回顾 设 G, H 是两个群

$\varphi: G \to H$ 使得 $\forall g_1, g_2 \in G$

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$$

则称 φ 是从 G 到 H 的同态

当 φ 是双射时，φ 是同构。

定义：如果 G, H 间存在同构

则称 G 和 H 是同构的

记为 $G \simeq H$.

引理 2.3. 设 G, H, K 是三个群

$\varphi: G \to H$, $\psi: H \to K$

是群同态. 则 $\psi\circ\varphi$ 是从 G 到 H 的群同态.

证.
$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[dr, "\psi\circ\varphi"'] & H \arrow[d, "\psi"] \\ & K \end{tikzcd}$$

$\forall g_1, g_2 \in G$

$\psi\circ\varphi(g_1 g_2)$

$= \psi(\varphi(g_1 g_2)) = \psi(\varphi(g_1)\cdot\varphi(g_2))$

$= \psi(\varphi(g_1))\cdot\psi(\varphi(g_2)) = \psi\circ\varphi(g_1)\cdot\psi\circ\varphi(g_2)$ ▢

命题 2.1 群同构 $\simeq$ 是所有群构成的集合上的等价关系

证：$\boxed{\text{自反}}$: $id_G: G \to G$ 是同构.

$\Rightarrow G \simeq G$

$\boxed{\text{对称}}$ 设群 G_1, G_2 是同构的

则 $\exists$ 同构 $\varphi: G_1 \to G_2$. 由引理 2.2

(iii). $\varphi^{-1}: G_2 \to G_1$ 也是同构.

于是 $G_2 \simeq G_1$

$\boxed{\text{传递}}$ 设三个群 G_1, G_2, G_3 满足

$G_1 \simeq G_2$, $G_2 \simeq G_3$. 则存在群同构

$\varphi: G_1 \to G_2$, $\psi: G_2 \to G_3$. 由引理 2.3

$\psi\circ\varphi: G_1 \to G_3$ 也是同构

即 $G_1 \simeq G_3$ ▢

群论的基本问题：

给定一类群、对这类群按同构分类

并找出每个等价类中的代表元

定义：当群 G 是无穷群时，称群 G 的阶是无穷的，记为 $|G|=\infty$

当群 G 是有限阶时，称群 G 中元素的个数为 G 的阶，记为 $|G|$.

例：考虑 2 阶群在同构意义下的分类

设 $G=\{e,a\}$ 是二阶群，e 是单位

	e	a
e	e	a
a	a	e

$$\varphi: G \longrightarrow (\mathbb{Z}_2, +, \bar{0})$$
$$e \longmapsto \bar{0}$$
$$a \longmapsto \bar{1}$$

φ 是双射.

$$\varphi(ee)=\varphi(e)=\bar{0}$$
$$\varphi(e)+\varphi(e)=\bar{0}+\bar{0}=\bar{0}$$

$$\varphi(ea)=\varphi(a)=\bar{1}$$
$$\varphi(e)+\varphi(a)=\bar{0}+\bar{1}=\bar{1}$$

$$\varphi(ae)=\varphi(a)=\bar{1}$$
$$\varphi(a)+\varphi(e)=\bar{1}+\bar{0}=\bar{1}$$
$$\varphi(aa)=\varphi(e)=\bar{0}$$
$$\varphi(a)+\varphi(a)=\bar{1}+\bar{1}=\bar{0}$$

于是 $\varphi(xy)=\varphi(x)+\varphi(y)$. $(\forall x,y\in G)$

$\Rightarrow \varphi$ 是同构. $\Rightarrow$ 二阶群~~都~~同构于

$$(\mathbb{Z}_2, +, \bar{0}).$$

例：4 阶群不只一个同构类

$\because$ $(\mathbb{Z}_2\times\mathbb{Z}_2, +, (\bar{0},\bar{0}))$ 不同构于

$$(\mathbb{Z}_4, +, \bar{0})$$

例：设 G 是群，$a\in G$

$$I_a: \begin{array}{l} G \longrightarrow G \\ g \longmapsto a^{-1}ga \end{array}$$

证明：I_a 是群同构.

