication : $AB = [c_{ij}]$ $\quad c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$

1.2 Groups

- def : Group.

Let G be a set and $*$ be an operation on $G \times G$, we say $G = (G, *)$ is a group if it satisfies:

1) Closure : if $a, b \in G$. then $a * b \in G$
2) Associativity : if $a, b, c \in G$. then $a * (b * c) = (a * b) * c$.
3) Identity : $\exists e \in G$. s.t. $a * e = a = e * a$ for all $a \in G$.
4) Inverse : $\forall a \in G$. $\exists b \in G$. s.t. $a * b = e = b * a$ $\quad$ b : inverse of a

- def. abelian group 交换的 ·

G is abelian if $a * b = b * a$ for all $a, b \in G$

- prop 1.1. Let G be a group and $a \in G$

(1) The identity of G is unique.

(2) The inverse of a is unique.

proof : (1) if e_1 & e_2 are both identities, then $e_1 = e_1 * e_2 = e_2$

(2) if b_1 & b_2 are both inverse of a, then $b_1 = b_1 * a * b_2 = b_2$

ex: The set $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ all abelian groups.
where the additive identity is 0 and the additive inverse of an element r is $(-r)$.

For a set S, let S^* denote the subset of S containing all elements with multiplicative inverse. Then $(\mathbb{Q}^*,\cdot)$ $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$ are abelian groups.

ex. The set $(M_n(\mathbb{R}),+)$ is an abelian group. where the additive identity is $\mathbb{0}$ and the additive inverse of $M=[a_{ij}]$ is $-M=[-a_{ij}]$

The set $(M_n(\mathbb{R}),\cdot)$ is not an abelian group since not all matrix is invertible.

ex. Let G & H be groups. Their direct product is the set $G\times H$ with component-wise operation defined by $(g_1,h_1)*(g_2,h_2)=(g_1*_G g_2, h_1*_H h_2)$

$G\times H$ is a group. identity (e_G,e_H). inverse: $(g,h)^{-1}=(g^{-1},h^{-1})$

By induction: $G_1,G_2,\cdots,G_n$ are groups $\Rightarrow$ $G_1\times G_2\times\cdots\times G_n$ is a group

Notation: Given group G. $g_1,g_2\in G$. $g_1*g_2=g_1g_2$. identity by 1.

inverse of g : g^{-1}

define $g^n=g*\cdots*g$. $g^{-n}=(g^{-1})^n$ $g^0=1$

- prop 1.2 Let G be a group. $g,h\in G$. we have

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

(2) $(gh)^{-1}=h^{-1}g^{-1}$

(3) $g^n*g^m=g^{n+m}$ for all $n,m\in\mathbb{Z}$

(4) $(g^n)^m=g^{nm}$ for all $n,m\in\mathbb{Z}$

proof. (2) $(gh)(h^{-1}g^{-1})=g(hh^{-1})g^{-1}=gg^{-1}=1=(gh)(hg)^{-1}$

* $(gh)^n=g^nh^n$ 不成立 matrix

- prop 1.3 Let G be a group and $g, h \in G$. Then

(1) They satisfy left & right cancellation more precisely.

- $gh = gf \Rightarrow h = f$
- $hg = fg \Rightarrow h = f$

(2) Given $a, b \in G$. $ax = b$. $ya = b$ have unique solution for $x, y \in G$

proof. (1) $gh = gf$

$g^{-1}gh = g^{-1}gf$ (by left cancellation)

$h = f$

(2) let $x = a^{-1}b$. $\Rightarrow ax = a(a^{-1}b) = (aa^{-1})b = b$.

if u is another solution, then $au = b = ax \Rightarrow u = x$

similarly, $y = ba^{-1}$ is also a unique solution.

1.3 Symmetric Groups

多边形

- def. permutation of Ω. S_Ω

Given a non-empty set of Ω, a permutation of Ω is a bijection from Ω to Ω. The set of all permutations of Ω is denoted by S_Ω.

ex. Consider $\Omega = \{1, 2, 3\}$ which has six different permutations

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

indicate the bijection: 每个 element 一一对应

$\sigma: \{1, 2, 3\} \to \{1, 2, 3\}$ with $\sigma\{1\}=1$. $\sigma\{2\}=3$. $\sigma\{3\}=2$.

* To consider the order of general S_n for $\sigma \in S_n$, we have n choices for $\sigma(1)$

- def. symmetric group. S_n

The permutation of set X form group S_X. If $X = \{1, 2, \cdots, n\}$.
We can write S_n instead of S_X.

S_n is · symmetric group. · set of all permutations of n elements $(=n!)$

- prop 1.4 $|S_n| = n!$ → symmetric group in size (S_n is a group with $n!$ elements)

Given $\sigma, \tau \in S_n$, we can compose them to get a third element $\sigma\tau$.
where $\sigma\tau : \{1, 2, \cdots, n\} \to \{1, 2, \cdots, n\}$. $x \mapsto \sigma(\tau(x))$

Since both σ & τ are bijection. so is $\sigma\tau$.

ex. $\sigma = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$ $\tau = \begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$

$\sigma\tau(1) = \sigma(\tau(1)) = \sigma(2) = 4$
$\sigma\tau(2) = \sigma(\tau(2)) = \sigma(4) = 2$

$\sigma\tau = \begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}$ $\tau\sigma = \begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$ $\Rightarrow$ $\sigma\tau \neq \tau\sigma$

- def. converse permutation

The identity permutation. ε is defined as $\varepsilon(a)=a$. $\forall a \in \{1, \dots, m\}$.

Then for any $\sigma \in S_n$. we have $\sigma\varepsilon = \sigma = \varepsilon\sigma$

Finally, for $\sigma \in S_n$. Since it is a bijection. there exist a unique bijection $\underline{\sigma^{-1} \in S_n}$

$\sigma^{-1}(x) = y \iff \sigma(y) = x$ converse permutation of σ

$\sigma^{-1}\sigma = \sigma\sigma^{-1} = \varepsilon$

ex. the inverse $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$ is $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$

- prop 1.5. 1). $\sigma, \tau \in S_n$. $\sigma\tau \in S_n$

2) $\sigma(\tau\mu) = (\sigma\tau)\mu$ (相当于 associativity)

3) There exist $\varepsilon \in S_n$. s.t $\sigma\varepsilon = \sigma = \varepsilon\sigma$ (相当于 identity)

4) $\forall \sigma \in S_n$. $\exists\, \sigma^{-1} \in S_n$. s.t $\sigma^{-1}\sigma = \sigma\sigma^{-1} = \varepsilon$

S_n is a group. → symmetric group of deg n

Q. Write down all the rotations and reflection of an equilateral triangle.

方法: represent element in a permutation in a cycle.

cycles are disjoint if they have no numbers in common

σ can be composed to 4 cycles $\underline{(1\ 3\ 7\ 2)\ (4\ 6)\ (5\ 9\ 8)\ (10)}$

- theorem 1.6 (Cycle decomposition Theorem)

If $\sigma \in S_n$ with $\sigma \neq \varepsilon$. Then σ is a product of disjoint cycles of length at least 2.

每个cycle中的数只会对应到唯一的数，且在本cycle中

The factorication is unique up to the order of factors.

* S_n 中的每个 permutation 可以被视为 permutation in S_{n+1} by fixing the number $n+1$

$(1, 2, 3) \to (1, 2, 3)$ equivallent to $(1, 2, 3, 4) \to (1, 2, 3, 4)$

1.4 Cayley Tables

- def. Cayley Table

Given $x, y \in G$, the product xy is the entry of the table in the row corresponding to x and the column corresponding to y. Such a table is called Cayley Table

ep. $(\mathbb{Z}_2, +)$

$\mathbb{Z}_2$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$(\mathbb{Z}^*, *)$

$\mathbb{Z}^*$	1	-1
1	1	-1
-1	-1	1

如果 cayley table symmetric $\downarrow$ 则里面是 abelian

- Cancellation Rule

the entry in each row/column are all distinct.

- def. isomorphic 同构 $\cong$

label Cayley table 中的 index. 发现两个 table 构成相同 (能编的)

ep. 如果将 1 换成 $[0]$. -1 换成 $[1]$. $\mathbb{Z}^*$ & $\mathbb{Z}_2$ in Cayley Table 依然不变 $\downarrow$ isomorphic $\mathbb{Z}^* \cong \mathbb{Z}_2$

- def. Cyclic Group. C_n (由 power 的形式组成)

The cyclic group of order n is $C_n = \{1, a, a^2, \cdots, a^{n-1}\}$. with $a^n = 1$ and $a, a^2, \cdots, a^{n-1}$ distinct.

写作 $C_n = \langle a : a^n = 1 \rangle$ $\rightarrow$ generator of C_n

C_n	1	a	$\cdots$	a^{n-2}	a^{n-1}
1	1	a	$\cdots$	a^{n-2}	a^{n-1}
a	a	a^2	$\cdots$	a^{n-1}	1
a^2	a^2	a^3	$\cdots$	1	a
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
a^{n-2}	a^{n-2}	a^{n-1}	$\cdots$	a^{n-4}	a^{n-3}
a^{n-1}	a^{n-1}	1	$\cdots$	a^{n-3}	a^{n-2}

$\leftarrow$ Cayley table of C_n

- prop 1.14. Let G be a isomorphism group. Then.

1) $|G| = 1 \Rightarrow G \cong \{1\}$

2) $|G| = 2 \Rightarrow G \cong C_2$

3) $|G| = 3 \Rightarrow G \cong C_3$

4) $|G| = 4 \Rightarrow G \cong C_4$ or $G \cong K_4 \cong C_2 \times C_2$

proof. 1) $|G| = 1 \Rightarrow G = \{1\}$

2) $|G| = 2 \Rightarrow G = \{1, g\}.\ (g \neq 1)$.

Cayley table: C_2

G	1	g
1	1	g
g	g	1

$\therefore G \cong C_2$

3) $|G| = 3 \Rightarrow G = \{1, g, h\}$ $(g \neq 1,\ h \neq 1,\ g \neq h)$

Cayley table: C_3

G	1	g	h
1	1	g	h
g	g	h	1
h	h	1	g

$\therefore G \cong C_3$

4) $|G| = 4 \Rightarrow G = \{1, f, g, h\}$ $(1, f, g, h$ not equal to each other$)$

Cayley table of G:

C_4	1	f	g	h
1	1	f	g	h
f	f	f^2	gf	hf
g	g	fg	g^2	hg
h	h	fh	gh	h^2

By Cancellation Rule, $gf \neq g \neq f$ $\therefore gf = 1$ or $gf = h$

case 1. $gf = 1$

C_4	1	f	g	h
1	1	f	g	h
f	f	h	1	g
g	g	1	h	f
h	h	g	f	1

$\leftarrow K_4$

case 2. $gf = h$

C_4	1	f	g	h
1	1	f	g	h
f	f	1	h	g
g	g	h	1	f
h	h	g	f	1

$\xrightarrow{\text{equivalent to}}$

$gh = hg = f$. $f^2 = g^2 = h^2 = 1$

C_4	1	f	g	h
1	1	f	f^2	f^3
f	f	1	f^3	f^2
g	f^2	f^3	1	f
h	f^3	f^2	f	1

C_4

C_4	1	f	g	h
1	1	f	g	h
f	f	g	h	1
g	g	h	1	f
h	h	1	f	g

K_4

Prove $K_4 \cong C_2 \times C_2$:

$C_2 = \{1, k\}$ $\quad k^2 = 1$

$C_2 \times C_2 = \{(1,k) \times (1,g)\}$

$C_2 \times C_2$	$(1,1)$	$(g,1)$	$(1,h)$	(g,h)
$(1,1)$	$(1,1)$ 1	$(g,1)$ g	$(1,h)$ h	(g,h) f
$(g,1)$	$(g,1)$	$(\cancel{g^2},1)$	(g,h)	$(\cancel{g^2},h)$
$(1,h)$	$(1,h)$	(g,h)	$(1,\cancel{h^2})$	$(g,\cancel{h^2})$
(g,h)	(g,h)	$(\cancel{g^2},h)$	$(g,\cancel{h^2})$	$(\cancel{g^2},\cancel{h^2})$

2. Subgroups

2.1 Subgroup

- def. subgroup

  Let G be a group and $H \subseteq G$ be a subset of G.

  If H itself is a group, then we say H is a subgroup of G.

- Subgroup Test:

  Since G is a group, for $h_1, h_2, h_3 \in H$ then $h_1(h_2h_3) = (h_1h_2)h_3$.

  H is a subgroup of G $\Leftrightarrow$ 同时满足 ① $h_1, h_2 \in H \Rightarrow h_1h_2 \in H$
  ② $1_G \in H$
  ③ $h \in H \Rightarrow h^{-1} \in H$

  ep. Let G be a group. Then $\{1\}$, G are subgroups of G

  ep. We have a chain of groups $(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \subseteq (\mathbb{R}, +) \subseteq (\mathbb{C}, +)$

  ep. $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$
  ↳ special linear group of order n over $\mathbb{R}$.

  $$SL_n = (SL_n(\mathbb{R}), \cdot) = \{M \in M_n(\mathbb{R}) : \det(M) = 1\} \subseteq GL_n(\mathbb{R})$$

  subgroup test: ① $I \in SL_n(\mathbb{R})$
  ② Let $A, B \in SL_n(\mathbb{R}) \Rightarrow \det(AB) = \det(A)\det(B) = 1$
  ③ Let $A \in SL_n(\mathbb{R}) \Rightarrow \det(A^{-1}) = \frac{1}{\det(A)} = 1$

- def. center. $(Z(G))$

  Given a group G, we define centre of G to be $Z(G) = \{z \in G : zg = gz \ \forall g \in G\}$

  $Z(G) = G \Leftrightarrow G$ is abelian   centre 里的 element 能组成 G 的一个 subgp

- prop 2.1. Let H & K be subgroups of G.

  Then $H \cap K = \{g \in G : g \in H \text{ and } g \in K\}$ is also a subgroup of G

- prop 2.2. Finite subgroup test

If H is a finite non-empty subset of group G,

then H is a subgroup of G $\Leftrightarrow$ H is closed under its operation

proof: $(\Rightarrow)$ obvious

$(\Leftarrow)$ For $H \neq \emptyset$, let $h \in H$.

① $\because$ H is closed under its opertion

$\therefore$ $h, h^2, h^3, \cdots$ are all in H.

② $\because$ H is finite

$\therefore$ elements are not distinct. $h^n = h^{n+m}$

By cancellation. $h^m = 1$ $\therefore 1 \in H$.

③ $1 = h^{m-1} h \Rightarrow h^{-1} = h^{m-1}$ $h^{-1} \in H$.

By subgroup test, H is subgroup of G.

- prop 2.3. ① $1 \in Z(G)$

② $y, z \in Z(G)$ $yz \in Z(G)$

$\forall g \in G$. $(yz)g = y(zg) = y(gz) = (gy)z = g(yz)$

③ $z \in Z(G)$ $z^{-1} \in G$ $g \in G$. $z^{-1}g = (g^{-1}z)^{-1} = (zg^{-1})^{-1} = gz^{-1}$

ex. consider $(\mathbb{Z}, +)$. Since $k = \underbrace{1 + \cdots + 1}_{k \text{ 个 } 1}$. 1 is a generator of $(\mathbb{Z}, +)$.

similary -1 is a generator.

But if $k \neq \pm 1$. 1 cannot be obtained via scalar multiplication.

Let G be a group. $g \in G$. suppose $\exists k \in \mathbb{Z}$. $k \neq 0$. s.t $g^k = 1$.

then $g^{nk} = (g^k)^n = 1$ $\forall n \in \mathbb{Z}$. Assume $k > 0$

By the well ordering principle, there exists a smallest possible integer n s.t. $g^n = 1$

2.2 Alternating Groups

- def. transposition

A transposition $\sigma \in S_n$ is a cycle (i.e. $\sigma = (a\ b)$ with $a, b \in \{1, \cdots, n\}$, $a \neq b$)

ep. Consider permutation $(1\ 2\ 4\ 5) \in S_5$

Also, the composition $(1\ 2)(2\ 4)(4\ 5)$ can be computed as:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \\ 1 & 4 & 3 & 5 & 2 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$$

Thus $(1\ 2\ 4\ 5) = (1\ 2)(2\ 4)(4\ 5)$ joint

Also, the factorization into transpositions are not unique.

$(1\ 2\ 4\ 5) = (1\ 2\ 4)(4\ 5)$

- Thm 2.3 Parity Theorem

If a permutation σ has 2 factorizations. $\sigma = \gamma_1 \cdots \gamma_r = \mu_1 \cdots \mu_s$ where each γ_i & μ_j is a transposition then $r \equiv s \pmod 2$

$3 \equiv 1 \pmod 2$

- def. permutation

A permutation σ is even (or odd) if it can be written as product of an even (or odd) number of transposition.

ep. 上面 example 中, permutation σ is odd (拆成3个 subgp 相乘)

$(1\ 2)(3\ 4)(5\ 6)$ 这个 permutation 里有3个 transposition

* by theo 2.3. a permutation is either even or odd.

- Thm 2.4 For $n \geq 2$, let A_n denote the set of all even permutations in S_n.

\# transposition = even

1) $e \in A_n$ identity
2) $a, b \in A_n \Rightarrow ab \in A_n \quad a^{-1} \in A_n$
3) $|A_n| = \frac{1}{2} n!$

A_n is a subgroup of S_n. called "Alternating group of degree n"

A_n is a subgp of S_n.

ep. 1) $(1\ 2)$ 2) $a = (1\ 2)(3\ 4)$ $a^{-1} = (3\ 4)(1\ 2)$

2.3 Order of element

- Notation If G is a group and $g \in G$. denote $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$.

$x = g^m,\ y = g^n \in \langle g \rangle \quad (m, n \in \mathbb{Z}) \Rightarrow xy = g^{m+n} \in \langle g \rangle$

- prop 2.5 If G is a group. $g \in G$. then $\langle g \rangle$ is a subgroup of G

- def. cyclic group & generator.

Let G be a group and $g \in G$. $\langle g \rangle$ is the cyclic subgroup of G. generated by g.

