

近世代数 (抽象代数) 笔记

管清文

2020 年 3 月 7 日

目录

1 基本概念

1.1 代数运算

注意 1 近世代数 (或抽象代数) 的主要内容就是研究所谓**代数系统**, 即带有运算的集合。

定义 2 (映射)

$$A_1 \times A_2 \times \cdots \times A_n \rightarrow D$$

$$(a_1, a_2, \cdots, a_n) \mapsto d = \phi(a_1, a_2, \cdots, a_n) = \overline{(a_1, a_2, \cdots, a_n)}$$

注意 3 判断一个法则 ϕ 是映射的充要条件: (i) 都有象 (ii) 象唯一。

定义 4 (代数运算)

$$A \times B \rightarrow D$$

$$(a, b) \mapsto d = \phi(a, b) = \circ(a, b) = a \circ b$$

注意 5 $A = B$ 时, 对于代数运算 $A \times A \rightarrow D$, $a \circ b$ 和 $b \circ a$ 都有意义, 但不一定相等。

定义 6 (A 的代数运算, 二元运算) 假如 \circ 是一个 $A \times A \rightarrow A$ 的代数运算 (即 $A = B = D$), 我们说集合 A 对于代数运算 \circ 来说是闭的, 也说, \circ 是 A 的**代数运算**或**二元运算**。

1.2 运算律

定义 7 (结合率) 我们说, 一个集合 A 的代数运算 \circ 满足结合律, 假如对于 A 的任何三个元素 a, b, c 来说都有

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

定义 8 假如对于 A 的 n ($n \geq 2$) 个固定的元素 a_1, a_2, \cdots, a_n 来说, 所有的加括号方式 $\pi(a_1 \circ a_2 \circ \cdots \circ a_n)$ 都相等, 我们就把这些步骤可以得到的唯一的结果, 用 $a_1 \circ a_2 \circ \cdots \circ a_n$ 来表示。

定理 9 若 A 的代数运算 \circ 满足结合律, 则对于 A 的任意 n ($n \geq 2$) 个元素 a_1, a_2, \cdots, a_n 来说, 对于任意的加括号的方法 π , $\pi(a_1 \circ a_2 \circ \cdots \circ a_n)$ 都相等, $a_1 \circ a_2 \circ \cdots \circ a_n$ 也就总有意义。

定义 10 (交换律) A 上的二元运算 \circ , $a \circ b = b \circ a$ (a 与 b 可交换) $\forall a, b \in A$ 成立, 则称 \circ 满足**交换律**。

定理 11 若 A 上的二元运算 \circ 满足结合律与交换律, 则 $a_1 \circ a_2 \circ \cdots \circ a_n$ 可以任意交换顺序。

定义 12 (分配率) \odot 和 \oplus 都是 A 上的二元运算,

i) 若 $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$, $\forall a, b, c$, 则称 \odot 和 \oplus 满足**第一分配率**。

ii) 若 $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$, $\forall a, b, c$, 则称 \odot 和 \oplus 满足**第二分配率**。

定理 13 若 A 上的二元运算 \oplus 满足结合律, \odot 和 \oplus 满足第一分配率, 则

$$a \odot (b_1 \oplus b_2 \oplus \cdots \oplus b_n) = (a \odot b_1) \oplus (a \odot b_2) \oplus \cdots \oplus (a \odot b_n)$$

定理 14 若 A 上的二元运算 \oplus 满足结合律, \odot 和 \oplus 满足第二分配率, 则

$$(a_1 \oplus a_2 \oplus \cdots \oplus a_n) \odot b = (a_1 \odot b) \oplus (a_2 \odot b) \oplus \cdots \oplus (a_n \odot b)$$

1.3 同态

定义 15 (满射) 映射 $\phi: A \rightarrow \bar{A}$ 被称为**满射**, 如果 $\forall \bar{a} \in \bar{A}, \exists a \in A$ s.t. $\bar{a} = \phi(a)$. (ϕ^{-1} 都有象)

定义 16 (单射) 映射 $\phi: A \rightarrow \bar{A}$ 被称为**单射**, 如果 $\forall a, b \in A, a \neq b \Rightarrow \phi(a) \neq \phi(b)$. (ϕ^{-1} 象唯一)

定义 17 (一一映射) 既是满射又是单射.

