

近世代数 (抽象代数) 笔记

管清文

2020 年 3 月 31 日

目录

0.1	Highlights	3
0.2	基本概念	3
0.2.1	映射	3
0.2.2	等价关系与集合划分	4
0.2.3	代数运算	5
0.2.4	运算律	5
0.2.5	同态	5
第一章	群	7
1.1	群论	7
1.1.1	群的定义和性质	7
1.1.2	群的同态	8
1.1.3	变换群	8
1.1.4	置换群	8
1.1.5	循环群	9
1.1.6	子群	9
1.1.7	子群的陪集	10
1.1.8	不变子群、商群	10
1.1.9	同态与不变子群	11
1.2	特殊的群	11
1.2.1	加群	11
第二章	环	12
2.1	环与域	12
2.1.1	环的定义	12
2.1.2	子环、环的同态	12
2.1.3	理想	14
2.1.4	剩余类环、同态与理想	14
2.1.5	最大理想	15
2.1.6	商域	15
2.2	特殊的环	15
2.2.1	交换环	15
2.2.2	无零因子环	16
2.2.3	整环	16
2.2.4	除环、域	17
2.2.5	一元多项式环 $R[x]$	18
2.3	具体的环	19
2.3.1	整数环	19

2.3.2	$M_n[K]$	19
第三章	线性空间	20
第四章	套娃	21
4.1	数域 K 上的一元多项式环 $K[x]$	21
4.1.1	整除关系, 带余除法	22
4.1.2	最大公因式	22
4.1.3	不可约多项式	23
第五章	xxx	24
5.1	整环里的因子分解	24
5.1.1	素元、唯一分解	24
5.1.2	唯一分解环	25
5.1.3	主理想环	25
5.1.4	欧氏环	25
5.1.5	多项式环的因式分解	26
5.1.6	因式分解与多项式的根	26
5.2	扩域	27
5.2.1	单扩域	27
5.2.2	代数扩域	28

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.

说明

- 关于一一映射的说法都被改成了双射 (Bijection), 因为在英文资料中, one-to-one 表示的是单射 (Injection), 容易引起歧义.
- 所有的当且仅当的命题 (定理、...) 都被写成以下形式:

命题 5 假定 blablabla, 那么

$$p \Leftrightarrow q$$

0.1 Highlights

0.2 基本概念

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。

说明 2 规定 $-\infty < n, -\infty + n = -\infty, \forall n \in \mathbb{N}$ 规定 $-\infty + (-\infty) = -\infty$.

0.2.1 映射

定义 3 (映射)

$$\begin{aligned} \phi: A &\rightarrow D \\ a &\mapsto d = \phi(a) = \bar{a} \end{aligned}$$

其中 A 称为**定义域 (Domain)**, D 称为**陪域 (Codomain)**, $\{\phi(a) \mid a \in A\}$ 称为**值域 (Image)**, 记作 $f(A)$ 或者 $\text{Im } f$.

定义 4 对于映射 $f: A \rightarrow B, g: C \rightarrow D$

$$f = g \stackrel{\text{def}}{\iff} A = B \ \& \ C = D \ \& \ f(a) = g(a) \ \forall a \in A$$

定义 5 (满射) 映射 $\phi: A \rightarrow B$ 被称为**满射**, 如果 $B = \text{Im } \phi$, 换句话说

$$\forall b \in B \implies b \in \text{Im } \phi \text{ (即 } \exists a \in A \text{ 使得 } \phi(a) = b).$$

它对应 ϕ^{-1} 都有象.

定义 6 (单射) 映射 $\phi: A \rightarrow \bar{A}$ 被称为**单射**, 如果 A 中不同元素的在 ϕ 下的象不同, 换句话说

$$\text{设 } a_1, a_2 \in A, \phi(a_1) = \phi(a_2) \implies a_1 = a_2$$

它对应 ϕ^{-1} 象唯一

定义 7 (变换) 从 A 到 A 的映射 $\tau: A \rightarrow A, a \mapsto \tau(a)$ 叫 A **变换**, 我们也用 a^τ 表示 $\tau(a)$. 如果 τ 是满射 (单射、双射), 则称为**满变换 (单变换、双射变换)**.

定义 8 (映射的乘法) 设 $f: A \rightarrow B, g: B \rightarrow C$, 令

$$(g \circ f)(a) \triangleq g(f(a)), \forall a \in A$$

则称 $g \circ f$ 是 g 与 f 的**乘积**.

说明 9 映射的乘法满足结合律, 即 $h \circ (g \circ f) = (h \circ g) \circ f$.

定义 10 若 $f: A \rightarrow A, a \mapsto a$, 则 f 是 A 上的**恒等变换**, 记作 1_A .

命题 11 设 $f: A \rightarrow B$, 则 $f \circ 1_A = 1_B \circ f = f$

定义 12 (可逆映射) 设 $f: A \Rightarrow B$, 如果存在 $g: B \rightarrow A$ 使得 $g \circ f = 1_A$, 且 $f \circ g = 1_B$, 那么称 f 是可逆映射, 把 g 称为 f 的逆映射.

说明 13 若 f 可逆, 则 f 的逆映射唯一, 把 f 的逆映射记作 f^{-1} . f^{-1} 也是可逆映射, 并且 $(f^{-1})^{-1} = f$.

定理 14 $f: A \rightarrow B$ 是可逆映射 $\iff f$ 是双射.

0.2.2 等价关系与集合划分

定义 15 (集合的划分) 如果集合 A 是他的一些非空子集的并集, 其中每两个不相等的子集的交是空集 (称为**不相交**), 那么把这些子集组成的集合称为 A 的一个**划分**.

定义 16 (二元关系[Relation]) $S \times S$ 的一个子集 W 称为 S 上的一个二元关系. 若 $(a, b) \in W$, 则称 a 和 b 有 W 关系, 记作 $a \sim_W b$. 若 $(a, b) \notin W$, 则称 a 和 b 没有 W 关系.

说明 17 整除是一个二元关系.

定义 18 (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 19 设 \sim 是 S 上的一个等价关系, 任给 $a \in S$, 令

$$\bar{a} \triangleq \{x \in S \mid x \sim a\}$$

则把 \bar{a} 称为 a 的**等价类**.

说明 20 $x \in \bar{a} \iff x \sim a$

说明 21 (代表) 由于 $a \sim a$, 因此 $a \in \bar{a}$, 把 a 称为 \bar{a} 的一个**代表**.

性质 22 $\bar{a} = \bar{b} \iff a \sim b$

性质 23 $\bar{a} \neq \bar{b} \implies \bar{a} \cap \bar{b} = \emptyset$

定理 24 如果集合 S 上有一个等价关系 \sim , 那么所有等价类组成的集合是 S 的一个划分.

定理 25 如果集合 S 中有一个划分, 那么可以在 S 上建立一个等价关系, 使得这个划分是由所有等价类组成的.

定义 26 (商集) 集合 S 的一个划分也称为 S 的一个**商集**, 是 S 的所有等价类组成的集合.