If $G = \langle g \rangle$, for some $g \in G$. then G is a cyclic group and g a generator of G

ep. Consider $(\mathbb{Z}, +)$ Note that $\forall k \in \mathbb{Z}$. we can write $k = k \cdot 1$

Thus $(\mathbb{Z}, +) = \langle 1 \rangle$ Similarly $(\mathbb{Z}, +) = \langle -1 \rangle$ $(-k = k \cdot (-1))$

observe that $\forall n \in \mathbb{Z}$ with $n = \pm 1$. there exist no $k \in \mathbb{Z}$ s.t $k \cdot n = 1$

Thus, ± 1 are only generators of $(\mathbb{Z}, +)$

- def. order of g $o(g)$

Let G be a group. $g \in G$.

If n is the smallest positive integer st $g^n = 1$, then order of g is n $o(g) = n$

If no such n exist. then g has infinite order $o(g) = \infty$ 无法循环

- prop 2.6 Let G be a gp. $o(g) = n \in \mathbb{N}$ $k \in \mathbb{Z}$.

1) $g^k = 1 \Leftrightarrow n \mid k$

2) $g^k = g^m \Leftrightarrow k \equiv m \pmod{n}$

3) $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$ (elements all distinct)

proof: 1) ($\Leftarrow$) Let $n = qk$. $q \in \mathbb{Z}$.

$g^n = g^{qk} = (g^k)^q = 1^q = 1$

($\Rightarrow$) Let $n = qk + r$. $0 \le r < k$

$g^n = g^{qk+r} = g^r = 1$

$\because k$ is smallest pos int $g^k = 1$ $n = qk$ $k \mid n$

$\therefore r$ can only be 0

2) $g^{k-m} = 1$ (by cancellation law)

$\because n \mid k - m$ (by (1))

$\therefore k \equiv m \pmod{n}$

3) prove existence:

for $k \geq n$. $k = qn + r$. $(0 \le r \le n-1)$ $g^k = g^r \in \langle g \rangle$

prove unique:

$g^a = g^b$ $0 \le a, b \le n-1$

$g^{a-b} = 0 \iff a - b = 0$

$\because a - b < r$ $\therefore a = b$

- prop 2.7. Let G be a gp. $g \in G$. $o(g) = \infty$. $k \in \mathbb{Z}$.

1) $g^k = 1 \iff k = 0$

2) $g^k = g^m \iff k = m$

3) $\langle g \rangle = \{1, g, g^2, \cdots\}$ (elements all distinct)

proof: 1) ($\Leftarrow$) $g^0 = 1$

($\Rightarrow$) If $g^k = 1$. Assume $k > 0$

implies $o(g)$ is finite contradiction

2) $g^k = g^m$ $g^{k-m} = 1$

$k - m = 0$ (by (1))

- prop 2.8 Let G be a gp. $g \in G$. $o(g) = n \in \mathbb{N}$.

If $d \in \mathbb{N}$, then $o(g^d) = \frac{n}{\gcd(n,d)}$

$d \mid n \Rightarrow o(g^d) = \frac{n}{d}$

proof: Let $n_1 = \frac{n}{\gcd(n,d)}$ $d_1 = \frac{d}{\gcd(n,d)}$ $\gcd(n_1, d_1) = 1$

$(g^d)^{n_1} = (g^d)^{\frac{n}{\gcd(n,d)}} = (g^n)^{\frac{d}{\gcd(n,d)}} = 1$ $o(g^d) \mid n$

↓ Show n_1 is the smallest integer.

$(g^d)^r = 1$ $(r \in \mathbb{N})$.

$\because o(g) = n.$ $n \mid dr$ (prop 2.6)

$\therefore dr = nq$ $(q \in \mathbb{Z})$

$\frac{d}{\gcd(n,d)} = \frac{n}{\gcd(n,d)} q$ $d_1 r = n_1 q$

$\because (d_1, n_1) = 1$ $n_1 \mid r$

$\therefore (g^d)^{n_1} = 1$

ep. $o(g) = 10$. $d = 2$. $o(g^2) = \frac{10}{\gcd(2,10)} = 5$

$e = g^{10}$ $(g^2)^5 = g^{10}$

2.4 Cycle groups

- def. Cyclic group

  If $G = \langle g \rangle$ for some $g \in G$. Then G is a cyclic group.

- prop 2.9 Every cyclic group is abelian.

  proof: For $a, b \in G$, we have $a = g^m$ and $b = g^n$ for some $m, n \in \mathbb{Z}$.

  $$ab = g^m \cdot g^n = g^{m+n} = g^{n+m} = g^n \cdot g^m = b \cdot a$$

  * The converse of prop 2.9 is not true

  eg. The Klein group $K_4 \cong C_2 \times C_2$ is abelian. but K_4 not cyclic.

- prop 2.10 Every subgroup of a cyclic group is cyclic

  proof. Let $G = \langle g \rangle$ be cyclic and H be a subgroup of G.

  - If $H = \{1\}$. then $H = \langle 1 \rangle$ is cyclic.
  - If $H \neq \{1\}$. then $\exists\, g^k \in H$. with $k \in \mathbb{Z}$. $\wedge$ $k \neq 0$.

  $\because$ H is group $\therefore$ $g^{-k} \in H$.

  Assume $k \in \mathbb{N}$. Let m be the smallest pos int. s.t. $g^m \in H$

  $\because g^m \in H$ $\therefore \langle g^m \rangle \subseteq H$.

  对于每个 $h \in H \subseteq G = \langle g \rangle$. 可写作 $h = g^k$ $(k \in \mathbb{Z})$

  $\because k = mq + r$ $(0 \leq r < m)$ by division algorithm

  $\therefore g^k = g^{k-mq} = (g^k)(g^m)^{-q} \in H$.

  $\because 0 \leq r < m$. $\wedge$ $r = 0$

  $\therefore m \mid k$ $g^k \in \langle g^m \rangle$. $\Rightarrow$ $H = \langle g^m \rangle$.

- prop 2.11. Let $G = \langle g \rangle$ be a cyclic group with $o(g) = n \in \mathbb{N}$.

  Then $G = \langle g^k \rangle \iff \gcd(k, n) = 1$.

  proof: by prop 2.8 $o(g^k) = \dfrac{n}{\gcd(n,k)} = n$.

— theo 2.12 Fundamental theorem of finite cyclic group.

Let $G = \langle g \rangle$ be a cyclic group of order $n \in \mathbb{N}$.

1) H is a subgroup $\Rightarrow$ $H = \langle g^d \rangle$ for some $d \mid n$. $\to |H| \mid n$

2) Conversely. $k \mid n \Rightarrow \langle g^k \rangle$ is the unique subgroup of G of order k.

proof. (1) by prop 2.10. H is cyclic. $H = \langle g^m \rangle$ for some $m \in \mathbb{N}$.

Let $d = \gcd(m, n)$

Claim $H = \langle g^m \rangle \subseteq \langle g^d \rangle$

$\hookrightarrow$ $\because d \mid m$ $\therefore m = kd$ $(k \in \mathbb{Z})$

$\therefore g^m = g^{kd} = (g^d)^k = \langle g^d \rangle$

$\therefore H = \langle g^m \rangle \subseteq \langle g^d \rangle$.

Claim $H = \langle g^d \rangle$

$\because d = \gcd(m, n)$ $\therefore \exists x, y \in \mathbb{Z}$. s.t $d = mx + ny$.

$\therefore g^d = g^{mx+ny} = (g^m)^x (g^n)^y = (g^m)^x \cdot 1^y \in \langle g^m \rangle$

cyclic gp of order 1

$\therefore \langle g^d \rangle \subseteq \langle g^m \rangle$

$\therefore H = \langle g^d \rangle$. $G = \langle g \rangle = \langle g^k \rangle$ $\gcd(k, n) = 1$

(2) By prop 2.8, the cyclic subgroup $\langle g^{\frac{n}{k}} \rangle$ is of order $\frac{n}{\gcd(n, \frac{n}{k})} = k$

To show uniqueness, let K be a subgroup of G which is of order k with $k \mid n$.

By (1). let $K = \langle g^d \rangle$ with $d \mid n$.

By prop 2.6. & 2.8. $k = |K| = o(g^d) = \frac{n}{\gcd(n, d)} = \frac{n}{d}$.

$\therefore d = \frac{n}{k}$ $K = \langle g^{\frac{n}{k}} \rangle$

2.5 Non-cyclic group

- def. subgroup of G generated by X.

Let X be a nonempty subset of a group G, and let

$\langle X\rangle = \{ x_1^{k_1}, x_2^{k_2}, \cdots, x_m^{k_m} : x_i \in X,\ k_i \in \mathbb{Z},\ m \geq 1 \}$.

denote the set of all products of powers of (non necessarily distinct) element of X.

$\because$ $1 = x_1 \in \langle X\rangle$ and $(x_1^{k_1}, \cdots, x_m^{k_m})^{-1} = x_m^{-k_m}$ $\quad x_1^{-k_1} \in \langle X\rangle$

$\therefore$ $\underline{\langle X\rangle}$ is a subgroup of G containing X.

ex. The Klein 4 group $K_4 = \{1, a, b, c\}$ $\quad a^2 = b^2 = c^2 = 1.$ $\quad ab = c.$

$\Rightarrow = \langle a, b : a^2 = 1 = b^2 \quad ab = ba\rangle$

ex. The symmetric gp of degree 3.

$S_3 = \{\varepsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ $\quad \sigma^3 = \varepsilon = \tau^2$ $\quad \sigma\tau = \tau\sigma^2$ $\quad$ (can take $\sigma = (1\ 2\ 3)$, $\tau = (1\ 2)$)

$\therefore S_3 = \langle \sigma, \tau : \sigma^3 = \varepsilon = \tau^2 \quad \sigma\tau = \tau\sigma^2\rangle$

σ, τ 可被 $\sigma, \tau\sigma$ 或 $\sigma, \tau\sigma^2$ … 代替

- def. dihedral group D_n

For $n \geq 2$. the dihedral group of order $2n$ is defined by

$D_{2n} = \{1, a, \cdots, a^{n-1}, b, ba, \cdots, ba^{n-1}\}$ where $a^n = 1 = b^2$. $aba = b$.

$= \langle a, b : a^n = 1 = b^2 \quad aba = b\rangle$

When $n=2$ or $n=3$, $D_4 \cong K_4$ $\quad D_6 \cong S_3$

3. Normal Subgroup

3.1 Homomorphisms and Isomorphisms

- def. homomorphism

Let G & H be gps. A mapping $\alpha: G \to H$ is homomorphism if:

$$\alpha(a *_G b) = \alpha(a) *_H \alpha(b) \quad \text{for all } a, b \in G.$$

To simplify notation. 写作 $\alpha(ab) = \alpha(a)\alpha(b) \quad \forall a, b \in G$

ex. consider the determinant map $\det: (GL_n(\mathbb{R}), \cdot) \to \mathbb{R}^*$ $A \mapsto \det(A)$.

$\because \det(AB) = \det(A)\det(B)$ $\quad \therefore$ mapping is HM.

- prop 3.1.

Let $\alpha: G \to H$ be a gp HM.

Then 1) $\alpha(e_G) = e_H$

2) $\alpha(g^{-1}) = \alpha(g)^{-1} \quad \forall g \in G$

3) $\alpha(g^k) = \alpha(g)^k \quad \forall g \in G,\ k \in \mathbb{Z}$

- def. isomorphism

Let G & H be gps. Consider $\alpha: G \to H$.

If α is HM. α is bijective. Then α is an isomorphism.

$① \Leftrightarrow ②$

① onto ② one-to-one $\quad$ G & H are isomorphic. $G \cong H$

- prop 3.2.

1) The identity map $G \to G$ is an IM.

2) $\sigma: G \to H$ is an IM. $\Rightarrow$ the inverse map $\sigma^{-1}: H \to G$ is also IM

3) $\sigma: G \to H$. $\tau: H \to K$ are IM, the composite map $\tau\sigma: G \to K$ is also IM

$\Rightarrow$ $\cong$ is an equivalent relation ex. Let $\mathbb{R}^+ = \{ r \in \mathbb{R} . \ r > 0 \}$.

Claim : $(\mathbb{R}, +)$ is isomorphic to $(\mathbb{R}^+, \cdot)$

Define $\sigma = (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ by $\sigma(r) = e^r$ where e is the exponential f'n.

* the exponential map $\mathbb{R} \to \mathbb{R}^+$ is bijection.

Also, $r, s \in \mathbb{R}$. $\sigma(r+s) = e^{r+s} = e^r \cdot e^s = \sigma(r)\sigma(s)$

Thus, σ is IM. $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$

ex. Claim $(\mathbb{Q}, +)$ is not isomorphic to $(\mathbb{Q}^*, \cdot)$

Suppose that $\tau : (\mathbb{Q}, +) \to (\mathbb{Q}^*, \cdot)$ is an IM.

Then τ is onto. $\Rightarrow \exists\, q \in \mathbb{Q}$. s.t $\tau(q) = 2$. 写作 $\tau(\frac{q}{2}) = a \in \mathbb{Q}$

$\because \tau$ is a HM.

$\therefore a^2 = \tau(\frac{q}{2})\tau(\frac{q}{2}) = \tau(\frac{q}{2} + \frac{q}{2}) = \tau(q) = 2$

contradicts the fact that $a \in \mathbb{Q}$.

$\therefore$ such τ doesn't exist $(\mathbb{Q}, +) \ncong (\mathbb{Q}^*, \cdot)$

3.2 Cosets & Lagrange's Theorem

- def. Left / right coset

Let H be a subgroup G. $a \in G$,

the right coset of H generated by a: $Ha = \{ha : h \in H\}$

the left coset of H generated by a: $aH = \{ah : h \in H\}$

$H1 = 1 = 1H$ $a \in Ha$ & $a \in aH$ Since $1 \in H$

* aH & Ha are not subgroups of G.

* $Ha \neq aH$ (若 G abelian, 则 $Ha = aH$)

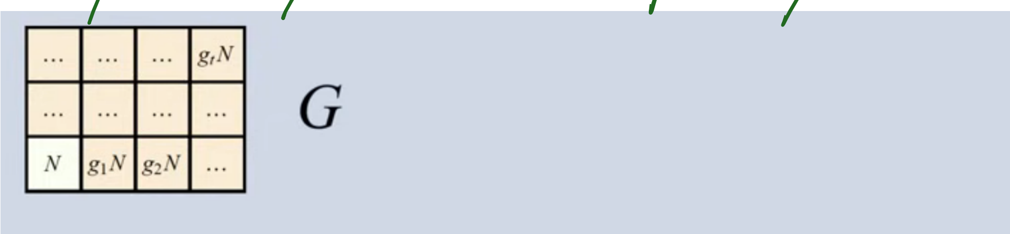
Group : G Subgroup: $N \subseteq G$

Use N to make cosets : $N, g_1N, g_2N, \dots$

- Do cosets always form a group? No.

For cosets act like a gp :

$x \cdot y \in (xN)(yN)$ i.e $(xN)(yN) = xyN$



G may *not* be abelian $\Longrightarrow$ left cosets may differ from right cosets

ep. $D_6 = D_{2\cdot 3} = \{I, a, a^2, b, ab, a^2b\}$ $a^3 = b^2 = I$. $ba = a^2b$

*	I	a	a^2	b	ab	a^2b
I	I	a	a^2	b	ab	a^2b
a	a	a^2	I	ab	a^2b	b
a^2	a^2	I	a	a^2b	b	ab
b	b	a^2b	ab	I	a^2	a
ab	ab	b	a^2b	a	I	a^2
a^2b	a^2b	ab	b	a^2	a	I

$H = \{I, b\} \subseteq D_6$.

left cosets of H:

$I \cdot H = \{I, b\}$

$a \cdot H = \{a, ab\}$

$a^2 \cdot H = \{a^2, a^2b\}$

left cosets of H:

$H \cdot I = \{I, b\}$

$H \cdot a = \{a, a^2b\}$

$H \cdot a^2 = \{a^2, ab\}$

- prop 3.3

Let H be a subgp of G. $a, b \in G$

1) $Ha = Hb \Leftrightarrow ab^{-1} \in H$

$Ha = H \Leftrightarrow a \in H$ (此时 $b=1$)

2) $a \in Hb \Rightarrow Ha = Hb$

3) either $Ha = Hb$ or $Ha \cap Hb = \emptyset$.

Thus the distinct right cosets of H forms a partition of G.

proof: (1) ($\Rightarrow$) If $Ha = Hb$. then $a = 1 \cdot a \in Ha = Hb$

$\therefore a = hb$ for some $h \in H$. $ab^{-1} = h \in H$

($\Leftarrow$) $\because ab^{-1} \in H$

$\therefore \forall h \in H \quad ha = h(ab^{-1})b \in Hb$

$\therefore Ha \subseteq Hb$

$\because ab^{-1} \in H \quad H$ is a subgp

$\therefore (ab^{-1})^{-1} = ba^{-1}$

$\therefore \forall h \in H, \quad hb = h(ba^{-1})a \in Ha$

$\therefore Hb \subseteq Ha$

So $Ha = Hb$

(2) If $a \in Hb$, then $ab^{-1} \in H$.

by (1), $Ha = Hb$

(3) case 1: $Ha \cap Hb = \emptyset$ obvious

case 2: $Ha \cap Hb \neq \emptyset$

$\Rightarrow \exists x \in Ha \cap Hb$

$\because x \in Ha \quad \therefore Ha = Hx$ (by (2))
$\because x \in Hb \quad \therefore Hb = Hx$ (by (2))

So $Ha = Hx = Hb$

- def. index

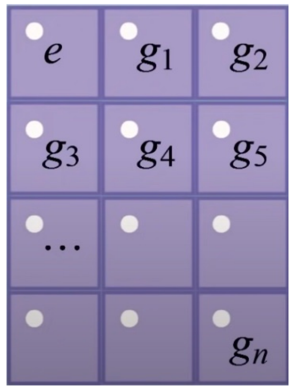
  by prop 3.3. G can be written as a disjoint union of right cosets of H.

  index $[G:H]$ = # distinct right / left coset of H in G.

- Lagrange Theorem.

  Let H be a subgroup of a finite group G $\Rightarrow |H| \mid |G|$. $[G:H] = \frac{|G|}{|H|}$

proof:



G split into non-overlapping left cosets: $H, g_1H, g_2H, \cdots$

$gh_1 = gh_2 \Rightarrow g^{-1}(gh_1) = g^{-1}(gh_2)$

$\Rightarrow h_1 = h_2$ (所以是non-overlap的) prop 3.3

each coset has size $|H| = d$

Let $k = [G:H]$. k: # cosets.