注意 18 (一一映射判别) (i) 是映射 (都有象、象唯一) (ii) 满的 (iii) 单的.

定义 19 (变换) 从 A 到 A 的映射 $\tau: A \rightarrow A, a \mapsto \tau(a) = a^\tau$ 叫 A 上的变换.

- 如果 τ 是满的, 则称为**满变换**.
- 如果 τ 是单的, 则称为**单变换**.
- 如果 τ 是一一的, 则称为**一一变换**.

定义 20 (同态映射) 对于 $\phi: A \rightarrow \bar{A}$, A 上有二元运算 \circ , \bar{A} 上有二元运算 $\bar{\circ}$. 如果 $\overline{\phi(a) \circ \phi(b)} = \phi(a \circ b)$, 则称 ϕ 是 A 到 \bar{A} 的同态映射.

注意 21 (同态映射判别) (i) 是映射 (都有象、象唯一) (ii) $\overline{\phi(a) \circ \phi(b)} = \phi(a \circ b)$

定义 22 (同态满射、同态) 如果 A 到 \bar{A} 存在 一个同态映射 ϕ , 且它是满的, 则称 A 与 \bar{A} (关于 \circ 与 $\bar{\circ}$ 来说) **同态**. 称这个映射是一个**同态满射**.

注意 23 (同态满射判别) (i) 是映射 (都有象、象唯一) (ii) 同态 (iii) 满

定义 24 (同构映射、同构) 如果 A 到 \bar{A} 存在 一个同态映射 ϕ , 且它是既是满的又是单的 (一一的), 则称 A 与 \bar{A} (关于 \circ 与 $\bar{\circ}$) **同构**, 记为 $A \cong \bar{A}$. 称这个映射是一个 (关于 \circ 与 $\bar{\circ}$ 的) **同构映射** (简称同构).

注意 25 (同构映射判别) (i) 是映射 (都有象、象唯一) (ii) 同态 (iii) 满 (iv) 单

定理 26 假定对于代数运算 \circ 和 $\bar{\circ}$ 来说, A 与 \bar{A} 同态, 那么

- 若 \circ 满足结合律, $\bar{\circ}$ 也满足结合律;
- 若 \circ 满足交换律, $\bar{\circ}$ 也满足交换律.

定理 27 \odot 和 \oplus 是 A 的两个代数运算, $\bar{\odot}$ 和 $\bar{\oplus}$ 是 \bar{A} 的两个代数运算, 有 ϕ 既是 A 与 \bar{A} 的关于 \odot 和 $\bar{\odot}$ 的同态满射, ϕ 也是 A 与 \bar{A} 的关于 \oplus 和 $\bar{\oplus}$ 的同态满射, 则

- 若 \odot 和 \oplus 满足第一分配率, 则 $\bar{\odot}$ 和 $\bar{\oplus}$ 也满足第一分配率.
- 若 \odot 和 \oplus 满足第二分配率, 则 $\bar{\odot}$ 和 $\bar{\oplus}$ 也满足第二分配率.

定义 28 (自同构) 对于 \circ 和 $\bar{\circ}$ 来说的一个 A 与 A 之间的 同构映射 叫做一个对于 \circ 来说的 A 的**自同构**.

1.4 等价关系与集合分类

定义 29 (关系[Relation]) $R: A \times A \rightarrow D = \{\text{对}, \text{错}\}$, 若 $R(a, b) = \text{对}$, 称 (a, b) 满足关系 R , 记为 $a R b$.

定义 30 (等价关系) 如果 \sim 是 A 的元素间的关系, 满足

- 自反性, $\forall a \in A, a \sim a$.
- 对称性, $\forall a, b \in A$, 若 $a \sim b$, 则 $b \sim a$.
- 传递性, $\forall a, b, c \in A$, 若 $a \sim b, b \sim c$, 则 $a \sim c$.