定义 27 (\mathbb{Z}_p [模 n 的剩余类]) $\{[0], [1], \dots, [n-1]\}$, $[i] = \{kn + i \mid k \in \mathbb{Z}\}$

0.2.3 代数运算

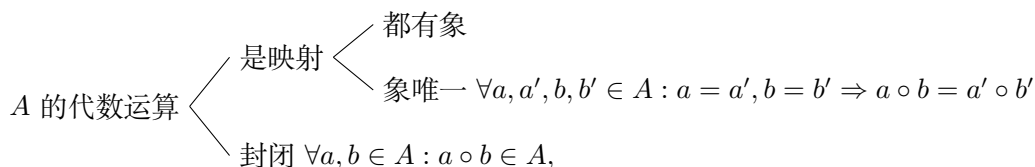
定义 28 (代数运算)

$$A \times B \rightarrow D$$

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

定义 29 (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.

说明 30 (A 的代数运算判别)



0.2.4 运算律

定义 31 (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 32 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, \dots, a_n 来说, 对于任意的加括号的方法 π , $\pi(a_1 \circ a_2 \circ \dots \circ a_n)$ 都相等, 我们用 $a_1 \circ a_2 \circ \dots \circ a_n$ 来表示.

定义 33 (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 34 若 A 上的代数运算 \circ 满足结合律与交换律, 则 $a_1 \circ a_2 \circ \dots \circ a_n$ 可以任意交换顺序.

定义 35 (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 满足左分配率.
- (2) 若 $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c), \forall a, b, c$, 则称 \odot 和 \oplus 满足右分配率.

定理 36 若 A 上的二元运算 \oplus 满足结合律, \odot 和 \oplus 满足左分配率, 则

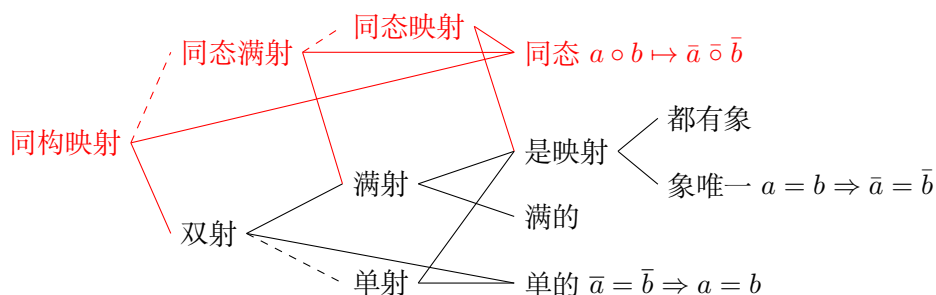
$$a \odot (b_1 \oplus b_2 \oplus \dots \oplus b_n) = (a \odot b_1) \oplus (a \odot b_2) \oplus \dots \oplus (a \odot b_n)$$

定理 37 若 A 上的二元运算 \oplus 满足结合律, \odot 和 \oplus 满足右分配率, 则

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

0.2.5 同态

说明 38 (映射判别)



定义 39 (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 $\bar{\circ}$. 称 ϕ 是 A 到 \bar{A} 的**同态映射**, 如果 $\forall a, b \in A, \bar{a} := \phi(a), \bar{b} := \phi(b)$ 有 $a \circ b \mapsto \bar{a} \bar{\circ} \bar{b}$.

定义 40 (同态满射、同态) 如果 A 到 \bar{A} 存在 一个同态映射 ϕ , 且它是满射, 则称 A 与 \bar{A} (关于 \circ 与 $\bar{\circ}$) **同态**. 称这个映射是一个**同态满射**.

定义 41 (同构映射、同构) 如果 A 到 \bar{A} 存在 一个同态映射 ϕ , 且它是双射, 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 42 同构关系是一个等价关系.

定理 43 假定对于代数运算 \circ 和 $\bar{\circ}$ 来说, A 与 \bar{A} 同态, 那么

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

定理 44 \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

- (1) 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.
- (2) 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.

第一章 群

1.1 群论

1.1.1 群的定义和性质

注意 45 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 (a, b) 的象写成 ab

定义 46 (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.

定理 47 (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 48 (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 49 (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 50 (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 51 (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 52 (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 53 (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 54 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 55 (乘积的逆等于逆的乘积) $\forall a, b \in G, (ab^{-1})^{-1} = ba^{-1}$

定义 56 规定 $\forall n \in \mathbb{Z}^+ : a^n = \underbrace{aa \cdots a}_{n\uparrow}, a^0 = e, a^{-n} = (a^{-1})^n$

命题 57 $\forall n, m \in \mathbb{Z} : a^n a^m = a^{n+m}, (a^n)^m = a^{mn} \quad (\Rightarrow (a^{-1})^{-1} = a)$

定义 58 (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 59 (III'[消去律]) 群的乘法满足: $ax = ax' \Rightarrow x = x', ya = y'a \Rightarrow y = y'$

推论 60 在群里, $ax = b$ 和 $ya = b$ 都有唯一解.

定理 61 (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.

1.1.2 群的同态

定理 62 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 63 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 64 G 与 \bar{G} 关于他们的乘法同构, 则 G 是群 $\Leftrightarrow \bar{G}$ 是群.

1.1.3 变换群

定义 65 (变换的乘法) $\tau_1 \tau_2 : a \mapsto (a^{\tau_1})^{\tau_2}$

定理 66 (变换乘法结合) $(\tau_1 \tau_2) \tau_3 = \tau_1 (\tau_2 \tau_3)$

定理 67 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 中的变换一定是双射变换.

定义 68 (变换群) 如果一个集合 A 的若干 双射变换 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 69 一个集合 A 上的所有双射变换做成一个变换群 G .

定理 70 任何一个群都与一个变换群同构.

定理 71 一个变换群的单位元一定是恒等变换.

1.1.4 置换群

定义 72 (置换) 有限集合 上的 双射变换 叫做置换, 一般用 π 表示.

定义 73 (置换群) 有限集合上的若干置换做成的群叫置换群.

定义 74 (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 75

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

定义 76 (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.

命题 77 $(i_1 i_2 \cdots i_k)^{-1} = (i_k \cdots i_2 i_1).$

命题 78 k -循环置换的阶是 k .

命题 79 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 80 两个没有共同数字的循环置换可以交换.

命题 81 任何一个有限群都与一个置换群同构.

1.1.5 循环群

定义 82 (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 83 (\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 84 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 $G \cong \mathbb{Z}_n$.

说明 85 于是 $|(a)| = n$, 其中 n 为 a 的阶.

命题 86 一个循环群一定是交换群.

命题 87 a 生成一个阶是 n 的循环群 G , 则 a^r 也生成 G , 如果 $\gcd(r, n) = 1$.

命题 88 G 是循环群, 且 G 与 \bar{G} 同态, 则 \bar{G} 也是循环群.

命题 89 G 是无限阶循环群, \bar{G} 是任何循环群, 则 G 与 \bar{G} 不同态.

1.1.6 子群

定义 90 (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 91 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 92 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 93 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 94 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) $a, b \in H \Rightarrow ab \in H$

说明 95 (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 96 (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 97 $S = \{a\}$ 时, $\langle S \rangle = \langle a \rangle$.

命题 98 循环群的子群也是循环群.

命题 99 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) $a, b \in H \Rightarrow ab \in H$.

1.1.7 子群的陪集

定义 100 群 G , 子群 H , 规定 G 上的关系 $\sim: a \sim b \Leftrightarrow ab^{-1} \in H$

定理 101 上面规定的关系 \sim 是等价关系.

定义 102 (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 103 包含元 a 的右陪集 $= Ha = \{ha \mid h \in H\}$

定义 104 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 105 (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 106 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 107 (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 108 右陪集所含元素的个数等于子群 H 所含元素的个数.