$\therefore d \cdot k = n \Rightarrow d \mid n \Rightarrow |H| \mid |G|$

proof summary: 1. Pick a subgroup of G: H.

2. Cover G with cosets

3. Cosets do not overlap

ex. $|G| = 323 = 17 \times 19$.

divisors of 323: 1. 17. 19. 323.

possible subgp orders: 1. 17. 19. 323

standard subgp: G ($|G| = 323$) $\{e\}$ ($|\{e\}| = 1$)

other subgps: order = 17 or 19 ＊但不是一定存在

ex. $|A_4| = 12$.

divisors of 12: 1, 2, 3, 4, 6, 12

subgps: # subgp with order 1 = 1 # order 2 = 3 # order 3 = 4

order 4 = 1 # order 6 = 0 # order 12 = 1

- Cor 3.5

1) G is a finite group. $g \in G \Rightarrow o(g) \mid |G|$

2) G is a finite gp with $|G| = n \Rightarrow \forall g \in G.\ g^n = 1.$

ex. For $n \in \mathbb{N}$. with $n \geq 2$. let $\mathbb{Z}_n^*$ be the set of (multiplicative) invertible elements in $\mathbb{Z}_n$.

Let the Euler's ϕ-function $\phi(n)$. denote the order of $\mathbb{Z}_n^*$.

i.e. $\phi(n) = \#\{[k] : k \in \{0, 1, 2, \cdots, n-1\}, \gcd(k, n) = 1\}$.

as a direct consequence of cor 3.5. we suppose that if $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$. $\leftarrow$ Euler's Theorem.

If $n = p$. (prime), then Euler's theorem implies Fermat's little theorem. which states that $a^{p-1} \equiv 1 \pmod{p}$

By constructing Cayley's table. we show that $|G| = 2 \Rightarrow G \cong C_2$
$|G| = 3 \Rightarrow G \cong C_3$.

- Cor 3.6

G is a group with $|G| = p$. (prime) $\Rightarrow G \cong C_p$. (cyclic gp order p)

proof: Let $g \in G$ with $g \neq 1$. by Cor 3.5. $o(g) \mid p$.

$\because g \neq 1$. $p \in$ prime. $\therefore o(g) = p$.

$\because$ by prop 2.6. $|\langle g \rangle| = o(g) = p$. So. $G = \langle g \rangle \cong C_p$

- Cor 3.7

Let H & K be finite subgroups of G.

$\gcd(|H|, |K|) = 1 \Rightarrow H \cap K = \{1\}$

proof: By prop 2.1. $H \cap K$ is a subgp of H & K.

By lagrange theorem. $|H \cap K| \mid |H|$. $|H \cap K| \mid |K|$.

$\therefore |H \cap K| \mid \gcd(|H|, |K|)$

i.e $|H \cap K| \mid 1$. $\Rightarrow H \cap K = \{1\}$.

3.3 Normal Subgroup

If H is a subgroup of a group G. $g \in G$. then gH & Hg are not always the same.

- def. normal $\triangleleft$

Let H be a subgroup of G.

If $gH = Hg$ $\forall g \in G$, then H is normal in G. $H \triangleleft G$

ex. $\{1\} \triangleleft G$. $G \triangleleft G$

ex. The center $Z(G)$ of G.

$Z(G) = \{z \in G : zg = gz$ for all $g \in G\}$ is an abelian subgroup of G.

By definition. $Z(G) \triangleleft G$.

↳ Every subgroup of $Z(G)$ is normal in G.

ex.

$\mathbb{Z}$	"Integers mod 5"	
	$r = 0:\ \{\ldots -15, -10, -5, 0, 5, 10, 15 \ldots\}$	$5\mathbb{Z}$ ← normal subgp
	$r = 1:\ \{\ldots -14, -9, -4, 1, 6, 11, 16 \ldots\}$	$1+5\mathbb{Z}$
	$r = 2:\ \{\ldots -13, -8, -3, 2, 7, 12, 17 \ldots\}$	$2+5\mathbb{Z}$
	$r = 3:\ \{\ldots -12, -7, -2, 3, 8, 13, 18 \ldots\}$	$3+5\mathbb{Z}$
	$r = 4:\ \{\ldots -11, -6, -1, 4, 9, 14, 19 \ldots\}$	$4+5\mathbb{Z}$

→ coset

congruence classes $\mathbb{Z} \bmod 5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

Quotient group $\mathbb{Z}/5\mathbb{Z}$: group of cosets.

↳ not a subgp of $\mathbb{Z}$

adding cosets : $(1+5\mathbb{Z}) + (3+5\mathbb{Z}) = 4+5\mathbb{Z}$

$$
\begin{array}{rl}
(1+5\mathbb{Z}) = & \{\cdots, -9, -4, 1, 6, 11, \cdots\} \\
+\ (3+5\mathbb{Z}) = & \{\cdots, -12, -7, -2, 3, 8, \cdots\} \\
\hline
(4+5\mathbb{Z}) = & \{\cdots, -11, -6, -1, 4, 9, \cdots\}
\end{array}
$$

- Normality Test.

Let H be a subgroup of G. The following are equivalent:

1) $H \triangleleft G$

☆ 2) $gHg^{-1} \subseteq H \quad \forall g \in G$ → 一般用这个证明（任意 $h \in H$, $ghg^{-1} \in H$）

3) $gHg^{-1} = H \quad \forall g \in G$

proof: 1) ⇒ 2) Let $x \in gHg^{-1}$, $x = ghg^{-1}$ for some $h \in H$.

By 1), $gh \in gH = Hg$.

$\therefore gh = h_1 g$ for some $h_1 \in H$

$\Rightarrow x = ghg^{-1} = h_1 g g^{-1} = h_1 \in H$.

$gHg^{-1} \subseteq H$

2) ⇒ 3) If $g \in G$, then by 2), $gHg^{-1} \subseteq H$.

将 g^{-1} 替换 g. 得 $g^{-1}Hg \subseteq H$. $\qquad g(\underbrace{g^{-1}Hg}_{\subseteq H})g^{-1} = H$

$\Rightarrow H \subseteq gHg^{-1} \qquad \therefore g^{-1}Hg = H$.

3) ⇒ 1) $gHg^{-1} = H$. $\Rightarrow gH = Hg$.

ex. Let $G = GL_n(\mathbb{R})$ (matrix with $\det \neq 0$) $\quad H = SL_n(\mathbb{R})$ (满足 GL_n. 且 $\det = 1$ (一般))

for $A \in G$, $B \in H$. $\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1})$

$= \det(A) \cdot 1 \cdot \frac{1}{\det(A)}$

$= 1$

$\therefore ABA^{-1} \in H$. $\quad AHA^{-1} \subseteq H$. $\quad \forall A \in G$.

By normality test. $H \triangleleft G$. i.e. $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$

- prop 3.9.

通过 Lagrange thm 判断

If H is a subgroup of G. $[G:H]=2$. then $H \trianglelefteq G$.

proof: Let $g \in G$.

If $g \in H$. then $G = H \cup Hg$. a disjoint union.

$\because [G:H]=2$.

$\therefore G = \underbrace{H}_{g \in H} \cup \underbrace{Hg}_{g \notin H}$. (disjoint union)

Thus $Hg = G \setminus H$

Similarly. $gH = G \setminus H$.

Thus $Hg = gH$ for all $g \in G$. i.e $H \trianglelefteq G$.

ex. Let A_n be the alternating group contained in S_n.

$\because [S_n : A_n] = 2$ $\rightarrow \frac{|S_n|}{|A_n|} = \frac{2n}{n} = 2$ Lagrange thm

$\therefore$ by prop 3.9. $A_n \trianglelefteq S_n$

ex. Let $D_{2n} = \langle a, b : a^n = 1 = b^2. \ aba = b \rangle$ be the dihedual gp of order $2n$.

$\because [D_{2n} : \langle a \rangle] = 2$. $\rightarrow \frac{|D_{2n}|}{|\langle a \rangle|} = n$.

$\therefore$ by prop 3.9. $\langle a \rangle \trianglelefteq D_{2n}$.

Let H & K be subgroup of a group G

The intersection $H \cap K$ is the largest subgroup of G contained in both H & K.

If there is a smallest subgroup of G containing both H & K.

* $H \cup K$ is the smallest subset containing H & K

- Lemma 3.10.

Let H & K be subgroups of G. T.F.A.E

1) HK is subgp of G

2) $HK = KH$

3) KH is subgp of G

2) $\Rightarrow$ 1) • $\because$ $1 \cdot 1 \in HK$ $hk \in HK$.

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

• for hk, $h_1k_1 \in HK$.

we have $kh_1 \in KH = HK$, $kh_1 = h_2k_2$.

$(hk)(h_1k_1) = h(kh_1)k_1 = h(h_2k_2)k_1 = (hh_2)(k_2k_1) \in HK$.

By Subgp test. HK is a subgp of G.

1) $\Rightarrow$ 2) ($\subseteq$) Let $kh \in KH$. Since H & K are subgps of G. we have $h^{-1} \in H$. and $k^{-1} \in K$.

$\because$ HK is also a subgp of G. we have $kh = (h^{-1}k^{-1})^{-1} \in HK$.

$\therefore KH \subseteq HK$

($\supseteq$) If $hk \in HK$. HK is a subgp of G.

$(hk)^{-1} = k^{-1}h^{-1} \in HK$ $k^{-1}h^{-1} = h_1k_1$

Thus. $hk = k_1^{-1}h_1^{-1} \in KH$ $\therefore HK \subseteq KH$.

$HK = KH$

- prop 3.11.

Let H & K be subgroups of a gp G.

1) $H \triangleleft G \lor K \triangleleft G \Rightarrow HK = KH$ is a subgp of G.

2) $H \triangleleft G \land K \triangleleft G \Rightarrow HK \triangleleft G$

proof: 1) Assume $H \triangleleft G$.

$$HK = \bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = KH.$$

By lemma 3.10. $HK = KH$ is a subgroup of G.

2) Let $g \in G$. $hk \in HK$.

$\because H \triangleleft G$. $K \triangleleft G$.

$$\therefore g^{-1}(hk)g = g^{-1}(hgg^{-1}k)g$$
$$= (g^{-1}hg)(g^{-1}kg) \in HK$$

$\therefore HK \triangleleft G$.

- def. normalier $N_G(H)$

Let H be a subgp of a gp G. The normalier of H. ($N_G(H)$) is:

$$N_G(H) = \{g \in G : gH = Hg\}.$$

* $H \triangleleft G \Leftrightarrow N_G(H) = G$

$N_G(H)$: 满足 $gH = Hg$ 的 g

$[G:H]$: distinct subgp

若 $|H|=1$. 则 $|N_G(H)| = [G:H]$

- Cor 3.12.

Let H & K be subgps of a gp G. $K \subseteq N_G(H) \Rightarrow HK = KH$ is a subgp of G.

- Thm 3.13.

$H \lhd G$ and $K \lhd G$ satisfy $H \cap K = \{1\}$ $\Rightarrow$ $HK \cong H \times K$.

proof: Let $m, n \in \mathbb{N}$ $\gcd(m, n) = 1$

Let G be a cyclic gp of order mn. $G = \langle a \rangle$.

$o(a) = mn$

Let $H = \langle a^n \rangle$ $K = \langle a^m \rangle$

$|H| = o(a^n) = m$ $|K| = o(a^m) = n$

$|H||K| = mn = |G|$

$G \cong H \times K$

→ We only need to consider cyclic gp of prime order.

→ Claim 1: If $H \lhd G$ and $K \lhd G$ satisfy $H \cap K = \{1\}$.

then $hk = kh$ $\forall h \in H$ and $k \in K$.

prove claim 1: Consider $x = hk(kh)^{-1} = hkh^{-1}k^{-1}$

$khk^{-1} \in kHk^{-1} \in H$

$\therefore x = h(kh^{-1}k^{-1}) \in H$

Similarly. $x \in K$. $\because x \in H \cap K = \{1\}$ $\therefore hkh^{-1}k^{-1} = 1$ $\Rightarrow hk = kh$

Since $H \lhd G$, by prop 3.11. HK is a subgroup of G.

→ Claim 2: σ is an IM.

Define $\sigma: H \times K \mapsto HK$. $(h, k) \to hk$ $\forall h \in H$ $k \in K$.

prove claim 2: Let (h, k) $(h_1, k_1) \in H \times K$. By Claim 1. $h_1 k = k h_1$.

$$\sigma((h,k)\cdot(h_1,k_1)) = \sigma((hh_1, kk_1))$$
$$= hh_1kk_1$$
$$= hkh_1k_1 \text{ (by claim 1)}$$
$$= \sigma((h,k))\,\sigma((h_1,k_1))$$

$\therefore \sigma$ is a HM.

$\because$ by def of HK. σ is onto

$\therefore \sigma((h,k)) = \sigma((h_1,k_1)) \Rightarrow hk = h_1k_1$

$\therefore h_1^{-1}h = k_1k^{-1} \in H \cap K = \{1\}$

$\therefore h_1^{-1}h = 1 \quad k_1k^{-1} = 1$. i.e $h_1 = h$. $k_1 = k$.

$\therefore \sigma$ is 1 to 1. Claim 2 holds

So $HK \cong H \times K$

- Cor 3.14

Let G be a finite group, $H, K \triangleleft G$, $H \cap K = \{1\}$. $|H||K| = |G|$.

Then $G \cong H \times K$

proof: $\because H, K \triangleleft G \quad \therefore HK \hat{\leq} G \quad (3.11)$

By Lagrange thm $|HK| \mid |G|$

$\because H \cap K = \{1\} \quad \therefore \gcd\{|H|, |K|\} = 1$

$\therefore |HK| = |H||K| = |G|$

$\because$ size 一样 & $HK \hat{\leq} G \quad \therefore HK = G$.

$\because HK \cong H \times K \quad \therefore G \cong H \times K$

4. Isomorphism Theorems

4.1 Quotient Group

- def. multiplication

Let G be a gp, K be a subgroup of G. It is natural to ask if we can make the set of right cosets of K. i.e $\{Ka : a \in G\}$ into a gp.

A natural way to define <u>multiplication</u> on this set is: $Ka \cdot Kb = Kab \quad a, b \in G$. $(*)$

Note $Ka = Ka_1$, $Kb = Kb_1$. $a \neq a_1$. $b \neq b_1$

$\therefore$ in order for $(*)$ to make sense. a necessary condition is:

$$Ka = Ka_1. \quad Kb = Kb_1. \Rightarrow Kab = Ka_1b_1$$

In this case, the multiplication $KaKb = Kab$ is well-defined.

- def. quotient gp (of G by K) $\quad G/K$

Let $K \triangleleft G$. The gp G/K of all cosets of K in G is called the <u>quotient gp</u> of G by K.

$\varphi : G \to G/K$ given by $\varphi(a) = Ka$ is <u>coset map</u>

identity: K.

inverse of $x \cdot K$ is $x^{-1} \cdot K$.

K is normal subgp of G. $\quad K \triangleleft G$

- Simple group

The only normal subgps of G are $\{e\}$ & G. $\Rightarrow$ G is simple subgp

- def. kernel $\quad Ker(\alpha)$

$\alpha : G \to H$ is a HM gp $\quad$ Kernel of α: $Ker(\alpha) = \{g \in G : \alpha(g) = e\}$

- def. image $im(\alpha)$

$im(\alpha) = \alpha(G) = \{\alpha(g) : g \in G\} \subseteq H$

* if α is surjective. Then $im\,\alpha = H$

- def. $\bar{\alpha}$.

$K = Ker(\alpha)$ $\quad \bar{\alpha} : G/K \to im(\alpha)$ $\quad \bar{\alpha}(Kg) = \alpha(g)$

$Kg = Kg_1 \Leftrightarrow gg_1^{-1} \in K$

$\Leftrightarrow \alpha(gg_1^{-1}) = 1$

$\Leftrightarrow \alpha(g) = \alpha(g_1)$

$\because \bar{\alpha}$ is one to one and well defined

$\therefore \bar{\alpha}$ is onto

- Lemma 4.1

Let K be a subgp G. TFAE:

1) $K \triangleleft G$

2) $a.b \in G$. the multiplication $Ka\,Kb = Kab$ is well-defined.

proof: (1) $\Rightarrow$ (2) Let $Ka = Ka_1$ $\quad Kb = Kb_1$

Thus $aa_1^{-1} \in K$. $bb_1^{-1} \in K$.

To get $Kab = Ka_1b_1$, it need to show $ab(a_1b_1)^{-1} \in K$.

$\because K \triangleleft G$. $\quad \therefore aKa^{-1} \subseteq K$.

Thus $ab(a_1b_1)^{-1} = ab(b_1^{-1}a_1^{-1}) = a(bb_1^{-1})a_1^{-1}$

$= a(bb_1^{-1})a^{-1}aa_1^{-1} = (a(bb_1^{-1})a^{-1})(aa_1^{-1}) \in K$

$\hookrightarrow Kab = Ka_1b_1$

(2) $\Rightarrow$ (1) If $a \in G$. to show $K \triangleleft G$. we need $aka^{-1} \in K$ for all $k \in K$.

$\because Ka = Ka$ $\quad Kk = K1$.

$\therefore$ by (2), $Kak = Ka\,k_1 = Ka$ $\quad \therefore aka^{-1} \in K$ $\quad K \triangleleft G$.

- prop 4.2

Let $K \triangleleft G$. $G/K = \{Ka : a \in G\}$ (指 set of cosets of K)

1) G/K is a gp under the operation $KaKb = Kab$.

2) The mapping $\varphi : G \to G/K$. given by $\varphi(a) = Ka$. is an onto HM.

3) $[G:K]$ is finite $\Rightarrow |G/K| = [G:K]$

$|G|$ is finite $\Rightarrow |G/K| = \frac{|G|}{|K|}$

proof: 1) by lemma 4.1. The operation is well-defined and G/K is closed under the operation.

$\because KaK1 = Ka = K1Ka$.

$\therefore$ The identity of G/K is $K = K1$. for all $Ka \in G/K$.

$\because KaKa^{-1} = K1 = Ka^{-1}Ka$.

