信息安全的数学基础 (1)

唐　灯

上海交通大学网络空间安全学院

第三章 环和域

§3.1 环和域的定义

§3.2 理想与商环

§3.3 环的同态基本定理

§3.4 同态的应用

§3.5 素理想与极大理想

§3.6 环的特征与素域

§3.7 多项式环

§3.1 环和域的定义

- 环的定义
- 环的基本性质
- 零因子和逆元
- 无零因子环
- 整环和域
- 子环
- 子环的判定

环的定义

定义 1

设 R 是一个非空集合. 如果在 R 上定义了两个代数运算 “ $+$” (称为加法) 和 “ $\cdot$” (称为乘法), 并且满足

(1) R 关于加法为阿贝尔群;
(2) R 关于乘法满足结合律, 即对任意的 $a, b, c \in R$ 有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
(3) R 关于加法和乘法满足分配律, 即对任意的 $a, b, c \in R$ 有
$a \cdot (b + c) = a \cdot b + a \cdot c$ 和 $(b + c) \cdot a = b \cdot a + c \cdot a$,

则称 $(R, +, \cdot)$ 为一个**环** (ring), 或简称 R 为环.

环的定义

注 1.1

(1) 由环的定义知环 R 关于加法是一个阿贝尔群, 称为环 R 的加法群, 记为 $(R,+)$. R 的加法单位元常用 0 表示, 称为环 R 的零元. R 中元素 a 的加法逆元称为 a 的负元, 记作 $-a$;

(2) 如果环 R 的乘法还满足交换律, 则称 R 为**交换环** *(commutative ring)*. 如果环 R 关于乘法有单位元, 即存在元素 e 使得对任意 $a \in R$ 都有 $ae = ea = a$, 则称 R 为**含幺环** *(ring with identity)*, 并称 e 为 R 的**单位元** *(identity)*. 如果环 R 是有单位元的交换环, 则称 R 为**含幺交换环**. 若环 R 有单位元 e, 则 e 唯一.

例

例 2

设 $R=\{0\}$, 规定 $0+0=0, 0\cdot 0=0$, 则 R 构成环, 称为**零环**. 零环是唯一的有单位元且单位元等于零元的环, 并且零元也可逆的环.

例 3

整数集 $\mathbb{Z}$、有理数集 $\mathbb{Q}$、实数集 $\mathbb{R}$、复数集 $\mathbb{C}$ 对于通常数的加法与乘法构成有单位元 1 的交换环, 分别称为整数环、有理数域、实数域、复数域.

例 4

全体偶数的集合

$$2\mathbb{Z}=\{2z \mid z\in\mathbb{Z}\}$$

对于通常数的加法与乘法构成一个没有单位元的交换环.

例

例 5

实数域 $\mathbb{R}$ 上全体 n $(n>1)$ 阶方阵 $M_n(\mathbb{R})$ 的集合关于矩阵的加法与乘法构成一个有单位元 E (单位矩阵) 的非交换环, 称为数域 $\mathbb{R}$ 上的 n **阶实矩阵环**.

例 6

设 m 为大于 1 的正整数, 则 $\mathbb{Z}$ 的模 m 剩余类集

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1}\}$$

关于剩余类的加法和乘法构成有单位元 $\overline{1}$ 的交换环, 称为**模 m 剩余类环** (residue class ring).

例

例 7

设 $R_1, R_2, \cdots, R_n$ 为 n 个环. 令

$$R = R_1 \times R_2 \times \cdots \times R_n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in R_i, i = 1, 2, \cdots, n\}.$$

对任意的 $(a_1, a_2, \cdots, a_n), (b_1, b_2, \cdots, b_n) \in R$, 规定

$$(a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) = (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n),$$

$$(a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n) = (a_1 b_1, a_2 b_2, \cdots, a_n b_n),$$

则 R 关于上面所定义的加法与乘法构成一个环. 这个环称为环 $R_1, R_2, \cdots, R_n$ 的**外直积** (external direct product). 显然, R 有单位元的充分必要条件是每个 R_i 都有单位元, R 是交换环的充分必要条件是每个 R_i 都是交换环.

环的基本性质

定理 8

设 R 是一个环, 则

(1) 对任意 $a \in R$ 有$-(-a) = a$ 和 $a \cdot 0 = 0 \cdot a = 0$, 其中 0 是 R 的零元;

(2) $(-a) \cdot b = a \cdot (-b) = -a \cdot b$, $(-a) \cdot (-b) = a \cdot b$, 其中 $-a$ 表示 a 在加法群中的负元;

(3) 对任意 $n \in \mathbb{Z}$, $a, b \in R$, $(na) \cdot b = a \cdot (nb) = n(a \cdot b)$, 其中当 $n > 0$ 时 na 表示在加法群中 n 个 a 相加, 当 $n < 0$ 时 na 表示在加法群中 $-n$ 个 a 相加后的负元;

(4) 对于 R 中元素 a_i $(1 \leq i \leq m)$ 和 b_j $(1 \leq j \leq n)$, 则

$$\left(\sum a_i\right) \cdot \left(\sum b_j\right) = \sum_i \sum_j a_i \cdot b_j.$$

证明

(1) 因为 $-a$ 是 a 的负元, 因此 a 也是 $-a$ 的负元, 即 $-(-a) = a$. 此外, 因为 $a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 = a \cdot 0 + 0$, 由群的加法消去律得 $a \cdot 0 = 0$. 同理可证$0 \cdot a = 0$.

(2) 因为 $(-a) \cdot b + a \cdot b = (-a + a) \cdot b = 0 \cdot b = 0$, 所以 $(-a) \cdot b$ 是 $-a \cdot b$ 的负元, 因此有 $(-a) \cdot b = -a \cdot b$. 同理可证, $a \cdot (-b) = -a \cdot b$. 进一步, $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$.

(3) 当 $n = 0$, 即为情形 (1). 其次, 当 $n > 0$ 时, 注意到 $na = (n-1)a + a$, 对 n 做归纳法可得 $na = a + \cdots + a$. 因此, $(na) \cdot b = (a + \cdots + a) \cdot b = a \cdot b + \cdots a \cdot b = a \cdot (nb) = n(a \cdot b)$. 类似可证当 $n < 0$ 时 $(na) \cdot b = a \cdot (nb) = n(a \cdot b)$.

(4) 当 $i = 1$ 时, 注意到 $\sum b_j = b_1 + (b_2 + \cdots + b_n)$, 利用分配律并对 j 做归纳法可得 $a_1 \cdot (\sum b_j) \sum_j a_1 \cdot b_j$. 当 $i > 1$ 时, 注意到 $\sum a_j = a_1 + (a_2 + \cdots + a_m)$, 于是利用分配律并对 i 做归纳法可得结论.

推论 9

若环 R 满足 $e = 0$, 则 $R = \{0\}$.

证明: 对任意 $a \in R$, 则 $a = a \cdot e = a \cdot 0 = 0$.

注 9.1

今后, 如无特别声明, 我们总是假定环 R 有单位元并且 $R \neq \{0\}$, 因此在 R 中 $e \neq 0$.

零因子和逆元

定义 10

设环R 有单位元 e, 则

(1) 若两个元素 $a, b \in R \setminus \{0\}$ 满足 $a \cdot b = 0$, 则称 a 为 R 的一个**左零因子** (left zero-divisor), b 为 R 的一个**右零因子** (right zero-divisor). 左零因子与右零因子统称为**零因子**.

(2) 对任意 $a \in R$. 如果存在 $b \in R$ 使得 $ab = ba = e$, 则称 a 是 R 的一个**单位** (unit), 并称 b 为 a 的**逆元** (inverse element); 对任意 $a \in R$, 若 a 可逆, 则 a 的逆元唯一, 记为 a^{-1}.

无零因子环

注 10.1

(1) 环 R 有左零因子则必有右零因子. 若 R 无零因子, 则称为**无零因子环**. 环 R 为无零因子环当且仅当对任意 $a, b \in R$, 若 $a \cdot b = 0$ 则必有 $a = 0$ 或 $b = 0$.

(2) 环 R 中单位的集合构成一个群, 称为 R 的**单位群** *(group of units)*, 记为 $U(R)$.

证明: (2) 显然 $e \in U(R)$, 并且对任意 $a, b \in U(R)$ 有 $(ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = e$, 于是 $ab \in U(R)$, 从而 $U(R)$ 满足封闭性. 对任意 $a \in U(R)$, 由于 $a^{-1}a = aa^{-1} = e$, 于是 $a^{-1} \in U(R)$. 由此可知 $U(R)$ 为群.

例

例 11

例 5 中 n 阶实矩阵环的单位群是 $\mathrm{GL}_n(\mathbb{R})$. 例 6 中模 m 剩余类环的单位群是 $U(m)$;

例 12

$\mathbb{Z}_6$ 的全部零因子为

$$\overline{2}, \overline{3}, \overline{4}.$$

例 13

所有形如

$$\begin{pmatrix} 0 & 0 \\ x & y \end{pmatrix}, \quad x, y \in \mathbb{R}$$

的矩阵可组成环. 其左右零因子分别是

$$\begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix}, a \neq 0 \text{ 与 } \begin{pmatrix} 0 & 0 \\ x & y \end{pmatrix}, x, y \text{ 不全为零.}$$

无零因子环

定理 14

在一个无零因子的环中, 两个**消去律**成立, 即对任意的 $a, b, c \in R$, $c \neq 0$, 如果 $ac = bc$ 或 $ca = cb$, 则 $a = b$.

证明: 设 $ac = bc$, 则

$$(a - b)c = 0.$$

由于 R 无零因子, 且 $c \neq 0$, 因此 $a - b = 0$. (否则, c 就是 R 的一个零因子). 从而 $a = b$, 所以在 R 中右消去律成立. 同理可证, 左消去律也成立.

无零因子环

注 14.1

如果环 R 中两个消去律有一个成立, 则 R 必是无零因子环, 从而另一个消去律也成立.

证明: 假定环 R 中左消去律成立. 考察 $ab = 0$, $a, b \in R$. 如果 $a \neq 0$, 则 $ab = 0 = a0$. 由左消去律得 $b = 0$, 所以 R 无零因子, 从而 R 是无零因子环. 同理可证, 如果环 R 中右消去律成立. 则 R 也是无零因子环

整环和域

定义 15

设 R 是一个有单位元 $e \neq 0$ 的环, 则

(1) 若 R 是无零因子的交换环, 则 R 称为**整环** (domain);

(2) 若 R 中每个非零元都可逆, 则称 R 是一个**除环** (division ring). 非交换的除环称为**体** (skew-field);

(2) 若 R 是一交换的除环, 则称 R 是一个**域** (field).

有限域

注 15.1

(1) 若环 $(F,+,\cdot)$ 为域, 则 $F\setminus\{0\}$ 关于乘法亦是一个阿贝尔群, 称为域的乘法群, 记为 $(F,\cdot)$.
(2) 若域 $(F,+,\cdot)$ 的元素个数有限, 则称 F 为**有限域**.

例 16

整数环 $\mathbb{Z}$, 数域 F 上的一元多项式环 $F[x]$ 都是整环.

例 17

环 $\mathbb{Z}/6\mathbb{Z}$ 中, $2\cdot 3=4\cdot 3=0$, 故 $2,3,4$ 为 $\mathbb{Z}/6\mathbb{Z}$ 的零因子. $\{1,5\}$ 为 $\mathbb{Z}/6\mathbb{Z}$ 的单位群, $\mathbb{Z}/6\mathbb{Z}$ 不是整环.

例

例 18

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 都是域, 分别称为有理数域、实数域和复数域.

例 19

设 p 为素数, 则 $\mathbb{Z}_p$ 是一个含 p 个元素的有限域.

证明: 首先, $\mathbb{Z}_p$ 是一个有单位元的含 p 个元素的交换环, 又因为 $\mathbb{Z}_p$ 的单位群 $U(p) = \mathbb{Z}_p^*$, 所以 $\mathbb{Z}_p$ 中每个非零元都可逆, 因此 $\mathbb{Z}_p$ 是一个域.

子环

定义 20

设 $(R, +, \cdot)$ 是一个环, S 是 R 的一个非空子集. 如果 S 关于 R 的运算构成环, 则称 S 为 R 的一个子环 (subring), 记作 $S < R$.

注 20.1

由子环的定义立即可知, 环 R 本身以及由单独一个零元 $\{0\}$ 所构成的集合关于 R 的运算都构成 R 的子环. 这两个子环称为 R 的**平凡子环**.

子环的判定

定理 21 (子环判定定理)

设 R 是一个环, S 是 R 的一个非空子集, 则 $S < R$ 的充分必要条件是

(1) 对任意的 $a, b \in S, a - b \in S$;

(2) 对任意的 $a, b \in S, ab \in S$.

例

例 22

设 d 是一个整数, $a = dz_1, b = dz_2$ 是 d 的任意两个倍数, 则

$$a - b = d(z_1 - z_2), \quad ab = d(dz_1 z_2)$$

仍是 d 的倍数. 所以 d 的倍数全体

$$d\mathbb{Z} = \{dz \mid z \in \mathbb{Z}\}.$$

构成整数环 $\mathbb{Z}$ 的一个子环. 易知, 如果 $d \neq \pm 1$ 且 $d \neq 0$, 则 $d\mathbb{Z}$ 是一个没有单位元的环. 这个例子告诉我们, 即使一个环有单位元, 其子环也可能没有单位元. 同样, 即使一个环没有单位元, 其子环也可能有单位元 (参见上文直积例子).

