近世代数 (抽象代数) 笔记

管清文

2020 年 3 月 13 日

目录

性质 (Property) 结果值得一记, 但是没有定理深刻.

注意 (Remark) 涉及到一些结论，更像是非正式的定理.

说明 (Note) 就是注解.

1 基本概念

1.1 代数运算

说明 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)

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

定义 3 (代数运算)

$$
\begin{aligned}
&A \times B \to D \\
&(a, b) \mapsto d = \phi(a, b) = \circ(a, b) = a \circ b
\end{aligned}
$$

定义 4 (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**.

说明 5 (A 的代数运算判别)

A 的代数运算
- 是映射
  - 都有象
  - 象唯一 $\forall a, a', b, b' \in A : a = a', b = b' \Rightarrow a \circ b = a' \circ b'$
- 封闭 $\forall a, b \in A : a \circ b \in A,$

1.2 运算律

定义 6 (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 $(a \circ b) \circ c = a \circ (b \circ c)$

定理 7 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，我们用 $a_1 \circ a_2 \circ \cdots \circ a_n$ 来表示.

定义 8 (交换律) 如果 A 上的代数运算 $\circ$ 满足 $\forall a, b \in A : a \circ b = b \circ a$，则称 $\circ$ 满足**交换律**. 对于 $a, b \in A$, 如果 $a \circ b = b \circ a$, 则称 a, b **可交换**.

定理 9 若 A 上的代数运算 $\circ$ 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 10 (分配率) $\odot$ 和 $\oplus$ 都是 A 上的代数运算,

(1) 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.

(2) 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 11 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

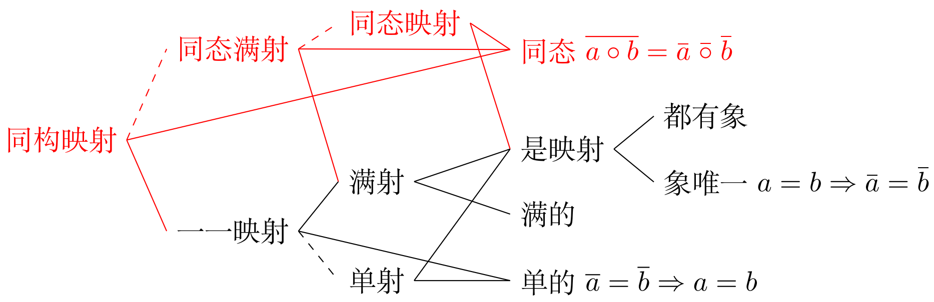
$$a \odot (b_1 \oplus b_2 \oplus \cdots \oplus b_n) = (a \odot b_1) \oplus (a \odot b_2) \oplus \cdots \oplus (a \odot b_n)$$

定理 12 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

说明 13 (映射判别)



定义 14 (变换) 从 A 到 A 的映射 $\tau : A \to A, a \mapsto \tau(a)$ 叫 A **变换**, 我们也用 a^τ 表示 $\tau(a)$. 如果 τ 是满 (单、一一) 的, 则称为**满变换** (**单变换**、**一一变换**).

定义 15 (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 ϕ 是 A 到 $\bar{A}$ 的同态映射.

定义 16 (同态满射、同态) 如果 A 到 $\bar{A}$ $\boxed{\text{存在}}$ 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**.

定义 17 (同构映射、同构) 如果 A 到 $\bar{A}$ $\boxed{\text{存在}}$ 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).

命题 18 同构关系是一个等价关系.

定理 19 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 20 $\odot$ 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

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 21 (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 22 (关系[Relation]) $R : A \times A \to D = \{对, 错\}$, 若 $R(a, b) =$ 对 , 称 (a, b) 满足关系 R, 记为 $a\,R\,b$.

定义 23 (等价关系) 如果 $\sim$ 是 A 的元素间的关系，满足

(1) 自反性, $\forall a \in A, a \sim a$.

(2) 对称性, $\forall a, b \in A$, 若 $a \sim b$, 则 $b \sim a$.

