CH9、代數系統

代數系統

目錄：

9.1 代數系統

2+3=5

2×3=6

a*b

定義：

*：A×B→C function

ex：∀ a∈ A, b∈ B, ∃! c∈ C ∋ *(a, b)=c，記作 a*b=c

當 A=B=C=S 時，稱*為 Binary Operation on S

定義：

$*_1, \ldots, *_k$ 為 S 上之 Binary Operation

稱(S, $*_1, \ldots, *_k$)為代數系統(Algebraic System, AS)

*表示法：二元運算表

(S, *)：Algebraic System,，S={$a_1, \ldots, a_n$}

	a_1	a_2	…	a_n
a_1	a_1*a_1	a_1*a_2		a_1*a_n
a_2	a_2*a_1	…		
…				
a_n	a_n*a_1			a_n*a_n

+	1	2	3
1	*2*	*3*	*4*
2	*3*	*4*	*5*
3	*4*	*5*	*6*

定義：

(S, *)：Algebraic System

1. 若∀ a, b ∈ S ⟹ a*b ∈ S，稱(S, *)具封閉性 Closed(Closure)。例：(ℤ, +)、(ℤ, -)、(ℤ, ×)；但(ℤ, ÷)不是
2. 若∀ a, b ∈ S ⟹ a*b=b*a，稱(S, *)具交換性 Commutative。例：(ℤ, +)、(ℤ, ×)；但(ℤ, -)、(ℤ, ÷)不是
3. 若∀ a, b ∈ S ⟹ (a*b)*c=a*(b*c)，稱(S, *)具結合性(Associative)；例：(ℤ, +)、(ℤ, ×)；但(ℤ, -)、(ℤ, ÷)不是

例(99 淡江)：S={[x, y] | x, y∈R}，[x, y]□[w, z]=[x+w, (b+d)/2]

1. *∀[a, b], [c, d] ∈S*
[a, b]□[c, d] = [a+c, (b+d)/2] ∈S
故(S, □)具 Closed

2. *∀[a, b], [c, d] ∈S*
[a, b]□[c, d] = [a+c, (b+d)/2]
[c, d]□[a, b] = [c+a, (d+b)/2]
故(S, □)具 Commutative

3. $\forall [a, b], [c, d], [x, y] \in S$
$([a, b]\square[c, d])\square[x, y] = [a+c, (b+d)/2]\square[x, y] = [a+c+x, ((b+d)/2+y)/2]$
$[a, b]\square([c, d]\square[x, y]) = [a, b]\square[c+x, (d+y)/2] = [a+c+x, (b+(d+y)/2)/2]$
兩者不相等，故(S, □)不具 Associative

$2+\underline{0}=2$
$-5+\underline{0}=-5$
$3\times\underline{1}=3$

定義：
(S, *)：Algebraic System
1. 若$\exists\ e_l\in S \ni \forall\ a\in S, e_l*a=a$，稱 e_l 為(S, *)之左單位元素 Left Identity
2. 若$\exists\ e_r\in S \ni \forall\ a\in S, a*e_r=a$，稱 e_r 為(S, *)之左單位元素 Right Identity
   例：(ℤ, -)之右單位元素為 0，但無左單位元素
3. 若$\exists\ e\in S \ni \forall\ a\in S, e*a=a=a*e$，稱 e 為(S, *)之單位元素 Identity
   例：(ℤ, +)之單位元素為 0

*	a	b	c
a	*b*	*c*	*a*
b	*a*	*b*	*c*
c	*c*	*b*	*a*

b 為左單位元素(列相同)、無右單位元素(無行相同)

定理：
(S, *)：Algebraic System，具有左單位元素 e_l、右單位元素 e_r，則 $e_l=e_r$
(單位元素必唯一)

證明：
$e_l=e_l*e_r=e_r$

例(98 成大)：
S={a, b, c, d, e}
1. S 上具 Closed 之 Binary Operation 個數為何？
2. 其中具 Commutative 之 Binary Operation 個數為何？
3. S 上具 Closed 具 c 為 Identity 之 Binary Operation 個數為何？
4. S 上具 Cosed 及 Identity 之 Binary Operation 個數為何？
5. 其中具 Commutative 之 Binary Operation 個數為何？

*	*a*	*b*	*c*	*d*	*e*
a					
b					
c					
d					
e					

1. *5^{25}*
2. *5^{15}*
3. *5^{16}*
4. *5×5^{16}*
5. *5×5^{10}*

定義

(S, *)：Algebraic System，具 Identity e，a ∈ S

1. 若∃ b_l∈S ∋ b_l*a=e，稱 b_l 為 A 之左反元素 Left Inverse
2. 若∃ b_r∈S ∋ a*b_r=e，稱 b_r 為 A 之右反元素 Right Inverse
3. 若∃ b∈S ∋ b*a=e=a*b，稱 b 為 A 之反元素 Inverse
4. 若∀ a∈S，a 之 Inverse 存在，稱(S, *)具 Inverse Property
   例：(ℤ, -)無單位元素，故沒有 Inverse Property

*	a	b	c
a	*c*	*a*	*b*
b	*a*	*b*	*c*
c	*b*	*c*	*a*

a→c, b→b, c→a

9.2 群

名稱	Closed	Associative	Identity	Inverse Preporty	*Commutative*
半群(Semigroup)	O	O			*(若有：交換半群)*
單群(Monoid)	O	O	O		*(若有：交換單群)*
群(Group)	O	O	O	O	*(若有：交換群)*
交換群(Abelian Group) *//以一數學家之命命名*	O	O	O	O	*O*

