# 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)**

$$A_1 \times A_2 \times \cdots \times A_n \to D$$
$$(a_1, a_2, \cdots, a_n) \mapsto d = \phi(a_1, a_2, \cdots, a_n) = \overline{(a_1, a_2, \cdots, a_n)}$$

**注意 3** 判断一个法则 $\phi$ 是映射的充要条件: (i) 都有象 (ii) 象唯一.

**定义 4 (代数运算)**

$$A \times B \to D$$
$$(a, b) \mapsto d = \phi(a, b) = \circ(a, b) = a \circ b$$

**注意 5** $A = B$ 时, 对于代数运算 $A \times A \to D$, $a \circ b$ 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 $A \times A \to A$ 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 $\pi$, $\pi(a_1 \circ a_2 \circ \cdots \circ a_n)$ 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 $\phi : A \to \bar{A}$ 被称为**满射**, 如果 $\forall \hat{a} \in \bar{A}, \exists a \in A$ s.t. $\bar{a} = \hat{a}$. ($\phi^{-1}$ 都有象)

**定义 16 (单射)** 映射 $\phi : A \to \bar{A}$ 被称为**单射**, 如果 $\forall a, b \in A, a \neq b \Rightarrow \bar{a} \neq \bar{b}$. ($\phi^{-1}$ 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 $\tau : A \to A, a \mapsto \tau(a) = a^\tau$ 叫 $A$ 上的变换.

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

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

**定义 22 (同态满射、同态)** 如果 $A$ 到 $\bar{A}$ $\boxed{\text{存在}}$ 一个同态映射 $\phi$, 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 $\bar{A}$ $\boxed{\text{存在}}$ 一个同态映射 $\phi$, 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

i) 若 $\circ$ 满足结合律, $\bar{\circ}$ 也满足结合律;
ii) 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 $\phi$ 既是 $A$ 与 $\bar{A}$ 的关于 $\odot$ 和 $\bar{\odot}$ 的同态满射, $\phi$ 也是 $A$ 与 $\bar{A}$ 的关于 $\oplus$ 和 $\bar{\oplus}$ 的同态满射, 则

i) 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.
ii) 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 $\circ$ 来说的一个 $A$ 与 $A$ 之间的 $\boxed{\text{同构映射}}$ 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])** $R : A \times A \to D = \{\text{对}, \text{错}\}$, 若 $R(a, b) =$ 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

i) 自反性, $\forall a \in A, a \sim a$.
ii) 对称性, $\forall a, b \in A$, 若 $a \sim b$, 则 $b \sim a$.
iii) 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)** $\{[0],[1],\cdots,[n-1]\}$, $[i]=\{kn+i \mid k\in\mathbb{Z}\}$

# 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 $\boxed{\text{代数运算}}$. 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 $A\times A\to A$, 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 $a^n=\underbrace{aa\cdots a}_{n\text{个}}, a^0=e, a^{-n}=(a^{-1})^n, n\in\mathbb{Z}^+$

**定理 47** $a^na^m=a^{n+m},(a^n)^m, n,m\in\mathbb{Z}$

**定理 48** $\forall a,b\in G,(ab^{-1})^{-1}=ba^{-1}$

**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 $\dfrac{n}{\gcd(r,n)}$.

**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 $\boxed{\text{有限集合}}$ $G \neq \emptyset$, 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 $\boxed{\text{一一变换}}$ 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)** $\boxed{\text{有限集合}}$ 上的 $\boxed{\text{一一变换}}$ 叫做**置换**, 一般用 $\pi$ 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 $A = \{a_1, a_2, \cdots, a_n\}$ 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 $a_{i_3}$，$\cdots$，$a_{i_{k-1}}$ 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** $(i_1\, i_2\, \cdots_k)^{-1} = (i_k\, \cdots\, i_2\, i_1)$.

**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 $G = (a)$, 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，$G = \{[0], [1], \cdots, [n-1]\}$, 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 $G \cong \mathbb{Z}_n$.

**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 $\gcd(r, d) = 1$.

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

### 2.6 子群

**定义 81 (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 82** 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 83** 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 84** 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 85** 一个群 $G$ 的一个非空 $\boxed{\text{有限}}$ 子集 $H$ 做成 $G$ 的子群，当且仅当 (i) $a, b \in H \Rightarrow ab \in H$

**注意 86 (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 87 (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 $(S)$.

**定理 88** $S = \{a\}$ 时, $(S) = (a)$.

**定义 89** 群 $G$, 子群 $H$, 规定 $G$ 上的关系 $\sim$: $a \sim b \Leftrightarrow ab^{-1} \in H$

**定理 90** 上面规定的关系 $\sim$ 是等价关系.

**定义 91 (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 92** 包含元 $a$ 的右陪集 $= Ha = \{ha \mid h \in H\}$

**定义 93** 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 $'$ 是等价关系.

**定义 94 (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 95** 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 96 (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 97** 右陪集所含元素的个数等于子群 $H$ 所含元素的个数.

**定理 98** $H$ 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 99 (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.

**注意 100** 待证明: 阶是 $n$ 的元素生成的循环子群的阶是 $n$.

**定义 101 (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 102** $S_1, S_2, \cdots, S_m \subseteq$ 群 $G$, 规定子集的乘法 $S_1S_2\cdots S_m = \{s_1s_2\cdots s_m \mid s_i \in S_i\}$. 可以证明这个乘法满足结合律.

**定理 103** 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 104** 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 105** 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 106** $N$ 是群 $G$ 的不变子群, 在其陪集 $\{aN, bN, cN, \cdots\}$ 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 107 (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 108** 对于有限群, $|G/N| = \frac{|G|}{|N|}$.

**定理 109** 一个群 $G$ 与它的商群 $G/N$ 同态.

**定义 110 (核)** $\phi$ 是群 $G$ 到群 $\bar{G}$ 的一个同态满射, $\bar{G}$ 的单位元 $\bar{e}$ 在 $\phi$ 之下的所有原象做成的 $G$ 的子集叫做 $\phi$ 的**核**.

**定理 111** $G$ 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 112** 一个群只和 “相当于” 它的商群同态

**定义 113** $\phi$ 是 $A \to \bar{A}$ 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 114** $G$ 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 115** 这也体现了同态的性质，前面有的后面也有!

# 3 环与域