

# Algebra

# 抽象代数 — 姚慕生

第一章 预备知识	1
§ 1.1 集合	1
§ 1.2 Cartesian 积	3
§ 1.3 等价关系与商集	4
§ 1.4 映射	6
§ 1.5 二元运算	8
§ 1.6 偏序与 Zorn 引理	9

第二章 群论	12
§ 2.1 群的概念	12
§ 2.2 子群及傍集	16
§ 2.3 正规子群与商群	21
§ 2.4 同态与同构	26
§ 2.5 循环群	32
§ 2.6 置换群	37
§ 2.7 群对集合的作用	43
§ 2.8 Sylow 定理	48
§ 2.9 群的直积	53
§ 2.10 有限生成 Abel 群	59
§ 2.11 正规群列与可解群	66
§ 2.12 低阶有限群	71

第三章 环论	78
§ 3.1 基本概念	78
§ 3.2 子环、理想与商环	85
§ 3.3 环的同态	90
§ 3.4 整环、分式域	94
§ 3.5 唯一分解环	99
§ 3.6 PID 与欧氏整区	103
§ 3.7 域上的一元多项式环	106
§ 3.8 交换环上的多项式环	111
§ 3.9 素理想	115
§ 3.10 模	118

第四章 域与 Galois 理论	125
§ 4.1 域的扩张	125
§ 4.2 代数扩域	129
§ 4.3 尺规作图问题	132
§ 4.4 分裂域	136
§ 4.5 可分扩域	143
§ 4.6 正规扩域	148
§ 4.7 Galois 扩域与 Galois 对应	151
§ 4.8 有限域	159
§ 4.9 分圆域	160
§ 4.10 一元方程式的根式求解	165
§ 4.11 正规基定理	171
§ 4.12 域的超越扩张	174

## 第一章：预备知识

## 1.1 集合

$a \in A \Leftrightarrow a \notin A$  元素  $A \cap B, A \cup B, A - B = \{x | x \in A \text{ 但 } x \notin B\}$

$\forall A \in A, \exists a \in B \Rightarrow A \subset B$  集合  $M_{m \times n}(F), M_n(F)$  一方阵,  $GL_n(F) = \{A \in M_n(F) | |A| \neq 0\}$

指标集:  $I$  为集合,  $\forall \alpha \in I$ , 有  $A_\alpha$  这样一集合与之对应

$$\bigcup_{\alpha \in I} A_\alpha = \{x | \exists \alpha \in I \text{ s.t. } x \in A_\alpha\} \quad \bigcap_{\alpha \in I} A_\alpha = \{x | \forall \alpha \in I \text{ s.t. } x \in A_\alpha\}$$

## 1.2 Cartesian 积

def:  $A \times B = \{(a, b) | a \in A, b \in B\}$   $(a, b) = (c, d) \Leftrightarrow a = c \text{ 且 } b = d$

## 1.3 等价关系、商集

def:  $A, B$  为集合,  $A \times B$  的一个子集  $R$  is called  $A$  到  $B$  的一个关系,  $A \times A$  的子集 is called  $A$  上的关系

若  $(a, b) \in R \subset A \times B$ , 称  $a$  与  $b$   $R$  相关, 记为  $a R b$

def: set  $R$  为  $A$  上的关系, 若  $R$  满足: ① 自反性,  $a \in A, (a, a) \in R$  关系  $R$  is called  $A$  上的等价关系.  
 ② 对称性, 若  $(a, b) \in R, (b, a) \in R$   
 ③ 传递性,  $(a, b) \in R, (b, c) \in R$ , 则  $(a, c) \in R$

等价类:  $[a] = \{x \in A | x \sim a\}$ : ① 若  $[a] = [b] \Leftrightarrow a \sim b$   
 $[a] = \{x \in A | x \sim a\}, x \sim a, a \sim b, x \sim b, [a] = [b]$  (proof).  
 ② 若  $[a] \cap [b] = \emptyset \Leftrightarrow a \sim b$ .  
 $[a] \cap [b] = C, a \sim c, c \sim b, a \sim b$  为矛盾.

