

Capable

Only paper with outstanding quality deserves this name.

Notes on

Algebraic Structures

II

~~Mathematical Logic~~

II

Based on Basic Algebra I, Nathan Jacobson.

B5 27lines
8mm | 40 sheets
179X252mm

M·G 晨光

Chap 1. Monoid and Groups

Def 1.1. 设 M 为非空集合, 在 M 上定义一个二元运算 $\cdot: M \times M \rightarrow M$, $(a, b) \mapsto a \cdot b$

满足: 1) $\forall a, b, c \in M$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ 结合律

2) $\exists 1 \in M$, s.t. $\forall a \in M$, $a \cdot 1 = 1 \cdot a = a$. 称 1 为 M 的单位元

则称 $(M, \cdot, 1)$ 为么半群. 简称 M 为么半群 (Monoid)

Ex. 1) $(\mathbb{Z}, +, 0)$, $(\mathbb{Z}, \cdot, 1)$, $(\mathbb{Z}_+, \cdot, 1)$, $(\overline{\mathbb{Z}_-}, +, 0)$

2) 设 A 为非空集合, $(P(A), \cup, \emptyset)$, $(P(A), \cap, A)$.

3) 设 S 为非空集合, $M(S) = \{f \mid f: S \rightarrow S \text{ 映射}\}$,

对 $f, g \in M(S)$, 定义 $(f \cdot g)(a) = f(g(a))$, $\forall a \in S$

则 $\forall f, g, h \in M(S)$, $(f \cdot g) \cdot h = f \cdot (g \cdot h)$

那么 $(M(S), \cdot, 1_S)$ 构成么半群. 称为 S 上变换的么半群.

monoid of transformations on S . 这是重要的例子.

Ex. 变换的么半群.

$S = \{1, 2\}$. $|M(S)| = 2^2 = 4$.

$M(S)$ 中: $\alpha_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$, $\alpha_2 = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$, $\alpha_3 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$, $\alpha_4 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$

设 $(M, \cdot, 1)$ 为么半群. 若有 $1 \in M$, $\forall a \in M$, $1a = a1 = a$.

$1' \in M$, $\forall a \in M$, $1'a = a1' = a$.

则 $11' = 1$, 而 $11' = 1'$. 故 $1 = 1'$.

即: 么半群单位元唯一

设 $(M, \cdot, 1)$ 为么半群, $\forall N \subseteq M$. 若: N 对 M 的乘法也构成一个么半群.

则称 N 为 M 的子么半群 (Submonoid).

N 是 M 的子么半群 iff. ① $1 \in N$, ② $\forall a, b \in N$, $\forall a \cdot b \in N$ (封闭) (结合律自然满足)

No. _____

Date. _____

设 $\mathbb{M} = \{a_1, a_2, \dots, a_n\}$, $1 = a_1$, $(\mathbb{M}, \cdot, a_i=1)$ 为么半群.

$1 \quad a_2 \cdots a_j \cdots a_n$

1 a_2 : a_i : a_n

为乘法表

$$\text{P30 习题 2.(2). 分类讨论. } \begin{cases} x_1y_1 + 2x_2y_2 = x_1z_1 + 2x_2z_2 \\ x_1y_2 + x_2y_1 = x_1z_2 + x_2z_1 \end{cases} \rightarrow \begin{cases} x_1(y_1 - z_1) = 2x_2(z_2 - y_2) \\ x_1(y_2 - z_2) = x_2(z_1 - y_1) \end{cases}$$

当 $x_1=0, x_2 \neq 0$.

当 $x_1 \neq 0, x_2=0$.

当 $x_1 \neq 0, x_2 \neq 0$. 设 $y_1 \neq z_1$, 则必有 $y_2 \neq z_2$. 两式相除.

$$\frac{y_1 - z_1}{y_2 - z_2} = 2 \frac{z_2 - y_2}{z_1 - y_1} \Rightarrow (y_1 - z_1)^2 = 2(y_2 - z_2)^2. \text{ 而 } y_1, z_1, y_2, z_2 \in \mathbb{Z}. \text{ 矛盾.}$$

4. $(M, \cdot, 1)$ monoid.

定义. $a \times b = amb \forall m \in M$.

$$(1) \forall a, b, c \in M, (a \times b) \times c = (amb) \times c = ambmc$$

$$a \times (b \times c) = a \times (bmc) = ambmc.$$

$$(2) \text{要求: } \forall a \in M, a \times b = b \times a = a.$$

$$\text{即 } amb = bma = a.$$

$$\text{令 } a=1. \text{ 则 } mb = bm = 1.$$

且 m 必须可逆, 才有这样的 b .

在么半群 $(M, \cdot, 1)$.

$a \in M$. 若 $\exists b \in M$, s.t. $ab = ba = 1$. 则称 a 为可逆元 (invertible). 并称 b 为 a 的逆元. 记作 $b = a^{-1}$.

若有 $ab = ba = 1$ 且 $ab' = b'a = 1$. 则 $b = b \cdot 1 = b(ab') = (ba)b' = 1 \cdot b' = b'$.

即若 a 可逆, 那么其逆唯一. 记 $U(M)$ 为 M 上所有可逆元组成之集合.

对 $(M, \cdot, 1)$

Ex. 1) 对 $S, M(S)$. 若 $f \in M(S)$ 可逆. 则须存在 $g \in M(S)$ s.t. $f \cdot g = g \cdot f = 1$. 在 $M(S)$ 中
这要求 f 为双射. 另一方面, 若 f 为双射, 则必有如此的 g . 即 f 可逆.
讲. f 为双射

2). 对 $(P(A), \cup, \emptyset)$. 若 $B \in P(A)$, $\exists C \in P(A)$, s.t. $B \cup C = C \cup B = \emptyset$.

则必须 $B = \emptyset$. 即只有 \emptyset 可逆.

3). 对 $(P(A), \cap, A)$. 类似地, 只有 A 可逆.

4). $(\mathbb{Z}, \cdot, 1)$ 只有 1 可逆. $(\mathbb{Z}^-, \cdot, 0)$ 只有 0 可逆.

Def 1.2 设 $(G, \cdot, 1)$ 为么半群. 若 G 的每个元素均为可逆元, 则称 G 为群 (Group).

具体地, 设 G 为非空集合. \cdot 为 G 上二元运算. 满足.

1). $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, $\forall a, b, c \in G$.

2). $\exists 1 \in M$, s.t. $\forall a \in G$, $a \cdot 1 = 1 \cdot a = a$.

3) $\forall a \in G$, $\exists b \in G$, s.t. $a \cdot b = b \cdot a = 1$.

(非零有理数)

Ex. 1). $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{Q}^*, \cdot, 1)$, $(\mathbb{R}^*, \cdot, 1)$.

2). ~~设 S 为非空集合~~. 对么半群 $(M, \cdot, 1)$, $(U(M), \cdot, 1)$ 一定为群.

$\forall a, b \in U(M)$, 则 $(ab)^{-1} = b^{-1}a^{-1}$. 因为 $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$
 $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = 1$.

结合律是自然的. 而 1 可逆, $1^{-1} = 1$. 故 $1 \in U(M)$. 得证

3). 设 S 为非空集合, $U(M(S)) = \{f \mid f: S \rightarrow S \text{ 为双射}\}$. 称为 S 上而衰换群.

若 S 为有限集, $|S| = n$. 称 $U(M(S))$ 为 S 上 \mathbb{Z} 对称群 (Symmetric Groups) 记作 S_n .

$$S = \{1, 2, \dots, n\}, \quad S_n = \left\{ \begin{pmatrix} 1, 2, \dots, n \\ 1, 2, \dots, n' \end{pmatrix} \mid \{1, 2, \dots, n'\} = \{1, 2, \dots, n\} \right\}.$$

$$|S_n| = n!$$

设 M_1, M_2, \dots, M_n 为么半群. $M_1 \times M_2 \times \dots \times M_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in M_i, i=1, \dots, n\}$

定义乘法 $(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (a_1 b_1, \dots, a_n b_n)$

$I^k = (1, 1, 1, \dots, 1)$ 构成么半群, 称为么半群的直和.

对群同样成立.

$$H \neq \emptyset.$$

设 $(G, \cdot, 1)$ 为群, $H \subseteq G$, 若 $(H, \cdot, 1)$ 构成群, 称 H 为 G 的子群 (Subgroup). 记作 $H \trianglelefteq G$.

H 是 G 的子群 iff. 1). $\forall a, b \in H, a \cdot b \in H$.

2). $1 \in H$ (由 1), 可推出, 因为 $a \cdot a^{-1} \in H$.

3) $\forall a \in H, a^{-1} \in H$

iff. 1). $\forall a, b \in H, a \cdot b^{-1} \in H$

2). $\forall a \in H, a^{-1} \in H$.

iff. $\forall a, b \in H, a \cdot b^{-1} \in H$.

$H \neq \emptyset$. 取 $\exists a \in H$. 则 $a \cdot a^{-1} = 1 \in H$.

$\forall a \in H, 1 \cdot a^{-1} = a^{-1} \in H$.

$\forall a, b \in H, b^{-1} \in H \therefore a \cdot (b^{-1})^{-1} = ab \in H$.

No.

Date.

Def. 1.3 设 $(M, \cdot, 1)$, $(M', \cdot', 1')$ 为么半群, 若存在一个双射 $f: M \rightarrow M'$ 满足:

- 1) $f(1) = 1'$
- 2) $f(ab) = f(a)f(b), \forall a, b \in M.$

则称 f 为 M 到 M' 的同构映射, 称 M 与 M' 同构, 记为 $M \cong M'$ (isomorphism).

注: ① ② \Rightarrow 1). 要证 $f(1)b = b f(1) = b, \forall b \in M', 1 \in M.$

$\because f$ 为满射, $\exists a \in M$, s.t. $f(a) = b$.

$\therefore b f(1) = f(a)f(1) = f(a \cdot 1) = f(a) = b$. 类似地 $f(1) \cdot b = f(1)f(a) = f(1 \cdot a) = f(a) = b$.

$$\therefore f(1) = 1'$$

② 设 $f: M \rightarrow M'$ 为映射, 满足 1). $f(1) = 1'$, 2). $f(ab) = f(a)f(b), \forall a, b \in M$.

则称 f 为同态映射, 称 M 与 M' 同态 (homomorphism).

若 f 为单射, 则称 f 为单同态 (monomorphism).

若 f 为满射, 则称 f 为满同态 (epimorphism).

③ 群同态、群同构 (都只要满足 2). 不证).

设 $(G, \cdot, 1)$, $(G', \cdot', 1')$ 为群, $f: G \rightarrow G'$ 为映射, 满足 $f(g_1 g_2) = f(g_1) f(g_2)$,

$\forall g_1, g_2 \in G$, 则 $f(1) = 1'$. (群同态-).

证: $f(1) = f(1 \cdot 1) = f(1)f(1) \in G'$. $f(1)^{-1}f(1) = f(1)^{-1}f(1)f(1) \cdot 1' = f(1)$. \square .

而且. $\forall g \in G$, $g g^{-1} = g^{-1}g = 1$. 则 $f(g)f(g^{-1}) = f(gg^{-1}) = f(1) (= 1') = f(g^{-1}g) = f(g)f(g)$

$\therefore (f(g))^{-1} = f(g^{-1})$.

群同构定义与么半群同构相同.

④

Ex. $f: (\mathbb{R}, +, 0) \rightarrow (\mathbb{R}^+, \cdot, 1)$, $a \mapsto e^a, \forall a \in \mathbb{R}$.

f 为双射且 $f(ab) = e^{a+b} = e^a e^b = f(a)f(b)$.

同构映射可能有多个, 找到一个即可证明两群同构.

⑤ 设 $f: M \rightarrow M'$ 为 M 到 M' 的同构, M, M' 均为么半群 (或群).

$f^{-1}: M' \rightarrow M$, $\forall b' \in M', f(b') = b$, 这里 $f(b) = b'$. 则 f' 是 M' 到 M 的同构.

只需要证: $\forall a', b' \in M', f'^{-1}(a'b') = f'^{-1}(a')f'^{-1}(b')$.

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

$$\therefore f^{-1}(a')f^{-1}(b') = f^{-1}(a'b').$$

⑥ $A = \{\text{群}\}$. 定义关系 R : 对 $G_1, G_2 \in A$, $(G_1, G_2) \in R \Leftrightarrow G_1 \cong G_2$.

自反: 显然

对称: 由⑤可得.

传递: $f: G_1 \rightarrow G_2$ 同构, $h: G_2 \rightarrow G_3$ 同构.

$$\forall a, b \in G_1, (hf)(ab) = h(f(ab)) = h(f(a)f(b)) = h(f(a))h(f(b)) \text{ 故 } R \text{ 是等价关系.}$$

~~Cayley Th:~~ (1) 任何么半群同构于变换么半群

(2) 任何群同构于变换群.

(1). 设 $(M, \cdot, 1)$ 为任意么半群. 定义: $\forall a \in M, a_L: M \rightarrow M, \forall b \in M, a_L(b) = ab \in M$.

称此映射为左平移 (left transformation). $M_L = \{a_L \mid a \in M\} \subseteq M(M)$.

$$\forall c \in M, (a_L b_L)(c) = a_L(b_L(c)) = a_L(bc) = a(bc) = (ab)_L(c).$$

即 $a_L b_L = (ab)_L \in M_L$. 单位元为 1_L .

$$h: M \rightarrow M_L = \{a_L \mid a \in M\}, \forall a \in M, h(a) = a_L.$$

h 显然满. 而且, 若若 $a_L(1) = b_L(1)$, 则 $a \cdot 1 = b \cdot 1$, 即 $a = b$. 故 h 单. 人为双射.

综上, h 为同构. $M \cong M_L \subseteq M(M)$.

即任何么半群同构于某个 $M(s)$ 的某个子么半群.

(2). 当 M 为群. $a_L: M \rightarrow M, \forall b \in M, a_L(b) = ab$. 则 a_L 为双射.

单射: 若 $b_1, b_2 \in M, a_L(b_1) = a_L(b_2)$. 则 $ab_1 = ab_2$. $a^{-1}ab_1 = a^{-1}ab_2$. $b_1 = b_2$.

满射: $\forall b \in M$ 有 $a^{-1}b \in M$. $a_L(a^{-1}b) = a a^{-1}b = b$.

而且, $(a_L)^{-1} = (a^{-1})_L$. 且 $M_L \subseteq U(M(M))$

M_L 为群, $a \rightarrow a_L$ 为群同构.

特别地, 设 G 为有限群. $|G| = n$. 则 $G \cong G_L \leq S_n$.

也有: 右平移: $G_R = \{a_R \mid a \in G\}$, $a_R: G \rightarrow G$, $\forall g \in G, a_R(g) = ga$. 由于: $(a_R b_R)(c) = a_R(b_R(c)) = a_R(cb) = cba = (ba)_R(c)$. 不保持乘法. (但称为反同构).

No.

Date.

Ex. 1) $(\mathbb{R}, +, 0)$, $a \in \mathbb{R}$. $\alpha_L: \mathbb{R} \rightarrow \mathbb{R}$, $\forall b \in \mathbb{R}$; $\alpha_L(b) = a+b$.

2) $\mathbb{R}^X \mathbb{R}$, 乘法 $(a,b)(c,d) = (ac, ad+b)$.

找单位元. 设为 (c,d) . 则 $(a,b)(c,d) = (ac, ad+b) = (a,b) = (c,d)(a,b)$
 $= (ca, cb+d)$.

$$\begin{cases} ac=a \\ ad+b=b \end{cases} \text{由 } a, b \text{ 任意} \Rightarrow \begin{cases} c=1 \\ d=0 \end{cases}$$

求逆元: 对 (a,b) . 设逆元为 (c,d) . $(a,b)(c,d) = (1,0)$, $(a,b) = (1,0)$

$$ac=1 \Rightarrow c=\frac{1}{a}, ad+b=0 \Rightarrow d=-\frac{b}{a} \text{, 则 } (a,b)^{-1} = \left(\frac{1}{a}, -\frac{b}{a}\right).$$

No. _____

Date. _____

广义结合律 (generalized associativity) 对 $(M, \cdot, 1)$:

$\forall a_1, \dots, a_n \in M$. a_1, a_2, \dots, a_n 任意加括号的方式, 结果都相等. 等于标准加括号方式,
 $((\dots((a_1 a_2) a_3) \dots a_{n-1}) a_n)$.

当 $n=1, 2$, 显然.

设 $n \leq k$ 时, 成立. (第二数学归纳法).

当 $n=k+1$ 时, $a_1 a_2 \dots a_{k+1} = (a_1 \dots a_s)(a_{s+1} \dots a_k)$

$$= (a_1 \dots a_s)((\dots((a_{s+1} a_{s+2}) a_{s+3}) \dots a_k) a_{k+1}).$$

利用三元素结合律 $= ((a_1 \dots a_s)(a_{s+1} \dots a_k)) a_{k+1}$.

$= ((\dots((a_1 a_2) a_3) \dots a_{k-1}) a_k) a_{k+1}$. 即标准方式.

加括号方式: $b_n = \sum_{k=1}^{n-1} b_k b_{n-k}$

另一种方式证广义结合律:

定义. $\prod_{i=1}^n a_i = a_1, \prod_{i=1}^n = (\prod_{i=1}^n a_i) \cdot a_n$ (其实就是上述标准加括号方式).

先证, 设 $(M, \cdot, 1)$ 为么半群, $a_1, \dots, a_{n+m} \in M$, $n, m \in \mathbb{Z}_+$. 则

$$(\prod_{i=1}^n a_i) \cdot (\prod_{j=1}^m a_{n+j}) = \prod_{i=1}^{n+m} a_i.$$

当 $m=1$ 时, 显然成立 (定义).

设当 $m=k$ 时, 命论成立.

则当 $m=k+1$ 时, $(\prod_{i=1}^n a_i) \cdot (\prod_{j=1}^{k+1} a_{n+j}) = (\prod_{i=1}^n a_i) \cdot ((\prod_{j=1}^k a_{n+j}) a_{n+k+1})$

$$= ((\prod_{i=1}^n a_i) (\prod_{j=1}^k a_{n+j})) a_{n+k+1} \xrightarrow{\text{归纳假设}} (\prod_{i=1}^n a_i) a_{n+k+1} = \prod_{i=1}^{n+k+1} a_i.$$

$(M, \cdot, 1)$ 为么半群. 若 $\forall a, b \in M$, $ab = ba$. 则称 M 为交换的么半群. 类似地有交换群 (commutative).

设 M 为么半群, $a \in M$: $C(a) = \{b \in M \mid ab = ba\}$ 为 a 的中心化子 (centralizer).

由于 1) $|a = a| = a \Rightarrow 1 \in C(a)$

2) 若 $b, c \in C(a)$, 即 $ab = ba, ac = ca$. 则

$$(ba)(bc)a = b(ac)a = b(ac) = (ba)c = (ab)c = a(bc). \text{ 故 } bc \in C(a).$$

$\therefore C(a)$ 为 M 的子么半群.

3) 对于群的情形. $\forall b \in C(a)$. 若 $ab = ba$, 则

$$b^{-1}(ab)b^{-1} = b^{-1}(ba)b^{-1}. \quad b^{-1}a = ab^{-1}. \quad \therefore b^{-1} \in C(a).$$

$\therefore C(a)$ 为 G 的子群. ($C(a) \leq G$)

设 M 为么半群. $M_\alpha, \alpha \in I$ (指标), 均为 M 的子么半群. 则 $\bigcap_{\alpha \in I} M_\alpha$ 也为 M 的子么半群.

1) $\forall a, b \in \bigcap_{\alpha \in I} M_\alpha$, 即对 $\forall \alpha \in I$, $a, b \in M_\alpha \Rightarrow ab \in M_\alpha, \alpha \in I \Rightarrow ab \in \bigcap_{\alpha \in I} M_\alpha$.

$\Rightarrow \forall a, b \in \bigcap_{\alpha \in I} M_\alpha, 1 \in M_\alpha$

2) $\forall \alpha \in I, 1 \in M_\alpha \Rightarrow 1 \in \bigcap_{\alpha \in I} M_\alpha$

3) 群的情况. $\forall a \in \bigcap_{\alpha \in I} M_\alpha, M_\alpha$ 为 G 的子群. $\therefore a^{-1} \in M_\alpha, \alpha \in I \Rightarrow a^{-1} \in \bigcap_{\alpha \in I} M_\alpha$.

即有:

子么半群(群)的交还是子么半群(群).

$\bigcap_{a \in M} C(a) = \{b \in M \mid \forall a \in M, ab = ba\} = C(M)$, 称为 M 的中心. 是 M 的子么半群.

广义交换律. 设 $a_1, a_2, \dots, a_n \in M$, M 为么半群. $a_i a_j = a_j a_i, 1 \leq i, j \leq n$.

$a_1 a_2 \cdots a_n = a_1 a_2 \cdots a_n$, 其中 $\{1', 2', 3', \dots, n'\} = \{1, 2, 3, \dots, n\}$. (1 到 n 元素的置换).

当 $n=1, 2$ 显然. 设 $n \leq k$ 时结论成立. 则当 $n=k+1$ 时.

$$\begin{aligned} a_1 a_2 \cdots a_{(k+1)}' &= (a_1 a_2 \cdots a_{(i-1)}') (a_{i'} \cdots a_{(k+1)}) \xrightarrow[i=k+1]{\text{归纳假设}} (a_1 a_2 \cdots a_{(i-1)}') (a_{(i+1)}' \cdots a_{(k+1)} a_{k+1}) \\ &= (a_1 a_2 \cdots a_{(k+1)}') a_{k+1} \end{aligned}$$

$$= a_1 a_2 \cdots a_{k+1}.$$

No. _____

Date. _____

$a' = a, a^n = a^{n-1}a = (\cdots((aa)a)\cdots)a \in M, (M, \cdot, 1)$ 为半群.

由广义结合律. $\forall n, m \geq 1, a^n a^m = a^{n+m}$

记: $a^0 = 1$, 上式对任意 $n, m \geq 0$ 成立.

设 a 为 M 的可逆元, 即 $a^{-1} \in M$. 记 $a^{-n} = (a^{-1})^n$. 则 $\forall n, m \in \mathbb{Z}, a^n a^m = a^{n+m}$.

分情况讨论可证.

对 $ab \in M$. 若 $ab = ba$, 则 $(ab)^n = a^n b^n$. ($= (ab)(ab)\cdots(ab)$)

设 G 为交换群, 则常写作 $(G, +, 0)$. 乘法写作 $a+b$, a 的 n 次幂写作 na .

No.

Date.

子集生成的子么半群与子群

设 (M, \cdot) 为么半群, $S \subseteq M$, $S \neq \emptyset$. M 中是否存在包含 S 的最小子么半群? 如果存在, 是否唯一?

唯一: 设 $H(S), H'(S)$ 都为 M 中包含 S 的最小子么半群. 由“最小”

$$H(S) \subseteq H'(S) \text{ 且 } H'(S) \subseteq H(S). \text{ 故 } H(S) = H'(S).$$

存在: $\{M_\alpha\}$, $\alpha \in I$ 为所有包含 S 的子么半群. 则 $S \subseteq \bigcap_{\alpha \in I} M_\alpha$, 而且 $\bigcap_{\alpha \in I} M_\alpha$ 是最小的.

记 $\langle S \rangle = \bigcap_{\alpha \in I} M_\alpha$, 称为由 S 生成的子么半群.

$$\langle S \rangle = \{1, a_1 a_2 \cdots a_k | a_1, a_2, \dots, a_k \in S\} \subseteq M.$$

记 $H = \langle S \rangle$. 由 $S \subseteq H$, 则 H 是包含 S 的子么半群.

$$\langle S \rangle = \{1, a_1 a_2 \cdots a_k | a_1, a_2, \dots, a_k \in S\}.$$

若 H 是包含 S 的子么半群. $\because S \subseteq H$, $\{1, a_1 \cdots a_k | a_1, \dots, a_k \in S\} \subseteq H$.

而又 $\{1, a_1 \cdots a_k | a_1, \dots, a_k \in S\}$ 是包含 S 的子么半群. 故上式成立.

对群的情况, S 生成的子群 $\langle S \rangle = \{a_1 \cdots a_k | a_i \text{ 或 } a_i^{-1} \in S, 1 \leq i \leq k\}$.

设 G 为群, $a \in G$; $\langle a \rangle$ 称为由 a 生成的循环群. (cyclic group generated by a)

$$\langle a \rangle = \{1, a, a^{-1}, a^2, a^{-2}, \dots\}.$$

若 $a^i \neq a^j$, $i \neq j$, $i, j \in \mathbb{Z}$. $\langle a \rangle$ 为无限阶循环群. 记 $o(a) = +\infty$.

$$\varphi: (\mathbb{Z}, +, 0) \rightarrow \langle a \rangle, n \mapsto a^n. \text{ 则}$$

$$\forall n, m \in \mathbb{Z}, \varphi(n+m) = a^{n+m} = a^n a^m = \varphi(n) \varphi(m), \text{ 及 } \varphi(0) = a^0 = 1.$$

$\langle a \rangle$ 中任何元素都是 a 的 n 次幂. 故 φ 为满同态. 当 $\langle a \rangle$ 无限阶, φ 为同构.

若 $\exists i, j$, 使得, s.t. $a^i = a^j$. 不妨设 $i > j$. 则 $a^i = a^j \Rightarrow a^{i-j} = 1$, $i-j > 0$.

故存在正整数 r , s.t. $a^r \neq 1$. 设 r 是使 $a^r = 1$ 的最小正整数. 称 r 为 a 的阶 (order), 记为 $o(a)$. 则 $\langle a \rangle = \{a^0=1, a, a^2, \dots, a^{r-1}\}$. 因为:

$$\forall m \in \mathbb{Z}, m = qr + r', 0 \leq r' < r. \therefore a^m = a^{qr+r'} = a^{qr} \cdot a^{r'} = a^{r'}.$$

No.

Date.

综上，1) 当 $\text{o}(a)=+\infty$ 时 $\langle a \rangle = \{a^0=1, a, a^{\pm 1}, a^2, a^{-2}, \dots\}$.

2) 当 $\text{o}(a)=r$ 时 $\langle a \rangle = \{a^0=1, a, a^2, \dots, a^{r-1}\}$.

考虑

设 G 为群, $a \in G$. 求 $\langle a \rangle$ 的所有子群.

设 H 为 $\langle a \rangle$ 的子群. 当 $H=\{1\}=\langle 1 \rangle=\langle a^0 \rangle$.

当 $H \neq \{1\}$. 取 s 为 $a^n \in H$ 的最小正整数. $m=s \min\{m \in \mathbb{Z}_+ \mid a^m \in H\}$.

则 $H=\langle a^s \rangle$. 证明: $\forall a^n \in H, m=q_s s + s'$, $0 \leq s' < s$, $\therefore a^n=a^{qs+s'}=a^{qs}a^{s'}$.

$\therefore a^{s'}=a^n \cdot (a^s)^{-q}$. $a^n \in H, a^s \in H$. 故 $a^{s'} \in H$. 但 $s' < s$. 故 $s'=0$. (s 的最小性)

所以. 循环群的子群是循环群.

$\therefore H \subseteq \langle a^s \rangle$. 而 $\langle a^s \rangle \subseteq H$ 显然.