//交換性只是個形容詞，而不是只有 Abelian Group 才有交換性；只是交換群常見與重要，所以特別給予一個『以數學家命名』的專有名詞

例：

$(\mathbb{Z}, +)$：交換群

$(\mathbb{R}, +)$：交換群

$(\mathbb{R}, *)$：交換單群*(∵0 不存在 Inverse Property)*

$(\mathbb{R}^*, *)$：交換群

$(P(x), \cup)$：交換單群*(P(x)為 Power Set。P(x)={Φ, {1}, {2}, {1, 2}}, when x={1, 2})*

$A \cup \underline{\Phi} = A$，Φ 為單位元素

$A \cup \underline{X} = \Phi$，X 不存在

$(P(x), \cap)$：交換單群

$A \cap \underline{P(x)} = A$，P(x)為單位元素

$A \cap \underline{X} = P(x)$，X 不存在

$(P(x), \oplus)$：交換群

$A \oplus \underline{\Phi} = A$，Φ 為單位元素

$A \oplus \underline{A} = \Phi$，A 為反元素

$(\mathbb{R}^{m\times m}, *)$：非交換單群*(矩陣乘法無交換性)*

例：$G=\mathbb{R}^*$, $a*b=ab/2$，證：$(G, *)$ is an abelian group？

1. *Closed*：$\forall a, b \in G$, 則 $a \neq 0, b \neq 0$
   $\Longrightarrow a*b=ab/2 \neq 0 \Longrightarrow a*b \in G$
2. *Associative*：$\forall a, b, c \in G$
   $(a*b)*c = ab/2 * c = abc/4$
   $a*(b*c) = a * bc/2 = abc/4$
3. *Commutative*：$\forall a, b \in G$
   $a*b = ab/2 = ba/2 = b*a$
4. *Identity*：
   取 $e=2 \in G$, $\forall a \in G$, $e*a = a*e = a*2 = a2/2 = a$
   $\Longrightarrow e=2$ 為$(G, *)$之 Identity
5. *Inverse*：
   $\forall a \in G$，取 $b=4/a \in G$, $b*a = a*b = a*4/a = (a \times 4/a)/2 = 2 = e$
   $\Longrightarrow b$ 為 a 之 Inverse

定理：$(G, *)$：group

1. G 之 Identity 存在且唯一，記作 e
2. $\forall a \in G$, a 之 Inverse 存在唯一，記作 a^{-1}

證明：

1. 設 b, c 皆為 a 之 Inverse $\Longrightarrow a*b = e = b*a, a*c = e = c*a$
   $b = b*e = b*(a*c) = (b*a)*c = e*c = c$

(G, *)：a*b

(G, Δ)：aΔb

G：ab*(可省略中間的運算符號)*

定理：G：group，a, b∈G

1. $(a^{-1})^{-1} = a$
2. $(ab)^{-1} = b^{-1}a^{-1}$

證明：

1. $a\,a^{-1} = e = a^{-1}a$

   $\Longrightarrow (a^{-1})^{-1} = a$
2. $(ab)(b^{-1}a^{-1}) = a\,e\,a^{-1} = a\,a^{-1} = e$

   $(b^{-1}a^{-1})(ab) = b^{-1}\,e\,b = b^{-1}\,b = e$

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

例(5 個)(99 輔大)：G：group，若$\forall\, a \in G, a^2=e$ *//a2=(a*a)*

證：G is an abelian group？

$\forall a, b \in G$，則 $a^2=b^2=e$

$\Longrightarrow a^{-1}=a, b^{-1}=b$

$\because ab \in G,\ \therefore (ab)^2 = e, (ab)^{-1} = ab$

$\Longrightarrow b^{-1}a^{-1}=ab \Longrightarrow ba = ab$ (Commutative)

Notation：

(S, *)：Algebraic System，且具結合性

$a^2=a*a$

$a^3=a*a*a$

$a^k=a*\ldots*a$(共 k 個)

$a^0=e$

$a^{-k}=(a^k)^{-1}$

在加法群(ℤ, +)中：

a^k記作 ka = 3(2) = 6　　*//表示 2 加 3 次*

a^{-k}記作-ka = -3(2) = -6

Note：

G：group

1. 若 $ab=c$

   $\Longrightarrow a^{-1}ab = a^{-1}c$

   $\Longrightarrow eb = a^{-1} c \Longrightarrow b=a^{-1} c$
2. 若 $ab=c$

   $\Longrightarrow a=cb^{-1}$
3. 若 $ab=ac$

   $b = a^{-1}ac = ec = c$ $\therefore$群具有消去性

定義：$(S, *)$：Algebraic System

1. 若$\forall a, b, c \in S, a*b=a*c \Longrightarrow b=c$，稱$(S, *)$具左消去性
2. 若$\forall a, b, c \in S, b*a=c*a \Longrightarrow b=c$，稱$(S, *)$具右消去性
3. 若$(S, *)$具有左、右消去性，稱$(S, *)$具有消去性