证：$\forall g_1, g_2 \in G$

$$I_a(g_1g_2)=a^{-1}g_1g_2a=(a^{-1}g_1a)(a^{-1}g_2a)$$
$$=I_a(g_1)\,I_a(g_2)$$

于是 I_a 是同态：

$\forall g\in G \quad I_a(aga^{-1}) = a^{-1}(aga^{-1})a$

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

I_a 是满射. 设 $g_1, g_2\in G$

且 ~~设~~ $I_a(g_1)=I_a(g_2)$ 则

$$a^{-1}g_1a = a^{-1}g_2a$$

同时左乘 a 得 $g_1a=g_2a$

同时右乘 a^{-1} 得 $g_1=g_2$

I_a 是单射. 于是 I_a 是同构

定义：设 G 是群. $\varphi: G\to G$ 是同构 则称 φ 是自同构.

§2.3 子群 ~~和生成元~~

定义：设 $(G,*,e)$ 是群. $H\subset G$ 如果 $(H,*,e)$ 也是群. 则称 H 是 G 的子群 (subgroup)

注：G 有两个平凡子群 $(\{e\},*,e)$ 和 $(G,*,e)$.

引理 2.4 设 G 是群. $H\subset G$. 如果 $\forall h_1,h_2\in H$, $h_1h_2^{-1}\in H$, 则 H 是 G 的子群

证：设 e 是 G 中的单位元，$h\in H$

则 $hh^{-1}\in H \Rightarrow e\in H$

进而 $eh^{-1}\in H \Rightarrow h^{-1}\in H$.

下面验证：$\forall h_1,h_2\in H$, $h_1h_2\in H$

即 H 关于 G 中的运算封闭. 换言之 G 上的运算也是 H 上的运算

$\because h_2\in H$. $\therefore h_2^{-1}\in H$ 于是

$$h_1(h_2^{-1})^{-1}\in H$$

注意到 $(h_2^{-1})^{-1} = h_2$ 这是因为

[$\cancel{(h_2^{-1})^{-1}h_2=e}$ $h_2^{-1}h_2 = h_2h_2^{-1} = e$

$\Rightarrow h_2 = (h_2^{-1})^{-1}$ (命题2.1).]

于是 $h_1h_2 \in H$

H 中结合律由 G 中结合律自然

导出。 ~~于是 H 是群~~ $\boxed{}$

综上所述：H 关于 G 的的运算

和 G 中的单位元构成群 即

H 是 G 的子群。 ▢

例：设 H 是所有偶数的集合

证明：$(H, +, 0)$ 是 $(\mathbb{Z}, +, 0)$

的子群。且 H 与 $\mathbb{Z}$ 同构

证：设 $a, b \in H$ $\quad a-b \in H$

$\Rightarrow$ H 是 $\mathbb{Z}$ 的子群

$$\varphi: \mathbb{Z} \longrightarrow H$$
$$n \longmapsto 2n$$

$$\varphi(n+m) = 2(n+m) = 2n+2m$$
$$= \varphi(n) + \varphi(m)$$

φ 是同态。φ 显然是~~双射~~ $\Rightarrow \varphi$ 是同构。

例：$A_n = \{\sigma \in S_n \mid \sigma \text{ 是偶置换}\}$

证明 A_n 是 S_n 的子群。

证：设 $\sigma, \tau \in A_n$ 则

$$\sigma = (i_1, j_1) \cdots (i_{2s}, j_{2s}).$$
$$\tau = (k_1, l_1) \cdots (k_{2t}, l_{2t})$$

其中 (i_p, j_p)，(k_q, l_q) 是 S_n 的对换

$p = 1, \dots, 2s, \quad q = 1, \dots, 2t$

$$\tau^{-1} = (k_{2t}, l_{2t}) \cdots (k_1, l_1)$$

$$\sigma\tau^{-1} = (i_1, j_1) \cdots (i_{2s}, j_{2s})(k_{2t}, l_{2t}) \cdots (k_1, l_1)$$

仍在 A_n 中 于是 A_n 是 S_n 的

子群。

补充内容 Lagrange 定理

设 G 是有限群。H 是 G 的子群

则 $|H| \mid |G|$.