则称 \sim 为等价关系.

定义 31 (集合分类、划分) 集合 A 分成若干子集, 满足 (i) 每个元素属于都某子集 (ii) 每个元素只属于某子集. 这些类的全体叫做**集合 A 的一个分类**.

$$A = A_1 \cup A_2 \cup \cdots \cup A_n, A_i \cap A_j = \emptyset, i \neq j$$

定理 32 集合上的一个分类, 确定一个集合的元素之间的等价关系.

定理 33 集合上的一个等价关系, 确定一个集合的分类.

定义 34 (模 n 的剩余类) $\{[0], [1], \dots, [n-1]\}$, $[i] = \{kn + i \mid k \in \mathbb{Z}\}$

2 群论

2.1 群的定义和性质

注意 35 群是一个代数系统 (定义代数运算的集合), 其中群里只有一个代数运算. 便利起见 $\phi(a, b) = a \circ b$ 写成 ab

定义 36 (群[Group]的第一定义) 在集合 $G \neq \emptyset$ 上规定一个叫做乘法的 代数运算. 这个代数系统被称为群, 如果

- I 乘法封闭, $\forall a, b \in G, ab \in G$
- II 乘法结合, $\forall a, b, c \in G, (ab)c = a(bc)$
- III $\forall a, b \in G, ax = b, ya = b$ 在 G 中都有解.

注意 37 (乘法) 以后提到乘法, 都是指某个集合 A 上的代数运算 $A \times A \rightarrow A$, 自然要求 I(乘法封闭).

定理 38 (左单位元) 对于群 G 中至少有一个元 e , 叫做 G 的一个左单位元, 使得 $\forall a \in G$ 都有 $ea = a$.

定理 39 (左逆元) 对于群 G 中的任何一个元素 a , 在 G 中存在一个元 a^{-1} , 叫做 a 的左逆元, 能让 $a^{-1}a = e$.

定义 40 (群[Group]的第二定义) 在集合 $G \neq \emptyset$ 上规定乘法. 这个代数系统被称为群, 如果

- I 乘法封闭
- II 乘法结合
- IV 左单位元: $\exists e \in G$ 使 $ea = a$ 对 $\forall a \in G$ 都成立.
- V 左逆元: $\forall a \in G, \exists a^{-1}$ 使 $a^{-1}a = e$.

定义 41 (群的阶) 如果 $|G|$ 有限, 称其为有限群, 称他的阶是 G 的元素个数.

如果 G 中有无穷多个元素, 称其为无限群, 称他的阶无限.

定义 42 (交换群、Abel 群) 群中交换律不一定成立, 如果乘法满足交换律 ($\forall a, b \in G, ab = ba$), 则称之为交换群 (Abel 群).

定理 43 (单位元) 在一个群 G 里存在且只存在一个元 e , 使得 $ea = ae = a$ 对于 $\forall a \in G$ 成立. 这个元素被称为群 G 的单位元.

定理 44 (逆元) 对于群 G 的任意一个元素 a 来说, 有且只有一个元素 a^{-1} , 使 $a^{-1}a = aa^{-1} = e$. 这个元素被称为 a 的逆元, 或者简称逆.

注意 45 证明 a^{-1} 是 a 的逆的方法: $a^{-1}a = e$ 或者 $aa^{-1} = e$

定义 46 规定 $a^n = \underbrace{aa \cdots a}_{n\uparrow}, a^0 = e, a^{-n} = (a^{-1})^n, n \in \mathbb{Z}^+$

定理 47 $a^n a^m = a^{n+m}, (a^n)^m, n, m \in \mathbb{Z}$ (灰色: 它说明了 $(a^{-1})^{-1} = a$)

命题 48 (乘积的逆等于逆的乘积) $\forall a, b \in G, (ab^{-1})^{-1} = ba^{-1}$

定义 49 (元素的阶) 在一个群 G 中, 使得 $a^n = e$ 的最小正整数, 叫做 a 的阶. 若这样的 n 不存在, 称 a 是无穷阶的, 或者叫 a 的阶是无穷.