设 $\text{o}(a)=r$, 求证 $\text{o}(a^s)=\frac{r}{(r,s)}$ (证互整除)

设 $\text{o}(a^s)=m$ (一定有限, 因为不论如何, $(a^s)^r=1$). $\therefore (a^s)^{\frac{r}{(r,s)}}=a^{\frac{rs}{(r,s)}}=(a^r)^{\frac{s}{(r,s)}}=1$

$\therefore m \mid \frac{r}{(r,s)}$ $\therefore a(a^s)^m=1 \therefore a^{ms}=1 \therefore r \mid ms \therefore \frac{r}{(r,s)} \mid \frac{ms}{(r,s)}=\frac{m \cdot \frac{s}{(r,s)}}{(r,s)}$

而 $\frac{s}{(r,s)}, \frac{r}{(r,s)}$ 互素. 故 $\frac{r}{(r,s)} \mid m$. 所以 $m=\frac{r}{(r,s)}$.

设 G 为群, $a \in G$, 求 $\langle a \rangle$ 的所有子群.

1) 当 $\text{o}(a)=+\infty$, $\langle a \rangle = \{a^0=1, a, a^{\pm 1}, a^2, a^{-2}, \dots\}$. 由群, $a^2 \neq a^0$.

$\{1\} \neq H \subseteq \langle a \rangle$. $\langle a^s \rangle, s=1, 2, \dots$ 各不相同. 故所有子群为 $\{\langle a^s \rangle \mid s=0, 1, 2, \dots\} \sim \mathbb{N}$.

2) 当 $\text{o}(a)=r$, $\langle a \rangle = \{1, a, a^2, \dots, a^{r-1}\}$. 设 $H \subseteq \langle a \rangle$.

当 $H=\{1\}=\langle 1 \rangle$.

当 $H \neq \{1\}$. 这时, $H=\langle a^s \rangle$, 其中 s 为 $a^n \in H$ 的最小正整数 m .

则 $s \mid r$. 设 $r=qs+s'$, $0 \leq s' < s$. $\therefore a^r=a^{qs+s'}=a^{qs} \cdot a^{s'}=1$.

$\therefore a^{s'}=(a^s)^{-q} \subseteq H$. 由 s 的取法知 $s'=0$. 故 $s \mid r$, 即 $r=qs$.

$\therefore H=\langle a^s \rangle=\{1, a^s, a^{2s}, \dots, a^{(r-1)s}\}$, $|H|=\frac{r}{s}$.

反之. 若 $q \mid r$, $r=o(a)$, $\langle a \rangle$ 一定有一个 q 阶子群 $\langle a^{\frac{r}{q}} \rangle$, 且是唯一的 $\langle a \rangle$ 的阶子群.

No.

Date.

设 $H \leq \langle a \rangle$, $|H| = g$, $g \mid r$. 则 $H = \langle a^p \rangle$. 由于 $a^m \in H$ 的最小正整数, 则有 $p \mid r$, $\frac{r}{p} = q$, $p = \frac{r}{q}$.

$\forall n \in \mathbb{Z}_+$, 一定存在 n 阶循环群: $\mathbb{Z}/\langle n \rangle = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\} = \langle \bar{1} \rangle$, $\bar{i} + \bar{j} \equiv \bar{i+j}$:
 $\{e^{\frac{2\pi k i}{n}}, |k=0, 1, \dots, n-1|\} = \langle e^{\frac{2\pi i}{n}} \rangle$

欧拉函数 $\varphi(n)$: 所有小于 n 与 n 互质的正整数个数

对 $\langle a \rangle$: $\circ(a) = r$, 所有 a^k , k 与 r 互质都是 a^k 的生成元; $\langle a \rangle$ 有 $\varphi(r)$ 个生成元。

$H \leq \langle a \rangle$, $|H| = k$. 令 $s = \frac{r}{k}$. $H = \langle a^s \rangle = \langle a^{\frac{r}{k}} \rangle$. H 的生成元个数为 $\varphi(s)$.

$H = \langle a^m \rangle$, $(m, k) = 1$.

无限阶循环群, 不考虑负指数幂, 只有一个生成元。

Cor. 设 $\circ(a) = r < +\infty$, $H \leq \langle a \rangle$, $H \neq \{a\}$. $|H| = g$ ($\because g \mid r$):

则 $H = \{b \mid b \in \langle a \rangle, b^g = 1\}$.

证. $\because H \leq \langle a \rangle$, $|H| = g$, $\therefore H \subseteq \langle a^{\frac{r}{g}} \rangle$. 记 $s = \frac{r}{g}$. $H = \langle a^s \rangle = \{1, a^s, a^{2s}, \dots, a^{(g-1)s}\}$.

而 $(a^s)^g = 1$, 故, 左边 \subseteq 右边。

反之: 设 $b \in \langle a \rangle$, $b^g = 1$. $\therefore b^g = (a^m)^g = a^{mg} = 1$. 又 $\circ(a) = r$. $\therefore r \mid mg$

$\therefore \frac{r}{g} \mid m \Rightarrow s \mid m$. $\therefore b \in \langle a^s \rangle$.

设 G 为有限群, 所以 G 中每个元素的阶均为有限数. $G = \{g_1, g_2, \dots, g_n\}$.

存在 $m \in \mathbb{Z}_+$, s.t. $\forall g \in G, g^m = 1$. 令 m 为使 $g^k = 1$, $\forall g \in G$ 的最小正整数 k .

称 m 为 G 的指数 (exponent). 记为 $\exp G$.

Th 1.4. Let G be a finite abelian group. Then G is cyclic iff. $\exp G = |G|$.

" \Rightarrow ". $G = \langle a \rangle$, $\circ(a) = n$. 则 $\exp G = n = |G|$.

" \Leftarrow ". 由 lemma 1. 设 G 为群, $a, b \in G$, $ab = ba$, $\circ(a) = m$, $\circ(b) = n$, $(m, n) = 1$. 则

$$\circ(ab) = mn$$

即: $\circ(ab)^s = s \cdot \circ(ab)^{mn} = a^{mn} b^{mn} = 1 \Rightarrow s | mn$.

$$\therefore 1 = (ab)^{sm} = a^{sm} b^{sm} = b^{sm}, \therefore n | sm. \text{ 而 } (n, m) = 1, \therefore n | s$$

$$1 = (ab)^{sm} = a^{sn} b^{sn} = a^{sn}, \therefore m | sn, \therefore m | s. \therefore mn | s.$$

Lemma 2. G . Abelian group, finite. g an element of maximal order.

Then $\exp G = \circ(g)$

i) $\forall h \in G$, 证 $\circ(h) \mid \circ(g)$: $\circ(g) = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, $\circ(h) = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$

$$\circ(g) = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} \Rightarrow \circ(h) = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, p_1, p_2, \dots, p_k \text{ 为素数}, f_i, e_i \geq 0.$$

只要证 $e_i \leq f_i, \forall i \in \mathbb{N}$.

反设存在某个 $e_i > f_i$, 不妨设 $e_1 > f_1$.

$$\text{令 } g_1 = g^{p_1^{f_1}}, h_1 = h^{p_1^{e_2} p_2^{e_3} \cdots p_k^{e_k}}$$

$$\circ(g_1) = p_1^{f_2} \cdots p_k^{f_k}, \circ(h_1) = p_1^{e_1} \cdot \text{且 } \circ(g_1), \circ(h_1) \text{ 互素}$$

$$\circ(g_1 h_1) \stackrel{\text{Lemma}}{=} p_1^{e_1} p_2^{f_2} \cdots p_k^{f_k} > \circ(g). \text{ 矛盾.}$$

设 g 为 G 的最大阶元素, $\therefore \circ(g) = \exp G = |G|$. $\therefore G = \langle g \rangle$.

因为 $\langle g \rangle \leq G$.

又子群和本身数目一样多:

No.

Date.

置换的循环分解. Cycle decomposition of permutations.

对 $\alpha \in S_n$. 若 $\alpha(i_1) = i_2, \alpha(i_2) = i_3, \dots, \alpha(i_r) = i_1, \alpha(j) = j$; 当 $j \neq i_1, i_2, \dots, i_r$

即 $\alpha = \begin{pmatrix} i_1 & i_2 & \dots & i_r & i_r & i_{r+1} & \dots & i_n \\ i_2 & i_3 & \dots & i_r & i_1 & i_{r+1} & \dots & i_n \end{pmatrix}$ 称 α 为循环置换 (cyclic permutation).

记作 $\alpha = (i_1 i_2 \dots i_r) = (i_1 i_2 \dots i_r i_1) = \dots$ r-循环.

$$(i_1 i_2 \dots i_r)^k = \begin{cases} (i_1 i_{k+1} i_{2k} \dots i_{(r-1)k}) & , 1 \leq k < r, \text{底数上省略 mod } r, \\ (i_1 i_2 \dots i_r) & , k=r. \end{cases}$$

若对 $(i_1 i_2 \dots i_r), (j_1 j_2 \dots j_k) \in \{i_1, \dots, i_r\} \cap \{j_1, \dots, j_k\} = \emptyset$, 则称为不相交的循环置换.

对不相交的循环置换, 其合成交换, 即 $(i_1 \dots i_r)(j_1 \dots j_k) = (j_1 \dots j_k)(i_1 \dots i_r)$.

对不相交的循环置换的积, 其阶

$$\circ ((r_1 i_1 \dots i_{r_1})(j_1 \dots j_{r_2}) \dots (l_1 \dots l_{r_s})) = [r_1, r_2, \dots, r_s], \text{ 为各置换阶的最小公倍数.}$$

任意置换可以分解为不相交的循环置换的乘积.

对 $\alpha \in S_n$, $\forall i_1 \in \{1, 2, \dots, n\}$, $\alpha(i_1) = i_2, \alpha(i_2) = i_3, \dots, \alpha(i_{r_1}) = i_1$ \rightarrow 只能回到 i_1 , 不能回到中间别的. 因为 α 双射.

于是有 $(i_1 \dots i_{r_1})$,

对 $j_1 \in \{i_1, \dots, i_{r_1}\}$, $\alpha(j_1) = j_2, \alpha(j_2) = j_3, \dots, \alpha(j_{r_2}) = j_1$. 有 $(j_1 \dots j_{r_2})$.

如此做下去, 得 $\alpha = (i_1 \dots i_{r_1}) (j_1 \dots j_{r_2}) \dots (l_1 \dots l_{r_k})$. (可能包括 1-循环 (i)).
 $\{i_1, \dots, i_{r_1}\} \cup \{j_1, \dots, j_{r_2}\} \cup \{l_1, \dots, l_{r_k}\} = \{1, \dots, n\}$, 且两之互不相交.

例. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 6 & 5 \end{pmatrix} = (13)(24)(56)$

No. _____

Date. _____

若 $\alpha = (i_1 \dots i_r)(j_1 \dots j_n) \dots (l_1 \dots l_{n_k})$

$$= (i'_1 \dots i'_{r'}) \dots (j'_1 \dots j'_{n'}) \dots (l'_1 \dots l'_{n_k'})$$

若 i_j 在 $(i'_1 \dots i'_{r'})$ 中，则也必 $i_j \rightarrow i_{j'}, l_1 \rightarrow l_{j'}, \dots$

故在不考虑顺序时，不相交循环置换分解唯一。

称 (ab) 为对换 (transposition).

$(i_1 i_2 \dots i_r) = (i_1 i_r)(i_2 i_{r-1}) \dots (i_{r-1} i_2)(i_r i_1)$, 可对每个 i_j 验证两边相等。

这种写法并不唯一。 $= (i_1 i_2)(i_2 i_3) \dots (i_m i_n)$ (长度也可以不一样)

\Rightarrow 任意一个置换可分解为若干个对换的乘积，这种分解不唯一。

↓ ↗

循环置换 对换数: $\alpha = (i_1 \dots i_r)(j_1 \dots j_n) \dots (l_1 \dots l_{n_k})$, 不相交
(唯一) 定 $N(\alpha) = (r_1 - 1) + (r_2 - 1) + \dots + (r_k - 1)$.

但是，任意一个置换分解为对换的乘积，对换的个数的奇偶性唯一。

$$(ab)(a c_1 \dots c_h b d_1 \dots d_k) = (bd_1 \dots d_k)(a c_1 \dots c_h), a, b, c_i, d_j 各不相等$$

$$\text{两边左乘 } (ab) \text{ 有: } (ab)(bd_1 \dots d_k)(ac_1 \dots c_h) = (ac_1 \dots c_h bd_1 \dots d_k)$$

$$N((ac_1 \dots c_h bd_1 \dots d_k)) = h + k + 2 - 1 = h + k + 1.$$

$$N((bd_1 \dots d_k)(ac_1 \dots c_h)) = k + h$$

$$\Rightarrow N((ab)\alpha) = \begin{cases} N(\alpha) - 1, & \text{若 } a, b \text{ 出现在 } \alpha \text{ 的同一个循环置换中.} \\ N(\alpha) + 1, & \text{若 } a, b \text{ 分别出现在 } \alpha \text{ 的不同的循环置换中.} \end{cases}$$

$$\text{对 } \alpha = (i_1 \dots i_r)(j_1 \dots j_n) \dots (l_1 \dots l_{n_k}) = (a_1 b_1)(a_2 b_2) \dots (a_m b_m)$$

$$\text{则 } 1 = (a_1 b_1)(a_{m-1} b_{m-1}) \dots (a_1 b_1) \alpha$$

$$0 = N(1) = N((a_1 b_1)(a_{m-1} b_{m-1}) \dots (a_1 b_1)(a_1 b_1) \alpha)$$

$$N(a_1 b_1) \alpha = N(\alpha) \pm 1, \quad N((a_1 b_1)(a_1 b_1) \alpha) = (N(\alpha) \pm 1) \pm 1, \dots$$

$$\Rightarrow 0 = N(\alpha) + \sum_{i=1}^m \varepsilon_i, \quad \varepsilon_i = \pm 1. \quad \Rightarrow \varepsilon_i \text{ 全换为 } 1, \frac{m}{2} \varepsilon_i \text{ 奇偶不一致}$$

故 m 与 $N(\alpha)$ 奇偶性相同。

No.

Date.

对 $\alpha \in S_n$, 若分解为奇(偶)个对换之积, 则称 α 为奇(偶)置换.

A_n : S_n 中所有偶置换组成的集合. alternating group.

$A_n \subseteq S_n$ (偶置换之积之逆仍为偶置换, 故闭) 称为交错群.

$|A_n| = \frac{n!}{2}$: 设 $A_n = \{\alpha_1, \dots, \alpha_m\}$, 对 $a, b \in \{1, 2, \dots, n\}$, $(ab)\alpha_i, (ab)\alpha_j$ 互不相等.

同理对任一奇置换 β , 则 $(ab)\beta$ 为偶置换: $(ab)\beta \circ \alpha_i = (ab)(ab)\beta = \beta = (ab)\alpha_i$.

故 $\{(ab)\alpha_1, \dots, (ab)\alpha_m\}$ 即是所有奇置换的集合. 奇、偶置换数目相同, 而 $|S_n| = n!$

故 $|A_n| = n!/2$

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

作业: P₅₁ T 1~5

No. _____

Date. _____

轨道和陪集

S 为集合, G 为 S 的变换群 ($G \leq \text{U}(M(S))$), 在 S 上定义关系 \sim :

$\forall a, b \in S, a \sim b \Leftrightarrow \exists g \in G, \text{s.t. } b = g(a) \quad \text{记作} \quad g \cdot a$

则 \sim 为 S 上的等价关系, 因为,

① $\forall a \in G$, 因为 $a = 1 \cdot (a) = 1 \cdot a$, 1 为 G 上的单位元, 即恒等映射, 故 $a \sim a$; 自反.

② 若 $a \sim b$, 则 $\exists g \in G$, s.t. $b = g(a)$, $\therefore a = g^{-1}(b)$. $g^{-1} \in G$, $\therefore b \sim a$. 对称.

③ 若 $a \sim b, b \sim c$, $\therefore \exists g_1, g_2 \in G$, s.t. $b = g_1(a), c = g_2(b) \therefore c = (g_2 \circ g_1)(a)$.

$g_2 \circ g_1 \in G \therefore a \sim c$. 传递.

$\therefore \sim$ 为 S 上的等价关系.

$$\forall a \in S, [a] = \{b \in S \mid a \sim b\} = \{b \in S \mid \exists g \in G, \text{s.t. } b = g(a) = g \cdot a\}$$

$$= G \cdot a = \{g(a) \mid g \in G\} = \{g \cdot a \mid g \in G\}.$$

记作.

称 $[a]$ 为 a 在 G 下的轨道 (orbit). 划分: $S = \bigcup_{a \in S} [a]$

轨道构成了 S 的一个划分. 称 G 作用 (act) 于 S 上.

特殊情形. 设 G 为群, 左平移 $\forall g \in G, g_L: G \rightarrow G, a \mapsto ga$, 右平移 $g_R:$

$G \rightarrow G, a \mapsto ag$. $G_L = \{g_L \mid g \in G\}$ 为 G 的变换群, $g_L h_L = (gh)_L, g_L^{-1} = (g^{-1})_L$

在 G 上定义等价关系 \sim : $\forall a, b \in G, a \sim b \Leftrightarrow \exists g \in G, \text{s.t. } b = g_L(a) = ga$

若 $S = [a] = G \cdot a$, 则称 G 是可迁的 (transitive). 上面 G_L 的情况, 有 $\forall a, b \in G$,

$$b = (ba^{-1})a = (ba^{-1})_L(a).$$

故 G_L 作用于 G 是可迁的.

设 G 为群, H 为 G 的子群. $G_L = \{g_L \mid g \in G\}, H_L = \{h_L \mid h \in H\}, h_L: G \rightarrow G, a \mapsto ha$.

$\therefore H_L \leq G_L$. H_L 也是 G 的一个变换群. 在 G 上定义等价关系 \sim :

$\forall a, b \in G, a \sim b \Leftrightarrow \exists h_L \in H_L \text{ (} h \in H \text{)}, \text{s.t. } b = h_L(a) = ha$.

No. _____

Date. _____

那么 $\forall a \in G$, $\overset{a}{H} = \{h_1(a) | h_1 \in H\} = \{ha | h \in H\} = Ha$.

称 Ha 为 a 关于 H 的右陪集 (the right coset of a relative to H).

$$G = \bigcup_{a \in G} \overset{a}{H} = \bigcup_{a \in G} Ha.$$

Ha 构成 G 的一个划分.

r 个右陪集

当 G 为有限群, $G = Ha_1 \cup \dots \cup Ha_r$, 有有限个划分的块. $\therefore \bar{I} = H : I = H = \bar{h}$, $h \in H$. 即其中一定有一个等价类是 H 本身. 由于是等价类, 右陪集两之间要么相同, 要么不相交.

$\forall a \in G$, $H \leq G$, $\bar{I} = H$, $\bar{a} = Ha$. 则有双射中: $H \rightarrow Ha$, $h \mapsto ha$. 它是双射, 因为: 单: $h_1 a = h_2 a \Rightarrow h_1 a a^{-1} = h_2 a a^{-1} \Rightarrow h_1 = h_2$; 满: $\forall ha \in Ha$, 有 $h \in H$.

一般地, $\forall a, b \in G$, $H \leq G$, 有 $\varphi: Ha \rightarrow Hb$, $\forall ha \in Ha$, $h \in H$, $\varphi(ha) = hb$. 为双射.

因此, 每个右陪集中元素数目相同, 都等于 $|H|$. 所以, 若 G 有 r 个右陪集, 则 $|G| = |H| \cdot r$, $\therefore |H| \mid |G|$. 子群的阶一定整除大群的阶. 记 $r = \frac{|G|}{|H|} = [G : H]$, 称为 H 在 G 上的指标 (index). 则有定理:

Th1. 设 G 为有限群, H 为 G 的子群, 则 $|H| \mid |G|$, $|G| = |H| \cdot [G : H]$.

进一步,

Th2. G 为有限群, $a \in G$, 则 $\overset{o(a)}{\longrightarrow} |G|$.

因为 $\langle a \rangle \leq G$, 故 $\overset{o(a)}{\longrightarrow} |\langle a \rangle| \mid |G|$.

对左陪集 aH 的情况, 上述叙述类似地成立.

例子. $S = \{1, \dots, n\}$, $\alpha \in S_n$, $\alpha = (i_1 \dots i_r)(j_1 \dots j_s) \dots (l_1 \dots l_u)$

$\langle \alpha \rangle \leq S_n$. 求 $\langle \alpha \rangle$ 在 S 上所有的轨道: i_1, \dots, i_r 在同一轨道, j_1, \dots, j_s 在另一轨道, ...

No. _____
Date. _____

P53 T1. $\alpha \in S_4$, $\alpha = (1234)$. . $\langle \alpha \rangle = \{(1), (1234), (13)(24), (1432)\}$

$$\langle \alpha \rangle \cdot 1 = \langle \alpha \rangle = \langle \alpha \rangle (1234) = \langle \alpha \rangle (13)(24) = \dots$$

$$\langle \alpha \rangle (12) = \{(12), (134), (1423), (243)\}.$$

$$\langle \alpha \rangle (13) = \dots$$

...

- 若 $|S_4| / |\langle \alpha \rangle| = 4! / 4 = 6$ 个右陪集

T2. G 为有限群, $H \leq K \leq G$, $[H : K]$ 为有限. 求证 $[G : K] = [G : H][H : K]$

$$[G : H] = \frac{|G|}{|H|}, [H : K] = \frac{|H|}{|K|}. \text{ 故右边} = \frac{|G|}{|K|} = [G : K].$$

T3. $H_1, H_2 \leq G$ 且 $H_1 \cap H_2 = \{e\}$. $(H_1 \cap H_2)a = H_1 \cap H_2a$.

$\forall h_1a \in H_1 \cap H_2a$, $h_1 \in H_1$ 且 $a \in H_2$. 故 $h_1 \in H_1 \cap H_2$, $h_1a \in$ 左边.

左边 \subseteq 右边也显然.

② 求证 $[G : H_1], [G : H_2]$ 有限 $\Rightarrow [G : (H_1 \cap H_2)]$ 有理

若 $H_1a \cap H_2b \neq \emptyset$. 则 $\forall c \in H_1a \cap H_2b$, $c \in H_1a$, 则 $c = h_1a$, $h_1 \in H_1$. 则 H_1c
 $= (H_1h_1)a = H_1a$; 又 $c \in H_2b$, 故 $h_1a = H_2b$. 故 $H_1a \cap H_2b = H_1c \cap H_2c$
 $= (H_1 \cap H_2)c$

$\because [G : H_1]$ 有理, $\therefore G = H_1a_1 \cup \dots \cup H_1a_m$.

$[G : H_2]$ 有理, $\therefore G = H_2b_1 \cup \dots \cup H_2b_n$.

$$\therefore G = (H_1a_1 \cup \dots \cup H_1a_m) \cap (H_2b_1 \cup \dots \cup H_2b_n)$$

$$= \bigcup_{1 \leq i \leq m} (H_1a_i \cap H_2b_j) \stackrel{\text{由题意}}{=} \bigcup_{1 \leq i \leq m} (H_1 \cap H_2)c_i \stackrel{\text{由题意}}{\subseteq} \bigcup_{1 \leq i \leq m} H_1c_i \stackrel{\text{由题意}}{\subseteq} G$$

同余 congruence

对 $n \in \mathbb{Z}_+$, 在 \mathbb{Z} 上定义关系 \equiv , $\forall a, b \in \mathbb{Z}, a \equiv b \Leftrightarrow n|(a-b) \Leftrightarrow a \equiv b \pmod{n}$

它是等价关系: ① $\forall a \in \mathbb{Z}, a \equiv a$; ②. 若 $a \equiv b, b \equiv c$ 则 $a \equiv c$; ③ $a \equiv b, b \equiv c \Rightarrow a \equiv c$.

在群 $(\mathbb{Z}, +, 0)$ 上, 若 $a \equiv b \pmod{n}, c \equiv d \pmod{n}$, 则 $a+c \equiv b+d \pmod{n}$. 三关系保持
其加法运算.

在么半群 $(\mathbb{Z}, \cdot, 1)$ 上, 若 $a \equiv b, c \equiv d \pmod{n}$, 则亦有 $ac \equiv bd \pmod{n}$. 三关系保持乘法运算.

保持运算的等价关系称为同余关系, 定义如下:

设 $(M, \cdot, 1)$ 为么半群, \equiv 为 M 上的等价关系, 且若 $a \equiv b, c \equiv d$, 则 $ac \equiv bd$
则称 \equiv 为 M 上的同余关系, 简称为同余.

设 S 为集合, \sim 为 S 上等价关系, $\bar{S} = \{\bar{a} | a \in S\} = S/\sim$ 为商集.

设 $(M, \cdot, 1)$ 为么半群, \equiv 为 M 上同余关系, $\bar{M} = \{\bar{a} | a \in M\} = M/\equiv$. 在 \bar{M} 上可定义乘法:

$\forall \bar{a}, \bar{b} \in \bar{M}, \bar{a} \cdot \bar{b} = \bar{ab}$. 要证 · 是运算, 则要证 $\bar{a} = \bar{a}', \bar{b} = \bar{b}' \Rightarrow \bar{ab} = \bar{a'b'}$. (代表元可
有多种选取): $a \equiv a', b \equiv b'$, 则 $ab \equiv a'b'$, 则 $\bar{ab} = \bar{a'b'}$. 即 $\bar{ab} = \bar{a'}\bar{b}'$.

同余关系保证了 \bar{M} 上的 · 是一个运算!

例, 对 $(\mathbb{Z}, +, 0)$ 上之同余 $\equiv \pmod{n}$.

$$\bar{0} = \{kn | k \in \mathbb{Z}\} = \bar{n} = \overline{2n} \dots$$

~~商而太实~~ $(\bar{M}, \cdot, \bar{1})$ 为么半群: $(\bar{a}, \bar{b}) \cdot \bar{c} = \bar{ab} \cdot \bar{c} = \overline{abc} = \overline{a \cdot (bc)} = \bar{a} \cdot \bar{bc}$

所以反元 $\bar{1}$ 满足 $\bar{a} \cdot \bar{1} = \bar{1} \cdot \bar{a} = \bar{a}$, 即 $\bar{a} \cdot \bar{1} = \bar{a}$, 则 $\bar{1} = \bar{a} \cdot (\bar{b} \cdot \bar{c})$.

设 \equiv 为群 G 上的同余关系, 则 $(\bar{G}, \cdot, \bar{1})$ 也是群. $\bar{G} = \{\bar{a} | a \in G\}$. $\forall \bar{a} \in \bar{G}, \exists a \in G, a^{-1} \in G$
 $\therefore \bar{a} \cdot \bar{a}^{-1} = \overline{aa^{-1}} = \bar{1}$. $\bar{G} = G/\equiv$ 是关于同余关系的商群.

设 G 为群, K 为 G 的子群, 如果满足: $\forall g \in G, \exists k \in K, gkg^{-1} \in K$. 则称 K 为 G 的
($g^{-1}kg \in K$).

No.

Date.

正规子群 (normal subgroup). 记作 $K \trianglelefteq G$

条件也可写成等价的:

- 1) $\forall g \in G, gKg^{-1} \subseteq K$; $gKg^{-1} = \{gkg^{-1} \mid k \in K\}$. $K \subseteq gKg^{-1}$.
- 2) $\forall g \in G, gKg^{-1} = K$. $\because g \in G$, 则 $g^{-1} \in G$. $\therefore g^{-1}Kg \subseteq K$; 则 $gKg^{-1} \subseteq K$.
- 3) $\forall g \in G, gK = Kg$.

若一个群的正规子群只有它本身和 $\{1\}$, 则称它为单群 (simple group).

交换群的所有子群都是正规子群.

若群 G 是交换的单群, 且有不止一个元素:

取 G 中的 $a \neq 1$, 则 $\langle a \rangle \leq G$, 且 $\langle a \rangle \neq \{1\}$. 故 $\langle a \rangle = G$, 而且 $\text{o}(a)$ 为素数. 否则, 若 $\text{o}(a) = p_1 p_2$, 则 $\langle a^p \rangle$ 是正规子群, 矛盾.