$(\mathbb{Z}, \cdot)$ $2x=2y \Longrightarrow x=y$ *//就算不具有反元素，依然可以具有消去性*

定義：G：group，$|G|$稱 G 之 order，記作 $o(G)$ *//G 內之元素個數*

//『群』其實就是『集合』，只是內部元素可以執行特定的運算，且符號封閉性、交換性、具有單位元素、反元素特性…等

9.3 二個有限群

定義：

$n \in \mathbb{Z}^+$，在 $\mathbb{Z}$ 上定義一 Equivalent Relation $\equiv_n$ by $a \equiv_n b \Leftrightarrow n \mid (a-b)$對應等價類集合

$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$

n=5

$[0] = \{\ldots, -5, 0, 5, \ldots\}$

$[1] = \{\ldots, -4, 1, 6, \ldots\}$

$[2] = \{\ldots, -3, 2, 7, \ldots\}$

$[3] = \{\ldots, -2, 3, 8, \ldots\}$

$[4] = \{\ldots, -1, 4, 9, \ldots\}$

$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$

在 $\mathbb{Z}_n$ 上定義$+_n$ by $[a] +_n [b] = [a+b]$

$[1] +_5 [2] = [3]$、$[3] +_5 [4] = [7] = [2]$

$\Longrightarrow [a] +_n [b] = [(a+b) \bmod n]$

$(\mathbb{Z}_n, +_n)$為一 Abelian group with order n 稱為 Congruence of modulo n

Note：

1. $e = [0]$
2. $[a^{-1}] = [n-a]$
3. $\mathbb{Z}_{12} = \{0, 1, \ldots, 11\}$
   2+5=7、9+8=5、-5=7　//加法群中，5^{-1} 記作-5
4. $\mathbb{Z}_n \equiv \mathbb{Z} \pmod n$
5. $\mathbb{Z}_n = \{0, 1\}$

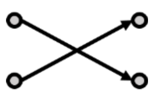
		even	odd
	+	0	1
even	0	*0*	*1*
odd	1	*1*	*0*

定義：

$A=\{1, \ldots, n\}$

$S_n = \{\alpha \mid \alpha = A \rightarrow A$ 1-1 且 onto$\}$

收集 function 等於是排列(Permutation)



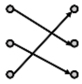
$(S_n, \circ)$：group with order n!

稱為 Permutation Group 或 Symmetric Group 排列群、重排群、對稱群

In general, S_n 不為 Abelian Group

Note：

1. $\alpha \in S_n$ 記作 α $\begin{pmatrix} 1 & \dots & n \\ \alpha(1) & \dots & \alpha(n) \end{pmatrix}$ = 兩列式



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

2. $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

3. $\alpha^{-1} = \begin{pmatrix} \alpha(1) & \dots & \alpha(n) \\ 1 & \dots & n \end{pmatrix}$

4. 運算：無交換性*(非交換群)*

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

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ *(兩者不相等)*

(還有單列式寫法)

定義：

$\alpha \in S_n$，若$\exists\ i_1, \dots, i_k \in \{1, \dots, n\}$

使 $\alpha(i_1) = i_2, \alpha(i_2) = i_3, \dots, \alpha(i_{n-1}) = i_n, \alpha(i_n) = i_1$，且 $\alpha(i) = i, \forall\ i \notin \{i_1, \dots, i_k\}$

稱 α 為 k-cycle，記作$(i_1, \dots, i_k)$：單列式

1. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 4 & 6 & 4 \end{pmatrix}$

   $1 \to$ $3 \to 5 \to 6 = (1\ 3\ 5\ 6)$

2. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} = (2, 4)$ *//2-cycle*

   $2 \leftrightarrow 4$ 又稱 Transposition(交換、換位、對調)

3. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 2 & 7 & 6 & 1 \end{pmatrix} = (1\ 3\ 5\ 7) \circ (2\ 4) \circ (6)$

   //非 4-cycle 或 k-cycle，但可寫成 2 個 k cycle 合成

   $= (1\ 3\ 5\ 7) \circ (2\ 4) = (2\ 4) \circ (1\ 3\ 5\ 7)$ *//順序可換，因為無相關*

Note：

1. $\forall\ \alpha \in S_n, \alpha$ 可寫成 Disjoint k-cycle 之合成
2. 每個 k-cycle 可寫成 Transposition 合成

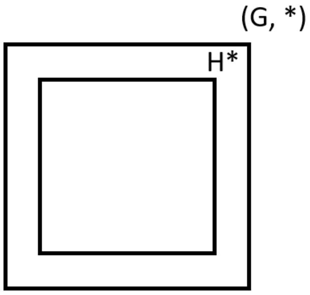
   公式：$(a_1\ a_2 \dots a_k) = (a_1\ a_2) \circ (a_2\ a_3) \circ \dots \circ (a_{k-1}\ a_k)$
3. $\forall\ \alpha \in S_n, \alpha$ 可寫成 Transposition 合成

   $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & A \\ 3 & 4 & 5 & 7 & 6 & A & 8 & 1 & 9 & 2 \end{pmatrix}$

   若 Transposition 個數為 even，稱 α 為 Even Permutation

   若 Transposition 個數為 odd，稱 α 為 Odd Permutation

9.4 **子群**



比較小的群，用相同運算

定義：

$(G, *)$：group

1. $H \subseteq G$
2. $(H, *)$：group

稱 H 為 G 之 Subgroup，記作 $H \subseteq_s G$

定理：

已知 G：group，$H \subseteq G$，$H \neq \Phi$

$H \subseteq_s G \Leftrightarrow \forall a, b \in H, ab^{-1} \in H$ *//b-1 為 b 在 G 之反元素*