定理 109 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 110 (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 111 阶是素数的群一定是循环群.

命题 112 阶是 p^m 的群 (p 是素数) 一定包含一个阶是 p 的子群.

命题 113 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.

1.1.8 不变子群、商群

定义 114 (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 115 $S_1, S_2 \subseteq$ 群 G , 规定子集的乘法 $S_1 S_2 = \{s_1 s_2 \mid s_1 \in S_1, s_2 \in S_2\}$. 显然这个乘法满足结合律.

定理 116 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 117 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 118 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 119 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 120 (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 121 对于有限群, $|G/N| = \frac{|G|}{|N|}$.

命题 122 H 是 G 的子群, N 是 G 的不变子群, 则 HN 是 G 的子群.

1.1.9 同态与不变子群

定理 123 一个群 G 与它的商群 G/N 同态.

定义 124 (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 125 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 126 一个群只和“相当于”它的商群同态

定义 127 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 128 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 129 这也体现了同态的性质, 前面有的后面也有!

命题 130 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 131 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 132 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.

1.2 特殊的群

1.2.1 加群

定义 133 (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 134 (Σ) n 个元的和 $a_1 + a_2 + \cdots + a_n$ 用符号 $\sum_{i=1}^n a_i$ 来表示.

定义 135 n 个 a 的和 $\sum_{i=1}^n a$ 我们用 na 表示.

定义 136 (零元) 加群唯一的单位元用 o 来表示, 并且把它叫做零元.

定义 137 (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 138 加群满足以下运算规则

- (1) $o + a = a + o = a$
- (2) $-a + a = a - a = o$
- (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 139 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) $a, b \in S \Rightarrow a - b \in S$.

第二章 环

2.1 环与域

2.1.1 环的定义

定义 140 (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 141 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 $a^n = \underbrace{aa \cdots a}_{n \uparrow}, n \in \mathbb{Z}^+,$ 则 $a^m a^n = a^{m+n}, (a^m)^n = a^{mn}$

2.1.2 子环、环的同态

定义 142 (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 143 若 S 是环 R 的一个非空子集, 则 S 是 R 的子环 $\iff a, b \in S \Rightarrow a-b \in S, ab \in S$.

命题 144 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 145 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.

说明 146 (环的同态、环的同构) 我们说两个环 R 和 \bar{R} 同态 (同构), 如果存在一个 R 到 \bar{R} 的满射 (双射), 使得 R 与 \bar{R} 对于两个环的一对加法以及一对乘法来说都同态.

注意 147 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 148 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 $1 \Rightarrow \bar{R}$ 也有单位元 $\bar{1}$, 且 $\bar{1}$ 是 1 的象.
- R 无零因子 $\nRightarrow \bar{R}$ 无零因子
- R 有零因子 $\nRightarrow \bar{R}$ 有零因子
- R 是整环 (除环、域) $\nRightarrow \bar{R}$ 是整环 (除环、域)

命题 149 若 R 和 \bar{R} 都是环, 且 R 与 \bar{R} 同态, 则

- R 无零因子 $\nRightarrow \bar{R}$ 无零因子
- R 有零因子 $\nRightarrow \bar{R}$ 有零因子
- R 是整环 (除环、域) $\nRightarrow \bar{R}$ 是整环 (除环、域)

命题 150 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 151 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 152 集合 A 和 \bar{A} 之间有一个双射 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 153 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 154 (!)

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

命题 155 一个除环的中心是一个域.

2.1.3 理想

定义 156 (! 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 157 一个环至少有两个理想 (1) $I = \{0\}$, 叫做 R 的**零理想**. (2) $I = R$, 叫做 R 的**单位理想**.

定理 158 一个除环 R 只有两个理想, 就是零理想和单位理想.

说明 159 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 160 一个环除了以上两个理想之外, 可能有其他理想.

命题 161 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 162 (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 163 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 $\sum x_i ay_i, x_i, y_i \in R$.
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 164 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, \dots, a_m 的最小理想.

定义 165 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 166 两个元素生成的理想, 可能是主理想, 也可能不是.

命题 167

- 群 G 的两个子群的交集还是 G 的子群.
- 两个不变子群的交集还是不变子群.
- 两个子环的交集还是子环.
- 两个子整环的交集还是子整环.
- 两个子除环的交集还是子除环.
- 两个子域的交集还是子域.
- 两个理想的交集还是一个理想.

2.1.4 剩余类环、同态与理想

说明 168 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 $a \equiv b \pmod{I}$ 表示 (读作 a 同余 b 模 I), 即 $a \equiv b \pmod{I} \Leftrightarrow a \sim b \Leftrightarrow a - b \in I$. 且类 $[a]$ 所包含的元素可以写成 $\{a + u \mid u \in I\}$

定理 169 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 170 (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 171 (!) 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 172 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 173 环-群, 子环-子群, 理想-不变子群

命题 174 ϕ 是环 R 到环 \bar{R} 的一个同态满射: ϕ 是 R 与 \bar{R} 之间的同构映射 $\Leftrightarrow \phi$ 的核是零理想.

2.1.5 最大理想

定义 175 (最大理想) 如果一个环 R 的理想 $I(I \neq R)$, 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 176 假定 $I(I \neq R)$ 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 177 若有单位元 ($\neq 0$) 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 178 (!) R 是有单位元的交换环, $I(I \neq R)$ 是 R 的理想: R/I 是域 $\Leftrightarrow I$ 是 R 的最大理想.

命题 179 \mathbb{Z}_n 是域 $\Leftrightarrow n$ 是素数.

2.1.6 商域

定理 180 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 $\frac{a}{b}$ ($a, b \in R, b \neq 0$) 所做成的, 这里 $\frac{a}{b} = ab^{-1} = b^{-1}a$.

定义 181 (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 $\frac{a}{b}$ ($a, b \in R, b \neq 0$) 所做成的.

定理 182 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 183 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.

2.2 特殊的环

2.2.1 交换环

定义 184 (交换环) 一个环 R 叫做交换环, 如果 $ab = ba, \forall a, b \in R$.

命题 185 在一个交换环中 $(ab)^n = a^n b^n$.

2.2.2 无零因子环

说明 186 $ab = 0 \Rightarrow a = 0$ 或者 $b = 0$ 在环里不一定成立.

定义 187 (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. 左零因子和右零因子统称为零因子.

注意 188 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 189 (!) 在一个没有零因子的环里, 左右消去律都成立.

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

$$2. d \neq 0, bd = cd \Rightarrow b = c$$

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 190 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.

命题 191 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 192 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 193 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.

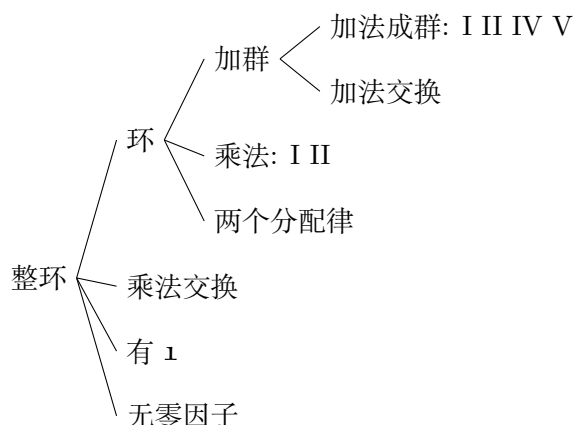
定义 194 (无零因子环的特征) 在一个无零因子环 R 中, 所有非零元关于加法的阶, 叫做 R 的特征.