另一方面, 对任意素数阶循环群也易证是单群.

设 G 为群, 三为 G 上同余关系, 则

- 1) $T = \{a \in G \mid a \equiv 1\}$ 为 G 的正规子群.
 - ① $\forall h, g \in T$, $h \in T, \bar{g} \in T$. \because 三为同余关系. $\therefore \bar{hg} = \bar{h}\bar{g} = \bar{1}$. $\therefore hg \in T$.
 - ② $\forall h \in T$, $(\bar{h})^{-1} = \bar{h^{-1}}$, 又 $\bar{h} = \bar{1}$, 故 $(\bar{h})^{-1} = (\bar{1})^{-1} = \bar{1} = \bar{T}$. $\therefore \bar{h^{-1}} = \bar{1}$, $h^{-1} \in T$.

$\therefore T$ 为 G 的一个子群.

- 2) $\forall g \in G, \forall h \in T$, 要证 $ghg^{-1} \in T$. $\because \bar{ghg^{-1}} = \bar{g}\bar{h}\bar{g^{-1}} = \bar{g}\bar{h}\bar{1}\bar{g^{-1}} = \bar{gg^{-1}} = \bar{1}$. $\therefore ghg^{-1} \in T$. $\therefore T$ 为 G 的正规子群.

2) 设 $K \trianglelefteq G$, 在 G 上定义二元关系三: $\forall a, b \in G, a \equiv b \Leftrightarrow a^{-1}b \in K$, 则三为 G 上的同余关系.

- ① $\forall g \in G, g^{-1}g = 1 \in K$. $\therefore g \in T$. 自反.
- ② 若 $a \equiv b$, 则 $a^{-1}b \in K$. $\therefore b^{-1}a = (a^{-1}b)^{-1} \in K$. $\therefore b \equiv a$. 对称.
- ③ 若 $a \equiv b, b \equiv c$, 则 $a^{-1}b \in K, b^{-1}c \in K$. $\therefore a^{-1}c = (a^{-1}b)(b^{-1}c) \in K$.

No.

Date.

\sim 为 G 上等价关系.

④ 若 $a \equiv b, c \equiv d \Rightarrow a^{-1}b \in K, c^{-1}d \in K \Rightarrow (ac)^{-1}bd = c^{-1}a^{-1}bd = c^{-1}(a^{-1}b)d \in K$

由 $K \trianglelefteq G, \forall g \in G, k \in K, gk \in Kg \subseteq K, k' \in K, gk = k'g \in K \Rightarrow c^{-1}(a^{-1}b)d = k'c^{-1}d \in K$

又 $c^{-1}d \in K \Rightarrow k'c^{-1}d \in K \Rightarrow (ac)^{-1}bd \in K, ac \equiv bd$

3) G 上的同余关系与 G 上的正规子群之间存在一个双射.

$\Psi: A = \{G\text{上的同余关系}\} \rightarrow B = \{G\text{上的正规子群}\}$

\equiv 为 G 上同余关系, $\Psi(\equiv) = \bar{I}$

K 为 G 上正规子群, $\Psi(K) = \equiv, \forall a, b \in G, a \equiv b \Leftrightarrow a^{-1}b \in K$

只要证 Ψ, Ψ' 互逆:

设 \equiv 为 G 上同余关系, $\Psi(\equiv) = \bar{I} = \{a \in G \mid a \equiv I\}$ 为 G 的正规子群.

由正规子群 \bar{I} 来定义 G 上同余关系 \equiv_1 :

$\forall a, b \in G, a \equiv_1 b \Leftrightarrow a^{-1}b \in \bar{I}$.

$a \equiv_1 b \Leftrightarrow a^{-1}b \in \bar{I} \Leftrightarrow \overline{a^{-1}b} = \bar{I} \Leftrightarrow \bar{a} = \bar{b} \Leftrightarrow a \equiv b$

$\therefore \equiv_1 = \equiv, \Psi' \Psi = I$.

反之, 设 $K \trianglelefteq G$, 在 G 上定义同余关系 $\equiv: a \equiv b \Leftrightarrow a^{-1}b \in K$. $\Psi(K) = \equiv$.

$\bar{I} = \{a \in G \mid a \equiv I\} = \{a \in G \mid I \equiv a\} = \{a \in G \mid I^{-1}a = a \in K\} = K$

故 $\Psi \Psi' = I$.

设 $K \trianglelefteq G$, 在 G 上定义等价关系 $\equiv: \forall a, b \in G, a \equiv b \Leftrightarrow a^{-1}b \in K \Leftrightarrow b \in aK$

$\therefore \bar{a} = \{b \in G \mid a \equiv b\} = \{b \in G \mid b \in aK\} = aK = Ka$.

$G/\equiv = \{\bar{a} \mid a \in G\} = \{aK \mid a \in G\}$. 记作 G/K . 商群 (quotient group)

其上的运算是 $\bar{a} \cdot \bar{b} = \bar{ab}$. $\bar{a}(aK)(bK) = (ab)K, (aK)^{-1} = a^{-1}K, \bar{I} = I \cdot K = K$.

$H \trianglelefteq G, K \trianglelefteq G$. 记 $HK = \{hk \mid h \in H, k \in K\}$.

No.

Date.

$$P58. \# T_9. G_1, G_2, G_1 \trianglelefteq G_2. \text{ 求证 } |G_1/G_2| = \frac{|G_1||G_2|}{|G_1 \cap G_2|}$$

$\forall g_1g_2 \in G_1G_2, \exists h_1h_2 \in G_1G_2 \quad \therefore g_1g_2 = h_1h_2 \Leftrightarrow h_1^{-1}g_1 = h_2^{-1}g_2 \in K = G_1 \cap G_2$

令 $h_1^{-1}g_1 = h_2^{-1}g_2 = k \in G_1 \cap G_2$, 则 $g_2g_1 = h_1h_2 \Leftrightarrow h_1 = kg_2, h_2 = g_1k^{-1}, k \in G_1 \cap G_2$
有多少 k , 也就有多少个 h_1 , 有多少个 h_2 . $|G_1/G_2| = \frac{|G_1||G_2|}{|G_1 \cap G_2|}$

同态

逆元

对么半群 M, M' , 若映射 $\eta: M \rightarrow M'$ 满足:

$$1) \eta(ab) = \eta(a)\eta(b), \forall a, b \in M$$

$$2) \eta(1) = 1'$$

称 η 为 M 到 M' 的同态 (homomorphism). 群同态定义相同, 而且:

① 若 G, G' 为群, 映射 $\eta: G \rightarrow G'$ 满足 $\forall a, b \in G, \eta(ab) = \eta(a)\eta(b)$, 则

$$\eta(1 \cdot 1) = \eta(1) = \eta(1) \cdot \eta(1) \in G', \text{ 两边左乘 } (\eta(1))^{-1} \text{ 得 } \eta(1) = 1'.$$

故群的情况只要满足 1).

② 设 M, M' 为么半群, $\eta: M \rightarrow M'$ 为满射, 满足 $\eta(ab) = \eta(a)\eta(b), \forall a, b \in M$.

$$\text{则 } \eta(1) = 1'.$$

$$\forall a' \in M', \text{ 要证 } a'\eta(1) = a' = \eta(1)a'.$$

$$\because \eta \text{ 为满射}, \therefore \exists a \in M, \text{ s.t. } \eta(a) = a' \therefore a'\eta(1) = \eta(a)\eta(1) = \eta(a \cdot 1) = \eta(a) = a'$$

另一个等式一样. $\therefore \eta(1) = 1'$. $\eta(1)$ 为 M' 之单位元

例: ① 设 G 为群, $\forall a \in G$,

$\eta: (\mathbb{Z}, +, 0) \rightarrow G, n \mapsto a^n$ 是同态. 因为

$$\forall m, n \in \mathbb{Z}, \eta(m+n) = a^{m+n} = a^m a^n = \eta(m)\eta(n);$$

$$2) \eta: S_3 \rightarrow \{1, -1\}, \alpha \mapsto \text{sg}(\alpha)$$

② 设 M, M' 为么半群, $\eta: M \rightarrow M'$ 为同态. 则 $\forall a \in M, n \in \mathbb{Z}, \eta(a^n) = (\eta(a))^n$

$n > 0$. 里述. 因为 $\eta(a^n) = \eta(a)\eta(a)^{n-1}$.

$$n=0. \eta(a^0) = \eta(1) = 1' = \eta(a)^0.$$

当 a 为 M 的可逆元时, $\forall n \in \mathbb{Z}_+, \eta(a^{-n}) = (\eta(a^{-1}))^n$.

$$\because a \cdot a^{-1} = 1 \therefore \eta(a \cdot a^{-1}) = \eta(1) = 1' = \eta(a)\eta(a^{-1}), \eta(a^{-1}a) = \eta(1) = 1' = \eta(a^{-1})\eta(a) \therefore \eta(a^{-1}) = \eta(a)^{-1}$$

$$\text{因此, } \eta(a^{-n}) = \eta((a^{-1})^n) = (\eta(a^{-1}))^n = (\eta(a)^{-1})^n = \eta(a)^{-n}$$

Th. 1.7

设 M, M' 为么半群; $\eta_1: M \rightarrow M'$; $\eta_2: M \rightarrow M'$ 为同态; S 为 M 的生成元集, 即 $M = \langle S \rangle$. 如果

No.

Date.

$\forall a \in S, \eta_1(a) = \eta_2(a)$, 则 $\eta_1 = \eta_2$.

$\because \eta_1(1) = 1' = \eta_2(1)$. $\forall b \in M, b \neq 1$, 则 $b = s_1 \cdots s_k$, $s_i \in S$, $0 \leq i \leq k$.

$\therefore \eta_1(b) = \eta_1(s_1 \cdots s_k) = \eta_1(s_1) \cdots \eta_1(s_k) = \eta_2(s_1) \cdots \eta_2(s_k) = \eta_2(s_1 \cdots s_k) = \eta_2(b)$.

对于群的情况, $\forall b \in M$, $b \neq s_1 \cdots s_k$, $s_i \in S$ 或 $s_i^{-1} \in M$, $0 \leq i \leq k$.

$\eta_1(b) = \eta_1(s_1 \cdots s_k) = \eta_1(s_1) \cdots \eta_1(s_k)$. $\forall a \in S$, $\eta_1(a) = \eta_2(a)$ 由 $\eta_1(a)^{-1} = \eta_2(a)^{-1}$, $\eta_1(a^{-1}) = \eta_2(a^{-1})$. 由此, $\forall a \in S$, a 或 $a^{-1} \in S$, 则 $\eta_1(a) = \eta_2(a)$.

$\eta_1(s_1) \cdots \eta_1(s_k) \xrightarrow{S \cong S \cong S} \eta_2(s_1) \cdots \eta_2(s_k) = \eta_2(s_1 \cdots s_k) = \eta_2(b)$.

设 M 为么半群 (或群), 同态 $\eta: M \rightarrow M$ 称为 M 的自同态 (endomorphism); 若 η 为同构, 则称 η 为自同构 (automorphism).

$\text{End}(M) = \{\eta \mid \eta: M \rightarrow M \text{ 为 } M \text{ 的自同态}\}$, 构成么半群.

设 M_1, M_2, M_3 为么半群, $\eta_1: M_1 \rightarrow M_2$, $\eta_2: M_2 \rightarrow M_3$ 均为同态.

则 $\forall a, b \in M_1$, $(\eta_2 \circ \eta_1)(ab) = \eta_2(\eta_1(ab)) = \eta_2(\eta_1(a)\eta_1(b)) = \eta_2(\eta_1(a))\eta_2(\eta_1(b)) = (\eta_2 \circ \eta_1)(a) \cdot (\eta_2 \circ \eta_1)(b)$.

$\eta_2(\eta_1(1)) = \eta_2(\eta_1(1)) = \eta_2(1') = 1''$. $\therefore \eta_2 \circ \eta_1$ 为同态.

由此, 对 $\eta_1, \eta_2 \in \text{End}(M)$, $\eta_1 \circ \eta_2 \in \text{End}(M)$. 封闭. 恒等映射也是同态.

故 $\text{End}(M)$ 构成么半群. $\text{End}(M) \subseteq M(M)$.

$\text{Aut}(M) = \{\eta \mid \eta: M \rightarrow M \text{ 为 } M \text{ 的同构}\}$, 构成群.

设 $\eta: M \rightarrow M_2$ 为同构. 则 $\eta^{-1}: M_2 \rightarrow M_1$ 也为同构. 因为:

$\forall c, d \in M_2$, 要证 $\eta^{-1}(cd) = \eta^{-1}(c) \eta^{-1}(d)$.

$\eta(\eta^{-1}(cd)) = cd$.

$\eta(\eta^{-1}(c) \eta^{-1}(d)) = \eta(\eta^{-1}(c)) \eta(\eta^{-1}(d)) = cd$.

设 M 为么半群, \equiv 为 M 上的同余关系, $\bar{M} = M/\equiv = \{\bar{a} \mid a \in M\}$ 也为么半群. $\bar{a}\bar{b} = \bar{ab}$.

No.

Date.

$\nu: M \rightarrow \bar{M}$, $a \mapsto \bar{a}$ 为同态;

$$\nu(ab) = \bar{ab} = \bar{a}\bar{b} = \nu(a)\nu(b), \quad \nu(1) = \bar{1};$$

ν 称为自然同态.

同态基本定理. 设 M, M' 为么半群, $\eta: M \rightarrow M'$ 为同态. 则

1) $\eta(M)$ 是 M' 的子么半群, 当 M 为群时, $\eta(M)$ 为 M' 的子群.

$\forall \eta(a), \eta(b) \in M$, 由 $a, b \in M$, $\because \eta(a)\eta(b) = \eta(ab) \in \eta(M)$, 故 $\eta(M)$ 上乘法封闭.

$$1' = \eta(1) \in \eta(M).$$

$\therefore \eta(M)$ 是 M' 的子么半群.

当 M 为群, 只要证其中每个元素都有逆元.

$\forall \eta(a) \in \eta(M)$, $a \in M$. $(\eta(a))^{-1} = \eta(a^{-1})$. M 为群, 则 $a^{-1} \in M$. $(\eta(a))^{-1} = \eta(a^{-1}) \in \eta(M)$.

$\therefore \eta(M)$ 为 M' 的子群.

2) 在 M 上定义关系 E_η : $\forall a, b \in M$, $a E_\eta b \Leftrightarrow \eta(a) = \eta(b)$. 则 E_η 为 M 上的同余关系.

且存在唯一的同态映射 $\bar{\eta}: M/E_\eta \rightarrow M'$, 使得图

$$\begin{array}{ccc} M & \xrightarrow{\eta} & M' \\ \downarrow \nu & \nearrow \bar{\eta} & \\ \bar{M} = M/E_\eta & & \end{array}$$

交换, 其中 $\nu: M \rightarrow \bar{M}$ 为自然同态, $\forall a \in M$, $\nu(a) = \bar{a}$. 而且, $\bar{\eta}$ 为单同态.

\hookrightarrow 即 $\bar{\eta} \circ \nu = \eta$.

E_η 显然是等价关系. M 上的. 若 $a E_\eta b$, $c E_\eta d$, $a, b, c, d \in M$. $\because \eta(a) = \eta(b)$, $\eta(c) = \eta(d)$. $\therefore \eta(ac) = \eta(a)\eta(c) = \eta(b)\eta(d) = \eta(bd)$. $\therefore ac E_\eta bd$. $\therefore E_\eta$ 为同余关系. 则

$\bar{M} = M/E_\eta = \{\bar{a} \mid a \in M\}$, 其中 $\bar{a} = \{b \in M \mid b E_\eta a\} = \{b \in M \mid \eta(b) = \eta(a)\}$.

定义 $\bar{\eta}: M \rightarrow M'$, $\forall \bar{a} \in \bar{M}$, $\bar{\eta}(\bar{a}) = \eta(a)$. 先证明 $\bar{\eta}$ 为映射: $\forall \bar{a}, \bar{b} \in \bar{M}$, 若 $\bar{a} = \bar{b}$, $\therefore \exists a, b \in M$ 使 $a E_\eta b$. $\therefore \eta(a) = \eta(b)$. $\therefore \bar{\eta}(\bar{a}) = \bar{\eta}(\bar{b})$.

再证 $\bar{\eta}: \bar{M} \rightarrow M'$ 是同态: $\forall \bar{a}, \bar{b} \in \bar{M}$, $\bar{\eta}(\bar{a}\bar{b}) = \bar{\eta}(\bar{a}\bar{b}) = \eta(ab) = \eta(a)\eta(b) = \bar{\eta}(\bar{a})\bar{\eta}(\bar{b})$,

No.

Date.

$\bar{\eta}(\bar{1}) = \eta(1) = 1'$. $\therefore \bar{\eta}$ 为 \bar{M} 到 M' 的同态.

$\forall a \in M$, $(\bar{\eta}\nu)(a) = \bar{\eta}(\nu(a)) = \bar{\eta}(\bar{a}) = \eta(a)$. $\therefore \bar{\eta}\nu = \eta$, 使得图交换.

此外, $\bar{\eta}$ 是单同态, 因为 $\bar{\eta}(\bar{a}) = \bar{\eta}(\bar{b}) \Rightarrow \eta(a) = \eta(b) \Rightarrow a \sim_{\eta} b \Rightarrow \bar{a} = \bar{b}$.

若还存在同态映射 ψ 使得 $\eta = \psi\nu$. $\forall a \in M$, $(\psi\nu)(a) = \psi(\bar{a}) = \eta(a)$, 故 $\psi(\bar{a}) = \bar{\eta}(\bar{a})$. $\psi = \bar{\eta}$. $\bar{\eta}$ 唯一.

\therefore 当 $\eta: M \rightarrow M'$ 为满同态, 则 $\bar{\eta}: \bar{M} \rightarrow M'$ 为同构.

实际上, $\bar{\eta}: \bar{M} \rightarrow \eta(M)$ 也是同构, $\eta(M) \cong M/E_\eta$

3) 对群的情况, 记 $M = G$.

记 $\bar{1} = \{b \in G \mid b \sim_{E_\eta} a\} = \{b \in G \mid \eta(b) = 1'\} = \text{ker } \eta = \eta^{-1}(1')$, 同态核 (kernel).

在这种情况下, $G \xrightarrow{\eta} G'$

$$\begin{array}{ccc} G & \xrightarrow{\eta} & G' \\ \downarrow \nu & \nearrow \bar{\eta} & \\ G = G/E_\eta & & \\ & = G/K & \end{array}$$

$= G/K$. $K = \text{ker } \eta = \eta^{-1}(1')$.

$\bar{a} = aK = Ka$.

P63. T6 G a group, $a \in G$, $I_a: G \rightarrow G$, $\forall g \in G$, $I_a(g) = \underline{ag^{-1}}$

① 若 $I_a(g_1) = I_a(g_2)$, $\therefore ag_1a^{-1} = ag_2a^{-1}$. $\therefore g_1 = g_2$ } 双射.

② $\forall b \in G$, $I_a(a^{-1}ba) = b$

③ $\forall g_1, g_2 \in G$, $I_a(g_1g_2) = \cancel{a(g_1g_2)a^{-1}} = a(g_1g_2)a^{-1} = (ag_1a^{-1})(ag_2a^{-1}) = I_a(g_1)I_a(g_2)$

$\Rightarrow I_a$ 是 G 的自同构. Call I_a the inner automorphism (or conjugation) of G .

记 $I_m = \{I_a \mid a \in G\} \subseteq \text{Aut}(G)$.

$\eta: G \rightarrow \text{Aut}(G)$, $\forall a \in G$, $\cancel{\eta(a)} = I_a$.

$\forall a, b \in G$, $\eta(ab) = I_{ab}$, $\eta(a)\eta(b) = I_a I_b$.

$\forall g \in G$, $I_{ab}(g) = abg(ab)^{-1} = abgb^{-1}a^{-1} = aI_b(g)a^{-1} = I_a(I_b(g)) = (I_a I_b)(g)$

作业: P63 T1~5

No.

Date.

有同志 $G \xrightarrow{\eta} \text{Aut } G$, $a \mapsto I_a$.

$\ker \eta = \{a \in G \mid \eta(a) = 1\} = \{a \in G \mid I_a = 1\}$. 因为 $\forall g \in G$, $a g a^{-1} = g \cdot a g = g a$.

a 与 G 上任意元素交换, 则 $a \in C(G)$; $\ker \eta = C(G)$.

$$G \xrightarrow{\eta} \text{Aut } G$$

$$\downarrow \nu$$

$$\bar{G} = G/C(G)$$

$$\bar{\eta}: \bar{G} \rightarrow \text{Aut } G,$$

$$\forall \bar{a} \in \bar{G}, \bar{\eta}(\bar{a}) = \bar{\eta}(aC(G)) = \eta(a).$$

$$\text{记 } \eta(G) = \{I_a \mid a \in G\} = \text{Inn}(G).$$

则 $\bar{\eta}: \bar{G} \rightarrow \eta(G) = \text{Inn}(G)$. 是满射. $\text{Inn}(G) \cong G/C(G)$.

核

No.

Date.

 $\forall g \in G, gkg^{-1} \in K. \quad \forall h \in H, hkh^{-1} \in K.$
 $\Rightarrow K \trianglelefteq H$

Th 1.8. G a group, $K \trianglelefteq G$, $H \leq G$ and $K \subseteq H$. Then.

- 1) $\bar{H} = H/K \subseteq \bar{G} = G/K$ 2) and $H \rightarrow \bar{H} = H/K$ is a bijective map of the set of subgroups of G containing K with the set of subgroups of \bar{G} .
- 3) $H \leq G$, $K \subseteq G$. Then $H \trianglelefteq G \Leftrightarrow H/K \trianglelefteq G/K$.

Proof. 1) $H \leq G$, $K \subseteq G$, $\therefore K \trianglelefteq H$.

$$\forall \bar{h}_1, \bar{h}_2 \in H/K, h_1, h_2 \in H, \bar{h}_1 = h_1K, \bar{h}_2 = h_2K \Rightarrow \bar{h}_1\bar{h}_2^{-1} = (h_1K)(h_2K)^{-1} = h_1h_2^{-1}K \in H/K$$

$$(\bar{h}_1)^{-1} = (h_1K)^{-1} = h_1^{-1}K \in H/K. \quad \therefore H/K \trianglelefteq G/K.$$

2)

No.

Date.

No. _____

Date. _____

G. a group, $H \leq G$, $K \trianglelefteq G$, Then

1) $HK \leq G$, $HK = KH$.

$h_1k_1, h_2k_2 \in HK$. $h_1h_2k_1'k_2 \in HK$, $k_1' \in K$.

$\forall h \in H, k \in K$, $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}k'$, $k' \in K$. $(hk)^{-1} \in HK$.

$\Rightarrow HK \leq G$.

而且, $K \trianglelefteq G$, 故 $hK = Kh$, $\forall h \in H$. 故 $KH = HK$.

2) $K \trianglelefteq HK$, $HK \trianglelefteq H$.

$\forall h \in H$. $\forall k \in HK$, $hkh^{-1} \in \cancel{HK} \in HK$.

3) $H \xrightarrow{\cong} HK/K$ 是满同态

$H \leq (\mathbb{Z}, +, 0)$. 若 $n \in H$, 则 $-n \in H$.

令 s 为 H 中最小正整数. 则 $\forall n \in H$, $n = qs+r$, $0 \leq r < s$. $r = n - qs \in H$. 由 s 的取法, $r=0$. $n=qs$. 故 $H = \langle s \rangle$.

$\eta: (\mathbb{Z}, +, 0) \rightarrow \langle a \rangle = \{1, a^{\pm 1}, a^{\pm 2}, \dots\}$, $n \mapsto a^n$. 是满同态.

$\text{ker } \eta = \{n \in \mathbb{Z} \mid a^n = 1\} \trianglelefteq \mathbb{Z}$

1) $\text{ker } \eta = \{0\}$. η 是单的. 则 $\mathbb{Z} \cong \langle a \rangle$

2) $\text{ker } \eta \neq \{0\}$, 且 $\text{ker } \eta = \langle s \rangle$. 实际上, $s = o(a)$. $\therefore \mathbb{Z}/\langle s \rangle \cong \langle a \rangle$

$\mathbb{Z}/\langle s \rangle = \{1, \bar{1}, \dots, \bar{s-1}\}$.

若 $H \leq \mathbb{Z}$, $\langle s \rangle \subseteq H$. 则 $H = \langle s \rangle$, $\langle s \rangle \leq k$. $\therefore s \in \langle k \rangle$. $\therefore k|s$.

No.

Date.

对 $G \times S$ 的作用.Variables. 定义二元关系 $a \sim b$ iff. $\exists g \in G$, s.t. $b = g(a) = ga$.满足: ① $\forall s \in S$, $1 \cdot s = s$, $1 \in G$.② $\forall g_1, g_2 \in G$, $\forall s \in S$; $(g_1 g_2) \cdot s = g_1 \cdot (g_2 \cdot s)$

存在同态

设 S 是集合, G 是群, $T: G \rightarrow \text{Sym } S$: ① $T(1) = 1_S$, ② $T(g_1 g_2) = T(g_1) T(g_2)$, $g_1, g_2 \in G$.定义映射 $G \times S \rightarrow S$, $(g, s) \mapsto T(g)(s) \stackrel{\text{定义}}{=} g \cdot s$ 满足: ① $1 \cdot s = T(1)(s) = 1_S(s) = s$, $\forall s \in S$.

$$\begin{aligned} \text{② } (g_1 g_2) \cdot s &\stackrel{\text{定义}}{=} T(g_1 g_2)(s) = (T(g_1) T(g_2))(s) = T(g_1)(T(g_2)(s)) = T(g_1)(g_2 \cdot s) \\ &= g_1 \cdot (g_2 \cdot s) \end{aligned}$$

Def. 1.7. A group G is said to act on the set S if there exists a map $(g, x) \mapsto g \cdot x$ of $G \times S$ into S satisfying

$$1) 1 \cdot s = s, \forall s \in S$$

$$2) (g_1 g_2) \cdot s = g_1 \cdot (g_2 \cdot s), \forall g_1, g_2 \in G, s \in S.$$

有 $G \rightarrow \text{Sym } S$ 的同态就有 G 对 S 上的作用.

反过来.

而若有这样的作用, 定义 $T: G \rightarrow \text{Sym } S$, $\forall g \in G$, $T(g)(s) = g \cdot s$, $\forall s \in S$. 则 T 是同态 $\rightarrow G$ 在 S 上的作用本质上是存在 G 到 S 的变换群的同态.若 G 是群, $T: G \rightarrow M(S)$ 是么半群意义的同态. 满足

$$T(1) = 1_S, T(g_1 g_2) = T(g_1) T(g_2).$$

那么: $\forall g \in G$: $T(g g^{-1}) = T(g) T(g^{-1}) = T(g^{-1}) T(g) = 1_S$. $\therefore g \in G$ 全被映射到 $M(S)$ 的 1_S 里.Examples. 1. G a group, $S = G$. $G \times G \rightarrow G$, $(g, s) \mapsto gs$ (看作左平移)

$$① 1 \cdot s = s, ② (g_1 g_2) \cdot s = g_1 \cdot (g_2 \cdot s) = g_1 \cdot g_2 s = g_1 \cdot g_2 \cdot s$$

2. G a group. $\Rightarrow S = G$, $G \times G \rightarrow G$, $(g, s) \mapsto sg^{-1}$

$$\textcircled{1} \quad 1 \cdot s = s \cdot 1^{-1} = s. \quad \textcircled{2} \quad (g_1 g_2) \cdot s = s(g_1 g_2)^{-1} = s g_2^{-1} g_1^{-1} = (g_2 \cdot s) g_1^{-1} = g_1 \cdot (g_2 \cdot s).$$

3. G a group, $S = G$. $G \times G \rightarrow G$, $(g, s) \mapsto g \cdot s = gsg^{-1}$ (共軛作用) action by conjugation

$$\textcircled{1} \quad 1 \cdot s = 1s^{-1} = s. \quad \textcircled{2} \quad (g_1 g_2) \cdot s = g_1 g_2 s(g_1 g_2)^{-1} = g_1 g_2 s g_2^{-1} g_1^{-1} = g_1(g_2 \cdot s) g_1^{-1} = g_1 \cdot (g_2 \cdot s)$$

4. 已有 $G \cdot S$. $H \leq G$. $\exists \times H \times S \rightarrow S$, $(h, s) \mapsto h \cdot s$, 它是 H 在 S 上的子作用

5. G a group, $H \leq G$, let $G/H = \{aH \mid a \in G\}$ (H not necessarily normal)

$$G \times G/H \rightarrow G/H$$

$\therefore G$ acts on G/H $\wedge \forall g \in G, aH \in G/H, g \cdot (aH) = (ga)H$

let G act on S . $G \times S \rightarrow S$.