定理 50 假定群的元 a 的阶是 n , 则 a^r 的阶是 $\frac{n}{\gcd(r, n)}$.

定理 51 (III'[消去律]) 群的乘法满足: $ax = ax' \Rightarrow x = x', ya = y'a \Rightarrow y = y'$

推论 52 在群里, $ax = b$ 和 $ya = b$ 都有唯一解.

定理 53 (有限群的另一定义) 一个带有乘法的 有限集合 $G \neq \emptyset$, 若满足 I、II、III', 则 G 是一个群.

2.2 群的同态

定理 54 G 与 \bar{G} 关于他们的乘法同态, 则 G 是群 $\Rightarrow \bar{G}$ 也是群.

定理 55 假定 G 和 \bar{G} 是两个群, 在 G 到 \bar{G} 的一个同态满射之下, G 的单位元 e 的象是 \bar{G} 的单位元, G 的元 a 的逆元 a^{-1} 的象是 a 的象的逆元 ($\overline{a^{-1}} = \bar{a}^{-1}$).

注意 56 总结下来, 如果 A 与 \bar{A} 同态, 那么前者有什么后面就也有什么:

- 前面有结合, 后面就也有结合
- 前面有交换, 后面就也有交换
- 前面有分配, 后面就也有分配
- 前面是群, 后面就也是群

定理 57 G 与 \bar{G} 关于他们的乘法同构, 则 G 是群 $\Leftrightarrow \bar{G}$ 是群.

2.3 变换群

定义 58 (变换的乘法) $\tau_1 \tau_2 : a \mapsto (a^{\tau_1})^{\tau_2}$

定理 59 (变换乘法结合) $(\tau_1 \tau_2) \tau_3 = \tau_1 (\tau_2 \tau_3)$

定理 60 G 是集合 A 的若干变换构成的集合, 如果 G 基于变换的乘法做成一个群, 则 G 中的变换一定是一一变换.

定义 61 (变换群) 如果一个集合 A 的若干 一一变换 对于变换的乘法能够做成一个群, 则称这个群为 A 的一个变换群.

定理 62 一个集合 A 上的所有一一变换做成一个变换群 G .

定理 63 任何一个群都与一个变换群同构.

定理 64 一个变换群的单位元一定是恒等变换.

2.4 置换群

定义 65 (置换) 有限集合 上的 一一变换 叫做置换, 一般用 π 表示.

定义 66 (置换群) 有限集合上的若干置换做成的群叫置换群.

定义 67 (对称群) 一个 n 元集合 $A = \{a_1, a_2, \dots, a_n\}$ 上的所有置换 (有 $n!$ 个) 做成的群叫做 n 次对称群, 用 S_n 来表示.

定理 68

$$\left. \begin{aligned} \pi_1 &= \begin{pmatrix} j_1 & \cdots & j_k & j_{k+1} & \cdots & j_n \\ j_1^{(1)} & \cdots & j_k^{(1)} & j_{k+1} & \cdots & j_n \end{pmatrix} \\ \pi_2 &= \begin{pmatrix} j_1 & \cdots & j_k & j_{k+1} & \cdots & j_n \\ j_1 & \cdots & j_k & j_{k+1}^{(2)} & \cdots & j_n^{(2)} \end{pmatrix} \end{aligned} \right\} \Rightarrow \pi_1 \pi_2 = \begin{pmatrix} j_1 & \cdots & j_k & j_{k+1} & \cdots & j_n \\ j_1^{(1)} & \cdots & j_k^{(1)} & j_{k+1}^{(2)} & \cdots & j_n^{(2)} \end{pmatrix}$$

定义 69 (k -循环置换) 如果 S_n 中的置换满足 a_{i_1} 的象是 a_{i_2} , a_{i_2} 的象是 a_{i_3} , \dots , $a_{i_{k-1}}$ 的象是 a_{i_k} , a_{i_k} 的象是 a_{i_1} , 其他元素, 如果还有的话, 象是不变的, 则称之为 k -循环置换. 用 $(i_1 i_2 i_3 \cdots i_{k-1} i_k)$ 或 $(i_2 i_3 \cdots i_{k-1} i_k i_1)$ 或 \cdots 或 $(i_k i_1 i_2 i_3 \cdots i_{k-1})$ 来表示.