定理 195 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 196 整环、除环以及域的特征或者是无限大, 或者是一个素数.

2.2.3 整环

说明 197 (!! 整环的判别)



定义 198 (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 199 一个环如果有单位元, 则唯一. 用 1 来表示.

定义 200 (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 201 如果 a 有逆元, 则唯一.

命题 202 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 203 (模 n 的剩余类环) $R = \{[0], [1], \dots, [n-1]\}$, 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 $1 = [1]$.

定义 204 (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 205 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.

定理 206 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) $1 \in S$.

定义 207 (! 整除) 对于整环 I , 若 $a \in I$, 存在 $b, c \in I$ 使 $a = bc$, 则称 b 能整除 a , 记作 $b \mid a$, 称 b 为 a 的因子. 若 b 不是 a 的因子, 则记作 $b \nmid a$.

命题 208 整除关系是一个二元关系, 满足

- (1) 反身性, $a \mid a$
- (2) 对称性
- (3) 传递性, $a \mid b, b \mid c \Rightarrow a \mid c$

定义 209 (相伴) 如果 $a \mid b$ 且 $b \mid a$, 则称 a 与 b 相伴, 记作 $a \sim b$.

定义 210 (相伴等价定义) 元 b 叫做元 a 的相伴元, 如果存在一个单位 ϵ 使得 $b = \epsilon a$.

2.2.4 除环、域

命题 211 对于元素个数 ≥ 2 的环, $1 \neq 0$, 且 0 没有逆元.

定义 212 (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 213 (域) 一个交换除环叫做一个域.

性质 214 除环没有零因子.

性质 215 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 216 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.

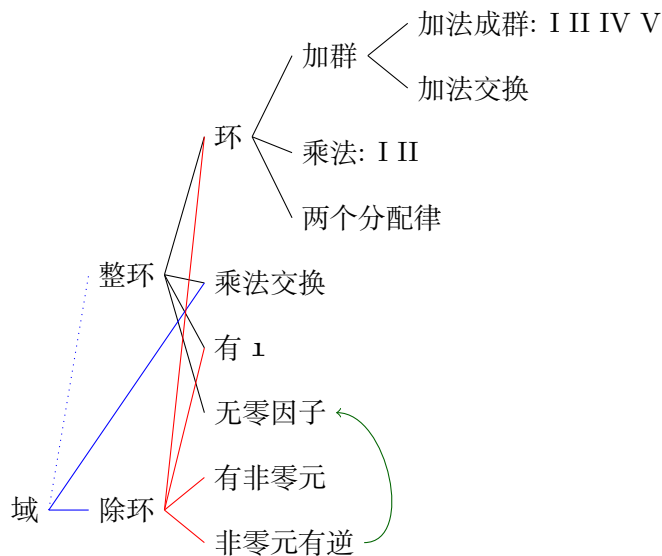
说明 217 在除环 R 中, 方程 $ax = b, ya = b (a \neq 0)$ 都有唯一解, 分别是 $a^{-1}b$ 和 ba^{-1} , 他们未必相等. 在一个域里 $a^{-1}b = ba^{-1}$, 用符号 $\frac{b}{a}$ 表示.

性质 218 域满足以下计算法则

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

命题 219 存在不是域的除环, 例如四元数除环.

说明 220 ! 环、整环、域之间的关系:



命题 221 一个至少有两个元且没有零因子的有限环, 是一个除环.

定理 222 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 223 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) $\forall a, b \in S, b \neq 0 \Rightarrow ab^{-1} \in S$.

2.2.5 一元多项式环 $R[x]$

说明 224 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 $\alpha \in R_0$, 则 $\sum_{i=0}^n a_i \alpha^i = a_0 + a_1 \alpha + a_2 \alpha^2 + \cdots + a_n \alpha^n$ ($a_i \in R$) 有意义, 且 $\in R_0$.

定义 225 (多项式) 一个可以写成 $a_0 + a_1 \alpha + \cdots + a_n \alpha^n$ ($a_i \in R, n \in \mathbb{Z}^+$) 形式的 R_0 的元叫做 R 上的关于 α 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 $R[\alpha]$ 来表示.

说明 226 (环上的多项式构成一个环) 在 $R[x]$ 上定义

$$\begin{aligned} \text{加法: } \sum_i a_i \alpha^i + \sum_i b_i \alpha^i &= \sum_i (a_i + b_i) \alpha^i \\ \text{乘法: } \left(\sum_{i=0}^m a_i \alpha^i \right) \left(\sum_{j=0}^n b_j \alpha^j \right) &= \sum_{i=0}^m \sum_{j=0}^n a_i b_j \alpha^{i+j} = \sum_{i=s}^{mn} \left(\sum_{i+j=s} a_i b_j \right) \alpha^s \end{aligned}$$

都为初等代数里的计算方法, 则 $R[\alpha]$ 构成一个交换环.

定义 227 (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 228 (!) R 上的一个未定元 x 的多项式 $f(x)$ (简称一元多项式) 的表法唯一, 即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 229 (多项式的次数) 令 $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0, a_n \neq 0$ 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, 记作 $\deg f(x)$. 0 次多项式等同于 R 中的非零元, 多项式 0 (称为零多项式) 的次数规定为 $-\infty$.

说明 230 数域 K 上的一元多项式 $K[x]$ 对于加法和数量乘法成为数域 K 上的一个无限维线性空间, $\Omega = \{1, x, x^2, \dots, x^n, \dots\}$ 是 $K[x]$ 的一个基.

命题 231 对于给定的 R_0 来说, R_0 未必含有 R 上的未定元.

定理 232 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 233 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, \dots, 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 $\sum_{i_1 i_2 \cdots i_n} a_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ ($a_{i_1 i_2 \cdots i_n} \in R$, 但只有有限个 $a_{i_1 i_2 \cdots i_n} \neq 0$) 形式的元.

定义 234 一个有上述形式的元叫做 R 上的 x_1, x_2, \dots, 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, \dots, x_n 的多项式环. 这个环我们也用符号 $R[x_1, x_2, \dots, x_n]$ 来表示.

命题 235 假定 R 是一个整环, 那么 R 上的一元多项式环也是一个整环.

2.3 具体的环

2.3.1 整数环

定义 236 (整数环) 整数关于普通加法和乘法构成的环.

命题 237 整数环是一个整环.

2.3.2 $M_n[K]$

说明 238 数域 K 上的所有 n 级矩阵 $M_n[K]$, 对于矩阵的加法和乘法构成一个环.

第三章 线性空间

第四章 套娃

4.1 数域 K 上的一元多项式环 $K[x]$

说明 239 数域 K 上的一元多项式环 $K[x]$ 是一个欧式环、主理想环、唯一分解环、整环.

性质 240 设 $f(x), g(x) \in K[x]$, 则

$$\begin{aligned}\deg(f(x) + g(x)) &\leq \max(\deg f(x), \deg g(x)) \\ \deg(f(x)g(x)) &= \deg f(x) + \deg g(x)\end{aligned}$$

推论 241 设 $f(x), g(x) \in K[x]$, 则

$$f(x) \neq 0, g(x) \neq 0 \implies f(x)g(x) \neq 0$$

推论 242 (消去律) 设 $f(x), g(x), h(x) \in K[x]$, 则

$$f(x)g(x) = f(x)h(x) \ \& \ f(x) \neq 0 \implies g(x) = h(x)$$

说明 243 任给 $A \in M_n(K)$, 矩阵 A 的多项式组成的集合 $K[A]$. 容易验证非空集合 $K[A]$ 对于矩阵的减法和乘法封闭, 从而 $K[A]$ 是环 $M_n(K)$ 的一个子环. 且 $K[A]$ 是有单位元的交换环.