$\Leftrightarrow \forall a, b \in H, ab \in H$、且 $\forall a \in H, a^{-1} \in H$

證明：

$\Longrightarrow$ Trivial

$\Longleftarrow$

1. Identity：
   $\because H \neq \Phi$，$\therefore \exists\, a \in H$
   $\therefore aa^{-1} = e \in H$
2. Inverse：
   $\forall a \in H$，$\because e \in H$，$\therefore ea^{-1} = a^{-1} \in H$
3. Closed：
   $\forall a, b \in H$，由 2.得 $b^{-1} \in H$，由已知 $(ab^{-1})^{-1} \in H$
   $\Longrightarrow ab \in H$
4. Associative：
   結合性與集合大小無關，$\because$ G 具結合性 $\therefore$ H 具結合性

例：證 $(\mathbb{Z}_e, +) \subseteq_s (\mathbb{Z}, +)$

$\forall a, b \in \mathbb{Z}e,$

$ab^{-1} \Longrightarrow a+(-b)$

$a+(-b) \in \mathbb{Z}_e$

定理：
已知 a：group，$\Phi \neq H \subseteq G$, H finite
$H \subseteq_s G \Leftrightarrow \forall a, b \in H, ab \in H$

證明：
$\Longrightarrow$ Trivail
$\Longleftarrow$
1. $\forall a \in H$, Claim：$a^{-1} \in H$
   $\Longrightarrow a^2 \in H, a^3 \in H, a^n \in H$
   $\because$ H finite，$\therefore \exists\, i<j \ni a^i=a^j$
   $\Longrightarrow a^{j-i} = e \Longrightarrow aa^{j-i-1} = e$
   $\therefore a^{-1} = a^{j-i-1} \in H$
   ($j=i+1$ 時，$a=e, a^{-1} = e = a^0$)
2. $\forall a, b \in H$，由 1.得 $b\text{-}1 \in H$
   由已知，$ab^{-1} \in H \Longrightarrow H \subseteq_s G$

例：
$\mathbb{Z}_{12} = \{0, \ldots, 11\}$
$H = \{0, 3, 6, 9\} \subseteq_s G$
$L = \{0, 1, 2, 3\}\ !\subseteq_s G$
$\mathbb{Z}_4 = \{0, 1, 2, 3\}$
$L \neq \mathbb{Z}_4$，$\because$運算不一樣

定理：
$H, K \subseteq_s G$
1. $H \cap K \subseteq_s G$
2. $H \cup K$ 未必為 G 之 Subgroup　　*//$3+4=7 \neq H \cup K$, $H \cup K = \{0, 3, 4, 6, 8, 9\}$*

證明：
1. $H \cap K \subseteq_s G$
   $\because e \in H \cap K, \therefore H \cap K \neq \Phi$
   $\forall a, b \in H \cap K \Longrightarrow a, b \in H \subseteq_s G \Longrightarrow ab^{-1} \in H$
   $\Longrightarrow ab \in K \subseteq_s G \Longrightarrow ab^{-1} \in K$
   $\therefore ab^{-1} \in H \cap K$

9.5 循環群

$(\mathbb{Z}, +)$ a=3　　$a^2=6, a^3=9, a^4=12, a^5=15, a^6=18$

$a^2 \cdot a^4 = a^6$　　6+2=18

定義：

G：group，若$\exists\, a \in G \ni G = \{a^k \mid k \in \mathbb{Z}\}$

稱 G 為 Cyclic Group，且稱 a 為 G 之 generator，記作 G=<a>

例：G= $\mathbb{Z}_{12}$

<3> = {3, 6, 9, 0}運算是$+_n$

造不出{0, …, 11} $\Longrightarrow$ 3 不為 G($\mathbb{Z}_{12}$)之 generator

<5> = {5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0}

$\Longrightarrow 5^k$ 可造{0, …, 11} $\Longrightarrow$ 5 為 G($\mathbb{Z}_{12}$)之 generator

$a^3 \cdot a^5=a^8$、$a^{-4}=(a^4)^{-1}=-1(4)=-1(8)=4=8$

$a^4 \cdot (a^{-4}) = a^4 \cdot a^8 = a^{12} = 0$

Note：

1. $H = \langle a\rangle = \{ak \mid k \in \mathbb{Z}\} \Longrightarrow H \subseteq_s G$，稱 G 為 Cyclic Subgroup
2. $a \in G$，使 $a^n=e$ 之最小正整數 n 稱 a 之 Order，記作 o(a)
3. $H = \langle a\rangle = \{a, a^2, \ldots, a^{n-1}, a^n\}, n = o(a) = o(H)$

> 定理：
> $G = \langle a\rangle, o(G)=n$，則 $o(a^n) = n/\gcd(m, n)$

例(97 中山)：

1. 列出 $\mathbb{Z}_{40}$ 中，order 為 10 之所有元素
2. G=<a>, o(G)=40，列出 G 中 order 為 10 之所有元素

1. $\mathbb{Z}40 = \langle 1\rangle \Longrightarrow 4, 12, 28, 36$　　　　// $\mathbb{Z}40 = \langle 3\rangle \Longrightarrow 12, 36, 84(4), 108(28)$