例 23

设 I 为 $\mathbb{Z}$ 的子环. 证明: 存在唯一的非负整数 d, 使

$$I = d\mathbb{Z} = \{dz \mid z \in \mathbb{Z}\}$$

证明: **存在性**. (1) 如果 $I = \{0\}$, 则取 $d = 0$, 有 $I = d\mathbb{Z}$.

(2) 如 $I \neq \{0\}$, 则有 $z > 0$, 使 $z \in I$. 令

$$d = \min\{z \in I \mid z > 0\},$$

则 $d > 0$ 且 $d \in I$. 易知 $d\mathbb{Z} \subseteq I$. 又对 $z \in I$ 有 $q, r \in \mathbb{Z}, 0 \leq r < d$ 使

$$z = dq + r.$$

从而 $r = z - dq \in I$. 因为 $r \in I, 0 \leq r < d$, 由 d 的选取知 $r = 0$, 所以 $z \in d\mathbb{Z}$, 从而 $I \subseteq d\mathbb{Z}$. 由此得 $I = d\mathbb{Z}$. 这就证明了存在性.

唯一性. 设 $I = d_1\mathbb{Z} = d_2\mathbb{Z}, d_1 \geq 0, d_2 \geq 0$.

(1) 如果 $d_1 = 0$ 则 $I = \{0\}$, 所以 $d_2 = 0$, 从而 $d_1 = d_2$.

(2) 如果 $d_1 > 0$, 则 $d_2 > 0$. 因为 $d_1 \in I$, 所以 $d_2 \mid d_1$. 同理, $d_1 \mid d_2$. 所以 $d_1 = \pm d_2$. 又因为 d_1, d_2 都非负, 所以 $d_1 = d_2$.

练习

例 24

求 $\mathbb{Z}_{18}$ 的所有子环.

解: 设 I 为 $\mathbb{Z}_{18}$ 的任一子环, 则 I 是 $\mathbb{Z}_{18}$ 的加法子群. 注意到 $\mathbb{Z}_{18}$ 是循环群, 因此 $I = \langle \bar{r} \rangle$, 其中 $\bar{r}$ 可能的取值为 $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{6}, \overline{9}$, 即 $\mathbb{Z}_{18}$ 有 6 个子加群:

$$I_1 = \{\overline{0}\};\ I_2 = \langle \overline{1} \rangle = \mathbb{Z}_{18};$$

$$I_3 = \langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}\} = \overline{2}\mathbb{Z}_{18};$$

$$I_4 = \langle \overline{3} \rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}, \overline{12}, \overline{15}\} = \overline{3}\mathbb{Z}_{18};$$

$$I_5 = \langle \overline{6} \rangle = \{\overline{0}, \overline{6}, \overline{12}\} = \overline{6}\mathbb{Z}_{18};$$

$$I_6 = \langle \overline{9} \rangle = \{\overline{0}, \overline{9}\} = \overline{9}\mathbb{Z}_{18}.$$

显然它们都是 $\mathbb{Z}_{18}$ 的子环, 所以 $\mathbb{Z}_{18}$ 共有 6 个子环

$$\{\overline{0}\}, \mathbb{Z}_{18}, \overline{2}\mathbb{Z}_{18}, \overline{3}\mathbb{Z}_{18}, \overline{6}\mathbb{Z}_{18}, \overline{9}\mathbb{Z}_{18}.$$

§3.1 环和域的定义

- 环的定义
- 环的基本性质
- 零因子和逆元
- 无零因子环
- 整环和域
- 子环
- 子环的判定

§3.2 理想与商环

- 理想
- 理想的和与交
- 主理想
- 生成理想
- 商群的运算
- 商环

理想

定义 25

设 R 为环, I 为 R 的非空子集, 如果 I 满足

(1) 对任意的 $r_1, r_2 \in I, r_1 - r_2 \in I$;

(2) 对任意的 $r \in I, s \in R, rs, sr \in I$,

则称 I 为环 R 的**一个理想** (ideal), 记作 $I \triangleleft R$. 又如果 $I \subsetneq R$, 则称 I 为 R 的**真理想** (proper ideal).

注 25.1

(1) 由理想的定义可知, 如果 I 为 R 的理想, 则 I 必为 R 的子环.

(2) $\{0\}$ 与 R 本身显然都是 R 的理想. 这两个理想称为 R 的**平凡理想** *(trivial ideal)*.

(3) 设 R 为包含单位元的环, 若有 $I \triangleleft R$ 且 $e \in I$, 则 $I = R$.

(4) 若 R 为域, 则 R 只有平凡理想.

例

例 26

试求 $\mathbb{Z}$ 的所有理想.

解: 设 I 为 $\mathbb{Z}$ 的任一理想, 则 I 为 $\mathbb{Z}$ 的子环. 由例 23 知存在 $d \in \mathbb{Z}$, $d \geq 0$, 使得 $I = d\mathbb{Z}$.

反之, 设 I 为 $\mathbb{Z}$ 的任一子环, 那么存在 $d \in \mathbb{Z}$, 使 $I = d\mathbb{Z}$, 则对任意的 $r = dx, s = dy \in I, z \in \mathbb{Z}$,

$$r - s = dx - dy = d(x - y) \in I,$$
$$rz = zr = (dx)z = d(xz) \in I,$$

所以 $d\mathbb{Z}$ 为 $\mathbb{Z}$ 的理想.

由此知, I 为 $\mathbb{Z}$ 的理想当且仅当 I 为 $\mathbb{Z}$ 的子环. 因此 $\mathbb{Z}$ 的全部理想为 $d\mathbb{Z}$, 其中 $d \in \mathbb{Z}, d \geq 0$.

理想的和与交

定义 27

设 R 为环, I, J 都是 R 的理想, 集合

$$I + J = \{a + b \mid a \in I, b \in J\} \quad \text{与} \quad I \cap J$$

分别称为理想 I 与 J 的和与交.

定理 28

设 R 为环, I, J 都是 R 的理想, 则 I 与 J 的和与交都是 R 的理想.

定理 29

设 R 是环, 则

(1) R 的任意有限多个理想的和还是 R 的理想;
(2) R 的任意 *(*有限或无限*)* 多个理想的交还是 R 的理想.

证明

(1) 设 $a, b \in I + J, x \in R$, 则有 $a_1, b_1 \in I, a_2, b_2 \in J$, 使 $a = a_1 + a_2$, $b = b_1 + b_2$. 从而

$$a - b = (a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) \in I + J,$$

$$xa = x(a_1 + a_2) = xa_1 + xa_2 \in I + J,$$

$$ax = (a_1 + a_2)x = a_1x + a_2x \in I + J,$$

所以 $I + J$ 为 R 的理想.

(2) 对任意的 $a, b \in I \cap J, x \in R$, 则 $a, b \in I$ 且 $a, b \in J$, 从而

$$a - b, ax, xa \in I \text{ 且 } a - b, ax, xa \in J,$$

所以

$$a - b, ax, xa \in I \cap J.$$

因此 $I \cap J$ 为 R 的理想.

主理想

定义 30

设 R 是环. 对任意 $a \in R$, 令

$$\Sigma = \{I \lhd R \mid a \in I\},\ \langle a \rangle = \bigcap_{I \in \Sigma} I,$$

则 $\langle a \rangle$ 称为 R 的由 a 生成的**主理想** (principal ideal).

注 30.1

(1) 因为 $a \in I\,(I \in \Sigma)$, 所以 $a \in \langle a \rangle$, 从而 $\langle a \rangle \in \Sigma$;

(2) 由于 $\langle a \rangle$ 是包含 a 的理想, 并且 $\langle a \rangle$ 是所有包含 a 的理想的交, 所以 $\langle a \rangle$ 是 R 的包含 a 的最小理想.

主理想

定理 31

设 R 为环, $a \in R$, 则

(1) $\langle a \rangle = \{\sum_{i=1}^{n} x_i a y_i + xa + ay + ma \mid x_i, y_i, x, y \in R, n \in \mathbb{N}, m \in \mathbb{Z}\}$;

(2) 如果 R 是含幺环, 则

$$\langle a \rangle = \left\{ \sum_{i=1}^{n} x_i a y_i \mid x_i, y_i \in R, n \in \mathbb{N} \right\};$$

(3) 如果 R 是交换环, 则 $\langle a \rangle = \{xa + ma \mid x \in R, m \in \mathbb{Z}\}$;

(4) 如果 R 是有单位元的交换环, 则 $\langle a \rangle = aR = \{ar \mid r \in R\}$.

证明

(1) 设

$$I = \left\{ \sum_{i=1}^{n} x_i a y_i + xa + ay + ma \mid x_i, y_i, x, y \in R, n \in \mathbb{N}, m \in \mathbb{Z} \right\}.$$

易知 I 为 R 的理想. 因为 $a = 1 \cdot a \in I\,(1 \in \mathbb{Z})$, 所以 I 为包含 a 的理想, 从而 $\langle a \rangle \subseteq I$. 又因为 $\langle a \rangle$ 是由 a 生成的理想, 所以 $\langle a \rangle$ 必包含所有的形如

$$xay, xa, ay \text{ 与 } ma \quad (x, y \in R, m \in \mathbb{Z})$$

的元素及这些元素的和. 因此 $\langle a \rangle \supseteq I$. 于是 $\langle a \rangle = I$. (2) 如果 R 有单位元 e, 则

$$ma = (me)ae(m \in \mathbb{Z}), \quad xa = xae, \quad ay = eay$$

都是形如 xay 的元素. 所以

$$\langle a \rangle = \left\{ \sum_{i=1}^{n} x_i a y_i \mid x_i, y_i \in R, n \in \mathbb{N} \right\}.$$

证明 (续)

(3) 如果 R 是交换环, 则 $xay = xya, ay = ya.$ 从而

$$\sum_{i=1}^{n} x_i a y_i + xa + ya + ma = \sum_{i=1}^{n} x_i y_i a + xa + ya + ma = x'a + ma, \quad x' \in R,$$

所以 $\langle a \rangle = \{xa + ma \mid x \in R, m \in \mathbb{Z}\}.$

(4) 如果 R 是有单位元 e 的交换环, 则 $ma = (me)a$, 所以

$$\langle a \rangle = \{xa \mid x \in R\} = aR.$$

主理想

推论 32

整数环 $\mathbb{Z}$ 的每个理想都是主理想.

推论 33

模 m 剩余类环 $\mathbb{Z}_m$ 的每个理想都是主理想.

证明: 设 I 为 $\mathbb{Z}_m$ 的任一个理想, 则 $(I, +)$ 是循环群, 从而

$$I = \langle a \rangle,$$

所以 I 为主理想.

生成理想

注 33.1

设 R 为环, $a_1, a_2, \cdots, a_s \in R$, 则 $\langle a_1 \rangle, \langle a_2 \rangle, \cdots, \langle a_s \rangle$ 都是 R 的理想. 令

$$\langle a_1, a_2, \cdots, a_s \rangle = \langle a_1 \rangle + \langle a_2 \rangle + \cdots + \langle a_s \rangle,$$

则 $\langle a_1, a_2, \cdots, a_s \rangle$ 为 R 的理想, 称为 R 的由 $a_1, a_2, \cdots, a_s$ 生成的理想.
易知, $\langle a_1, a_2, \cdots, a_s \rangle$ 是 R 的含 $a_1, a_2, \cdots, a_s$ 的最小理想.

例

例 34

在 $\mathbb{Z}$ 中, 如果 $a, b \in \mathbb{Z}$, 则 $\langle a, b\rangle$ 是怎样的主理想?

解: (1) 如果 a, b 都是零, 则显然 $\langle a, b\rangle = \{0\} = \langle 0\rangle$.

(2) 如果 a, b 不全为零, 设 a, b 的最大公因子为 d, 则存在 $s, t \in \mathbb{Z}$, 使

$$d = as + bt \in \langle a, b\rangle,$$

所以 $\langle d\rangle \subseteq \langle a, b\rangle$. 又因为 a, b 都是 d 的倍数, 所以 $a, b \in \langle d\rangle$, 从而 $\langle a, b\rangle \subseteq \langle d\rangle$. 所以

$$\langle a, b\rangle = \langle d\rangle,$$

即 $\langle a, b\rangle$ 是由 a, b 的最大公因子 d 所生成的主理想 $\langle d\rangle$.

商群的运算

定义 35

设 R 是一个环, I 是环 R 的一个理想, 从而 $(I,+)$ 是 $(R,+)$ 的正规子群, 于是有商群:

$$R/I = \{\bar{x} = x + I \mid x \in R\},$$

其加法运算定义为

$$\bar{x} + \bar{y} = \overline{x+y}, \quad x, y \in R.$$

在 R/I 规定乘法运算为

$$\bar{x} \cdot \bar{y} = \overline{xy}, \quad x, y \in R.$$

定理 36

设 R 是一个环, I 是环 R 的一个理想. 则 R/I 关于定义 *35* 中所规定的加法和乘法运算构成环.

证明: (1) 设 $x_1, y_1, x_2, y_2 \in R$, 且 $\bar{x}_1 = \bar{x}_2, \bar{y}_1 = \bar{y}_2$, 则 $x_1 - x_2, y_1 - y_2 \in I$, 从而

$$\begin{aligned} x_1y_1 - x_2y_2 &= x_1y_1 - x_1y_2 + x_1y_2 - x_2y_2 \\ &= x_1(y_1 - y_2) + (x_1 - x_2)y_2 \in I. \end{aligned}$$

由此得 $\overline{x_1y_1} = \overline{x_2y_2}$. 所以以上规定运算定义了 R/I 的乘法运算.

