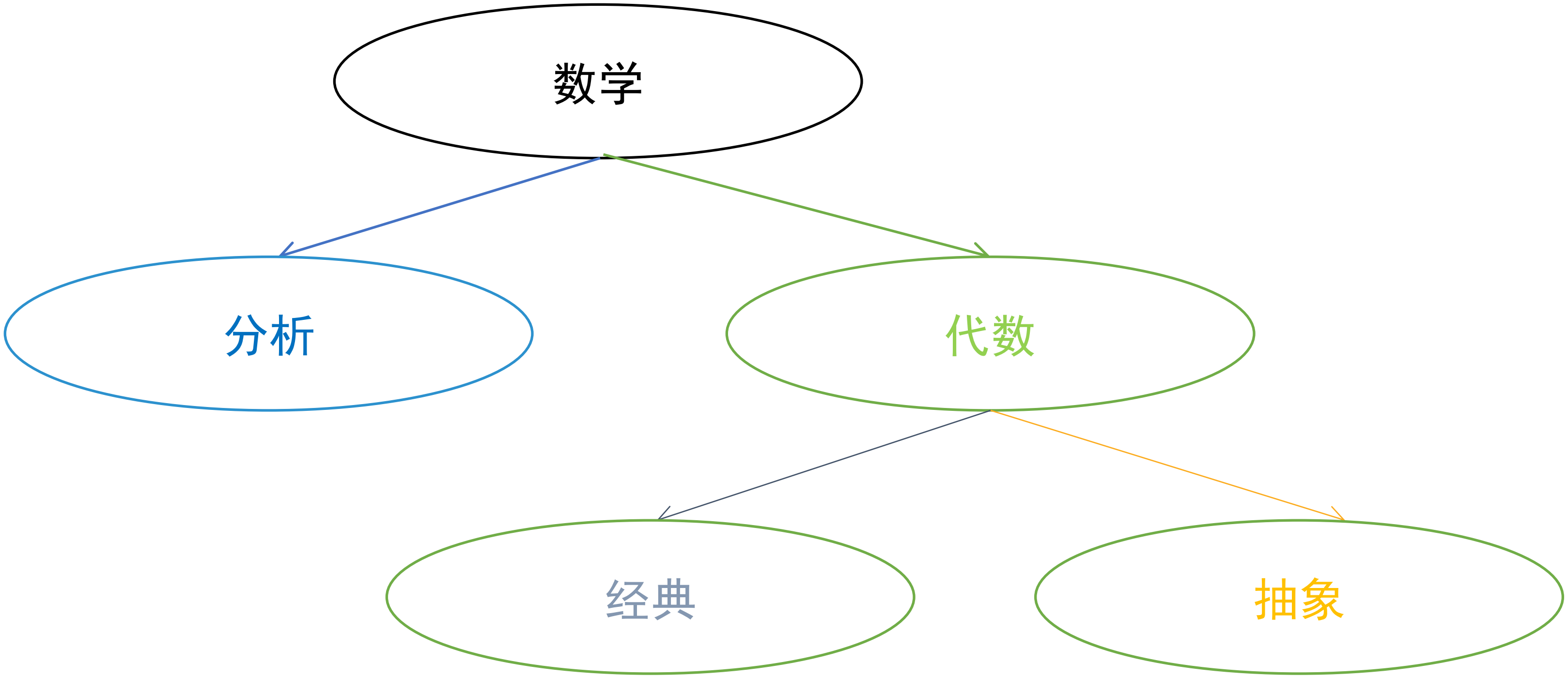
近世代数

计算机科学与技术学院
苏敬勇

数学

- 数学 --- 分析 & 代数
- 代数---经典代数（初等代数、高等代数、线性代数等）& 近世代数
- 近世代数---抽象代数



近世代数

- 代数系统 --- 一个集合，含有一种或多种代数运算
- 近世代数---研究各种代数系统的一门学科
- 抽象代数---一般来说，不仅研究的集合是抽象的，而且其运算也是抽象的。因此，近世代数也常被称作抽象代数。
- 群、环和域---最重要的分支