说明 244 KI 是 $K[A]$ 的一个子环.

定理 245 (一元多项式环的通用性质) 设 K 是一个数域, R 是一个有单位元 $1'$ 的交换环. 且 K 到 R 的一个子环 R_1 (含有 $1'$) 有一个同构映射 τ . 任给 $t \in R$, 令

$$\begin{aligned}\sigma_t : K[X] &\rightarrow R \\ f(x) = \sum_{i=0}^n a_i x^i &\mapsto \sum_{i=0}^n \tau(a_i) t^i \triangleq f(t)\end{aligned}$$

则 σ_t 是 $K[x]$ 到 R 的一个映射, 且 $\sigma_t(x) = t$, 且 σ_t 保持加法、乘法运算, 即

$$f(x) + g(x) = h(x), f(x)g(x) = p(x) \implies f(t) + g(t) = h(t), f(t)g(t) = p(t)$$

称 σ_t 是 x 用 t 带入.

说明 246 定理回答了为什么多项式环的未定元可以带入特定的值.

$$\left. \begin{array}{ccc} K[x] & \xrightarrow{\text{子环}} & \text{数域 } K \\ \sigma \downarrow & & \tau \downarrow \cong \\ \text{含么交换环 } R & \xrightarrow{\text{子环}} & \text{含么子环 } R_1 \end{array} \right\} \implies \left\{ \begin{array}{l} \forall t \in R, \exists \sigma_t : K[X] \rightarrow R \\ f(x) = \sum_{i=0}^n a_i x^i \mapsto \sum_{i=0}^n \tau(a_i) t^i \triangleq f_\tau(t) \\ \text{满足} \\ \sigma_t(x) = t \\ f(x) + g(x) = h(x) \Rightarrow f_\tau(t) + g_\tau(t) = h_\tau(t) \\ f(x)g(x) = p(x) \Rightarrow f_\tau(t)g_\tau(t) = p_\tau(t) \end{array} \right.$$

4.1.1 整除关系, 带余除法

命题 247 (!) 在 $K[x]$ 中, $g(x) \mid f(x) \ \& \ f(x) \neq 0 \implies \deg g(x) \leq \deg f(x)$.

命题 248 若 $f(x), g(x) \in K[x]$, 那么

$$f(x) \sim g(x) \iff f(x) = cg(x) \ (c \in K^*)$$

定理 249 (带余除法) 设 $f(x), g(x) \in K[x]$, 且 $g(x) \neq 0$, 则 唯一 的存在 $K[x]$ 中一对多项式 $h(x), r(x)$, 使得

$$f(x) = h(x)g(x) + r(x), \deg r(x) < \deg g(x)$$

我们把 $h(x)$ 叫做**商式**, $r(x)$ 叫做**余式**.

说明 250 因为证明用到逆元, 所以要是至少是除环 (我还没确定够不够), 普通环肯定不行.

推论 251 设 $f(x), g(x) \in K[x]$, 且 $g(x) \neq 0$, 则

$$g(x) \mid f(x) \iff g(x) \text{ 除 } f(x) \text{ 的余式是 } 0.$$

命题 252 (整除性不随数域的扩大而改变) 设 $f(x), g(x) \in K[x]$, $g(x) \neq 0$, 数域 E 包含 K , 则在 $K[x]$ 中 $g(x) \mid f(x) \iff$ 在 $E[x]$ 中 $g(x) \mid f(x)$

4.1.2 最大公因式

定义 253 (因式) 如果 $g(x) \mid f(x)$, 则 $g(x)$ 称为 $f(x)$ 的一个**因式**, $f(x)$ 称为 $g(x)$ 的一个**倍式**.

定义 254 (公因式) $K[x]$ 中, 若 $c(x) \mid f(x)$ 且 $c(x) \mid g(x)$, 则称 $c(x)$ 是 $f(x)$ 和 $g(x)$ 的一个**公因式**.

定义 255 (最大公因式) 设 $f(x), g(x) \in K[x]$, 如果有 $K[x]$ 中的一个多项式 $d(x)$ 满足

- (1) $d(x) \mid f(x)$ 且 $d(x) \mid g(x)$
- (2) $f(x)$ 与 $g(x)$ 的任一公因式 $c(x) \mid d(x)$

那么称 $d(x)$ 是 $f(x)$ 与 $g(x)$ 的一个**最大公因式**.

说明 256 $\forall f(x) \in K[x]$, $f(x)$ 与 0 的一个最大公因式是 $f(x)$. 特别的 0 与 0 的一个最大公因式是 0.

说明 257 接下来探索 $f(x) \neq 0$ 与 $g(x) \neq 0$ 的最大公因式是否存在? 如果存在, 如何求? 有多少个?

引理 258 设 $f(x), g(x) \in K[x]$, 且 $g(x) \neq 0$, 如果有下式成立

$$f(x) = h(x)g(x) + r(x)$$

那么

$$c(x) \mid f(x) \ \& \ c(x) \mid g(x) \iff c(x) \mid g(x) \ \& \ c(x) \mid r(x)$$

从而

$$d(x) \text{ 是 } f(x) \text{ 与 } g(x) \text{ 的一个最大公因式} \iff d(x) \text{ 是 } g(x) \text{ 与 } r(x) \text{ 的一个最大公因式}$$

定理 259 (!) $K[x]$ 中任意一对多项式 $f(x)$ 与 $g(x)$ 都有一个最大公因式 $d(x)$, 并且存在 $u(x), v(x) \in K[x]$ 使得

$$u(x)f(x) + v(x)g(x) = d(x)$$

说明 260 设 $d_1(x), d_2(x)$ 都是 $f(x)$ 与 $g(x)$ 的最大公因式, 则 $d_1(x) \mid d_2(x)$ 且 $d_2(x) \mid d_1(x)$, 从而 $d_1(x) \sim d_2(x)$.

说明 261 当 $f(x)$ 与 $g(x)$ 不全为 0 时, 它们的最大公因式是非零多项式. 用 $(f(x), g(x))$ 表示 $f(x)$ 与 $g(x)$ 的首项系数为 1 的最大公因式, 简称**首一最大公因式**.

命题 262 (首一最大公因式不随数域的扩大而改变) 设 $f(x), g(x) \in K[x]$, 且 $g(x) \neq 0$, 数域 $E \supseteq K$, 则 $f(x)$ 与 $g(x)$ 在 $K[x]$ 中的首一最大公因式 = $f(x)$ 与 $g(x)$ 在 $E[x]$ 中的首一最大公因式.

定义 263 (互素) 在 $K[x]$ 中, 若 $(f(x), g(x)) = 1$, 则称 $f(x)$ 和 $g(x)$ **互素**.

说明 264 $f(x)$ 与 $g(x)$ 互素 $\iff f(x)$ 与 $g(x)$ 的任一公因式 $c(x)$ 是零次多项式.

定理 265 (!) 在 $K[x]$ 中 $f(x)$ 与 $g(x)$ 互素 \iff 存在 $u(x), v(x) \in K[x]$ 使得 $u(x)f(x) + v(x)g(x) = 1$.