证明 (续)

(2) 对任意的 $x, y, z \in R$,

$$(\bar{x} \cdot \bar{y}) \cdot \bar{z} = \overline{xy} \cdot \bar{z} = \overline{xyz},\ \bar{x} \cdot (\bar{y} \cdot \bar{z}) = \bar{x} \cdot \overline{yz} = \overline{xyz},$$

所以 R/I 关于乘法满足结合律.

(3) 对任意的 $x, y, z \in R$,

$$\begin{aligned}
\bar{x} \cdot (\bar{y} + \bar{z}) &= \bar{x} \cdot \overline{y + z} = \overline{x(y + z)} \\
&= \overline{xy + xz} = \overline{xy} + \overline{xz} \\
&= \bar{x} \cdot \bar{y} + \bar{x} \cdot \bar{z}, \\
(\bar{y} + \bar{z}) \cdot \bar{x} &= \overline{y + z} \cdot \bar{x} = \overline{(y + z)x} \\
&= \overline{yx + zx} = \overline{yx} + \overline{zx} \\
&= \bar{y} \cdot \bar{x} + \bar{z} \cdot \bar{x},
\end{aligned}$$

所以 R/I 关于加法与乘法满足两个分配律. 因此 R/I 关于所规定的运算构成环.

商环

定义 37

称环 R/I 为环 R 关于它的理想 I 的**商环** (quotient ring).

定理 38

设 R 为环, I 是 R 的理想, 则

(1) $\overline{0} = I$ 为 R/I 的零元;

(2) 如果 R 有单位元 e, 且 $e \notin I$, 则 $\bar{e} = e + I$ 为 R/I 的单位元;

(3) 如果 R 是交换环, 则 R/I 也是交换环.

例

例 39

设 $m \in \mathbb{Z}, m > 1$, 则

$$\mathbb{Z}/\langle m\rangle = \{\bar{a} = a + \langle m\rangle \mid a = 0, 1, 2, \cdots, m-1\}$$

且

$$\bar{a} + \bar{b} = \overline{a+b}, \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

因此, $\mathbb{Z}$ 对于 $\langle m\rangle$ 的商环就是 $\mathbb{Z}$ 关于模 m 的剩余类环, 即

$$\mathbb{Z}/\langle m\rangle = \mathbb{Z}_m.$$

注 39.1

由例 *39* 可知, $\mathbb{Z}/\langle m\rangle$ 为域的充分必要条件是 m 为素数.

§3.3 环的同态基本定理

- 环的同态
- 同态的基本性质
- 同态的核
- 环同态基本定理
- 环的第二同构定理
- 环的扩张定理

同态

定义 40

设 R 和 R' 为两个环, ϕ 是集合 R 到 R' 的映射. 如果对任意的 $a, b \in R$, 有

(1) $\phi(a+b) = \phi(a) + \phi(b)$;

(2) $\phi(ab) = \phi(a)\phi(b)$,

则称 ϕ 为环 R 到环 R' 的一个**同态映射** (homomorphism), 简称**同态**. 当同态映射 ϕ 作为集合映射是满射时, 称 ϕ 为**满同态** (epimorphism); 当同态映射 ϕ 作为集合映射是单射时, 称 ϕ 为**单同态** (monomorphism); 当同态映射 ϕ 作为集合映射是一一映射时, 称 ϕ 为 R 到 R' 的**同构** (isomorphism), 记作 $\phi : R \cong R'$.

零同态

例 41

设 R 与 R' 是两个环. 对任意的 $a \in R$, 令

$$\begin{aligned} \phi: \quad & R \longrightarrow R', \\ & a \longmapsto 0, \end{aligned}$$

则对任意的 $a, b \in R$,

$$\phi(a+b) = 0 = \phi(a) + \phi(b),$$
$$\phi(ab) = 0 = \phi(a)\phi(b),$$

所以 ϕ 是 R 到 R' 的一个同态. 这个同态称为**零同态** (zero homomorphism).

例

例 42

设 $R=\mathbb{Z}, R'=\mathbb{Z}_m$. 对任意的 $a\in\mathbb{Z}$, 令

$$\begin{aligned}\psi:\ \mathbb{Z} &\longrightarrow \mathbb{Z}_m,\\ a &\longmapsto \bar{a},\end{aligned}$$

则 ψ 为 $\mathbb{Z}$ 到 $\mathbb{Z}_m$ 的满映射. 又对任意的 $a,b\in\mathbb{Z}$,

$$\psi(a+b)=\overline{a+b}=\bar{a}+\bar{b}=\psi(a)+\psi(b),$$

$$\psi(ab)=\overline{ab}=\bar{a}\bar{b}=\psi(a)\psi(b).$$

从而 ψ 为 $\mathbb{Z}$ 到 $\mathbb{Z}_m$ 的满同态.

自然同态

例 43

设 R 是环, I 是 R 的理想. 对任意的 $a \in R$, 令

$$\begin{array}{rccc} \eta: & R & \longrightarrow & R/I, \\ & a & \longmapsto & \bar{a}, \end{array}$$

则 η 为 R 到它的商环 R/I 的满映射. 又对任意的 $a, b \in R$,

$$\eta(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \eta(a) + \eta(b),$$

$$\eta(ab) = \overline{ab} = \bar{a}\bar{b} = \eta(a)\eta(b),$$

所以 η 为 R 到它的商环 R/I 的一个满同态. 这个同态称为**自然同态** (natural homomorphism).

同态的基本性质

定理 44

设 ϕ 是环 R 到 R' 的同态, 则对任意的 $a \in R$,

(1) $\phi(0_R) = 0_{R'}$;

(2) $\phi(na) = n\phi(a), \quad \forall n \in \mathbb{Z}$;

(3) $\phi(a^n) = (\phi(a))^n, \quad \forall n \in \mathbb{N}$.

证明: (1) $\phi(0_R) + 0_{R'} = \phi(0_R) = \phi(0_R + 0_R) = \phi(0_R) + \phi(0_R)$. 由加法群的消去律立即可得 $\phi(0_R) = 0_{R'}$.

(2) $\phi(na) = \phi((n-1)a + a) = \phi((n-1)a) + \phi(a) = \cdots =$
$(n-1)\phi(a) + \phi(a) = n\phi(a)$.

(3) $\phi(a^n) = \phi\left(a^{n-1}a\right) = \phi\left(a^{n-1}\right)\phi(a) = \cdots = (\phi(a))^{n-1}\phi(a) = (\phi(a))^n$.

同态的基本性质

定理 45

设 R 与 R' 都是含幺环, e 与 e' 分别是它们的单位元, ϕ 是 R 到 R' 的环同态.

(1) 如果 ϕ 是满同态, 则 $\phi(e) = e'$;
(2) 如果 R' 为无零因子环且 $\phi(e) \neq 0$, 则 $\phi(e) = e'$;
(3) 如果 $\phi(e) = e'$, 则对 R 的任一单位 u, $\phi(u)$ 是 R' 的单位, 且 $(\phi(u))^{-1} = \phi\left(u^{-1}\right)$.

证明

(1) 对任意的 $a' \in R'$, 因 ϕ 是满映射, 所以存在 $a \in R$, 使 $\phi(a) = a'$, 则

$$\phi(e)a' = \phi(e)\phi(a) = \phi(ea) = \phi(a) = a',$$

$$a'\phi(e) = \phi(a)\phi(e) = \phi(ae) = \phi(a) = a'.$$

因此, $\phi(e)$ 是单位元, 由单位元的唯一性得 $\phi(e) = e'$.

(2) 令 $r' = \phi(e)$, 则 $r' \neq 0$, 从而

$$r'e' = r' = \phi(e) = \phi(ee) = \phi(e)\phi(e) = r'\phi(e).$$

因为 R' 无零因子, 所以消去律成立. 在上式两边消去 r' 得 $e' = \phi(e)$.

(3) 设 u 为 R 的任一单位, 则

$$e' = \phi(e) = \phi\left(uu^{-1}\right) = \phi(u)\phi\left(u^{-1}\right),$$

$$e' = \phi(e) = \phi\left(u^{-1}u\right) = \phi\left(u^{-1}\right)\phi(u),$$

所以 $\phi(u)$ 是 R' 的单位, 且 $(\phi(u))^{-1} = \phi\left(u^{-1}\right)$.

同态的核

定义 46

设 ϕ 为环 R 到环 R' 的同态映射. 称集合

$$K = \{a \in R \mid \phi(a) = 0\}$$

为环同态 ϕ 的**核** (kernel), 记作 $\operatorname{Ker}\phi$.

定理 47

设 ϕ 为环 R 到 R' 的环同态, 则 $\operatorname{Ker}\phi$ 为 R 的理想.

证明: 对任意的 $a, b \in \operatorname{Ker}\phi, r \in R$, 有

$$\phi(a-b) = \phi(a) - \phi(b) = 0 - 0 = 0,$$

$$\phi(ra) = \phi(r)\phi(a) = \phi(r)0 = 0,$$

$$\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0.$$

从而 $a-b, ra, ar \in \operatorname{Ker}\phi$, 所以 $\operatorname{Ker}\phi$ 为 R 的理想.

环同态基本定理

定理 48 (环同态基本定理)

设 ϕ 是环 R 到 R' 的满同态, 则有环同构

$$\tilde{\phi} : R/\operatorname{Ker}\phi \cong R'.$$

证明: (1) 记 $K = \operatorname{Ker}\phi$, 则 K 为环 R 的理想. 对任意的 $\bar{a} \in R/K$, 令

$$\begin{aligned} \widetilde{\phi} : \quad R/K &\longrightarrow R', \\ \bar{a} &\longmapsto \phi(a). \end{aligned}$$

(2) 设 $\bar{a} = \bar{b}$, 即 $a - b \in K$, 则 $\phi(a - b) = 0$, 从而 $\phi(a) = \phi(b)$, 于是

$$\widetilde{\phi}(\bar{a}) = \phi(a) = \phi(b) = \widetilde{\phi}(\bar{b}),$$

所以 $\widetilde{\phi}$ 是 R/K 到 R' 的映射.

证明 (续)

(3) 对任意的 $\bar{a}, \bar{b} \in R/K$, 有

$$\widetilde{\phi}(\bar{a}+\bar{b}) = \widetilde{\phi}(\overline{a+b}) = \phi(a+b) = \phi(a)+\phi(b) = \widetilde{\phi}(\bar{a})+\widetilde{\phi}(\bar{b}),$$

$$\widetilde{\phi}(\bar{a}\bar{b}) = \widetilde{\phi}(\overline{ab}) = \phi(ab) = \phi(a)\phi(b) = \widetilde{\phi}(\bar{a})\widetilde{\phi}(\bar{b}),$$

所以 $\widetilde{\phi}$ 是 R/K 到 R' 的同态映射.

(4) 对任意的 $a' \in R'$, 因为 ϕ 是满同态, 所以存在 $a \in R$ 使 $\phi(a) = a'$. 从而

$$\widetilde{\phi}(\bar{a}) = \phi(a) = a'.$$

于是, $\widetilde{\phi}$ 是 R/K 到 R' 的满同态.

(5) 设 $\bar{a}, \bar{b} \in R/K$, 如果 $\widetilde{\phi}(\bar{a}) = \widetilde{\phi}(\bar{b})$, 则

$$\phi(a-b) = \widetilde{\phi}(\overline{a-b}) = \widetilde{\phi}(\bar{a}) - \widetilde{\phi}(\bar{b}) = 0.$$

从而 $a-b \in \operatorname{Ker}\phi$, 由此得 $\bar{a} = \bar{b}$, 所以 $\tilde{\phi}$ 是 R/K 到 R' 的单同态.

这就证明了 $\tilde{\phi}$ 是 R/K 到 R' 的同构映射.

例

例 49

由例 42 知, ψ 是 $\mathbb{Z}$ 到 $\mathbb{Z}_m$ 的满同态. 注意到 $\operatorname{Ker}\psi = \langle m \rangle$, 则由环同态基本定理得

$$\mathbb{Z}/\langle m \rangle \cong \mathbb{Z}_m.$$

环的第二同构定理

定理 50 (环的第二同构定理)

设 S 为 R 的子环, I 为 R 的理想, 则 $S \cap I$ 是 S 的理想且

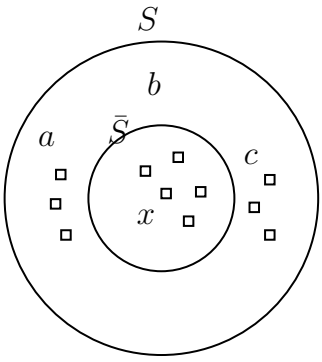
$$S/(S \cap I) \cong (S + I)/I.$$

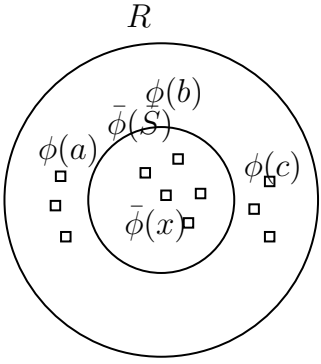
证明: 作业.