第一章

- 1. 集合
- 2. 映射 & 变换
- 3. 代数运算
- 4. 运算律
- 5. 同态与同构
- 6. 等价关系与集合分类

集合

- $|A|$： 集合A的元素个数，称作势（Cardinality）
- P(A): A的幂集，A的所有子集的集合

$$|A| = n \quad \Rightarrow \quad |P(A)| = 2^n$$

映射

- 映射定义
- 集合 $A,B,\quad \forall x\in A\quad \exists$唯一的 $\quad y\in B$

$$\varphi:\quad x\rightarrow y\quad or\quad \varphi(x)=y$$

- 映射类别

➢满射 $\quad \varphi:\quad A\rightarrow B,\quad \forall y\in B,\exists x\in A,\quad st.\quad \varphi(x)=y$

$$\Updownarrow$$

满射的充分必要条件是 $\varphi(A)$=B

➢ 单射 $\quad \varphi:\quad A\rightarrow B,\quad \forall x_1,x_2\in A,x_1\neq x_2\quad \Rightarrow\quad \varphi(x_1)\neq\varphi(x_2)$

➢ 双射："满"&"单" $\quad \varphi:\quad X\rightarrow Y$

- 两有限集A,B之间可以建立双射的充分必要条件：$|A|=|B|$
- 设*A*与*B*是两个所含元素个数相等的有限集合，则*A*到*B*的映射是双射当且仅当是满（单）射。

变换

- 定义：集合A到其自身的映射，叫做集合A的一个变换。
- “恒等变换” $I(x)=x$
- 任意n元有限集共有 $n!$ 个双射变换。

一个双射变换 $\Leftrightarrow$ 全排列

$$\varphi=\begin{pmatrix} 1 & 2 & \ldots & n \\ \varphi(1) & \varphi(2) & \ldots & \varphi(n) \end{pmatrix}$$

“一个n元/阶置换” or “一个n次置换”

代数运算

- 定义：集合M上的一个法则$\circ$，如果对于集合上的每一组有序对 $a,b\in M$ ，总存在唯一的 $d\in M$ ，使得 $a\circ b=d$. 那么，这样一个法则 $\circ$就被成为集合M 上的代数运算。
- T(M)：集合M上所有变换构成的集合
- S(M)：M的全体双射变换作成的集合 $n!$
- "乘法表"——有限集上的代数运算的设计 n^{n^2}

$\circ$	a_1	a_2	$\cdots$	a_n
a_1	a_{11}	a_{12}	$\cdots$	a_{1n}
a_2	a_{21}	a_{22}	$\cdots$	a_{2n}
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
a_n	a_{n1}	a_{n2}	$\cdots$	a_{nn}

运算律

- 结合律

$$(a \circ b) \circ c = a \circ (b \circ c)$$

- 交换律

$$a \circ b = b \circ a$$

- 分配律

$$a \circ (b \oplus c) = (a \circ b) \oplus (a \circ c)$$

$$(b \oplus c) \circ a = (b \circ a) \oplus (c \circ a)$$

同态

- 同态映射：　$\varphi(a\circ b)=\varphi(a)\bar{\circ}\varphi(b)$
- 两代数系统同态：存在同态满射 $M\sim\overline{M}$
- 定理1

➢ 代数系统 M 和 $\overline{M}$ 分别有代数运算 $\circ$ 和 $\bar{\circ}$，若 $M\sim\overline{M}$ 则会有以下结论成立：

(1) $\circ$ 满足结合律，那么 $\bar{\circ}$ 也满足结合律。

(2) $\circ$ 满足交换律，那么 $\bar{\circ}$ 也满足交换律。

- 定理2

➢ $\circ$ 和 $\oplus$ 是代数系统 M 上的两个代数运算，$\bar{\circ}$ 和 $\bar{\oplus}$ 是代数系统 $\overline{M}$ 上的两个代数运算；φ 是 M 到 $\overline{M}$ 的一个满射，且对 $\circ$ 与 $\bar{\circ}$，$\oplus$ 与 $\bar{\oplus}$ 同态；那么如果 $\circ$ 对 $\oplus$ 满足左（右）分配律，那么 $\bar{\circ}$ 对 $\bar{\oplus}$ 也将满足左（右）分配律。

同构

- 同态双射：　$M \cong \bar{M}$

- 性质

➢ 1. $M \cong M$　　反身性

➢ 2. 若$M_1 \cong M_2$ ，那么$M_2 \cong M_1$　　对称性

➢ 3. 若 $M_1 \cong M_2$ 且 $M_2 \cong M_3$，那么 $M_1 \cong M_3$　　传递性

- 意义

代数系统M上所有的运算性质都可以自动的传递给所有与之同构的代数系统上。

等价关系

- 关系定义

➢ 集合M上的一个法则R，如果对与M上的任意一对元素a和b总能由其判断出是否满足关系R，或者说，要么满足关系R要么不满足关系R，那么R就称为集合M上元素之间的一个关系，或者简称为M的一个关系。