2. G={ a, a2, …, a40} //a40=e

$o(a^m)=40/\gcd(40, m) = 10 \Longrightarrow \gcd(40, m) = 4$

$\Longrightarrow 40=2^3\times5 \Longrightarrow m=2^2\times1, 2^2\times3, 2^2\times7, 2^2\times9$

$\Longrightarrow a^4, a^{12}, a^{28}, a^{36}$

> 定理：
> G = <a>：Cyclic Group
> $\Longrightarrow$ G：abelian Group
>
> 證明：
> $\forall\, x, y \in G$，令 $x=a^k, y=a^l$
> $xy = a^k \cdot a^l = a^{k+l} = a^{l+k} = a^l \cdot a^k = yx$
> $\Longrightarrow$ 具 Commutative
> (反例：k_4 為 Abelian Group，但不為 Cyclic Group)

Note：

$\mathbb{Z}_4$：

+	0	1	2	3
0	*0*	*1*	*2*	*3*
1	*1*	*2*	*3*	*0*
2	*2*	*3*	*0*	*1*
3	*3*	*0*	*1*	*2*

群之二元運算表中，每列每行之元素皆相異：

*		a_j		a_k
a_i		a_i*a_j		a_i*a_k

若 $a_i*a_j = a_i*a_k$，∵群有消去性

∴$a_j=a_k$, 但 $a_j \neq a_k$

討論：G is a group：

1. o(G)=1 ⟹ G={e}：Abelian Group, Cyclic Group
2. o(G)=2 ⟹ G={e, a}：Abelian Group, Cyclic Group

	e	a
e	*e*	*a*
a	*a*	*e*

$a^2=e$, G=<a>

3. o(G)=3 ⟹ G={e, a, b}：Abelian Group, Cyclic Group

	e	a	b
e	*e*	*a*	*b*
a	*a*	*2.b*	*1.e*
b	*b*	*1.e*	*2.a*

$a^2=b$, $a^3=e$ ⟹ G = <a> = <b> ⟹ Cyclic Group

4. o(G)=4 ⟹ G={e, a, b, c}：Abelian Group

Case 1：$a^{-1}=e$ ⟹ aa-1=e, ae=e, a=e (→←)

Case 2：$a^{-1}=a$ ⟹ $a^2=e$

(1)右下 2×2 格假設為： ⟹ Abelian, Cyclic

	e	a	b	c
e	*e*	*a*	*b*	*c*
a	*a*	*e*	*1.c*	*2.b*
b	*b*	*1.c*	**a**	**e**
c	*c*	*2.b*	**e**	**a**

(2) 右下 2×2 格假設為：⟹ Abelican，但是為 k_4，且 $a^2=b^2=c^2=e$

⟹ o(G)=2 ⟹ Note Cyclic

	e	a	b	c
e	*e*	*a*	*b*	*c*
a	*a*	*e*	*1.c*	*2.b*
b	*b*	*1.c*	**e**	**a**
c	*c*	*2.b*	**a**	**e**

Case 3：$a^{-1}=c$，同上方式分析

結論：

1. $o(G) \leq 3 \Longrightarrow$ Cyclcic 且 Abelian Group
2. $o(G) = 4 \Longrightarrow$ 在同構觀點之下，只有 2 種：
   (1) $\mathbb{Z}_4$：Cyclic, Abelian Group
   (2) k_4：Abelian 但非 Cyclic　*//k_4 又稱 Klein 4-group*

//$S_3 = G$, $o(G) = 3! = 6 \Longrightarrow$ 不具交換性，非 Abelian

9.6 陪集

定義：

$H \subseteq_s G, a \in G$

1. $aH = \{ah \mid h \in H\}$：H 之 Left Coset 左陪集
2. $Ha = \{ha \mid h \in H\}$：H 之 Right Coset 右陪集 *//抽象時運算符號可省略*

$G = \mathbb{Z}12, H=\{0, 3, 6, 9\}$

$0+H = \{0, 3, 6, 9\} = 3+H = 6+H = 9+H$

$1+H = \{1, 4, 7, 10\} = 4+H = 7+H = 10+H$

$2+H = \{2, 5, 8, 11\} = 5+H = 8+H = 11+H$

Note：

f：$H \rightarrow Ah$ by $f(h)=ah \Longrightarrow f$：1-1 且 onto

定義：

$H \subseteq_s G$，定義 2 個 Equivalent Relation on G

1. $a \equiv_l b \Leftrightarrow a^{-1}b \in H$
2. $a \equiv_r b \Leftrightarrow ba^{-1} \in H$

Lemma

1. 在$\equiv_l$中，$[a] = Ah$
2. 在$\equiv_r$中，$[a] = Ah$

證明：

1. $[a] = \{x \mid a \equiv_l x\} = \{x \mid a^{-1}x \in H\}$
   $= \{x \mid a^{-1}x = h, h \in H\} = \{x \mid x = ah, h \in H\} = aH$

