# 计算学部金牌讲师团 2023 数理逻辑与近世代数复习提纲

（系笔者自行总结，仅作为复习参考）

## 一、近世代数部分

**半群、幺半群：**

**基本定义和简单性质及相应代数系统判定**

**群：**

**基本定义及相应代数系统判定**

交换群的简单性质、子群的等价判定

**对称群、变换群、同构的相关证明**

- **群的 Cayley 同构定理**：任何一个群同构于某个变换群。

关于**循环群子群的证明、子群阶的相关证明计算**

**同态下子群以及正规性的证明**、商群的简单定义以及同态的相关证明

- **群的同态基本定理**：设$\varphi: G_1 \to G_2$的满同态，$E = Ker\ \varphi$，则$G_1/E = G_2$。

**环：**

运用**环体域的基本定义来判定代数系统、无零因子环的判定**

## 二、数理逻辑部分

命题逻辑的基本概念，**逻辑蕴涵逻辑等价判定**；

**主范式的求解**，联结词的完备集相互表示；

**PC 的证明，ND 的证明**；

自然语句**一阶谓词的形式化**

**2023.2.15**

计算学部金牌讲师团

附件：计算学部金牌讲师团 2023 近世代数基础知识梳理总结

# 第 1 章  半群和幺半群

## §1.1  若干基本概念

**映射：** 设$X$和$Y$是两个非空集合，一个从$X$到$Y$的映射是一个满足以下两个条件的$X \times Y$的子集$f$：

1) 对$X$的每一个元素$x$，存在一个$y \in Y$使得$(x, y) \in f$；
2) 若$(x, y)$、$(x, y') \in f$，则 $y = y'$。

**二元代数运算：** 设$X$是一个集合，一个从$X \times X$到$X$的映射$\varphi$称为$X$上的二元代数运算。符号表示："$\circ$"或"$\bullet$",称为乘法，记为$x \circ y$称作$x$与$y$的积。

**一元代数运算：** 一个从集合$X$到集合$Y$的映射称为$X$到$Y$的一个一元代数运算。当$X = Y$时，则称此一元代数运算为$X$上的一元代数运算。

**注：$X$上的一元和二元代数运算均满足运算的封闭性。**

**代数系：** 设"$\circ$"是非空集合$S$上的一个二元代数运算，则称二元组$(S, \circ)$为一个(有一个代数运算的)代数系。

**运算律：**

1) 结合律：设"$\circ$"是$X$上的一个二元代数运算。如果$\forall a, b, c \in X$有： $(a \circ b) \circ c = a \circ (b \circ c)$则称此二元代数运算适合结合律。
2) 交换律：若对$\forall a, b \in X$有：$a \circ b = b \circ a$ 则称此二元代数运算适合交换律。
3) 分配律：设$(S, \circ, +)$是具有两个二元代数运算"$\circ$"和"$+$"的代数系。
   - 左分配律：如果$\forall a, b, c \in S$，有：$a \circ (b + c) = (a \circ b) + (a \circ c)$则称"$\circ$"对"$+$"满足左分配律。
   - 右分配律：如果$\forall a, b, c \in S$，有：$(b + c) \circ a = (b \circ a) + (c \circ a)$则称"$\circ$"对"$+$"满足右分配律。
   - 合成：如果二元代数运算"$\circ$"满足交换律，则左分配律与右分配律合为一，此时称"$\circ$"对"$+$"满足分配律。

**运算律相关定理：**

1) 设$(S, \circ)$是一个代数系，如果二元代数运算"$\circ$"适合结合律，则$\forall a_i \in S, i = 1,2,3, \cdots n$，$n$个元素$a_1, a_2, \cdots, a_n$的乘积仅与这$n$个元素及其次序有关而唯一确定。

2) 设$(S, \circ)$是一个代数系，如果二元代数运算"$\circ$"适合结合律和交换律，则$\forall a_i \in S, i = 1,2,3, \cdots n$，$n$个元素$a_1, a_2, \cdots, a_n$的乘积仅与这$n$个元素有关而与它们的次序无关。