$\therefore$ the inverse of Ka is Ka^{-1}.

$Ka(KbKc) = (KaKb)Kc$ (by associativity of G)

$\therefore G/K$ is a group

2) φ is clearly onto.

$\therefore \varphi(a)\varphi(b) = KaKb = Kab = \varphi(ab)$

$\therefore \varphi$ is an onto HM

3) If $[G:K]$ is finite, then $|G/K| = [G:K]$ (by def of index $[G:K]$)

$\because |G|$ is finite

$\therefore |G/K| = [G:K] = \frac{|G|}{|K|}$

- prop 4.3

$\alpha : G \to H$. α is HM.

1) $\operatorname{im}(\alpha)$ is a subgp of H

2) $\operatorname{Ker}(\alpha) \lhd G$

proof: 2) $g \in G$. $h \in \operatorname{Ker}(\alpha)$

$$ghg^{-1} \qquad \alpha(g)\alpha(h)\alpha(g^{-1})$$
$$= \alpha(g)\alpha(g^{-1})$$
$$= 1$$

$\therefore ghg^{-1} \in \operatorname{Ker}(\alpha)$

$\therefore \operatorname{Ker}(\alpha) \lhd G$

ep. Consider determinant map $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$.

$\operatorname{Ker}(\det) = SL_n(\mathbb{R}) \Rightarrow SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$

ep. $\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases} \qquad \sigma \in S_n.$

$\operatorname{Ker}(\operatorname{sgn}) = A_n \Rightarrow A_n$ is normal

$$\begin{tikzcd} G \arrow[rr, "\alpha"] \arrow[dr, "\varphi"'] & & H \\ & G/K \arrow[ur, "\bar{\alpha}"'] & \end{tikzcd}$$

$\alpha : G \to H$ a homomorphism. $K = \operatorname{Ker}(\alpha)$

$\varphi : G \to G/K$ coset map isomorphism

$\bar{\alpha} : G/K \to \operatorname{im}(\alpha) \qquad \bar{\alpha}(Kg) = \bar{\alpha}(\varphi(g)) = \alpha(g)$

- thm 4.4 (First isomorphism Thm)

If a map $\alpha: G \to H$ be a group Homomorphism.

Then $G/Ker(\alpha) \cong im(\alpha)$

proof: Let $K = Ker\ \alpha$.

$\because K \lhd G$. G/K is a gp.

$\therefore$ Define $\bar{\alpha}: G/K \to im\ \alpha$ be $\bar{\alpha}(Kg) = \alpha(g)$ $Kg \in G/K$

$Kg = Kg_1 \Leftrightarrow gg_1^{-1} \in K$.

$\Leftrightarrow \alpha(gg_1^{-1}) = 1$

$\Leftrightarrow \alpha(g) = \alpha(g_1)$

$\therefore \bar{\alpha}$ is well-defined. & one-to-one. & clearly onto

→ For $g, h \in G$.

$\bar{\alpha}(KgKh) = \bar{\alpha}(Kgh) = \alpha(gh) = \alpha(g)\alpha(h)$

$= \bar{\alpha}(Kg)\bar{\alpha}(Kh)$

$\therefore \bar{\alpha}$ is HM $\therefore im\alpha \cong G/Ker\ \alpha$

- prop 4.5

$\alpha: G \to H$ is a HM. $K: Ker(\alpha)$

α function uniquely as $\alpha = \bar{\alpha}$ where $\varphi: G \to G/K$ is the coset map

$\bar{\alpha} = \bar{\alpha}(Kg) = \alpha(g)$ φ is onto. $\bar{\alpha}$ is one-to-one

G is a cyclic gp $G = \langle g \rangle$

$\alpha: (\mathbb{Z}, +) \to G$ defined $\alpha(n) = g^k$ $\forall n \in \mathbb{Z}$. α is onto

if $o(g) = \infty$. $Ker(\alpha) = \{0\}$ by 1st IM. $G \cong \mathbb{Z}/\{0\} \cong \mathbb{Z}$

$Kernel(\alpha) = \{n \in \mathbb{Z} \wedge mod(o(g)) = 0\}$ $G \cong \mathbb{Z}_{o(g)}$

if G is cyclic $G \cong \mathbb{Z}$ or $G \cong \mathbb{Z}_K$. where K = order of G

– Thm 4.6 (2nd IM theorem)

Let H & K be subgps of G. $K \lhd G$.

Then HK is a subgp of G. $K \lhd HK$. $H \cap K \lhd H$. $HK/K \cong H/H\cap K$

proof: $\because K \lhd G$ $\therefore HK$ is a subgp (prop 3.11)

$HK = KH$. $K \lhd HK$

Consider the map $\alpha: H \to HK/K$. $\alpha(h) = Kh$.

Thus α is a HM.

If $x \in HK = KH$. $x = kh$. Then $Kx = K(kh) = Kh = \alpha(h)$

Thus α is onto.

By prop 3.3. $\operatorname{Ker}\alpha = \{h \in H : Kh = K\} = \{h \in H : h \in K\} = K \cap H$

By 1st IM theorem. $H/H\cap K \cong HK/K$.

– Thm 4.7 (3rd IM theorem)

Let $K \subseteq H \subseteq G$ be gps with $K \lhd G$. $H \lhd G$. Then H/K is G/K.

proof: Define $\alpha: G/K \to G/H$. by $\alpha(Kg) = Hg$ $\forall g \in G$

Note that if $kg = kg_1$. then $gg_1^{-1} \in K \subseteq H$.

$\therefore Hg = Hg_1$. α is well-defined

It is clear that α is onto. $\operatorname{Ker}(\alpha) = \{Kg : Hg = H\}$

$= \{Kg : g \in H\} = H/K$.

By 1st IM thm. $(G/K)/(H/K) \cong G/H$

5. Group Actions

5.1 Cayley's Theorem

- Cayley's Thm

If G is a finite gp of order n. Then G is isomorphism to a subgroup of S_n.

Every subgp $\cong$ a collection of permutations

proof. Let $G = \{g_1, \cdots, g_n\}$. S_G : G in permutation gp.

prove $S_G \cong S_n$:

$S_G = \operatorname{im} \alpha$

$\sigma : G \to S_G$. ← injective HM. surjective when 限制 codomain to its image

$\mu_a : G \to G$ $\quad \mu_a(g) = ag$ $\quad a \in G$. $g \in G$. → bijection. $\mu_a \in S_G$

$\sigma : G \to S_G$ $\quad \sigma(a) = \mu_a$

↓ 用定义证明 μ_a 同时也是 1-1 & HM

- $\mu_a = \mu_b \Rightarrow \mu_a(1) = \mu_b(1) \Rightarrow a = b$. one to one
- $\mu_a \mu_b = \mu_{ab} \Leftarrow \mu_a \mu_b(g) = \mu_a(bg) = abg = \mu_{ab}(g)$ HM

$\therefore$ By 1st IM thm. $G \cong \operatorname{im} \sigma$. $\quad \therefore S_G \cong S_n$

* Sometimes we can find a smaller int m. s.t. G is contained in S_m

ex. Let H be a subgp of G. $[G:H] = m < \infty$

$X = \{g_1 H, g_2 H, \cdots, g_m H\}$ be the set of all distinct left coset of H in G

For $a \in G$. define $\lambda_a : X \to X$ by $\lambda_a(gH) = agH$ $\quad \forall gH \in X$.

Then λ_a is a bijection.

$\therefore \lambda_a$ is a bijection. $\lambda_a \in S_X$, (the permutation gp of X)

Consider map $\tau : G \to S_X$ defined by $\tau(a) = \lambda_a$.

For $a, b \in G$. $\lambda_{ab} = \lambda_a \lambda_b$. $\quad \therefore \tau$ is HM

* if $a \in \operatorname{Ker} \tau$. then λ_a is the identity permutation

$aH = \lambda_a(H) = H$ $\quad \therefore \operatorname{Ker} \tau \subseteq H$

- Thm 5.2 Extended Cayley's Theorem

Let H be a subgp of a gp G with $[G:H]=m<\infty$.

If G has no normal subgp contained in H except $\{1\}$,

then G is isomorphic to a subgp of S_m.

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

$\ker\tau = K \subseteq H$

H 不能 contain a normal subgp of G

$G/K = \text{im}\,\tau$

$\Leftrightarrow \frac{|G|}{|K|} = |\text{im}\,\tau|$

$\Leftrightarrow \frac{|G|}{|K|} = |G| \quad (\tau(G) = \text{im}(\alpha))$

$\Leftrightarrow |K| = 1$

proof: $|X| = [G:H] = m \quad S_X \cong S_m.$

$\tau: G \to S_X \quad \Leftarrow HM \quad \underbrace{\ker\tau}_{} \overset{=K}{} \subseteq H.$

$\frac{|G|}{|K|} = |\text{im}\,\tau|$

$|K| = 1$

$\therefore$ By 1st IM Thm, $G/\ker\tau \cong \text{im}\,\tau.$

$\because \ker\tau \subseteq H. \quad \ker\tau \triangleleft G.$

$\therefore \ker\tau = \{1\}. \quad \Rightarrow \tau$ is injective.

$\therefore G \cong \text{im}\,\tau. \quad S_X \cong S_m$

- Cor 5.3

Let G be a finite gp and p be smallest prime s.t $p \mid |G|$

If H is a subgp of G with $[G:H]=p$, then $H \trianglelefteq G$.

(generalization of prop 3.9)

$|G| = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ p_1最小

$[G:H] = \frac{|G|}{|H|} = p_1 \Rightarrow H \trianglelefteq G$

prof. Let X be the set of all distinct left cosets of H in G.

$\Rightarrow |X| = p$. $S_X \cong S_p$

Let $\tau: G \to S_X \cong S_p$ be the gp HM defined in the above example

with $K = \ker \tau \subseteq H$.

所有gK组成的gp ($K \trianglelefteq G$)

By the 1st IM thm, $G/K \cong \operatorname{im} \tau \subseteq S_p$.

$\therefore G/K$ is IM to a subgp of S_p.

$\because K \subseteq H$. if $[H:K]=k$

$\therefore |G/K| = \frac{|G|}{|K|} = \frac{|G|}{|H|}\frac{|H|}{|K|} = pk$

By lagrange thm, $pk \mid p! \Rightarrow k \mid (p-1)!$

$\because k \mid |H|$, which divides $|G|$ and p is the smallest prime dividing $|G|$.

$\therefore$ every prime divisor of k must be $\geq p$ unless $k=1$.

Combining this with $k \mid (p-1)!$, this focus $k=1$ which implies $K=H$

$\therefore H \trianglelefteq G$.

5.2 Group Actions

- def. (left) group action

  Let G be a gp. X be a non-empty set.

  A (left) group action of G on X is a mapping $G \times X \to X$.

  $(a, x) \mapsto ax$. s.t 1) $1 \cdot x = x \quad \forall x \in X$

  2) $a \cdot (b \cdot x) = (ab)x \quad \forall a, b \in G.\ x \in X$.

  ↳ G acts on X.

  * Let G be a gp acting on a set $X \neq \emptyset$.

  For $a, b \in G$. $x, y \in X$.

  By 1) & 2). $a \cdot x = b \cdot y$. $\Leftrightarrow (b^{-1}a) \cdot x = y$

  $ax = ay \Leftrightarrow x = y$.

ex. If G is a gp. Let G acts on itself. i.e. $X = G$

by $ax = axa^{-1}$ for all $a, x \in G$. $1 \cdot x = 1x1^{-1} = x$.

$a \cdot (b \cdot x) = a(bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = (ab)x$.

↳ G acts on itself by conjugation.

- Remark

  For $a \in G$. define $\sigma_a : X \to X$ by $\sigma_a(x) = ax$. for all $x \in X$.

  Then 1) $\sigma_a \in S_X$

  2) $\theta : G \to S_X$ given by $\theta(a) = \sigma_a$. is a gp HM with

  $\mathrm{Ker}\,\theta = \{a \in G : ax = x \ \forall x \in X\}$.

  the gp HM $\theta : G \to S_X$ gives an equivalent def of gp action of G on X

  If $X = G$. $|G| = n$. $\mathrm{Ker}\,\theta = 1$. then the map $\theta : G \to S_G \cong S_n$ shows

  that G is isomorphism to a subgp of S_n. ← Cayley's thm

- def. orbit & stabilier

Let G be a gp acting on a set X and $x \in X$.

orbit of X : $G \cdot x = \{ g \cdot x : g \in G \} \subseteq X$

stabilier of X: $S(x) = \{ g \in G : g \cdot x = x \} \subseteq G$

- Prop 5.4.

Let G be a gp action on a set $X \neq \emptyset$. $x \in X$.

Then (1) $S(x)$ is a subgp of G

(2) $\exists$ a bijection from $G \cdot x$ to $\{ g S(x) : g \in G \}$

$|G x| = [G : S(x)]$

proof: (1) Since $1 \cdot x = x$. we have $1 \in S(x)$.

Also, if $g, h \in S(x)$, then $(gh) \cdot x = g(h \cdot x) = g \cdot x = x$

$g^{-1} x = g^{-1}(g x) = (g^{-1} g) x = 1 \cdot x = x$

Thus. $gh, g^{-1} \in S(x)$.

By Subgp test, $S(x)$ is a subgp of G.

(2) Consider the map $\varphi : G \cdot x \to \{ gS : g \in G \}$ defined by $\varphi(g \cdot x) = gS$.

$gx = hx \Leftrightarrow (h^{-1} g) \cdot x = x$ $\quad$ $\mathbb{Z}_5$. $h = [1]$ $\quad$ $g = [5]$

$\Leftrightarrow h^{-1} g \in S$ $\quad$ h 与 g 表示的东西相同

$\Leftrightarrow gS = hS$ $\quad$ well-defined 指它俩 output 相同

Thus φ is well-defined

$\because \varphi$ is clearly onto. & bijection

$\therefore |G \cdot x| = |\{ gS : g \in G \}| = [G : S]$

- Thm 5.5 Orbit Decomposition Thm.

Let G be a gp acting on a finite set $X \neq \phi$.

$X_f = \{x \in X : ax = x \quad \forall a \in G\}$ $\quad$ (* $x \in X_f \Leftrightarrow |G \cdot x| = 1$)

Let $G \cdot x_1, G \cdot x_2, \cdots, G x_n$ denote distinct nonsingleton orbits i.e $|G \cdot x_i| > 1$.

Then $|X| = \underbrace{|X_f|}_{\text{sigleton}} + \sum_{i=1}^{n} \underbrace{[G : S(x_i)]}_{\text{nonsingleton}}$. $\quad \frac{|G|}{|S_i|}$

proof: Note that for $a, b \in G$. $x, y \in X$

$ax = by \Leftrightarrow (b^{-1}a) \cdot x = y$.

$\Leftrightarrow y \in Gx$

$\Leftrightarrow Gx = Gy$.

$\therefore$ The 2 orbits are either disjoint or the same

which follows that the orbit form a disjoint union of X.

$\because x \in X_f \Leftrightarrow |G x| = 1$

$\therefore X \setminus X_f$ contains all nonsingletons orbits. which are disjoint.

By prop 5.4, $|X| = |X_f| + \sum_{i=1}^{n} |G x_i|$

$= |X_f| + \sum_{i=1}^{n} [G : S(x_i)]$

→ Let G be a gp acting on itself by conjugation.

Then $G_f = \{x \in G : gxg^{-1} = x \quad \forall g \in G\}$

$= \{x \in G : gx = xg \quad \forall g \in G\}$. which is center of G.

($G_f = Z(G)$)

→ For $x \in G$

$S(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\}$

The set is called centralier of X and is denoted by $S(x) = C_G(x)$

In this case, the orbit $G \cdot x = \{gxg^{-1} : g \in G\}$ is conjugate class of X.

- Cor 5.6 Class equation.

Let G be a finite gp and let $\{gx_1g^{-1} : g \in G\}, \cdots, \{gx_ng^{-1} : g \in G\}$ denote the distinct nonsingleton conjugate classes

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

- Lemma 5.7

Let G be a gp of order p^m acting on a finite set $X \neq \phi$.

Let $X_f = \{x \in X : a \cdot x = x \quad \forall a \in G\}$

Then $|X| \equiv |X_f| \pmod p$

proof: By Thm 5.5.

$|X| = |X_f| + \sum_{i=1}^{n} [G : S(x_i)]$ with $[G : S(x_i)] > 1 \quad (1 \leq i \leq n)$

$\because [G : S(x_i)]$ divides $|G| = p^m$ and $[G : S(x_i)] > 1$.

$\therefore p \mid [G : S(x_i)]$ for all i.

$\therefore |X| \equiv |X_f| \pmod p$

$[G : S(x_i)] = \dfrac{|G| \longrightarrow = p^m}{|S(x_i)| \longrightarrow \text{subgp of } G}$

$|S_{x_i}| \,\big|\, |G| \Rightarrow \underbrace{|S_{x_i}|}_{p^k (k \leq m)} \,\big|\, p^m$

- Thm 5.8 Cauchy Thm → 铺垫 Sylow

Recall that as a consequence of Lagrange Thm

If a gp G is finite. $g \in G$. then $o(g) \mid |G|$

相反的问题：If $m \mid |G|$, Does G contain an element of order m?

Let p be a prime and G a finite gp.

If $p \mid |G|$, then G contains an element of order p.

proof: Define $X = \{(a_1, \cdots, a_p) : a_i \in G.\ a_1 \cdots a_p = 1\}$

$\because a_p = (a_1 \cdot a_2 \cdots a_{p-1})^{-1}$ is uniquely defined

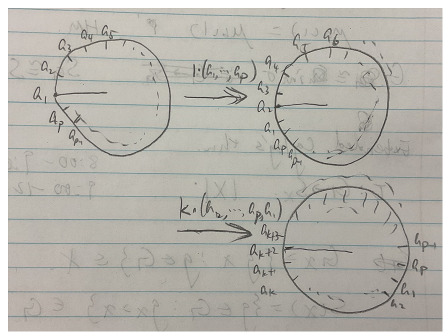
$\therefore$ If $|G| = n$, we have $\underline{|X| = n^{p-1}}$ 对于每个 a_i 都有 n 种选择. 最后 a_p 是 uniquely determined

$\because p \mid n$ $\therefore |X| \equiv 0 \pmod p$

Let the $\mathbb{Z}_p = (\mathbb{Z}_p, +)$. act on X by cycling 每个 element 移 k 位 逆时针

i.e. for $k \in \mathbb{Z}_p$. $\underline{k(a_1, \cdots, a_p) = (a_{k+1}, a_{k+2}, \cdots, a_p, a_1, \cdots a_k)}$

one can verify that this action is well-defined.