- 等价关系定义

➢ 若集合M上的一个关系R满足以下三个条件：

(1) 对$\forall a \in M$，总有aRa ---- 反身性

(2) 若aRb，那么bRa ---- 对称性

(3) 若aRb，bRc，那么aRc ---- 传递性

那么关系R就被称为集合M的一个等价关系。

记为“～”，$a \sim b$ 就表示a与b等价。

集合的分类

- 定义

➢若把集合 M 的全体元素分成若干个互不相交的子集 (i.e., 任二子集之间没有公共元素), 则称每一个子集 M 的一个类, 类的全体叫做M 的一个分类 。

- 定理 1

➢ 集合的一个分类决定了集合的一个等价关系.

- 定理 2

➢集合的一个等价关系决定了集合的一个分类。

第二章

- 群的定义和初步性质
- 元素的阶
- 子群
- 循环群
- 变换群
- 置换群
- 陪集、指数和Lagrange定理

群的定义

- 群

定义 1：非空集合G,$\circ$是它的一个代数运算，如果满足以下条件：

Ⅰ：结合律成立，即对G中任意元素 a, b , c 都有

$$(a\circ b)\circ c=a\circ(b\circ c)$$

Ⅱ：G中有元素 e ，叫做G的**左单位元**，它对G中每个元素 a 都有

$$e\circ a=a$$

Ⅲ：对G中每个元素 a ，在G中都有元素 a^{-1}， 叫做 a 的**左逆元**，使

$$a^{-1}\circ a=e$$

则称G对代数运算 $\circ$ 作成一个群。

- 群的阶：一个群G中包含元素的个数称为群G的阶，记为 $|G|=n$ 。
- n次单位根群，四元数群。。。。

群的初步性质

- **性质**
- **定理 1**：群G的左单位元也是右单位元，并且是唯一的。
- **定理 2**：群G中任意元素a的左逆元a^{-1}也是右逆元，并且唯一。
- **推论 1**：在群中消去律成立。

- **半群**：设S是一个非空集合，如果它有一个代数运算满足结合律，则称S是一个半群。
- **幺半群**：如果一个半群S有单位元（既是左单位元又是右单位元），则称S为有单位元的半群，或简称**幺半群（monoid）**。

- **定理 3**：设G是一个半群。则G作成群的充要条件是，对G中任意元素a，b，方程 $ax=b$，$ya=b$ 在G中都有解。
- **推论 2**：有限半群G作成群的充分必要条件是，在G中两个消去律成立。

群中元素的阶

- **定义 1**：设a为群G中的一个元素，使 $a^n=e$ 的最小正整数n，叫做元素a的阶。如果这样的阶不存在，称a的阶为无限。元素a的阶常用 $|a|$ 来表示。
- **定理 1**：**有限群中每个元素的阶均有限。**
- **定义 2**：若群G中**每个元素的阶都有限**，则称G为**周期群**；若G中除单位元e外，其余元素的阶均无限，则称G为**无扭群**；既不是周期群又不是无扭群的群称为**混合群**。
- **定理 2**：设群G中元素a的阶是n，则 $a^m=e \Leftrightarrow n|m$
- **定理 3**：若群中元素a的阶是n，则 $|a^k|=\dfrac{n}{(k,n)}$
- **推论 1**：在群中若$|a|=st$，则 $|a^s|=t$。其中 s,t 是正整数。
- **推论 2**：在群中若$|a|=n$，则 $|a^k|=n \Leftrightarrow (k,n)=1$。
- **定理 4**：群中a的阶为m，b的阶为n，当ab=ba，且（m，n）=1时 $|ab|=|a|\cdot|b|$
- **定理 5**：设G为交换群，且G中所有元素有最大阶m，则G中每个元素的阶都是m的因数，从而群G中每个元素均满足方程 $x^m=e$ 。

子群定义

- 子群
- **定义 1**：设G是一个群，H是G的一个**非空子集**。如果H本身对G的乘法也作成一个群，则称H为群G的一个**子群**。
- 如果 $|G|>1$ ，则群G至少有两个子群，一个是只由单位元e作成的子群 $\{e\}$ （以后常简记为e），另一个是G本身。这两个子群称为群G的**平凡子群**。别的子群，如果存在的话，叫做G的**非平凡子群**或**真子群**。

$$H \leq G, \qquad H < G$$

子群性质

- **定理 1**：设G是群，$H \leq G$ 。则子群H的单位元就是群G的单位元，H中元素a在H中的逆元就是a在群G中的逆元。
- **定理 2**：群G的一个非空子集H作成子群的充要条件是：