一个集合若能表示为两两互不相交子集之并, 则称这些子集族为该集合的一个划分

记  $A_\alpha, \alpha \in I$  为  $A$  的一族子集: ①  $A = \bigcup_{\alpha \in I} A_\alpha$  ②  $\forall \alpha \neq \beta, A_\alpha \cap A_\beta = \emptyset$

称  $A_\alpha, \alpha \in I$  为  $A$  的划分.

班级:

姓名:

编号:

第 2 页

def: set " $\sim$ " 为集合 A 上的一个等价关系, A 上所有等价类的集合 is called A 关于 " $\sim$ " 的商集  $A/\sim$   
 $A/\sim = \{[a] | a \in A\}$ .

## 1.4 映射.

def: A, B 为集合, M 为 A 到 B 的关系 ( $M \subseteq A \times B$ ) if M 满足:  $\forall a \in A, \exists! b \in B$ , s.t.  $(a, b) \in M$   
M is called A 到 B 的映射 A-定义域 B-值域, 记为:  $f: A \rightarrow B$

def: ①  $f: A \rightarrow B$   $b = f(a)$ , b is called a 的像, a is called b 的原像.  
 $a \mapsto b = f(a)$

②  $\text{Im } f = \{b \in B | \exists a \in A \text{ s.t. } b = f(a)\}$   $\text{Im } f \neq A$  在 f 下的像

③  $f^{-1}(b) = \{a \in A | f(a) = b\}$  B 的所有原像.

④  $A' \subseteq A$   $f(A') = \{b = f(a) | a \in A'\}$ .  $\text{⑤ } B' \subseteq B$   $f^{-1}(b') = \{a \in A | f(a) \in B'\}$

def:  $f: A \rightarrow B$  ①  $\text{Im } f = B$ , f 为满射 ②  $a \neq a' \in A \Rightarrow f(a) \neq f(a') \in B$ , f 为单射  
③ f 既单又满, f 为双射

def:  $f: A \rightarrow B$   $g: B \rightarrow C$   $g \circ f: A \rightarrow C$

def:  $f: A \rightarrow B$ ,  $\exists g: B \rightarrow A$  s.t.  $g \circ f = \text{Id}_A$ ,  $f \circ g = \text{Id}_B$  称 f 可逆, g 为 f 的一个逆.

f 可逆, f 为双射 (次要)

corollary: f 可逆, f 的逆 g  $\exists!$

## 1.6 偏序和 Zorn 引理

Def. : 设  $A$  为一个非空集合,  $P$  是  $A$  上一个关系, 若  $P$  满足以下条件:

(1)  $\forall a \in A, (a, a) \in P$

(2) 若  $(a, b) \in P$  且  $(b, c) \in P$ , 则  $a = c$

(3) 若  $(a, b) \in P, (b, c) \in P$ , 则  $(a, c) \in P$

则称  $P$  是  $A$  上一个偏序关系, 带偏序关系的集合称为 偏序集/半序集

Zorn lemma: 设  $S$  是偏序集, 若  $S$  中每根链均有上界, 则  $S$  有极大元

# 数学作业纸

2.28

科目 algebra.

班级:

姓名:

编号:

第 3 页

## 1.5 二元运算

def:  $S$  为一个集合,  $S \times S \rightarrow S$  的一个映射 is called  $S$  上的一个二元运算

set "\*" 与 "·" 为  $S$  上 2 种运算, 都应满足.

结合律: (1)  $\forall a, b, c \in S$ , 均有  $a * (b * c) = (a * b) * c$

交换律: (2)  $\forall a, b \in S$ , 均有  $a * b = b * a$

左分配律: (3)  $\forall a, b, c \in S$ , 均有  $a * (b * c) = (a * b) * (a * c)$

左 --- :  $(b * c) * a = (b * a) * (c * a)$

对称群:  $(GF, \circ, 1_G)$

第二章: 群论

①  $(F, +, 0)$

$G \in \mathbb{N}$   
 $O_n(\mathbb{R})$

$(GL_n(F), *, E)$ .