命题 266 (互素性不随数域的扩大而改变) 设 $f(x), g(x) \in K[x]$, 且 $g(x) \neq 0$, 数域 $E \supseteq K$, 则

$$f(x) \text{ 与 } g(x) \text{ 在 } K[x] \text{ 中互素} \iff f(x) \text{ 与 } g(x) \text{ 在 } E[x] \text{ 中互素}$$

性质 267 (!) 在 $K[x]$ 中, 若 $f(x) \mid g(x)h(x)$, 且 $(f(x), g(x)) = 1$, 则 $f(x) \mid h(x)$.

性质 268 在 $K[x]$ 中, 若 $f(x) \mid h(x)$, $g(x) \mid h(x)$, 且 $(f(x), g(x)) = 1$, 则 $f(x)g(x) \mid h(x)$.

性质 269 在 $K[x]$ 中, 若 $(f(x), h(x)) = 1$, 且 $(g(x), h(x)) = 1$, 则 $(f(x)g(x), h(x)) = 1$.

推论 270 在 $K[x]$ 中, 若 $(f_i(x), h(x)) = 1, i = 1, \dots, s$, 则 $(f_1(x) \cdots f_s(x), h(x)) = 1$.

4.1.3 不可约多项式

定义 271 设 $f(x) \in K[x]$, $\deg f(x) > 0$, 如果 $f(x)$ 的因式只有零次多项式和 $f(x)$ 的相伴元, 那么称 $f(x)$ 是在 K 上**不可约**的, 否则称 $f(x)$ 在 K 上**可约**.

定理 272 设 $p(x) \in K[x]$, 且 $\deg p(x) > 0$, 则下列命题等价

- (1) $p(x)$ 在 K 上不可约
- (2) $\forall f(x) \in K[x]$, 有 $(p(x), f(x)) = 1$ 或 $p(x) \mid f(x)$
- (3) 在 $K[x]$ 中, 从 $p(x) \mid f(x)g(x)$ 可推出 $p(x) \mid f(x)$ 或 $p(x) \mid g(x)$
- (4) 在 $K[x]$ 中, $p(x)$ 不能分解成两个次数比 $p(x)$ 低的多项式的乘积

推论 273 $K[x]$ 中, 若不可约多项式 $p(x) \mid f_1(x) \cdots f_s(x)$, 则 $p(x) \mid f_j(x)$, 其中 $j \in \{1, \dots, s\}$.

推论 274 $K[x]$ 中, 一次多项式是不可约的.

推论 275 $f(x) \in K[x]$, $\deg f(x) > 0$

$$f(x) \text{ 可约} \iff f(x) \text{ 能够分解成两个次数比 } f(x) \text{ 低的多项式的乘积.}$$

定理 276 (唯一因式分解定理) $K[x]$ 中每一个次数大于 0 的多项式 $f(x)$ 都能 唯一 分解成 K 上有限多个不可约多项式的乘积. 其中唯一性是指若 $f(x) = p_1(x) \cdots p_s(x) = q_1(x) \cdots q_t(x)$, 则 $s = t$, 且适当排列因式的次序, 有 $p_i(x) \sim q_i(x)$.

说明 277 (标准分解式)

$$f(x) = ap_1(x)^{\ell_1} p_2(x)^{\ell_2} \cdots p_m(x)^{\ell_m}$$

称为 $f(x)$ 的**标准分解式**, 其中 $p_1(x), p_2(x), \dots, p_m(x)$ 是两两不等的首一不可约多项式, $\ell_i > 0, i = 1, 2, \dots, m$.

定义 278 设 $f(x) \in K[x]$, $\deg f(x) > 0$, 若不可约多项式 $p(x)$ 满足 $p^k(x) \mid f(x)$, 且 $p^{k+1}(x) \nmid f(x)$, 则称 $p(x)$ 是 $f(x)$ 的 k **重因式**.

- 当 $k = 0$ 时, $p(x)$ 不是 $f(x)$ 的因式.
- 当 $k = 1$ 时, $p(x)$ 称为 $f(x)$ 的**单因式**.
- 当 $k \geq 2$ 时, $p(x)$ 称为 $f(x)$ 的**重因式**.

第五章 XXX

5.1 整环里的因子分解

5.1.1 素元、唯一分解

定义 279 (单位) 整环 I 的元 ϵ 叫做 I 的一个单位, 如果 ϵ 有逆. (整环里面随便一个可逆的元都叫做一个单位)

定理 280 ϵ_1 和 ϵ_2 是单位 $\Rightarrow \epsilon_1\epsilon_2$ 是单位; ϵ 是单位 $\Rightarrow \epsilon^{-1}$ 也是单位.

命题 281 a 和 b 不是单位 $\Rightarrow ab$ 不是单位.

说明 282 相伴元对应的关系是一个等价关系.

定义 283 (平凡因子、真因子) $\forall a \in$ 整环 I , 所有的单位以及 a 的相伴元, 叫做 a 的平凡因子. 其余的 a 的因子, 如果还有的话, 叫做 a 的真因子.

定义 284 (素元) 一个整环 I 的一个元 p 叫做一个素元, 如果 p (1) 既不是零元, (2) 也不是单位, 并且 (3) p 只有平凡因子.

定理 285 p 是素元, ϵ 是单位 $\Rightarrow \epsilon p$ 也是素元.

定理 286 (!!) 若 I 是整环, $a \in I, a \neq 0$, 则 a 有真因子 $\Leftrightarrow \exists b, c$ 都不是单位使得 $a = bc$.

推论 287 $a \neq 0$, a 有真因子 $b (a = bc) \Rightarrow c$ 也是 a 的真因子.

说明 288 a 有真因子 $\Rightarrow \exists b, c$ 为 a 的真因子使得 $a = bc$

定义 289 (唯一分解) 我们说, $a \in$ 整环 I , 在 I 里有**唯一分解**, 假如以下条件都能被满足

- (i) 能分解: $a = p_1 p_2 \cdots p_r$ (p_i 是 I 的素元).
- (ii) 若同时 $a = q_1 q_2 \cdots q_s$ (q_i 是 I 的素元), 则 $r = s$, 且我们可以把 q_i 的次序调换, 使得 $q_i = \epsilon_i p_i$ (ϵ_i 是 I 的单位)。

说明 290 若 a 在环 I 中有**唯一分解**, 则 $a \neq 0$ 且 a 不是单位.

说明 291 一个整环的 $\neq 0$ 也不是单位的元, 不一定都有**唯一分解**.

命题 292 0 不是任何元的真因子.

命题 293 定义 I 为所有可以写成 $\frac{m}{2^n}, m \in \mathbb{Z}, n \in \mathbb{N}$ 形式的有理数, 则 I 是整环, 其单位是所有等于 $2^n, n \in \mathbb{Z}$ 的数.

5.1.2 唯一分解环

定义 294 (唯一分解环) 一个整环 I 叫做一个**唯一分解环**, 如果 I 的每一个既 $\neq 0$ 也不是单位的元, 都有唯一分解.

定理 295 一个唯一分解环有以下性质,

(iii) 素元 $p \mid ab \Rightarrow p \mid a$ 或 $p \mid b$.

定理 296 如果一个整环 I 满足:

(i) $\forall a \in I, a \neq 0, a$ 不是单位, 都可以写成 $a = p_1 p_2 \cdots p_r$ (p_i 是素元).