G act on S effectively if T is injective, $T: G \rightarrow M(S)$, $\forall g \in G, T(g): S \rightarrow S$.

$$\forall s \in S, T(g)(s) = g \cdot s \in S. \quad \ker T = \{1\}.$$

$$\rightarrow \forall s \in S, g \cdot s = s \Rightarrow g = 1$$

若此作用 effective. (ii)

若 $g \in G$, $gah = ah$ for any $aH \in G/H$. $\Rightarrow g = 1$.

$$a^{-1}gah = H, \forall a \in G.$$

$$a^{-1}ga \in H, \forall a \in G.$$

$$\Leftrightarrow g \in \bigcap_{a \in G} aHa^{-1}, \forall a \in G.$$

$$g \in \bigcap_{a \in G} aHa^{-1}.$$

$$\bigcap_{a \in G} aHa^{-1} = \{1\}.$$

$G \times G/H \rightarrow G/H, (g, aH) \mapsto gah$ 不是 effective, 因为 若 $g(aH) = aH$, $gaH = aH$.

~~$g^{-1}a^{-1}g \in aHa^{-1}$~~ . 不止一个 g 满足 ~~$g^{-1}a^{-1}g \in aHa^{-1}$~~

G a group, S, S' sets. G acts on S . $T: G \rightarrow \text{Sym } S$

G act. on S' . $T': G \rightarrow \text{Sym } S'$

No.

Date.

$G \cdot S, \forall a \in S, \text{stab } a = \{g \in G \mid ga = g\}$

if there exists a bijection $\varphi: S \rightarrow S'$ s.t. for every $g \in G$,

$$\begin{array}{ccc} S & \xrightarrow{g \cdot s} & S \\ \downarrow \varphi & & \downarrow \varphi \\ S' & \xrightarrow{g \cdot s} & S' \end{array}$$

is commutative.

i.e. $\forall s \in S, \forall g \in G, \varphi(gs) = g\varphi(s), (gs)' = g \cdot s'$

Then the actions T and T' are called equivalent.

e.g. $G \times G \rightarrow G, (g, s) \mapsto gs$

$G \times G \rightarrow G, (g, s) \mapsto sg^{-1}$

let $\varphi: G \rightarrow G, s \mapsto s^{-1}$

$\forall g \in G, \forall s \in G, \varphi(gs) = (gs)^{-1} = s^{-1}g^{-1} = \varphi(s)g^{-1} = g \cdot \varphi(s)$

G act on $S, \forall a, b \in S, a \sim b \Leftrightarrow \exists g \in G, \text{ s.t. } b = ga$

① $\forall a \in S, a \sim a$.

② If $a \sim b$, then $b = ga \cdot g^{-1}b = g^{-1}(ga) = (g^{-1}g)a = 1a = a \cdot b \sim a$.

③ If $a \sim b, b \sim c$, then $a \sim c$

$\forall a \in S, \bar{a} = \{b \in S \mid \exists g \in G, \text{ s.t. } b = ga\} = Ga = \{ga \mid g \in G\}$. orbit

If $S = G \cdot a, a \in S$, transitive (証明省略).

G a group, $H \subseteq G$. $G \times G/H \rightarrow G/H, (g, aH) \mapsto g a H$.

$\forall aH, bH \in G/H$, there exists $g = ba^{-1} \in G$ s.t. $bH = g(aH) = gaH$.

G acts on S transitively. $a \in S \wedge S \geq G \cdot a$. $\varphi: G \rightarrow S = Ga, g \mapsto g \cdot a \in S$

$\forall g_1, g_2 \in G, g_1 \sim g_2 \Leftrightarrow \varphi(g_1) = \varphi(g_2) \Leftrightarrow g_1 a = g_2 a \Leftrightarrow g_2^{-1}g_1 a = a \Leftrightarrow g_2^{-1}g_1 \in \text{stab } a$

No.

Date.

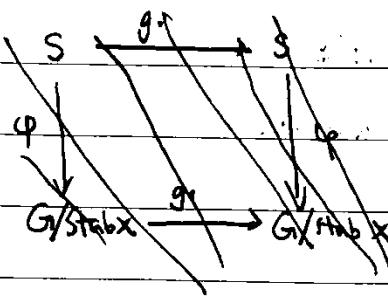
$\Leftrightarrow g \in g \cdot \text{stab}_x \cdot \bar{\varphi}: G_x/\text{stab}_x \rightarrow S, \forall \bar{g} = g \cdot \text{stab}_x \in G_x/\text{stab}_x, \bar{\varphi}(\bar{g}) = \varphi(g)$.

~~$\bar{g}_1 \bar{g}_2 = g_1 \cdot g_2$~~ $\bar{g}_1 = \bar{g}_2 \Rightarrow \bar{\varphi}(\bar{g}_1) = \bar{\varphi}(\bar{g}_2)$. $\therefore \bar{\varphi}$ is surjective.

φ_{is} \Rightarrow

G acts on S transitively ~~on~~, $S = Gx, x \in S$.

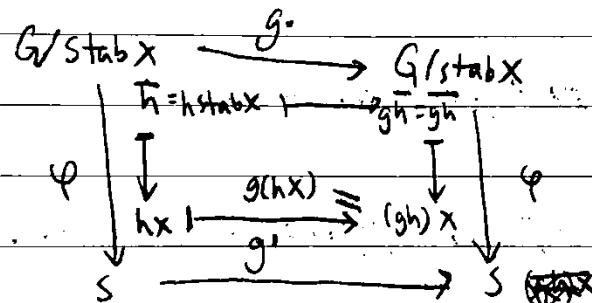
~~$\varphi: G/\text{stab}_x \rightarrow S, g \cdot \text{stab}_x \mapsto g \cdot x$~~ \Rightarrow ~~surjective~~



$\forall s \in S = Gx \rightarrow s = h \cdot x, h \in G$. $\varphi(g \cdot h \cdot x) = \varphi(gh \cdot x) = \bar{gh} = gh \cdot \text{stab}_x$

$$g \cdot \varphi(h \cdot x) = g \cdot \bar{h} = \bar{gh}$$

$\varphi: G/\text{stab}_x \rightarrow S, g \cdot \text{stab}_x \mapsto g \cdot x$ \Rightarrow ~~surjective~~.



即：群作用实质上只有一种，即作用在陪集空间上

$$|S| = |G/\text{stab}_x| = [G : \text{stab}_x] = \frac{|G|}{|\text{stab}_x|}$$

G acts on S : ~~both~~ $\Leftrightarrow \exists g \in G, \forall x \in S$

$\forall x, y \in S, x \sim y \Leftrightarrow \exists g \in G, \text{s.t. } y = gx$

$\forall x \in S, \bar{x} = \{y \in S \mid \exists g \in G, \text{s.t. } y = gx\} = \text{G}x$

$S = \bigcup_{x \in S} \bar{x}; \bar{x}_i = G \cdot x_i \subset S$; $Gx \cdot Gx \nrightarrow Gx$; $\nexists G \times S \rightarrow S$ 限制在 Gx_i 上 ~~且~~ 适用。

$$(g, h \cdot x_i) \xrightarrow{\quad} gh \cdot x_i$$

No.

Date.

而且 $G|_{Gx_i}$ 是可逆作用 (有 Gx_i 上)

$$S = \bigcup_{x_i \in S} \bar{x}_i \cup \dots \cup \bar{x}_n = Gx_1 \cup \dots \cup Gx_n$$

$$|S| = \sum_{i=1}^n |\bar{x}_i| = \sum_{i=1}^n |Gx_i|.$$

$G \rightarrow Gx_i$ 对应于 $G/G\text{stab } x_i \rightarrow Gx_i$

$$= \sum_{i=1}^n [G : \text{stab } x_i]$$

考虑共轭作用: $G \times G \rightarrow G$, $(g, a) \mapsto gag^{-1}$

共轭类: $\bar{a} = \{b \in G \mid \exists s \in G \text{ s.t. } b = gag^{-1}\}$. i.e. $G \cong \bigcup \bar{a}_i$

$$|\bar{a}_i| = |G/\text{stab } a_i| \quad \because \text{stab } a_i = \{g \in G \mid gag^{-1} = a\} = \{g \in G \mid gag^{-1} = a\} = C(a_i)$$

$$|G| = \sum [G : \text{stab } a_i] = \sum [G : C(a_i)] = |C(G)| + \sum [G : \text{stab } b_i]$$

(不会只有一个元素 $\Leftrightarrow x_i \in C(G)$)

Th. 1.11 Any finite group G of prime order has a center $C \neq \emptyset$

$$|G| = |C(G)| + \sum [G : \text{stab } x_i], \quad x_i \notin C(G)$$

$$p \mid |G| \quad \text{又 } |G| = p^k, \quad p \mid [G : \text{stab } x_i], \quad \forall i \quad p \nmid |C(G)|$$

故 $\text{stab } x_i \subseteq C(G)$, $G \times S \rightarrow S$, $(g, x) \mapsto gx$

$\forall i \quad (C(G)x) \subseteq x \in \text{stab } S$, 故 $\forall i \quad C(G)x = x$

$$\text{③ } (g_1 g_2)x = g_1(g_2x), \quad \forall g_1, g_2 \in G, x \in S$$

$\Pi(S) = \{S_1, S_2, \dots, S_k\}$ a partition of S , 若 $\forall S_i \in \Pi(S)$, 都 $\forall g \in G, g \cdot S_i \in \Pi(S)$.

称 $\Pi(S)$ 是稳定的. 对任何集合 S , $\Pi = \{S\}$ 和 $\Pi\{\{a_i\} \mid a_i \in S\}$ 一定稳定.

若被 Π 所稳定的划分只有两个(最小、最大). 则 Π 是本原的(primitive).

作业:

No.

Date.

素数阶子群一定为循环群。

$|A_4| = \frac{1}{2}|S_3| = 12$, $6 \mid 12$, 但 A_4 没有六阶的子群。

~~p a prime number, if $p^k \mid |G|$, then G has a subgroup of order p^k~~

Sylow I. If p is a prime, $p^k \mid |G|$, then G contains a $\overset{k \geq 0}{\text{subgroup}}$ of order p^k .

Proof: 当 $|G| = 2$, 显然成立。

~~该处未写明~~ 当 $|G| = n$, 假设对所有小于 n 的情形都成立。

特殊情形: Cauchy: 设 G 为有限的 Abel 群, $p \mid |G|$, p 为素数, 则 G 一定包含 p 阶子群。

当 $|G| \geq 2$, 显然成立, 当 $|G| = n > 2$ 时, 假设对所有小于 n 的情形都成立。

$\forall a \in G, a \neq 1$. $\circ(a) = r$. 且 $p \mid r$. 即 $r = pr'$. 则 $\circ(a^{r'}) = p$, $|\langle a^{r'} \rangle| = p$.

且 $p \nmid r$, $|G/\langle a \rangle| = \frac{|G|}{|\langle a \rangle|}$. 故 $p \mid |G/\langle a \rangle|$.

$\therefore |G/\langle a \rangle| < |G|$ 且 $p \mid |G/\langle a \rangle|$. 由归纳假设知, $G/\langle a \rangle$ 一定包含一个 p 阶子群. 即存在 $\bar{b} \in G/\langle a \rangle$, $\circ(\bar{b}) = p$. 设 $\circ(b) = s$, $\bar{b}^s = \bar{1}$. 故 $p \mid s$. 令 $s = ps'$, 则 $\circ(b^{ps'}) = p$. $|\langle b^{ps'} \rangle| = p$.

而在一般情形, $|G| = |C(G)| + \sum [G : \text{stab } x_i] = |C(G)| + \sum [G : C(x_i)]$, $x_i \notin C(G)$.

① 当 $p \nmid |C(G)|$, 则 $p \nmid [G : C(x_i)]$, 对某个 i .

$p^k \mid |G|$, $|G| = [G : C(x_i)] |C(x_i)|$. $\therefore p^k \mid |C(G)|$. 又 $\because |C(G)| < |G|$.

由归纳假设, $C(x_i)$ 包含 p^k 阶子群。

② 当 $p \mid |C(G)|$, 由 Cauchy 定理, $C(G)$ 包含一个 p 阶子群 $\langle a \rangle$, $\circ(a) = p$.

$a \in C(G)$, 故 $\langle a \rangle \subseteq G$. $\therefore |G/\langle a \rangle| = \frac{|G|}{|\langle a \rangle|} = \frac{|G|}{p} \therefore p \nmid |G|$, $\therefore p^{k-1} \mid |G/\langle a \rangle|$

由归纳假设知, $G/\langle a \rangle$ 有一个 p^{k-1} 阶子群 \bar{H} . 则在 G 中有 $H \geq \langle a \rangle$ 的 H 与 \bar{H} 一一对应, $\bar{H} = H/\langle a \rangle$. $\therefore |H| = p^k$.

若 $p^k \mid |G|$ 但 $p^{k+1} \nmid |G|$. 由 Sylow I 定理, 在 G 有 p^k 阶子群, 称为 Sylow p -子群。

Sylow II (i) Any two Sylow p -subgroups of G are conjugate in G . i.e., if P_1

No.

Date.

and P_2 are Sylow p -subgroups, then there exists an $a \in G$ s.t. $P_2 = aP_1a^{-1}$

(2) The number of Sylow p -subgroups is a divisor of the index of any Sylow p -subgroup and is $\equiv 1 \pmod{p}$

(3) Any subgroup of order p^k is contained in a Sylow subgroup.

$\Pi = \{H \mid H \leq G\}$, $\forall x \in G \times H \rightarrow H, (g, h) \mapsto g \cdot H = ghg^{-1}$. \bar{g} 证据这个作用.

$\bar{H} \triangleleft H \in \Pi$, $\bar{H} = G \cdot H = \{g \cdot H \mid g \in G\} = \{ghg^{-1} \mid g \in G\}$, $|\bar{H}| = [G : \text{stab } H]$

~~由 $H \triangleleft G$, $\forall g \in G, g \cdot H = H$ 且 $g \cdot H = H \Rightarrow g \in \text{stab } H$.~~ H 的稳定化子

$\text{stab } H = \{g \in G \mid g \cdot H = H\} = \{g \in G \mid ghg^{-1} = H\} = N(H)$. $H \trianglelefteq N(H)$

Lemma. Let P be a Sylow p -subgroup of G , H a subgroup of order p^j contained in $N(P)$. Then $H \subset P$.

Proof. $\because P \trianglelefteq N(P)$. $\forall H \leq N(P)$. $HP = PH \leq N(P)$, $P \trianglelefteq HP$

$\therefore HP / P \cong H / (H \cap P)$. $\therefore |H / (H \cap P)| \mid |H|$, $|H / (H \cap P)| = p^{j'}$

$\therefore |HP| = |P| |HP / P| = p^k p^{j'}$. 而 P 为 Sylow p -子群, 故 $j' = 0$. $HP = P$.

$\therefore H \subset P$.

Proof (of Sylow II). Let Π be the set of Sylow p -subgroups of G , let G act on Π by conjugation.

$\Pi = \{H \mid H \trianglelefteq G \text{ 且 Sylow } p\text{-子群}\}$. $\forall g \in G, \forall H \in \Pi, g \cdot H = ghg^{-1}$.

~~设元素集中一个轨道, $\Sigma = G \cdot \Pi$, $H \in \Pi$, $R \subseteq \Sigma$, P 在 Σ 上~~

$\forall \Sigma, g \in R, g \cdot H = ghg^{-1}$ $\forall g \in P, g \cdot P = gp^{-1} = P$. P 在轨道上数 $\#$. 而若 $P' = gp'g^{-1}, \forall g \in P$, $\therefore P \subset N(P')$, $\therefore P = P'$. 即 $\#$ 为 1 轨道只有 1 个.

$\forall H \in \Pi$, $\bar{H} = G \cdot H = \{ghg^{-1} \mid g \in G\}$, $|H| = [G : \text{stab } H] = [G : N(H)]$. $\therefore \text{stab } H = \{g \in G \mid ghg^{-1} = H\} = N(H)$, H 的稳定化子 (normalizer)

idea:

Proof of Sylow II. (p is a prime). Π' = the set of all sylow p -subgroups of G .
 $H \in \Pi'$, $gH = gHg^{-1}$. $G \times \Pi' \rightarrow \Pi'$. 是 G 在 Π' 上的共轭作用. 则要证
 所有 Sylow p -子群共轭. 只要证 G 作用于 Π' 可逆.

G a finite group, p a prime. Π : the set of all sylow p -subgroups of G .
 $G \times \Pi \rightarrow \Pi$. $\{g, H\} \mapsto gH = gHg^{-1}$.

Σ ~~is~~ one of the orbits under this action.

$$\Sigma = \{gH = \{gHg^{-1} \mid g \in G\}\}. |\Sigma| = [G : \text{stab } H] = [G : N(H)] / [G : H]$$

$\forall P \in \Sigma$, P acts on Σ by conjugation. $\forall g \in P, H \in \Sigma, (g, H) \mapsto gHg^{-1}$

$$\forall P \in \Sigma, \bar{P} = \{g \cdot P \mid g \in P\} = \{gPg^{-1} \mid g \in P\} = \{P\}, |\bar{P}| = 1.$$

假设 $P' \in \Sigma$ 且 $|\bar{P}'| = 1$, $P' \neq P$. $\bar{P}' = P \cdot P' = \{gP'g^{-1} \mid g \in P\}$. 反一个元素. 则

$\forall g \in P, gP'g^{-1} = P' \therefore P \subset N(P')$. 由 Lemma, $P = P'$. 则 P 作用于 Σ 上,
 阶数为 1 的轨道只有一个. 而由 $|\Sigma| = [G : s] = [G : \text{stab } s]$, 其他轨道的元素
 个数被 P 整除. 故 $|\Sigma| \equiv 1 \pmod{p}$.

Claim: $\Pi = \Sigma$.

若另外还有轨道 Σ' (G 作用于 Π 上的). 任取 $P' \in \Sigma'$, 命 P' 作用于 Σ 上.

$$P' \times \Sigma \rightarrow \Sigma, (g, H) \mapsto gH = gHg^{-1}.$$

若 $H \in \Sigma$ 所在的轨道 $\bar{H} = \{gHg^{-1} \mid g \in P'\}$, $|\bar{H}| = 1$. 则 $\bar{H} = \{H\} \therefore \forall g \in P'$,

$gHg^{-1} = H \therefore P' \subset N(H) \therefore P' = H$. 但 $P' \in \Sigma'$, $H \in \Sigma$, 矛盾.

P' 作用于 Σ 每个轨道的阶不为 1. $|\Sigma| \equiv 0 \pmod{p}$. 矛盾. 故 $\Pi = \Sigma$.

而对 $H \leq G, |H| = p^d \therefore H \times \Pi \rightarrow \Pi, (h, K) \mapsto hK = hKh^{-1}$. 由 $|\Pi| \equiv 1 \pmod{p}$,

$\exists H \ni p^d$. 故 H 作用于 Π 一定有阶数为 1 的轨道. $\bar{P}, |\bar{P}| = 1$.

$$\bar{P} = {}^H P = \{hPh^{-1} \mid h \in H\} = \{P\} \therefore H \subset N(P).$$

Prop. 3. $\alpha \in S_n, S_n \times S_n \rightarrow S_n, (\beta, \alpha) \mapsto {}^\beta \alpha = \beta \alpha \beta^{-1}$. 若 $\alpha = (i_1 \dots i_s)(j_1 \dots j_t) \dots (l_1 \dots l_u)$. 则 $\beta \alpha \beta^{-1} = (\beta(i_1) \dots \beta(i_s))(\beta(j_1) \dots \beta(j_t)) \dots (\beta(l_1) \dots \beta(l_u))$
 $\alpha \sim \gamma$ iff. $\gamma = \beta \alpha \beta^{-1}, \beta \in S_n$.

↗
↙

No.

Date.

$$\alpha = (i_1 \dots i_{s_1})(j_1 \dots j_{s_2}) \cdots (l_1 \dots l_{s_k}), \quad s_1 \geq s_2 \geq \cdots \geq s_k, \quad s_1 + \cdots + s_k = n.$$

$$\text{Def'}. \quad \alpha = (i_1 \dots i_{n_1})(j_1 \dots j_{n_2}) \cdots (l_1 \dots l_{n_k}) \cdots$$

$$n_1 = n_2 = \cdots = n_{g_1} > n_{g_1+1} = \cdots = n_{g_1+g_2} > n_{g_1+g_2+1} = \cdots$$

$$n_1 + \cdots + n_g = n.$$

$$\left(\prod_{i=1}^g n_i\right) \left(\prod_{j=1}^k g_j!\right)$$

P83-84

11. $|G| = p^m$, p a prime, ~~n~~ the number of subgroups of G with order p^k . S the set of subsets of G of cardinality p^k .

$$G \times S \rightarrow S, (g, A) \mapsto g \cdot A = gA$$

$$\text{If } A \in S, H_A = \text{stab } A = \{g \in G \mid gA = A\} \leq G.$$

$$H_A \times A \rightarrow A, (h, a) \mapsto ha \in A.$$

$$A = \bigcup \bar{a}_i, |A| = \sum |\bar{a}_i| \quad \bar{a}_i = H_A \cdot a_i \quad A = \bigcup H_A \cdot a_i \quad |H_A| \cdot \# \text{orbits} = |A| = p^k.$$

$$\therefore |H_A| \mid p^k$$

$$12. \quad S_0 = \{A \in S \mid |H_A| = p^k\}, \quad \bar{S}_0 = \{A \in S \mid |H_A| < p^k\}, \quad B \in \bar{S}_0, \quad gB \in \bar{S}_0.$$

$$A \in S_0, \quad gA \in S_0, \quad g \in G. \quad H_{gB} = \{g' \in G \mid g'gB = gB\} = \{g' \in G \mid g^{-1}g'gB = B\}.$$

$$g^{-1} H_{gB} g = H_B$$

$$G \times \bar{S}_0 \rightarrow \bar{S}_0, (g, B) \mapsto gB$$

$$B \in \bar{S}_0, \quad \bar{B} = \bigcap_{g \in G} \{gB \mid g \in G\} \quad |\bar{B}| = [G : \text{stab } B] = [G : H_B] = |G| / |H_B|$$

由 \bar{S}_0 定义, $|H_B| < p^k$.

$$|S| - |S_0| \equiv |S - S_0| = |\bar{S}_0| = |\bigcup \bar{B}_i| \equiv 0 \pmod{p^m}$$

对 $R, +, \cdot, \bar{\cdot}, 1 \neq 0$, 若

1) $(R, +, 0)$ 为交换群

2) $(R, \cdot, 1)$ 为幺半群

3) $\forall a, b, c \in R, a \cdot (b+c) = ab+ac, (a+b) \cdot c = ac+bc$

则称 $(R, +, \cdot, 0, 1)$ 为环 (ring). $(R, +, 0)$ 称为 R 的加群, $(R, \cdot, 1)$ 称为 R 的乘法幺半群

设 $(R, +, \cdot, 0, 1)$ 为环, S 为 R 的非空子集, 若 S 对 R 中 $+,\cdot$ 构成一个环, 则称 S 为 R 的子环 (subring).

设 $(R, +, \cdot, 0, 1)$ 为环, $\emptyset \neq S \subseteq R$, 则 S 为 R 的子环 iff.

① $\forall a, b \in S, a-b \in S$

$$\Leftrightarrow \begin{cases} \forall a, b \in S, a+b \in S, \text{ 且} \\ \forall a \in S, -a \in S \end{cases}$$

② $\forall a, b \in S, ab \in S$

③ $1 \in S$

分配律由于在 R 上的而在 S 上自然成立.

$$\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

$$(a+b\sqrt{2}) - (c+d\sqrt{2}) = (a-c) + (b-d)\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

...

$$\Rightarrow \mathbb{Z}[\sqrt{2}] \leq (R, +, \cdot, 0, 1)$$

而且, $\mathbb{Q} \leq R$

$$\mathbb{Z}[\sqrt{-1}] = \{a+b\sqrt{-1} \mid a, b \in \mathbb{Z}\} \leq (R, +, \cdot, 0, 1)$$

$$(a+b\sqrt{-1})(c+d\sqrt{-1}) = (ac-bd)+(ad+bc)\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$$

$\mathbb{Z}[\sqrt{-1}]$: 高斯整数环.

No.

Date.

$[0,1]$ 上所有实连续函数 $f: [0,1] \rightarrow \mathbb{R}$ 关于 $f+g, f \cdot g \in$ 构成环。

$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\} \xrightarrow{\text{写作}} \{0, 1, \dots, n-1\}$, $x+y = x+y \bmod n, \forall x, y \in \mathbb{Z}_n$,

$x \cdot y = x \cdot y \bmod n$, $-x = n-x$, 则 $\mathbb{Z}_n \bmod n$ 的运算构成环。

设 $(R, +, \cdot, 0, 1)$ 为环, 则

$$\textcircled{1} \quad \forall a \in R, 0 \cdot a + 0 \cdot a = (0+0) \cdot a = 0 \cdot a \quad \cancel{0 \cdot a = 0}$$

$$0 \cdot a + 0 \cdot a + (-0 \cdot a) = 0 \cdot a + (-0 \cdot a)$$

$$0 \cdot a = 0.$$

$$\textcircled{2} \quad \forall a, b \in R, -(ab) = (-a)b = a(-b), \text{ 因为}$$

$$ab + (-a)b = (a+(-a))b = 0 \cdot b = 0 \Rightarrow (-a)b = -ab$$

$$\textcircled{3} \quad \forall a, b, c, d \in R, (a+b)(c+d) = ac+ad+bc+bd; \text{ 因为}$$

$$(a+b)(c+d) = (a+b)c + (a+b)d = ac+bc+ad+bd.$$

$$\textcircled{4} \quad \text{一般地, } \forall a_i, b_j \in R, 1 \leq i \leq m, 1 \leq j \leq n.$$

$$(a_1+a_2+\dots+a_m)(b_1+b_2+\dots+b_n) = \sum_{i=1}^m \sum_{j=1}^n a_i b_j$$

$$\textcircled{5} \quad (a+b)^2 = (a+b)(a+b) = a^2 + ab + ba + b^2 \quad \text{而且, 当 } ab = ba, (a+b)^2 = a^2 + 2ab + b^2.$$

$$\text{更一般地, 当 } ab = ba, (a+b)^n = a^n + C_n^1 a^{n-1} b + C_n^2 a^{n-2} b^2 + \dots + b^n$$

$$\therefore (a+b)^n = a^n + \sum_{k=1}^n [C_n^{k-1} a^{n-k} b + C_n^k a^{n-k} b^2 + \dots + C_n^{n-1} a b^{n-1} + C_n^n b^n]$$

$$C = \{f \mid f \text{ 为 } \mathbb{R} \text{ 上的连续函数}\}, \quad f+g: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto f(x) + g(x), \quad 0: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto 0.$$

$$f \cdot g: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto f(g(x)), \quad 1: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto x$$

$$\text{分配律: } f, g, h \in C, (f \circ (g+h))(x) = f((g+h)(x)) = f(g(x) + h(x)). \text{ 打不成}$$

$$f(g(x)) + f(h(x)) \quad (\text{另举反例}) \quad \text{这不是环.}$$

对环 $(R, +, \cdot, 0, 1)$.