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

- **定理 3**：群G的一个非空子集H作成子群的充要条件是：$a,b \in H \Rightarrow ab^{-1} \in H$

注：群G的有限子集H作成子群的充要条件是，H对G的乘法封闭，

$$a,b \in H \Rightarrow ab \in H$$

- **定义2**：令G是一个群，G中元素a如果同G中每个元素都可换，则称a是群G的一个**中心元素**。
- **定理 4**：群G的中心元素作成的集合 $C(G)$ 是G的一个子群，称为群G的**中心**。

子群乘积

- **推论 1**：设H是群G的一个**非空子集**，则

$$H \le G \Leftrightarrow HH = H \quad \& \quad H^{-1} = H$$

- **推论 2**：设H是群G的一个**非空子集**，则$H \le G \Leftrightarrow HH^{-1} = H$

特别地，若H是群G的一个非**空有限子集**，则 $H \le G \Leftrightarrow HH = H$

注：一个群的两个子群的乘积一般不再是子群。但在一定条件下可以是子群。

- **定理 5**：设H，K是群G的两个子群，则 $HK \le G \Leftrightarrow HK = KH$

循环群

- **定义**：如果群G可以由一个元素a生成，即 $G=\langle a\rangle$，则称G为由a生成的一个**循环群**，并称a为G的**一个生成元**。

注：循环群必为交换群

- **定理 1**：设 $G=\langle a\rangle$ 为任一循环群，则

1）当 $|a|=\infty$ 时，$G=\langle a\rangle=\{\cdots,a^{-3},a^{-2},a^{-1},e,a^{1},a^{2},a^{3},\cdots\}$ **为无限循环群，与整数加群同构。**

2）当 $|a|=n$ 时，$G=\langle a\rangle=\{e,a^{1},a^{2},\cdots a^{n-1}\}$**为n阶循环群，且与n次单位根群同构。**

- **推论1**：n阶群是循环群 $\Leftrightarrow$ G有n阶元素。

- **定理2**：无限循环群$\langle a\rangle$有两个生成元，即 a 与 a^{-1}；n阶循环群有 $\varphi(n)$ 个生成元，其中$\varphi(n)$ 为Euler函数。

- **定理3**：循环群的子群仍为循环群。

- **定理4**：无限循环群G有无限多个子群；当 $G=\langle a\rangle$ 为n阶循环群时，对n的每个正因数k，G中有且只有一个k阶子群，这个子群为$\langle a^{n/k}\rangle$ 。

变换群

- **定义 1**：由M的一些变换关于变换的乘法所作成的群，称为M的**一个变换群**；由M的若干个双射变换关于变换乘法作成的群，称为M的**一个双射变换群**；由M的若干个非双射变换关于变换乘法作成的群，称为M的**非双射变换群**。
- **定理 1**：设M为任一非空集合，$S(M)$ 为M的全体双射变换作成的集合。则$S(M)$ 关于变换的乘法作成一个群。
- **定义 2**：称集合M的双射变换群$S(M)$ 为M上的**对称群**，当$|M|=n$，其上的对称群用S_n 表示，并称为**n元对称群**。
- **定理 2**：设G是集合M的一个变换群，则

  G是双射变换群 $\Leftrightarrow$ G中含有M的单（满）射变换。
- **推论 1**：设G是集合M的一个变换群。则

  G是双射变换群 $\Leftrightarrow$ G包含恒等变换。
- **定理 3**：（A. Cayley, 1821-1895）**任何群都与一个（双射）变换群同构**。
- **推论 2**：任何n阶有限群都同n元对称群 S_n 的一个子群同构。