$AA^T = E$

2.1 群的概念

②  $(F^*, \times, 1)$

$SO_n(R)$

$|A|=1$

def:  $S$  为非空集,  $S$  上  $\exists$  二元运算 " $\cdot$ ",  $\forall x, y \in S$ ,  $\exists! z \in S$  与之对应,  $\underline{S \text{ 为半群}}$

结合律-半群 结合+交换 - 交换半群

if  $\exists e \in S$ , s.t.  $\forall a \in S$ , 有  $ea = ae = a$ ,  $e$  is called  $S$  的幺元, 半群 is called 幺半群

def: 让一个么半群  $G$  (幺元为  $e$ ) 满足:  $\forall a \in G$ ,  $\exists a'$ , s.t.  $a'a = aa' = e$ ,  $a'$  为逆元,  $a^{-1}$  称为群  $|G|$  represent  $G$  的元素个数, 让  $|G|=n$ ,  $G$  为  $n$  阶群

性质: 1. 群的幺元是唯一的 2. 群  $G$  中  $\forall a$ , 其  $a^{-1}$  也唯一 3. 群  $G$  中  $\forall a$  有  $(a^{-1})^{-1} = a$

4.  $a, b \in$  群  $G$ ,  $(ab)^{-1} = b^{-1}a^{-1}$  5.  $\forall a, b \in$  群  $G$ ,  $ax=b$   $ya=b$  在  $G$  中有唯一解.

6. if  $au = bu$ , 则  $a = b$  if  $va = vb$ , 则  $a = b$

## 数学作业纸

班级:

姓名:

编号:

第 4 页

2.2 子群及陪集 coset  $G$  的子群:  $\{e\}, G$ def:  $G$  为群,  $H$  为  $G$  的子群, 让  $H$  在  $G$  运算下也为群,  $H$  is called  $G$  的子群theorem:  $H$  为  $G$  的非空子集, 让  $H$  满足以下条件之一则  $H$  为  $G$  的子群(1)  $\forall a, b \in H, ab^{-1} \in H$ (2)  $\forall a, b \in H, ab \in H$ 

(proof)

归纳分析 旗归旗

$$\begin{aligned} AE + Eij &= (E + Eij)A \\ AEij &= Eij A \Rightarrow AAE \end{aligned}$$

corollary:  $H$  为群  $G$  的有限子集,  $\forall a, b \in H$ , 有  $ab \in H$ , 则  $H$  为  $G$  的子群.空间的 U 一般不构成空间  
(U 包含时成立)

$$c_1, c_2 \in C \quad c_1 c_2 \in C \quad c_1^{-1} \in C$$

def:  $G$  为群,  $C = \{c \in G \mid gc = cg, \forall g \in G\}$ ,  $c$  中元素与  $G$  中元素的乘法可交换,  $C$  is called  $G$  的中心

theorem: 群的 center 必为子群. (proof)

$$\begin{aligned} c_1 g = c_1 g c_2 &= g c_1 c_2 \in G \\ c_1 = g & \quad c_1 c_2^{-1} = g \quad g c_2^{-1} = c_1 g \end{aligned}$$

def:  $S$  为群  $G$  的子集,  $G$  中包含集合  $S$  的所有子群的交 is called 由  $S$  生成的子群,  $\langle S \rangle$ 

def

theorem:  $S$  为  $G$  的子集, 则  $\langle S \rangle = \{a_1^{e_1} \cdot a_2^{e_2} \cdot \dots \cdot a_n^{e_n} \mid n \in \mathbb{N}, a_i \in S, e_i \in \mathbb{Z}\}$ 

prop

$$\langle S \rangle = \bigcap_{H \leq G} S \subset H$$

 $\begin{array}{l} a_1, a_2 \in H \\ a_1 a_2 \in H \\ a_1 a_2 \in \langle S \rangle \end{array}$ 

?

def: set  $a$  为群  $G$  的元素,  $\text{ord}(a) = n$ , 则由  $a$  生成的  $G$  的循环子群  $\langle a \rangle$  的阶为  $n$ .def: set  $a$  为群  $G$  的元素, 让  $\exists$  minimal  $n \in \mathbb{N}$  st.  $a^n = e$ , call  $n$  为元素  $a$  的周期(e 的周期为 1, 用  $\text{ord}(a)$  表示 让  $\exists n$  st.  $a^n = e$ ,  $\text{ord}(a) / \infty$ )prop:  $a$  为  $G$  的元素, 且  $\text{ord}(a) = n$ , 若  $m$  为整数, 且  $a^m = e$ , 则  $n | m$ 

$$\langle S \rangle = H$$

①  $H \cup L$  非空, 封闭) ③  $\langle S \rangle$  为群  $\Rightarrow H \subset \langle S \rangle$ ④  $S \subset H$ 

$$H \subset \langle S \rangle$$

# 数学作业纸

科目 Algebra.