3) 设$(S, \circ, +)$是具有两个二元代数运算的代数系。如果加法"$+$"满足结合律"$\circ$"对"$+$"满足左(右)分配律，则对$\forall a_i \in S, i = 1,2,3, \cdots n$,有：

$$a \circ (a_1 + a_2 + \cdots + a_n) = (a \circ a_1) + (a \circ a_2) + \cdots + (a \circ a_n)$$

$$(a_1 + a_2 + \cdots + a_n) \circ a = (a_1 \circ a) + (a_2 \circ a) + \cdots + (a_n \circ a)$$

**单位元素**：设$(S, \circ)$是一个代数系，

- 左单位元素：如果存在一个元素$a_l \in S$使得$\forall a \in S$有：$a_l \circ a = a$，则称$a_l$为乘法"∘"的左单位元素；
- 右单位元素：如果存在一个元素$a_r \in S$使得$\forall a \in S$有：$a \circ a_r = a$，则称$a_r$为乘法"∘"的右单位元素；
- 单位元素：如果存在一个元素$e \in S$使得$\forall a \in S$有：$e \circ a = a \circ e = a$，则称$e$为乘法"∘"的单位元素。
- **重要定理：设$(S, \circ)$是一个代数系，如果二元代数运算"∘"既有左单位元$a_l$又有右单位元$a_r$，则$a_l = a_r$，从而有单位元。**

**零元素**：设$(S, \circ)$是一个代数系。若存在一个元素$z \in S$使得$\forall a \in S$有：$z \circ a = a \circ z = z$ 则称$z$是"∘"的零元素

**简记形式**：设$(S, \circ)$是一个代数系。$A, B \subseteq S$定义：$A \circ B = \{a \circ b \mid a \in A且b \in B\}$简记为$AB$。而把$a \circ b$写成$ab$。 特别地，当$A = \{a\}$时，$AB = \{a\}B$，简记为$aB$，即： $aB = \{a \circ b \mid b \in B\}$, $Ba = \{b \circ a \mid b \in B\}$ 。

## §1.2 半群与幺半群的概念

**半群**：设"∘"是非空集合$S$上的一个二元代数运算，称为乘法。若对$\forall a, b, c \in S$有$(a \circ b) \circ c = a \circ (b \circ c)$则称集合$S$对乘法"∘"形成一个半群，记为$(S, \circ)$。即半群就是满足结合律的二元代数运算的代数系。

**交换半群**：设$(S, \circ)$为半群， 若乘法"∘"还满足交换律，则称为交换半群，或称为可换半群。

**有限半群**：只含有有限个元素的半群称为有限半群，否则称为无限半群。

如果半群$(S, \circ)$中既有左单位元又有右单位元，则左单位元与右单位元相等，从而有单位元素且单位元素是唯一的。

**幺半群**：有单位元素的半群$(S, \circ)$称为幺半群。其单位元素记为$e$， 幺半群记为$(S, \circ, e)$。若$S$为有限集， 则称为有限幺半群。把$S$的基数称为幺半群$(S, \circ, e)$的阶。

设$(S, \circ, e)$是一个幺半群，$m, n$是任意的非负整数，则$\forall a \in S$有：

$$a^m \circ a^n = a^{m+n} \Rightarrow (a^m)^n = a^{mn}$$

如果$(S, \circ, e)$是可交换的，则对$\forall a, b \in S$有$(a \circ b)^n = a^n \circ b^n$，其中，

$$a^0 = e，a^{n+1} = a^n \circ a，n \geq 0$$

**幺半群的逆**：设$(S, \circ, e)$是一个幺半群，元素$a \in S$，

- 如果存在一个元素$a_l \in S$使得$a_l \circ a = e$，则称$a_l$为$a$的左逆元素；

- 如果存在一个元素$a_r \in S$使得$a \circ a_r = e$，则称$a_r$为$a$的右逆元素；
- 如果存在一个元素$b \in S$使得$a \circ b = b \circ a = e$，则称$b$为$a$的逆元素。
- 幺半群$(S, \circ, e)$中元素$a$若有左逆元素$a_l$又有右逆元素$a_r$，则$a_l = a_r$，于是$a$有逆元素且$a$的逆元素唯一，记为$a^{-1}$。