(3) 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 24 (集合分类、划分) 集合 A 分成若干子集，满足 (1) 每个元素属于都某子集 (2) 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 25 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 26 集合上的一个等价关系，确定一个集合的分类.

定义 27 ($\mathbb{Z}_p$[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 28 群是一个代数系统 (定义代数运算的集合), 它只有一个代数运算, 被称为乘法. 便利起见 $\phi(a,b)$ 写成 ab

之前写成 $a \circ b$

定义 29 (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

以后简称乘法

I 乘法封闭, $\forall a, b \in G, ab \in G$

代数运算要求封闭性

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.

定理 30 (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 31 (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 32 (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 33 (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 34 (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 35 (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 36 (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**.

说明 37 证明 a^{-1} 是 a 的逆的方法: $a^{-1}a = e$ 或者 $aa^{-1} = e$ (不用都说明).

性质 38 (乘积的逆等于逆的乘积) $\forall a, b \in G, (ab^{-1})^{-1} = ba^{-1}$

定义 39 规定 $\forall n \in \mathbb{Z}^+ : a^n = \underbrace{aa\cdots a}_{n\text{个}}, a^0 = e, a^{-n} = (a^{-1})^n$

命题 40 $\forall n,m\in\mathbb{Z}: a^n a^m = a^{n+m}, (a^n)^m = a^{mn} \quad (\Rightarrow (a^{-1})^{-1}=a)$

定义 41 (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 42 假定群的元 a 的阶是 n, 则 a^r 的阶是 $\dfrac{n}{\gcd(r,n)}$.

定理 43 (III'[消去律]) 群的乘法满足: $ax=ax' \Rightarrow x=x', ya=y'a \Rightarrow y=y'$

推论 44 在群里, $ax=b$ 和 $ya=b$ 都有唯一解.

定理 45 (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 46 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 47 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 $(\overline{a^{-1}}=\bar{a}^{-1})$.

定理 48 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 49 (变换的乘法) $\tau_1\tau_2 : a\mapsto (a^{\tau_1})^{\tau_2}$

定理 50 (变换乘法结合) $(\tau_1\tau_2)\tau_3=\tau_1(\tau_2\tau_3)$

定理 51 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 52 (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 53 一个集合 A 上的所有一一变换做成一个变换群 G.

定理 54 任何一个群都与一个变换群同构.

定理 55 一个变换群的单位元一定是恒等变换.

2.4 置换群

定义 56 (置换) $\boxed{\text{有限集合}}$ 上的 $\boxed{\text{一一变换}}$ 叫做**置换**, 一般用 π 表示.

定义 57 (置换群) 有限集合上的若干置换做成的群叫**置换群**.

定义 58 (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 59

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

定义 60 (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.

命题 61 $(i_1\, i_2\, \cdots i_k)^{-1} = (i_k\, \cdots\, i_2\, i_1)$.

命题 62 k-循环置换的阶是 k.

命题 63 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.

命题 64 两个没有共同数字的循环置换可以交换.

命题 65 任何一个有限群都与一个置换群同构.

2.5 循环群

定义 66 (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 67 ($\mathbb{Z}_n$[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 68 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 $G \cong \mathbb{Z}_n$.

自然 $|G| = n$, 或者说 $|(a)| = n$

命题 69 一个循环群一定是交换群.

命题 70 a 生成一个阶是 n 的循环群 G, 则 a^r 也生成 G，如果 $\gcd(r, d) = 1$.

命题 71 G 是循环群, 且 G 与 $\bar{G}$ 同态，则 $\bar{G}$ 也是循环群.

命题 72 G 是无限阶循环群, $\bar{G}$ 是任何循环群, 则 G 与 $\bar{G}$ 同态.

2.6 子群

定义 73 (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 74 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 75 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 76 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 77 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) $a, b \in H \Rightarrow ab \in H$

说明 78 (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 79 (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 80 $S=\{a\}$ 时, $(S)=(a)$.

命题 81 群 G 的两个子群的交集也是 G 的子群.