推廣：

$H \subseteq_s G$

1. H 在 G 中，相異 Left Coset 形成 G 之一分割
2. H 在 G 中，相異 Right Coset 形成 G 之一分割

定理：(Lagrange) G：finite group, $H \subseteq_s G$ 則 $o(G)=o(H) \cdot k$ 其中 k 為 H 在 G 中，相異 Left Coset 個數 證明： 令 $a_1H, \ldots, a_kH$ 為相異 Left Coset，則 a_1H,形成 G 之分割 $\therefore o(G) = \lvert a_1H \rvert + \ldots + \lvert a_kH \rvert$ $= o(H) + \ldots + o(H)$ $= o(H) \cdot k$

推廣：
G：finite group, $H \subseteq_s G$
則 o(H) | o(G)
若 G 為有限群，則子群的元素個數整除母群元素個數，且 k 為 G 之相異陪集數

例(95 中山)：
$H, K \subseteq s\ G, K \subset H \subset G$
o(G)=660, o(K)=66, o(H)=？

66|o(H), o(H)|660 $\Longrightarrow$ o(H) = 66 · k1, 660 = o(H) · k2
*660 = 66 · k1 · k2，∴k1 · k2 = 10 = 1*10 = 2*5 = 5*2 = 10*1*
*∴o(H) = 66, 66*2, 66*5, 660，但 K⊂H，且 H⊂G $\Longrightarrow$ K≠H 且 H≠G*
*$\Longrightarrow$ o(H) = 66*2 或 66*5*

定理(94 中山)：
G：group, o(G)=p：Prime
則 G 為 Cyclic Group

證明：
找生成員，Prime 至少 2，∴o(G)至少 2，而生成員不找 e，因 e 只會生成自己，但 o(G)=2，還要有其他元素
∵o(G)=p≥2
∴ ∃ a ∈ G-{a}
令 H = <a> = {ak | k ∈ ℤ}
∵任意數可生成循環子群
∴$H \subseteq s\ G$
$\Longrightarrow$ o(H) | o(G)
$\Longrightarrow$ o(H) = 1 或 p(若 1 則 e)
$\Longrightarrow$ o(H) = p
∵ea ∈ H，∴o(H)≥2
$\Longrightarrow$ o(H)=p
$\Longrightarrow$ G = H = <a>：Cyclic Group

Note：
G：group, o(G)≤5 $\Longrightarrow$ G：Abelian

證明：
1~4 前面討論過了(k_4 為 Abelian，但不為 Cyclic)
且 5 為質數，故為 Abelian

9.8 同態與同構

+	0	1	2	3
0	*0*	*1*	*2*	*3*
1	*1*	*2*	*3*	*0*
2	*2*	*3*	*0*	*1*
3	*3*	*0*	*1*	*2*

*	e	a	b	c
e	*e*	*a*	*b*	*c*
a	*a*	*e*	*c*	*b*
b	*b*	*c*	*a*	*e*
c	*c*	*b*	*e*	*a*

$\Longrightarrow$ f(0)=e, f(1)=b, f(2)=a, f(3)=c

2+3=1 、a*c=b

f(2)*f(3) = f(1) = f(2+3)

定義：

(S, *), (T, Δ)：Algebraic System，若∃ f'：S→T function 滿足：

∀ a, b ∈ S, f(a*b) = f(a)Δf(b)，稱 f：由 S 到 T 之 Homormorphism(homo)同態函數

例：$(\mathbb{R}, +), (\mathbb{R}_e, \circ)$：group

f：$\mathbb{R}\to\mathbb{R}^+$ by $f(x)=10^x$

且 $\forall a, b \in S$

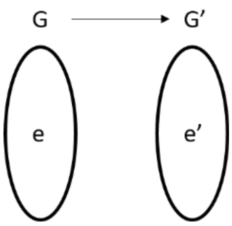
$f(a+b) = 10^{a+b} = 10^a \cdot 10^b = f(a) \cdot f(b)$

$\therefore (\mathbb{R}, +) \cong (\mathbb{R}_e, \circ)$, f is an isomorphism

---

定理(97 輔大)：

f：G→G' group homo



1. f'(e) = e'
2. f'(a^{-1}) = f^{-1}(a)

證明：

1. e'f(e) = f(e) = f(e*e) = f(e) · f(e)

   G'為 group 有消去性

   e' = f(e)
2. 證左、右反

   左反：f(a) · f(a^{-1}) = f(aa^{-1}) = f(e) = e'

右反：$f(a^{-1}) \cdot f(a) = f(a^{-1}a) = f(e) = e'$

$\Longrightarrow f^{-1}(a) = f(a^{-1})$

$$\begin{tikzcd} 2 \arrow[r] \arrow[d] \arrow[d, bend right=60, <->] & 10^{2} \arrow[d] \arrow[d, bend left=60, <->] \\ -2 \arrow[r] & 10^{-2} \end{tikzcd}$$

例：

f, g：G→G：group homo

$H=\{a \in G \mid f(a) = g(a)\}$

證：$H \subseteq_s G$

需證明以下三點：

1. $H \subseteq_s G$
2. $H \neq \Phi$
3. $\forall a, b \in H, ab^{-1} \in H$

1. $H \subseteq_s G$
2. $\because f(e) = e = g(e)$
   $\therefore e \in H, H \neq \Phi$
3. $\forall a, b \in H, f(a) = g(a)$ 且 $f(b) = g(b)$
   $\Longrightarrow f(ab^{-1}) = f(a) \cdot f(b^{-1}) = f(a) \cdot f(b)^{-1} = g(a) \cdot g(b)^{-1} = g(ab^{-1})$
   $\Longrightarrow ab^{-1} \in H$