环的扩张定理

定理 51 (环的扩张定理)

设 $\bar{S}$ 与 R 是两个没有公共元素的环, $\bar{\phi}$ 是环 $\bar{S}$ 到环 R 的单同态, 则存在一个与环 R 同构的环 S 及由环 S 到 R 的同构映射ϕ, 使 $\bar{S}$ 为 S 的子环且 $\phi|_{\bar{S}} = \bar{\phi}$.





证明

证明: (1) 令 $S = (R \setminus \bar{\phi}(\bar{S})) \cup \bar{S}$. 对任意的 $x \in S$, 规定

$$\phi(x) = \begin{cases} \bar{\phi}(x), & x \in \bar{S}, \\ x, & x \notin \bar{S}, \end{cases}$$

则由 $\bar{S}$ 与 R 没有公共元素这一条件可知 ϕ 是 S 到 R 一一对应, 且 $\phi|_{\bar{S}} = \bar{\phi}$.

(2) 对任意的 $x, y \in S$, 规定

$$x + y = \phi^{-1}(\phi(x) + \phi(y)),$$

$$x \cdot y = \phi^{-1}(\phi(x) \cdot \phi(y)),$$

易知, 如此定义的加法与乘法是 S 的代数运算.

(3) 由环的定义直接验证可知 $(S, +, \cdot)$ 构成环. 且对任意的 $x, y \in S$,

$$\phi(x + y) = \phi(x) + \phi(y),$$

$$\phi(xy) = \phi(x) \cdot \phi(y),$$

证明 (续)

所以 ϕ 是 S 到 R 的环同态. 又因为 ϕ 是一一对应, 即 ϕ 既是单的, 又是满的, 所以 ϕ 是环同构, 即 $\phi : S \cong R$.

(4) 由 S 的定义知 $\bar{S}$ 是 S 的非空子集, 且对任意的 $x, y \in \bar{S}$,

$$\begin{aligned} x \underset{S}{+} y &= \phi^{-1}(\phi(x) \underset{R}{+} \phi(y)) = \phi^{-1}(\bar{\phi}(x) + \bar{\phi}(y)) \\ &= \phi^{-1}\left(\bar{\phi}\left(x \underset{\bar{S}}{+} y\right)\right) = \phi^{-1}(\phi(x \underset{\bar{S}}{+} y)) \\ &= x \underset{\bar{S}}{+} y. \end{aligned}$$

同理可证,

$$x \underset{S}{\cdot} y = x \underset{\bar{S}}{\cdot} y.$$

从而知 S 的加法与乘法在 $\bar{S}$ 上的限制就是环 $\bar{S}$ 的加法与乘法, 所以 $\bar{S}$ 为 S 的子环.

§3.3 环的同态基本定理

- 环的同态
- 同态的基本性质
- 同态的核
- 环同态基本定理
- 环的第二同构定理
- 环的扩张定理

§3.4 同态的应用

- 环的外直积
- 环的内直积
- 中国剩余定理
- 未定元
- 一元多项式环的定义
- 整环的商域

环的外直积

定义 52

设 $R_1, R_2, \cdots, R_n$ 为 n 个环. 构造集合 $R_1, R_2, \cdots, R_n$ 的笛卡尔积

$$R = \prod_i^n R_i = R_1 \times \cdots \times R_n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in R_i, i \in [n]\}.$$

对任意的 $(a_1, a_2, \cdots, a_n), (b_1, b_2, \cdots, b_n) \in R$, 规定

$$(a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) = (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n),$$

$$(a_1, a_2, \cdots, a_n) \cdot (b_1, b_2, \cdots, b_n) = (a_1 b_1, a_2 b_2, \cdots, a_n b_n),$$

则 R 关于上面所定义的加法与乘法构成一个环. 这个环称为环 $R_1, R_2, \cdots, R_n$ 的**外直积** (external direct product).

环的外直积

注 52.1

设 $R=\prod_{i=1}^{n} R_i$ 是环 $R_1, R_2, \cdots, R_n$ 的外直积, 则

(1) 如果 $0_1, 0_2, \cdots, 0_n$ 分别是 $R_1, R_2, \cdots R_n$ 的零元, 则 R 中的零元是 $(0_1, 0_2, \cdots, 0_n)$;

(2) 如果 $e_1, e_2, \cdots, e_n$ 分别是 $R_1, R_2, \cdots R_n$ 的单位元, 则 $(e_1, e_2, \cdots, e_n)$ 是 R 的单位元;

(3) R 有单位元的充分必要条件是每个 R_i 都有单位元, R 是交换环的充分必要条件是每个 R_i 都是交换环.

外直积的性质

定理 53

$R = \prod_{i=1}^{n} R_i$ 是环 $R_1, R_2, \cdots, R_n$ 的外直积, $0_1, 0_2, \cdots, 0_n$ 分别是环 $R_1, R_2, \cdots R_n$ 的零元, 则

(1) 令 $R'_k = \{0_1\} \times \cdots \times \{0_{k-1}\} \times R_k \times \{0_{k+1}\} \times \cdots \times \{0_n\}$, 则 R'_k 是 R 的一个理想, 且同构于 R_k;

(2) $R = \sum_{i=1}^{n} R'_k$;

(3) 环 R 中的任意元素都能用 $R'_1, \cdots, R'_n$ 的元素之和唯一地表示, 即如果 $a_1 + \cdots + a_n = b_1 + \cdots + b_n$, 其中 $a_k, b_k \in R'_k$, 那么对所有 $k \in [n]$, 都有 $a_k = b_k$.

环的内直积

定义 54

如果环 R 的理想 $R_1, \cdots, R_n$ 满足下述两个条件:

(1) $R = \sum_{i=1}^{n} R_i$;

(2) 环 R 中的任意元素都能用 $R_i, \cdots, R_n$ 的元素之和唯一地表示, 即如果 $a_1 + \cdots + a_n = b_1 + \cdots + b_n$, 其中 $a_i, b_i \in R_i$, 那么对所有 $i \in [n]$, 都有 $a_i = b_i$,

则称 $R = \sum_{i=1}^{n} R_i$ 是 $R_1, \cdots, R_n$ 的**内直积** (internal direct product).

内直积的性质

定理 55

如果环 R 是其理想 $R_1, \cdots, R_n$ 的内直积, 则 $R \cong \prod_{i=1}^{n} R_i$.

证明: 考虑如下映射:

$$\begin{aligned} \phi: \quad \prod_{i=1}^{n} R_i &\longrightarrow R, \\ (r_1, \cdots, r_n) &\longmapsto \sum_{i=1}^{n} r_i. \end{aligned}$$

显然映射 ϕ 是一个加法同态映射.

现在考虑乘法的同态映射. 如果 $a \in R_i$ 且 $b \in R_j$, 其中 $i \neq j$, 那么 $ab \in R_i \cap R_j$. 因此有 $ab = 0_i + ab = ab + 0_j$, 其中 $0_i, 0_j$ 分别是 R_i 和 R_j 的零元. 于是由内直积定义第 (2) 条可知 $ab = 0$. 从而对任意 $(a_1, \cdots, a_n), (b_1, \cdots, b_n) \in \prod_{i=1}^{n} R_i$ 都有

证明 (续)

$$\begin{aligned}\phi\big((a_1,\cdots,a_n)(b_1,\cdots,b_n)\big) &= \phi\big((a_1b_1,\cdots,a_nb_n)\big)\\ &= a_1b_1+\cdots+a_nb_n\\ &= (a_1+\cdots+a_n)(b_1+\cdots+b_n)\\ &= \phi\big((a_1,\cdots,a_n)\big)\phi\big((b_1,\cdots,b_n)\big).\end{aligned}$$

因此 f 对上述乘法也是一个同态映射.

若有 $\phi\big((r_1,\cdots,r_n)\big)=\phi\big((s_1,\cdots,s_n)\big)$, 其中 $r_i,s_i\in R_i$, 则有 $\sum_{i=1}^n r_i=\sum_{i=1}^n s_i$, 由内直积定义第 (2) 条可知对任意 $i\in[n]$ 都有 $r_i=s_i$. 由内直积定义第 (1) 条立即可知 ϕ 是满射.

综上, 映射 ϕ 是一个从 $\prod_{i=1}^n R_i$ 到 R 的一个环同构, 从而 $R\cong\prod_{i=1}^n R_i$.

内直积的判定

定理 56

设 $R_1, \cdots, R_n$ 是环 R 的理想, 则下述三个条件等价:

(1) R 是 $R_1, \cdots, R_n$ 的内直积;

(2) $(R_1 + \cdots + R_{i-1}) \cap R_i = \{0\}$, 对任意 $i = 2, \cdots, n$;

(3) $(R_1 + \cdots + R_{i-1} + R_{i+1} + \cdots + R_n) \cap R_i = \{0\}$, 对任意 $i = 2, \cdots, n$.

中国剩余定理

定理 57 (中国剩余定理)

设 R 是含么环, $I_1, \cdots, I_n$ 为环 R 的理想. 并且对任意 $1 \leq i \neq j \leq n$, I_i 和 I_j 互素, 即 $I_i + I_j = R$. 则有环同构

$$R/\left(I_1 \cap \cdots \cap I_n\right) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_n.$$

证明: 首先证明

$$I_i + \prod_{j \neq i} I_j = R, 1 \leq i \leq n.$$

根据题设, $I_1 + I_2 = I_1 + I_3 = R$, 从而

$$\begin{aligned} R = RR = \left(I_1 + I_2\right)\left(I_1 + I_3\right) &= {I_1}^2 + I_2 I_1 + I_1 I_3 + I_2 I_3 \\ &\subseteq I_1 + I_2 I_3 \subseteq R, \end{aligned}$$

因此 $R = I_1 + I_2 I_3$. 再将 $R = I_1 + I_2 I_3$ 与 $R = I_1 + I_4$ 相乘可得 $R = I_1 + I_2 I_3 I_4$. 归纳下去即得 $R = I_1 + I_2 I_3 \cdots I_n$. 类似可得

$$I_i + \prod I_j = R, 1 \leq i \leq n.$$

证明 (续)

令

$$\phi : R \longrightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_n,$$
$$r \longmapsto (r + I_1, r + I_2, \cdots, r + I_n).$$

容易验证 ϕ 是 R 到 $R/I_1 \times R/I_2 \times \cdots \times R/I_n$ 上的环同态. 注意到 $R/I_1 \times R/I_2 \times \cdots \times R/I_n$ 的零元是 $(I_1, I_2, \cdots, I_n)$, 则显然有 $\operatorname{Ker}\phi = \{r \mid r \in I_1 \cap I_2 \cap \cdots \cap I_n\}$. 根据环同态基本定理, 要证明定理中的同构关系, 只需证明 ϕ 是满射即可, 即对任意 $r_1, r_2, \cdots, r_n \in R$ 及 $(r_1 + I_1, r_2 + I_2, \cdots, r_n + I_n)$, 存在 $r \in R$ 使得 $\phi(r) = (r_1 + I_1, r_2 + I_2, \cdots, r_n + I_n)$.

证明 (续)

取 $e \in R$, 则对任意 $1 \leq i \leq n$, 存在 $a_i \in I_i, b_i \in \prod_{j \neq i} I_j$ 使得 $a_i + b_i = e$. 从而有 $b_i = e - a_i \in e + I_i$, 并且对任意 $j \neq i$ 有 $b_i \in I_j$ (因为 $b_i \in \prod_{j \neq i} I_j$, 因此 $b_i \in \cap_{j \neq i} I_j$), 于是

$$\phi(b_i) = (I_1, \cdots, I_{i-1}, e + I_i, I_{i+1}, \cdots, I_n),$$

从而

$$\phi(r_i b_i) = (I_1, \cdots, I_{i-1}, r_i + I_i, I_{i+1}, \cdots, I_n).$$

令 $r = r_1 b_1 + r_2 b_2 + \cdots + r_n b_n$, 即知 $\phi(r) = (r_1 + I_1, r_2 + I_2, \cdots, r_n + I_n)$. 从而 ϕ 是满射.

未定元

定义 58

设 R 是一个含幺环, $\bar{R}$ 是 R 的扩环, x 是 $\bar{R}$ 中的一个元素. 如果 x 满足

(1) $\forall r \in R, xr = rx$;

(2) $1x = x$;

(3) 对 R 的任意一组不全为零的元素 $a_0, a_1, a_2, \cdots, a_n$,

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \neq 0,$$

则称 x 为 R 上的一个**未定元** (indeterminate).

未定元的存在性

定理 59

设 R 是一个含幺环, 则一定存在环 R 上的一个未定元 x.

证明: (1) 构造集合

$$\bar{S} = \{(a_0, a_1, \cdots, a_n, \cdots) \mid a_0, a_1, \cdots, a_n, \cdots \in R\}.$$

(2) 对 $\alpha = (a_0, a_1, \cdots, a_n, \cdots), \beta = (b_0, b_1, \cdots, b_n, \cdots) \in \bar{S}$, 规定

$$\alpha + \beta = (a_0 + b_0, a_1 + b_1, \cdots, a_n + b_n, \cdots),$$

$$\alpha \cdot \beta = (c_0, c_1, \cdots, c_n \cdots),$$

其中 $c_k = \sum_{i+j=k} a_i b_j \, (k = 0, 1, 2, \cdots, n, \cdots)$, 则如此定义的加法 "+" 和乘法 "$\cdot$" 显然都是 $\bar{S}$ 的代数运算.