证: $\forall g_1, g_2 \in G$. 我们称 g_1, g_2 关于 H 等价 如果 $g_1 g_2^{-1} \in H$. 此时 记 $g_1 \sim_H g_2$

验证: $\sim_H$ 是等价关系

$\boxed{\text{自反}}$ $\forall g \in G$, $g g^{-1} = e \in H$

$g \sim_H g$ ✓

$\boxed{\text{对称}}$ 设 $g_1 \sim_H g_2$. 则 $g_1 g_2^{-1} \in H$

因为 H 是子群 所以 $(g_1 g_2^{-1})^{-1} \in H$

即 $g_2 g_1^{-1} \in H$. 于是 $g_2 \sim_H g_1$

$\boxed{\text{传递}}$ 设 $g_1 \sim_H g_2$, $g_2 \sim_H g_3$. 则

$g_1 g_2^{-1} \in H$, $g_2 g_3^{-1} \in H$

因为 H 是子群 $(g_1 g_2^{-1})(g_2 g_3^{-1}) \in H$

$\Rightarrow g_1 g_3^{-1} \in H \Rightarrow g_1 \sim_H g_3$

$\sim_H$ 是等价关系

设 $G/\sim_H = \{[g_1], \ldots [g_k]\}$

记号 $\forall g \in G$ $Hg = \{hg \mid h \in H\}$.

断言 $[g_i] = Hg_i$, ~~$i=1,2,\ldots k$.~~

且 $|Hg_i| = |H|$, $i = 1, 2, \ldots k$

~~断言的证明~~

证 $\forall g \in Hg_i$ $\exists h \in H$ 使得

$g = h g_i$

$g g_i^{-1} = h \Rightarrow g \sim_H g_i \Rightarrow g \in [g_i]$

反之, $g \in [g_i]$. $g g_i^{-1} \in H$

$\exists h \in H$ 使得 $g g_i^{-1} = h \Rightarrow g = h g_i$

由此可知 $[g_i] = Hg_i$

设 $H = \{h_1, \ldots h_d\}$ 则 $Hg_i = \{h_1 g_i, \ldots h_d g_i\}$

若 $h_1 g_i = h_2 g_i \Rightarrow h_1 = h_2$

于是 $h_1 g_i, \ldots h_d g_i$ 两两不同

即 $|Hg_i| = d = |H|$ 断言成立

由第一章命题 6.3

$G = Hg_1 \cup \cdots \cup Hg_k$ 且 $Hg_i \cap Hg_j = \emptyset$ $(i \neq j)$

划分

于是 $|G| = |Hg_1| + \cdots + |Hg_k| = k|H|$

$\Rightarrow |H| \mid |G|$ □

例：$|A_n| = \frac{n!}{2}$ $|A_n| \mid |S_n|$

$S_n = A_n \cup (12)A_n(12)$

例：设 G 是有限群，$|G|$是素数

则 G 没有非平凡子群

证：设 $|G| = p$ 一素数，H 是 G

的子群 $|H| \mid p \Rightarrow |H| = 1$ 或 $|H| = p$

即 $H = \{e\}$ 或 $H = G$ □

例 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 中非平凡子群的阶数也可能是2

$G_1 = \{(\bar{0},\bar{0}), (\bar{1},\bar{0})\}$, $G_2 = \{(\bar{0},\bar{0}), (\bar{0},\bar{1})\}$, $G_3 = \{(\bar{0},\bar{0}), (\bar{1},\bar{1})\}$

都是 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 中的子群.

验证 G_3 是子群 $(\bar{1},\bar{1}) + (\bar{1},\bar{1}) = (\bar{0},\bar{0})$

$\Rightarrow -(\bar{1},\bar{1}) = (\bar{1},\bar{1})$

$$\left.\begin{array}{l}(\bar{0},\bar{0}) - (\bar{0},\bar{0}) = (\bar{0},\bar{0})\\(\bar{0},\bar{0}) - (\bar{1},\bar{1}) = (\bar{1},\bar{1})\\(\bar{1},\bar{1}) - (\bar{0},\bar{0}) = (\bar{1},\bar{1})\\(\bar{1},\bar{1}) - (\bar{1},\bar{1}) = (\bar{0},\bar{0})\end{array}\right\} \in G_3 \checkmark$$

§2.4 生成元

设：设 G 是群，$S \subset G$ 非空

记 $\langle S \rangle := \{x_1^{i_1} \cdots x_n^{i_n} \mid n \in \mathbb{Z}^+, x_1, \ldots x_n \in S, i_1, \ldots i_n \in \mathbb{Z}\}$

其中 $x_1, \ldots x_n$ 中可能有相同元素.