命题 82 循环群的子群也是循环群.

命题 83 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 84 群 G, 子群 H, 规定 G 上的关系 $\sim$: $a\sim b\Leftrightarrow ab^{-1}\in H$

定理 85 上面规定的关系 $\sim$ 是等价关系.

定义 86 (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 87 包含元 a 的右陪集 $=Ha=\{ha\mid h\in H\}$

定义 88 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 89 (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 90 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 91 (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 92 右陪集所含元素的个数等于子群 H 所含元素的个数.

定理 93 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 94 (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 $|G|$.

命题 95 阶是素数的群一定是循环群.

命题 96 阶是 p^m 的群 (p 是素数) 一定包含一个阶是 p 的子群.

命题 97 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 98 有限非交换群至少有 6 个元素.

2.8 不变子群、商群

定义 99 (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 100 $S_1,S_2,\cdots,S_m\subseteq$ 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 101 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 102 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 103 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 104 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 105 (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 106 对于有限群, $|G/N| = \frac{|G|}{|N|}$.

命题 107 两个不变子群的交集还是不变子群.

命题 108 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 109 一个群 G 与它的商群 G/N 同态.

定义 110 (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 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 ϕ 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!

命题 116 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 117 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 118 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

3.1 加群、环的定义

定义 119 (加群) 一个交换群叫做一个的**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 120 (Σ) n 个元的和 $a_1+a_2+\cdots+a_n$ 用符号 $\sum_{i=1}^{n} a_n$ 来表示.

定义 121 n 个 a 的和 $\sum_{i=1}^{n} a$ 我们用 na 表示.

定义 122 (零元) 加群唯一的单位元用 $\mathfrak{o}$ 来表示, 并且把它叫做**零元**.

定义 123 (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 124 加群满足以下运算规则

(1) $\mathfrak{o}+a=a+\mathfrak{o}=a$

(2) $-a+a=a-a=\mathfrak{o}$

(3) $-(-a)=a$

(4: 移项) $a+c=b \Leftrightarrow c=b-a$

(4) $-(a+b)=-a-b, -(a-b)=-a+b$

(5) $ma+na=(m+n)a, m(na)=(mn)a, n(a+b)=na+nb, \forall m,n\in\mathbb{Z}^+$

说明 125 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 126 (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: $a(b+c)=bc+ac, (a+b)c=ac+bc$

定理 127 环还满足以下运算规则

(7) $(a-b)c=ac-bc, c(a-b)=ca-cb$

(8) $\mathfrak{o}a=a\mathfrak{o}=\mathfrak{o}$

(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) $\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right)=\sum_{a=1}^{m}\sum_{b=1}^{n} a_ib_j$

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

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

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

3.2 交换律、单位元、零因子、整环

定义 128 (交换环) 一个环 R 叫做**交换环**, 如果 $ab=ba, \forall a,b\in R$.

命题 129 在一个交换环中 $(ab)^n=a^nb^n$.

定义 130 (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 131 一个环如果有单位元, 则唯一. 用 $\mathbb{1}$ 来表示.

定义 132 (整数环) 整数关于普通加法和乘法构成的环.

定义 133 (逆元) 若 $ba = \mathbb{1}$, 则称 b 为 a 的**左逆元**. 若 $ba = ab = \mathbb{1}$, 则称 b 为 a 的**逆元**.

命题 134 如果 a 有逆元, 则唯一.

命题 135 如果 a 有逆元, 则规定 $a^{-m} = (a^{-1})^m, a^0 = \mathbb{1}$. 则 $a^m a^n = a^{m+n}, (a^m)^n = a^{mn}, \forall m, n \in \mathbb{Z}$.

命题 136 (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 $\mathbb{0} = [0]$, 单位元 $\mathbb{1} = [1]$.

命题 137 $ab = \mathbb{0} \Rightarrow a = \mathbb{0}$ 或者 $b = \mathbb{0}$ 在环里不一定对.