**群**：每个元素都有逆元素的幺半群称为群。

# 第 2 章 群

## § 2.1 群的定义

**群**：设$G$为一非空集合，"$\circ$"为$G$上的二元代数运算，称为乘法，且满足：

1) 结合律：对$\forall a, b, c \in S$有：$(a \circ b) \circ c = a \circ (b \circ c)$；
2) 有左单位元 e：即对$\forall e \in G$，$e \circ a = a$；
3) 有左逆元素：即对$\forall a \in G$，$\exists b \in S$，使得$b \circ a = e$（$e$为上述左单位元）则称$(G, \circ)$为群。

**等价定义或判定定理：**

**定理一**：1) "$\circ$"满足结合律； 2) 对$\forall a, b \in G$，方程 $\begin{cases} ax = b \\ ya = b \end{cases}$ 在$G$中有解。

**定理二**：1) "$\circ$"满足结合律； 2) "$\circ$"满足左右消去律。(**有限群**)

**交换群（可换群）**：设$(G, \circ)$为群，乘法"$\circ$"满足交换律，即对$\forall a, b \in G$有 ：$a \circ b = b \circ a$，则$(G, \circ)$称为交换群（可换群），或称为阿贝尔群（Abel 群）

**有限群**：设$(G, \circ)$为群，且$G$是有限集，则称$(G, \circ)$为有限群，此时称$G$的基数$|G|$为$G$的阶。

**无限群**：设$(G, \circ)$为群，且$G$含有无穷多个元素。

## § 2.2 群的简单性质

**定理 1**；设为$(G, \circ)$群，则对$\forall a \in G$，$a$的左逆元也是$a$的右逆元。

**定理 2**：设为$(G, \circ)$群，则$G$的左单位元也是右单位元。

**定理 3**：设为$(G, \circ)$群，则对$\forall a, b \in G$有：$(a^{-1})^{-1} = a$，$(ab)^{-1} = b^{-1}a^{-1}$

**定理 4**：设为$(G, \circ)$群，则对$\forall a, b \in G$，方程：

$$\begin{cases} ax = b \\ ya = b \end{cases}$$

关于未知量$x$与$y$均有唯一解。

**定理 5**：设$G$为一非空集合， "$\circ$"为$G$上的二元代数运算，则$(G, \circ)$为群的充要条件为：1) "$\circ$"满足结合律 ； 2) 对$\forall a, b \in G$，方程 $\begin{cases} ax = b \\ ya = b \end{cases}$ 在$G$中有解。

**定理 6：** 设$(G,\ \circ)$为群，则$G$关于乘法"$\circ$"满足消去律，即对$\forall x,y,a \in G$有:

1) 若$ax = ay$，则$x = y$（称为左消去律）
2) 若$xa = ya$，则$x = y$（称为右消去律）

**定理 7：** $G$为非空有限集合，"$\circ$"为$G$上的二元代数运算，则$(G,\ \circ)$为群的充要条件:

1) "$\circ$"满足结合律；　2) "$\circ$"满足左右消去律。

**元素的阶：** 设$(G,\ \circ)$为群，$a \in G$，使$a^n = e$的最小正整数$n$称为$a$的阶，记为$o(a) = n$. 反之则称$a$的阶为无穷大。

注：若$a$的阶为无穷大，则不可能有$a^n = a^k (n > k)$；有限群的每个元素的阶不超过该有限群的阶。

## §2.3 子群、生成子群

**子群：** 设$(G,\ \circ)$为群，$S$是$G$的非空子集，若"$\circ$"在$S$中封闭且$S$对此乘法也构成一个群，则称$S$是$G$的一个子群。

**子群的性质：**

1) 设$G_1$为群$G$的子群，则$G_1$的单位元必是$G$的单位元；$G_1$的元素$a$在$G_1$中逆元素$a^{-1}$也是$a$在$G$中的逆元素。
2) 群$G$的任意多个子群的交还是$G$的子群。
3) 任一群不能是其两个真子群的并。
4) 群$G$的非空子集$S$为$G$的子群的充分必要条件是：
   - $\forall a,b \in S, ab \in S$
   - $\forall a \in S, a^{-1} \in S$