Let X_F be defined as Thm 5.5.

Then $(a_1, \cdots, a_p) \in X_F \iff a_1 = \cdots = a_p$

$\because (1, \cdots, 1) \in X_F$ $\therefore |X_F| \geq 1$

$\because |X| \equiv 0 \pmod p$ $|X_F| \geq 1$

$\therefore |X_F| \geq p$.

$\therefore$ There exists $a \neq 1$ s.t $(a, \cdots, a) \in X_F$

which implies $a^p = 1$

$\because p$ is a prime $a \neq 1$

$\therefore o(a) = p$

6. Sylow Theorem

6.1 P-Groups

- def. p-group.

  Let $p \in$ prime. A group in which every element has order of a non-negative power of p is a p-group

- Cor 6.1

  A finite gp G is a p-gp $\Leftrightarrow$ $|G|$ is a power of p. $|G| = p^n$

  proof: ($\Rightarrow$) prove by contradiction: $|G| = p^n p_2^{n_2} \cdots p_k^{n_k}$ $(k \geq 2)$

  $\because p_2 \mid |G|$ $\therefore$ By Cauchy's Thm. $\exists$ an element of order p_2

  $\therefore G$ is not a p-gp

  ($\Leftarrow$) $|G| = p^n$. $g \in G \Rightarrow o(g) \mid p^n$. $\therefore o(g) = p^\alpha$ $\alpha \leq n$

- Cor 6.2

  The center $Z(G)$ of a non-trivial finite p-gp contains more than 1 element $\{z : zg = gz\}$

  proof. Recall class equation (Cor 5.6) of G:

  $$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(x_i)] \quad \text{where } [G : C_G(x_i)] > 1$$

  $\because G$ is a p-gp

  $\therefore$ by Cor 6.1, $|G|$ is a power of p.

  by lemma 5.7. $|Z(G)| \equiv |G| \pmod p$ $\rightarrow p \mid |Z(G)|$

  $\because |Z(G)| \geq 1$ (Since $1 \in Z(G)$)

  $\therefore |Z(G)| \geq p$ ($Z(G)$ has at least p elements)

- Lemma 6.3

If H is a p-subgp of finite gp G.
then $[N_G(H):H] \equiv [G:H] \pmod p$

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

proof. Let X be the set of all left cosets of H in G. $|X| = [G:H]$

Let H act on X by left multiplication.

For $x \in G$, we have

$$
\begin{aligned}
xH \in X_F &\Leftrightarrow hxH = xH \quad \forall h \in H \\
&\Leftrightarrow x^{-1}hxH = H \quad \forall h \in H \\
&\Leftrightarrow x^{-1}Hx = H \\
&\Leftrightarrow x \in N_G(H)
\end{aligned}
$$

$\therefore |X_F|$ is the number of cosets xH with $x \in N_G(H)$

$|X_F| = [N_G(H):H]$

By lemma 5.7. $[N_G(H):H] = |X_F| \equiv |X| = [G:H] \pmod p$

- Cor 6.4

Let H be a p-subgp of a gp G.
If $p \mid [G:H]$, then $p \mid [N_G(H):H]$ and $N_G(H) \neq H$

proof: $\because p \mid [G:H]$

$\therefore$ By lemma 6.3. $[N_G(H):H] \equiv [G:H] = 0 \pmod p$

$\because p \mid [N_G(H):H]$ $\quad [N_G(H):H] \geq 1$ (Since $H \subseteq N_G(H)$)

$\therefore [N_G(H):H] \geq p$.

$\therefore N_G(H) \neq H$

6.2 Sylow's Three Theorems

- First Sylow Thm (Thm 6.5)

• Let G be a gp of order $p^n m$, where $p \in$ prime. $n \geq 1$ $\gcd(p,m)=1$
Then G contains a subgp of order p^i $\forall i: 1 \leq i \leq n$.

• Every subgp of G of order p^i $(i<n)$ is normal in some subgp of order p^{i+1}

proof. Prove by induction

$\rightarrow$ $i=1$ $|G|=p^n m$ $\gcd(p,m)=1 \Rightarrow G$ contain subgp order p^i

$\because p \mid |G|$ by Cauchy's Thm.

$\therefore G$ contains an element a of order p $|\langle a \rangle| = p$

$\rightarrow$ Suppose the statement holds for some $1 \leq i < n$.

H is a subgp of G with order p^i

$|H_1| = |H| \cdot \frac{|H_1|}{|H|} = p^i \cdot p = p^{i+1}$

Then $p \mid [G:H]$.

By Cor 6.4, $p \mid [N_G(H):H]$ $[N_G(H):H] \geq p$.

By Thm 5.8, $N_G(H)/H$ contains a subgp of order p.

Such a gp is of t. H_1/H, where H_1 is a subgp of $N_G(H)$ containing H

$\because H \triangleleft N_G(H)$ $\therefore H \triangleleft H_1$.

$\therefore |H_1| = |H| \cdot \frac{|H_1|}{|H|} = p^i \cdot p = p^{i+1}$

- def. Sylow p-subgp of G. size 最大的 p-gp

A subgp P of a gp G is said to be a Sylow p-subgp of G if P is a maximal p-gp of G.

i.e. $P \subseteq H \leq G$ with H a p-gp $\Rightarrow P = H$.

- Cor 6.6

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

Let H be a p-subgp of G.

1) H is a Sylow p-subgp $\Leftrightarrow$ $|H| = p^n$ Sylow p-gp 是最大的 p-gp

2) Every conjugate of a Sylow p-subgp is a Sylow p-subgp $a \cdot x = axa^{-1} \in G$

3) If there is only one Sylow p-subgp P, then $P \trianglelefteq G$.

- Second Sylow Thm (Thm 6.7)

If H is a p-subgp of a finite gp G, and P is any Sylow p-subgp of G, then there exists $g \in G$ s.t. $H \subseteq gPg^{-1}$

In particular, any 2 Sylow p-subgps of G are conjugate

proof: Let X be the set of all left cosets of P in G.

H act on X by left multiplication.

By lemma 5.7. $|X_f| \equiv |X| = [G:P] \pmod p$

$\because p \nmid [G:P]$ $\therefore |X_f| \neq 0$

Thus there exists $gP \in X_f$ for some $g \in G$.

$$\begin{aligned} gP \in X_f &\Leftrightarrow hgP = gP \quad \forall h \in H \\ &\Leftrightarrow g^{-1}hgP = P \quad \forall h \in H \\ &\Leftrightarrow g^{-1}Hg \subseteq P \\ &\Leftrightarrow H \subseteq gHg^{-1} \end{aligned}$$

If H is a Sylow p-subgp.

Then $|H| = |P| = |gPg^{-1}|$

$\therefore$ $H = gPg^{-1}$

- Third Sylow Thm

Let G be a finite gp and $p \in$ prime. $p \mid |G|$.

then the number of Sylow p-subgps of G divides $|G|$ and is of the form $kp+1$ for some $k \in \mathbb{N} \cup \{0\}$.

$|G| = p_1^{k_1} \cdots p_n^{k_n}$

存在 sylow gp with order : $p_1^{k_1}, p_2^{k_2}, \cdots, p_n^{k_n}$

* Suppose that G is a gp with $|G| = p^n m$ with $\gcd(p, m) = 1$.

Let n_p be the number of Sylow p-subgps of G.

By the Third Sylow Thm, we see that $n_p \mid p^n m$ $n_p \equiv 1 \pmod p$

$\because p \nmid n_p$ $\therefore n_p \mid m$

proof: By Thm 6.7, the number of Sylow p-subgp of G is the number of Conjugate of any one of them, say P. This number is $[G : N_G(P)]$ which is a divisor of G.

Let X be a set of all sylow p-subgps of G

P acts on X by conjugation.

Then $Q \in X_P \Leftrightarrow gQg^{-1} = Q$ for $\forall g \in P$.

$\Leftrightarrow P \leq N_G(Q)$

Both P and Q are Sylow p-subgps of G and $N_G(Q)$

$\therefore$ By Cor 6.6. They are conjugate in $N_G(Q)$

$\because Q \triangleleft N_G(Q)$

$\therefore$ this can only occur if $Q = P$

$\therefore Q = P$ $X_p = \{P\}$.

$\therefore$ By Lemma 5.7 $|X| \equiv |X_P| \equiv 1 \pmod p$

$\therefore |X| = kp+1$ for some $k \in \mathbb{N} \cup \{0\}$.

ex. Claim: every gp of order 15 is cyclic.

n_3 = # sylow 3

n_5 = # sylow 5 $\quad n_5 \mid 3 \quad n_5 \equiv 1 \pmod 5$

Let G be gp of order $15 = 3 \cdot 5$.

n_p be the number of sylow p-subgp of G.

By the third Sylow Thm. $n_3 \mid 5$ and $n_3 \equiv 1 \pmod 3$

Thus $n_3 = 1$. 相似 $n_5 = 1$.

It follows that $\exists$ only one Sylow-3 subgp and Sylow-5 subgp of G.

Thus, $P_3 \triangleleft G$ and $P_5 \triangleleft G$.

Consider $|P_3 \cap P_5|$, which divides 3 & 5.

Thus $|P_3 \cap P_5| = 1 \quad P_3 \cap P_5 = \{1\} \quad |P_3 P_5| = 15 = |G|$

It follows $G \cong P_3 \times P_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$

ex. There are 2 isomorphic classes of gps of order 21.

Let G be a gp of order $21 = 3 \cdot 7$.

n_p be the number of sylow p-subgp of G.

Thus we have $n_3 = 1$ or 7. $n_7 = 1$

It follows that G has unique Sylow 7-subgp : P_7

Note that $P_7 \triangleleft G$ and P_7 is cyclic . $P_7 = \langle x \rangle$. $x^7 = 1$

Let H be a sylow 3-subgp .

$\because |H| = 3$ $\therefore H$ is cyclic $H = \langle y \rangle$ with $y^3 = 1$

$\because P_7 \triangleleft G$. $\therefore y \cdot x y^{-1} = x^i$ $0 \le i \le 6$

$\therefore i^3 \equiv 1 \pmod 7$ $\therefore i = 1, 2, 4$

1) If $i = 1$, then $yxy^{-1} = x$ i.e. $yx = xy$ Thus G abelian, $G \cong \mathbb{Z}_{21}$

2) If $i = 2$, then $yxy^{-1} = x^2$ $\therefore G = \{x^i y^j : 0 \le i \le 6 . 0 \le j \le 2 . yxy^{-1} = x^2\}$

3) If $i = 4$, then $yxy^{-1} = x^4$ $y^2 x y^{-2} = y x^4 y^{-1} = x^{16} = x^2$

* y^2 is also a generator of H. Thus be replacing.

By replacing y by y^2, we get back to case (2). It following that there are 2 isomorphism classes of gps of order 21.

7. Finite Abelian group.

7.1 Primary Decomposition.

Notation: Let G be a gp. $m \in \mathbb{Z}$. We define $G^{(m)} = \{ g \in G : g^m = 1 \}$

- prop 7.1

Let G be an abelian gp. Then $G^{(m)}$ is a subgp of G.

proof: • $1 = 1^m \in G^{(m)}$

• Let $g, h \in G^{(m)}$

$\because$ G is abelian $\therefore (gh)^m = g^m h^m = 1$

$\therefore gh \in G^{(m)}$

• If $g \in G^{(m)}$

$(g^{-1})^m = g^{-m} = (g^m)^{-1}$ $\quad g^{-1} \in G^{(m)}$

By subgp test. $G^{(m)}$ is a subgp of G.

- prop 7.2

Let G be a finite abelian gp with $|G| = mk$ $\quad \gcd(m, k) = 1$.

Then 1) $G \cong G^{(m)} \times G^{(k)}$

2) $|G^{(m)}| = m \quad |G^{(k)}| = k$

proof: 1) $\because$ G is abelian $\therefore G^{(m)} \triangleleft G \quad G^{(k)} \triangleleft G$

$\because \gcd(m, k) = 1 \quad \therefore \exists x, y \in \mathbb{Z}$ s.t $mx + ky = 1$

Claim 1: $G^{(m)} \cap G^{(k)} = \{1\}$.

proof: If $g \in G^{(m)} \cap G^{(k)}$, then $g^m = 1 = g^n$.

$g = g^{mx+ky} = (g^m)^x (g^k)^y = 1$

Claim 2: $G = G^{(m)} \cdot G^{(k)}$

proof: If $g \in G$, then $1 = g^{mk} = (g^k)^m = (g^m)^k$

$g^k \in G^{(m)} \qquad g^m \in G^{(k)}$

$g = g^{mx+ky} = (g^m)^x (g^k)^y \in G^{(m)} G^{(k)}$

Combining Claim 1 & 2. by thm 3.13. $G \cong G^{(m)} \times G^{(k)}$

2) Let $|G^{(m)}| = m'$ $\quad |G^{(k)}| = k'$

By (1). $mk = |G| = m'k'$

Claim : $\gcd(m, k') = 1$

proof : Suppose $\gcd(m, k') \neq 1$

Then there exist a prime s.t $p \mid m$ $\quad p \mid k'$.

By Cauchy's thm. $\exists g \in G^{(k)}$ $\quad o(g) = p$.

$\because p \mid m$ $\quad \therefore g^m = (g^p)^{\frac{m}{p}}$ i.e $g \in G^{(m)}$

By (1). $g \in G^{(m)} \cap G^{(k)} = \{1\}$ $\rightarrow$ contradiction

$\because o(g) = p$ $\quad \therefore \gcd(m, k') = 1$

$\because m \mid m'k'$ $\quad \gcd(m, k') = 1$ $\quad \therefore m \mid m'$

Similarly, $k \mid k'$

$\because mk = m'k'$ $\quad \therefore m = m'$ $\quad k = k'$

- Thm 7.3 Primary Decomposition Thm. $\quad \uparrow$ General 的情况

Let G be a finite abelian gp with $|G| = p_1^{n_1} \cdots p_k^{n_k}$ ($p_1 \cdots p_k$ are distinct primes)

Then 1) $G \cong G^{(p_1^{n_1})} \times \cdots \times G^{(p_k^{n_k})}$

2) $|G^{(p_i^{n_i})}| = p_i^{n_i}$ $\quad (1 \le i \le k)$

ex. Let $G = \mathbb{Z}_{13}^*$.

Then $|G| = 12 = 2^2 \cdot 3$.

$G^{(4)} = \{a \in \mathbb{Z}_{13}^* : a^4 = 1\} = \{1, 5, 8, 12\}$

$G^{(3)} = \{a \in \mathbb{Z}_{13}^* : a^3 = 1\} = \{1, 3, 9\}$

By Thm 7.3. $\mathbb{Z}_{13}^* \cong \{1, 5, 8, 12\} \times \{1, 3, 9\}$

7.2 Structure Thm of Finite Abelian Groups

By Thm 7.3. a finite abelian gp is isomorphic to a direct product of finite abelian gps of prime power order. Thus is suffice to consider these gps now.

Recall: $|G| = p \Rightarrow G \cong C_p$.

$|G| = p^2 \Rightarrow G \cong C_{p^2}$ or $C_p \times C_p$

Q. How about $|G| = p^3 . p^4 \ldots$

- prop 7.4.

If G is a finite abelian p-gp that contains only 1 subgp of order p. Then G is cyclic.

扶习语说. if a finite abelian p-gp G is not cyclic. then G has at least 2 subgps of order p.

proof: Suppose $G \neq \langle g \rangle$.

Then the quotient group $G/\langle g \rangle$ is a non-trivial p-gp which contains an element z of order p by Cauchy's Thm.

In particular $z \neq 1$

Consider the coset map $\pi: G \to G/\langle g \rangle$

Let $x \in G$ satisfy $\pi(x) = z$.

$\because \pi(x^p) = \pi(x)^p = z^p = 1 \qquad \therefore x^p \in \langle y \rangle$

Thus $x^p = y^m$ for some $m \in \mathbb{Z}$.

case 1: If $p \nmid m$.

$\because o(y) = p^r$ for some $r \in \mathbb{N}$.

$\therefore$ By prop 2.11. $o(y^m) = o(y)$

$\because y$ is of maximal order

$\therefore o(x^p) < o(x) \leq o(y) = o(y^m) = o(x^p)$ leads to contradiction.

case 2: If $p \mid m$. Let $m = pk$. $(k \in \mathbb{Z})$

$\therefore x^p = y^m = y^{pk}$

$\because G$ is abelian

$\therefore (xy^{-k})^k = 1$

$\therefore xy^{-k}$ belongs to the one and only subgp of order p. Say H.

The cyclic gp $\langle y \rangle$ contains a subgp of order p. which must be the one and only H.

$\therefore xy^{-k} \in \langle y \rangle$ which implies $x \in \langle y \rangle$.

$\therefore z = \pi(x) = 1$. contradiction.

So. $G = \langle y \rangle$

- prop 7.5.

Let G be a finite abelian p-gp. C be a cyclic subgp of maximal order.
Then G contains a subgp B. s.t $G = CB$ $C \cap B = \{1\}$.
Thus by thm 3.13, we have $G \cong C \times B$

proof:

If $|G| = p$. we take $G = C$ $B = \{1\}$ and the result follows.

Suppose that the result holds for all abelian gp of order p^{n-1} with $n \in \mathbb{N}$. $n \geq 2$.

Consider $|G| = p^n$.

case 1 If $G = C$. then by $B = \{1\}$. the result follows

case 2 If $G \neq C$. then G is not cyclic

By prop 7.4.

Since C is cyclic. by Thm 2.12. It contains exactly one subgp of order p.

Thus there exist a subgp D of G with $|D| = p$. $D \nsubseteq C$.

$\therefore C \cap D = \{1\}$.

Consider coset map: $\pi : G \to G/D$.

If we consider π/C. the restriction of π on C.

then $\mathrm{Ker}\, \pi/C = C \cap D = \{1\}$.