证明 (续)

(3) 现证明 $\bar{S}$ 关于以上定义的加法 "$+$" 和乘法 "$\cdot$" 构成环.

由于 $\bar{S}$ 中的加法是对应分量相加, 而 R 关于加法构成加法群, 故 $(\bar{S}, +)$ 也是加法群, 其中 $(0, 0, \cdots, 0, \cdots)$ 是 $\bar{S}$ 的零元, 而 $\alpha = (a_0, a_1, \cdots, a_n, \cdots)$ 的负元是 $-\alpha = (-a_0, -a_1, \cdots, -a_n, \cdots)$.

设 $\alpha = (a_0, a_1, \cdots, a_n, \cdots)$, $\beta = (b_0, b_1, \cdots, b_n, \cdots)$, $\gamma = (d_0, d_1, \cdots, d_n, \cdots)$, $\alpha \cdot \beta = (c_0, c_1, \cdots, c_n, \cdots)$, $\beta \cdot \gamma = (e_0, e_1, \cdots, e_n, \cdots)$, 则 $(\alpha \cdot \beta) \cdot \gamma$ 中的第 t 个分量为

$$\sum_{k+s=t} c_k d_s = \sum_{k+s=t} \left(\sum_{i+j=k} a_i b_j \right) d_s = \sum_{i+j+s=t} a_i b_j d_s, \quad t = 0, 1, 2, \cdots,$$

而 $\alpha \cdot (\beta \cdot \gamma)$ 中的第 t 个分量为

$$\sum_{i+k=t} a_i e_k = \sum_{i+k=t} a_i \left(\sum_{j+s=k} b_j d_s \right) = \sum_{i+j+s=t} a_i b_j d_s, \quad t = 0, 1, 2, \cdots.$$

证明 (续)

于是它们对应的每个分量都相同, 故

$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma).$$

由于 $\alpha + \beta = (a_0 + b_0, a_1 + b_1, \cdots, a_n + b_n, \cdots)$, 因此 $(\alpha + \beta) \cdot \gamma$ 的第 k 个分量为

$$\sum_{i+j=k} (a_i + b_i)\, d_j = \sum_{i+j=k} a_i d_j + \sum_{i+j=k} b_i d_j, \quad k = 0, 1, 2, \cdots,$$

而上式右端恰为 $\alpha \cdot \gamma + \beta \cdot \gamma$ 中的第 k 个分量, 于是 $(\alpha + \beta) \cdot \gamma$ 与 $\alpha \cdot \gamma + \beta \cdot \gamma$ 中的每个对应分量都相同, 即 $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$. 同理可证另一分配律: $\gamma \cdot (\alpha + \beta) = \gamma \cdot \alpha + \gamma \cdot \beta$. 于是 $(\bar{S}, +, \cdot)$ 是一个环. 注意到对任意的 $\alpha = (a_0, a_1, \cdots, a_n, \cdots) \in \bar{S}$, 按定义的乘法有

$$\alpha \cdot (1, 0, 0, \cdots, 0, \cdots) = (1, 0, 0, \cdots, 0, \cdots) \cdot \alpha = \alpha,$$

因此 $(1, 0, 0, \cdots, 0, \cdots)$ 是 $\bar{S}$ 的单位元, 记为 $\bar{1}$, 即

$$\bar{1} = (1, 0, 0, \cdots, 0, \cdots).$$

于是 $(\bar{S}, +, \cdot)$ 是一个含幺环.

证明 (续)

(4) 令

$$S = \{\bar{r} = (r, 0, 0, \cdots, 0, \cdots) \mid r \in R\}.$$

以下证明 S 为 $\bar{S}$ 的子环, 且 S 有单位元 $\bar{1}$.

显然, 对于任意的 $\overline{r_1} = (r_1, 0, 0, \cdots, 0, \cdots), \overline{r_2} = (r_2, 0, 0, \cdots, 0, \cdots) \in S$, 有

$$\overline{r_1} - \overline{r_2} = (r_1 - r_2, 0, 0, \cdots, 0, \cdots) \in S,$$

$$\overline{r_1} \cdot \overline{r_2} = (r_1 r_2, 0, 0, \cdots, 0, \cdots) \in S.$$

于是 S 是 $\bar{S}$ 的子环, 显然 $\bar{1}$ 为 S 的单位元.

证明 (续)

(5) 注意到对任意 $\bar{r}=(r,0,0,\cdots,0,\cdots)\in S$,
$\alpha=(a_0,a_1,\cdots,a_n,\cdots)\in\bar{S}$, 有

$$\bar{r}\cdot\alpha=(ra_0,ra_1,\cdots,ra_n,\cdots),$$

$$\alpha\cdot\bar{r}=(a_0r,a_1r,\cdots,a_nr,\cdots),$$

于是, 若令 $\bar{x}=(0,1,0,\cdots,0,\cdots)$, 则

(i) 对任意的 $\bar{r}\in S$, 有

$$\bar{x}\cdot\bar{r}=\bar{r}\cdot\bar{x}=(0,r,0,\cdots,0,\cdots);$$

(ii) $\overline{1}\bar{x}=\bar{x}$;

(iii) 对任意的 $n\in\mathbb{N}$,

$$\bar{x}^n=(\underbrace{0,0,\cdots,0}_{n\text{个零}},1,0,0,\cdots).$$

于是, 对任意一组不全为零的元素 $\overline{a_i}\in S\,(i=0,1,2,\cdots,n)$, 有

$$\overline{a_0}+\overline{a_1}\bar{x}+\overline{a_2}\bar{x}^2+\cdots+\overline{a_n}\bar{x}^n=(a_0,a_1,\cdots,a_n,0,\cdots)\neq 0,$$

证明 (续)

(6) 令

$$\begin{aligned}\phi: \quad & R \longrightarrow \bar{S}, \\ & r \longmapsto \bar{r} = (r, 0, \cdots, 0, \cdots),\end{aligned}$$

则 ϕ 是环 R 到 $\bar{S}$ 的单同态, 且 $\phi(R) = S$.

(7) 因 $R \cap \bar{S} = \emptyset$, 从而由环的扩张定理知, 存在 R 的扩环 $\bar{R}$ 以及 $\bar{R}$ 到 $\bar{S}$ 的同构映射 $\bar{\phi}$, 使 $\bar{\phi}\big|_R = \phi$.

证明 (续)

(8) 令 x 为 $\bar{x}$ 在 $\bar{\phi}$ 下的原象, 即 $x \in \bar{R}$ 且 $\bar{\phi}(x) = \bar{x}$, 则

(i) 对任意的 $r \in R$, 由于

$$\bar{\phi}(rx) = \bar{\phi}(r)\bar{\phi}(x) = \phi(r)\bar{\phi}(x) = \bar{r}\bar{x} = \bar{x}\bar{r} = \bar{\phi}(x)\bar{\phi}(r) = \bar{\phi}(xr),$$

所以 $rx = xr$;

(ii) 因为

$$\bar{\phi}(1x) = \bar{\phi}(1)\bar{\phi}(x) = \phi(1)\bar{x} = \bar{1}\bar{x} = \bar{x},$$

所以 $1x = x$;

(iii) 对任意一组不全为零的元素 $a_i \in R\,(i = 0, 1, 2, \cdots, n)$, 因为

$$\begin{aligned}\bar{\phi}\left(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n\right) &= \bar{a}_0 + \bar{a}_1\bar{x} + \bar{a}_2\bar{x}^2 + \cdots + \bar{a}_n\bar{x}^n \\ &= (a_0, a_1, \cdots, a_n, 0, \cdots) \neq 0,\end{aligned}$$

所以

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \neq 0.$$

从而可知 x 为 R 上的一个未定元.

一元多项式

定义 60

设 R 是一个含幺环, x 是 R 上的一个未定元, $a_0, a_1, a_2, \cdots, a_n \in R$. 称形如

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

的表达式为 R 上 (关于 x 的) **一元多项式** (polynomial), 其中 $a_i x^i$ 称为多项式 $f(x)$ 的 i 次项 (term), a_i 称为 i 次项的**系数**, a_0 也称为**常数项** (constant term). 如果 $a_n \neq 0$, 则称 a_n 为**首项系数** (leading coefficient), 并称 $f(x)$ 的**次数**为 n, 记作 $\deg f(x) = n$. 系数全为零的多项式称为零多项式, 零多项式的次数规定为 $-\infty$, 并且规定
$(-\infty) + (-\infty) = -\infty, (-\infty) + n = (-\infty), (-\infty) < n$, 其中 $n \in \mathbb{Z}$.

一元多项式

注 60.1

由未定元存在性的讨论可知, R 上的一个多项式 $f(x)$ 是它的扩环 $\bar{R}$ 中的一个元素. 由此进一步可推出, R 上的多项式全体

$$R[x] = \left\{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \mid n \geq 0, a_0, a_1, a_2, \cdots, a_n \in R\right\}$$

关于 $\bar{R}$ 的运算 $\bar{\phi}$ 构成 R 的一个扩环. 特别地, R 上的一元多项式环 $R[x]$ 同构于以下 $\bar{S}$ 的子环

$$\{(a_0, a_1, \cdots, a_n, \cdots) \mid a_0, a_1, \cdots, a_n, \cdots \in R, \text{且仅有有限多个 } a_i \neq 0\}.$$

一元多项式环

定义 61

设 R 是一个含幺环, x 是 R 上的一个未定元. 称环 $R[x]$ 为 R 上的以 x 为未定元的**一元多项式环** (polynomial ring).

注 61.1

设 $f(x)=\sum_{i=0}^{n} a_i x^i, g(x)=\sum_{i=0}^{m} b_i x^i \in R[x], n \geq m$, 则 $f(x)$ 和 $g(x)$ 在 $R[x]$ 中的加法为

$$f(x)+g(x)=\sum_{i=0}^{n}\left(a_i+b_i\right)x^i,$$

其中当 $m<i\leq n$ 时 $b_i=0$; $f(x)$ 和 $g(x)$ 在 $R[x]$ 中的乘法为

$$f(x)g(x)=\sum_{i=0}^{m+n} c_i x^i,$$

其中 $c_k=\sum_{0\leq i\leq n, 0\leq j\leq m, i+j=k} a_i b_j, k=0,1,\cdots,m+n.$

商域的构造思想

- 在整数环中, 可逆元仅有 ± 1, 这使得像 $2x = 1$ 这样的方程在整数环中就没有解.
- 方程有解, 则需要由整数环出发, 去构造一个更大的代数体系–有理数域.
- 有理数域是由所有形如 $\frac{a}{b}\,(a, b \in \mathbb{Z}, b \neq 0)$ 的分数所组成的, 并且它还以整数环作为它的子环.
- 对一般的环, 是否也可以把它扩充为一个更大的环, 使其上每个非零元都可逆?
- 有零因子的环以及非交换环都无法达到目的.
- 设 D 是整环, 1 是 D 的单位元, 则由 D 可以构造一个包含 D 的域.
- 商域的主要构造思想是给定一种集合并定义运算得到域, 最后利用环的扩张定理.

商域的构造

1. 构作集合 S

令

$$S = \{(a, b) \mid a, b \in D, b \neq 0\}.$$

2. 在 S 上定义一个等价关系

对任意 $(a, b), (c, d) \in S$,令

$$(a, b) \sim (c, d) \Longleftrightarrow ad = bc.$$

(1) 由 $ab = ba$, 得 $(a, b) \sim (a, b)$, 所以“$\sim$”具有反身性;

(2) 如果 $(a, b) \sim (c, d)$, 则 $ad = bc$, 从而 $cb = da$, 于是 $(c, d) \sim (a, b)$, 所以“$\sim$”具有对称性;

(3) 设 $(a, b) \sim (c, d), (c, d) \sim (e, f)$, 则 $ad = bc, cf = de$, 所以 $adcf = bcde$. 如果 $c = 0$, 则因 $d \neq 0$, 所以 $a = e = 0$, 于是 $af = be$, 从而 $(a, b) \sim (e, f)$. 如果 $c \neq 0$, 则因 $d \neq 0$, 所以 $cd \neq 0$. 因 D 为整环, 消去 cd 得 $af = be$, 从而 $(a, b) \sim (e, f)$, 所以“$\sim$”具有传递性. 因此“$\sim$”是 S 的一个等价关系.

商域的构造 (续)

3. 由等价关系得到商集 F

对任意的 $(a,b) \in S$, 记 S 中 (a,b) 所在的等价类为

$$\left[\frac{a}{b}\right] = \{(c,d) \in S \mid (c,d) \sim (a,b)\}.$$

令

$$F = S/\sim = \left\{ \left[\frac{a}{b}\right] \mid a,b \in D, b \neq 0 \right\},$$

则

$$\left[\frac{a}{b}\right] = \left[\frac{c}{d}\right] \Longleftrightarrow ad = bc.$$

商域的构造 (续)

4. 定义 F 的运算, 使 F 构成一个域

(1) 对任意的 $\left[\frac{a}{b}\right], \left[\frac{c}{d}\right] \in F$, 规定

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad+bc}{bd}\right],$$

$$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right].$$

如果 $\left[\frac{a'}{b'}\right] = \left[\frac{a}{b}\right], \left[\frac{c'}{d'}\right] = \left[\frac{c}{d}\right]$, 则有 $a'b = ab', c'd = cd'$, 从而

$$\begin{aligned}(ad+bc)b'd' &= adb'd' + bcb'd' = a'bdd' + bb'c'd \\ &= (a'd' + b'c')\, bd,\end{aligned}$$

$$acb'd' = a'bcd' = a'bc'd = bda'c'.$$

商域的构造 (续)

由此得

$$\left[\frac{ad+bc}{bd}\right]=\left[\frac{a'd'+b'c'}{b'd'}\right],$$

$$\left[\frac{ac}{bd}\right]=\left[\frac{a'c'}{b'd'}\right],$$

所以“$+$”与“$\cdot$”都是 F 的代数运算.