称 $\langle S \rangle$ 是由 ~~Q~~ ~~x_1~~ S 生成的子群

验证：$\langle S \rangle$ 是子群

设 $x, y \in \langle S \rangle$

则 $x = x_1^{i_1} \cdots x_m^{i_m}$. $y = y_1^{j_1} \cdots y_n^{j_n}$

其中 $x_1 \ldots x_m, y_1 \ldots y_n \in S$

$xy^{-1}=x_1^{i_1}\cdots x_m^{i_m}y_n^{-j_n}\cdots y_1^{-j_1}\in\langle S\rangle$

S 称为 $\langle S\rangle$ 的一组生成元

特别地 当 $\langle S\rangle=G$ 时，S 是 G 的生成集

记号：当 $S=\{x_1,\cdots x_k\}$ $\langle S\rangle$ 也记为 $\langle x_1,\cdots x_k\rangle$

例：$(\mathbb{Z},+,0)=\langle 1\rangle$

$\langle \mathbb{Z}_n,+,\bar{0}\rangle=\langle \bar{1}\rangle$

S_n 由所有的循环生成

也可由所有的对换生成

书上 p128，10 $S_n=\langle (12),(123\cdots n)\rangle$

$GL_n(\mathbb{R})$ 可以由所有的 n 阶初等矩阵生成（第二章 定理 6.1）

~~Cayley 定理~~

Cayley 定理：

设 G 是群，$T_G=\{f:G\to G\mid f$ 是双射$\}$

$(T_G,\circ,id_G)$ 是群

Cayley 定理：G 同构于 T_G 的某个子群

引理 2.5 设 G,H 是两个群，$\varphi:G\to H$ 是群同态，则 $im(\varphi)$ 是 H 的子群。

设 $h_1,h_2\in im(\varphi)$，$\exists\, g_1,g_2\in G$，使得

$\varphi(g_1)=h_1$，$\varphi(g_2)=h_2$

引理

$\varphi(g_1g_2^{-1})=\varphi(g_1)\varphi(g_2^{-1})=\varphi(g_1)\varphi(g_2)^{-1}$

$=h_1h_2^{-1}$

$\Rightarrow h_1h_2^{-1}\in im(\varphi)\Rightarrow im(\varphi)$ 是子群 ▯

（引理 2.4）

注：如果 $\varphi: G \to H$ 的单同态

则 $G \simeq \mathrm{im}(\varphi)$.

Cayley 定理的证明

$$\varphi: G \longrightarrow T_G$$
$$g \longmapsto L_g: a \mapsto ga \text{（左乘）}$$

由引理2.1. $L_g \in T_G$

$\forall g_1, g_2 \in G$

$$\varphi(g_1 g_2) = L_{g_1 g_2}$$

$\forall g \in G$, $L_{g_1} \circ L_{g_2}(g) = L_{g_1}(L_{g_2}(g))$

$= L_{g_1}(g_2 g) = (g_1 g_2) g = L_{g_1 g_2}(g)$

$L_{g_1} \circ L_{g_2} = L_{g_1 g_2}$

$\Rightarrow \varphi(g_1 g_2) = \varphi(g_1) \circ \varphi(g_2)$

φ 是同态.

设 $\varphi(g_1) = \varphi(g_2)$

则 $L_{g_1} = L_{g_2} \Rightarrow L_{g_1}(e) = L_{g_2}(e) \Rightarrow g_1 = g_2$.

φ 是单同态.

$\Rightarrow G \simeq \mathrm{im}(\varphi)$ ▨

推论2.1 设 G 是 n 阶有限群

则 G 同构于 S_n 的某个子群

证：因为 $T_G = S_n$ ▨

§2.5 循环群.