   **推论：群$G$的非空子集$S$为$G$的子群的充分必要条件：　$\forall a,b \in S, ab^{-1} \in S$**
5) 群$G$的**有限**非空子集$F$是$G$的子群的充分必要条件是$FF \subseteq F$，即　:

$$\forall a,b \in F, ab \in F$$

**生成子群：** 设$M$是群$G$的非空子集，则$G$的包含$M$的所有子群的交称为由$M$生成的子群，记为$(M)$。

**迭代扩张算法：** 设$(G,\ \circ)$为群，$A$为$G$的非空子集，则由$A$扩充为$G$的生成子群$(A)$方法:

1) 构造可逆性$A_0 = A \cup \{a^{-1} |\ \forall a \in A\}\ //A \cup A^{-1}$
2) 构造封闭性$A_{n+1} = A_n \cup A_n A_n$
3) 验证$A_{n+1} A_{n+1} \subseteq A_{n+1}$

**中心：** 设$(G,\ \circ)$为群，$a \in G$, 对$\forall x \in G$，有$ax = xa$，则称$a$为 $G$的中心元素。由$G$的中心元素所构成的集合$C$称为$G$的中心，即：$C = \{a|\ \forall x \in A, ax = xa, a \in G\}$

注：群$G$的中心$C$是$G$的可交换子群。
**换位子：** 设$(G, \circ)$为群，对$\forall a, b \in G$，$aba^{-1}b^{-1}$称为$a$与$b$的换位子。
**换位子群：** $G$的所有换位子的集合所生成的子群。

## §2.4 变换群、同构

**同构：** 设$(G_1, \circ)$与$(G_2, *)$为群，若存在一一映射$\varphi: G_1 \to G_2$，使得对$\forall a, b \in G_1$有$\varphi(a \circ b) = \varphi(a) * \varphi(b)$则称$G_1$与$G_2$同构，记为$G_1 \cong G_2$称$\varphi$为$G_1$到$G_2$的一个同构。
注：同构的两个群，除了在元素和代数运算的表示符号不同 外，他们的性质完全一样， 抽象地看是一样的。
**同构的性质：**
- 自反性：$G_1 \cong G_1$
- 对称性：若$G_1 \cong G_2$，则$G_2 \cong G_1$
- 传递性：若$G_1 \cong G_2$，$G_2 \cong G_3$，则$G_1 \cong G_3$

**对称群：** 设$S$为非空集合，$f: S \to S$的一一映射，记$Sym(S) = \{f \mid f: S \to S\}$，则$Sym(S)$关于映射的合成运算构成一个群，称为$S$上的对称群。 当$S = \{1,2,3, \dots, n\}$时， 则$Sym(S) = S_n$为所有$n$次置换之集，称为$n$次对称群。
**变换群：** $Sym(S)$的任一子群称为$S$上的一个变换群。
**置换群：** $S_n$的任一子群称为置换群。
**群的 Cayley 同构定理：** 任何一个群同构于某个变换群。**（证明不作要求）**
- 推论：任一$n$阶有限群同构于$n$次对称群$S_n$的一个$n$阶子群。即有限群同构于某个置换群。**（要点：1. 构造基于群$G$的变换群； 2. 构造同构映射）**

**自同构：** 设$(G, \circ)$为群，$\varphi: G \to G$上的一一映射，且对$\forall a, b \in G$有$\varphi(a \circ b) = \varphi(a) \circ \varphi(b)$，则称$\varphi$为$G$的一个自同构。
**自同构群：** 设$(G, *)$为群，则$G$的所有自同构之集$A(G)$对映射的合成运算构成一个群，称为$G$的自同构群。
*__内自同构：__ 群$G$的由其元素$a$确定的自同构$\varphi(x) = axa^{-1}$，$\forall x \in G$称为 G 的内自同构。群$G$所有内自同构之集是$G$的自同构群的一个子群，称为内自同构群
*__外自同构：__ $G$的其他自同构称为外自同构。

## §2.5 循环群

**循环群：** 若群$G$由其中的某个元素$a$生成的，记为$G = (a)$，$a$称为$G$的生成元。
- 循环群必为交换群（类似循环半群必为交换半群）；
- 设$G = (a)$，且$a$的阶为无穷，则$G = \{\cdots, a^{-n}, \cdots, a^{-2}, a^{-1}, e, a^1, a^2, \cdots, a^n, \cdots\}$