班级:

姓名:

编号:

第 5 页

def: set  $H$  为群  $G$  的子群,  $a \in G$ , 则称集合  $Ha = \{ha \mid h \in H\}$  是  $G$  的一个右陪集 / 右旁集

$aH = \{ah \mid h \in H\}$  是  $G$  的一个左陪集 / 左旁集

构造的  $n$  阶可交换群:  $a \oplus b = \begin{cases} a+b & a+b < n \\ a+b-n & a+b \geq n \end{cases}$

非交换群: 1. Hamilton 四元数群 (有无  $\dim > 4$  的 situation?)

2.  $A(S) \longleftrightarrow \{1 \sim n\}$  的所有排列 }  $A(S)$ : 从  $S \rightarrow S$  | 双射 }

$\sigma \longleftrightarrow \sigma(1) \cdots \sigma(n)$   $|A(S)| = n!$ , 记为  $S_n$

# 第二章：群论

## 2.1 群的概念

Def:  $S$  为非空集,  $S$  上  $\exists$  二元运算 “.” (乘法).  $\forall x, y \in S$ , always  $\exists!$  元  $x \cdot y \in S$  与之对应  
该乘法满足结合律, 则称  $S$  为 半群

若半群又满足交换律, 半群又称 交换半群

若半群  $S$  中  $\exists$  元素  $e$  st.  $\forall a \in S$  有  $ea=ae=a$ , 则称  $e$  为  $S$  的 幺元, 这样的群称为 么半群

Def: 一个么半群  $G$  (幺元为  $e$ ) 若满足以下条件则称为 群:

对  $\forall a \in G$ ,  $\exists a'$ , st.  $a'a = aa' = e$ , 元素  $a'$  称为逆元, 记为  $a^{-1}$

若群  $G$  满足交换律, 称为 Abel 群

## 2.2 子群及商集

Def 1:  $G$  为群,  $H$  为  $G$  的子集, 若  $H$  在群  $G$  的运算下也为群, 则称  $H$  为群  $G$  的子群.

prop:  $H$  为群  $G$  的非空子集, 若  $H$  满足以下条件之一, 则  $H$  为  $G$  的子群:

$\frac{1}{2}$  子群

(1)  $a, b \in H, ab \in H$  且  $a^{-1} \in H$

(2)  $a, b \in H, ab^{-1} \in H$

proof

Corollary:  $H$  为群  $G$  的有限子集, 若  $a, b \in H$ , 有  $ab \in H$ , 则  $H$  为  $G$  的子群

Def 2:  $G$  为一个群,  $C = \{c \in G \mid g c = c g, \forall g \in G\}$  称  $C$  为  $G$  的中心

prop: 群的中心必是子群 proof

$$\langle C \rangle = \bigcap_{H \in S} H \quad (\text{其中 } S \text{ 是 } G \text{ 的所有子群})$$

Def 3:  $S$  为群  $G$  的子集,  $G$  中包含集合  $S$  的所有子群的交称为由  $S$  生成的子群, 记为  $\langle S \rangle$

$n=0 \quad n=1 \quad n=2$   
 $\{e\} \quad \{a, a^2\} \quad \{a, a^2, a^3\}$   
 $\emptyset \Rightarrow \langle \emptyset \rangle$   
 $\langle \emptyset \rangle \text{ 为 } G \text{ 的子群}$      $\langle S \rangle \text{ 为 } G \text{ 的子群}$

$\langle \emptyset \rangle \text{ 为 } G \text{ 的子群}$      $\langle S \rangle \text{ 为 } G \text{ 的子群}$