置换群

- **定义1**：n元对称群S_n的任意一个子群，都叫做一个**n元置换群**，简称为**置换群**。
- **定理1**：不相连轮换相乘时可以交换。
- **定理2**：每个（非轮换）置换都可表为不相连轮换之积；每个轮换都可表为对换之积，因此，每个置换都可表为对换之积。

$$(i_1 i_2 \cdots i_k) = (i_1 i_k)(i_1 i_{k-1}) \cdots (i_1 i_3)(i_1 i_2)$$

- **定理3**：**每个置换表示成对换乘积时，其对换个数的奇偶性不变。**
- S_n中所有偶置换作成一个$\frac{n!}{2}$阶子群，记为A_n，称为**n元交代（交错）群**。
- **Klein四元群**：$K_4 = \{(1),(12)(34),(13)(24),(14)(23)\}$
- **定理4**：k-轮换的阶为k；不相连轮换乘积的阶为各因子阶的最小公倍数。
- **定理5**：设有n元置换$\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$，则对任意n元置换$\sigma$，有

$$\sigma\tau\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}$$

陪集

- **定义1**：设H是群G的一个子群，$a \in G$。则称群G的子集

$$aH = \{ax | x \in H\}$$

为群G关于子群H的一个左陪集。而称

$$Ha = \{xa | x \in H\}$$

为群G关于子群H的一个右陪集。

- **左陪集性质**
- **1）**$a \in aH$
- **2）**$a \in H \Leftrightarrow aH = H$
- **3）**$b \in aH \Leftrightarrow aH = bH$
- **4）**$aH = bH$**，即a与b同在一个左陪集中** $\Leftrightarrow$ $a^{-1}b \in H$**（或** $b^{-1}a \in H$**）**
- **5）若** $aH \bigcap bH \neq \Phi$**，则** $aH = bH$

指数和Lagrange定理

- **定理1**：设H是群G的一个子群，又令 $L=\{aH|a\in G\}$， $R=\{Ha|a\in G\}$

  则在L和R之间存在一个双射，

- **定义2**：群G中关于子群H的互异的左（或右）陪集的个数叫做**H在G里的指数**，记为 $(G:\ H)$。

- **定理2**：（J. L. Lagrange）设H是有限群G的一个子群，则

$$|G|=|H|(G:H)\quad\text{，即}\ (G:H)=\frac{|G|}{|H|}\ 。$$

从而任何子群的阶和指数都是群G的阶的因数。

- **推论1**：有限群中每个元素的的阶都整除群的阶。

- **注：素数阶群必为循环群**。

- **定理3**：设G是一个有限群，又 $K\le H\le G$，则 $(G:H)(H:K)=(G:K)$

- **定理4**：设H，K是群G的两个有限子群，则 $|HK|=\dfrac{|H|\cdot|K|}{|H\cap K|}$

- **推论2**：设p，q是两个素数且p<q，则pq阶群G最多有一个q阶子群。

第三章

- 群同态与同构的简单性质
- 正规子群和商群
- 群同态基本定理
- 群的同构定理
- 群的自同构群

群同态与同构的简单性质

- **定理1**：设G是一个群，$\bar{G}$ 是一个有代数运算（也称为乘法）的集合。如果 $G \sim \bar{G}$，则 $\bar{G}$ 也是一个群。

- **推论**：设 φ 是群G到群$\bar{G}$ 的一个同态映射（不一定是满射）。则群G的单位元的像是群 $\bar{G}$ 的单位元，G的元素a的逆元的像是a的像的逆元。即 $\varphi\left(a^{-1}\right)=\varphi(a)^{-1}$

- **定理2**：设φ是群G 到群 $\bar{G}$ 的一个同态映射（不一定是满射），则

1）当 $H \leq G$时，有$\varphi(H) \leq \bar{G}$，且$H \sim \varphi(H)$；

2）当 $\bar{H} \leq \bar{G}$时，有$\varphi^{-1}\left(\bar{H}\right) \leq G$，且在 φ 之下诱导出$\varphi^{-1}\left(\bar{H}\right)$ 到$\bar{H}$ 的一个同态映射。

- **定理3**：群G到群 $\bar{G}$ 的同态映射φ 是单射的充分必要条件是，群 $\bar{G}$ 的单位元 $\bar{e}$ 的逆像只有e。

正规子群定义

- **定义1**：设N是群G的一个子群。如果对G中每个元素 a都有

$$aN = Na\text{，即 } aNa^{-1} = N\text{，}$$

则称N是G的一个正规子群（或不变子群）。

就是说正规子群的**任何一个左陪集都是一个右陪集**，因此简称为**陪集**。

记为 $N \trianglelefteq G$；若N不是G的正规子群记为 $N \ntrianglelefteq G$。

若 $N \trianglelefteq G$ 且 $N \neq G$，则记为 $N \triangleleft G$。

•任意一个群G都至少有其平凡子群｛e｝与G本身是其正规子群，称为G的**平凡正规子群**。G的其他正规子群若存在的话称为G的**非平凡正规子群**。

•任意一个群G的中心是其正规子群，$C \trianglelefteq G$。

•交换群的任意一子群都是该群的正规子群。

•设$N \trianglelefteq G$，又 $N \leq H \leq G$，则 $N \trianglelefteq H$

•例子： $A_n \trianglelefteq S_n$ $K_4 \triangleleft A_4$

正规子群定理

- **定理1**：设G是群，$N \le G$。则 $N \trianglelefteq G \Leftrightarrow aNa^{-1} \subseteq N$ （$\forall a \in G$）。
- **注**：本定理也可改述为：G是群，$N \le G$，则