定义 138 (零因子) 在一个环 R 中, 若 $a \neq \mathbb{0}, b \neq \mathbb{0}$ 但 $ab = \mathbb{0}$, 则称 a 是 R 的**左零因子**, b 是 R 的**右零因子**.

注意 139 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 140 在一个没有零因子的环里, 两个消去律都成立.

1. $a \neq \mathbb{0}, ab = ac \Rightarrow b = c$
2. $a \neq \mathbb{0}, ba = ca \Rightarrow b = c$

反过来, 在一个环里如果 $\boxed{\text{有一个}}$ 消去律成立，那么这个环没有零因子.

推论 141 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 142 (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: $\mathbb{1}a = a\mathbb{1} = a$.
3. R 没有零因子: $ab = \mathbb{0} \Rightarrow a = \mathbb{0}$ 或 $b = \mathbb{0}$

命题 143 整数环是一个整环.

命题 144 对于有单位元的环来说, 加法适合交换律是环定义里其他条件的结果.

命题 145 二项式定理 $(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n}b^n$ 在交换环中成立.

3.3 除环、域

命题 146 对于元素个数 ≥ 2 的环, $\mathbb{1} \neq \mathbb{0}$, 且 $\mathbb{0}$ 没有逆元.

定义 147 (除环) 一个环 R 叫做一个**除环**, 如果

1. R 至少含有一个不等于零的元.
2. R 有单位元.
3. R 的任何一个非零元都有逆.

定义 148 (域) 一个交换除环叫做一个**域**.

性质 149 除环没有零因子.

性质 150 除环 R 的所有非零元对于乘法来说做成一个群 R^*, 我们把 R^* 叫做**除环 R 的乘群**.

说明 151 对于一个环 R 来说, 从 R^* 是对于乘法做成一个群, 也能推出 R 是除环.

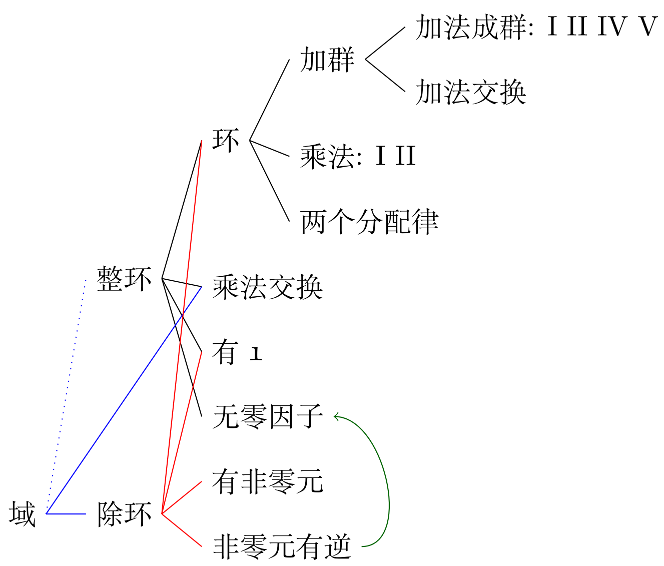
说明 152 在除环 R 中, 方程 $ax=b, ya=b(a\neq 0)$ 都有唯一解, 分别是 $a^{-1}b$ 和 ba^{-1}, 他们未必相等. 在一个域里 $a^{-1}b=ba^{-1}$, 用符号 $\dfrac{b}{a}$ 表示.

性质 153 域满足以下计算法则

1. $\dfrac{a}{b}=\dfrac{c}{d}\Leftrightarrow ad=bc$.
2. $\dfrac{a}{b}+\dfrac{c}{d}=\dfrac{ad+bc}{bd}$.
3. $\dfrac{a}{b}\dfrac{c}{d}=\dfrac{ac}{bd}$.