对其乘法幺半群 $(R, \cdot, 1)$.

① 若 $\forall a, b \in R$, $ab = ba$, 则称 R 为交换环.

② 记 $R^* = R - \{0\}$. 若 $(R^*, \cdot, 1)$ 为 $(R, \cdot, 1)$ 的子幺半群, 则称 $(R, +, \cdot, 0, 1)$ 为整环 (domain). 整环 $\Leftrightarrow \forall a, b \in R^*$, $ab \in R^*$. 即非零元相乘仍非零.

$[0, 1] \rightarrow R$ 的所有连续函数之环也前节之例者不是整环.

$$f(x) = \begin{cases} 0, & 0 \leq x \leq \frac{1}{2}, \\ x - \frac{1}{2}, & \frac{1}{2} \leq x \leq 1. \end{cases} \quad g(x) = \begin{cases} x - \frac{1}{2}, & 0 \leq x \leq \frac{1}{2}, \\ 0, & \frac{1}{2} \leq x \leq 1. \end{cases} \quad f(x)g(x) = 0.$$

设 $(R, +, \cdot, 0, 1)$ 为环, $a \in R$, 若存在 $b \neq 0$, s.t. $ab = 0$, 则称 a 为 b 的左零因子.

若 $ba = 0$, 则 a 为 b 的右零因子 (left/right zero divisor).

零元总非零因子. R 整环 且 每个非零元都不是零因子.

$\forall a, b, c \in R$, $a \neq 0$, 若 $(ab = ac \Rightarrow b = c)$, 则称 R 满足左消去律.

$(bba = ca \Rightarrow b = c)$, 右.

如果 R 满足左和右消去律, 称 R 满足消去律.

R 是整环 iff. R 满足消去律.

" \Rightarrow ": 若 $ab = ac$, 则 $ab - ac = a(b - c) = 0$. 必选 $b - c = 0$, $b = c$. 否则 $a \neq 0$ 有零因子.

" \Leftarrow ": R 满足消去律, 那么 $\forall a, b \in R^*$. 若 $ab = 0$, 则 $ab = a \cdot 0 \Rightarrow b = 0$. 矛盾.

③ 若 $(R^*, \cdot, 1)$ 为群, 则称 $(R, +, \cdot, 0, 1)$ 为除环 (division group).

④ 若 $(R^*, \cdot, 1)$ 为交换群, 则称 $(R, +, \cdot, 0, 1)$ 为域 (field).

No.

Date.

$$\{a+bi+cj+dk \mid a, b, c, d \in \mathbb{R}\}, i^2=j^2=k^2=-1, ij=k=-ji, jk=i=-kj, ki=j=-ik$$

按正常的+, · 构成非交换的除环.

任何有限的整环都是除环.

$R^* = \{b_1, b_2, \dots, b_n\}$. 若 $a \in R^*$, ab_i, ab_j 对 $a \in R^*$. 则 $\{ab_1, \dots, ab_n\} \subseteq R^*$. 否则, $abi=abj$, 由整环消去, $b_i=b_j$. 矛盾. 而 $i \in R^*$. 故 $\exists i$, $abi=1$. $a^{-1}=b_i$.

这个证明对无限情形不可用. 因为即使 $\{ab_1, ab_2, \dots\}$ 与 $\{b_1, b_2, \dots\}$ 基数相同, 前者仍可能为后者的子集.

$(R, +, \cdot, 0, 1)$ 为环.

$$M_n(R) = \left\{ A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \mid a_{ij} \in R, 1 \leq i, j \leq n \right\}$$

$$= \{(a_{ij})_{n \times n} \mid a_{ij} \in R\}$$

$$(a_{ij})_{n \times n} + (b_{ij})_{n \times n} = (a_{ij} + b_{ij})_{n \times n}, \quad 0 = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}.$$

$$(a_{ij})_{n \times n} \cdot (b_{ij})_{n \times n} = (c_{ij})_{n \times n}, \quad c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}, \quad \text{+} \quad \cancel{\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}}. \quad 1 = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

构成环(未说交换).

环上的n阶对角矩阵 $\text{diag}(a_1, \dots, a_n) = \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix}$ 所有n阶对角矩阵 $M_n(R)$ 的子环

$$\begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix} = \begin{pmatrix} a_1 b_{11} & a_1 b_{12} & \cdots & a_1 b_{1n} \\ a_2 b_{21} & a_2 b_{22} & \cdots & a_2 b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_n b_{n1} & a_n b_{n2} & \cdots & a_n b_{nn} \end{pmatrix}$$

流量矩阵. $\text{diag}(a, \dots, a) = \begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}$ 也构成子环.

环同态: ~~映射~~ $\varphi: R \rightarrow R_2$ 之满足

$$1) \quad \varphi(a+b) = \varphi(a) + \varphi(b), \quad \forall a, b \in R \quad (\text{加群的同态})$$

$$2) \quad \varphi(ab) = \varphi(a)\varphi(b), \quad \forall a, b \in R. \quad \} \quad (\text{乘法么半群的同态})$$

$$3) \quad \varphi(1) = 1_{R_2}$$

者称作 环 R_1 到环 R_2 的同态.

$\varphi: R \rightarrow M_n(R), \quad a \mapsto \begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix}$ 是环的单同态.

将 R 看作 $M_n(R)$ 的子环. $a \in R$ 看作 $\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix} \in M_n(R)$. 写作 $\begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix} = a$.

$$a \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} = \begin{pmatrix} a & & & \\ & a & & \\ & & \ddots & \\ & & & a \end{pmatrix} \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}$$

No. _____

Date. _____

设 R 为交换环. (自此之后在本节中)

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, \text{ 定义 } |A| = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = \sum_{i_1, i_2, \dots, i_n} Sg(\alpha) \rightarrow a_{1i_1} a_{2i_2} \cdots a_{ni_n}, \alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

交换行列式之两行、值变为原来的负元.

余子式 (cofactor)

$$A_{ij} = (-1)^{i+j} \begin{vmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2j} & \cdots & a_{2n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn} \end{vmatrix}$$

$$\begin{aligned} |A| &= \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = a_{11} A_{11} + a_{12} A_{12} + \cdots + a_{1n} A_{1n} \quad \text{按行展开} \\ &= a_{1j} A_{1j} + a_{2j} A_{2j} + \cdots + a_{nj} A_{nj} \quad \text{按列展开.} \end{aligned}$$

$$\sum_{k=1}^n a_{ik} A_{jk} = \begin{cases} |A|, & i=j, \\ 0, & i \neq j. \end{cases} \quad \sum_{k=1}^n a_{ki} A_{kj} = \begin{cases} |A|, & i=j, \\ 0, & i \neq j. \end{cases}$$

上述证明与线性代数中相同.

$$\text{对 } A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}. \text{ 定义 伴随矩阵 } adj(A) = \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix}$$

$$A \cdot adj(A) = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix} = \begin{pmatrix} |A| & & & \\ & |A| & & \\ & & \ddots & \\ & & & |A| \end{pmatrix} = |A| \cdot adj(A) \cdot A.$$

$$|A_{nxn} B_{nxn}| = |A| |B|.$$

$A = (a_{ij})_{nxn}$, 若存在 $B = (b_{ij})_{nxn}$ s.t. $AB = BA = I$ 则称 A 为可逆的. 记 $B = A^{-1}$.

$A = (a_{ij})_{n \times n}$, 若 A 可逆, 则 $\exists B = (b_{ij})_{n \times n}$, s.t. $AB = BA = I$.

$$|AB| = 1 = 1, |A||B| = 1.$$

$$|BA| = 1 = 1 = |B||A|.$$

$\therefore |A|$ 在 R 为可逆元, 不仅是 $|A| = 0$ (!).

反过来, 设 $|A|$ 为 R 上可逆元, 则 $A^{-1} = \text{adj}(A) / |A|$.

$$A \cdot |A|^{-1} \text{adj}(A) = |A|^{-1} \cdot A \cdot \text{adj}(A) = |A|^{-1}|A| = 1. \text{ 同样, } |A|^{-1} \text{adj}(A) \cdot A = 1.$$

若 $A \in M_n(F)$, F 为域, 由 F 上每个非零元可逆, A 可逆 iff. $|A| \neq 0$

No.

Date.

四元数 Quaternions

第一个非交换除环.

$$Q = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

$$i^2 = j^2 = k^2 = ijk = -1 \Rightarrow ij = k, jk = i, ki = j \quad (\text{两边同乘} \dots)$$

$$\cdots -ji, \cdots -kj, \cdots -ik$$

从矩阵环三角底考虑

$$\overline{a+bi} = a - bi, \quad \overline{-x} = -\bar{x}$$

$$M_2(\mathbb{C}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mid \alpha, \beta, \gamma, \delta \in \mathbb{C} \right\}, \quad H = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C} \right\}$$

$$\forall \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}, \begin{pmatrix} \delta & \gamma \\ -\bar{\gamma} & \bar{\delta} \end{pmatrix} \in H, \quad \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \cdot \begin{pmatrix} \delta & \gamma \\ -\bar{\gamma} & \bar{\delta} \end{pmatrix} = \begin{pmatrix} \alpha - \delta & \beta - \gamma \\ -\bar{\beta} + \bar{\delta} & \bar{\alpha} - \bar{\gamma} \end{pmatrix}$$

$$= \begin{pmatrix} \alpha - \delta & \beta - \gamma \\ -(\beta - \gamma) & \alpha - \delta \end{pmatrix}$$

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \begin{pmatrix} \delta & \gamma \\ -\bar{\gamma} & \bar{\delta} \end{pmatrix} = \begin{pmatrix} \alpha\delta - \beta\bar{\gamma} & \alpha\gamma + \beta\bar{\delta} \\ -\bar{\beta}\delta - \bar{\alpha}\bar{\gamma} & -\bar{\beta}\gamma + \bar{\alpha}\bar{\delta} \end{pmatrix} = \begin{pmatrix} \alpha\delta - \beta\bar{\gamma} & \alpha\gamma + \beta\bar{\delta} \\ -\bar{\alpha}\gamma + \bar{\beta}\bar{\delta} & \bar{\alpha}\bar{\delta} - \bar{\beta}\bar{\gamma} \end{pmatrix}$$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H.$$

$\therefore H$ 是 $M_2(\mathbb{C})$ 的子环.

$$\left| \begin{array}{cc} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{array} \right| = \alpha\bar{\alpha} + \beta\bar{\beta} = |\alpha|^2 + |\beta|^2 \neq 0$$

$\therefore \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}$ 可逆 iff. $\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \neq 0$.

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}^{-1} = (|\alpha|^2 + |\beta|^2)^{-1} \begin{pmatrix} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{pmatrix}$$

$$\text{在 } M_2(\mathbb{C}) \text{ 中记 } \mathbf{i} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & \sqrt{-1} \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{i}, \mathbf{j}, \mathbf{k} \in H$$

如此的 i, j, k 滿足四元數的定义中对 i, j, k 的要求。

$$\forall \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \vee \begin{pmatrix} a+b\sqrt{-1} & c+d\sqrt{-1} \\ -c+d\sqrt{-1} & a-b\sqrt{-1} \end{pmatrix} \in H, a, b, c, d \in \mathbb{R},$$

$$\begin{pmatrix} a+b\sqrt{-1} & c+d\sqrt{-1} \\ -c+d\sqrt{-1} & a-b\sqrt{-1} \end{pmatrix} = a + b \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} + c \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix} = a+bi+cj+dk.$$

D100. 1. $x = a_0 + a_1 i + a_2 j + a_3 k, a_0, a_1, a_2, a_3 \in \mathbb{R}$.

$$\bar{x} = a_0 - a_1 i - a_2 j - a_3 k, \forall x, y \in H, \bar{x+y} = \bar{x} + \bar{y}, \bar{xy} = \bar{x} \bar{y} \bar{x}, x = \bar{x} \Leftrightarrow x \in \mathbb{R}$$

1) 單位

$$2) x = \begin{pmatrix} a_0 + a_1 \sqrt{-1} & a_2 + a_3 \sqrt{-1} \\ -a_2 + a_3 \sqrt{-1} & a_0 - a_1 \sqrt{-1} \end{pmatrix}, y = \begin{pmatrix} b_0 + b_1 \sqrt{-1} & b_2 + b_3 \sqrt{-1} \\ -b_2 + b_3 \sqrt{-1} & b_0 - b_1 \sqrt{-1} \end{pmatrix}$$

$$xy = \left(\begin{array}{cc} \dots & \dots \\ \dots & \dots \end{array} \right)$$

$$\bar{y}x = \left(\begin{array}{cc} \dots & \dots \\ \dots & \dots \end{array} \right)$$

2. 定义 $|x|^2 = N(x) = x\bar{x} = a_0^2 + a_1^2 + a_2^2 + a_3^2$. 证 $N(xy) = N(x)N(y)$

$$x^2 - 2a_0x + N(x) = 0$$

No.

Date.

设 $(R, +, \cdot, 0, 1)$ 为环, 三为 R 上等价关系, 且保持 ~~相等~~ $+, \cdot$ 运算. 即若 $a \equiv b, c \equiv d$, 则 $a+c \equiv b+d, ac \equiv bd$. 则称 三为环 R 上同余关系.

二元

例. 对于 $(\mathbb{Z}, +, \cdot, 0, 1)$, $n \in \mathbb{N}^*$, 在 \mathbb{Z} 上定义同余关系 三. $\forall a, b \in \mathbb{Z}, a \equiv b$ iff. $n | (a-b)$, $a \equiv b \pmod{n}$. 若 $a \equiv b \pmod{n}, c \equiv d \pmod{n}$, 则 $n | (a-b) \wedge n | (c-d)$, $a+c \equiv b+d \pmod{n}, ac \equiv bd \pmod{n}$.

命題和定理

三为环 R 上的同余关系. 则 三为 $(R, +, 0)$ 上的同余关系. $\bar{0} = \{a \in R \mid a \equiv 0\}$ 为 $(R, +, 0)$ 上的正规子群. $\forall a \in R, b \in \bar{0}, a \equiv a, b \equiv 0$. 又三保持乘法. $\therefore ab \equiv a \cdot 0, ab \equiv 0, ba \equiv 0, a=0, ba \in \bar{0}$.

I 为 $(R, +, 0)$ 的子群. 即 $\forall a \in R, b \in I$, 均有 $ab \in I, ba \in I$. 则称 I 为 R 的理想 (Ideal). $\bar{0}$ 是 R 的理想.

$$ab^{-1} \in I \Leftrightarrow R.$$

反之. 设 I 为 R 的理想. 在 R 上定义二元关系 三, $\forall a, b \in R, a \equiv b$ iff. $a-b \in I$.

则 三为 $(R, +, 0)$ 的同余关系. 若 $a \equiv b, c \equiv d$: 即 $a-b \in I, c-d \in I, ac-bd = ac-ad+ad-bd = a(c-d)+(a-b)d$. 由理想定义. $(c-d) \in I \Rightarrow a(c-d) \in I$, $a-b \in I \Rightarrow (a-b)d \in I$. 故 $ac-bd \in I$.

1. 设 三为 R 上的同余关系. 则 $\bar{0} = \{a \in R \mid a \equiv 0\}$ 为 R 的理想.

2. 设 I 为 R 的理想. 在 R 上定义二元关系 三, $\forall a, b \in R, a \equiv b$ iff. $a-b \in I$. 则 三为 R 上的同余关系.

i. ① $\bar{0}$ 为 $(R, +, 0)$ 的正规子群

$$\text{② } \forall a \in R, b \in \bar{0}, b \equiv 0, a \equiv a. \therefore ba \equiv 0a = 0, ab \equiv a0 = 0, ba, ab \in \bar{0}.$$

设 三为 R 上的同余关系. $\because \bar{0}$ 为 R 上的理想. 利用理想 $\bar{0}$ 在 R 上定义同余关系 三.

No. _____

Date. _____

$\forall a, b \in R$: $a \equiv b \Leftrightarrow a-b \in \bar{0} \Leftrightarrow a-b \equiv 0 \Leftrightarrow a \equiv b$. (反过来也易证)

由此，理想和同余关系互逆地对应一个由子群的正规子群和同余关系)

设 $(R, +, \cdot, 0, 1)$ 为环，三为 R 的同余关系。要证此两概念有关系：

$$R/\equiv = \{\bar{a} \mid a \in R\}, \bar{a} + \bar{b} = \bar{a+b}, \bar{a} \cdot \bar{b} = \bar{ab}, \bar{a}(\bar{b} + \bar{c}) = \bar{a}\bar{b} + \bar{a}\bar{c} = \bar{a}(b+c)$$

$$= \bar{ab+ac} = \bar{ab} + \bar{ac} = \bar{a}\bar{b} + \bar{a}\bar{c}$$

$(R/\equiv, +, \cdot, \bar{0}, \bar{1})$ 为环。

$$\bar{a} = a + \bar{0}; \bar{a} + \bar{b} = a + b - a + \bar{0} = a + \bar{b} = \bar{a+b}$$

$$\forall b \in \bar{a}, a \equiv b \Leftrightarrow 0 \equiv b-a \Leftrightarrow b-a \in \bar{0} \Leftrightarrow b \in a + \bar{0} = \bar{a}$$

$$\forall b \in a + \bar{0}, b = a + k, k \in \bar{0} \Leftrightarrow b = a + 0 = a$$

设 R 为环，三为 R 的同余关系。 $R/\equiv = \{\bar{a} \mid a \in R\}$ 。 $(R/\equiv, +, \cdot, \bar{0}, \bar{1})$ 称为 R 关于三的商环。 $\bar{I} = \bar{0}$ ， $R/\bar{I} = \{a + \bar{I} \mid a \in R\}$ 。 $(a + \bar{I}) + (b + \bar{I}) = a + b + \bar{I}$ ， $(a + \bar{I})(b + \bar{I}) = ab + \bar{I}$ 。

设 R 为环， $S \subset R$ ，由 S 生成的子环 $\langle S \rangle$ 为所有包含 S 的 R 的子环的交。

$$S = \{a_1, \dots, a_n\} \subset R, \langle S \rangle = \{0, 1, \text{所有关于 } a_1, \dots, a_n \text{ 的多项式}\}$$

记作 (S) \nearrow 所有理想之交

由 S 生成的理想，它含 S 的最小微理想，对理想 I, J ， $I \cap J$ 也是理想。

$I + J = \{a+b \mid a \in I, b \in J\}$ 是包含 $I \cup J$ 的最小微理想。

$$\text{若 } S = \{a_1, \dots, a_n\}, (a_1, \dots, a_n) = \bigcap_{x_i, y_i \in R} \{ \sum_{i=1}^n x_i^{(1)} a_1 y_i^{(1)} + \sum_{i=1}^n x_i^{(2)} a_2 y_i^{(2)} + \dots + \sum_{i=1}^n x_i^{(n)} a_n y_i^{(n)} \}$$

若 R 为交换环。 $(a_1, \dots, a_n) = \{x_1 a_1 + \dots + x_n a_n \mid x_1, \dots, x_n \in R\}$

一个元素生成的理想 $\langle a \rangle$ 称为主理想。

若环的任一理想都为主理想，则该环称为主理想环。

No.

Date.

P

除环的理想只有 $\{0\}$ 和它本身. 因为, 若 $I \neq R$, $I \neq \{0\}$, $a \in I$, $a \neq 0$, 则 $ba^{-1} \in I$.
 $\forall x \in R$, $x = x \cdot 1 \in I$.

Th 2.2. 设 R 是交换环, 则 R 为域 iff. R 只有两个理想 $\{0\}, R$.
"⇒": 显然.

"⇐": 只要证 R 为除环. 任取 $a \in R, a \neq 0$, 则 $\langle a \rangle = R$. 附图 $| \in \langle a \rangle = R$.

又 $\langle a \rangle = \{xa \mid x \in R\}$, 故 $1 = a'a^{-1} \in \langle a \rangle$, $a' \in R$, 即 a' 为 R 的逆元. $\therefore R^*$ 是群.

对 $(\mathbb{Z}, +, \cdot, 0, 1)$, $\mathbb{Z} = \langle 1 \rangle$, $\langle 1 \rangle$ 为 \mathbb{Z} 的子群, 其子群为 $\langle k \rangle = \{nk \mid n \in \mathbb{Z}\}$.

设 I 为 \mathbb{Z} 的一个理想. I 为 $(\mathbb{Z}, +, 0)$ 的子群. $I = \langle k \rangle = \{nk \mid n \in \mathbb{Z}\}$.

反之若 I 为 $(\mathbb{Z}, +, 0)$ 的子群. $\because I = \langle k \rangle = \{nk \mid n \in \mathbb{Z}\}$ 是 \mathbb{Z} 的理想.

$$\textcircled{1} \quad \langle k \rangle \subset \langle l \rangle \Leftrightarrow l \mid k.$$

$$\textcircled{2} \quad m, n \in \mathbb{Z} \quad (\text{即 } \langle m \rangle + \langle n \rangle = \langle d \rangle), \quad d = (m, n). \quad \because \text{因为 } (m, n) = 1,$$

$$\langle m \rangle \subseteq d \Rightarrow d \mid m, \quad \langle n \rangle \subseteq d \Rightarrow d \mid n.$$

另外, 若 $h \mid m, h \mid n$. 由 $d \in \langle m \rangle + \langle n \rangle$, $d = mx + ny$, $x, y \in \mathbb{Z}$ 则一定 $b \mid d$.

$\mathbb{Z}/\langle k \rangle = \{\bar{0}, \dots, \bar{k-1}\}$, $\bar{i} = \{i + nk \mid n \in \mathbb{Z}\}$. 若 k 为合数, 则 $\mathbb{Z}/\langle k \rangle$ 不是整环, 因为 $\bar{x}\bar{y} = \bar{0}$. 有零因子! 而若 k 为素数, $\mathbb{Z}/\langle k \rangle$ 是域. 对 $\bar{a} \in \mathbb{Z}/\langle k \rangle$, $\bar{a} \neq \bar{0}$, 即 $k \nmid a$. $\because k \nmid a$. $\because k$ 为素数. $\therefore (a, k) = 1$. $1 = ax + ky$, $x, y \in \mathbb{Z}$. $\therefore \bar{a}^{-1} = \bar{x}$

$$\begin{aligned} \bar{a}\bar{x} + \bar{k}\bar{y} &= \bar{a}\bar{x} + \bar{0} = \bar{a}\bar{x} = \bar{x}\bar{a} \\ \therefore \bar{a}^{-1} &= \bar{x} \end{aligned}$$

对环 R , $V(R) = \{a \in R \mid a \text{ 为 } R \text{ (对 } F \text{ 来说的) 可逆元}\}$.

No.

Date.

$$\cup(\mathbb{Z}/\langle k \rangle) = \{\bar{a} \mid 0 \leq a \leq k-1, (a, k) = 1\}, \text{ 因为:}$$

设 $(a, k) = 1$. 则 $1 = ax + ky, x, y \in \mathbb{Z}$. $\bar{k} = \bar{0}$. 故 $\bar{1} = \bar{ax+ky} = \bar{ax} + \bar{ky} = \bar{a}\bar{x} + \bar{0} = \bar{a}\bar{x}$

反过来. 设 \bar{a} 为 $\mathbb{Z}/\langle k \rangle$ 的可逆元. 则 $\exists \bar{x} \in \mathbb{Z}/\langle k \rangle$ s.t. $\bar{a}\bar{x} = \bar{1}$. $\therefore ax - 1 = ky$

$\therefore ax + ky = 1$. 即: 若 $d | a$ 且 $d | k$ 则 $d | 1$. 即 $(a, k) = 1$.

故 $\mathbb{Z}/\langle k \rangle$ 的可逆元素是 \bar{a} , a 与 k 互素

$$k > 1. \varphi(k) = |\{a \in \mathbb{Z}_+ \mid 1 \leq a \leq k, (a, k) = 1\}|. \text{ 欧拉函数}$$

$$\varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \varphi(7) = 6, \varphi(8) = 4, \dots$$

p 为素数时. $\varphi(p) = p-1$, $\varphi(p^n) = |\{p, 2p, 3p, \dots, (p^{n-1}-1)p \text{ (因为 } p \nmid sp^n)\}| = p^n(1-\frac{1}{p})$

$$n \in \mathbb{Z}_+, \varphi(n) = ?:$$

若 $n, m \in \mathbb{Z}_+, (m, n) = 1$, 则 $\varphi(mn) = \varphi(m)\varphi(n)$

$n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, p_1, \dots, p_s 为互不相同的素数.

$$\varphi(n) = \varphi(p_1^{k_1}) \cdots \varphi(p_s^{k_s}) = p_1^{k_1}(1 - \frac{1}{p_1}) \cdots p_s^{k_s}(1 - \frac{1}{p_s}) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_s})$$

$$|\cup(\mathbb{Z}/\langle k \rangle)| = \varphi(k)$$

若 $(a, k) = 1$ 则 $\bar{a} \in \cup(\mathbb{Z}/\langle k \rangle)$. 又 $|\cup(\mathbb{Z}/\langle k \rangle)| = \varphi(k)$, $\bar{a}^{\varphi(k)} = \bar{1}$. $\therefore a^{\varphi(k)} \equiv 1 \pmod{k}$

\Rightarrow 当 $(a, k) = 1$ 时, $a^{\varphi(k)} \equiv 1 \pmod{k}$, $k \nmid (a^{\varphi(k)} - 1)$

特别地, 当 p 为素数, $(a, p) = 1$, $a^{p-1} \equiv 1 \pmod{p}$

No.

Date.

设 $(R, +, 0, \cdot, 1)$, $(R', +, 0, \cdot, 1')$ 为环.

若 $\varphi: R \rightarrow R'$ 满足 $\forall a, b \in R$,

$$1) \varphi(a+b) = \varphi(a) + \varphi(b)$$

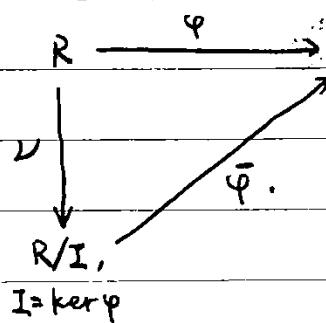
$$2) \varphi(ab) = \varphi(a)\varphi(b)$$

$$3) \varphi(1) = 1'$$

则称 φ 为 R 到 R' 的环同态 (既是加群的同态, 又是乘法幺半群的同态).

在 R 上定义二元关系 \equiv : $\forall a, b \in R$, $a \equiv b \Leftrightarrow \varphi(a) = \varphi(b)$. 易知 \equiv 为 R 上的同余关系.

三对应的理想 $\bar{0} = \{a \in R \mid a \equiv 0\} = \{a \in R \mid \varphi(a) = 0'\}$. $\varphi^{-1}(0') = \ker \varphi$.