(2) 对任意的 $\left[\frac{a}{b}\right],\left[\frac{c}{d}\right],\left[\frac{e}{f}\right]\in F$,

$$\left(\left[\frac{a}{b}\right]+\left[\frac{c}{d}\right]\right)+\left[\frac{e}{f}\right]=\left[\frac{ad+bc}{bd}\right]+\left[\frac{e}{f}\right]=\left[\frac{adf+bcf+bde}{bdf}\right]$$

$$=\left[\frac{a}{b}\right]+\left[\frac{de+cf}{df}\right]=\left[\frac{a}{b}\right]+\left(\left[\frac{c}{d}\right]+\left[\frac{e}{f}\right]\right),$$

商域的构造 (续)

$$\left(\left[\frac{a}{b}\right]\cdot\left[\frac{c}{d}\right]\right)\cdot\left[\frac{e}{f}\right]=\left[\frac{ac}{bd}\right]\cdot\left[\frac{e}{f}\right]=\left[\frac{ace}{bdf}\right]$$
$$=\left[\frac{a}{b}\right]\cdot\left[\frac{ce}{df}\right]=\left[\frac{a}{b}\right]\cdot\left(\left[\frac{c}{d}\right]\cdot\left[\frac{e}{f}\right]\right),$$

所以加法与乘法满足结合律.

(4) 对任意的 $\left[\frac{a}{b}\right],\left[\frac{c}{d}\right],\left[\frac{e}{f}\right]\in F$,

$$\left(\left[\frac{a}{b}\right]+\left[\frac{c}{d}\right]\right)\cdot\left[\frac{e}{f}\right]=\left[\frac{ad+bc}{bd}\right]\cdot\left[\frac{e}{f}\right]=\left[\frac{ade+bce}{bdf}\right]$$
$$=\left[\frac{ade}{bdf}\right]+\left[\frac{bce}{bdf}\right]=\left[\frac{ae}{bf}\right]+\left[\frac{ce}{df}\right]$$
$$=\left[\frac{a}{b}\right]\cdot\left[\frac{e}{f}\right]+\left[\frac{c}{d}\right]\cdot\left[\frac{e}{f}\right],$$

所以乘法对加法也满足分配律.

商域的构造 (续)

(5) 对任意的 $\left[\frac{a}{b}\right] \in F$,

$$\left[\frac{0}{1}\right] + \left[\frac{a}{b}\right] = \left[\frac{0 \cdot b + 1 \cdot a}{1 \cdot b}\right] = \left[\frac{a}{b}\right],$$

所以 $\left[\frac{0}{1}\right] = 0_F$ 为 F 的零元.

(6) 对任意的 $\left[\frac{a}{b}\right] \in F$,

$$\left[\frac{1}{1}\right] \cdot \left[\frac{a}{b}\right] = \left[\frac{1 \cdot a}{1 \cdot b}\right] = \left[\frac{a}{b}\right],$$

所以 $\left[\frac{1}{1}\right] = 1_F$ 为 F 的单位元. 显然 $0_F \neq 1_F$.

商域的构造 (续)

(7) 对任意的 $\left[\frac{a}{b}\right] \in F$, 有 $\left[\frac{-a}{b}\right] \in F$ 且

$$\left[\frac{a}{b}\right] + \left[\frac{-a}{b}\right] = \left[\frac{ab - ba}{b^2}\right] = \left[\frac{0}{1}\right] = 0_F,$$

所以 F 的每个元都有负元.

(8) 对任意的 $\left[\frac{a}{b}\right] \neq 0_F$, 有 $a \neq 0$, 所以 $\left[\frac{b}{a}\right] \in F$. 而

$$\left[\frac{a}{b}\right] \cdot \left[\frac{b}{a}\right] = \left[\frac{ab}{ab}\right] = \left[\frac{1}{1}\right] = 1_F,$$

所以 F 的每个非零元都可逆.

这就证明了 F 是一个域.

商域的构造 (续)

5. 由 F 构作一个包含 D 的域

令

$$\begin{aligned} \phi: \quad & D \longrightarrow F \\ & x \longmapsto \left[\frac{x}{1}\right], \end{aligned}$$

则 ϕ 为 D 到 F 的映射.

(1) 对任意的 $x, y \in D$, 如果 $\left[\frac{x}{1}\right] = \left[\frac{y}{1}\right]$, 则 $x \cdot 1 = y \cdot 1$, 即 $x = y$, 所以 ϕ 为 D 到 F 的单映射.

商域的构造 (续)

(2) 对任意的 $x, y \in D$,

$$\phi(x+y) = \left[\frac{x+y}{1}\right] = \left[\frac{x}{1}\right] + \left[\frac{y}{1}\right] = \phi(x) + \phi(y),$$

$$\phi(x \cdot y) = \left[\frac{xy}{1}\right] = \left[\frac{x}{1}\right] \cdot \left[\frac{y}{1}\right] = \phi(x) \cdot \phi(y),$$

所以 ϕ 为 D 到 F 的同态映射.

(3) $D \cap F = \emptyset$, 从而由环的扩张定理知, 存在 D 的扩环 Q 及环同构

$$\tilde{\phi} : Q \cong F.$$

因为 F 是域, 所以 Q 也是域.

商域的构造方法

定理

每一个整环都可以扩充为一个域.

注: Q 的元素的表达式

因为域 Q 包含 D, 所以也一定包含 D 的每个非零元的逆元, 从而也一定包含这些元素的乘积, 因此 Q 一定包含全体形如

$$ab^{-1}, \quad a, b \in D, b \neq 0$$

的元素.

又对任意的 $\left[\frac{a}{b}\right] \in F$, 由环的扩张定理的证明及 ϕ 的定义, 有

商域的构造方法

$$
\begin{aligned}
\widetilde{\phi}^{-1}\left(\left[\frac{a}{b}\right]\right) &= \widetilde{\phi}^{-1}\left(\left[\frac{a}{1}\right]\cdot\left[\frac{1}{b}\right]\right) \\
&= \widetilde{\phi}^{-1}\left(\left[\frac{a}{1}\right]\right)\cdot\widetilde{\phi}^{-1}\left(\left[\frac{1}{b}\right]\right) \\
&= \widetilde{\phi}^{-1}\left(\left[\frac{a}{1}\right]\right)\cdot\widetilde{\phi}^{-1}\left(\left(\left[\frac{b}{1}\right]\right)^{-1}\right) \\
&= a\left(\widetilde{\phi}^{-1}\left(\left[\frac{b}{1}\right]\right)\right)^{-1} \\
&= ab^{-1}.
\end{aligned}
$$

商域的构造方法

这说明 Q 的每个元素都可表为

$$ab^{-1}, \quad a, b \in D, b \neq 0$$

的形式, 所以

$$Q = \left\{ ab^{-1} \mid a, b \in D, b \neq 0 \right\}.$$

因为 Q 是域, 故可记 $\frac{a}{b} = ab^{-1}$. 这样

$$Q = \left\{ \frac{a}{b} \mid a, b \in D, b \neq 0 \right\},$$

即 Q 由所有的商 $\frac{a}{b}\,(a, b \in D, b \neq 0)$ 所组成. 这同有理数域的构成是类似的.

商域的定义

定义

称域 Q 为整环 D 的商域 (quotient field).

例

整数环 $\mathbb{Z}$ 的商域就是有理数域 $\mathbb{Q}$.

例

域 F 的商域就是其本身.

商域的性质

定理

设 D 与 D' 是同构的两个整环, 则它们的商域也同构.

证明: 设 Q, Q' 分别是 D 与 D' 的商域, $\phi : D \to D'$ 是环同构. 记 $\phi(a) = a'$, $\forall a \in D$, 则由以上讨论知

$$Q = \left\{ \frac{a}{b} \mid a, b \in D, b \neq 0 \right\}, \quad Q' = \left\{ \frac{e}{f} \mid e, f \in D', f \neq 0 \right\}.$$

定义 $\tilde{\phi} : Q \to Q', \frac{a}{b} \mapsto \frac{a'}{b'}$.

若 $\frac{a}{b} = \frac{c}{d}$, 则 $ab^{-1} = cd^{-1}$, 从而 $ad = bc$, 于是 $\phi(ad) = \phi(bc)$, 即 $a'd' = b'c'$, 所以 $\frac{a'}{b'} = \frac{c'}{d'}$. 故 $\tilde{\phi}$ 是映射.

证明 (续)

对任意 $\frac{a}{b}, \frac{c}{d} \in Q$, 有

$$\begin{aligned}
\widetilde{\phi}\left(\frac{a}{b}+\frac{c}{d}\right) &= \phi\left(\frac{ad+bc}{bc}\right) = \frac{(ad+bc)'}{(bd)'} \\
&= \frac{a'd'+b'c'}{b'd'} = \frac{a'}{b'}+\frac{c'}{d'} \\
&= \tilde{\phi}\left(\frac{a}{b}\right)+\tilde{\phi}\left(\frac{c}{d}\right), \\
\widetilde{\phi}\left(\frac{a}{b}\cdot\frac{c}{d}\right) &= \widetilde{\phi}\left(\frac{ac}{bc}\right) = \frac{(ac)'}{(bd)'} \\
&= \frac{a'c'}{b'd'} = \frac{a'}{b'}\cdot\frac{c'}{d'} \\
&= \widetilde{\phi}\left(\frac{a}{b}\right)\tilde{\phi}\left(\frac{c}{d}\right),
\end{aligned}$$

证明 (续)

于是 $\tilde{\phi}$ 是环同态. 而 $\tilde{\phi}(1)=\tilde{\phi}\left(\frac{1}{1}\right)=\frac{1'}{1'}=1'$, 故 $\widetilde{\phi}\neq 0$. 于是 $\operatorname{Ker}\tilde{\phi}\neq Q$. 而 $\operatorname{Ker}\tilde{\phi}$ 是 Q 是理想, 又 Q 是域, 所以 $\operatorname{Ker}\tilde{\phi}=0$, 即 $\tilde{\phi}$ 是单射. 又由于 Q' 中的元素都具有形式 $\frac{e}{f}$ (其中 $f\neq 0, e, f\in D'$). 由 ϕ 是 D 到 D' 的满射知, 存在 $a, b\in D$, 使得 $e=a', f=b'$, 故

$$\frac{e}{f}=\frac{a'}{b'}=\widetilde{\phi}\left(\frac{a}{b}\right).$$

所以 $\tilde{\phi}$ 是满射, 即 $\tilde{\phi}$ 是域同构, 从而 Q 与 Q' 同构.

§3.5 素理想与极大理想

- 素理想
- 素理想与整环
- 极大理想
- 极大理想与域
- 极大理想与素理想

素理想

定义 62

设 R 是一个交换环, P 是 R 的真理想. 如果对任意的 $a, b \in R$, 由 $ab \in P$, 可推出 $a \in P$ 或 $b \in P$, 则称 P 为 R 的一个**素理想** (prime ideal).

例 63

试求 $\mathbb{Z}_{18}$ 的素理想.

解: $\mathbb{Z}_{18}$ 一共有 6 个理想 (以下我们将 $\mathbb{Z}_m$ 中的元素 $\bar{a}$ 简记为 a):

$\{0\}, \mathbb{Z}_{18}, \langle 2\rangle, \langle 3\rangle, \langle 6\rangle, \langle 9\rangle$.

解 (续)

(1) 显然, $\mathbb{Z}_{18}$ 不是 $\mathbb{Z}_{18}$ 的素理想. 又因为 $2 \cdot 3 = 6 \in \langle 6 \rangle$, 而 $2, 3 \notin \langle 6 \rangle$, 所以 $\langle 6 \rangle$ 也不是 $\mathbb{Z}_{18}$ 的素理想. 同理可证, $\{0\}$ 与 $\langle 9 \rangle$ 都不是 $\mathbb{Z}_{18}$ 的素理想.

(2) 考察 $\langle 3 \rangle$. 设 $a, b \in \mathbb{Z}_{18}, ab \in \langle 3 \rangle$, 则 $ab = r \cdot 3$ (在 $\mathbb{Z}_{18}$ 中), 即 $ab \equiv 3r \pmod{18}$, 所以 $18 \mid ab - 3r$ (在 $\mathbb{Z}$ 中), 从而存在 $l \in \mathbb{Z}$ 使

$$ab - 3r = 18l.$$

因 $3 \mid 18$, 所以 $3 \mid ab$, 从而 $3 \mid a$ 或 $3 \mid b$. 由此得 $a \in \langle 3 \rangle$ 或 $b \in \langle 3 \rangle$, 所以 $\langle 3 \rangle$ 为 $\mathbb{Z}_{18}$ 的素理想.

同理可证, $\langle 2 \rangle$ 也是 $\mathbb{Z}_{18}$ 的素理想, 所以 $\mathbb{Z}_{18}$ 的素理想为 $\langle 2 \rangle$ 与 $\langle 3 \rangle$.