命题 154 $R=\{(\alpha,\beta)\mid\alpha,\beta\in\mathbb{C}\},(\alpha_1,\beta_1)+(\alpha_2,\beta_2)=(\alpha_1+\alpha_2,\beta_1+\beta_2),(\alpha_1,\beta_1)(\alpha_2,\beta_2)=(\alpha_1\alpha_2-\beta_1\overline{\beta_2})(\alpha_1\beta_2+\beta_1\overline{\alpha_2})$ 做成一个除环, 叫做**四元数除环**, 它不是交换环 (所以不是域).

说明 155 环、整环、域之间的关系:



命题 156 一个至少有两个元且没有零因子的有限环，是一个除环.

3.4 无零因子环的特征

命题 157 对于模 p 的剩余类环 $\mathbb{Z}_p$, p 是素数 $\Leftrightarrow\mathbb{Z}_p$ 做成一个域.

命题 158 在一个环 R 里, 对于加法的阶, 可能有的元素是无限的，有的元素是有限的.

定理 159 在一个无零因子环中, 所有非零元素 R 对于加法的阶都相同: 要么都无限大, 要么都有限且相等.

定义 160 (无零因子环的特征) 在一个无零因子环 R 中, 所有非零元关于加法的阶，叫做 R 的**特征**.

定理 161 如果无零因子环 R 的特征是一个有限整数 n, 则 n 一定是素数.

推论 162 整环、除环以及域的特征或者是无限大，或者是一个素数.

3.5 子环、环的同态

定义 163 (子环) 一个环 R 的非空子集 S 如果对于 R 的代数运算来说也是环 (整环、除环、域), 则称 S 是 R 的一个**子环** (**子整环**、**子除环**、**子域**).

定理 164 若 S 是环 R 的一个非空子集, 则 S 是 R 的子环的充要条件是 $a, b \in S \Rightarrow a - b \in S, ab \in S$.

定理 165 若 S 是整环 R 的一个非空子集, 则 S 是 R 的子整环的充要条件是 $(1) a, b \in S \Rightarrow a - b \in S, ab \in S; (2) \imath \in S$.

定理 166 若 S 是除环 R 的一个非空子集, 则 S 是 R 的子除环的充要条件是 (1) S 有非零元; (2) $a, b \in S \Rightarrow a - b \in S$; (3) $\forall a, b \in S, b \neq 0 \Rightarrow ab^{-1} \in S$.

定理 167 若 S 是域 R 的一个非空子集, 则 S 是 R 的子域的充要条件是 (1) S 有非零元; (2) $a, b \in S \Rightarrow a - b \in S$; (3) $\forall a, b \in S, b \neq 0 \Rightarrow ab^{-1} \in S$.

命题 168 环 R 的可以同每个元交换的元做成一个 j 交换子环 $N = \{n \mid an = na, \forall a \in R\}$, 这个子环称为 R 的中心.

定理 169 若 R 是环, R 到 $\bar{R}$ 有一个满射使得对于两个运算都同态, 则 $\bar{R}$ 也是一个环.

注意 170 总结下来, 如果 A 与 $\bar{A}$ 同态，那么前面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
- 前面是环，后面就也是环

定理 171 若 R 和 $\bar{R}$ 都是环, 且 R 与 $\bar{R}$ 同态, 则

- R 的零元的象是 $\bar{R}$ 的零元.
- R 的元 a 的负元的象是 a 的象的负元 ($\overline{-a} = -\bar{a}$)
- R 是交换环 $\Rightarrow$ $\bar{R}$ 也是交换环
- R 有单位元 $\imath \Rightarrow \bar{R}$ 也有单位元 $\bar{\imath}$, 且 $\bar{\imath}$ 是 $\imath$ 的象.
- R 无零因子 $\not\Rightarrow$ $\bar{R}$ 无零因子
- R 有零因子 $\not\Rightarrow$ $\bar{R}$ 有零因子
- R 是整环 (除环、域) $\not\Rightarrow$ $\bar{R}$ 是整环 (除环、域)

命题 172 若 R 和 $\bar{R}$ 都是环, 且 R 与 $\bar{R}$ 同态, 则

- R 无零因子 $\not\Rightarrow$ $\bar{R}$ 无零因子
- R 有零因子 $\not\Rightarrow$ $\bar{R}$ 有零因子
- R 是整环 (除环、域) $\not\Rightarrow$ $\bar{R}$ 是整环 (除环、域)