$\forall: R \rightarrow R/I$, $a \mapsto a+I = \bar{a}$. 则一定存在唯一的同态 $\bar{\varphi}: R/I \rightarrow R'$, st. $\varphi = \bar{\varphi} \circ u$, 且 $\bar{\varphi}$ 为单同态.

由于 $\varphi(a) = (\bar{\varphi} \circ u)(a) = \bar{\varphi}(a+I) = \bar{\varphi}(\bar{a})$. 故如下定义:

$$\bar{\varphi}: R/I \rightarrow R', \quad \bar{a} = a+I \mapsto \varphi(a).$$

1) 若 $\bar{a} = \bar{b}$, $\therefore \varphi(a) = \varphi(b)$, $\therefore \bar{\varphi}(\bar{a}) = \bar{\varphi}(\bar{b})$. $\bar{\varphi}$ 是映射.

$$2) \bar{\varphi}(\bar{a+b}) = \bar{\varphi}(\bar{a+b}) = \varphi(a+b) = \varphi(a) + \varphi(b) = \bar{\varphi}(\bar{a}) + \bar{\varphi}(\bar{b})$$

$$3) \bar{\varphi}(\bar{a}\bar{b}) = \bar{\varphi}(\bar{ab}) = \varphi(ab) = \varphi(a)\varphi(b) = \bar{\varphi}(\bar{a})\bar{\varphi}(\bar{b}).$$

$$4) \bar{\varphi}(\bar{1}) = \varphi(1) = 1'. \quad \text{若 } \bar{\varphi} \text{ 是同态, 则且唯一.}$$

若 $\varphi: R \rightarrow R'$ 是环同态. $I = \ker \varphi = \{a \in R \mid \varphi(a) = 0'\} \trianglelefteq R$, $K \trianglelefteq R \Rightarrow K \subset I$. 则对下图

$$\begin{array}{ccc}
 R & \xrightarrow{\varphi} & R' \\
 \downarrow & \nearrow \bar{\varphi} & \\
 L: R \rightarrow R/K, & & \\
 a \mapsto \bar{a} = a + K & & \\
 R/K & &
 \end{array}$$

$\bar{\varphi}: R/K \rightarrow R'$, $a+K \mapsto \varphi(a)$ 是同态.

单同态 $\Leftrightarrow K=I$.

对 $H' \leq R/K$, 用令

设 R 为环, $K \trianglelefteq R$ 为 R 的理想. 则

$H = \bigcup H'$, 是证 $H/K = H'$

设 $\{H | H \trianglelefteq R, K \trianglelefteq H\} \rightarrow \{R/K\}$ 的所有子环}, $H \mapsto H/K$ 是双射.

且 $H \trianglelefteq R \Leftrightarrow H/K \trianglelefteq R/K$.

进一步. 当 $H \trianglelefteq R$, 由 $R \rightarrow \frac{R}{K} \rightarrow \frac{R/K}{H/K}$.

$$\frac{R}{H} \cong \frac{R/K}{H/K}.$$

设 R 为环, $K \trianglelefteq R$, $H \trianglelefteq R$ (子环).

$\varphi: H \rightarrow (H+K)/K$, $h \mapsto h+K = \bar{h}$ 是同态.

$$\ker \varphi = \varphi^{-1}(0+K) = H \cap K.$$

$$H/H \cap K \cong (H+K)/K.$$

$(R, +, \cdot, 0, 1)$ 的最小子环; $\langle 1 \rangle = \{n \cdot 1 | n \in \mathbb{Z}\}$. 称为素环.

No.

Date.

设 D' 为除环, $D \subseteq D'$, D 为 D' 的子环, 则 D 是整环(无零因子).

反过来, 给定整环 D , 是否存在一个除环 D' , 使 D 为 D' 的子环.

即, 是否存在单射 $\eta: D \rightarrow D'$, 是单同态 (不成立, 见习题).

给定一个交换的整环, 一定存在一个域 F , 使得 D 为 F 的子环.

设 F' 为域, D 为 F' 子环, 则 D 是交换的整环.

问: 由 D 生成的域是什么 (包含 D 的最小的子域, 所有包含 D 的子域之交)

$$F = \{ab^{-1} \mid a, b \in D, b \neq 0\} \subseteq F'$$

即: $(ab^{-1})(cd^{-1}) = ab^{-1}cd^{-1} \in F$, $a, b, c, d \in D$, $b, d \neq 0$.

$$1) ab^{-1} + cd^{-1} = (ad + bc)(bd)^{-1} \in F. \text{ 加法封闭}$$

$$2) -ab^{-1} \rightarrow (ab^{-1}) = (-a)b^{-1} \in F. \text{ 负元封闭.}$$

$$3) (ab^{-1})(cd^{-1}) = (ac)(bd)^{-1} \in F. \text{ 乘法封闭.}$$

$$4) \forall ab^{-1} \in F, ab^{-1} \neq 0, (ab^{-1})^{-1} = ba^{-1} \in F. \text{ 逆元封闭.}$$

所以 F 是 F' 的包含 D 的子域.

而且, 对任何 F' 的子域 F'' , $F'' \supseteq D$, 那么 $\forall a, b \in D, b \neq 0, ab^{-1} \in F''$,

$ab^{-1} \in F''$. 所以 $F'' \supseteq F$. \square

给定一个交换的整环 D , ab^{-1} 这样的表示不唯一, 对 $ab^{-1}, cd^{-1} \in F$, $ab^{-1} = cd^{-1} \iff ad = bc$.

给定一个交换的整环 D , $D^* = D - \{0\}$, $D \times D^* = \{(a, b) \mid a \in D, b \in D^*\}$.

在 $D \times D^*$ 中定义关系 \sim : $(a, b) \sim (c, d) \iff ad = bc$. 则 \sim 为 $D \times D^*$ 的等价关系.

$$1) (a, b) \sim (a, b), 2) \text{若 } (a, b) \sim (c, d), \text{ 则 } (c, d) \sim (a, b).$$

$$3) \text{若 } (a, b) \sim (c, d), (c, d) \sim (e, f), \text{ 则 } ad = bc, cf = de \iff af = be. (a, b) \sim (e, f).$$

$$D \times D^* / \sim = \{[(a, b)] \mid a, b \in D, b \neq 0\}, [(a, b)] = \{(c, d) \in D \times D^* \mid (a, b) \sim (c, d)\}.$$

No.

Date.

都是等价类。

记 $D \times D^*/\sim = \{ \frac{a}{b} \mid a, b \in D, b \neq 0 \}$. 在 $D \times D^*/\sim$ 中定义 +, \cdot 及 $\bar{1}$.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

若 $\frac{a}{b} = \frac{a'}{b'}, \frac{c}{d} = \frac{c'}{d'}$, 则 $(\overline{a}, \overline{b}) = (\overline{a'}, \overline{b'})$, $ab' = ba'$, $cd' = dc'$

$$\begin{aligned} & \cancel{\frac{ad+bc}{bd}} = ad'b'd' + bc'b'd' = ba'dd' + dc'bb' \\ & (a'd' + b'c')bd = a'd'bd + b'c'bd = a'd'bd + b'c'bd. \end{aligned}$$

$$\therefore \frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}. \text{ 即 } \frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}, + \text{ 运算. (唯一性 - 确定).}$$

交换律结合律易证成立。

$$0 = \frac{0}{b}, b \in D, b \neq 0.$$

$$-\frac{a}{b} = \frac{-a}{b}, \text{ 因为 } \frac{a}{b} + \frac{-a}{b} = \frac{ab+b(-a)}{b} = \frac{0}{b} = 0.$$

而且也验证 $D \times D^*/\sim$ 的非零元对·构成群. $1 = \frac{b}{b}, b \in D, b \neq 0, (\frac{a}{b})^{-1} = \frac{b}{a}$
以及分配律成立.综上, $(D \times D^*/\sim, +, \cdot, 0, 1)$ 为域. $0 = \frac{0}{b}, b \neq 0, 1 = \frac{b}{b}, b \neq 0$. $\eta: D \rightarrow D \times D^*/\sim, a \mapsto \overline{(a, 1)} = \frac{a}{1}$. $\forall a, b \in D$. 若 $\eta(a) = \eta(b)$, 则 $\frac{a}{1} = \frac{b}{1}$, $a \cdot 1 = b \cdot 1$. $a = b$. 是单射.可证保持 +. 故 η 是单同态. 于是可以将 D 视作 $D \times D^*/\sim$ 的子环.给定一个交换的整环 D , 一定存在域 F , s.t. D 为 F 的子域.

$$D \times D^*/\sim = \{ \overline{(a, b)} \mid a, b \in D, b \neq 0 \} = \left\{ \frac{a}{b} \mid a, b \in D, b \neq 0 \right\} \quad \frac{b}{1}^{-1} = \left(\frac{b}{1} \right)^{-1} = \frac{1}{b}.$$

也就是 $F = \{ ab^{-1} \mid a, b \in D, b \neq 0 \}$. 称为 D 的分式域 (the field of fractions of D) \mathbb{Q} 是 \mathbb{Z} 的分式域.Th 2.9. Let D be a commutative domain, F its field of fractions. Then any monomorphism η_0 of D into a field F' has a unique extension to a

monomorphism of η_F of F into F' : $\eta_F(a) = \eta_D(a)$, $\eta_F(ab^{-1}) = \eta_D(ab)^{-1}$

$\eta_D: D \rightarrow F'$. 单同态. $\eta_F: F \rightarrow F'$. 单同态, s.t. $\eta_F|_D = \eta_D$.

定义 $\eta_F: F \rightarrow F'$; $ab^{-1} \mapsto \eta_D(a)\eta_D(b)^{-1}$

1) 若 $ab^{-1} = cd^{-1} \in F$, $\therefore ad = bc \therefore \eta_D(ad) = \eta_D(bc) \therefore \eta_D(a)\eta_D(d) = \eta_D(b)\eta_D(c)$.

$\eta_D(a)\eta_D(b)^{-1} = \eta_D(c)\eta_D(d)^{-1} \therefore \eta_F(ab^{-1}) = \eta_F(cd^{-1})$. η_F 是映射.

2) 证明 η_F 是加法同态.

$$\begin{aligned} \eta_F(ab^{-1} + cd^{-1}) &= \eta_F((ad+bc)(bd)^{-1}) = \eta_D(ad+bc)\eta_D(bd)^{-1} \\ &= (\eta_D(a)\eta_D(d) + \eta_D(b)\eta_D(c))(\eta_D(b)\eta_D(d)^{-1}) = \eta_D(a)\eta_D(b)^{-1} + \eta_D(c)\eta_D(d)^{-1} \\ &= \eta_F(ab^{-1}) + \eta_F(cd^{-1}) \end{aligned}$$

同理 平乘. $\eta_F(ac \cdot bd^{-1}) = \eta_F(ac \cdot (bd)^{-1}) = \eta_D(ac)\eta_D(bd)^{-1}$

\vdots $\eta_D(a)\eta_D(c)\eta_D(b)^{-1}\eta_D(d)^{-1} = \eta_F(ab^{-1})\eta_F(cd^{-1})$

3) $\eta_F(a) = \eta_F(\frac{a}{1}) = \eta_F(a|^{-1}) = \eta_D(a)\eta_D(1)^{-1} = \eta_D(a)$. $\therefore \eta_F$ 是 η_D 的扩张.

4) 而且 若有 η'_F 亦是 $F \rightarrow F'$ 的单同态. 且 $\eta'_F|_D = \eta_D$. $\therefore F$ 是 D 生成的. $\eta'_F \in \eta_F$

在 D 上像相等. 则 $\eta'_F = \eta_F$ 证 $\eta_F = \eta'_F$. $\eta'_F|_D = \eta_D = \eta_F|_D$

由于 F 是 D 生成的. $\therefore \eta'_F = \eta_F$.

5) $\eta_F(ab^{-1}) = \eta_F(cd^{-1}) \Rightarrow \eta_D(a)\eta_D(b)^{-1} = \eta_D(c)\eta_D(d)^{-1} \Rightarrow \eta_D(a)\eta_D(d) = \eta_D(c)\eta_D(b) \Rightarrow$
 $\eta_D(ad) = \eta_D(bc) \Rightarrow ad = bc \Rightarrow ab^{-1} = cd^{-1}$.

从而 η_F 是单同态.

P118. 1. 域的分式域是它本身.

4. D 为交換整环. $a, b \in D$. $a^m = b^n$, $a^n = b^m$, $n, m \in \mathbb{Z}^+$; $(n, m) = 1$.

$| \Rightarrow mx + ny$. $x, y \in \mathbb{Z}$. 在 $F = D \times D^\times$ 上, $a = a^{mx+ny} = (a^m)^x(a^n)^y = (b^n)^x(b^m)^y = b^{nx+ny} = b$.

No.

Date.

从此往后之书中，所有环^环默认为交换环。

R, R' 为交换环， $R \leq R'$, $U \in R'$. 问在 R' 中，包含 R 和 U 的最小子环 $\langle R, U \rangle$ 。
记为 $R[U]$.

若 $R \leq R'$, $U, V \subset R'$, 则显然 $R[UUV] = R[U][V]$.

设 $R \leq U = \{u_1, u_2, \dots, u_s\}$, $\therefore R[U] = \langle R[u_1, \dots, u_s] \rangle = R[\overbrace{u_1, \dots, u_s}]$

设 $R \leq R'$, $U \in R'$, $\{R[U] = \{a_0 + a_1u_1 + a_2u_2 + \dots + a_nu_n \mid a_i \in R, 0 \leq i \leq n, n \geq 0\}$

$$\sum_{i=0}^n a_i u^i + \sum_{j=0}^m b_j u^j = \sum_{i=0}^n (a_i + b_i) u^i. \text{ 都写成 } n. \text{ 因为若 } n \neq m, \text{ 互补零即可。}$$

$$\left(\sum_{i=0}^n a_i u^i \right) \left(\sum_{j=0}^m b_j u^j \right) = \sum_{k=0}^{m+n} c_k u^k, \quad c_k = \sum_{i+j=k} a_i b_j, \quad 0 \leq k \leq m+n; \quad \text{加。集封闭}$$

这种 $R[U]$ 中元素的表示法并不唯一。何时 $\sum_{i=0}^n a_i u^i = \sum_{j=0}^m b_j u^j$?

R 为交换环。 x 为未定元 (indeterminate), 设定 $x^0 = 1$, $0 \cdot x = 0$.

$$R[x] = \{a_0 + a_1x + \dots + a_nx^n \mid a_i \in R, 0 \leq i \leq n, n \geq 0\}$$

$$= \left\{ \sum_{i=0}^n a_i x^i \mid a_i \in R, 0 \leq i \leq n, n \geq 0 \right\}. \quad (\text{只是形式表达式}, x \text{ 未记号})$$

$$\text{定义相等: } \sum_{i=0}^n a_i x^i = \sum_{j=0}^m b_j x^j \text{ iff. } m=n, a_i = b_i, 0 \leq i \leq n.$$

$$\text{定义加法: } \sum_{i=0}^n a_i x^i + \sum_{j=0}^m b_j x^j = \sum_{i=0}^n (a_i + b_i) x^i$$

$$\text{定义乘法: } \left(\sum_{i=0}^n a_i x^i \right) \left(\sum_{j=0}^m b_j x^j \right) = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) x^k$$

可知形式 $R[x]$ 关于以上运算构成交换环。

$R[x]$ 也可看作 $R \times R \times \dots \times R \times \dots = \{(a_0, a_1, a_2, \dots, a_n, \dots) \mid a_i \in R, a_0, a_1, \dots, \text{中只有有限个非零元}\}. (a_0, a_1, \dots) = (b_0, b_1, \dots) \text{ iff. } a_i = b_i, i = 0, 1, 2, \dots$

$$\text{且: } (a_0, a_1, \dots, a_n, \dots) + (b_0, b_1, \dots, b_n, \dots) = (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, \dots)$$

No.

Date.

乘: $(a_0, a_1, a_2, \dots)(b_0, b_1, b_2, \dots) = (c_0, c_1, c_2, \dots)$, $c_k = \sum_{i+j=k} a_i b_j$

$$(a_0, a_1, a_2, \dots)(b_0, b_1, b_2, \dots) = (c_0, c_1, c_2, \dots), c_k = \sum_{i+j=k} a_i b_j$$

有至多 $m+n$ 个非零元

$\eta: R \rightarrow R \times R \times \dots$, $a \mapsto (a, 0, 0, \dots, 0, \dots)$ 则

$$\text{Var} \in R, \eta(a+b) = (a+b, 0, 0, \dots) = (a, 0, 0, \dots) + (b, 0, 0, \dots) = \eta(a) + \eta(b)$$

$$\eta(ab) = (ab, 0, 0, \dots) = (a, 0, 0, \dots)(b, 0, 0, \dots) = \eta(a)\eta(b)$$

$\eta(1) = (1, 0, 0, \dots)$ 为 $R \times R \times \dots$ 中单位元

故 η 是单同态. 可看作 $R \subseteq R \times R \times \dots$

在 $R \times R \times \dots$ 上, $R \subseteq R \times R \times \dots$: $\forall a \in R, a = (a, 0, 0, \dots)$

令 $x = (0, 1, 0, 0, \dots)$. 则 $x^2 = (0, 0, 1, 0, 0, \dots)$, $x^3 = (0, 0, 0, 1, 0, 0, \dots)$, \dots
位: 0, 1, ..., n-1

$$x^n = (\underbrace{0, \dots, 0}_{n-1}, 1, 0, 0, \dots)$$

这样, $(a_0, a_1, a_2, \dots) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots$

这样, $(a_0, a_1, a_2, \dots) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots$

Th 2.10. R, S 为环. $\eta: R \rightarrow S$ 为同态. $\eta \in S$: 则 η 可以唯一地扩张为 $\eta_u: R[x] \rightarrow S$ 的同态, s.t. $\eta_u|_R = \eta$, $\eta_u(x) = u$.

证明: 令 $\eta_u(\sum_{i=0}^n a_i x^i) = \sum_{i=0}^n \eta(a_i) u^i$ 令 $\eta_u: R \rightarrow S$, $\sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n \eta(a_i) u^i$.

若 $\sum_{i=0}^n a_i x^i = \sum_{i=0}^m b_i x^i$, 则 $a_i = b_i$, os is m. 故 $\eta_u(\sum_{i=0}^n a_i x^i) = \eta_u(\sum_{i=0}^m b_i x^i)$, 故 η_u 是映射.

$$\eta_u\left(\sum_{i=0}^n a_i x^i + \sum_{j=0}^m b_j x^j\right) = \eta_u\left(\sum_{i=0}^n (a_i + b_i) x^i\right) = \sum_{i=0}^n (a_i + b_i) u^i = \sum_{i=0}^n a_i u^i + \sum_{i=0}^n b_i u^i = \eta_u\left(\sum_{i=0}^n a_i x^i\right) + \eta_u\left(\sum_{j=0}^m b_j x^j\right).$$

$$\eta_u\left(\left(\sum_{i=0}^n a_i x^i\right) \left(\sum_{j=0}^m b_j x^j\right)\right) = \eta_u\left(\sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j\right) x^k\right) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j\right) u^k = \left(\sum_{i=0}^n a_i u^i\right) \left(\sum_{j=0}^m b_j u^j\right)$$

$$= \eta_u\left(\sum_{i=0}^n a_i x^i\right) \eta_u\left(\sum_{j=0}^m b_j x^j\right). \text{故 } \eta_u \text{ 是同态.}$$

No. _____

Date. _____

$$\forall a \in R, \eta_u(a) = \eta(a). \quad \text{且 } \eta_u|_R = \eta.$$

$$\text{而 } \eta_u(x) = \eta(1) \cdot u = u.$$

$R[x]$ 由 R, x 生成. 又 η_u 为同态, 故 R, x 的像既已确定, 同态也唯一确定.

$$R \leq S, u \in S, \eta: R \rightarrow S, a \mapsto a.$$

$$\text{则 } \eta_u: R[x] \xrightarrow{R[u] \leq S} \sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n a_i u^i.$$

$$\text{Im } \eta_u = \text{Im } (\eta) = \left\{ \eta\left(\sum_{i=0}^n a_i x^i\right) \mid a_i \in R, 0 \leq i \leq n, n \geq 0 \right\}.$$

$$= \left\{ \sum_{i=0}^n a_i u^i \mid a_i \in R, 0 \leq i \leq n, n \geq 0 \right\} = R[u].$$

$$\ker \eta = \left\{ \sum_{i=0}^n a_i x^i \mid \eta\left(\sum_{i=0}^n a_i x^i\right) = 0 \right\} = \left\{ \sum_{i=0}^n a_i x^i \mid \sum_{i=0}^n a_i u^i = 0 \right\} = I, \text{ 为理想}.$$

当 $\ker \eta = \{0\}$, $R[x] \cong R[u]$. 称 u 为 R 上超越元.

当 $\ker \eta \neq \{0\}$: 称 u 为 R 上代数元.

对一般情形. 由于 $\eta: R[x] \rightarrow R[u] \leq S$ 为满同态 ($\text{Im } \eta = R[u]$).

$$R[x]/I \cong R[u].$$

$$\Rightarrow \ker \eta = \{0\}, \text{ 即 } u \text{ 为超越元时. } R[x] \cong R[u], \sum_{i=0}^n a_i u^i = \sum_{i=0}^n b_i u^i \text{ iff. } a_i = b_i, \forall i \in \mathbb{N}.$$

$$\text{当 } \ker \eta = I \neq \{0\}, \sum_{i=0}^n a_i u^i - \sum_{i=0}^n b_i u^i \in I \Leftrightarrow \sum_{i=0}^n a_i x^i - \sum_{i=0}^n b_i x^i \in I.$$

$$\text{由 } \eta(a) = a, \forall a \in R, \text{ 知 } I \cap R = \{0\}.$$

Corollary. $R[u] \cong R[x]/I$, where x is an indeterminate and I is an ideal in $R[x]$ s.t. $I \cap R = 0$.

Th. 2.11. R, S 为交换环, $\eta: R \rightarrow S$ 为同态, $u_1, u_2, \dots, u_n \in S$. 则存在唯一同态

$$\eta_{u_1, \dots, u_n}: R[x_1, \dots, x_n] \rightarrow S, \text{ s.t. } \forall a \in R, \eta_{u_1, \dots, u_n}(a) = \eta(a); \eta_{u_1, \dots, u_n}(x_i) = u_i.$$

由 $R[x_1, \dots, x_n] = R[x_1] \cdots [x_n]$, 一↑个↑步↑加↑.

$$\eta_{u_1}: R[\oplus x_1] \rightarrow S, \forall a \in R, \eta_{u_1}(a) = a; \eta_{u_1}(x_1) = u_1;$$

No.

Date.

$$\eta_{univ} : R[x_1, \dots, x_n] \rightarrow S, \quad \eta_{univ}|_{R[x_i]} = \eta_{u_i}, \quad \eta_{univ}(x_i) = u_i.$$

$$\eta_{univ_1, \dots, u_n} : R[x_1, \dots, x_n] \rightarrow S$$

x_1, \dots, x_n 的添加顺序没有关系.

Theorem 2.12. $\nexists f : R[x_1, \dots, x_n] \in R[x_1, \dots, x_n], \sum_{i_1, i_2, \dots, i_n} a_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} = 0$ iff:

$$a_{i_1, i_2, \dots, i_n} = 0 \quad \forall i_1, i_2, \dots, i_n.$$

用归纳法. 若对 $n-1$ 成立, 则对 n .

$$\sum_{i_1, i_2, \dots, i_n} a_{i_1, i_2, \dots, i_n} x_1^{i_1} \dots x_{n-1}^{i_{n-1}} x_n^{i_n} = f_0(x_1, \dots, x_{n-1}) + f_1(x_1, \dots, x_{n-1}) x_n + \dots + f_n(x_1, \dots, x_{n-1}) x_n^n = 0.$$

$$\Rightarrow f_0(x_1, \dots, x_{n-1}) = 0.$$

$R \leq S, u_1, \dots, u_n \in S$.

$$\eta_{univ} : R[x_1, \dots, x_n] \rightarrow S, g \mapsto g \in R, x_i \mapsto u_i, (s) \in S.$$

$$\ker \eta_{univ} = I = \{0\} : \text{代数无关.}$$

$$\ker \eta_{univ} = I \neq \{0\}.$$

$f(x) \in R[x]$, $f(x) = a_0 + a_1 x + \dots + a_n x^n$, $a_n \neq 0$.

degree of $f(x)$: $\deg(f(x))$

$\deg(f(x)) = n$, a_n the leading coefficient of $f(x)$.

$\deg(a) = 0$, $a \in R$, $a \neq 0$.

$\deg(0) = \deg(1) = -\infty$. $f(x) = \sum_{i=0}^n a_i x^i$, $g(x) = \sum_{j=0}^m b_j x^j$.

$\deg(f(x) + g(x)) \leq \max\{\deg(f(x)), \deg(g(x))\}$. 前项可能相消.

$\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$, 当 R 为整环 (无零因子)

≤ 否则.

若 R 为整环, 则 $R[x]$ 为整环. 则若 $f(x)g(x) = 1$, $\deg(f(x)) + \deg(g(x)) = 0$.

因此 $R[x]$ 上可逆元只有 R 上的可逆元. 于是得到:

Th 2.13 若 D 为整环, 则 $D[x_1, \dots, x_n]$ 也为整环; 且 $D[x_1, \dots, x_n]$ 的可逆元均为 D 中的可逆元.

Th 2.14

$f(x), g(x) \in R[x]$, $f(x) = a_0 + a_1 x + \dots + a_n x^n$, $g(x) = b_0 + b_1 x + \dots + b_m x^m$, $b_m \neq 0$.

则一定存在 R $k \in N$, $q(x), r(x) \in R$, s.t. $b_m^k f(x) = q(x)g(x) + r(x)$, $\deg(r(x)) < \deg(g(x))$

证. 当 $\deg(f(x)) < \deg(g(x))$, $f(x) = 0 \cdot g(x) + f(x)$

当 $\deg(f(x)) \geq \deg(g(x))$, $b_m f(x) - a_n x^{n-m} g(x) = f(x)$. $\deg(f(x)) < \deg(f(x))$.

前项: $a_n b_m x^n$. $a_n b_m x^n$.

$\therefore b_m f(x) = a_n x^{n-m} g(x) + f(x)$. 由归纳假设 $b_m^k f(x) = g f_1(x)g(x) + r_1(x)$, $\deg(r_1(x)) < \deg(g(x))$

$\therefore b_m^k f(x) = a_n x^{n-m} g(x) + f_1(x)g(x) + r_1(x) = (a_n x^{n-m} f_1(x))g(x)$

$b_m^{k+1} f(x) = (a_n b_m x^{n-m} + f_1(x))g(x) + r_1(x)$.

当 $R = F$ 为域. $f(x) = g(x)g(x) + r(x)$, $\deg(r(x)) < \deg(g(x))$. 若另外还有

No.

Date.

$$f(x) = g_1(x)g(x) + r_1(x), \deg r_1(x) < \deg g(x).$$

(Pm) $(g(x) - g_1(x))g(x) = r_1(x) - r(x)$. F 为域. $F[x]$ 无零因子.

~~由~~ (ii) $\deg(r_1(x) - r(x)) \leq \deg g(x)$. 故必有 $g(x) - g_1(x) = 0$.

否则 $\deg \text{LHS} > \deg \text{RHS}$. $\therefore g(x) = g_1(x)$, $\therefore r_1(x) = r(x)$.