定理 70 $(i_1 i_2 \cdots i_k)^{-1} = (i_k \cdots i_2 i_1)$.

定理 71 k -循环置换的阶是 k .

定理 72 任何一个置换都可以写成若干没有共同数字的循环置换的乘积.

定理 73 两个没有共同数字的循环置换可以交换.

定理 74 任何一个有限群都与一个置换群同构.

2.5 循环群

定义 75 (循环群) 若一个群 G 的每一个元都是 G 的某一固定元 a 的乘方, 我们就称 G 是一个循环群, a 是 G 的一个生成元, 并记 $G = \langle a \rangle$, 且说 G 是由元 a 生成的.

定义 76 (\mathbb{Z}_n [模 n 的剩余类加群]) G 包含所有模 n 的剩余类, $G = \{[0], [1], \dots, [n-1]\}$, 定义乘法 (叫做加法) $[a] + [b] = [a + b]$, 可以证明 $(G, +)$ 做成一个群, 叫做模 n 的剩余类加群.

定理 77 假定 G 是由 a 生成的循环群, 则 G 的构造可以完全由 a 的阶来决定:

- 如果 a 的阶无限, 则 $G \cong \mathbb{Z}$.
- 如果 a 的阶为 n , 则 $G \cong \mathbb{Z}_n$. ! 灰色 (自然 $|G| = n$, 或者说 $|(a)| = n$) 灰色!

定理 78 一个循环群一定是交换群.

定理 79 a 生成一个阶是 n 的循环群 G , 则 a^r 也生成 G , 如果 $\gcd(r, n) = 1$.

定理 80 G 是循环群, 且 G 与 \bar{G} 同态, 则 \bar{G} 也是循环群.

定理 81 G 是无限阶循环群, \bar{G} 是任何循环群, 则 G 与 \bar{G} 不同态.

2.6 子群

定义 82 (子群) 如果一个群 G 的一个子集 H 关于群 G 的乘法也能做成一个群, 则称 H 为 G 的一个子群.

定理 83 一个群 G 的一个非空子集 H 做成 G 的子群, 当且仅当

- (i) $a, b \in H \Rightarrow ab \in H$
- (ii) $a \in H \Rightarrow a^{-1} \in H$

推论 84 若 H 是 G 的子群, 则, H 的单位元就是 G 的单位元, a 在 H 中的逆就是 a 的 G 中的逆.

定理 85 一个群 G 的一个非空子集 H 做成 G 的子群, 当且仅当 (iii) $a, b \in H \Rightarrow ab^{-1} \in H$

定理 86 一个群 G 的一个非空 有限 子集 H 做成 G 的子群, 当且仅当 (i) $a, b \in H \Rightarrow ab \in H$

注意 87 (验证非空集合是群的方法) (1) I, II, III (2) I、II、IV、V (3) 有限集: I, II, III' (4) 子群: (i), (ii) (5) 子群: (iii) (6) 有限子群: (i)

定义 88 (生成子群) 对于群 G 的非空子集 S , 包含 S 的最小子群, 被称为由 S 生成的子群, 记为 $\langle S \rangle$.

定理 89 $S = \{a\}$ 时, $\langle S \rangle = \langle a \rangle$.

命题 90 群 G 的两个子群的交集也是 G 的子群.

命题 91 循环群的子群也是循环群.

命题 92 H 是群 G 的一个非空子集, 且 H 的每个元素的阶都有限, 则 H 做成子群的充要条件是 (i) $a, b \in H \Rightarrow ab \in H$.