$$N \trianglelefteq G \Leftrightarrow axa^{-1} \in N \qquad (\forall a \in G, \forall x \in N)$$

- **注**：正规子群的正规子群不一定是原群的正规子群。即，正规子群不具有传递性。

- **定理2**：设 φ 是群G到群 $\bar{G}$ 的同态满射，则

1）$N \trianglelefteq G \;\Rightarrow\; \varphi(N) \trianglelefteq \bar{G}$ ；

2）$\bar{N} \trianglelefteq \bar{G} \;\Rightarrow \varphi^{-1}(\bar{N}) \trianglelefteq G$ 。

- **定理3**：群G的一个正规子群与一个子群的乘积是一个子群；两个正规子群的乘积仍是一个正规子群。

商群

- **定理4**：群G的正规子群N的全体陪集对于陪集乘法作成一个群，称为G关于N的**商群**，记为G/N。

1）$(aN)^m = a^m N \quad (\forall m \in Z)$

2）$|G/N| = (G:N)$

3）Lagrange定理变形：$|G| = |N| \cdot (G:N) = |N| \cdot |G/N| \qquad |G/N| = \frac{|G|}{|N|}$

- **定理5（A.L.Cauchy）**：设G是一个pn阶有限交换群，其中p是一个素数，则G有p阶元素，从而有p阶子群。
- **推论**：pq（p，q为互异素数）阶交换群为循环群。

- **定义2**：每个子群都是正规子群的非交换群，称为**哈密顿群。**
- **定义3**：阶大于1且只有平凡正规子群的群，称为**单群**。
- **定理6**：有限交换群G为单群的充要条件是，群G的阶为素数。

群同态基本定理

- **定理1：** 设N是群G的任一正规子群，则

$$G \sim G/N，$$

即任何群均与其商群同态。

- **定义：** 设 φ 是群G到群 $\bar{G}$ 的一个同态映射，$\bar{G}$ 的单位元在 φ 之下所有逆象作成的集合，叫做 φ 的**核**，记为 $Ker\varphi$。群G中所有元在 φ 之下的像作成的集合 $\varphi(G)$，称为 φ 的像集。记为 $\mathrm{Im}\,\varphi$ 。

- $Ker\varphi \le G$，$\mathrm{Im}\,\varphi \le \bar{G}$
- 定理1中同态映射 τ 的核就是N。
- **定理2：** （**群同态基本定理**）设 φ 是群G到群 $\bar{G}$ 的一个同态满射。则

$$N = Ker\varphi \trianglelefteq G \quad，且 \quad G/N \cong \bar{G}$$

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\tau"'] & \bar{G} \\ G/N \arrow[ur, "\sigma"'] & \end{tikzcd}$$

注：每个群能且只能同它的商群同态。（同构意义下）

群同态基本定理

- **推论1**：设G与$\bar{G}$是两个有限群。如果$G \sim \bar{G}$，则$\left|\bar{G}\right| \Big| \left|G\right|$ 。
- **定理3**：设G与$\bar{G}$是两个群且$G \sim \bar{G}$。若G是循环群，则$\bar{G}$也是循环群。即循环群的同态像必为循环群。
- **注：同态满射下，循环群的生成元的像也是生成元。**
- **推论2**：循环群的商群也是循环群。

- **引理**：设φ是群G到群$\bar{G}$的一个同态映射，又$H \le G$。如果$H \supseteq Ker\varphi$，则

$$\varphi^{-1}\left[\varphi\left(H\right)\right] = H \text{ 。}$$

- **定理4**：设φ是群G到$\bar{G}$的一个同态满射，核是K，则G的包含K的所有子群与$\bar{G}$的所有子群间可建立一个保持包含关系的双射。

群的同构定理

- **定理1（第一同构定理）：** 设φ是群G到群 $\bar{G}$ 的一个同态满射，又 $Ker\varphi \subseteq N \trianglelefteq G$