$\langle a \rangle = \{a^0, a^1, a^2, \dots, a^n, \dots, a^{-1}, a^{-2}, \dots, a^{-n}\}$

$a^0 = e$

$a^{-1} = a^{n+1}$

$a^{-2} = a^{n+2}$

$\dots$

$a^{-n} = a^{2n+1}$

$a^{n+1} = a^{2n+2}$

$\dots$

$a^{2n+1} = a^{2n+2}$

$\dots$

$a^{2n+2} = a^{2n+3}$

$\dots$

$\dots$

$a^{2n+3} = a^{2n+4}$

$\dots$

$$Z = \{1\} \quad Z' = \{1, -1\} = \langle 1 \rangle$$

$$\begin{aligned} G &= \{1, -1, i, -i\} \quad G = \{a + bi \mid a^2 + b^2 = 1\} \\ n &= \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} = \{1, \omega, \omega^2, \dots, \omega^{n-1}\} \\ &\text{n元素} \end{aligned}$$

$$G = \langle a \rangle, \text{ 则 } G = \{a^n \mid n \in \mathbb{Z}\}$$

左右陪集

左陪集

$$G = \bigcup_{i=1}^r a_i H \quad \text{if } a_1 \cap a_2 = \emptyset \quad (\text{互不交})$$

$$\Rightarrow |G| = |a_1 H| + |a_2 H| + \dots + |a_r H|$$

$$|a_1 H| = |a H| = H \Rightarrow |G| = S |H|$$

(有限群必定有周期).

$G$  is group  $S \subset G$

① if  $H = \langle s \rangle$  R.I.  $s$  element is called 生成元  $|S| < \infty$ ,  $H$  is called 有限生成子群

②  $G = \langle s \rangle$  R.I.  $G$  is called 循环群  $s = \langle a \rangle$ ,  $G = \langle a \rangle$  is called 循环群  $G = \langle a \rangle$

def: (陪集)  $G$  is group,  $a \in G$ ,  $H \subset G$ ,  $Ha = \{ha \mid h \in H\}$  is called  $G$ 中  $H$  的右陪集  
 $aH = \{ah \mid h \in H\}$  is called  $G$ 中  $H$  的左陪集

prop : ①  $Ha = Hb \iff ab^{-1} \in H$

proof ②  $H$  为有限群,  $|Ha| = |Hb|$

③  $Ha \neq Hb$ , R.I.  $Ha \cap Hb = \emptyset$

①'  $aH = bH \dots$

②'  $|aH| = |bH| \dots$

③'  $aH \neq bH \dots$

(Lagrange 定理): set  $H$  是有限群  $G$  的子群, 则  $|H|$  是  $|G|$  的因子 /  $G$  中  $H \subset G$  则  $|H| \mid |G|$

$$|G| < \infty$$

proof

theorem: 若  $H$  为有限群  $G$  的子群, 则  $|G| = |H| \cdot [G:H]$  ( $[G:H]$  means  $\{gH \mid g \in G\}$  在  $H$  中的像数)

corollary: 若  $|G| < \infty$ , 则 由单位元素的周期必是  $|G|$  的因子

若  $|G| < \infty$ ,  $\forall a \in G$ ,  $a^{|G|} = e$

若  $|G| = p$ ,  $p$  为素数, 则  $G$  为循环群

Euler 定理: 若  $a, n$  都是正整数且  $a$  与  $n$  互素, 则  $a^{\varphi(n)} \equiv 1 \pmod{n}$

Fermat 小定理: set  $p$  为素数,  $a$  为自然数, 则  $a^p \equiv a \pmod{p}$ .