2.7 子群的陪集

定义 93 群 G , 子群 H , 规定 G 上的关系 $\sim: a \sim b \Leftrightarrow ab^{-1} \in H$

定理 94 上面规定的关系 \sim 是等价关系.

定义 95 (右陪集) 由上述等价关系确定集合的分类叫做 H 的右陪集.

定理 96 包含元 a 的右陪集 $= Ha = \{ha \mid h \in H\}$

定义 97 群 G , 子群 H , 规定 G 上的关系 $\sim': a \sim' b \Leftrightarrow b^{-1}a \in H$. 可以证明 \sim' 是等价关系.

定义 98 (左陪集) 由上述等价关系 $\sim': a \sim' b \Leftrightarrow b^{-1}a \in H$, 确定集合的分类叫做 H 的左陪集, 包含元 a 的左陪集可以用 $aH = \{ah \mid h \in H\}$ 表示.

定理 99 一个子群的右陪集与左陪集个数相等: 个数或者都是无穷大, 或者都有限且相等.

定义 100 (指数) 一个群 G 的一个子群 H 的右陪集 (或左陪集) 的个数叫做 H 在 G 里的指数.

定理 101 右陪集所含元素的个数等于子群 H 所含元素的个数.

定理 102 H 是一个有限群 G 的子群, 那么 H 的阶 n 和他在 G 中的指数 j 都能整除 G 的阶 N , 并且 $N = nj$

定理 103 (元素的阶整除群的阶) 一个有限群 G 的任何一个元 a 的阶能够整除 G 的阶 $|G|$.

注意 104 待证明: 阶是 n 的元素生成的循环子群的阶是 n .

命题 105 阶是素数的群一定是循环群.

命题 106 阶是 p^m 的群 (p 是素数) 一定包含一个阶是 p 的子群.

命题 107 若我们把同构的群看做一样的, 一共只存在两个阶是 4 的群, 它们都是交换群.

命题 108 有限非交换群至少有 6 个元素.

2.8 不变子群、商群

定义 109 (不变子群) 群 G 的子群 N 叫做 G 的不变子群, 如果 $\forall a \in G$, 有 $Na = aN$. 一个不变子群 N 的一个左 (或右) 陪集叫做 N 的一个陪集.

定义 110 $S_1, S_2, \dots, S_m \subseteq$ 群 G , 规定子集的乘法 $S_1 S_2 \cdots S_m = \{s_1 s_2 \cdots s_m \mid s_i \in S_i\}$. 可以证明这个乘法满足结合律.

定理 111 已知一个群 G 有一个子群 N , N 是不变子群的充要条件是 $aNa^{-1} = N, \forall a \in G$.

定理 112 已知一个群 G 有一个子群 N , N 是不变子群的充要条件是 $a \in G, n \in N \Rightarrow ana^{-1} \in N$.

定理 113 如果 N 刚好包含 G 的所有具有以下性质的元 n ,

$$na = an, \forall a \in G$$

则 N 是 G 的不变子群. 我们称这个不变子群是 G 的中心.

定理 114 N 是群 G 的不变子群, 在其陪集 $\{aN, bN, cN, \dots\}$ 上定义的乘法 $(xN, yN) \mapsto (xy)N$, 则这个乘法是此陪集的二元运算, 且此陪集对于上面规定的乘法来说构成一个群.

定义 115 (商群) 一个群 G 的一个不变子群 N 的所有陪集关于陪集的乘法做成的群叫做 G 的商群, 用 G/N 表示.

定理 116 对于有限群, $|G/N| = \frac{|G|}{|N|}$.

命题 117 两个不变子群的交集还是不变子群.

命题 118 H 是 G 的子群, N 是 G 的不变子群, 则 HN 是 G 的子群.

2.9 同态与不变子群

定理 119 一个群 G 与它的商群 G/N 同态.

定义 120 (核) ϕ 是群 G 到群 \bar{G} 的一个同态满射, \bar{G} 的单位元 \bar{e} 在 ϕ 之下的所有原象做成的 G 的子集叫做 ϕ 的核.