  $\bar{N}=\varphi(N)$ ，则 $G/N \cong \bar{G}/\bar{N}$ 。

$$\begin{tikzcd}
 & G \arrow[r, "\varphi"] \arrow[dd, equal] & \bar{G}=\varphi(G) \arrow[dd, equal] \arrow[dr, dash] & \\
G/N \arrow[ur, dash] \arrow[dr, dash] & & & \bar{G}/\bar{N} \\
 & N \arrow[r, "\varphi"] & \bar{N}=\varphi(N) \arrow[ur, dash] &
\end{tikzcd}$$

- **推论：** 设H，N是群G的两个正规子群，且$N \subseteq H$，则 $G/H \cong G/N/H/N$
- **定理2（第二同构定理）：** 设G是群，又 $H \leq G$, $N \trianglelefteq G$。

  则 $H \cap N \trianglelefteq H$ ，且 $HN/N \cong H/(H \cap N)$

- **定理3（第三同构定理）：** 设G是群，又$N \trianglelefteq G$， $\bar{H} \leq G/N$ 。则

1）存在G的唯一子群$H \supseteq N$，且$\bar{H}=H/N$；

2）又当 $\bar{H} \trianglelefteq G/N$ 时，有唯一的$H \trianglelefteq G$使

$$\bar{H}=H/N \text{ 且 } G/H \cong G/N/H/N$$

自同构群&内自同构群

- **自同构群定义**：群G的全体自同构关于变换乘法作成一个群。这个群称为**群G的自同构群，记为AutG。**
- **定理2**：无限循环群的自同构群是一个2阶循环群；n阶循环群的自同构群是一个$\varphi(n)$阶群，其中 $\varphi(n)$为Euler函数。
- **推论2**：无限循环群的自同构群与3阶循环群的自同构群同构。

- **定理3**：设G是一个群，$a \in G$。则

1）$\tau_a : x \to axa^{-1} \quad (\forall x \in G)$是G的一个自同构，称为**G的一个内自同构**；

2）G的全体内自同构作成一个群，称为**G的内自同构群**，记为 $InnG$；

3）$InnG \trianglelefteq AutG$。

•**注**：对于群G的正规子群来说，总有 $aNa^{-1} \subseteq N$ 或 $\tau_a(N) \subseteq N$ ，其中 $\forall a \in G, \forall \tau_a \in InnG$，也就是说正规子群N是关于G的所有内自同构不变的子群，因此正规子群又常被称为**不变子群**。

特征子群&全特征子群

- **定义1**：对群G的所有自同构都不变的子群，亦即对G的任何自同构 σ，都有

$$\sigma(N) \subseteq N$$

的子群N，叫做G的**一个特征子群**。

- **定义2**：设H是群G的一个子群。如果H对G的每个自同态映射都不变，即对G的每个自同态映射 φ 都有 $\varphi(H) \subseteq H$，则称H为群G的一个**全特征子群**。

$$\text{全特征子群} \subseteq \text{特征子群} \subseteq \text{正规子群}$$

- **定理4**：设C是群G的中心，则

$$InnG \cong G / C$$

第四章

- 环的定义
- 环的零因子和特征
- 除环和域

环的定义

- **定义1**：设非空集合R有两个代数运算，一个叫做加法（一般用+表示），另一个叫做乘法。如果：

1）R对加法作成一个加群；

2）R对乘法满足结合律：

$$(ab)c = a(bc)\ ;$$

3）乘法对加法满足左右分配律：

$$a(b+c) = ab+ac,\quad (b+c)a = ba+ca,$$

其中a,b,c为R中任意元素，则称R对这两个代数运算作成一个环。

- 若环R的乘法满足交换律，即对R中任意元素 a,b，都有 $ab=ba$ ，则称R为交换环（可换环）；否则称R为非交换环（非可换环）。
- 一个环可能既无左单位元又无右单位元，如偶数环；也可能只有左单位元，而无右单位元，或者只有右单位元而无左单位元。