## 2.3 正规子群与商群

### 正规子群

Def 1: let  $G$  为群,  $H$  为  $G$  的子群,  $\forall a \in G$ , 总成立  $Ha = aH$ , 称  $H$  为  $G$  的正规子群 / 不变子群  $H \trianglelefteq G$

Prop: let  $H$  为群  $G$  的子群 ①  $\forall g \in G$ ,  $\forall h \in H$ , 使  $ghg^{-1} \in H$ , 则  $H$  为  $G$  的正规子群  
 ②  $\forall g \in G$ ,  $gHg^{-1} = H$ , 则  $H$  为  $G$  的正规子群

Proof

def:  $G$  is group,  $H \trianglelefteq G$ , def  $a \cdot b \Leftrightarrow ah = bh$  (proof) 证明这个为等价关系.

$$G/a = \{ah \mid a \in G\}$$

Def:  $G$  is group,  $H \trianglelefteq G$ ,  $a \cdot b \Leftrightarrow ah = bh$ , 由  $G/a = \{ah \mid a \in H\}$

根据  $G/a \times G/b \rightarrow G/b$  this is well defined.  
 $(ah, bh) \mapsto abh$

$\Leftarrow$   
 设  $H$  为  $G$  的正规子群. if  $Ha = H_1, Hb = H_2$ , to prove  $Hab = H_1H_2$ ,  
 $Ha = H_1, Hb = H_2 \Rightarrow aH_1 = H_2b \Rightarrow abH_1 = H_2b$ , 由  $(ab)H_1 = abH_1 \in H$   
 $(ab)H_1 = abH_1 = abH_1^1 = abH_1^1H_2^1 = abH_1^1H_2^1 \in H$   
 $\exists h \in H, abh = abH_1^1H_2^1 \in H$   
 $abh = abH_1^1H_2^1 \Rightarrow Hab = H_1H_2$

$\Rightarrow$   
 由且  $Hab$  为  $H$  的子群,  $gHabg^{-1} \in H$   
 $Hg \cdot Habg^{-1} = Hg \cdot H_1H_2g^{-1} = Hg \cdot H_1g^{-1} \cdot H_2g^{-1} = HgH_1g^{-1} \cdot H_2g^{-1} = HgH_1g^{-1} = H$   
 $HgH_1g^{-1} = Hg^{-1}$   
 $gHabg^{-1} = Hab$   $\square$

Lemma: let  $H$  为  $G$  的子群,  $\bar{H}$  为  $H$  全体右陪集所成集合.  $\bar{H} = \{Hb \mid b \in H\}$

$$(H_a)(H_b) = H(ab) \Leftrightarrow H \trianglelefteq G$$

Def:  $(G/a, \cdot)$  构成一个群 ( $G/a$  称为商群, 记为  $G/H$ )

$H$  — 群  
 $H/a$  — 集合

Def 2: let  $G$  为一个群,  $H$  为  $G$  的正规子群,  $\bar{H}$  为  $H$  的右陪集的集合,  $\bar{H}$  在  $Ha \cdot Hb = Hab$  底下构成的群 称为  $G$  关于  $H$  的商群, 记为  $\bar{G} = G/H$

商群  $\bar{G}$  中的元素常用元素的等价类  $\bar{a}$  来表示 ( $\bar{a} = Ha$ ,  $\bar{b} = Hb$ )

$$(Ha) \cdot (Hb) = H(ab) \Leftrightarrow \bar{a} \cdot \bar{b} = \bar{ab}$$

Abel 群 子群 为 正规子群

群  $\rightarrow$  子群  $\rightarrow$  商集 + 运算  $\rightarrow$  商群.

单群:  $G$  中只有  $\{e\}$  与  $G$  无非正规子群 (simple group)  
(有限单群分类定理) EGA SSB

prop: 素数阶群一定是单群. (lagrange定理)

prop: the subgroup of Abel group 正规子群

prop3:  $|G| < \infty$   $|G/H| = \frac{|G|}{|H|}$  (lagrange).