定理 121 G 和 \bar{G} 是两个群, 且 G 与 \bar{G} 同态, 则这个同态满射的核 N 是 G 的一个不变子群, 且 $G/N \cong \bar{G}$.

注意 122 一个群只和“相当于”它的商群同态

定义 123 ϕ 是 $A \rightarrow \bar{A}$ 的满射, 取 $S \subseteq A$, 定义 S 的象是 S 中所有元素的象做成的集合. 取 $\bar{S} \subseteq \bar{A}$, 定义 \bar{S} 的原象是 \bar{S} 中所有元素的原象做成的集合.

定理 124 G 和 \bar{G} 是两个群, 且 G 与 \bar{G} 同态, 则在这个同态满射之下:

- (1) G 的一个子群 H 的象 \bar{H} 也是 \bar{G} 的一个子群.
- (2) G 的一个不变子群 N 的象 \bar{N} 也是 \bar{G} 的一个不变子群.
- (1') \bar{G} 的一个子群 \bar{H} 的原象 H 也是 G 的一个子群.
- (2') \bar{G} 的一个不变子群 \bar{N} 的原象 N 也是 G 的一个不变子群.

注意 125 这也体现了同态的性质, 前面有的后面也有!

命题 126 假定群 G 与群 \bar{G} 同态, \bar{N} 是 \bar{G} 的不变子群, N 是 \bar{N} 的逆象, 则 $G/N \sim \bar{G}/\bar{N}$.

命题 127 假定群 G 与 \bar{G} 是两个有限循环群, 他们的阶各是 m 和 n , 则 G 与 \bar{G} 同态 $\Leftrightarrow n \mid m$

命题 128 假定群 G 是一个循环群, N 是 G 的一个子群, 则 G/N 也是循环群.

3 环与域

定义 129 (加群) 一个交换群叫做一个加群, 如果我们把这个群的代数运算称为加法, 并且用符号 $+$ 表示.

定义 130 n 的元的和 $a_1 + a_2 + \cdots + a_n$ 用符号 $\sum_{i=1}^n a_i$ 来表示.

定义 131 n 个 a 的和 $\sum_{i=1}^n a$ 我们用 na 表示.

定义 132 (零元) 加群唯一的单位元用 0 来表示, 并且把它叫做零元.

定义 133 (负元) 元 a 的唯一的逆元我们用 $-a$ 来表示, 并且把它叫做 a 的负元. $a + (-b)$ 我们简写成 $a - b$.

定理 134 加群满足以下运算规则

- (1) $0 + a = a + 0 = a$
- (2) $-a + a = a - a = 0$
- (3) $-(-a) = a$
- (4: 移项) $a + c = b \Leftrightarrow c = b - a$
- (4) $-(a + b) = -a - b, -(a - b) = -a + b$
- (5) $ma + na = (m + n)a, m(na) = (mn)a, n(a + b) = na + nb, \forall m, n \in \mathbb{Z}^+$

注意 135 非空子集 S 做成子群的充要条件变成了

- (i) $a, b \in S \Rightarrow a + b \in S$ (ii) $a \in S \Rightarrow -a \in S$

- 或者 (iii) $a, b \in S \Rightarrow a - b \in S$.

定义 136 (环) 一个集合 R 叫做一个环, 如果

1. R 是一个加群: R 关于一个叫做加法的代数运算做成一个交换群.
2. R 对于另一个叫做乘法的代数运算是封闭的.
3. R 关于乘法结合
4. 分配率: $a(b + c) = bc + ac, (a + b)c = ac + bc$

注意 137 (环的判别) 判断一个代数系统是环的条件:

- (i) 加法 (构成交换群): I. 加法封闭 II 加法结合 IV 有零元 V 负元 X 加法交换
- (ii) 乘法: I. 乘法封闭 II 乘法结合
- (iii) 两种运算的关系: 分配率