定义：设 G 可以由一个元素生成. 则称 G 是循环群

例：$(\mathbb{Z}, +, 0) = \langle 1 \rangle$ 无穷阶循环群

$(\mathbb{Z}_n, +, \bar{0}) = \langle \bar{1} \rangle$. n 阶循环群

结论：在同构意义下. 循环群只有这些.

定义：设 G 是群，$g\in G$，如果存在 $n\in\mathbb{Z}^+$，使得 $g^n=e$ → G 中单位元

则称 g 是有限阶的。否则 g 是无穷阶的。当 g 是有限阶时，最小的正整数称为 g 的阶，记为 $\mathrm{ord}(g)$。当 g 无穷阶时 $\mathrm{ord}(g)=\infty$

~~定理2.1 设~~

引理2.6. 设 G 是群，$g\in G$，且 $\mathrm{ord}(g)=n$。则 $\boxed{|\langle g\rangle| = n}$

证：$\langle g\rangle=\{g^0, g^1, \cdots g^{n-1}\}$，$g^0 = e$

特别地，$|\langle g\rangle|=n$

证：设 $i,j\in\{0,1,\dots,n-1\}$，$i\geq j$

若 $g^i=g^j \Rightarrow g^{i-j}=e$

$\Rightarrow 0\leq i-j<n \Rightarrow i=j$.

于是 $\{g^0, g^1, \dots g^{n-1}\}$ 中元素两两不同 ①

$\forall\ a\in\langle g\rangle$，$a=g^k$，$k\in\mathbb{Z}$

由除法 $k=qn+r$，$r\in\{0,1,\dots,n-1\}$

$$a=g^{qn+r}=(g^n)^q g^r=e^q g^r=g^r$$

$\Rightarrow g^r\in\{g^0, g^1, \dots g^{n-1}\}$

$\Rightarrow \langle g\rangle=\{e, g, \dots g^{n-1}\}$ □

定理2.1. 设 G 是无穷阶循环群

则 $G\simeq(\mathbb{Z},+,0)$

证：设 $G=\langle g\rangle$. ~~由引理2.6 ord(g)~~

则 $\{\dots g^{-2}, g^{-1}, e, g^1, g^2, \dots\}$ 两两不同

否则 $\exists\ i,j\in\mathbb{Z}$，$i>j$ 使得

$g^i=g^j \Rightarrow g^{i-j}=e$，$i-j>0$

$\Rightarrow \mathrm{ord}(g)<\infty \Rightarrow \langle g\rangle$ 有限

（引理2.6）

→←

$\varphi: G \longrightarrow \mathbb{Z}$
$g^i \longmapsto i$ 是良定义的满射

$\varphi(g^i)=\varphi(g^j) \Rightarrow i=j$ 单射.

$\varphi(g^i \cdot g^j) = \varphi(g^{i+j}) = i+j$

$= \varphi(g^i)+\varphi(g^j)$. φ 是同态

φ 是同构.

定理 2.2 设 G 是 n 阶循环群 $n>1$

则 $G \simeq (\mathbb{Z}_n, +, \bar{0})$

证: 设 $G=\langle g\rangle$ 则 $\mathrm{ord}(g)<\infty$

由引理 2.6. $\mathrm{ord}(g)=n$

因 $G=\{g^0, g, \dots g^{n-1}\}$, $g^0 = e$

$\varphi: G \longrightarrow \mathbb{Z}_n$

$g^i \longmapsto \bar{i}$. $i\in\{0,1\dots n-1\}$

良定义. 单射. 满射

$\varphi(g^i g^j) = \varphi(g^{i+j})$

$= \varphi(g^{sn+r})$, 其中 $i+j=sn+r$ 由带余除法确定 10

$= \varphi(g^r) = \bar{r}$

$\varphi(g^i)+\varphi(g^j) = \bar{i}+\bar{j} = \overline{i+j} = \bar{r}$

$\Rightarrow \varphi(g^i g^j) = \varphi(g^i)+\varphi(g^j)$ ☐

故 φ 是同构

引理 2.7 ~~定理 2.3~~ 设 G 是有限群. $g\in G$

则 $\mathrm{ord}(g) \mid |G|$

证: $\langle g\rangle \subset G \Rightarrow |\langle g\rangle| \,\big|\, |G|$ (Lagrange.