Thus by 1st IM thm. $\pi(C) \cong C$.

Let y be a generator of the cyclic gp C. i.e. $C = \langle y \rangle$

$\because \pi(C) \cong C$. $\quad \pi(C) = \langle \pi(y) \rangle$

$\therefore$ By the assumption on C. $\pi(C)$ is a cyclic gp of G/D of maximal order

$\because |G/D| = p^{n-1}$

$\therefore$ by inductive hypothesis. G/D contains a subgp E s.t. $G/D = \pi(C)E$

$\pi(C) \cap E = \{1\}$

Let $B = \pi^{-1}(E)$ i.e $\pi(B) = E$

Claim 1 $\quad G = CB$.

proof : Note that E is a subgp containing $\{1\}$.

We have $\pi^{-1}(\{1\}) = D \subseteq B$.

If $x \in G$. $\because \pi(C)\pi(B) = \pi(C)E = G/D$.

$\therefore \exists\ u \in C \quad v \in B$. s.t $\pi(x) = \pi(u)\pi(v)$

$\because \pi(xu^{-1}v^{-1}) = 1 \quad \therefore xu^{-1}v^{-1} \in D \subseteq B$

$\because v \in B \quad \therefore xu^{-1} \in B$

$\because B$ is abelian $\quad \therefore x = uxu^{-1} \in CB$.

Claim 2 : $C \cap B = \{1\}$

proof : Let $x \in C \cap B$.

Then $\pi(x) \in \pi(C) \cap \pi(B)$

$= \pi(C) \cap E$

$= \{1\}$

$\because \pi(x) = 1$ in G/D

$\therefore x \in D.$

$\because x \in C \cap D = \{1\}$

$\therefore x = 1$

By Claim 1 & Claim 2. the result follows by induction.

- Thm 7.6.

Let G be a finite abelian p-gp.

Then G is isomorphic to a distinct product of cyclic gps.

proof: By Prop 7.5. There exist a cyclic gp C_1 a subgp B_1 of G. s.t $G \cong C_1 \times B_1$

$\because |B_1| \mid |G|$ by Lagrange Thm.

$\therefore B_1$ is also a p-gp.

$\therefore$ If $B_1 \neq \{1\}$. by prop 7.5. $\exists$ a cyclic gp C_2 & B_2. s.t $B_1 \cong C_2 \times B_2$

Continue in this way to get cyclic gp $C_1, \cdots, C_k$ until we get $B_k = \{1\}$

for some $k \in \mathbb{N}$. $\therefore G \cong C_1 \times C_2 \times \cdots \times C_k$.

- Thm 7.7 Structure Thm of finite abelian gps.

If G is a finite abelian gp. Then $G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$ (p_i not necessarily distinct)

where $\mathbb{Z}_{p_i^{n_i}} = (\mathbb{Z}_{p_i^{n_i}}, +) \cong C_{p_i^{n_i}}$ are cyclic gps of order $p_i^{n_i}$ $(1 \leq i \leq k)$

The numbers $p_i^{n_i}$ are uniquely determined up to their order.

- Thm 7.8 Invariant Factor Decomposition of finite abelian gp.

Let G be finite abelian gp.

Then $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$ where $n_i \in \mathbb{N}$ $(1 \leq i \leq r)$ $n_1 > 1$ $n_1 \mid n_2 \mid \cdots \mid n_r$

ex. Consider an abelian gp G of order 48.

$\because 48 = 2^4 \cdot 3$

$\therefore$ by thm 7.3. G is isomorphic to $H \times \mathbb{Z}_3$. where H is an abelian gp of order 2^4

The options of H are $\mathbb{Z}_{2^4}$, $\mathbb{Z}_{2^3} \times \mathbb{Z}_2$, $\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2}$, $\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Thus we have
$$G \cong \mathbb{Z}_{2^4} \times \mathbb{Z}_3 \cong \mathbb{Z}_{48}$$
$$G \cong \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_{24}$$
$$G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \cong \mathbb{Z}_4 \times \mathbb{Z}_{12}$$
$$G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{12}$$
$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6.$$

判断 group of order n 是否 always abelian

看是否是 cyclic $\quad C_n = \langle g : g^n = 1 \rangle$

eg. $o(g) = 39$ Not abelian

order = 3 in subgp

$39 = 3 \times 13$ $\quad 13 = 3 \times 4 + 1$ $\Leftarrow$ 3rd Sylow Thm 可有13个或1个

不是 cyclic $\quad$ 是 cyc

$o(g) = 85$ abelian

$85 = 5 \times 17$ $\quad \gcd(5, 17) = 1$

8. Ring

8.1 Rings

- def. Ring R

  A set of R is a ring if it has 2 operations: addition $(+)$ & multiplication $(\cdot)$

  s.t $(R,+)$ is an abelian gp.

  $(R,\cdot)$ satisfies closure associativity and identity properties of a gp.

- Ring properties.

  If R is a ring. Then $\forall a.b.c \in R$.

  1) $a+b \in R$
  2) $a+b=b+a$
  3) $a+(b+c)=(a+b)+c$
  4) $\exists 0 \in R$. s.t $a+0=a=0+a$ (0: zero of R)
  5) $\exists -a \in R$. s.t $a+(-a)=0=(-a)+a$ ($-a$: negative of a)
  6) $ab := a\cdot b \in R$.
  7) $a(bc)=(ab)c$
  8) $\exists 1 \in R$. s.t $a\cdot 1=a=1\cdot a$ $\forall a \in R$. (1: unity of R)
  9) $a(b+c)=ab+ac$ $(b+c)a=ba+ca$ (distribution law)
  10) If $ab=ba$, Then R is commutative

ex. $\mathbb{Z}$. $\mathbb{Q}$. $\mathbb{R}$. $\mathbb{C}$ are concentrative ring with zero: 0 unity: 1

ex. For $n \in \mathbb{N}$. $n \geq 2$. $M_n(\mathbb{R})$ is a ring using matrix addition & multiplication

zero: zero matrix O identity matrix: I.

* $\because (R,\cdot)$ is not a gp

$\therefore$ there is no left or right cancellation.

ep. In $\mathbb{Z}$, $0\cdot x=0\cdot y \not\Rightarrow x=y$.

gp和ring不构成包含关系

Given a ring R, to distinguish the difference between multiples in addition & multiplication.

For $n \in \mathbb{N}$. $a \in R$. $na = a+\cdots+a$ (n个a相加)

$a^n = a\cdot\cdots\cdot a$ (n个a相乘)

Recall : for a gp G. $g \in G$. we have $g^0 = 1$ and $g^1 = g$ and $(g^{-1})^{-1} = g$

Thus for addition : $0 \cdot a = 0$ $1 \cdot a = a$ $-(-a) = a$

For $n \in \mathbb{N}$. Define $(-n)a = (-a) + \cdots + (-a)$ (n 了 $-a$ 相加)

$a^0 = 1$

If the multiplication inverse of a exist. : a^{-1}. $aa^{-1} = 1 = a^{-1}a$.

define $a^{-n} = (a^{-1})^n$

- prop 8.1

Let R be a ring $s \in R$.

1) If 0 is zero of R. then $0 \cdot r = r \cdot 0 = 0$

2) $(-r)s = r(-s) = -rs$

3) $(-r)(-s) = rs$

4) $\forall m, n \in \mathbb{Z}$. $(mr)(ns) = (mn)(rs)$

- def. trivial ring.

A ring with only one element. In this case. $\overset{\text{unity of } R.}{1} = 0$.

If R is a ring with $R \neq \{0\}$. $\because r = r \cdot 1$ $\forall r \in R$.

$\therefore$ we have $1 \neq 0$. R not trivial.

ex. $R_1, \cdots, R_n$ be rings. We define <u>componentwise operations</u> on the poduct $R_1 \times \cdots \times R_n$ as follows :

1) $(r_1, \cdots, r_n) + (s_1, \cdots, s_n) = (r_1 + s_1, \cdots, r_n + s_n)$

2) $(r_1, \cdots, r_n)(s_1, \cdots, s_n) = (r_1 s_1, \cdots, r_n s_n)$

One can check $R_1 \times \cdots \times R_n$ is a ring:

zero $(0_{R_1}, \cdots, 0_{R_n}) = (0, \cdots, 0)$.

unity $(1_{R_1}, \cdots, 1_{R_n}) = (r_1 s_1, \cdots, r_n s_n)$

The ring $R_1 \times \cdots \times R_n$ are <u>direct product</u> of $R_1, \cdots, R_n$.

- def. characteristic of R. $ch(R)$

If R is a ring. define characteristic of R. in terms of order of 1_R in additive gp $(R,+)$

$$ch(R) = \begin{cases} n & \text{if } o(1_R) = n \in \mathbb{N} \quad \text{in } (R,+) \quad \text{finite gp} \\ 0 & \text{if } o(1_R) = \infty \quad \text{in } (R,+) \quad \text{infinite gp} \end{cases}$$

For $k \in \mathbb{Z}$, $k \cdot R = 0$ means $kr = 0$ $\forall r \in R$.

by prop 8.1. $k \cdot r = k(1_R \cdot r) = (k \cdot 1_R) \cdot r$.

Thus $kR = 0 \Leftrightarrow k \cdot 1_R = 0$.

- prop 8.2

1) $ch(R) = n \in \mathbb{N}$ $\Rightarrow$ $kR = 0 \Leftrightarrow n \mid k$

2) $ch(R) = 0$ $\Rightarrow$ $kR = 0 \Leftrightarrow k = 0$

ex. $\mathbb{Z}$. $\mathbb{Q}$. $\mathbb{R}$. $\mathbb{C}$ has characteristic 0.

For $n \in \mathbb{N}$. $n \geq 2$. ring $\mathbb{Z}_n$ has characteristic n.

8.2 Subrings

- df. Subring

A subset S of a ring R is a subring if S is a ring itself with $1_S = 1_R$

* property (2) (3) (7) (9) of a ring automatically satisfy

Thus to show S is a subring.

- Subring Test

1) $1_R \in S$

2) if $s, t \in S$, then $s-t$, st are all in S.

* If 2) holds, then $0 = s-s \in S$ $\quad -t = 0-t \in S$

ex. We have a chain of commutative rings.

$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

ex. If R is a ring. the center $Z(G)$ of R is defined to be:

$$Z(G) = \{z \in R : zr = rz \quad \forall r \in R\}$$

* $1_R \in Z(R)$

* If $s, t \in Z(R)$. then for all $r \in R$.

$$(s-t)r = sr - tr = rs - rt = r(s-t)$$

$$(st)r = s(tr) = s(rt) = r(st)$$

By subring test. $Z(R)$ is a subring of R.

ex. Let $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z} \quad i^2 = -1\}$

Then one can show $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$.

called the ring of Gausian integer

8.3 Ideals

Let R be a ring and A an additive subgp of R.

$\because$ $(R, +)$ is abelian $\therefore A \triangleleft R$.

Thus we have additive quotient gp:

$$R/A = \{r+A : r \in R\} \text{ with } r+A = \{r+a : a \in A\}$$

- prop 8.3

Let R be a ring and A an additive subgp of R.

For $r, s \in R$, we have

1) $r+A = s+A \iff r-s \in A$

2) $(r+A)+(s+A) = r+s+A$

3) $0+A = A$ $\quad$ 0: additive identity of R/A

4) $-(r+A) = (-r)+A$ $\quad$ $-A$: additive inverse of $r+A$

5) $k(r+A) = kr+A$ $\quad \forall k \in \mathbb{Z}$

Since R is a ring, it is natural to ask if we could make R/A to be a ring.
A natural way to define multiplication in R/A is:

$$(r+A)(s+A) = rs+A \quad \forall r, s \in R. \quad (*)$$

$\ast$ We could have $r+A = r_1+A$, $s+A = s_1+A$ with $r \neq r_1$ $s \neq s_1$

Thus in order for $(*)$ to make sense, a necessary condition is:

$r+A = r_1+A$ $\quad s+A = s_1+A$ $\quad rs+A = r_1s_1+A$

In this case, $(r+A)(s+A)$ is <u>well-defined</u>

- prop 8.4

Let A be a additive subgp of a ring R. $a \in A$.

define $Ra = \{ra : r \in R\}$ $\quad aR = \{ar : r \in R\}$

The following statements are equivalent:

1) $Ra \subseteq A \quad aR \subseteq A$ for every $a \in A$.

2) For $r, s \in R$. the multiplication $(r+A)(s+A) = rs + A$. is well-defined in R/A.

proof: 1) $\Rightarrow$ 2) if $r+A = r_1 + A \quad s+A = s_1 + A$. We need to show $rs+A = r_1 s_1 + A$

$\because (r-r_1) \in A \quad (s-s_1) \in A$

$\therefore rs - r_1 s_1 = rs - r_1 s + r_1 s - r_1 s_1$

$= (r-r_1)s + r_1(s-s_1) \in (r-r_1)R + R(s-s_1) \subseteq A$

by prop 8.3 1). $rs + A = r_1 s_1 + A$.

2) $\Rightarrow$ 1) Let $r \in R$. $a \in A$.

by prop 8.1 1). $ra + A = (r+A)(a+A)$

$= (r+A)(0+A)$

$= 0 + A = A$

Thus $ra \in A$. $Ra \subseteq A$

- def. ideal.

An additive subgp A, of a ring R is an ideal of R if $aR \subseteq A$ for every a.

Thus A of R is an ideal of $0 \in A$ → additive subgp

For $a, b \in A$. r on R. We have $ra, ar \in A$. $a - b \in A$.

ex. If R is a ring. then $\{0\}$ & R are ideal.

ex. let R be commutative ring. $a_1 \cdots a_n \in R$;

Consider set I generated by $a_1 \cdots a_n$

ie. $I = \langle a_1, a_2, \cdots, a_n \rangle = \{ r_1 a_1 + \cdots + r_n a_n : r_i \in R \}$

Then I is ideal.

- prop 8.5

Let A be an ideal of a ring R.

If $1_R \in A$. then $A = R$

unity

proof: For every $r \in R$.

$\because$ A is an ideal. $1_R \in A$

$\therefore$ we have $r = r \cdot 1_R \in A$.

$R \subseteq A \subseteq R$ Hence $R = A$.

- prop 8.6

Let A be an ideal of a ring R.

Then the additive quotient gp R/A is a ring with multiplication:

$$(r+A)(s+A) = rs + A$$

The unity of R/A is $1 + A$.

- def. quotient ring

set of $ra = ar \in A$.

Let A be an ideal of a ring R.

The ring R/A is a quotient ring of R by A.

- def. principal ideal generated by a

对应 cyclic

Let R be a commutative ring. A be an ideal of R.

If $A = aR = \{ar : r \in R\} = Ra$. for some $a \in R$.

Then A is a principal ideal generated by a 写作 $A = \langle a \rangle$

(additive) $n \cdot a = 1$

- prop 8.7.

All ideals of $\mathbb{Z}$ are of the form $\langle a \rangle$ for some $n \in \mathbb{Z}$.

If $\langle n \rangle \neq \langle 0 \rangle$. $n \in \mathbb{N}$. Then the generator is uniquely determined.

proof:

Let A be an ideal of $\mathbb{Z}$.

- If $A=\{0\}$. Then $A=\langle 0\rangle$.
- If $A\neq\{0\}$. choose $a\in A$. with $a\neq 0$. and $|a|$ minimum

Clearly. $\langle a\rangle\subseteq A$.

To prove another inclusion. let $b\in A$.

By the division algorithm, we have $b=qa+r$. $q.r\in\mathbb{Z}$. $0\leq r<|a|$

if $r\neq 0$.

$\because A$ is an ideal $a, b\in A$

$\therefore r=b-qa\in A$. $|r|<|a|$. contradicts property of $|a|$

So $r=0$. $b=qa$. i.e. $b\in\langle a\rangle$ which follows $A=\langle a\rangle$.

假设 $A=\langle a\rangle=\langle a_1\rangle$

$\langle -2\rangle$ 和 $\langle 2\rangle$ 是一个东西

let $a_1\in A$, s.t. $\langle a_1\rangle=A$

then $a=q_1a_1$ for some $q_1\in\mathbb{Z}$

$a_1=qa$ for some $q\in\mathbb{Z}$

thus we have $a|a_1$ and $a_1|a$.

thus. $a=a_1$

8.4 Isomorphism Thms.

- def. ring homomorphism.

  Let R & S be rings.

  mapping $\theta: R \to S$ is a ring homomorphism if $\forall a, b \in R$:

  1) $\theta(a+b) = \theta(a) + \theta(b)$

  2) $\theta(ab) = \theta(ba)$

  3) $\theta(1_R) = 1_S$

ex. The mapping $k \to [k]$ for $\mathbb{Z}$ to $\mathbb{Z}_n$ is an onto ring HM

ex. If R_1 & R_2 be rings.

the projection $\pi_1 : R_1 \times R_2 \to R_1$ defined by $\pi_1(r_1 r_2) = r_1$ is an onto ring HM.

$\pi_2 : R_1 \times R_2 \to R_2$ defined by $\pi_1(r_1 r_2) = r_1$ is an onto ring HM.

- prop 8.8

  Let $\theta: R \to R$ is a ring HM. and $r \in R$. Then

  1) $\theta(0_R) = 0_S$

  2) $\theta(-r) = -\theta(r)$

  3) $\theta(kr) = k\theta(r)$ $\quad \forall k \in \mathbb{Z}$.

  4) $\theta(r^n) = \theta(r)^n$ $\quad \forall n \in \mathbb{N} \cup \{0\}$. non-negative

  5) if $u \in R^n$ (set of elements of R which has a multiplicative inverse)

     Then $\theta(u^k) = \theta(u)^k$ $\quad \forall k \in \mathbb{Z}$. unit of R

- def. ring isomorphism.

  A mapping of rings $\theta: R \to S$ is a ring isomorphism of θ is a homomorphism and θ is bijective.

  R & S are isomorphic. 记作 $R \cong S$.

- def. kernel & image

Let $\theta: R \to S$ be a ring HM.

The kernel of θ is defined by $\ker\theta = \{r \in R : \theta(r) = 0\} \subseteq R$. ideal

The image of θ is defined by $\operatorname{im}\theta = \theta(R) = \{\theta(r) : r \in R\} \subseteq S$.

subring

Group theorey 中, $\ker\theta$ & $\operatorname{im}\theta$ 分别是 additive subgps of R & S.