子环

- **定义3**：设S是环R的一个非空子集。如果S对R的加法与乘法也作成一个环，则称S是R的一个**子环**，记为$S \le R$ 或 $R \ge S$ 。
- **定理1**：环R的非空子集S作成子环的充要条件是

$$a,b \in S \Rightarrow a-b \in S$$
$$a,b \in S \Rightarrow ab \in S$$

- 当S为R的一个非空有限子集时，上述的充分必要条件改为对加法和乘法都封闭即可。

$S \le R$ ：当R有单位元时，S不一定有；当S有单位元时，R不一定有；即使二者都有单位元，此单位元也未必相同。

循环环

- 一个环关于其加法作成一个加群，用 $(R,+)$ 表示，并称其为环R的加群。如果 $(R,+)$ 是一个循环群，则称环R是一个循环环。即

若 $(R,+)=\langle a\rangle$ ，则循环环R可表示为

$$R=\{\cdots,-2a,-a,0,a,2a,\cdots\},\quad a^2=ka,\quad k\in Z$$

若a在加群 $(R,+)$ 中的阶为n，则R可表示为

$$R=\{0,a,2a,\cdots,(n-1)a\},\quad a^2=ka,\quad 0\le k\le n-1,\quad k\in Z$$

- **注：**

1）整数环是一个无限循环环。

2）循环环必是交换环。

3）循环环子环也为循环环。

4）循环环不一定有单位元。（例如：偶数环）

- **定理2：** 素数阶环，更一般地，阶为互异素数之积的有限环必为循环环。

环的零因子和特征

- **定义1**：设 $a \neq 0$ 是环R的一个元素。如果在R中存在元素 $b \neq 0$ 使 $ab = 0$，称 a 为 环R的一个**左零因子**。同样可以定义环R的一个**右零因子**。
- **定理1**：在环R中，若 a不是左零因子，则 $ab = ac, a \neq 0 \Rightarrow b = c$

  若 a 不是右零因子，则 $ba = ca, a \neq 0 \Rightarrow b = c$
- **推论**：若环R无左（或右）零因子，则消去律成立；反之，若R中有一个消去律成立，则R无左及右零因子，且另一个消去律也成立。

$$\text{无左零因子} \Leftrightarrow \text{无右零因子}$$

- **定义2**：阶大于1、有单位元且无零因子的交换环称为**整环**。
- **定义3**：若环R的元素（对加法）有最大阶n，则称n为环**R的特征。**
- **定理2**：设R是一个无零因子环，且 $|R| > 1$。则

1）R中所有非零元素（对加法）的阶均相同。

2）若R的特征有限，则必为素数。

- **定理3**：若环R有单位元，则单位元在加群 $(R, +)$ 中的阶就是R的特征。

除环和域

- **定义1**：设R是一个环。如果 $|R|>1$，又R有单位元且每个非零元都有逆元，则称R是一个**除环**（**或体**）。
- **可换除环**称为**域**。

- **定理1**：除环和域没有零因子。

  注：除环和域的特征只能是素数或无限。

  注：有限除环必为域。----魏得邦定理。
- **定理2**：阶大于1的有限环若有非零元不是零因子，则必有单位元，且每个非零又非零因子的元素都是可逆元。
- **推论**：阶大于1的有限环R若无零因子，则必为除环。
- **定理3**：设R是环且 $|R|>1$ 。则R是除环当且仅当对R中任意元素 $a\neq 0,b$，方程

  $ax=b \quad (\text{或}ya=b)$ 在R中有解。

子除环和子域

- 子除环、子域：

$$a,b \in F_1 \Rightarrow a-b \in F_1$$

$$0 \neq a,b \in F_1 \Rightarrow a^{-1}b \in F_1$$

域F中的子集 F_1，成子除环、子域的充分必要条件。

- 每个有理数都是二整数之商，且有理数域是包含整数环的最小数域。由此引出一般的整环和域之间的关系推广：
- **定义2**：设R是一个整环，K是包含R为其子环的一个域。则

$$F=\left\{\frac{b}{a}=a^{-1}b \middle| 0 \neq a,b \in R\right\}$$

作成K的一个包含R为其子环的子域（而且是包含R的最小域）。称F为整环R的**分式域或商域**。

- 分式域是存在的，而且对环的加法与乘法来说，**同构整环的分式域必同构**。

环的单位群

除环或域对加法作成一个交换群（加群），但对乘法只能作成一个半群。

但是除环的全体非零元对乘法作成群，而且域的全体非零元对乘法作成交换群。

更一般地，一个有单位元的环的全体可逆元对乘法显然也作成群。

- **定义3**：设R是一个有单位元的环，则R的可逆元也称为R的**单位**；R的全体可逆元（单位）作成的群，称为R的**乘群**或**单位群**，并用 R^* 或 $U(R)$ 表示。

结束语

祝大家获得**理想**的分数！