$\Rightarrow \mathrm{ord}\langle g\rangle \mid |G|$. 引理 2.6

定理 2.3. 设 G 是循环群,

则 G 的子群都是循环群

证：设 $G=\langle g\rangle$，H 是 G 的子群且 $|H|>1$

若 $h\in H$ 且 $h\neq e$（e 是 G 中单位元）

则 $\exists k\in\mathbb{Z}\setminus\{0\}$，使得 $h=g^k$。

$\because$ H 是子群 $\therefore$ $g^{-k}\in H$

由此可知 $\exists\, m\in\mathbb{Z}^+$，使得 $g^m\in H$

令 m 是最小的正整数 使得 $g^m\in H$

$\forall\, h\in H$，$\exists\, l\in\mathbb{Z}$ 使得 $h=g^l$

由整数除法 $l=qm+r$，$r\in\{0,1,\dots m-1\}$

$$h=g^l=g^{qm+r}=(g^m)^q g^r$$

$$\Rightarrow\quad g^r=h\cdot(g^m)^{-q}\in H$$

$\Rightarrow$ $r=0$ $\Rightarrow$ $h=(g^m)^q$

$\Rightarrow$ $H\subset\langle g^m\rangle$ $\Rightarrow$ $H=\langle g^m\rangle$ $\square$

例：求 $(\mathbb{Z}_6,+,\bar{0})$ 中的所有非平凡子群

二阶 $\langle\bar{3}\rangle$ 三阶 $\langle\bar{2}\rangle=\{\bar{0},\bar{2},\bar{4}\}$

$\{\bar{0},\bar{3}\}$

由 Lagrange's 定理 $\mathbb{Z}_6$ 中没有 4 阶和 5 阶子群。

例：设群 G 是素数阶的，则 $G\simeq(\mathbb{Z}_p,+,\bar{0})$。

证：设 $g\in G$ 不是单位元，则 $\mathrm{ord}(g)=p$ （引理2.6）

（引理2.7）$\Rightarrow|\langle g\rangle|=p$

于是 $G=\langle g\rangle$。

§3. 环

定义：设 $(R,+,0)$ 是交换群

$(R,\cdot,1)$ 是含幺半群

且 $0\neq 1$， $\forall\, x,y,z\in R$

$x(y+z)=xy+xz$

$(y+z)x=yx+zy$

则称 $(R,+,0,\cdot,1)$ 是环 (ring)

当 $(R, \cdot, 1)$ 是交换含幺半群时，R 称为交换环.

例：交换环 $(\mathbb{Z}, +, 0, \cdot, 1)$

$(\mathbb{Z}_m, +, \bar{0}, \cdot, \bar{1})$

非交换环：$(M_n(\mathbb{R}), +, O_{n\times n}, \cdot, E_n)$

例：设 $(R, +, 0, \cdot, 1)$ 是环

证明：① $\forall r\in R \quad 0r = r0 = 0$

② $\forall r\in R \quad r + (-1)r = r + r(-1) = 0$

即 $-r = (-1)r = r(-1)$

③ $(-1)(-1) = 1$

证：① $0 + 0 = 0$

$\Rightarrow r(0+0) = r0$

$\Rightarrow r0 + r0 = r0$ （分配）

$\Rightarrow r0 + r0 + (-r0) = r0 + (-r0)$

$\Rightarrow r0 + 0 = 0$ （结合）

$\Rightarrow r0 = 0$

类似 $r0 = 0$

② $1 + (-1) = 0$

$r(1+(-1)) = r0 = 0$

$r + r(-1) = 0 \Rightarrow r(-1) = -r$

③ ~~(-1)+~~ 令 $r = (-1)$

$(-1)(-1) = -(-1) = 1$ $\blacksquare$

定理3.1 （广义分配律）

设 $a_1, \dots, a_m, b_1, \dots, b_n \in R$ （环）

则 $(a_1 + \dots + a_m)(b_1 + \dots + b_n)$

$$= \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j = \sum_{j=1}^{n}\sum_{i=1}^{m} a_i b_j$$