定義：

(S, *)：Algebraic System, R 為 S 上之 Equivalent Relation

滿足$\forall$ a, b ∈ S, (a, b) ∈ R 且(c, d) ∈ R

稱 R 為(S, *)之一 Congruence Relation 同餘關係

		X		Y	
	*	a	b	c	d
X	a	a	a	d	c
	b	b	a	c	a
Y	c	c	b	a	b
	d	c	d	b	a

令a, b為X、c, d為Y

R 之應之分割{a, b}, {c, d}：不為同餘

*	a	b	c	d
a	a	a	d	c
b	b	a	c	d
c	c	d	a	b
d	d	d	b	a

*	X	Y
X	X	Y
Y	Y	X

R 為(T, Δ)之同餘關係

f(a) = X, f(b) = X, f(c) = Y, f(d) = Y

則 f：T→T’為 homo 且 onto，其中{X, Y}稱 Homomorphic Image 同態像集

例(98 交大)：

S：

*	a	b	c	d
a	*a*	*a*	*d*	*c*
b	*b*	*a*	*c*	*d*
c	*c*	*d*	*a*	*b*
d	*d*	*d*	*b*	*a*

T：

·	X	Y
X	*X*	*Y*
Y	*Y*	*X*

S 到 T 之 onto homorphism 是否存在？

No

9.9 環

2．3+3．4

定義：

(S, +, ．)：Algebraic System

1. (S, +)：Abelian(5 件要證)
2. (S, ．)：Semi-group(2 件要證)
3. ．對+具分配性

例：∀ a, b, c ∈ S

a．(b+c) = a．b + a．c

(b+c)．a = b．a + c．a

稱(S, +, ．)為 Ring 環(3 件→5+2+1=8 件)

Notataion

1. 加法單位元素：0 (zero)
2. 乘法單位元素：1 (unity)
3. a 之加法反元素：-a (negative, a 的負元素)
4. a 之乘法反元素：a^{-1} (inverse, a 的反元素)

例：

1. (ℤ, +, ．)：Ring
2. (ℝm×n, +, ．)：Ring
3. (P(x), ⊕, ∩)：Ring→zero：Φ；-A=A；unity=X(P(x)之宇集合)

例(95 成大)：

S=$\mathbb{R}^+$, a⊕b = ab, a⊗b = $a^{\log b}$

證：(S, ⊕, ⊗) 為 Ring

(若是直接從定義作，則需要證明 5+2+1 件事，故改以證明：

1. (S, ⊕)為交換群(by 為另一交換群之子群)

2. (S, ⊗)為 Semi-group

3. 分配性

三件事即可，證明如下：

1. (S, ⊕) = (ℝ+, ．)：Abelian Group(因為前者為後者之子群)

2. (S, ⊗)：Closed 與 Associative

(1) Closed：

∀a, b ∈ℝ+, a⊗b = $a^{\log b}$

log ab ∈ℝ, a^{logb} 必∈ℝ+

⟹ a⊗b ∈ℝ+

(2) Associative：

$a \otimes b \oplus c = a^{logb} \oplus c = (a^{logb})^{logc} = a^{logb \times logc} = (a^{logc})^{logb}$

3. 分配性：

∀a, b, c ∈S

$a \otimes (b \oplus c) = a \otimes (bc)$

Note：

$(\mathbb{Z}_n, +)$：Abelian Group

定義：$\cdot_n$ by $[a] \cdot_n [b] = [ab \bmod n]$

則$(\mathbb{Z}_n, +_n, \cdot_n)$ = Ring

$\mathbb{Z}_{12} = \{0, \ldots, 11\}$

2+5=7, 6+9=3, -3=9(∵3+9=12=0)

$2 \cdot 5=10, 6 \cdot 9= 54 \bmod 12 = 6$

定理(97 台大)：
已知$(\mathbb{R}, +, \cdot)$：Ring, $\Phi \neq S \subseteq \mathbb{R}$
$(S, +, \cdot)$為$(\mathbb{R}, +, \cdot)$之 Subring
$\Leftrightarrow \forall a, b \in S, a+(-b) \in S$ 且 $a \cdot b \in S$

證明：消去性

定理(97 台大)：
$(\mathbb{R}, +, \cdot)$ = Ring，$\Phi \neq S \subseteq \mathbb{R}$, S=finite
$(S, +, \cdot)$為$(\mathbb{R}, +, \cdot)$之 Subring
$\Leftrightarrow \forall a, b \in S, a+b \in S$ 且 $a \cdot b \in S$
$a, a^2, a^3 \in H \Longrightarrow a, 2a, 3a \in S$

Note：

R = {(矩) | a, b, c, d ∈ R}

$(\mathbb{R}, +, \cdot)$：Ring 具 unity：Z=(矩)

S = {(矩) | a ∈ R} → S ⊆ R

A + (-B) = (矩) ∈ S

A · B = (矩)

∴(S, +, ·)為(R, +, ·)之 Subring

(S, +, ·)之 unity 為(矩)

$f(a+b) = f(a) + f(b), f(e) = e'$

$f(ab) = f(a) \cdot f(b), f(a^{-1}) = f(a)^{-1}$

定理：
f：R→R'：Ring homo
1. $f(0) = 0'$
2. $f(-a) = -f(a)$
3. 若 f onto，則 $f(1) = 1'$乘法單位元素
4. 若 f onto，則 $f(a^{-1}) = f(a)^{-1}$