定理 138 环还满足以下运算规则

- (7) $(a - b)c = ac - bc, c(a - b) = ca - cb$
- (8) $0a = a0 = 0$
- (9) $(-a)b = a(-b) = -(ab)$
- (10) $(-a)(-b) = ab$
- (11) $a(b_1 + b_2 + \cdots + b_n) = ab_1 + ab_2 + \cdots + ab_n, (b_1 + b_2 + \cdots + b_n)a = b_1a + b_2a + \cdots + b_na$
- (12) $\left(\sum_{i=1}^m a_i\right)\left(\sum_{j=1}^n b_j\right) = \sum_{a=1}^m \sum_{b=1}^n a_i b_j$

$$\begin{aligned} (a_1 + a_2 + \cdots + a_m)(b_1 + b_2 + \cdots + b_n) &= a_1b_1 + a_1b_2 + \cdots + a_1b_n \\ &\quad + a_2b_1 + a_2b_2 + \cdots + a_2b_n \\ &\quad + \cdots \\ &\quad + a_mb_1 + a_mb_2 + \cdots + a_mb_n \end{aligned}$$

- (13) $(na)b = a(nb) = n(ab), n \in \mathbb{Z}^+$

- (14) 规定 $a^n = \underbrace{aa \cdots a}_{n \uparrow}, n \in \mathbb{Z}^+, \text{ 则 } a^m a^n = a^{m+n}, (a^m)^n = a^{mn}$

3.1 交换律、单位元、零因子、整环

定义 139 (交换环) 一个环 R 叫做交换环, 如果 $ab = ba, \forall a, b \in R$.

命题 140 在一个交换环中 $(ab)^n = a^n b^n$.

定义 141 (单位元) 对于环 R , 如果 $ea = ae = a, \forall a \in R$, 则称 e 是环 R 的单位元. 一般, 一个环未必有单位元.

命题 142 一个环如果有单位元, 则唯一. 用 1 来表示.

定义 143 (整数环) 整数关于普通加法和乘法构成的环.

定义 144 (逆元) 若 $ba = 1$, 则称 b 为 a 的左逆元. 若 $ba = ab = 1$, 则称 b 为 a 的逆元.

命题 145 如果 a 有逆元, 则唯一.

命题 146 如果 a 有逆元, 则规定 $a^{-m} = (a^{-1})^m, a^0 = 1$. 则 $a^m a^n = a^{m+n}, (a^m)^n = a^{mn}, \forall m, n \in \mathbb{Z}$.

命题 147 (模 n 的剩余类环) $R = \{[0], [1], \cdots, [n-1]\}$, 加法: $[a] + [b] = [a + b]$, 乘法: $[a][b] = [ab]$ 做成一个交换环, 被称为模 n 的剩余类环, 零元 $0 = [0]$, 单位元 $1 = [1]$.

命题 148 $ab = 0 \Rightarrow a = 0$ 或者 $b = 0$ 在环里不一定对.

定义 149 (零因子) 在一个环 R 中, 若 $a \neq 0, b \neq 0$ 但 $ab = 0$, 则称 a 是 R 的左零因子, b 是 R 的右零因子.

注意 150 左零因子不一定是右零因子. 但是如果有左零因子, 就一定有右零因子. 如果 R 是交换环, 则左零因子一定是右零因子.

定理 151 在一个没有零因子的环里, 两个消去律都成立.

1. $a \neq 0, ab = ac \Rightarrow b = c$

2. $a \neq 0, ba = ca \Rightarrow b = c$

反过来, 在一个环里如果 有一个 消去律成立, 那么这个环没有零因子.

推论 152 在一个环 R 中如果有一个消去律成立, 那么另一个消去律也成立.

定义 153 (整环) 一个环 R 叫做一个整环, 如果

1. 乘法适合交换律: $ab = ba$.

2. R 有单位元 1 : $1a = a1 = a$.

3. R 没有零因子: $ab = 0 \Rightarrow a = 0$ 或 $b = 0$

命题 154 整数环是一个整环.