命题 173 R 与 $\bar{R}$ 都是环, 且 $R \cong \bar{R}$, 则

- R 无零因子 $\Leftrightarrow$ $\bar{R}$ 无零因子.
- R 有非零元 $\Leftrightarrow$ $\bar{R}$ 有非零元.
- R 非零元有逆 $\Leftrightarrow$ $\bar{R}$ 非零元有逆

定理 174 R 与 $\bar{R}$ 都是环, 且 $R \cong \bar{R}$, 则

- R 是整环 $\Leftrightarrow$ $\bar{R}$ 是整环.
- R 是除环 $\Leftrightarrow$ $\bar{R}$ 是除环.
- R 是域 $\Leftrightarrow$ $\bar{R}$ 是域.

引理 175 集合 A 和 $\bar{A}$ 之间有一个一一映射 ϕ, 并且 A 有加法和乘法, 于是我们可以在 $\bar{A}$ 中规定加法和乘法，使得 A 与 $\bar{A}$ 关于一对加法和一对乘法来说都同构.

定理 176 假定 S 是环 R 的一个子环, S 在 R 中的补集 (R - S) 与另一个环 $\bar{S}$ 没有公共元, 并且 $S \cong \bar{S}$, 那么存在一个与 R 同构的环 $\bar{R}$，且 $\bar{S}$ 是 $\bar{R}$ 的子环.

说明 177

$$\left.\begin{array}{r} \text{环 R} \overset{\text{子环}}{\overline{\qquad}} \text{环 } S \\ \Big\updownarrow \cong_{\phi} \\ ? \underset{\text{子环}}{\overline{\qquad}} \text{环 } \bar{S} \\ \\ (R-S)\cap\bar{S}=\emptyset \end{array}\right\} \Rightarrow \exists \text{ 环 } ?=\bar{R}: \begin{cases} \bar{R}=(R-S)\cup\bar{S} \\ \forall \bar{x},\bar{y}\in\bar{R}: \begin{array}{l} \bar{x}+\bar{y}=\psi(x+y), \bar{x}\bar{y}=\psi(xy), \\ x=\psi^{-1}(\bar{x}), y=\psi^{-1}(\bar{y}) \end{array} \\ R\cong\bar{R}, \psi: x\mapsto \begin{cases} x & x\in R-S \\ \phi(x) & x\in S \end{cases} \end{cases}$$

命题 178 一个除环的中心是一个域.

3.6 多项式环

说明 179 假定 R_0 是一个有单位元的交换环, R 是 R_0 的子环, 并且包含 R_0 的单位元. 取 $x \in R_0$, 则 $\displaystyle\sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, a_i \in R$ 有意义, 且 $\in R_0$.

定义 180 (多项式) 一个可以写成 $a_0 + a_1 x + a_2 x^2 \cdots + a_n x^n, a_i \in R, n \in \mathbb{Z}^+$ 形式的 R_0 的元叫做 R 上的关于 x 的一个**多项式**, a_i 叫做多项式的**系数**. 我们把所有 R 上的 x 的多项式放在一起, 做成一个集合，用 $R[x]$ 来表示.

说明 181 (环上的多项式构成一个环) 在 $R[x]$ 上定义加法 $\sum a_i x^i + \sum b_i x^i = (a_i + b_i) x^i$, 乘法 $\displaystyle\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{mn}\left(\sum_{j=0}^{i} a_j b_{i-j}\right) x^i$, 都为初等代数里的计算法, 则 $R[x]$ 构成一个交换环.