↓ 由此引出

- prop 8.9.

Let $\theta: R \to S$ be a ring HM. Then

1) $\operatorname{im}\theta$ is a subring of S

2) $\ker\theta$ is an ideal of R.

proof:

1) ∵ $\operatorname{im}\theta = \theta(R)$ is an additive subgp of S.

∴ $\theta(R)$ is closed under multiplication

$1_S \in \theta(R) \to 1_S = \theta(1_R) \in \theta(R)$

if $s_1 = \theta(r_1)$ $s_2 = \theta(r_2)$ are in $\theta(R)$, then $s_1 s_2 = \theta(r_1)\theta(r_2) = \theta(r_1 r_2) \in \theta(R)$

∴ $\operatorname{im}\theta$ is a subring of S

2) ∵ $\ker\theta$ is an additive subgp of R

∴ $ra \cdot ar \in \ker\theta$ for all $r \in R$. $a \in \ker\theta$.

if $r \in R$ $a \in \ker\theta$. then $\theta(ra) = \theta(r)\theta(a) = \theta(r)\cdot 0 = 0$

Thus $ra \in \ker\theta$. 同理. $ar \in \ker\theta$

Thus $\ker\theta$ is an ideal of R.

- Thm 8.10 (1st IM Thm.)

Let $\theta: R \to S$ be a ring HM.

We have $R/\ker\theta \cong \operatorname{im}\theta$.

proof: Let $A = \ker\theta$.

$\because$ A is an ideal of R. $\therefore$ R/A is a ring.

Define the ring map $\bar{\theta}: R/A \to \operatorname{im}\theta$. $\bar{\theta}(r+A) = \theta(r)$ $\forall\, r+A \in R/A$.

$r+A = s+A$.

$\Rightarrow$ $r-s \in A$ $\Rightarrow$ $\theta(r-s) = 0$ $\Rightarrow$ $\theta(r) = \theta(s)$

$\therefore$ $\bar{\theta}$ is well-defined and 1-1

$\because$ $\bar{\theta}$ is clearly onto. $\bar{\theta}$ is a ring HM

$\therefore$ $\bar{\theta}$ is a ring IM and $R/\ker\theta \cong \operatorname{im}\theta$.

- prop 8.11.

Let R be a ring. A. B be subsets of R.

1) If A & B be 2 subrings of R. $1_A = 1_B = 1_R$.

Then $A \cap B$ is a subring of R.

2) If A is a subring. B is an ideal of R.

Then $A+B$ is a subring of R.

3) If A & B be ideals of R, then $A+B$ is an ideal of R.

- Thm 8.12 (2nd IM Thm)

Let A be a subring. B be an ideal of a ring R.

Then $A+B$ is a subring of B. B is an ideal of $A+B$.

$A \cap B$ is an ideal of A. $(A+B)/B \cong A/A\cap B$

- Thm 8.13 (3rd IM Thm)

Let A & B be ideals of a ring with $A \subseteq B$.

Then B/A is an ideal of R/A. and $(R/A)/(B/A) \cong R/B$.

$\forall z : n \mid z$

$$\gcd(m,n)=1 \Rightarrow \begin{cases} x \equiv b \pmod m & x \in \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \\ x \equiv c \pmod n & x \in \mathbb{Z}_m = \mathbb{Z}/m\cdot\mathbb{Z} \end{cases}$$

$\because \gcd(m,n)=1$

$\Rightarrow$ by 8.14 $x \in \mathbb{Z}_{mn}$.

ring ideal $\langle n \rangle$ $\langle m \rangle$

- Thm 8.14. CRT.

Let A. B be ideals of R.

1) If $A+B=R$. then $R/(A\cap B) \cong R/A \times R/B$.

2) If $A+B=R$ $A \cap B = \{0\}$. Then $R \cong R/A \times R/B$.

proof: (2) is a direct consequence of (1).

Thus it suffices to prove (1)

Define $\theta: R \to R/A \times R/B$. by $\theta(r) = (r+A, r+B)$ for all $r \in R$.

Then θ is a ring HM.

To show θ is onto. Let $(s+A, r+B) \in R/A \times R/B$ s.t $\in R$.

$\because A+B=R$

$\therefore \exists a \in A$. $b \in B$ s.t $a+b=1$

Let $r = sb+ta$.

Then $s-r = s-sb-ta = s(1-b)-ta = (s-t)a \in A$.

Thus $s+A = r+A$

同理 $\theta(r) = (r+A, r+B) = (s+A, t+B)$

$\therefore \operatorname{im}\theta = R/A \times R/B$

$\because \operatorname{Ker}\theta = A \cap B$

$\therefore$ by 1st IM thm. $R/(A\cap B) \cong R/A \times R/B$.

Let $m, n \in \mathbb{N}$. $\gcd(m, n) = 1$.

By Euclid Lemma. $1 = mr + ns$. for some $r, s \in \mathbb{Z}$

Then $1 \in m\mathbb{Z} + n\mathbb{Z}$. $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$.

$\because \gcd(m, n) = 1$ $\quad \therefore m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$

By CRT, we have:

- Cor 8.15

1) If $m, n \in \mathbb{N}$. $\gcd(m, n) = 1$. Then $\mathbb{Z}_{mn} = \mathbb{Z}_m \times \mathbb{Z}_n$

2) If $m, n \in \mathbb{N}$ $m, n \geq 2$. $\gcd(m, n) = 1$

Then $\varphi(m, n) = \varphi(m)\varphi(n)$. $\quad \underline{\varphi(m) = |\mathbb{Z}_m^*|}$

$\hookrightarrow$ Euler Phi-function

$\phi(m) = \#\{a : 1 \leq a \leq m . \gcd(a, m) = 1\}$

Phi function formula: ① $\phi(p^k) = p^k - p^{k-1}$

② $\phi(mn) = \phi(m)\phi(n)$

$F(n) = \phi(d_1) + \cdots + \phi(d_r) = n$ $\quad$ ($d_1, \cdots, d_n$是 n 的因数)

* Let $m, n \in \mathbb{Z}$. $\gcd(m, n) = 1$.

For $a, b \in \mathbb{Z}$. By Cor 8.14. for $[a] \in \mathbb{Z}_m$ $[b] \in \mathbb{Z}_n$.

$\exists [c] \in \mathbb{Z}_{mn}$ s.t $[c] = [a]$ in $\mathbb{Z}_m$. $[c] = [b]$ in $\mathbb{Z}_n$.

$\Rightarrow x \equiv a \pmod m$ $x \equiv b \pmod n$ has unique solution of the form $x \equiv c \pmod{mn}$

- prop 8.16

If R is a ring. $|R| = p$ ($p \in$ prime). Then $R \cong \mathbb{Z}_p$

proof: Define $\theta : \mathbb{Z}_p \to R$. $\quad \theta([k]) = k \cdot 1_R$

$\because R$ is an additive gp $|R| = p$

$\therefore$ By Lagrange thm. $o(1_R) = 1$ or p.

$\because \mathbb{1}_R \neq 0 \quad o(\mathbb{1}_R) = p.$

$$
\begin{aligned}
\therefore [k] = [m] &\iff p \mid k-m \\
&\iff |k-m| \cdot \mathbb{1}_R = 0 \\
&\iff k \cdot \mathbb{1}_R = m \cdot \mathbb{1}_R
\end{aligned}
$$

Thus, θ well-defined and one-to-one

Also, θ is ring HM.

$\because |\mathbb{Z}_p| = p = |R| \quad \theta$ is one-to-one

$\therefore \theta$ is onto

Thus $\mathbb{Z}_p \cong R$.

9. Commutative Ring

9.1 Integral domain & Fields

- Unit　　　　　　　　　u & u^{-1} 都在 R 中

  Let R be a ring.

  $u \in R$ be a unit if u has a multiplicative inverse in R, u^{-1}

- $uu^{-1} = 1 = u^{-1}u$.

- If u is a unit in R, $r, s \in R$. $ur = us \Leftrightarrow r = s$.

  Let R^* denote the set of all units in R.

  $(R^*, \cdot)$ is a gp. → 叫作 group of units of R.

  * 2 is a unit in $\mathbb{Q}$. but not a unit in $\mathbb{Z}$.

- division ring.　　　　除0外 每个 element u 都有 u^{-1}

  A ring $R \neq \{0\}$ is a division ring if $R^* = R \setminus \{0\}$

  i.e every non-zero element of R is a unit in R.

  ✱ A commutative division Ring is a field.

ex. $\mathbb{Q}$; $\mathbb{R}$; $\mathbb{C}$ are fields. $\mathbb{Z}$ is not a field.

ex. $[a][x] = [1]$ has solution in $\mathbb{Z}$ $\Leftrightarrow$ $\gcd(a, n) = 1$

Thus if $n = p$, is a prime, then $\gcd(a, p) = 1$ for all $a \in \{1, 2, \cdots, p-1\}$

Thus $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$. $\mathbb{Z}_p$ is a field.

However, if n is not a prime, $\exists$ a, b, $ab = n$ $1 < a \leq b < n$

Then, the non-zero congruence class $[a][b]$ are not units in $\mathbb{Z}_n$.

Since there is no sol s.t. $[a][x] = [1]$. Hence, $\mathbb{Z}_n^* \neq \mathbb{Z} \setminus \{0\}$

Thus, $\mathbb{Z}_n$ is a field $\Leftrightarrow$ n is prime

* If R is a division ring or field, then its only ideal are $\{0\}$ or R.

- Wedderburns Little Theorem

  Finite division ring is a field.

- Zero divisor

  Let $R \neq \{0\}$ be a ring. For $0 \neq a \in R$.

  a is a zero divisor if $\exists\, 0 \neq b \in R$. s.t. $ab = 0$

  ep. $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ is a zero divisor in $M_2(\mathbb{R})$

  在Matrix中. 所有RREF可化成 Identity matrix 的 都没 zero divisor.

- prop 4.1

  Given a ring R. TFAE:

  1) if $ab = 0$ in R, then $a = 0$ or $b = 0$

  2) if $ab = ac$ in R. $a \neq 0$. then $b = c$.

  3) if $ba = ca$ in R. $a \neq 0$ then $b = c$

proof:

1) $\Rightarrow$ 2) Let $ab = ac$ $a \neq 0$. $\Rightarrow a(b-c) = 0$.

$\because a \neq 0$ $\therefore b = c$

2) $\Rightarrow$ 1) Let $ab = 0$ in R.

case 1: $a = 0$ we are done

case 2: $ab = 0 = a \cdot 0$ $\Rightarrow b = 0$ done

1) $\Leftrightarrow$ 3) 同理

- integral domain

  A commutative ring $R \neq \{0\}$ is integral domain if it has no zero divison

  i.e. $ab = 0 \Rightarrow a = 0$ or $b = 0$

ex. If p is a prime. then $p \mid ab$
$\Rightarrow p \mid a$ or $p \mid b$.

i.e $[a][b]=[0]$ in $\mathbb{Z}_p$ $\Rightarrow$ $[a]=0$ or $[b]=0$

Thus $\mathbb{Z}_p$ is an integral domain.

However, $n=ab\,(1<a,b<n) \Rightarrow [a][b]=[0]$ ($[a]\neq[0]$ $[b]\neq[0]$)

Thus $\mathbb{Z}_n$ is an integral domain $\Leftrightarrow$ n is prime

commutative division ring $uu^{-1}=1$

- prop 9.2

Every field is an integral domain. $\rightarrow$ $ab=0 \Rightarrow a=0$ or $b=0$

proof. Let $ab=0$ in a field R.

We want to show $a=0$ or $b=0$

case 1: If $a=0$, then we are done.

case 2: If $a\neq 0$ then $a^{-1}ab=b=a^{-1}\cdot 0 \Rightarrow b=0$

Thus, R is an integral domain

* 1) Using the proof of 9.2. We can show that every subring of a field in an integral domain

2) The converse of prop 9.2 is not true.

ep. $\mathbb{Z}$ is an ID, but not a field.

ex. The Gaussian ring $\mathbb{Z}[i]=\{a+bi : a,b\in\mathbb{Z}\}$

$\because (\mathbb{Z}[i])^* = \{\pm 1, \pm i\}$ $\mathbb{Z}[i]$ is not a field.

- prop 9.3

Every finite integral domain is a field.

* infinite 不一定是 field ep. $\mathbb{Z}$. $GL_n(\mathbb{R}) \rightarrow n\times n$. $\det \neq 0$

proof: Let R be an ID. $a \in R$ $a \neq 0$.

Consider the map $\theta: R \to R$ defined by $\theta(r) = ar$

$\because$ R is an I.D. $ar = as$ $a \neq 0$

$\therefore$ $r = s$. $\therefore$ θ is injective.

In particular, $\exists$ $b \in R$ s.t $ab = 1$

$\because$ R is commutative,

$\therefore$ $ab = 1 = ba$ i.e. a is a unit

$\therefore$ R is a field.

- prop 9.4

The characteristic of any integral domain is either 0 or a prime p.

proof: Let R be an I.D.

1) If $ch(R) = 0$. Then we are done.

2) If $ch(R) = n \in \mathbb{N}$.

prove by contradiction: Suppose n is not a prime $n = ab$.

If 1 is the unity of R, then by prop 8.1. $(1 < a, b < n)$

$(a \cdot 1)(b \cdot 1) = (a \cdot b)(1 \cdot 1) = n \cdot 1 = 0$

$\because$ R is an ID.

$\therefore$ $a \cdot 1 = 0$ or $b \cdot 1 = 0$ which leads to a contradiction since $o(1) = n$.

$\therefore$ n is a prime.

※ Let R be an ID with $ch(R) = p$. a prime

首次 order 都 divides p.

For $a, b \in R$. we have $(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a b^{p-1} + b^p$

$\because$ p is a prime $p \mid \binom{p}{i}$ for all $1 \leq i \leq (p-1)$ $\frac{p!}{i!(p-i)!}$

$\because$ $ch(R) = p$ $\therefore$ $(a+b)^p = a^p + b^p$

9.2 Prime ideals & Maximal Ideals

- def. prime ideal

  Let R be a commutative ring. $ab=ba$

  An ideal $P \neq R$ of R is a prime ideal

  if every $r, s \in R$ satisfy $rs \in P$. Then $r \in P$ or $s \in P$

* Let p be a prime. $a, b \in \mathbb{Z}$.

Then $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

相当于 $ab \in p\mathbb{Z} \Rightarrow a \in p\mathbb{Z}$ $b \in p\mathbb{Z}$ → prime ideal

ex. $\{0\}$ is a prime ideal of $\mathbb{Z}$ $ab=0 \Rightarrow a=0$ $b=0$

ex. For $n \in \mathbb{N}$. $n \geq 2$.

$n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ $\Leftrightarrow$ n is a prime

- prop 9.5.

  If R is commutative ring, $rs = sr \in R$

  then an ideal P of R is a prime ideal $\Leftrightarrow$ R/P is int domain

proof: R & R/P → P: ideal of R. are commutative ring

$R/P \neq \{0\} \Leftrightarrow 0+P \neq 1+P$ → unity $1 \notin P$.

$\Leftrightarrow 1 \notin P$

$\Leftrightarrow P \neq R$. $R \neq R \cdot 1 \notin P$.

Also, for $r, s \in R$. we have:

P is a prime ideal $\Leftrightarrow rs \in P \Rightarrow r \in P$ or $s \in P$

$\Leftrightarrow (r+P)(s+P) = 0+P. \Rightarrow r+P = 0+P$ or $s+P = 0+P$

$\Leftrightarrow R/P$ is int domain

- maximal ideal

Let R be a commutative ring.

An ideal $M \neq R$ of R is a maximal ideal if whenever A is an ideal s.t. $M \subseteq A \subseteq R$. then $A = M$ or $A = R$.

ex. if $r \notin M$, then the ideal $\langle r \rangle + M = R$. if M is maximal

ex. $\mathbb{Z}_{10}$ in maximum ideal : $\mathbb{Z}_2$. $\mathbb{Z}_5$

- prop 9.6

If R is a commutative ring, then an ideal M of R is a maximal ideal $\Leftrightarrow$ R/M is a field

proof: ∵ R & R/M is a commutative ring,

∴ $R/M \neq \{0\}$ $\Leftrightarrow$ $0+M \neq 1+M$

$\Leftrightarrow$ $1 \notin M$

$\Leftrightarrow$ $M \neq R$. max & prime ideal : $M \neq R$

Also for $r \in R$, note that $r \notin M$ $\Leftrightarrow$ $r+M \neq 0+M$

M is a maximal ideal

$\Leftrightarrow$ $\langle r \rangle + M = R$ for any $r \notin M$

$\Leftrightarrow$ $1 \in \langle r \rangle + M$ for any $r \notin M$

$\Leftrightarrow$ for any $r \notin M$, $\exists$ $r+M \in R/M$ s.t. $(r+M)(s+M) = 1+M$

$\Leftrightarrow$ R/M is a field.

- cor 9.7 (结合 9.2 . 9.5 . 9.6)

Every maximal ideal of a commutative ring is a prime ideal.

* The converse of cor 9.7 is not true

ep. in $\mathbb{Z}$. $\{0\}$ is a prime ideal. but not a maximal ideal.

ex. Consider the ideal $\langle x^2+1 \rangle$ in the ring $\mathbb{Z}[x]$

The map $\theta : \mathbb{Z}[x] \to \mathbb{Z}[i]$ defined by:

$\theta(f(x)) = f(i)$ is surjective since $\theta(a+bx) = a+bi$

Also $\ker \theta = \langle x^2+1 \rangle$.

By 1st IM thm. $\mathbb{Z}[x]/\langle x^2+1 \rangle \cong \mathbb{Z}[i]$

$\because$ $\mathbb{Z}[i]$ is an ID, but not a field.

$\therefore$ the ideal $\langle x^2+1 \rangle$ is a prime, but not maximal.

$uu^{-1} = 1$

maximal ideal : R/M 是 field commutative division ring

max 是 prime

field 都是 ID

prime ideal : 是 int domain $ab = 0 \Rightarrow a = 0$ or $b = 0$

9.3 Fields of Fractions

We recall that every subring of a field is an ID.

The "converse" also hold. every integral domain R is isomorphic to a subring of a field F.

Let R be an ID. $D = R \setminus \{0\}$.