由 $f(x)$ 对超环 D , F 为其分式域

$$b_m^{-k} f(x) = g(x)g(x) + r(x), \deg r(x) < \deg g(x).$$

$$b_m^{-k} f(x) = g_1(x)g(x) + r_1(x), \deg r_1(x) < \deg g(x).$$

故在 F 上, $f(x) = b_m^{-k} g_1(x)g(x) + b_m^{-k} r(x)$.

$$f(x) = b_m^{-k_1} g_1(x)g(x) + b_m^{-k_1} r_1(x).$$

$$b_m^{-k} g(x) = b_m^{-k_1} g_1(x), \quad b_m^{-k} r(x) = b_m^{-k_1} r_1(x).$$

$$\Rightarrow g(x) = b_m^{k-k_1} g_1(x), \quad r(x) = b_m^{k-k_1} r_1(x).$$

Cor 1 If $f(x) \in R[x]$ and $a \in R$, then there exists a unique $g(x) \in R[x]$

s.t. $f(x) = (x-a)g(x) + f(a)$ ~~且~~

$$f(x) = (x-a)g(x) + r(x), \deg r(x) < \deg(x-a) = 1. \quad \text{用同余定理(代入),}$$

$$f(a) = (a-a)g(a) + r(a). \quad f(a) = r(a)$$

$$\therefore f(x) = (x-a)g(x) + f(a) = (x-a)g_1(x) + f(a).$$

$$\therefore (x-a)g(x) = (x-a)g_1(x). \quad (x-a)(g(x) - g_1(x)) = 0.$$

且系数不全为 0.

$$\Rightarrow g(x) = g_1(x).$$

Cor 2. $(x-a) | f(x)$ iff $f(a) = 0$. $(x-a) | f(x) : f(x) = (x-a)g(x)$

$R = F$ 域. $F[x] - f(x), g(x) \neq 0 \in F[x]$. $f(x) = g(x)g(x) + r(x)$. $\deg r(x) < \deg g(x)$.

设 F 为域, 则 $F[x]$ 一定为主理想整环。

证. 设 $I \trianglelefteq F[x]$

① $I = \{0\}$. 则 $I = (0)$.

② 若 $I \neq \{0\}$. 又 $g(x)$ 为 I 中次数最低的非零元. 则 $I = (g(x))$:

$\forall f(x) \in I$, $f(x) = g(x)g(x) + r(x)$, $\deg r(x) < g(x)$.

$\therefore r(x) = f(x) - g(x)g(x) \in I$. 所以 $r(x) = 0$ (由 $g(x)$ 为最低次项).

↓ 理想对称、左乘封闭.

$\therefore g(x) | f(x)$. $I = (g(x))$.

但 $F[x][y]$ 一定不是主理想.

$I = \{f(x) \in F[x_1] \cdots [x_n] \mid f(x_1) \text{ 要么为 } 0, \text{ 要么有因式 } 0\}$

若 $I = (a)$. a 一定为某多项式 $g(x)$, $\deg g(x) \geq 1$ (含常数项).

$g(x) | x_1, g(x) | x_2 \cdots$ 不可能.

No.

Date.

$R \leq S, u \in S, R[u] = \{\sum_{i=0}^n a_i u^i \mid a_i \in R\}$.

F 为域, $F \leq S, u \in S, F[u] = \{\sum_{i=0}^n a_i u^i \mid a_i \in F\}$: S 是交换环

$\varphi: F[x] \rightarrow F[u] \leq S, a \mapsto a, \forall a \in F, x \mapsto u$.

$\ker \varphi = (g(x))$, $g(x) \in F[x]$.

$\{f(x) \in F[x] \mid f(u)=0\}$

$g(x)$ 满足: 1) $g(u)=0$, 2) 若 $f(u)=0$, $\exists g(x) | f(x)$.

$g(x)$ 是使 $g(u)=0$ 的次数最低的多项式.

$f(x) \in F[x], f(x)$ 称为不可约多项式, 若 $f(x) \neq h(x)g(x), \deg h > 0, \deg g > 0$.

① $\ker \varphi = (g(x)) = \{0\}$ 时, u 为超越元, $F[x] \cong F[u]$

② 当 $g(x) \neq 0, g(x)$ 为不可约多项式, $F[x]/(g(x)) \cong F[u]$

$\overline{f(x)} \in F[x]/(g(x)), \overline{f(x)} \neq \overline{0}, \Rightarrow f(x) \notin (g(x)). (\overline{f(x)}, \overline{g(x)}) = 1$.

$f(x)h(x) + g(x)k(x) = 1, \overline{f(x)h(x)} + \overline{g(x)k(x)} = \overline{1} \Rightarrow \overline{f(x)h(x)} = \overline{1}$.

故 $F[x]/(g(x))$ 是域.

其他证法: 若 $I \trianglelefteq F[x]/(g(x)), I \neq 0$. 则 $\exists J, J \trianglelefteq F[x], J \supset (g(x))$,

s.t. $I = J/(g(x))$. J 也是主理想, $J = (f(x))$. $\exists f(x) = J \supset (g(x))$.

$g(x) \in (f(x)) \therefore g(x) = f(x)h(x), f(x) \in F^*$. 只能是常数 (g 不可约).

$\Rightarrow J = F[x]/(g(x))$. $F[x]/(g(x))$ 只有两个理想: 0 和本身. 故为域.

③ 当 $g(x) \neq 0$ 为可约多项式, 则 $F[x]/(g(x))$ 不是整环

$\epsilon F[x]$ 在 $F[x]$ 上
这样的 $g(x)$ 称为 u 的极小多项式. 若 S 为域, 则 极小多项式不可约

若 F 为有限域, 则 $|F| = p^m$, p 为素数.

No.

Date.

构造 5^2 个元素的域:

$$\mathbb{Z}_5 = \mathbb{Z} / \langle 5 \rangle = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4} \}$$

$\mathbb{Z}_5[x]$ 中找一个 2 次不可约多项式: $g(x) = x^2 + x + 1$ 满足条件

5^3 个元素的域:

$$\mathbb{Z}_5[x] \text{ 中找 } 3 \text{ 次不可约多项式: } g(x) = x^3 + x + 1. \quad \mathbb{Z}_5 / \langle x^3 + x + 1 \rangle$$

No.

Date.

F为域.

当 $\text{char } F = p$, 其素子域 $\{0, 1, \dots, (p-1) \cdot 1\} \cong \mathbb{Z}_p$ 当 $\text{char } F = 0$, 其素子域 $\{0, 1, \dots\} = \{n \mid n \in \mathbb{Z}\} \cong \mathbb{Z}$.故其素子域为 $\{(n \cdot 1)(m \cdot 1)^{-1} \mid m, n \in \mathbb{Z}, m \neq 0\} \cong \mathbb{Q}$.

素子域称为F的素域.

F为域, 其素域为 $\mathbb{Z}_p' = \{0, 1, \dots, (p-1) \cdot 1\}$. F可看作 \mathbb{Z}_p' 上的线性空间 $F_{\mathbb{Z}_p'}$. $\dim F_{\mathbb{Z}_p'} = m$. 则有一组 F 在 \mathbb{Z}_p' 上的基 e_1, \dots, e_m , s.t. $F_{\mathbb{Z}_p'}$ 中任一元素 \Rightarrow 可写成 $x_1 e_1 + \dots + x_m e_m$, $x_i \in \mathbb{Z}_p$. 故 $|F| = p^m$.

有理

故: 对域 F, $\text{char } F = p \Rightarrow |F| = p^m$.在 $\mathbb{Z}_p[x]$ 找一个 m 次不可约多项式 g(x), 则 $\mathbb{Z}_p[x]/(g(x))$ 为域; 且:

$$|\mathbb{Z}_p[x]/(g(x))| = p^m$$

$$\mathbb{Z}_5[x]/(x^2+x+1)$$

$$a_0 + a_1 x = a_0 + a_1 x + (x^2 + x + 1), a_0, a_1 \in \mathbb{Z}_5.$$

都在 \mathbb{Z}_5 中算.

$$\text{求 } \overline{x+1}^{-1}: (x+1, x^2+x+1) = 1. 1 = \overline{(x+1)} h(x) + \overline{(x^2+x+1)} k(x).$$

$$x^2+x+1 = \overline{(x+1)} \cdot x + \overline{1}$$

$$x+1 = \overline{x+1} + \overline{1} \quad \overline{1} = \overline{x^2+x+1} - \overline{(x+1)x}$$

$$\Rightarrow 1 = (x^2+x+1) - (x+1)x \quad \wedge \quad \overline{x+1}^{-1} = \overline{-x} = \overline{4x}$$

$$\mathbb{Z}_5[x]/(x^2+x+1). \quad x^2+x+1 = (x+1)(x^2-x+2) + 4.$$

$$x+1 = 4(4(x+1)). \quad 4 = (x^2+x+1) - (x+1)(x^2-x+2). \quad 4^{-1} = 4.$$

$$1 = 4(x^2+x+1) - 4(x+1)(x^2-x+2). \quad \overline{x+1}^{-1} = \overline{x^2-x+2}$$

Th 2.17

$f(x) \in F[x]$, $\deg f(x) = n$, F field. Then $f(x)$

Let F be a finite field, then $F^* = F - \{0\}$ is a cyclic group (multiplication)

F^* 为交换群, F^* 循环闭, $\exp F^* = |F^*|$

在 $F[x]$ 上, $x^{\exp F^*} - 1 = 0$. F^* 每个元素都是 $x^{\exp F^*} - 1 = 0$ 的根.

$\therefore |F^*| \leq \exp F^*$.

$\forall a \in F^*, a^{|F^*|} = 1 \quad \therefore \exp F^* \leq |F^*|. \quad \therefore |F^*| = \exp F^*$

$|F^*| = n$, $a \in F^*$, $\sigma(a) = n$. 称 a 为 F 的本原元.

p 素数. $(a, p) = 1$, ① $a^{p-1} \equiv 1 \pmod{p}$.

$\bar{a} \in \mathbb{Z}_p^*$. $|\mathbb{Z}_p^*| = p-1$. $\bar{a}^{p-1} = \bar{1} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$.

p 素数. ② $(p-1)! \equiv -1 \pmod{p}$.

3 是 \mathbb{Z}_7^* 生成元: $3^1 = 3$, $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, $3^6 = 1$.

$\sigma(3) = 6$.

F 为域, S 为非空集合. 记 $F^S = \{f \mid f: S \rightarrow F\}$.

在 F^S 上定义 $+$, \cdot : $\forall f, g \in F^S$, $f + g: S \rightarrow F$,

$$\forall x \in S, (f+g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(x)g(x).$$

$\forall a \in F$, 定义 $\alpha: S \rightarrow F$, $x \mapsto a$. S 中任一元素映射到 F 的 a .

$$0 = 0_S: S \rightarrow F, \forall x \in S, 0_S(x) = 0.$$

$$1 = 1_S: S \rightarrow F, \forall x \in S, 1_S(x) = 1.$$

$(F, +, \cdot, 0, 1)$ 是交换环.

$\varphi: F \rightarrow F^S$, $a \mapsto a_S$. 是单同态. 故可认为 $F \leq F^S$. F 是 F^S 的子环.

当 $S = F$, $F^F = \{f \mid f: F \rightarrow F\}$. 恒等映射 $s: F \rightarrow F$, $a \mapsto a$.

$$F \leq F^F \quad F[S] = \left\{ \sum_{i=0}^n a_i s^i \mid a_i \in F, n \geq 0 \right\}, \quad \left(\sum_{i=0}^n a_i s^i \right)(b) = \sum_{i=0}^n a_i s^i(b) = \sum_{i=0}^n a_i b^i.$$

$\varphi: F[x] \rightarrow F[S] \leq F^F$, $a \mapsto a_S$, $\forall a \in F$; $x \mapsto s$ 同态.

则 φ 是单射 (而且 φ 一定满, 故为同构) 的充要条件是 F 是无限域.

1) 设 F 是无限域. 证 $\ker \varphi = 0$.

若存在 $f(x) \neq 0$, $f(s) = 0$. 设 $f(x) = a_0 + a_1 x + \dots + a_n x^n$. ($a_n \neq 0$).

$$a_0 + a_1 s + \dots + a_n s^n = 0. \quad \forall b \in F, (a_0 + a_1 s + \dots + a_n s^n)(b) = 0.$$

则 $a_0 + a_1 b + \dots + a_n b^n = 0$, $\forall b \in F$. 但在域中, n 次多项式只能有 n 个根.

而 F 无限, 所以不可能. 假设不成立, $\ker \varphi = 0$. φ 单.

2) 证若 φ 是单设. 反设 F 是有限域. $F = \{a_1, \dots, a_m\}$. $|F| = m$.

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_m) \in F[x].$$

$$\varphi(f(x)) = (s - a_1) \cdots (s - a_m)$$

$$\varphi(f(x))(x) = f(x) \quad \forall x \in S = \{a_1, \dots, a_m\}. \quad (a_1 - a_1) \cdots (a_m - a_1) = 0.$$

$\varphi(f(x)) = 0$. 这与 φ 是同构矛盾.

或者说, 若 F 有限, 则 F^F 有限, $F[S] \leq F^F$ 有限. 但 $F[x]$ 无限.

所以不可为同构.

当 F 有限, 求 $\ker \varphi$

记 $\underbrace{F[x] \dots x^r F}_{r+1} = F^{(r)}$. 未 $\dots F^{(r)} = \{f \mid f: F^{(r)} \rightarrow F\}$

$\Leftrightarrow s_i: F^{(r)} \rightarrow F, (a_1, \dots, a_i, \dots, a_r) \mapsto a_i$

$F[s_1, \dots, s_r] \leq F^{(r)}$ (因为 $F \leq F^{(r)}$, $s_i \in F^{(r)}$)

$\varphi: F[x_1, \dots, x_r] \rightarrow F[s_1, \dots, s_r], a \mapsto a, \forall a \in F, x_i \mapsto s_i, 0 \leq i \leq r$

$f(x_1, \dots, x_r) \in F[x_1, \dots, x_r]$. F 无限, $f(x_1, \dots, x_r) \neq 0$.

则 $\exists a_1, \dots, a_r \in F$, s.t. $f(a_1, \dots, a_r) \neq 0$.

① 当 $r=1$, 已证

② 假设 $r=k$ 时成立. $\vdash r=k+1$ NT.

$$f(x_1, \dots, x_k, x_{k+1}) = B_0 + B_1 x_{k+1} + \dots + B_m x_{k+1}^m \neq 0.$$

其中, B_0, \dots, B_m 是关于 x_1, \dots, x_k 的多项式.

$B_m \neq 0$, 则由归纳假设, $\exists a_1, \dots, a_k$, s.t. $B_m(a_1, \dots, a_k) \neq 0$.

代入 a_1, \dots, a_k , 再用一次 $r=1$ 的情况, 得到 a_{k+1} , s.t.

$$f(a_1, \dots, a_{k+1}) \neq 0.$$

则 $\ker \varphi = 0$. φ 是单的.

若 $|F|=q$. $\varphi: F[x] \rightarrow F[s], a \mapsto a, \forall a \in F, F[x] \mapsto s$

则 $\ker \varphi = (x^q - x)$.

证: $\varphi(x^q - x) = s^q - s = 0$ (因为 F^* 是循环群. $\Leftrightarrow b^q = b^{q-1} \cdot b = 1 \cdot b = b$)

而若 $f(x) \in \ker \varphi$, 则 $f(x) = (x^q - x)g(x) + r(x)$ - deg $r(x) < q$.

$$0 = f(s) = (s^q - s)g(s) + r(s) = r(s). \quad \text{则 } \forall b \in F, r(b) = 0, r(x) = 0. \text{ 否则}$$

不行有 q 个不同根. $f(x) = (x^q - x)g(x) \in (x^q - x)$.

No.

Date.

当 $|F| = q$, $\varphi: F[x_1, \dots, x_r] \rightarrow F[s_1, \dots, s_r] \cap \alpha \mapsto a, \forall a \in F, x_i \mapsto s_i, |s| \leq r$

$$\ker \varphi = (x_1^q - x_1, \dots, x_r^q - x_r)$$

证明方法类似于使用归纳法,

$f(x_1, \dots, x_r)$ 且每个 x_i 的指数 $x_i^{m_i}, m_i < q$.

列方程 $f(a_1, \dots, a_k, x_{k+1}) = B_0(a_1, \dots, a_k) + \dots + B_m(a_1, \dots, a_k) x_{k+1}^m \neq 0$,

$\dots \Rightarrow \exists a_1, \dots, a_k$ 使 $f(\dots) \neq 0$.

可知 $(x_1^q - x_1, \dots, x_r^q - x_r) \subset \ker \varphi$.

设 $f(x_1, \dots, x_r) \in \ker \varphi$

$$x_i^{k_i} = (x_i^q - x_i) g_i(x_i) + r_i(x_i) \deg r_i(x_i) < q$$

(于是把每个 x_i 的次数降至小于 q)

$$f(x_1, \dots, x_r) = \sum_{i=1}^r a_i x_i^{k_i} + f'(x_1, \dots, x_r)$$

$$\stackrel{+}{\oplus}$$

$$\nexists f'(x_1, \dots, x_r) = 0 \Rightarrow f(x_1, \dots, x_r) \in (x_1^q - x_1, \dots, x_r^q - x_r)$$

$$F[x_1, \dots, x_r] := \{f(x_1, \dots, x_r) \in F[x_1, \dots, x_r] \mid f \in F\}$$

双射 $\pi: \{1, \dots, r\} \rightarrow \{1, \dots, r\}$

$\overline{\text{def}}: \{\pi: F[x_1, \dots, x_r] \rightarrow F[x_1, \dots, x_r], a \mapsto a, a \in F, x_i \mapsto x_{\pi(i)}\}$

若 $\exists \pi(f(x_1, \dots, x_r)) = f(x_1, \dots, x_r), \forall \pi \in S_r$

则称 $f(x_1, \dots, x_r)$ 为对称多项式。

对称

初等多项式

$$\left\{ \begin{array}{l} p_1 = x_1 + x_2 + \dots + x_r = \sum_{i=1}^r x_i \\ p_2 = \sum_{1 \leq i < j \leq r} x_i x_j \\ \dots \\ p_r = x_1 x_2 \dots x_r \end{array} \right.$$

单项式 $a x_1^{k_1} \dots x_r^{k_r}$ 的次数: $k_1 + \dots + k_r$.

齐次多项式 $f(x_1, \dots, x_r) = \sum a_{k_1, \dots, k_r} x_1^{k_1} \dots x_r^{k_r}$, 每个单项式次数相同.

将对称多项式 f 写作齐次多项式之和.

$f(x_1, \dots, x_r) = f_1(x_1, \dots, x_r) + \dots + f_m(x_1, \dots, x_r)$. f_i 是齐 n_i 次多项式.

只要证齐次多项式可用 p_1, \dots, p_r 表示.

在齐次多项式中, 最高次项 $x_1^{k_1} \dots x_r^{k_r}, x_1^{k'_1} \dots x_r^{k'_r}$. $k_1 + \dots + k_r = k'_1 + \dots + k'_r$

若 $k_1 = k'_1, \dots, k_s = k'_s, k_{s+1} > k'_{s+1}$. 则称 $x_1^{k_1} \dots x_r^{k_r} \geq x_1^{k'_1} \dots x_r^{k'_r}$.

(为了证明之便而给齐次的单项式一个顺序). 如. $x_1^3 x_2^2 > x_1^2 x_2^2 x_3 > x_1 x_2^3 x_3 > x_2^3 x_3^2$

$M_1 = x_1^{k_1} \dots x_r^{k_r}, N_1 = x_1^{k'_1} \dots x_r^{k'_r}$. 若 $M_1 > N_1$, 则 $M_1 N_1 > N_1 N_1$. $N \neq 0$.

若 $M_1 > N_1, M_2 > N_2$, 则 $M_1 M_2 > N_1 N_2$.

任何一个齐次对称多项式可表示为齐次对称多项式的多项式。

设 $f(x_1, \dots, x_r)$ 为齐次对称多项式。

$a x_1^{k_1} \cdots x_r^{k_r}$ 是 $f(x_1, \dots, x_r)$ 中的一项。则 $a x_{\pi(1)}^{k_1} \cdots a x_{\pi(r)}^{k_r} = x_{\pi(1)}^{k_1} \cdots x_{\pi(r)}^{k_r}$ 也是其中一项。 $\pi \in S_r$ 。

若 $a x_1^{k_1} \cdots x_r^{k_r}$ 是 f 的最高次项，则 $k_1 \geq k_2 \geq \cdots \geq k_r$ 。

$p_1^{k_1} \cdots p_r^{k_r}, k_i \geq 0$ 为最高项是 $x_1^{k_1} (x_1 x_2)^{k_2} \cdots (x_1 \cdots x_r)^{k_r}$ 。（由齐次多项式无序）

$$= x_1^{k_1+k_2+\cdots+k_r} x_2^{k_2+k_3+\cdots+k_r} \cdots x_r^{k_r}$$

设 $f(x_1, \dots, x_r)$ 为齐次对称多项式， $a x_1^{k_1} \cdots x_r^{k_r}$ 为 f 的最高项。

则 $k_1 \geq k_2 \geq \cdots \geq k_r$ 。因为 $a p_1^{k_1-k_2} p_2^{k_2-k_3} \cdots p_r^{k_r-k_r} = p_r^{k_r}$ 为最高项。

为 $a x_1^{k_1} x_2^{k_2} \cdots x_r^{k_r}$ ，故 $f(x_1, \dots, x_r) - a p_1^{k_1-k_2} p_2^{k_2-k_3} \cdots p_r^{k_r}$ 仍为齐次对称多项式。

重复上述过程，则 $f(x_1, \dots, x_r)$ 可写成两个对称多项式之多项式。

若 $\sum_{d \in D} a_{d_1 d_2 \cdots d_r} p_1^{d_1} \cdots p_r^{d_r} = 0$ ，则 $a_{d_1 d_2 \cdots d_r} = 0, \forall (d)$ 。

$p_1^{d_1} \cdots p_r^{d_r}$ 与 $p_1^{d'_1} \cdots p_r^{d'_r}$ 最高次项一样。iff. $(d_1, \dots, d_r) = (d'_1, \dots, d'_r)$

$$x_1^{d_1+d_2+\cdots+d_r} x_2^{d_2+d_3+\cdots+d_r} \cdots x_r^{d_r} = x_1^{d'_1+d'_2+\cdots+d'_r} x_2^{d'_2+d'_3+\cdots+d'_r} \cdots x_r^{d'_r}$$

$$\begin{cases} d_1 + \cdots + d_r = d'_1 + \cdots + d'_r \\ d_2 + d_3 + \cdots + d_r = d'_2 + d'_3 + \cdots + d'_r \\ \vdots \\ d_r = d'_r \end{cases} \Leftrightarrow d_i = d'_i, 1 \leq i \leq r.$$

那么，对其最高项 $a p_1^{d_1} \cdots p_r^{d_r} x_1^{d_1+d_2+\cdots+d_r} \cdots x_r^{d_r} = 0 \Rightarrow a = 0$ 。

$f(x) \in R[p_1, \dots, p_r][x]$ ， x 是代数元。则 $\exists x_i : f(x_i) = 0$

$$x_1^3 + x_2^3 + x_3^3 + x_1 x_2 + x_1 x_3 + x_2 x_3$$

把 ~~$x_1^3 + x_2^3 + x_3^3 + x_1 x_2 + x_1 x_3 + x_2 x_3$~~ 写成 $p_1 = x_1 + x_2 + x_3, p_2 = x_1 x_2 + x_1 x_3 + x_2 x_3, p_3 = x_1 x_2 x_3$ 。

$(x_1^3 + x_2^3 + x_3^3)$ 最高项为 x_1^3 。 $x_1^3 + x_2^3 + x_3^3 - p_1^3$

已知 $a = p_1^{k_1} \cdots p_r^{k_r}$, p_i 互不相同且素数, $k_i > 0$.
 $= h_1^{k'_1} \cdots h_s^{k'_s}$, h_i 互不相同且互质, $k'_i > 0$.
 $\Leftrightarrow r = s$, $p_i \equiv h_i$; $k_i = k'_i$.

设 M 为域的满是消去律的半群. 那 $ab = ac \Rightarrow b = c$; $a, b, c \in M$.
若 $a = bc$, 则称 b 为 c 的一个因子. “ $b \mid a$ ”或 $b \mid a$. a 为 b 的一个倍数.

$U(M)$ 表示 M 中所有可逆元的集合. $U(M) = \{a \in M \mid \exists b \in M, ab = ba = 1\}$.

称 $U(M)$ 中的元素为单位.

$\forall a, b \in M$. 若 $a \mid b, b \mid c$, 则 $a \mid bc$; $b \mid ad$, $a \mid adc$. “由消去律, $cd = 1$.
 c, d 均为单位. 故有 $a \mid ub$. u 为单位.

反过来. 若 $a \mid ub$, u 为单位, 则 $a \mid b$ 且 $b \mid u$.

若 $a \mid ub$, $u \in U(M)$. 则称 a, b 为相伴元 (associates), 记为 $a \sim b$.

对 $a \in M$, $u \in U(M)$, $a = ua^{-1}a$. 单位是任何元的因子.

若 b 为 a 的相伴元, 则 b 也为 a 的因子. $b = ua$, $a = u^{-1}b$.

若 $a = bc$, b, c 都不是单位. 则称 b, c 为 a 的真因子 (proper factor).

$a \in M$. 若 a 无真因子, 则称 a 为不可约元.

$a \in M$, $a = p_1^{k_1} \cdots p_r^{k_r}$, $k_i > 0$. p_1, \dots, p_r 互不相同且不可约元.
 $= u_1 p_1^{k_1} u_2 p_2^{k_2} \cdots u_r p_r^{k_r}$. 基 $u_1 \cdots u_r = 1$. u_i 为单位

~~唯一分解性:~~

若 $a = p_1^{k_1} \cdots p_r^{k_r}$, $k_i > 0$. p_1, \dots, p_r 互不相同且不可约元.

$= h_1^{k'_1} \cdots h_s^{k'_s}$, $k'_i > 0$. h_1, \dots, h_s ~~互不相同且互质~~, $r = s$.

则称为唯一分解公半群.

$k_i = k'_i$
 $u_1 \cdots u_r = 1$, $u_i \in U(M)$

No.

Date.

~~若 M 为半群, $a \in U(M)$ 且有消去律, 而且若~~

$$a \cdot p_1 = p_1' \cdots p_k'$$

设 M 为唯一分解的么半群, $a \in M$, $a \notin U(M)$. $a = p_1 \cdots p_s$, p_i 为不可约元. 称 s 为 a 的长度 (length of a). 则一定满足:

Division chain condition. (因子链条件).

$a_1, a_2, \dots, a_n, \dots, a_{i+1}$ 为 a_i 的真因子, 则 a_1, \dots, a_n, \dots 是有限长的链

\Leftrightarrow 若有 $a_1, \dots, a_n, \dots, a_{i+1} | a_i$, 则一定存在 $N \in \mathbb{N}$, s.t. $a_n \sim a_{N+1} \sim a_{N+2} \sim \dots$

设 M 为唯一分解么半群, 则 M 一定满足因子链条件.

$a, b \in M$, b 为 a 之真因子, $a = bc$, $b, c \notin U(M)$.

$a = p_1 \cdots p_s$, $b = p_1' \cdots p_{s_1}'$, $c = p_1'' \cdots p_{s_2}''$; p_i, p_i' , p_i'' 为不可约元. $\Rightarrow a = p_1 \cdots p_s =$

$$p_1' \cdots p_{s_1}', p_1'' \cdots p_{s_2}'' \quad \therefore s = s_1 + s_2 \quad s \geq s_1$$

prime 素元: $p \in M$. 若 $p | ab$, 则 $p | a$ 或 $p | b$. 则称 p 为 M 的素元 (prime).

Prime Condition: M 的每个不可约元都是素元

设 M 为唯一分解的么半群, 则 M 一定满足素元条件.