9.10 整域

定理：
(R, +, ‧)：Ring, $a \in R$
則 $a \cdot 0 = 0 = 0 \cdot a$

證明：
$0 + a \cdot 0 = a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0$
而(R, +)為 Abelian 存在消去性
$\Longrightarrow 0 = a \cdot 0$

Note：
$\mathbb{Z}6$：Ring
$2\neq0, 3\neq0$，但 $2 \cdot 3=0$，想避免這種情況
$\Longrightarrow$ zero divisor 零除元

定義：
(R, +, ‧) = Commutative Ring
$a \in R-\{0\}$, 若$\exists\, b\neq0 \ni ab=0$
稱 a 為 zero divisor

定義：
(R, +, ‧)：Commutative Ring with unith(乘法單位元素)
若 R 不具 zero divisor，稱 R 為 Intergral Domain 整域(也就是好環的意思)
如：$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
$a\neq0, b\neq0 \Longrightarrow ab\neq0$ (無零除元)
$\Leftrightarrow ab = 0 \Longrightarrow a=0$ 或 $b=0$

定理：
(R, +, ‧)：Commutative Ring，R 不具零除元
$\Leftrightarrow$ (R-{0}, ‧)具消去性

證明：
$\Longrightarrow$：
$\forall\, a, b, c \in R-\{0\}$，設 $ab = ac$
$a=0$ 或 $b-c=0$，但 $a, b, c\neq0$
故 $a=b$ (消去 a)

$\Longleftarrow$：
$\forall\, a, b, c \in R$
設 $ab=0$, Claim：no zero divisor ($a=0$ 或 $b=0$)
若 $a=0$ 得證
若 $a\neq0$，則 $ab=0$，$a\neq0$ 有消去性，$b=0$ 得證

9.11 體

$(R, +, \cdot)$：Commutative Ring with unity

若$\forall a \in R-\{0\}$, a 之 Inverse 存在，稱 R 為 Field(體)

例(94 淡江)：

$\mathbb{Q}(\sqrt{(3)}) = \{a+b\sqrt{(3)} \mid a, b \in \mathbb{Q}\}$，證：S 為一體？

原本應該要證 5+4+1+1=11 個條件(加法交換群)+(乘法交換單群)+(非零元素有反元素)+(分配性)
改成證：(為交換群之子群)+(皆有 Inverse)+(非零元素有反元素)+(分配性)，證明如下：

1. $\forall x, y \in S$，設 $x = a+b\sqrt{(3)}, y = c+d\sqrt{(3)}, x-y = (a-c) + (b-d)\sqrt{(3)} \in S$
2. $xy = (a+b\sqrt{(3)})(c+d\sqrt{(3)}) = (ac+3bd) + (ad+bc)\sqrt{(3)} \in S$
3. 因為 S 為 R 之 Subring(10 條件不用證)，故只要證非零反元素存在即可
   $\forall x = a+b\sqrt{(3)} \in S-\{0\}$
   取 $x' = (a-b\sqrt{(3)})/(a^2-3b^2) \in S$
   則 $x \cdot x' = 1$，x is an unit

定理：

F：Field $\Longrightarrow$ F：Integral Domain

證明：

$\Longrightarrow$：

$\forall a, b \in F$，設 $ab=0$

若 $a=0$ 得證

若 $a\neq0$，因 Field，故$\exists\, a^{-1}$

$\Longrightarrow b=a^{-1} \cdot 0 = 0$

$\Longleftarrow$：不成立

取反例：

$(\mathbb{Z}, +, \cdot)$為 Integral Domain($ab=0 \Leftrightarrow a=0$ 或 $b=0$)

但 $2 \in \mathbb{Z}, 2 \cdot x=1 \Longrightarrow x=1/2 \notin \mathbb{Z}$

$\therefore 2$ 不存在乘法反元素

定理(90 台大)：

$(R, +, \cdot)$：Ring，R：finite，R：Integral Domain $\Leftrightarrow$ R：Field

證明：

$\Longrightarrow$：Trival

$\Longleftarrow$：

令 $R=\{a_1, \ldots, a_n\}, |R|=n$ *(只要證 x 與 R 所有元素相乘仍為 R)*

$\forall x \in R-\{0\}$，取 $A=\{xa_1, \ldots, xa_n\} \subseteq R$

$\because a_1, \ldots, a_n$ 全相異，且 R-{0}在(R-{0}, $\cdot$)中具消去性，$\therefore xa_1, \ldots, xa_n$ 全相異

$\Longrightarrow |A|=n, A=R \Longrightarrow 1 \in A$

$\exists\, I \ni xa_i = 1$，$\therefore$x is unit

Note：

1. $\mathbb{Z}_n$ 中，a 為 unit ⇔ gcd(a, n) = 1
   a 有乘法反元素，則 $ax \equiv 1 \pmod{n}$
2. $\mathbb{Z}_n$：Field ⇔ n=Prime
   $\forall a \in \mathbb{Z}_n$ 都有乘法反元素個數
   ⟹ n 跟(0, …, n-1)皆互質 ⟹ n：Prime
3. 任何 Field 之元素個數必為 p^t
   p：Prime，$t \geq 1$，稱為 Galois Field，記作 GF(p^t)