Consider the set $X = R \times D = \{(r,s) : r \in R,\ s \in D\}$.

We say $(r,s) \equiv (r_1, s_1)$ on $X \Leftrightarrow rs_1 = r_1 s$

In particular 1) $(r,s) \equiv (r,s)$

2) $(r,s) \equiv (r_1, s_1) \Rightarrow (r_1, s_1) \equiv (r,s)$

3) $\begin{cases} (r,s) \equiv (r_1, s_1) \\ (r_1, s_1) \equiv (r_2, s_2) \end{cases} \Rightarrow (r,s) \equiv (r_2, s_2)$

- fraction $\frac{r}{s}$

Motivated by the case $R = \mathbb{Z}$. We define the fraction $\frac{r}{s}$ to be the equivalence class $[(r,s)]$ of the pair $(r,s) \in X$.

Let F denote the set of all these fractions. i.e

$$F = \{\tfrac{r}{s} : r \in R,\ s \in D\} = \{\tfrac{r}{s} : r, s \in R,\ s \neq 0\}$$

- addition & multiplication of F

$$\frac{r}{s} + \frac{r_1}{s_1} = \frac{rs_1 + r_1 s}{ss_1}$$

$$\frac{r}{s} \cdot \frac{r_1}{s_1} = \frac{rr_1}{ss_1}$$

(ss_1, $rs_1 + r_1 s$, rr_1 are elements of R)

- Thm 9.8.

Let R be an ID.

Then $\exists$ a field F consisting of fractions $\frac{r}{s}$. with $r.s \in R$. $s \neq 0$.

By identifying $r = \frac{r}{1}$ for all $r \in R$.

proof:

Note that $ss_1 \neq 0$. (Since R is an ID and thus these operations are well-defined.

Then one can show :

F becomes a field with the zero being $\frac{0}{1}$. unity being $\frac{1}{1}$.

Negation $\frac{r}{s}$ is $\frac{-r}{s}$.

Moreover, if $\frac{r}{s} \neq 0$ in F, then $r \neq 0$. $\Rightarrow \frac{s}{r} \in F$.

Then we have $\frac{r}{s} \cdot \frac{s}{r} = \frac{rs}{sr} = 1 \in F$

In addition, we have $R \cong R'$. $R' = \{\frac{r}{1} : r \in R\} \subseteq F$

10. Polynomial Rings

10.1. Polynomials

- Polynomial in x over R

  Let R be a ring and x be a variable.

  $R[x] = \{ f(x) = a_0 + a_1 x + \cdots + a_m x^m : m \in \mathbb{N} \cup \{0\} \quad a_i \in R \ (0 \le i \le m) \}$

  Such $f(x)$ is polynomial in x over R.

  $*$ $f(x) = 0 \Rightarrow a_0 = \cdots = 0.$ $\quad$ $*$ $\deg 0 = -\infty$

- Addition & multiplication on $R[x]$

  Let $f(x) = a_0 + a_1 x + \cdots + a_m x^m \in R[x]$

  $g(x) = b_0 + b_1 x + \cdots + b_n x^n \in R[x]$ with $m \le n$.

  Then we write $a_i = 0$ for $m+1 \le i \le n$.

  Addition on $R[x]$: $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1) x + \cdots + (a_n + b_n) x^n$

  Multiplication on $R[x]$: $f(x) \cdot g(x) = (a_0 + a_1 x + \cdots + a_m x^m)(b_0 + b_1 x + \cdots + b_n x^n)$

  $= a_0 b_0 + (a_1 b_0 + a_0 b_1) x + \cdots + a_m b_n x^{n+m}$

  $= c_0 + c_1 x + \cdots + c_{m+n} x^{m+n}$ $\quad c_i = \sum_{k=0}^{i} a_k b_{i-k}$

- prop 10.1

  Let R be a ring and x be variable

  1) $R[x]$ is a ring
  2) R is a subring of $R[x]$.
  3) If $Z = Z(R)$ denote the center of R, then $Z(R[x]) = Z[x]$

proof: 3) Let $f(x) = \sum_{i=0}^{m} a_i x^i \in Z[x]$ $\quad g(x) = \sum_{i=0}^{n} b_i x^i \in R[x]$.

$f(x) g(x) = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n}$ $\quad c_i = \sum_{k=0}^{i} a_k b_{i-k}$.

$\because a_i \in Z$. $\quad \therefore a_i b_j = b_j a_i \quad \forall i, j$.

$\therefore f(x)g(x) = g(x)f(x)$ $\quad Z[x] \subseteq Z(R[x])$.

To show the other inclusion, if $f(x) = \sum_{i=0}^{m} a_i x^i \in Z(R[x])$

then $f(x) \cdot b = b \cdot f(x) \quad \forall b \in R$.

$\Rightarrow a_i b = b a_i \quad 0 \le i \le m$

$\Rightarrow a_i \in Z$. $\quad Z(R[x]) \subseteq Z[x]$

$\Rightarrow Z(R[x]) = Z[x]$

- prop 10.2

Let R be an ID. Then

1) $R[x]$ is an ID.

2) if $f \neq 0$. $g \neq 0$ in $R[x]$. Then $\deg(fg) = \deg(f) + \deg(g)$

3) The units in $R[x]$ are R^*. the units in R.

proof: 2) Suppose $f(x) \neq 0$ $g(x) \neq 0$ are polynomials in $R[x]$.

$f(x) = a_0 + \cdots + a_m x^m \qquad g(x) = b_0 + \cdots + b_n x^n$. $\quad a_m \neq 0 \neq b_n$

Then $fg(x) = (a_m b_n) x^{m+n} + \cdots + a_0 b_0$

$\because R$ is an ID. $\quad a_m b_n \neq 0 \qquad f(x) g(x) \neq 0$.

$\therefore R[x]$ is an ID.

$\therefore \deg(fg) = \deg(f) + \deg(g)$

3) Let $u(x) \in R[x]$ be a unit with the inverse $v(x)$

$\because u(x) \cdot v(x) = 1 \qquad \therefore \deg u + \deg v = 0 \qquad u(x) \neq 0 \quad v(x) \neq 0$

$\because \deg u \geq 0 \qquad \deg v \geq 0$

$\therefore \deg u = 0 = \deg v$.

Thus $u(x), v(x)$ are units in R. $\quad (R[x])^* = R^*$

* In $\mathbb{Z}_4[x]$, $2x \cdot 2x = 4x^2 = 0$.

Thus $\deg(2x) + \deg(2x) \neq \deg(2x \cdot 2x)$

$\therefore$ The product formula in prop 10.2 only applies when R is an ID.

* To extend, the product formula in prop 10.2 to 0.

We define $\deg(0) = \pm\infty$.

10.2 Polynomial over a field.

- def. divides

  Let f be a field. $f(x), g(x) \in F(x)$

  $f(x)$ divides $g(x)$ if there exists $q(x) \in F[x]$ s.t $g(x) = q(x) \cdot f(x)$

  记作 $f(x) \mid g(x)$

- prop 10.3

  Let F be a field. $f(x), g(x), h(x) \in F[x]$

  1) $f(x) \mid g(x)$, $g(x) \mid h(x)$. $\Rightarrow f(x) \mid h(x)$

  2) $f(x) \mid g(x)$, $f(x) \mid h(x) \Rightarrow f(x) \mid (gu + hv)(x)$ for $u(x), v(x) \in F[x]$

- prop 10.4

  Let F be a field. $f(x), g(x) \in F[x]$ be monic polynomials.

  $f \mid g \wedge g \mid f \Rightarrow f(x) = g(x)$

proof: $\because f(x) \mid g(x)$ $g \mid f$.

$\therefore g(x) = r(x) f(x)$ $f(x) = s(x) g(x)$ for $s, r \in F[x]$.

$\therefore f = sg = srf$.

By prop 10.2. $\deg f = \deg s + \deg r + \deg f$. $\Rightarrow \deg s + \deg r = 0$

$\therefore f(x) = s g(x)$ for some $s \in F$

$\because$ both f & g are monic

$\therefore s = 1$. $\Rightarrow f = g$

* for $a, b \in \mathbb{Z}^+$, if $a \mid b$, $b \mid a$. $\Rightarrow a = b$

↳ The set of monic polynomials in $F[x]$ plays the same role as the set of positive integers in $\mathbb{Z}$.

- Division algorithm.

Let $\mathbb{F}$ be a field. $f(x)$. $g(x) \in \mathbb{F}[x]$ with $f(x) \neq 0$.

Then there exist unique $q(x)$. $r(x) \in F[x]$ s.t.

$$g(x) = q(x) f(x) + r(x) \quad \text{with } \deg r < \deg f.$$

* this includes the case for $r=0$. （同时解释 $\deg 0 = -\infty$）

proof: → Prove $q(x)$. $r(x)$ exist.

Prove by induction:

let $m = \deg$ $n = \deg g$.

If $n < m$. then $q(x) = 0$ $f(x) + g(x)$

Suppose $n \geq m$. and this holds for all $g(x) \in \mathbb{F}[x]$. with $\deg g < n$.

Write $f(x) = a_0 + a_1 x + \cdots + a_m x^m$ $a_m \neq 0$.

$g(x) = b_0 + b_1 x + \cdots + b_n x^n$

$\because \mathbb{F}$ is a field a_m^{-1} exists

$\therefore g_1(x) = g(x) - b_n a_m^{-1} x^{n-m} f(x)$

$= (b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0) - b_n a_m^{-1} x^{n-m} [a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0)$

$= 0 x^n + (b_{n-1} - b_n a_m^{-1} a_{m-1}) x^{n-1} + \cdots$

$\because \deg g_1 < n$. $\therefore$ By induction. $\exists q_1(x)$ $r_1(x) \in \mathbb{F}[x]$. s.t. $g_1(x) = q_1(x) f(x) + r_1(x)$

→ Prove uniqueness.

Suppose we have $g(x) = q_1(x) f(x) + r_1(x)$ with $\deg r_1 < \deg f$.

Then $r(x) - r_1(x) = (q_1(x) - q(x)) f(x)$

If $q_1(x) - q(x) \neq 0$. Then:

$$\deg (r - r_1) = \deg ((q_1 - q) f) = \deg (q_1 - q) + \deg f \geq \deg f.$$

which leads to a contradiction since $\deg (r - r_1) < \deg f$.

Thus. $q_1(x) - q(x) = 0$. $\Rightarrow$ $r(x) - r_1(x) = 0$

$\therefore q_1(x) = q(x)$ $r_1(x) = r(x)$

- prop 10.6

Let F be a field. $f(x)$ $g(x) \in F[x]$ with $f(x) \neq 0$ $g(x) \neq 0$

Then there exists $d(x) \in F[x]$ which satisfies the following:

1) $d(x)$ is monic   最高次项系数为1.

2) $d(x) \mid f(x)$ $d(x) \mid g(x)$

3) if $e(x) \mid f(x)$ $e(x) \mid g(x)$ $\Rightarrow$ $e(x) \mid d(x)$

4) $d(x) = u(x) f(x) + v(x) g(x)$ for some $u(x), v(x) \in F[x]$.

※ if both $d(x)$ & $d_1(x)$ satisfy the above conditions.

$\because$ $d(x) \mid d_1(x)$ $d_1(x) \mid d(x)$. both monic

$\therefore$ $d(x) = d_1(x)$ by prop 10.4.

greatest commute divisor of $f(x)$ and $g(x)$

写作 $d(x) = \gcd(f(x), g(x))$

- irreducible

Let F be a field, a poly $l(x) \neq 0$ in $F[x]$ is irreducible if $\deg l \geq 1$. and whenever $l(x) = l_1(x) l_2(x)$ in $F[x]$

$\deg l_1 = 0$ or $\deg l_2 = 0$

ex. if $l(x) \in F[x]$ satisfy $\deg l = 0$. Then $l(x)$ is irreducible

ex. if $\deg f = 2$ or 3. Then f is irred $\Leftrightarrow$ $f(d) \neq 0$. for any $d \in F$.

ex. Let $l(x), f(x) \in F[x]$. If $l(x)$ is irreducible and $l(x) \nmid f(x)$.

Then $\gcd(l(x), f(x)) = 1$

- prop 10.7

Let F be a field. $f(x), g(x) \in F[x]$

If $l(x) \in F[x]$ is irred and $l(x) \mid f(x)g(x)$. Then $l(x) \mid f(x)$ or $l(x) \mid g(x)$

* Let $f_1(x), \cdots, f_n(x) \in F[x]$ and let $l(x) \in F[x]$ be irreducible

If $l(x) \mid f_1(x) \cdots f_n(x) \Rightarrow l(x) \mid f_i(x)$ for some i.

- Thm 10.8 Unique factorization Thm.

Let F be a field. $f(x) \in F[x]$ with $\deg f \geq 1$. Then we can write $f(x) = c\, l_1(x) \cdots l_m(x)$ where $c \in F^*$ and $l_i(x)$ are monic irred polynomials.

The factorization is unique up to the order of l_i

* Using Thm 10.8. we can prove $\exists \infty$ irred polynomials in $F[x]$

- Prop 10.9

Let F be a field. Then all ideals of $F[x]$ are of the form $\langle h(x) \rangle = h(x) F[x]$ for some $h(x) \in F[x]$.

If $\langle h(x) \rangle \neq 0$ and $h(x)$ is monic. Then the generator is uniquely determined.

* Let $A \neq \{0\}$ be an ideal of $F[x]$.

by prop 10.9. $A = \langle h(x) \rangle$ for a unique monic poly $h(x) \in F[x]$.

Suppose $\deg h = m \geq 1$. Consider the quotient ring $R = F[x]/A$.

Thus $R = \{ \overline{f(x)} = f(x) + A : f(x) \in F[x] \}$.

$t = \bar{x} = x + A$. $f(x) = q(x)h(x) + r(x)$

By division algorithm, $R = \{ \overline{a_0} + \overline{a_1} t + \cdots + \overline{a_{m-1}} t^{m-1} = a_i \in F \}$

Consider the map $\theta : F \to R$ given by $\theta(a) = \bar{a} = a + A$.

$\because \theta$ is not the zero map. $\ker \theta$ is an ideal of F

$\therefore \ker \theta = \{0\}$ $\therefore \theta$ is a 1-1 ring HM

$\because F \cong \theta(F)$

$\therefore$ by identifying F with $\theta(F)$. $R = \{ a_0 + a_1 t + \cdots + a_{m-1} t^{m-1} : a_i \in F \}$

In R, $a_0 + a_1 t + \cdots + a_{m-1} t^{m-1} = b_0 + b_1 t + \cdots + b_{m-1} t^{m-1}$

$\Leftrightarrow a_i = b_i$ for all $0 \leq i \leq m-1$.

- prop 10.10.

Let F be a field and $h(x) \in F[x]$ with $\deg h = m \geq 1$.

Then the quotient ring $R = F[x]/\langle h(x) \rangle$ is given by :

$R = \{ a_0 + a_1 t + \cdots + a_{m-1} t^{m-1} : a_i \in F.\ h(t) = \bar{0} = 0 + A \}$.

in which an element of R can be uniquely represented in above form

- prop 10.11

Let F be a field. $h(x) \in F[x]$ with $\deg h \geq 1$. TFAE :

1) $F[x]/\langle h(x) \rangle$ is a field

2) $F[x]/\langle h(x) \rangle$ is an ID

3) $h(x)$ is irred in $F[x]$

ex. Since $\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$ which is a field.

The poly x^2+1 is irred in $\mathbb{R}[x]$.

proof:

(1) ⇒ (2) A field is an ID.

(2) ⇒ (3) if $h(x)=f(x)g(x)$ with $f(x), g(x) \in F[x]$.

then $(f(x)+A)(h(x)+A) = f(x)g(x)+A = h(x)+A = 0+A$. in $F[x]/A$.

By (2), either $f(x)+A = 0+A$ or $g(x)+A=0+A$

If $f(x)\in A = \langle f(x)\rangle$. then $f(x)=g(x)h(x)$ for some $g(x)\in F[x]$

Thus $h(x)=f(x)g(x) = q(x)h(x)g(x)$

$\because F[x]$ is an I.D. $\therefore q(x)g(x)=1$ $\deg g=0$

同理, if $g(x)\in A$, then $\deg f=0$. Thus $h(x)$ is irred in $F[x]$

(3) ⇒ (1) Note that $F[x]/A$ is a commutative ring

Thus to show it is a field, it suffices to show that every nonzero element of $F[x]/A$ has an inverse

Let $f(x)+A \neq 0+A$. in $F[x]/A$.

$\because h(x)$ is irred and $h(x)\nmid f(x)$. $\gcd(h(x), f(x))=1$

$\therefore$ by prop 10.6. there exist $u(x), v(x)\in F[x]$ s.t

$$1=u(x)h(x)+v(x)f(x)$$

$\therefore (v(x)+A)(f(x)+A) = 1+A$ (since $h(x)\in A$)

$\therefore f(x)+A$ has an inverse in $F[x]/A$.

$\Rightarrow F[x]/\langle h(x)\rangle$ is a field.

ex. Since x^2+x+1 has no root in $\mathbb{Z}_2$, it is irred in $\mathbb{Z}_2[x]$.

Thus $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle = \{a+bt,\ a,b\in\mathbb{Z}_2.\ t^2+t+1=0\}$ is a field of 4 elements

Analysis between $\mathbb{Z}$ & $F[t]$

	$\mathbb{Z}$	$F[x]$
elements	m	$f(x)$
size	$\lvert m \rvert$	$\deg f$
units	$\{\pm 1\}$ $\mathbb{Z}\setminus\{0\}/\langle \pm 1 \rangle \cong \mathbb{N}$	F^* $(F[x]\setminus\{0\})/F^* \cong \{\text{monic poly}\}$
unique factorization	$m = \pm p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ p: prime	$f: c\, l_1^{\alpha_1} \cdots l_r^{\alpha_r} \quad c \in F^*$ $l_i = l_i(t) =$ monic irred.
ideals	$\langle n \rangle$ (unique if $n \in \mathbb{N}$) $\mathbb{Z}/\langle n \rangle$ is a field $\Leftrightarrow$ n is prime	$\langle h(x) \rangle$ (unique if $h(x)$ is monic) $F[x]/\langle h(x) \rangle$ is a field $\Leftrightarrow$ $h(x)$ is irred