定义 182 (未定元) R_0 里得一个元 x 叫做 R 上的一个**未定元**, 如果在 R 里找不到不都等于零的元 $a_0, a_1, a_2, \cdots, a_n$, 使得 $a_0 + a_1 x + a_2 x^2 \cdots + a_n x^n = 0$

命题 183 R 上的一个未定元 x 的多项式 (简称**一元多项式**)，如果不计入系数是零的项, 只能用一种方式写成 $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ $(a_i \in R)$

定义 184 (多项式的次数) 令 $a_0 + a_1 x + a_2 x^2 \cdots + a_n x^n = 0, a_n \neq \mathrm{o}$ 是环 R 上的一个一元多项式, 那么非负整数 n 叫做这个多项式的**次数**, 多项式 o 没有次数.

命题 185 对于给定的 R_0 来说, R_0 未必含有 R 上的未定元.

定理 186 给了一个有单位元的交换环 R, 一定有一个环 R_0, R 上的未定元 $x \in R_0$ 存在，因此也就有 R 上的多项式环 $R[x]$ 存在.

说明 187 对于一个有单位元的交换环 R_0, 和它的一个子环 R, 其中 R 包含 R_0 的单位元. 我们从 R_0 里任意取出 n 个元 $x_1, x_2, \cdots, x_n$ 来, 那么我们可以做 R 上的 x_1 的多项式环 $R[x_1]$, 然后做 $R[x_1]$ 上的 x_2 的多项式环 $R[x_1][x_2]$. 这样下去，可以得到 $R[x_1][x_2]\cdots[x_n]$. 这个环包括所有可以写成 $\displaystyle\sum_{i_1 i_2 \cdots i_n} a_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ $(a_{i_1 i_2 \cdots i_n} \in R$, 但只有有限个 $a_{i_1 i_2 \cdots i_n} \neq 0)$ 形式的元.

定义 188 一个有上述形式的元叫做 R 上的 $x_1, x_2, \cdots, x_n$ 的一个多项式，$a_{i_1 i_2 \cdots i_n}$ 叫做多项式的系数. 环 $R[x_1][x_2]\cdots[x_n]$ 叫做 R 上的 $x_1, x_2, \cdots, x_n$ 的多项式环. 这个环我们也用符号 $R[x_1, x_2, \cdots, x_n]$ 来表示.

3.7 理想

定义 189 (理想) 环 R 的一个非空子集 I 叫做一个**理想子环** (简称**理想**), 如果

1. $a, b \in I \Rightarrow a - b \in I$
2. $a \in I, r \in R \Rightarrow ra, ar \in I$.

命题 190 一个环至少有两个理想 (1) $I = \{o\}$, 叫做 R 的**零理想**. (2) I = R, 叫做 R 的**单位理想**.

定理 191 一个除环 R 只有两个理想，就是零理想和单位理想.

说明 192 因此，理想这个概念对于除环或者域来说没有多大用处.

说明 193 一个环除了以上两个理想之外，可能有其他理想.

命题 194 给定一个环 R，a 是 R 中的任意一个元素，考虑最小的理想 I 使得 $a \in I$. 作集合 $I = \{(x_1ay_1 + x_2ay_2 + \cdots) + sa + at + na \mid x_i, y_i, s, t \in R, n \in \mathbb{Z}\}$, 则 I 是包含 a 的最小理想.

定义 195 (主理想) 上面的这样的 I 叫做元 a 生成的**主理想**, 用符号 (a) 来表示.

说明 196 一个主理想 (a) 的元的形式并不是永远像上面那样复杂.

1. 当 R 满足交换律时, 可以写成 $ra + na, r \in R, n \in \mathbb{Z}$.
2. 当 R 有单位元时, 可以写成 $\sum x_iay_i, x_i, y_i \in R$.
3. 当 R 既满足交换律又有单位元时, 可以写成 $ra, r \in R$.

命题 197 给定一个环 R，$a_1, a_2, \cdots, a_m \in R$，考虑最小的理想 I 使得 $a_1, a_2, \cdots, a_m \in I$. 做集合 $I = \{s_1 + s_2 + \cdots + s_m \mid s_i \in (a_i)\}$, 则 I 是包含 $a_1, a_2, \ldots, a_m$ 的最小理想.