证：先证：$\forall b \in R$

(*) $(a_1 + \dots + a_m)b = a_1 b + \dots + a_m b$

对 m 归纳 $m=1$ 显然

设 $m-1$ 时结论成立

$(a_1 + \dots + a_{m-1} + a_m)b = ((a_1 + \dots + a_{m-1}) + a_m)b$

（广义结合律）

$= (a_1+\cdots+a_{m-1})b + a_m b$ （分配律）

$= a_1 b + \cdots + a_{m-1}b + a_m b$

于是 (*) 成立

对 n 归纳： $n=1$. 即 (*)

设 $n-1$ 时结论成立. 当 n 时

$(a_1+\cdots+a_m)(b_1+\cdots+b_n)$

$= (a_1+\cdots+a_m)((b_1+\cdots+b_{n-1})+b_n)$

$= (a_1+\cdots+a_m)(b_1+\cdots+b_{n-1}) + (a_1+\cdots+a_m)b_n$

$= \sum_{i=1}^{m}\sum_{j=1}^{n-1} a_i b_j + \sum_{i=1}^{m} a_i b_n$

$= \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j$ $\cancel{+a_i b_n}$ 类似可得

$(a_1+\cdots+a_m)(b_1+\cdots+b_n) = \sum_{j=1}^{n}\sum_{i=1}^{m} a_i b_j$

推论 3.1 设 $a, b \in R$. $m, n \in \mathbb{Z}$

则 $(ma)(nb) = (mn)(ab)$

证: 情形1. $m>0$, $n>0$. 由定理3.1

~~由3 推论 自 推论~~

$(ma)(nb) = \sum_{i=1}^{m}\sum_{j=1}^{n} ab = (mn)ab$

情形2. $m=0$ 或 $n=0$. 不妨设 $m=0$

由符号约定 $0\cdot a = 0$ $[0_{\mathbb{Z}}\cdot a = 0_R]$

左 $= (ma)(nb) = 0_R(nb) = 0_R$

右 $= 0_{\mathbb{Z}}(ab) = 0_R$

情形3. $m<0$, $n>0$

$ma = (-m)(-a)$ 符号约定

$(-m)(-a)(nb) = \sum_{i=1}^{-m}\sum_{j=1}^{n} (\cancel{-ma}\,{-a})b$

$= (-mn)(-a)b = (-mn)[(-1)ab]$

$= (-mn)(-(ab)) = mn(ab)$.

自己分析 $m>0, n<0$ 和 $m<0, n<0$ 的情形 ∎

定义：设 R 是环，$a, b \in R$，如果

(i) $\exists\, a \neq 0$，但 $ab = 0$ 则称 b 是右零因子

(ii) $\exists\, b \neq 0$ 但 $ab = 0$ …… a 是左零因子

左和右零因子统称为零因子。0 是平凡零因子

注：当 R 是交换时，不区分左右零因子

定义：设 R 是环，$a \in R$，如果存在 $b \in R$

使得 $ab = ba = 1$，则称 a 是可逆元。

例：整数环 $\mathbb{Z}$ 中没有非平凡零因子，可逆元是 ± 1

有理数环中，没有非平凡零因子

任何非零元素都可逆

例：$M_n(\mathbb{R})$（矩阵环）中

① $A \in M_n(\mathbb{R})$ 可逆 $\Longleftrightarrow$ A 是可逆矩阵

② A 是零因子 $\Longleftrightarrow$ A 是不可逆的

验证②　设 A 不可逆，则 $\operatorname{rank}(A) < n$

$\exists\, \alpha_1 \ldots \alpha_n \in \mathbb{R}$，不全为零　使得

$A\vec{\alpha} = \vec{0}_n$，　其中 $\vec{\alpha} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$

$\Rightarrow \quad A(\vec{\alpha}, \underbrace{\vec{0}_n \ldots \vec{0}_n}_{n-1}) = O_{n\times n}$