例

例 64

设 n 为正整数, 则 $\langle n \rangle$ 为 $\mathbb{Z}$ 的素理想的充分必要条件是 n 为素数.

例 65

在 $\mathbb{Z}_2[x]$ 中, 由于 $x+1 \notin \langle x^2+1 \rangle$, 而 $(x+1)^2 = x^2+1 \in \langle x^2+1 \rangle$, 所以 $\langle x^2+1 \rangle$ 不是 $\mathbb{Z}_2[x]$ 的素理想.

定理 66

设 R 是有单位元 $e \neq 0$ 的交换环, I 是 R 的理想, 则 I 是 R 的素理想的充分必要条件是 R/I 是整环.

证明: 必要性. 设 I 为 R 的素理想, 则 I 为 R 的真理想, 所以 $R/I \neq \{\overline{0}\}$. 因 R 是有单位元的交换环, 所以 R/I 也是有单位元的交换环. 又设 $\bar{a}, \bar{b} \in R/I$ 使 $\bar{a} \cdot \bar{b} = \overline{0}$, 则 $ab \in I$, 从而有 $a \in I$ 或 $b \in I$. 由此得 $\bar{a} = \overline{0}$ 或 $\bar{b} = \overline{0}$. 这说明, 商环 R/I 无零因子, 所以 R/I 为整环.

充分性. 如果 R/I 为整环, 则 R/I 是 $\overline{e} \neq \overline{0}$ 的交换环, 于是 I 是 R 的真理想 (否则有 $I = R$, 于是 $R/I = \{\overline{0} = \overline{e}\}$). 又设 $a, b \in R$ 且 $ab \in I$, 则 $\bar{a} \cdot \bar{b} = \overline{ab} = I = \overline{0} \in R/I$, 所以必有 $\bar{a} = \overline{0}$ 或 $\bar{b} = \overline{0}$. 由此得 $a \in I$ 或 $b \in I$. 所以 I 为 R 的素理想.

极大理想

定义 67

设 R 是一个交换环, M 是 R 的真理想. 如果对 R 的任一包含 M 的理想 N, 必有 $N = M$ 或 $N = R$, 则称 M 为 R 的一个**极大理想** (maximal ideal).

注 67.1

(1) 设 I 是 R 的一个理想. 若 I 不是 R 的极大理想, 则一定存在 R 的一个理想 J 满足 $I \subsetneq J \subsetneq R$.

(2) 若 I 是 R 的一个理想, 要证明 I 是 R 的极大理想, 只须证明对 R 中满足 $I \subsetneq J \subseteq R$ 的任意理想 J 必有 $J = R$.

(3) 设 R 是一个有单位元 e 的交换环, I 是其一个极大理想. 任取 $a \in R \setminus I$, 则 $\langle a \rangle$ 是 R 的一个主理想, 从而 $\langle a \rangle + I$ 是 R 的一个真包含 I 的理想, 于是 $R = \langle a \rangle + I$.

例

例 68

$\mathbb{Z}_{18}$ 的极大理想是 $\langle 2\rangle$ 与 $\langle 3\rangle$.

例 69

设 p 是正整数. 则 $\langle p\rangle$ 是 $\mathbb{Z}$ 的极大理想当且仅当 p 是素数.

例 70

设 $R = 2\mathbb{Z}, I = 4\mathbb{Z}$ 为 R 的理想, 则 I 为 R 的极大理想, 但不是素理想.

例 71

设 R 是全体实函数的集合按通常函数的加法与乘法构成的一个环. 令

$$I = \{f(x) \in R \mid f(0) = 0\}.$$

则 I 为 R 的极大理想.

例

例 72

证明 $\left\langle x^2+1\right\rangle$ 为 $\mathbb{Z}_3[x]$ 的极大理想.

证明: 设 I 为 $\mathbb{Z}_3[x]$ 的任一理想使 $\left\langle x^2+1\right\rangle \subsetneq I$. 在 I 中任取一个不属于 $\left\langle x^2+1\right\rangle$ 的多项式 $f(x)$. 存在 $q(x), ax+b \in \mathbb{Z}_3[x]$, 使

$$f(x) = \left(x^2+1\right) q(x) + ax + b.$$

从而

$$ax + b = f(x) - \left(x^2+1\right) q(x) \in I.$$

因 $f(x) \notin \left\langle x^2+1\right\rangle$, 从而 $ax+b \notin \left\langle x^2+1\right\rangle$, 所以 a, b 不全为零.

证明 (续)

(1) 在 $\mathbb{Z}_3[x]$ 中, 如果 $a \neq 0$, 则 $a^2 + b^2 \neq 0$, 且

$$a^2 + b^2 = a^2\left(x^2 + 1\right) - (ax + b)(ax - b) \in I,$$

则

$$1 = \left(a^2 + b^2\right)^{-1}\left(a^2 + b^2\right) \in I,$$

其中 $(a^2 + b^2)^{-1}$ 是 $a^2 + b^2$ 在 $\mathbb{Z}_3$ 中的逆. 由此得 $I = \mathbb{Z}_3[x]$.

(2) 如果 $a = 0$, 则 $b \neq 0$ 且 $b \in I$, 于是 $1 = b^{-1}b \in I$, 从而 $I = \mathbb{Z}_3[x]$.

这就证明了 $\left\langle x^2 + 1 \right\rangle$ 是 $\mathbb{Z}_3[x]$ 的极大理想.

定理 73

设 R 是有单位元 e 的交换环, I 为 R 的理想, 则 I 是 R 的极大理想的充分必要条件是 R/I 是域.

证明: 必要性. 设 I 为 R 的极大理想, 则 $R/I \neq \{\overline{0}\}$. 因 R 是有单位元的交换环, 所以 R/I 也是有单位元的交换环. 又对任意的 $\bar{a} \in R/I$, 如果 $\bar{a} \neq \overline{0}$, 即 $a \notin I$, 则 $I \subsetneq \langle a \rangle + I \triangleleft R$, 所以 $\langle a \rangle + I = R$. 从而 $e \in \langle a \rangle + I$. 于是存在 $r \in R, b \in I$, 使 $e = ar + b$. 从而 $\bar{e} = \overline{ar + b} = \overline{ar} = \bar{a} \cdot \bar{r}$, 即 $\bar{a}$ 可逆, 所以 R/I 为域.

充分性. 设 R/I 为域, 则 $R/I \neq \{\overline{0}\}$ (域定义要求 $e \neq 0$), 所以 I 为 R 的真理想. 设 J 为 R 的任一真包含 I 的理想, 则有 $a \in J$ 且 $a \notin I$, 从而 $\bar{a} \neq \overline{0}$. 因 R/I 为域, 存在 $\bar{b} \in R/I$, 使 $\bar{a} \cdot \bar{b} = \bar{e}$. 于是 $e \in ab + I \subseteq J$, 从而 $J = R$. 所以 I 为 R 的极大理想.

极大理想与素理想

定理 74

设 R 是一个有单位元的交换环, 则 R 的每个极大理想都是素理想.

证明: 如果 I 是 R 的极大理想, 由定理 73, R/I 是域. 从而 R/I 是整环. 又由定理 66 知, I 是素理想.

例

例 75

例 72 中, $\langle x^2+1\rangle$ 是 $\mathbb{Z}_3[x]$ 的极大理想, 所以 $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ 是一个域. 如果记 $\theta=\bar{x}$, 则 $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ 可记为 $\mathbb{Z}_3[\theta]$, 易知

$$\mathbb{Z}_3[\theta]=\{0,1,-1,\theta,-\theta,1+\theta,-1+\theta,1-\theta,-1-\theta\},$$

并且其元素的运算满足

$$1+1=-1,$$
$$\theta^2=-1.$$

§3.6 环的特征与素域

- 环的特征
- 含幺环的特征
- 整环的特征
- 域的特征
- 素域
- 特征的性质

环的特征

定义 76

设 R 为环. 如果存在最小的正整数 n, 使得对所有的 $a \in R$, 有 $na = 0$, 则称 n 为环 R 的特征 (characteristic). 如果这样的正整数不存在, 则称环 R 的特征为 0. 环 R 的特征记作 $\operatorname{Char} R$.

例 77

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 的特征都等于 0. 一般地, 如果 R 是一个数环, 则 $\operatorname{Char} R = 0$.

例 78

设 $\mathbb{Z}_m$ 是模 m 剩余类环, 则对每个 $\bar{a} \in \mathbb{Z}_m$, 有

$$m\bar{a} = \overline{ma} = \overline{0}.$$

而对于任何正整数 $k < m$, 有

$$k\overline{1} = \bar{k} \neq \overline{0},$$

所以 $\operatorname{Char} \mathbb{Z}_m = m$.

含幺环的特征

定理 79

设 R 是有单位元 e 的环. 如果 e 关于加法的阶为无穷大, 那么 R 的特征等于 0. 如果 e 关于加法的阶等于 n, 那么 $\operatorname{Char} R = n$.

证明: 如果 e 关于加法的阶为无穷大, 那么不存在正整数 n, 使得 $ne = 0$. 所以由特征的定义知 $\operatorname{Char} R = 0$.

如果 e 关于加法的阶等于正整数 n, 则 $ne = 0$. 而且 n 是满足这一性质的最小正整数. 因此, 对于任意的 $a \in R$ 有

$$na = n(e \cdot a) = (ne) \cdot a = 0 \cdot a = 0.$$

于是, $\operatorname{Char} R = n$.

整环的特征

定理 80

整环的特征是 0 或者是一个素数.

证明: 由定理 79, 只要证明, 如果整环 R 的单位元 e 关于加法的阶有限, 则它必为素数.

设 e 关于加法的阶为 n. 显然 $n > 1$ (整环中 $e \neq 0$). 假设 $n = st, 1 \leqslant s, t \leqslant n$, 则可得

$$0 = ne = (st)e = s(te) = s(e \cdot te) = (se) \cdot (te).$$

故由整环 R 无零因子得 $se = 0$ 或 $te = 0$. 因为 n 是使得 $ne = 0$ 成立的最小正整数, 所以 $s = n$ 或 $t = n$. 因此 n 是素数.

域的特征

定义 81

设 F 是一个域, 将域 F 的特征 $\mathrm{Char}\, F$ 就定义为将域看作环时的特征.

定义 82

一个域 F 如果不含任何真子域, 则称 F 是一个素域 (prime field).

注 82.1

由于域是一类特殊的整环, 所以域的特征也只能是 *0* 或素数.

定理 83

在特征是素数 p 的交换环 R 中有

$$(a+b)^p = a^p + b^p, \quad a, b \in R.$$

证明: 在交换环中显然有

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + b^p.$$

由

$$\binom{p}{j} = \frac{p(p-1)\cdots(p-j+1)}{j!} \ (j = 1, 2, \cdots, p-1)$$

可得

$$\binom{p}{j} j! = p(p-1)\cdots(p-j+1).$$

显然 $p \nmid j!$, 因此 $p \mid \binom{p}{j}$, 所以 $\binom{p}{j}a^{p-j}b^j = 0 \, (j = 1, \cdots, p-1)$, 定理成立.

特征的性质

推论 84

在特征是素数 p 的交换环 R 中对任意正整数 k 有

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}, \quad a, b \in R.$$

§3.7 多项式环

- 未定元及其存在性
- 一元多项式 (环)
- 整除与最大公因式
- 多项式环的性质
- 域上的多项式环
- 多项式的根

§3.6 环的特征与素域

- 环的特征
- 含幺环的特征
- 整环的特征
- 域的特征
- 素域
- 特征的性质

整除

定义 85

设 R 是一个含幺环, x 是 R 上的一个未定元. 设 $f(x)$ 和 $g(x)$ 是 $R[x]$ 中的任意两个多项式, $g(x) \neq 0$. 如果存在一个多项式 $q(x) \in R[x]$ 使得

$$f(x) = q(x)g(x),$$

成立, 那么就称 $g(x)$ **整除** $f(x)$ 或者 $f(x)$ **可以被** $g(x)$ 整除, 记做 $g(x) \mid f(x)$. 这时我们把 $g(x)$ 叫做 $f(x)$ 的**因式**, 而把 $f(x)$ 叫做 $g(x)$ 的**倍式**. 显然, 对任意 $a \in U(R)$, a 和 $af(x)$ 都是 $f(x)$ 的因式, 称之为**平凡因式**, 否则称为**非平凡因式**. 如果一个次数大于零的多项式不能写成两个非平凡因式的乘积, 那么我们就称这个多项式是**不可约多项式**或**既约多项式**, 否则称为**可约多项式**.

注 85.1

设 R 是一个含幺环, x 是 R 上的一个未定元, $f(x) \in R[x]$ 是一个次数大于零的多项式, 则 $f(x)$ 为可约多项式当且仅当存在两个次数大于零的多项式 $g(x), h(x) \in R[x]$ 使得 $f(x) = g(x)h(x)$.

最大公因式

定义 86

设 R 是一个含幺环, x 是 R 上的一个未定元. 对任意 $f(x), g(x), h(x) \in R[x]$, 其中 $h(x)$ 是非零的首一多项式, 如果

(1) $h(x) \mid f(x), h(x) \mid g(x)$;

(2) 对任一多项式 $0 \neq d(x) \in R[x]$, 若有 $d(x) \mid f(x)$, $d(x) \mid g(x)$, 则 $d(x) \mid h(x)$,

则称 $h(x)$ 为 $f(x)$ 与 $g(x)$ 的**最大公因式**, 记为 $h(x) = \gcd(f(x), g(x))$.
特别地, 若 $\gcd(f(x), g(x)) = 1$, 则称 $f(x)$ 与 $g(x)$ 是**互素**的.