(iii) 素元 $p \mid ab \Rightarrow p \mid a$ 或 $p \mid b$.

则整环 I 是一个唯一分解环.

定义 297 (公因子) 元 c 叫做元 a_1, a_2, \cdots, a_n 的**公因子**, 如果 c 能同时整除 a_1, a_2, \cdots, a_n . 元 a_1, a_2, \cdots, a_n 的一个公因子 d 叫做 a_1, a_2, \cdots, a_n 的**最大公因子**, 如果 d 能被 a_1, a_2, \cdots, a_n 的每个公因子整除.

定理 298 若 I 是一个唯一分解环, $a, b \in I$, 则 a, b 在 I 里一定有最大公因子. 若 d, d' 都是 a, b 的最大公因子, 则它们只差一个单位因子: $d' = \epsilon d$ (ϵ 是单位).

推论 299 一个唯一分解环 I 的 n 个元 a_1, a_2, \cdots, a_n 在 I 里一定有最大公因子, a_1, a_2, \cdots, a_n 的两个最大公因子只能差一个单位因子.

定义 300 (互素) 我们说, 一个唯一分解环的元 a_1, a_2, \cdots, a_n 互素, 如果他们的最大公因子是单位.

命题 301 假定在一个唯一分解环里 $a_1 = db_1, a_2 = db_2, \cdots, a_n = db_n$ ($d \neq 0$), 我们有

$$d \text{ 是 } a_1, a_2, \cdots, a_n \text{ 的最大公因子} \Leftrightarrow b_1, b_2, \cdots, b_n \text{ 互素}.$$

5.1.3 主理想环

定义 302 (主理想环) 一个整环 I 叫做一个**主理想环**, 如果 I 的每一个理想都是一个主理想.

引理 303 假定 I 是一个主理想环, 若存在序列 a_1, a_2, \cdots ($a_i \in I$) 的每一个元素都是前面一个元素的真因子, 则这个序列一定是一个有限序列.

引理 304 (!) 假定 I 是一个主理想环, p 是 I 的一个素元, 则 p 生成的理想 (p) 一定是 I 的最大理想.

定理 305 一个主理想环 I 一定是一个唯一分解环.

命题 306 假定 I 是一个主理想环, 并且 $(a, b) = (d)$, 那么 d 是 a 和 b 的一个最大公因子, 因此 a 和 b 的任何一个最大公因子 d' 都可以写成 $d' = sa + tb$ ($s, t \in I$) 的形式.

命题 307 一个主理想环的非零最大理想都是由一个素元所生成的.

命题 308 两个主理想环 I 和 I_0 , I_0 是 I 的子环, a 和 b 是 I_0 的两个元, d 是这两个元在 I_0 里得一个最大公因子, 则 d 也是这两个元在 I 里的最大公因子.

5.1.4 欧氏环

定义 309 (欧氏环) 一个整环 I 叫做一个**欧氏环**, 如果

- 有一个从 I 的非零元所做成的集合到 ≥ 0 的整数集合的映射 ϕ 存在.
- 给定一个 I 的非零元 a , 则 I 的任何元 b 都可以写成 $b = aq + r$ ($q, r \in I$) 的形式, 这里或者 $r = 0$, 或者 $\phi(r) < \phi(a)$.

定理 310 任何欧氏环 I 一定是主理想环, 从而一定是一个唯一分解环.

说明 311 整数环是一个欧式环, 从而是一个主理想环, 因而是一个唯一分解环.

引理 312 假定 $I[x]$ 是整环 I 上的一个一元多项式环, $I[x]$ 的元 $g(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ 的最高系数 a_n 是 I 的一个单位. 那么 $I[x]$ 的任意多项式 $f(x)$ 都可以写成 $f(x) = q(x)g(x) + r(x)$ ($q(x), r(x) \in I[x]$) 的形式, 这里或者 $r(x) = 0$ 或者 $r(x)$ 的次数小于 $g(x)$ 的次数 n .

定理 313 (!) 一个域 F 上的一元多项式环 $F[x]$ 是一个欧式环. ($\Rightarrow F[x]$ 是主理想环 $\Rightarrow F[x]$ 是唯一分解环).

5.1.5 多项式环的因式分解

定义 314 一个素多项式 (多项式环的素元) 叫做**不可约多项式**, 一个有真因子的多项式叫做**可约多项式**.

命题 315 I 的单位是 $I[x]$ 仅有的单位.

定义 316 (本原多项式) $I[x]$ 的一个元 $f(x)$ 叫做一个**本原多项式**, 如果 $f(x)$ 的系数的最大公因子是单位.

命题 317 一个本原多项式 $\neq 0$.

命题 318 若本原多项式 $f(x)$ 可约, 则 $f(x) = g(x)h(x)$, 这里 $f(x)$ 和 $g(x)$ 的次数都 > 0 , 因而都 $< f(x)$ 的次数.

引理 319 假定 $f(x) = g(x)h(x)$, 那么 $f(x)$ 是本原多项式 $\Leftrightarrow g(x)$ 和 $h(x)$ 都是本原多项式.

引理 320 对于一个唯一分解环 I , 他的商域 Q 做成的一元多项式环 $Q[x]$, $Q[x]$ 中的每个不等于零的多项式 $f(x)$ 都可以写成 $f(x) = \frac{b}{a} f_0(x)$ 的样子. 这里 $a, b \in I$, $f_0(x)$ 是 $I[x]$ 上的本原多项式. 若 $g_0(x)$ 也有 $f_0(x)$ 的性质 (即 $f(x)$ 可以写成 $\frac{b'}{a'} g_0(x)$ 的形式), 则 $g_0(x) = \epsilon f_0(x)$ (ϵ 是 I 的单位).

引理 321 $I[x]$ 的一个本原多项式 $f_0(x)$ 在 $I[x]$ 里可约 $\Leftrightarrow f_0(x)$ 在 $Q[x]$ 里可约.

引理 322 $I[x]$ 中的一个次数 > 0 的本原多项式 $f_0(x)$ 在 $I[x]$ 中有唯一分解.

定理 323 一个唯一分解环 I 上的多项式环 $I[x]$ 也是唯一分解环.

定理 324 若 I 是唯一分解环, 那么 $I[x_1, x_2, \cdots, x_n]$ 也是, 其中 x_1, x_2, \cdots, x_n 是 I 上的未定元.

5.1.6 因式分解与多项式的根

定义 325 $a (\in \text{整环 } I)$ 叫做 $I[x]$ 的多项式的**根**, 如果 $f(a) = 0$.

定理 326 $a (\in \text{整环 } I)$ 是 $f(x)$ 的一个根 $\Leftrightarrow (x - a) \mid f(x)$.

定理 327 给定整环 I 的 k 个不同的元素 a_1, a_2, \cdots, a_k , 那么 a_1, a_2, \cdots, a_k 都是 $f(x)$ 的根 $\Leftrightarrow (x - a_1)(x - a_2) \cdots (x - a_k) \mid f(x)$.

推论 328 $I[x]$ 中的 n 次多项式 $f(x)$, 在 I 中最多有 n 个根.

定义 329 (重根) $a (\in I)$ 叫做 $f(x)$ 的一个**重根**, 如果 $(x - a)^k \mid f(x)$, k 是 ≥ 2 的整数.

定义 330 (导数) 对于 $I[x]$ 中的多项式 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, 定义它的**导数** $f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + a_1$

说明 331 这只是一个形式上的定义, 不能从极限的角度来理解.