证: p 为 M 之不可约元, $p | ab$. $a, b \in M$. 由 $a \in U(M)$, 且 $p | a$. 当 $b \in U(M)$, $p | b$,

当 $a, b \notin U(M)$, $\because a = p_1 \cdots p_s$, p_i 不可约, $b = p_1' \cdots p_t'$, p_i' 为不可约元. 所以:

$ab = p_1 \cdots p_s p_1' \cdots p_t'$. $\because p | ab$. $\therefore ab = p \cdot c$. (c 不是单位, 否则 p 能分解). 故 $c = q_1 \cdots q_m$.

q_i 不可约. $\therefore p \nmid p_1 p_1' \cdots p_t'$. $ab \nmid pc = p q_1 \cdots q_m$. 又 M 唯一分解. p 是 $p_1, p_1', p_2, p_2', \dots, p_s, p_t'$ 中某个. 故 p 是素元

注: M 未必交换, 消去法么半群. 若 M 满足因子链条件和素元条件, 则 M 唯一分解.

↓ ↓
素元 分解唯一

No.

Date.

因子链 \Rightarrow

$\forall a \in M, a \notin U(M)$. 则 a 一定有一个不可约元为 a 的因子. 即 $a = p_1 a_1$, p_1 不可约.
若 a 不可约, $a = a$. 若 a 不是不可约元, $a = bc$, $b, c \notin U(M)$. 若 b 不可约, 则 $a = b^2 c$,
 $p = b$ 为不可约元, 得证. 若 b 不是不可约元, $b = d e$, $d, e \in U(M)$.
这样立得. b 是 a 真因子. d 是 b 真因子. M 满足因子链条件. 故上述过程有限
步一定停止. 则一定有不可约元为 a 的因子. $a_1 = p_1 a_2$, p_1 不可约. 若 a_2 可约, 则
 $a_2 = p_2 a_3 \dots$ 此过程亦须有限. 最后得 $a_n = p_{n+1}$ 不可约. $\therefore a = p_1 p_2 \dots p_{n+1}$. 即若 M 满
足因子链条件, 则 M 之每一个单位元素可分解为不可约元之乘积.

若 M 还满足素元条件, 则上述公理唯一: $\forall a \in M, a \notin U(M)$. $a = p_1 \dots p_s$, p_i 不可约.
若又 $a = p'_1 \dots p'_t$, p'_i 不可约. 对 s 似数反证法. 当 $s=1$, (a 不可约). 则 $t=1$, $a=a$,
设 $s=k$ 时成立. 当 $s=k+1$ 时. $a = p_1 \dots p_{k+1} = p'_1 \dots p'_t$. $p_1 | p'_1 \dots p'_t$. p_1 不可约. 故是素
元. 不妨设. $p_1 | p'_1$. 又 p'_1 不可约. p_1, p'_1 相关. $\Rightarrow p_2 \dots p_{k+1} = (up'_1) p'_2 \dots p'_t$. 根据归纳
的归内假设. $k=t-1$. 取 $s=k+1=t$.

设 M 为唯一分解么半群. $\forall a, b \in M$, $d | a$, $d | b$. a, b 有最大公因子 d : ① $d | a$, $d | b$.
②. 若 $c | a$, $c | b$, 则 $c | d$. 则称 d 为 a, b 之最大公因子. 记作 (a, b) . $\forall a, b \in M$.
设 d_1, d_2 为 a, b 之最大公因子. 则 $d_1 | d_2$, $d_2 | d_1 \Rightarrow d_1 \sim d_2$.

$\forall a, b \in M$. (a, b) 一定存在. 若 $a \in U(M)$, 则 $(a, b) \sim a$. 若 $b \in U(M)$, 则 $(a, b) \sim b$. 若
 $a, b \notin U(M)$. $a = p_1^{k_1} \dots p_s^{k_s}$, p_i 不可约. $k_1 \geq k_2 \geq \dots \geq k_s$. $b = q_1^{t_1} \dots q_m^{t_m}$. 由引理 5 写 $a = p_1^{k_1} \dots p_s^{k_s}$,
 $b = p_1^{t_1} \dots p_s^{t_s}$, $k_i, t_i \geq 0$. 则若 $d | a$, $d = p_1^{d_1} \dots p_s^{d_s}$, $d_i \geq 0$. $(a, b) \sim p_1^{m_1} \dots p_s^{m_s}$,
 $m_i = \min\{k_i, t_i\}$.

a, b 的最小公倍数 c : ①. $a | c$, $b | c$ ②. 若 $a | d$, $b | d$ 则 $c | d$. 称 c 为 a, b 之最小公倍数
记作 $[a, b]$. $[a, b] \sim p_1^{n_1} \dots p_s^{n_s}$, $n_i = \max\{t_i, k_i\}$.

M 是唯一分解么半群 $\Leftrightarrow M$ 满足因子链条件、素元条件 $\Leftrightarrow M$ 满足因子链条件、最大公因子
且满足因子链. 最大公因子 \Rightarrow 素元.

定义: $(a_1, \dots, a_n) = d$: ①. $d | a_1, \dots, d | a_n$ ②. $c | a_1, \dots, c | a_n \Rightarrow c | d$.

则 $(a_1 b, c) = ((a_1 b), c) = (a_1, (b, c))$.

Lemma 1. $(a_1, \dots, a_n) = (a_1, \dots, a_{n-1}, a_n)$

Lemma 2. $(a, b, c) = (a, (b, c)) = ((a, b), c)$

Lemma 3. $c(a, b) \sim (ca, cb)$.

证. 若 $d = (a, b)$, $a = dx$, $b = dy$. $\therefore cd \mid ca$, $cd \mid cb$. 若 $e \in (ca, cb)$. $\therefore cd \mid e$. $e = cdw$.
 $ca = ex = cdwx$, $cb = ey = cdwy$. $\therefore a = dux$, $b = duly$. $du, dw \in u$ 为单位. $e = cdw$. $\therefore e \sim cd$

Lemma 4. If $(a, b) \sim 1$, and $(a, c) \sim 1$, then $(a, bc) \sim 1$.

证. $1 \sim (a, c) \sim (a, (ac, bc)) \sim (a, ac), bc \sim (a, bc)$.

Lemma 5. The gcd conditions implies the primeness condition.

Proof. Let p be irreducible, $p \nmid a$, $p \nmid b$. $\therefore (p, a) \sim 1$. $(p, b) \sim 1$. $\therefore (p, ab) \sim 1$.

主理想整环一定是一维分解环。

对 a_1, \dots, a_n, \dots $a_{i+1} \mid a_i$. $a_{i+1} \mid a_i \Leftrightarrow (a_i) \subset (a_{i+1})$.

$\therefore (a_1) \subseteq \dots \subseteq (a_n) \subseteq \dots$ $\bigcup_{i=1}^{\infty} (a_i) = (a)$ 仍是理想. 而 $\forall i < n$ $a \notin (a_n)$. $\therefore a \in (a_{n+1})$. \therefore
 $a \in (a_{n+1}), \dots$. $\therefore (a_n) = (a_{n+1}) = \dots$. \therefore 该序列有反. 满足因子链条件.

$\forall a, b \in D^*$. $(a, b) = (d)$. (R) d 一定为 a, b 之最大公因子。因为：

$(a) \subseteq (d)$. $\therefore d \mid a$. $(b) \subseteq (d)$. $\therefore d \mid b$. 又 $\because d \in (a, b)$. $\therefore d = ax + by$. 若有 c , $c \mid a$, $c \mid b$ 且 $c \mid d$.

一、 G 为群，满足

1) $\exists e \in G$, s.t. $\forall a \in G$, $ea = a$

2) $\forall a \in G$, $\exists a' \in G$, s.t. $a'a = e$

$\forall a \in G$, $\exists a' \in G$, s.t. $a'a = e$. $a' \in G$. 故 $\exists a'' \in G$, s.t. $a''a' = e$.

$$\text{则 } ae = a a' a = (ea)a' a = (\underline{a''a'}a)a' a = \cancel{a''a'}a = a''ea'a = a''a'a \\ = ea = a.$$

$$\text{又 } \cancel{\text{aa' = ea'a}} \cdot aa' = eaa' = a''a'aa' = a''a' = e. \quad \square$$

二、 G 为群, $H_1, H_2 \leq G$. ① $\forall x, y \in G$, 当 $H_1x \cap H_2y \neq \emptyset$ 时, $H_1x \cap H_2y = (H_1 \cap H_2)x$, $a \in H_1x \cap H_2y$.

由 $H_1x \cap H_2y \neq \emptyset$, 任取 $a \in H_1x \cap H_2y$. $\therefore a = h_1x = h_2y$, $h_1 \in H_1$, $h_2 \in H_2$.

$$H_1a = H_1h_1x = H_1x, \quad H_2a = H_2h_2y = H_2y. \quad \therefore H_1x \cap H_2y = H_1a \cap H_2a = (H_1 \cap H_2)a.$$

② $H_1 \leq G$, $H_2 \leq G$. 令 $G = S_3$. $H_1 = \{(1), (12)\}$, $H_2 = \{(1), (13)\}$.

$$H_1H_2 = \{(1), (12), (13), (12)(13) = (132)\}. \quad (132)^{-1} = (123) \notin H_1H_2. \quad H_1H_2 \text{ 不是群.}$$

③ $H_1 \leq G$, $H_2 \leq G$, 则 $H_1H_2 \leq G$.

$$\forall h_1h_2 \in H_1H_2, \quad h_1 \in H_1, \quad h_2 \in H_2. \quad k_1k_2 \in H_1H_2, \quad k_1 \in H_1, \quad k_2 \in H_2.$$

$$(h_1h_2)(k_1k_2) = h_1(h_2k_1)k_2. \quad \because H_2 \trianglelefteq G, \quad \therefore H_2k_1 = k_1H_2 \therefore h_2k_1 = k_1h_2' \\ = h_1(k_1h_2')k_2 = (h_1k_1)(h_2'k_2) \in H_1H_2.$$

$$\forall h_1h_2 \in H_1H_2, \quad (h_1h_2)^{-1} = h_2^{-1}h_1^{-1}. \quad \text{又 } H_2h_1^{-1} = h_1^{-1}H_2. \quad \therefore h_2^{-1}h_1^{-1} = h_1^{-1}h_2^{-1} \in H_2. \quad \therefore H_1H_2 \trianglelefteq G.$$

④ $H_1/H_1 \cap H_2 \cong H_1H_2/H_2$.

$$\varphi: H_1 \rightarrow H_1H_2/H_2, \quad h_1 \mapsto h_1H_2.$$

$$\ker \varphi = H_1 \cap H_2. \quad \text{又 } \varphi \text{ 满}$$

$$\therefore H_1/H_1 \cap H_2 \cong H_1H_2/H_2. \quad \square$$

三、设 R 为环. R 上同余关系与 R 的理想表相同.

$$\overset{A}{\sim} = \{R \text{ 上所有同余关系}\}, \quad B = \{R \text{ 所有的理想}\}.$$

No.

Date. / /

$$\forall \varepsilon \in A, I_\varepsilon = \bar{0} = \{a \in R \mid a \leq 0\}.$$

$$\forall a, b \in \bar{0}, \text{ 即 } a, b \leq 0. \quad \therefore -b \geq 0. \quad \therefore a-b \leq 0. \quad a-b \in \bar{0}. \quad (\text{因为 } -1 \leq -1)$$

$\therefore \bar{0}$ 为 R 的子加群.

$$\forall a \in \bar{0}, r \in R, \quad a \leq 0, \quad r \geq 1. \quad \text{故 } ar \leq 0, \quad ra \leq 0. \quad \boxed{ar, ra \in \bar{0}}$$

$$\therefore \bar{0} \trianglelefteq R.$$

反之: 设 $I \in B$. 在 R 上定义关系 \equiv : $\forall a, b \in R, a \equiv b \Leftrightarrow a-b \in I$.

\equiv 是等价关系(可证). 若 $a \equiv b, c \equiv d$. $(a+b)-(b+d) = (a-b)+(c-d) \in I$.

$$a+b \equiv c+d. \quad ac-bd = ac-bc+bc-bd = (a-b)c + b(c-d) \in I.$$

下证双射: $\forall \varepsilon \in A$, 令 $I_\varepsilon = \bar{0} \trianglelefteq R$. 再由 I_ε 定义 R 上同余关系 \equiv_ε .

$$\forall a, b \in R, a \equiv_\varepsilon b \Leftrightarrow a-b \in I_\varepsilon$$

$$\text{则 } a \equiv_\varepsilon b \Leftrightarrow a-b \in I_\varepsilon \Leftrightarrow a-b \leq 0 \Leftrightarrow a \leq b.$$

反之: $\forall I \in B$. 在 R 上定义同余关系 \equiv_I : $\forall a, b \in R, a \equiv_I b \Leftrightarrow a-b \in I$.

$$\text{令 } \bar{0} = \{a \in R \mid a \equiv_I 0\} = \{a \in R \mid a \in I\} = I.$$

□

四. 证明 Sylow 群 I . $|G|$ 有限. $p^k \mid |G|$, p 素. 则 $\exists H \leq G$ s.t. $|H| = p^k$.

援引理: 设 G 为有限交换群

五. 1) $S = Gx$. If G acts on S transitively.

$\varphi: G \rightarrow Gx = S, g \mapsto g \cdot x$. 在 G 上定义等价关系: $\forall g_1, g_2 \in G, g_1 \sim g_2 \Leftrightarrow \varphi(g_1) = \varphi(g_2) \Leftrightarrow g_1 \cdot x = g_2 \cdot x \Leftrightarrow g_2^{-1}g_1 \cdot x = x \Leftrightarrow g_2^{-1}g_1 \in \text{Stab } x \Leftrightarrow g_1 \in g_2 \cdot \text{Stab } x$.

$\bar{\varphi}: G/\text{Stab } x \rightarrow G \cdot x = S, g \cdot \text{Stab } x \mapsto g \cdot x$. φ 满. 故 $\bar{\varphi}$ 是双射.

$$\begin{array}{ccc} G/\text{Stab } x & \xrightarrow{g'} & G/\text{Stab } x \\ \bar{\varphi} \downarrow & & \downarrow \bar{\varphi} \\ S = G \cdot x & \xrightarrow{\text{是 } g'} & S = G \cdot x \end{array}$$

$\forall g \in \text{Stab } x \quad \forall g \cdot \text{Stab } x \in G/\text{Stab } x, g' \in G$,

$$\bar{\varphi}(g' \cdot g \cdot \text{Stab } x) = \bar{\varphi}(gg' \cdot \text{Stab } x) = gg' \cdot x = g'(g \cdot x) = g' \bar{\varphi}(g \cdot \text{Stab } x)$$

七. 1) 若 $\varphi: \mathbb{Q} \rightarrow \mathbb{Q}$ 是域的同构. 则 $\varphi = 1$.

$$\varphi(1) = 1, \varphi(0) = 0. \quad \forall m \in \mathbb{Z}_+, \varphi(m) = \varphi(\underbrace{1 + \dots + 1}_{m \uparrow}) = \underbrace{\varphi(1) + \dots + \varphi(1)}_{m \uparrow} = m$$

$$\forall m \in \mathbb{Z}_-, \varphi(m) = \varphi(-(-m)) = -\varphi(-m)$$

$$= -(-m) = m. \quad \therefore \forall m \in \mathbb{Z}, \varphi(m) = m.$$

$$\text{当 } m \neq 0, \varphi(m^{-1}) = (\varphi(m))^{-1} = m^{-1}. \quad \forall m, n \in \mathbb{Z}, n \neq 0, \varphi(mn) = \varphi(m)\varphi(n)^{-1} = mn^{-1} = m/n.$$

2). $\varphi: \mathbb{R} \rightarrow \mathbb{R}$ 是自同构. 则 $\varphi = 1$.

首先. $\forall m \in \mathbb{Q}$, 因为 $\varphi(1) = 1$, 故 $\varphi(m) = m$.

$$\forall a \in \mathbb{R}^+, \varphi(a) = \varphi(\sqrt{a} \cdot \sqrt{a}) = \varphi(\sqrt{a})^2 > 0. \quad \text{即若 } a > b, \text{ 则 } \varphi(a) > \varphi(b).$$

假定 $\varphi(a) < a$. 那么 $\exists m \in \mathbb{Q}$, s.t. $\varphi(a) < m < a$. $\because m < a$.

$$\therefore \varphi(m) < \varphi(a). \quad \therefore m < \varphi(a). \quad \text{矛盾.} \quad \square$$

1. $\mathbb{Z}_3[x]/(x^3 + 2x + 1)$. ~~待完成~~

No.

Date. / /

模. module. (线性空间之推广).

(M, +, 0)

作业: 4. 5.

引理1. 设 F 为有限域, F_q 是 F 的一个包含 q 个元素的子域. 那么: F_q 中所有元素都满足 $\alpha^q = \alpha$. 且若 F 中有一个元素 β 满足 $\beta^q = \beta$, 则 $\beta \in F_q$.

$$\forall \alpha \in F_q^*, \alpha^{q-1} = 1, \alpha^q = \alpha.$$

✓ 引理2. 设 F_q 是 q 个元素的有限域. $f(x)$ 是 $F_q[x]$ 上的一个 n 次不可约多项式.

$$\text{则 } f(x) \mid (x^{q^n} - x).$$

$$|F_q[x]/(f(x))| = q^n. \quad (g(x))^{\frac{q^n}{\text{char } F_q}} = g(x) \Rightarrow \overline{g(x)}^{\frac{q^n}{\text{char } F_q}} = \overline{g(x)};$$

$$(\bar{x})^{q^n} = \bar{x}, \quad \overline{x^{q^n}} = \bar{x}. \quad x^{q^n} - x \in \bar{0} = (f(x)) / f(x) \mid (x^{q^n} - x).$$

$$\text{对 } (a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + (f(x)))^q \in F_q[x]/(f(x)). \quad \text{char } F_q = p. \quad \therefore q = p^m.$$

$$(a+b)^p = a^p + C_p^1 a^{p-1} b + \dots + C_p^p b^p. \quad p \nmid C_p^1. \quad \text{故 } p \nmid C_p^1. \quad (a+b)^p = a^p + b^p.$$

$$(a+b)^{p^m} = a^{p^m} + b^{p^m} = a^q + b^q.$$

$$\begin{aligned} \therefore (a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + (f(x)))^q &= a^q + \cancel{(a_1 x)^q} + \dots + (a_{n-1} x^{n-1})^q + (f(x)) \\ &\quad - a_0 - a_1 x^q - \dots - a_{n-1} x^{q(n-1)} + (f(x)) \\ &= a_0 + a_1 x + \dots + a_{n-1} x^{n-1} + (f(x)). \end{aligned}$$

✓ 引理3. $f(x)$ 是 $F_q[x]$ 上的 m 次不可约多项式. 若 $m > n$, 则 $f(x) \mid (x^{q^n} - x)$

$$\text{反设 } f(x) \nmid (x^{q^n} - x). \quad |F_q[x]/(f(x))| = q^m. \quad \text{则 } x^{q^n} - x + (f(x)) = \bar{0}.$$

$$\text{而在 } F_q[x]/(f(x)) \text{ 中}, \quad \bar{x}^{q^n} = \bar{x}. \quad \text{那么 } (a_0 \bar{x} + a_1 \bar{x} + \dots + a_{m-1} \bar{x}^{m-1} + (f(x)))^{\frac{q^n}{\text{char } F_q}} =$$

$$a_0 + a_1 \bar{x} + \dots + a_{m-1} \bar{x}^{m-1} + (f(x)). \quad \text{所以 } F_q[x]/(f(x)) \text{ 上元素都满足 } x^{q^n} - x = 0.$$

但 $q^m > q^n$. 故与根之数矛盾.

引理4. 设 $m, n \in \mathbb{Z}_+$, $d = (m, n)$. 则 $(x^m - 1, x^n - 1) = x^d - 1$

$$\text{设 } m = q_n n + r_1, \quad 0 \leq r_1 < n. \quad \text{即 } (m, n) = (n, r_1)$$

$$(x^m - 1, x^n - 1) = (x^{q_n n} - 1, x^{r_1} - 1) = (x^{r_1} - 1, x^{r_1} - 1)$$

$$= (x^{r_1} - 1, x^{r_1} - 1) = (x^d - 1, x^d - 1)$$

引理5: $m, n \in \mathbb{Z}_+, d = (m, n)$. 则 $(x^{q^m} - x, x^{q^n} - x) = x^d - 1$

$$x^{q^m} - x = x(x^{q^{m-1}} - 1), \quad x^{q^n} - x = x(x^{q^{n-1}} - 1)$$

$$(x^{q^{m-1}} - 1, x^{q^{n-1}} - 1) = x^{(q^{m-1}, q^{n-1})} - 1 = x^{q^d - 1}$$

引理6. 设 F_q 是 q 个元素的有限域, $f(x)$ 是 $F_q[x]$ 中一个 n 次不可约多项式, 则

$$f(x) \mid (x^{q^n} - x) \iff d \mid n.$$

由引理2. $f(x) \mid (x^{q^d} - x)$

$$\text{“\Leftarrow”: 设 } d \mid n, \therefore (x^{q^d} - x, x^{q^n} - x) = (x^{q^d} - x)$$

$$\text{“\Rightarrow”: 设 } f(x) \mid (x^{q^n} - x), \therefore f(x) \mid (x^{q^d} - x, x^{q^n} - x). \text{ 令 } d' = (n, d)$$

$$f(x) \mid (x^{q^{d'}} - x) \text{ 由引理3. } d \leq d'. \text{ 又 } d' = (n, d) \leq d \therefore d = d'. \therefore d \mid n.$$

引理7. 设 F_q 是 q 个元素的有限域, 则 $\forall n \in \mathbb{Z}_+, x^{q^n} - x$ 无重因子

$$\text{证 } x^{q^n} - x = x(x^{q^{n-1}} - 1) \cdot \text{ 令 } f(x) = x^{q^{n-1}} - 1, f'(x) = (q^n - 1)x^{q^{n-2}}$$

又 $f(x)$ 有重根 即 $(f(x), f'(x)) \neq 1$. 则 $f(x)$ 无重因子

定理5. F_q 如上述, $n \in \mathbb{Z}_+$, p_1, p_2, \dots, p_m 是 n 个不同素因子, 用 $\Phi_{q^n}(x)$ 表示 $F_q[x]$

上所有首一的 n 次不可约多项式之乘积, 则

$$\Phi_{q^n}(x) = (x^{q^n} - x) \cdot \prod_{i=1}^m (x^{q^{n/p_i}} - x) \cdots \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq m}} (x^{q^{n/p_i p_j}} - x) \cdots (x^{q^{n/p_1 p_2 \cdots p_m}} - x)$$

再用 $|\Phi_{q^n}(x)|$ 表示 $F_q[x]$ 上所有 n 次不可约首一多项式之个数 则 不可约因子, 但还包

$$|\Phi_{q^n}(x)| = \frac{1}{n} (q^n - q^{n-1} - \sum_{i=1}^m q^{n/p_i} + \sum_{\substack{1 \leq i < j \leq m \\ 1 \leq k \leq m}} q^{n/(p_i p_j)} - \cdots + (-1)^m \cdot q^{n/(p_1 \cdots p_m)}) \text{ 所以要去掉.}$$

注: “ $x^{q^n} - x$ 无重因子” $\therefore x^{q^n} - x$ 可分解为 $F_q[x]$ 中一些两个不同的首一不可约多项式之积 (域工多项式环唯一分解).

设 $g(x)$ 为首一的 d 次不可约多项式. $d \mid n$. $d \mid n \therefore g(x) \mid (x^{q^n} - x)$.

$$n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}, d = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r} p_{r+1}^{e_{r+1}} \cdots p_m^{e_m}, f_i < e_i$$

$$\therefore d \mid \frac{n}{p_1}, d \mid \frac{n}{p_2}, \cdots, d \mid \frac{n}{p_r}, d \nmid \frac{n}{p_{r+1}}, \cdots, d \nmid \frac{n}{p_m}$$

$$d \mid \frac{n}{p_i p_j}, 1 \leq i < j \leq r, \cdots$$

$$1 - C_r^1 + C_r^2 - \cdots + (-1)^r C_r^r = 0, \text{ 故}$$

$$0 \leq |\Phi_{q^n}(x)| = \frac{1}{n} (q^n - \sum_{i=1}^m q^{n/p_i} + \cdots + (-1)^m q^{n/(p_1 \cdots p_m)})$$

且所有 $\Phi_{q^n}(x) \neq 0$. 所以 n 次不可约多项式存在

F, S 为有限域. $F \leq S$, $u \in S$. 求 S 中包含 F, u 的最小子域.

$F[u] = \{ \sum_{i=0}^n a_i u^i \mid a_i \in F \}$ 是 S 中包含 F, u 的最小子环.

u 一定是 $F[x]$ 上的代数元. 否则 $F[u]$ 无限. 所以一定存在不可约多项式 $f(x) \in F[x]$, s.t. $f(u) = 0$.

设 $f(x)$ 是 $F[x]$ 上首一的次数最低的多项式满足 $f(u) = 0$ 使 $f(u) = 0$ 的首一的次数最低的多项式. 称为 u 在 $F[x]$ 上的极小多项式. 它不可约.

若 $u \in F$.

设 u 在 $F[x]$ 上的极小多项式为 $f(x)$, $\deg f(x) > 0$.

因 $F[u] = F$. 则 $F[u] \cong F[x]/(f(x))$ 是域.

用 $F(u)$ 表示 设 F, S 为域. $F \leq S$, $u \in S$. 用 $F(u)$ 表示 S 中包含 F, u 的最小子域. 称 $F(u)$ 为 F 的单扩域.

1) 当 u 为 $F[x]$ 上的代数元. 则 $F(u) = F[u] \cong F[x]/(f(x))$. 其中 $f(x)$ 为 u 在 $F[x]$ 上的极小多项式. $\deg f(x) = m$.

2) 当 u 为 $F[x]$ 上超越元. 则 $F(u) = \{ f(u)/g(u) \mid f(x), g(x) \in F[x], g(x) \neq 0 \}$ 为 $F[u]$ 的分式域.

设 F_1, F_2 为有限域. 则 $F_1 \cong F_2$. 即 $|F_1| = |F_2|$

def 1. F 为有限域. F_q 为 F 的 q 个元素的子域. $\alpha \in F$. 则 α 一定是 $F_q[x]$ 上的代数元. α 在 $F_q[x]$ 上的极小多项式 $f(x)$ 一定存在. 且为不可约多项式. $\deg f(x) = n$. $F_q(\alpha) = F_q[\alpha] \cong F_q[x]/(f(x))$
 $|F_q(\alpha)| = q^n$. $f(x) \mid (x^{q^n} - x)$

" \Rightarrow " 是显然的.

" \Leftarrow ": $|F_1| = |F_2| = p^m$, p 为素数. $F_1^* = F_1 - \{0\}$ 为 $p^m - 1$ 阶循环群.

u 为 F_1^* 这个循环群的生成元. \mathbb{Z}_p 为 F_1 的素域. $\mathbb{Z}_p = \{0, 1, \dots, p-1\} \cong \langle 1 \rangle$.

$\mathbb{Z}_p \leq F_1$, $u \in F_1$. 设 u 在 $\mathbb{Z}_p[x]$ 上极小多项式为 $f(x)$. $\deg f(x) = k$.

$\therefore \mathbb{Z}_p(u) \cong \mathbb{Z}_p[x]/(f(x))$. $|\mathbb{Z}_p[x]/(f(x))| = p^k$

$k = m$. 因为: $\mathbb{Z}_p(u)$ 已含了 \mathbb{Z}_p 生成元.