循环群$G=(a)$为无穷循环群的充要条件是$a$的阶为无穷大；

- 设$G=(a)$，且$a$的阶为$n$，即有$a^n=e$，则 $G=\{e,a^1,a^2,\cdots,a^{n-1}\}$，
  循环群$G=(a)$为$n$阶循环群的充要条件是$a$的阶为$n$。
- 生成元的唯一性问题
  A. 设$G=(a)$，且$a$的阶为无穷， 则$a$与$a^{-1}$均为$G$的生成元；
  B. 设$G=(a)$，且$a$的阶为$n$， 则其生成元为$a^l$， 且$(l,n)=1$，$l>1$。

**循环群的同构：**

- 无穷循环群同构于整数加法群$(Z,+)$；
- 阶为$n$的有限循环群同构于$(Z_n, \oplus)$

**循环群的子群：**

- 循环群的子群仍为循环群
- 若 $G=(a)$ 为无穷循环群，则 $G$ 的子群为$\{e\}$，或为 $H=(a^m)=\{\cdots,a^{-2m},a^{-m},e,a^m,a^{2m},\cdots\}$，且为无限循环子群，从而同构于$G$。
- 若$G=(a)$为$n$阶循环群，且$a$的阶为$n$，则其子群的阶必整除$n$，对$n$的任意因子$m$，必有一个阶为$q=\frac{n}{m}$的子群$H=(a^m)=\{e,a^m,a^{2m},\cdots,a^{(q-1)m}\}$，$n=mq$，即$m\mid n$

## §2.6 子群的陪集

**左（右）陪集：**设$H$为群$G$的子群，$a$为$G$的任一元素，集合$aH$称为子群$H$的一个左陪集，$Ha$称为$H$的一个右陪集。

**陪集的性质：**

- 设$H$为群$G$的子群，$a\in G$，则$aH=H(Ha=H)$的充要条件是$a\in H$。
- 设$H$为群$G$的子群，则$\forall a,b\in G$，$aH=bH$当且仅当$a^{-1}b\in H$。
- 设$H$为群$G$的子群，则$\forall a,b\in G$，$aH=bH$或$aH\cap bH=\emptyset$。
- 设$H$为群$G$的子群，则$\forall a,b\in G$，有$|aH|=|bH|$。
- 设$H$为群$G$的子群， $S_l$为$H$的所有左陪集构成的集族，$S_r$为$H$所有右陪集构成的集族，则有$|S_l|=|S_r|$。
- 设$H$为群$G$的子群，则$H$的所有左陪集构成的集族是$G$的一个划分。

$$G=\bigcup_{a\in G} aH$$

**子集的指数：**设$H$为群$G$的子群，若$H$的所有不同的左陪集的个数为有限数$j$，则称$j$为$H$在$G$中的指数，记为$j=[G:H]$，否则说$H$在$G$中的指数为无穷大。

**Lagrange 定理：设$G$是一个阶为$N$的有限群，$H$为$G$的一个$n$阶子群，则**

$$N = n * [G:H]$$

- 推论 1 有限群中每个元素的阶能整除该有限群的阶。
- 推论 2 若有限群$G$的阶$P$为素数，则$G$是个循环群。
- 推论 3 设$G$是一个$N$阶群，则对$G$的每个元素$a$，都有 $a^N = e$。

## §2.7 正规子群、商群

**群子集：** 设$G$为群，对任意的集合$A$，满足$A \subseteq G$，称$A$为群子集。记为：$2^G = \{A \mid A为G的群子集\}$

**群子集上的乘法：** 对$\forall A, B \in 2^G$，$A \circ B = \{a \circ b \mid a \in A \wedge b \in B\}$则为$2^G$上的二元代数运算。且对$\forall A \in 2^G$，$A^{-1} = \{a^{-1} \mid a \in A\}$，显然若$A$为$G$的子群，则$A^{-1} = A$。

- 设$G$为群，则对$\forall A, B, C \subseteq G$有$(AB)C = A(BC)$，若$H$是$G$的子群，则：

$$HH = H, H^{-1} = H, HH^{-1} = H$$

- 设$A, B$为群$G$的子群，则$AB$是$G$的子群的充要条件是$AB = BA$。

**正规子群：** 设$H$为群$G$的子群，若对$\forall a \in G$，有$aH = Ha$，则称$H$是$G$的正规子群。

**正规子群的证明：**

- $\forall a \in G$，有$aH = Ha$。
- $\forall a \in G$，$aHa^{-1} = H$
- **$\forall a \in G$，$aHa^{-1} \subseteq H$**