命题 332 导数适合以下计算规则

- (i) $[f(x) + g(x)]' = f'(x) + g'(x)$.
- (ii) $[f(x)g(x)]' = f(x)g'(x) + f'(x)g(x)$
- (iii) $[f(x)^t]' = tf(x)^{t-1}f'(x)$, $t \in \mathbb{Z} \geq 2$

定理 333 假定 a 是 $f(x)$ 的一个根, 我们有

$$a \text{ 是一个重根} \Leftrightarrow (x - a) \mid f'(x)$$

推论 334 假定 $I[x]$ 是一个唯一分解环, $a \in I[x]$, $f(x) \in I[x]$, 我们有

$$a \text{ 是 } f(x) \text{ 的一个重根} \Leftrightarrow (x - a) \text{ 能够整除 } f(x) \text{ 和 } f'(x) \text{ 的最大公共因子.}$$

定义 335 如果 $(x - a)^k \mid f(x)$, 但是 $(x - a)^{k+1} \nmid f(x)$, $k \in \mathbb{Z}^+$, 则称 a 是 $f(x)$ 的 k 重根.

定理 336 a 是 $f(x)$ 的 k 重根 $\Rightarrow (x - a)^{k-1} \mid f'(x)$.

定理 337 假定整环 I 的特征是无穷的, 我们有

$$a \text{ 是 } f(x) \text{ 的 } k \text{ 重根} \Rightarrow a \text{ 是 } f'(x) \text{ 的 } k - 1 \text{ 重根.}$$

5.2 扩域

定义 338 (扩域) 一个域 E 叫做一个域 F 的**扩域 (扩张)**, 如果 F 是 E 的子域.

定理 339 令 E 是一个域.

- 若 E 的特征是 ∞ , 则 E 含有一个与有理数同构的子域;
- 若 E 的特征是素数 p , 则 E 含有一个域 $\mathbb{Z}/(p)$ 同构的子域, 其中 \mathbb{Z} 是整数环.

定义 340 (素域) 一个域叫做一个**素域**, 假如他不包含真子域.

说明 341 一个素域或者与有理数域 \mathbb{Q} 同构, 或者与 $\mathbb{Z}_p = \mathbb{Z}/(p)$ 同构.

说明 342 令域 E 是 F 的扩域. 我们从 E 中取一个子集 S . 我们用 $F(S)$ 表示包含 F 和 S 中的所有元素的 E 的最小子域, 把它叫做添加几个 S 于 F 所得的扩域.

说明 343 $F(S)$ 刚好包含 E 的一切可以写成 $\frac{f_1(\alpha_1, \alpha_2, \dots, \alpha_n)}{f_2(\alpha_1, \alpha_2, \dots, \alpha_n)}$ 形式的元, 其中 α_i 是 S 中的任意有限个元素, f_1 和 f_2 ($f_2 \neq 0$) 是这些 α 的多项式.

说明 344 若 S 是一个有限子集, $S = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$, 那么我们也把 $F(S)$ 记作 $F(\alpha_1, \alpha_2, \dots, \alpha_n)$.

定理 345 令 E 是 F 的一个扩域, S_1, S_2 是 E 的两个子集, 那么 $F(S_1)(S_2) = F(S_1 \cup S_2) = F(S_2)(S_1)$.

说明 346 于是我们可以把添加有限集归结为陆续添加单个元素: $F(\alpha_1, \alpha_2, \dots, \alpha_n) = F(\alpha_1)(\alpha_2) \cdots (\alpha_n)$.

定义 347 (单扩域) 添加一个元素 α 于域 F 所得的扩域 $F(\alpha)$ 叫做域 F 的**单扩域 (单扩张)**.

5.2.1 单扩域

定义 348 (代数元、超越元) 假定 E 是 F 的扩域, $\alpha \in E$. α 叫做域 F 上的一个**代数元**, 若 $\exists a_0, a_1, \dots, a_n$ 不都等于零, 使得 $a_0 + a_1\alpha + \dots + a_n\alpha^n = 0$. 如果这样的 a_0, a_1, \dots, a_n 不存在, α 叫做 F 上的一个**超越元**.

定义 349 (单代数扩域、单超越扩域) 若 α 是 F 上的一个代数元, $F(\alpha)$ 叫做 F 的一个**单代数扩域**; 若 α 是 F 上的一个超越元, $F(\alpha)$ 就叫做 F 的一个**单超越扩域**.

定理 350 若 α 是 F 上的一个超越元, 那么 $F(\alpha) \cong F[x]$ 的商域, 其中 $F[x]$ 是 F 上的一个未定元 x 的多项式环.

定理 351 若 α 是 F 上的一个代数元, 那么 $F(\alpha) \cong F[x]/(p(x))$, 其中 $p(x)$ 是 $F[x]$ 的一个 唯一 确定的、最高系数为 1 的不可约多项式, 并且 $p(\alpha) = 0$.

定理 352 令 α 是域 F 上的一个代数元, 并且 $F(\alpha) \cong F[x]/(p(x))$, 那么 $F(\alpha)$ 的每一个元都可以唯一的表达成 $\sum_{i=0}^{n-1} c_i \alpha^i$ ($c_i \in F$) 的形式, 这里 n 是 $p(x)$ 的系数. 要把两个多项式 $f(\alpha)$ 和 $g(\alpha)$ 相加, 只需把相应的系数相加; $f(\alpha)$ 与 $g(\alpha)$ 的乘积等于 $r(\alpha)$, 这里 $r(x)$ 是用 $p(x)$ 除 $f(x)g(x)$ 所得的余式.

定义 353 (极小多项式) $F[x]$ 中满足条件 $p(\alpha) = 0$ 的次数最低的多项式 $p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ ($c_i \in F$), 叫做元 α 的在 F 上的**极小多项式**, n 叫做 α 的在 F 上的**次数**.

说明 354 F 的单超越扩域是存在的, 且它们相互同构.

定理 355 对于任一给定的域 F 以及 F 上的一元多项式环 $F[x]$ 的给定不可约多项式 $p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$, 总存在 F 的单代数扩域 $F(\alpha)$, 其中 α 在 F 上的极小多项式是 $p(x)$.

定理 356 令 $F(\alpha)$ 和 $F(\beta)$ 是域 F 的两个单代数扩域, 并且 α 和 β 在 F 上有相同的极小多项式 $p(x)$. 那么 $F(\alpha) \cong F(\beta)$.

定理 357 在同构的意义下, 存在且仅存在域 F 的一个单扩域 $F(\alpha)$, 其中 α 的极小多项式是 $F[x]$ 的给定的, 最高次数为 1 的不可约多项式.

5.2.2 代数扩域

定理 358 (代数扩域) 若域 F 的扩域 E 的每一个元都是 F 上的一个代数元, 那么 E 叫做 F 的一个**代数扩域** (代数扩张).

定义 359 若是域 F 的一个扩域 E 作为 F 上的向量空间有维数 n , 那么 n 叫做**扩域 E 在 F 上的次数**, 记作 $(E : F)$. 这时 E 叫做 F 的一个**有限扩域**, 否则 E 叫做域 F 的一个**无限扩域**.

定理 360 令 I 是域 F 的有限扩域, 而 E 是 I 的有限扩域. 那么 E 也是 F 的有限扩域, 并且 $(E : F) = (E : I)(I : F)$.

说明 361 已经听不懂了!!! 感觉需要补高等代数中的向量空间的知识...