## 2.4 同态与同构

def:  $G_1, G_2 \text{ 为 group}$ ,  $f: G_1 \rightarrow G_2$ , 若  $\forall a, b \in G_1$ ,  $f(ab) = f(a)f(b)$   
则称  $f$  为一个  $G_1$  到  $G_2$  的群同态  
若  $f$  为双射, 则  $f$  为同构. 也称  $G_1, G_2$  同构  $G_1 \cong G_2$

$f: G_1 \rightarrow G_2$  同态

$$1. f(e_1) = e_2$$

若  $f: G_1 \rightarrow G_2$  为群同态, 则  $f(e_1)$  为  $G_2$  的幺元

$$2. \forall g \in G_1 \quad f(g^{-1}) = f^*(g)$$

群同态  $f: G_1 \rightarrow G_2$  将逆元变为逆元, 即  $f(g^{-1}) = f^*(g)$

$$3. \text{Im } f = \{y \mid \exists x \in G_1 \text{ s.t. } f(x) = y\} \subset G_2$$

$f: G_1 \rightarrow G_2$  为群同态, 则  $\text{Im } f$  是  $G_2$  的子群

$$4. \ker f = \{x \in G_1 \mid f(x) = e_2\} \subset G_1$$

$f: G_1 \rightarrow G_2$  为群同态,  $e_2$  为  $G_2$  幺元, 则  $\ker f = \{x \in G_1 \mid f(x) = e_2\}$

5. 同构关系是一个等价关系

proof

$\ker f$  为  $G_1$  的子群, 称为同态  $f$  的核.

### canonical

$$G: H \triangleleft G \quad \pi: G \rightarrow G/H$$

$$\text{自然映射} \quad g \mapsto gh$$

若  $G_1 = G_2$  且  $f: G \rightarrow G$  called 自同态

set  $H$  为群  $G$  的正规子群,  $G$  到商集  $G/G$  上的自然映射是群同态, called 自然同态.

### 同态基本定理:

设  $f$  是群  $G_1$  到  $G_2$  的满同态, 则  $f$  诱导出  $G_1/\ker f \rightarrow G_2$  的同构  $\bar{f}$ ,

其中  $\bar{f}(a) = f(a)$  对  $\forall a \in G_1$  成立

### 同态基本定理

1. 设  $f$  是  $G_1 \rightarrow G_2$  的群同态, 则  $G_1/\ker f \cong \text{Im } f$

$$\begin{array}{ccc} G_1 & \xrightarrow{f} & G_2 \\ \downarrow & & \uparrow j \\ G_1/\ker f & \xrightarrow{\bar{f}} & \text{Im } f \end{array}$$

2.  $\forall$  群同态  $f: G_1 \rightarrow G_2$  可分解为:  $f = j \circ \bar{f} \circ i$

$i: G_1 \rightarrow G_1/\ker f$  的映射  $\bar{f}: G_1/\ker f \rightarrow \text{Im } f$  同构  $j: \text{Im } f \rightarrow G_2$  同态

文字说明: 由  $\ker f \triangleleft G_1$  有  $\forall a \in G_1, \forall b \in \ker f$ ,  $f(ab) = f(a)f(b)$   
 $\Rightarrow f(a)f(b) = f(ab) \Rightarrow f(a)f(b)^{-1} = f(ab)b^{-1} = f(a)$   
 $\Rightarrow f(a) = f(a)$   
 $\therefore f(a) = f(a)$  对  $\forall a \in G_1$  成立

由  $\ker f \triangleleft G_1$  有  $\forall a \in G_1, \forall b \in \ker f$ ,  $f(ab) = f(a)f(b)$   
 $\Rightarrow f(ab) = f(a)f(b) \Rightarrow f(ab)b^{-1} = f(a)$   
 $\Rightarrow f(a) = f(a)$   
 $\therefore f(a) = f(a)$  对  $\forall a \in G_1$  成立

对应定理 设  $f: G_1 \rightarrow G_2$  为群上的满同态，则有

- 1) 若  $H$  为  $G_1$  的子群，则  $f(H)$  是  $G_2$  的子群
- 2) 若  $K$  为  $G_2$  的子群， $\{x \in G_1 \mid f(x) \in K\}$  是  $G_1$  子群，且  $f^{-1}(K) \cong \ker f$
- 3)  $\{G_1 \text{ 中包含 } \ker f \text{ 的子群}\} \xleftarrow{\text{1:1}} \{G_2 \text{ 的子群}\}$   
 $H \quad \quad \quad f(H)$   
 $H \trianglelefteq G_1 \iff f(H) \trianglelefteq G_2 \text{ 同时 } G_1/H \cong G_2/f(H)$