**商群：** 设$H$为群$G$的正规子群，$H$的所有左陪集构成的集族$S_l$对群子集乘法形成一个群，称为$G$对$H$的商群，记为$G/H$。

$$(S_l, \circ): aH \circ bH = abH$$

## §2.8 同态基本定理

**同态：** 设$(G_1, \circ)$与$(G_2, *)$为群，若存在映射$\varphi: G_1 \to G_2$， 使得对$\forall a, b \in G_1$有$\varphi(a \circ b) = \varphi(a) * \varphi(b)$则称$\varphi$为$G_1$到$G_2$上的一个同态。

- 满同态：若$\varphi$为满射，记为$G_1 \sim G_2$；
- 单同态：若$\varphi$为单射；
- 同构：若$\varphi$既为满射又为单射，即一一映射。

**同态的性质：**

**定理 1：** 设$(G_1, \circ)$与$(G_2, *)$为群，$\varphi: G_1 \to G_2$的同态，则对$\forall a \in G_1$有：

$$\varphi(e_1) = e_2，\varphi(a^{-1}) = (\varphi(a))^{-1}$$

**定理 2：** 设$(G_1, \circ)$为群，$(G_2, *)$是一个具有二元代数运算的代数系，$\varphi: G_1 \to G_2$的满射，且对$\forall a, b \in G_1$有$\varphi(a \circ b) = \varphi(a) * \varphi(b)$，则$G_2$是群。**（主证可逆）**

**定理 4：** 设$(G_1, \circ)$与$(G_2, *)$为群，$\varphi: G_1 \to G_2$的满同态，则：

1) 若$H$是$G_1$的子群，则$\varphi(H)$是$G_2$的子群；
2) 若$N$是$G_1$的正规子群，则$\varphi(N)$是$G_2$的正规子群；
3) 若$\overline{H}$是$G_2$的子群，则$\varphi(\overline{H})$是$G_1$的子群；
4) 若$\overline{N}$是$G_2$的正规子群，则$\varphi(\overline{N})$是$G_1$的正规子群；

**定理 3：** 设$(G_1, \circ)$与$(G_2, *)$为群，$\varphi: G_1 \to G_2$的满同态，则$\varphi^{-1}(e_2) = \{x | \varphi(x) = e_2, x \in G_1\}$是$G_1$的一个正规子群。

**核、同态象：** 设$(G_1, \circ)$与$(G_2, *)$为群，$\varphi: G_1 \to G_2$的满同态，则$G_1$的正规子群$\varphi^{-1}(e_2)$称为同态$\varphi$的核，记为$Ker\ \varphi$。$\varphi(G_1)$称为$\varphi$下的同态象。

**定理 5：** 设$N$是$G$的正规子群，则有：$G \sim G/N$（自然同态）。若$\varphi$是$G$到$G/N$的同态，则$Ker\ \varphi = N$

**群的同态基本定理：** 设$\varphi: G_1 \to G_2$的满同态，$E = Ker\ \varphi$，则$G_1/E = G_2$。**（证明不作要求）**

**定理 7：** 对于群$G$的任一满同态$\varphi$均可分解成一个自然同态$\gamma$与一个同构$f$的合成。即$\varphi = \gamma \circ f$，并且$f$是唯一的。

## 第 3 章 环和域

**环：** 设$S$为非空集合，$S$中有两个二元代数运算，分别称为加法“$+$”与乘法“$\circ$”，且满足：

1) $(S, +)$是一个 Abel 群；
2) $(S, \circ)$是一个半群；
3) 乘法对加法满足左右分配律

**无零因子环：** 无非零的左零因子，也没有非零的右零因子的环。即对$\forall a, b \in S$，若$ab = 0$，则必有$a = 0$或者$b = 0$。

**定理 1：** 环$S$是无零因子环的充要条件是在$S$中乘法满足消去律，即：

$$若a \neq 0，ab = ac，则b = c；$$

$$若a \neq 0，ba = ca，则b = c；$$

**整环：** 可换无零因子环。

**体：** 若环$S$满足：

1) 至少含有一个非零元素；
2) 非零元素的全体对乘法构成一个群。

**域：** 可换体称为域。注：体和域中没有零因子（因为关于乘法满足消去律）