定义 198 上面的这样的 I 叫做 $a_1, a_2, \cdots, a_m$ 生成的理想, 用符号 $(a_1, a_2, \cdots, a_m)$ 来表示.

说明 199 两个元素生成的理想, 可能是主理想，也可能不是.

3.8 剩余类环、同态与理想

说明 200 给定一个环 R 和 R 的一个理想 I, 则我们就加法来说, R 做成一个群, I 做成 R 的一个不变子群, 从而 I 的陪集 $[a], [b], [c], \cdots$ 做成 R 的一个分类, 叫做**模 I 的剩余类**. 同时这个分类描述 R 的元素之间的等价关系, 用符号 $a \equiv b \mod I$ 表示 (读作 a 同余 b 模 I), 即 $a \equiv b \mod I \Leftrightarrow a \sim b \Leftrightarrow a - b \in I$. 且类 $[a]$ 所包含的元素可以写成 $\{a + u \mid u \in I\}$

定理 201 假定 R 是一个环, I 是它的一个理想, $\bar{R}$ 是所有模 I 的剩余类做成的集合, 如果在 $\bar{I}$ 上规定加法和乘法 $[a] + [b] = [a + b], [a][b] = [ab]$. 那么 $\bar{I}$ 本身也是一个环, 并且 R 与 $\bar{R}$ 同态.

定义 202 (模 I 的剩余类环) 上面的 $\bar{R}$ 叫做环 R 的**模 I 的剩余类环**, 用符号 R/I 来表示.

定理 203 假定 R 与 $\bar{R}$ 是两个环, 并且 R 与 $\bar{R}$ 同态, 那么这个同态满射的核 I 是 R 的一个理想, 并且 $R/I \cong \bar{R}$

定理 204 在环 R 到环 $\bar{R}$ 的同态满射下:

(1) R 的一个子环的象 $\bar{S}$ 是 $\bar{R}$ 的一个子环.
(2) R 的一个理想 I 的象 $\bar{I}$ 是 $\bar{R}$ 的一个理想.
(3) $\bar{R}$ 的一个子环 $\bar{S}$ 的原象 S 是 R 的一个子环.
(4) $\bar{R}$ 的一个理想 $\bar{I}$ 的原象 I 是 R 的一个理想.

说明 205 环-群, 子环-子群, 理想-不变子群

3.9 最大理想

定义 206 (最大理想) 如果一个环 R 的理想 $I(\neq R)$, 除了 R 和 I 以外, 无其他包含 I 的理想, 称 I 为 R 的**最大理想**.

引理 207 假定 $I(\neq R)$ 是环 R 的一个理想: 剩余类环 R/I 除了零理想和单位理想外不再有其他理想 $\Leftrightarrow I$ 是最大理想.

引理 208 若有单位元 $(\neq \mathfrak{o})$ 的交换环 R 除了零理想和单位理想以外没有其他理想, 那么 R 一定是一个域.

定理 209 R 是有单位元的交换环, $I(\neq R)$ 是 R 的理想: R/I 是域 $\Leftrightarrow I$ 是 R 的最大理想.

命题 210 $\mathbb{Z}_n$ 是域 $\Leftrightarrow n$ 是素数.

3.10 商域

定理 211 若 R 是无零因子的交换环, 则存在一个包含 R 的域 Q, 使得 Q 刚好是由所有元 $\dfrac{a}{b}$ $(a, b \in R, b \neq \mathfrak{o})$ 所做成的，这里 $\dfrac{a}{b} = ab^{-1} = b^{-1}a$.

定义 212 (商域) 一个域 Q 叫做环 R 的一个**商域**, 如果 $Q \supseteq R$, 并且 Q 刚好是由所有元 $\dfrac{a}{b}$ $(a, b \in R, b \neq 0)$ 所做成的.

定理 213 假定 R 是一个有两个以上的元的环, F 是一个包含 R 的域，则 F 包含 R 的一个商域.

说明 214 一般来讲, 一个环很可能有两个以上的商域. 不过，同构的环的商域也同构，所以抽象的来讲，一个环最多只有一个商域.