theorem: 设  $f: G_1 \rightarrow G_2$  的群同态，则

$$1) f \text{ 为单同态} \iff \ker f = \{e\}$$

$$2) \text{ if } H \trianglelefteq G_1, H_2 \trianglelefteq G_2, \text{ 且 } f(H) \trianglelefteq f(H_2) \exists g_1 \in G_1, g_2 \in H_2 \text{ st. } f(g_1) = f(g_2) \quad (\eta_1, \eta_2 \text{ 为自然同态})$$

$$\begin{array}{ccc} G_1 & \xrightarrow{f} & G_2 \\ \eta_1 \downarrow & & \downarrow \eta_2 \\ G_1/H_1 & \xrightarrow{f} & G_2/H_2 \end{array}$$

商集到底代表什么

$$V/W = \{x + w \mid w \in W\}$$
$$x + W$$

✓

第一同构定理: 设  $H, N$  为群  $G$  的正规子群且  $H \subseteq N$ ，则

$$G/H/NH \cong G/N$$

第二同构定理:  $H \trianglelefteq G$ ,  $K \trianglelefteq G$  的子群，且  $KNH \trianglelefteq G$  且  $KH/H \cong K/H \cap K$

theorem:  $G$  is group,  $\text{Inn } G \trianglelefteq \text{Aut } G$  的正规子群且  $\text{Inn } G \cong G/C$   $C$  is the center of  $G$ .

## 2.5 循环群

--	--

北京林业大学 2023—2024 学年第 二 学期考试试卷 (A 卷)

课程名称: 近世代数 课程所在学院: 理学院

考试班级: 学号: 姓名: 成绩: \_\_\_\_\_

试卷说明:

1. 本次考试为闭卷考试, 本试卷有选择题 4 题, 填空题大部分, 请勿漏答;
2. 考试时间为 120 分钟, 请考生在规定时间内完成答卷;
3. 答题之前, 请将试卷上的考试信息填写完整, 并写上姓名、学号、姓名填写清楚;
4. 本试卷的答案写在试卷上;
5. 答题完毕, 请将试卷交回, 不得提出考场;
6. 考试中心规定: 请将遵守考场纪律, 诚信考试、公平竞争!

得分

一、(每小题3分, 共30分) 判断正误

1. ( ) 全体有理数在通常乘法下构成一个群.
2. ( ) 群中任何元素的周期和它的逆元的周期相等.
3. ( ) 给定群中, 两个正规子群的交还是正规子群.
4. ( )  $f: G \rightarrow G$  为群同态,  $g \in G$ , 则  $f(g^{-1}) = f(g)^{-1}$ .
5. ( ) 任意两个循环群, 如果它们的阶相同, 则它们一定同构.
6. ( ) 存在包含 8 个元素的域.
7. ( ) 所有整数构成有理数环的一个理想.
8. ( ) 实数域的任意非零自同态均为单同态.
9. ( ) 唯一分解整环中任何理想均为主理想.
10. ( ) 具有恒等元的交换环中, 极大理想为素理想.

得分

二、(12分) (1) 叙述正规子群和商群的定义. (2) 证明  $\mathbb{Z}_2$  为整数加法群的正规子群, 并写出商群  $\mathbb{Z}/\mathbb{Z}_2$  中的所有元素.

得分

三、(12分) 将置换  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$  写成不相交循环之积, 并求该置换的周期与奇偶性.

得分

四、(12分) (1) 叙述群的直积的定义; (2) 证明交换群与交换群的直积还是交换群.

得分

六、(12分) (1) 叙述不可约元的定义; (2) 判断多项式  $x^2+1$  在环  $\mathbb{Z}_{12}[x]$  中是否为不可约元并说明理由.

得分

五、(12分) 设  $R$  为带有恒等元的环. (1) 叙述零因子的定义; (2) 叙述可逆元的定义; (3) 讨论可逆元与零因子的关系并说明理由.

得分

七、(10分) 令  $F = \mathbb{Q}(\sqrt{2})$ . (1) 证明  $F$  为域; (2) 判断环  $F[x]$  中是否存在次数为 2 的不可约多项式. 如果存在请写出一个, 如果不存在请说明理由.