$\Rightarrow$ A 是左零因子。A 也是右零因子，

对 A^t 用同样的推理可知

命题 3.1　在剩余类环 $\mathbb{Z}_n$ 中，的元素 或者是零因子 可逆元

证：由命题 1.1 (1.2) 可知。

$\bar{m} \in \mathbb{Z}_n$ 是可逆元 $\Longleftrightarrow \gcd(m, n) = 1$

设 $\gcd(m, n) > 1$。若 $\gcd(m, n) = n$

则 $\bar{m} = \bar{0}$ 是平凡的零因子

设 $\bar{m}\neq\bar{0}$ 则 $g=\gcd(m,n)$ 满足 $1<g<n$

则 ~~$m=ag$~~ $m=ag$ $n=bg$，且 $\bar{b}\neq\bar{0}$

$abg=bm$ 而 $abg=an$

$\Rightarrow bm=an$

$\Rightarrow \bar{b}\,\bar{m}=\bar{0} \Rightarrow \bar{m}$ 是非平凡零因子

例：$\mathbb{Z}_{30}$ 中的零因子和可逆元

$\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6},\bar{7},\bar{8},\bar{9},\overline{10},\overline{20},\overline{21},\overline{18},\overline{19},\overline{11},\overline{12},\overline{13},\overline{14},\overline{15},\overline{16},\overline{17},\overline{22},\overline{23},\overline{24},\overline{25},\overline{26},\overline{27},\overline{28},\overline{29}\}$

$\bar{3}\;\overline{10}=\overline{30}=\bar{0}$

$\overline{14}\cdot\overline{15}=\overline{14\times15}=\overline{7\times30}=\bar{7}\;\overline{30}=\bar{0}$

定义：设R是环，如果R没有非平凡零因子，则称R为无零因子环（整环）。当R交换又无零因子时，R称为整环。

定理3.2 设D是无零因子整环，则 $\forall a,b,c\in D$，$a\neq0$，有

$ab=ac \Rightarrow b=c$（左消去律）

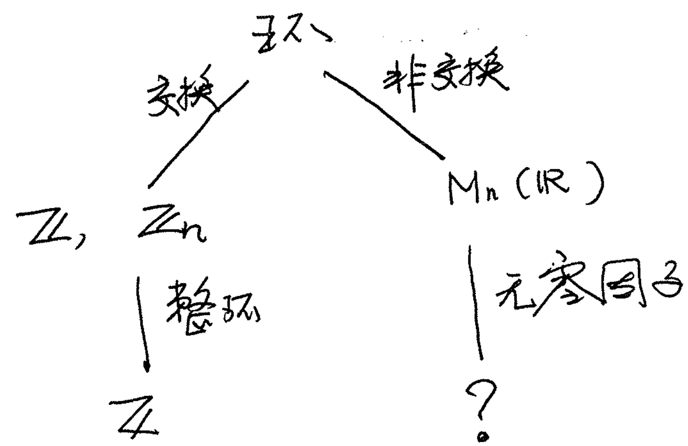
$ba=ca \Rightarrow b=c$（右消去律）

证：$ab=ac \Rightarrow a(b-c)=0$

$\Rightarrow b-c=0$（$\because a$ 不是零因子）

$\Rightarrow b=c$.

右消去律可以类似地证明。



定义：设 R, S 是两个环.

$\varphi: R \to S$ 是环同态如果

$\forall x, y \in R$ (i) $\varphi(x+y) = \varphi(x) + \varphi(y)$

(ii) $\varphi(xy) = \varphi(x)\varphi(y)$

(iii) $\varphi(1_R) = 1_S$.

例：设 $\varphi: R \to S$ 为环同态

则 $\varphi(0_R) = 0_S$

证： $\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R)$

$\Rightarrow \varphi(0_R) = 0_S$

例： $\pi_n: \mathbb{Z} \to \mathbb{Z}_n$ 是环同态

$m \longmapsto \overline{m}$

$\pi_n(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \pi_n(a) + \pi_n(b)$

$\pi_n(ab) = \overline{ab} = \overline{a}\,\overline{b} = \pi_n(a)\pi_n(b)$

$\pi_n(1) = \overline{1}$

例： ① $\overline{m} = \overline{0} \Rightarrow n \mid m$

设 ② $k_1, \ldots k_m \in \mathbb{Z}^+$，大于1两两互素

$\pi_{k_i}(x) = \overline{s_i}$， $i = 1 \ldots m$

$$\Rightarrow \begin{cases} x \equiv s_1 \mod k_1 \\ \vdots \\ x \equiv s_m \mod k_m \end{cases}$$

求解 x 的方法称为中国剩余算法.