多项式环的性质

定理 87

设 R 是一个含幺环, x 是 R 上的一个未定元.

(1) R 的零元 *0* 就是 $R[x]$ 的零元 *(*即零多项式*)*;
(2) $R[x]$ 是含幺环, 且 R 的单位元就是 $R[x]$ 的单位元;
(3) 如果 R 是无零因子环, 则 $R[x]$ 也是无零因子环, 且 $R[x]$ 的单位就是 R 的单位;
(4) 如果 R 是交换环, 则 $R[x]$ 也是交换环;
(5) 如果 R 是整环, 则 $R[x]$ 也是整环.

证明

(1) 对任意的 $f(x) \in R[x]$, 有 $0 + f(x) = f(x) + 0 = f(x)$. 所以 R 的零元就是 $R[x]$ 的零元.

(2) 对任意的 $f(x) \in R[x]$, 由于 $1 \cdot f(x) = f(x) = f(x) \cdot 1$, 所以 1 是 $R[x]$ 的单位元.

(3) 设 R 是无零因子环, $f(x) = \sum_{i=0}^{n} a_i x^i$ 与 $g(x) = \sum_{j=0}^{m} b_j x^j$ 是 $R[x]$ 中的任意两个非零元, 其中 $a_n, b_m \neq 0$, 则 $f(x)g(x)$ 的最高次项系数为 $a_n b_m$. 由于 R 是无零因子环, 因此 $a_n b_m \neq 0$, 于是 $f(x)g(x) \neq 0$, 所以 $R[x]$ 无零因子环. 又如果 $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ 是 $R[x]$ 的任意一个单位, 其中 $a_n \neq 0$, 则存在 $g(x) = \sum_{j=0}^{m} b_j x^j \in R[x]$, 其中 $b_m \neq 0$, 使得

$$f(x) \cdot g(x) = g(x) \cdot f(x) = 1.$$

证明 (续)

由于 $1 = f(x) \cdot g(x) = \sum_{k=0}^{n+m} c_k x^k$, 其中 $c_k = \sum_{i+j=k} a_i b_j$, $k = 0, 1, \cdots, n+m$, 故 x^{n+m} 的系数 $c_{n+m} = a_n b_m$, 于是得 $n = m = 0$, 且 $a_0 b_0 = 1$. 同理, 由 $g(x) \cdot f(x) = 1$ 得 $b_0 a_0 = 1$, 故 $f(x) = a_0 \in R$, 且 a_0 是 R 中的单位.

(4) 若 R 是交换环. 设 $f(x) = \sum_{i=0}^{n} a_i x^i, g(x) = \sum_{j=0}^{m} b_j x^j \in R[x]$, 有

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k, \quad g(x)f(x) = \sum_{k=0}^{n+m} d_k x^k,$$

则 $c_k = \sum_{i+j=k} a_i b_j = \sum_{i+j=k} b_j a_i = d_k, k = 0, 1, \cdots, n+m$. 于是 $f(x)g(x) = g(x)f(x)$. 所以 $R[x]$ 也是交换环.

(5) 若 R 是整环, 则 R 是有单位元的无零因子交换环, 故由 (2), (3), (4) 得 $R[x]$ 也是有单位元的无零因子交换环, 也就是整环.

多项式环的性质

引理 88

设 R 是一个含幺环, 则对任意 $f(x), g(x) \in R[x]$ 有

(1) $\deg(f+g) \leq \max(\deg f, \deg g)$;

(2) $\deg fg \leq \deg f + \deg g$;

(3) 如果 f 或者 g 的首项系数不是 R 中零因子, 则 $\deg fg = \deg f + \deg g$.

多项式环的性质

定理 89 (带余除法)

设 R 是一个含幺交换环, $R[x]$ 是 R 上的一元多项式环. 对任意 $f(x), g(x) \in R[x]$, 并且 $g(x)$ 的首项系数是 R 中单位, 则存在唯一一对多项式 $q(x), r(x) \in R[x]$ 使得 $f(x) = q(x)g(x) + r(x)$, 并且 $\deg r(x) < \deg g(x)$.

证明: 首先证明存在性. 令

$$\Sigma = \{f(x) - g(x)h(x) \mid h(x) \in R[x]\}.$$

因为 $g(x)$ 的首项系数是 R 中单位, 因此 $g(x) \neq 0$, 所以 $\Sigma \neq \{0\}$.

如果 $0 \in \Sigma$, 则有 $h(x) \in R[x]$, 使 $0 = f(x) - g(x)h(x)$, 取 $r(x) = 0, q(x) = h(x)$, 则有 $f(x) = g(x)q(x)$, 并且 $\deg r(x) = -\infty < \deg g(x)$.

证明 (续)

如果 $0 \notin \Sigma$, 则 $\deg g(x) \geq 1$ (否则若 $\deg g(x) = 0$, 则 g 为 R 中单位, 于是有 $f(x) - g(x)g^{-1}(x)f(x) = 0 \in \Sigma$). 取 $r(x) \in \Sigma$ 为 Σ 中次数最小的多项式, 则有 $q(x) \in R[x]$, 使 $r(x) = f(x) - g(x)q(x)$. 所以 $f(x) = g(x)q(x) + r(x)$. 下面用反证法证明 $\deg r(x) < \deg g(x)$. 假设 $\deg r(x) \geq \deg g(x)$. 设

$$g(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad a_n \neq 0, n \geq 1,$$

$$r(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m, \quad b_m \neq 0.$$

因为 $\deg r(x) \geq \deg g(x)$, 所以 $m \geq n$. 令

$$q_1(x) = q(x) + b_m a_n^{-1} x^{m-n}, \quad r_1(x) = r(x) - b_m a_n^{-1} g(x) x^{m-n},$$

则 $f(x) = g(x)q_1(x) + r_1(x)$, 于是 $r_1(x) \in \Sigma$. 因为 $0 \notin \Sigma$, 所以 $r_1(x) \neq 0$, 从而 $\deg r_1(x) < \deg r(x)$. 这与 $r(x)$ 的选取矛盾. 由此知 $\deg r(x) < \deg g(x)$.

证明 (续)

现证明唯一性. 设有

$$f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x),$$

其中 $\deg r_1(x) < \deg g(x)$, $\deg r_2(x) < \deg g(x)$, 则 $(q_1(x) - q_2(x))\, g(x) = r_2(x) - r_1(x)$. 由于 $g(x)$ 的首项系数是 R 中单位, 由引理 88 第 (3) 条可得

$$\deg(q_1 - q_2) + \deg g = \deg(r_2 - r_1) \leq \max(\deg r_1, \deg r_2) < \deg g.$$

这只有在 $\deg(q_1 - q_2) = \deg(r_2 - r_1) = -\infty$ 时才能成立, 于是 $q_1(x) - q_2(x) = 0 = r_1(x) - r_2(x)$, 即 $q_1(x) = q_2(x), r_1(x) = r_2(x)$. 这就证明了唯一性.

域上的多项式环

定理 90

设 F 是域, 则 $F[x]$ 中任一理想都是主理想, 即对任意 $I \triangleleft F[x]$, 必定存在多项式 $g \in F[x]$ 使得 $I = (g)$.

证明: 若 $I = (0)$, 则结果显然成立.

若 $I \neq (0)$, 则 I 中一定存在非零多项式. 假设 $g(x)$ 是 I 中一个次数最低的非零多项式, 下面我们证明 g 是 I 的一个生成元. 设 $f(x)$ 是 I 中的任意一元素. 则根据定理 89, 一定存在 $q(x), r(x) \in F[x]$ 使得

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

于是有 $r(x) = f(x) - q(x)g(x)$. 注意到 $g(x) \in I$, 因此 $q(x)g(x) \in I$, 从而 $r(x) = f(x) - q(x)g(x) \in I$. 由于 $\deg(r(x)) < \deg(g(x))$, 而 $g(x)$ 是 I 中次数最低的非零多项式, 因此必有 $r(x) = 0$, 即 $f(x) = q(x)g(x)$, 所以 $I = (g(x))$.

域上的多项式环

定理 91

设 F 是域, $f(x)$ 与 $g(x)$ 是 F 上不全为零的两个多项式, 则存在 F 上的多项式 $s(x), t(x)$ 使得

$$s(x)f(x) + t(x)g(x) = \gcd(f(x), g(x)).$$

域上的多项式环

定理 92

设 F 是域, $f(x) \in F[x]$ 是一个次数大于零的不可约多项式, 则 $(f(x))$ 是 $F[x]$ 的极大理想, 从而 $F[x]/(f(x))$ 是一个域.

证明: 设 I 是 $F[x]$ 的任一满足 $(f(x)) \subsetneq I$ 的理想, 则存在 $g(x) \in I, g(x) \notin (f(x))$. 由于 $f(x)$ 不可约, 故 $f(x)$ 与 $g(x)$ 互素, 于是存在 $u(x), v(x) \in F[x]$ 使得

$$u(x)f(x) + v(x)g(x) = 1,$$

故 $1 \in I$, 于是 $I = F[x]$, 即 $(f(x))$ 是 $F[x]$ 的极大理想. 进而可知 $F[x]/(f(x))$ 是一个域.

定理 93

设 F 是域, 设 $f(x), g(x), h(x)$ 是 F 上任意三个不全为 0 的多项式, 且有 $f(x) = q(x)g(x) + h(x)$, 其中 $q(x) \neq 0$. 则 $\gcd(f(x), g(x)) = \gcd(g(x), h(x))$.

定理 94 (辗转相除法)

设 $f(x), g(x)$ 是域 F 上的两个多项式, $g(x) \neq 0$. 记 $r_0(x) = f(x), r_1(x) = g(x)$, 并反复使用定理 *89* 给出的多项式除法, 我们有

$$\begin{aligned}
r_0(x) &= q_1(x)r_1(x) + r_2(x), \quad 0 \leq \deg(r_2(x)) < \deg(r_1(x)), \\
r_1(x) &= q_2(x)r_2(x) + r_3(x), \quad 0 \leq \deg(r_3(x)) < \deg(r_2(x)), \\
&\cdots\cdots \\
r_{k-1}(x) &= q_k(x)r_k(x) + r_{k+1}(x), \quad 0 \leq \deg(r_{k+1}(x)) < \deg(r_k(x)), \\
&\cdots\cdots
\end{aligned}$$

上述过程经过有限步后, 一定存在 k 使得 $r_{k+1}(x) = 0$. 这时得到的 $r_k(x)$ 就是多项式 $f(x), g(x)$ 的最大公因式.

多项式的根

定义 95

设 E 是含幺交换环, R 是 E 是子环. $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$. 对于每个 $\alpha \in E$, 定义

$$f(\alpha) = a_0 + a_1 \alpha + \cdots + a_n \alpha^n \in E \text{ (在 } E \text{ 中的运算)},$$

称 $f(\alpha)$ 是 $f(x)$ 在 α **处的取值**, 或叫将 $x = \alpha$ 代入 $f(x)$ 而得到的值. 如果 $f(\alpha) = 0$, 则称 α 是多项式 $f(x)$ 在环 E 中的**一个根**或零点.

注 95.1

设 E 是含幺交换环, R 是 E 是子环, $g(x), h(x) \in R[x]$. 当 $f(x) = g(x)h(x)$ 时, 对任意 $\alpha \in E$ 有 $f(\alpha) = g(\alpha)h(\alpha)$.

定理 96 (余数定理)

设 R 为含幺交换环, $f(x) \in R[x]$. 则对于每个元素 $\alpha \in R$, 均有唯一的多项式 $q(x) \in R[x]$, 使得 $f(x) = q(x)(x-\alpha) + f(\alpha)$.

证明: 在定理 89 中取 $g(x) = x - \alpha$, 则存在唯一的 $r(x) \in R[x]$ 和 $q(x) = \sum_{k=0}^{n-1} b_k x^k \in R[x]$ 使得 $f(x) = q(x)(x-\alpha) + r(x)$, 其中 $\deg r(x) < \deg(x-\alpha) = 1$. 于是 $r(x)$ 为常多项式, 即 $r(x) \in R$. 由于 R 为交换环, 将 $x = \alpha$ 代入 $f(x) = q(x)(x-\alpha) + r(x)$ 可得 $f(\alpha) = r(\alpha)$.

多项式的根

定理 97

设 R 是含幺交换环, $f(x) \in R[x], \alpha \in R$, 则 α 为 $f(x)$ 的根当且仅当 $(x-\alpha) \mid f(x)$.

证明: 必要性. 由定理 96 可得 $f(x) = q(x)(x-\alpha) + f(\alpha)$. 由于 $f(\alpha) = 0$, 于是有 $f(x) = q(x)(x-\alpha)$, 即 $(x-\alpha) \mid f(x)$.

充分性. 若 $(x-\alpha) \mid f(x)$, 则有 $h(x) \in R[x]$ 使得

$$f(x) = h(x)(x-\alpha).$$

由于 R 为交换环, 将 $x = \alpha$ 代入上式立即可得 $f(\alpha) = 0$, 即 α 为 $f(x)$ 的根.

定理 98

设 D 和 E 都是整环且 $D \subseteq E$, 则对于每个非零多项式 $f(x) \in D[x]$, 它在 E 中至多有 $\deg(f)$ 个不同的根.

证明: 设 $\alpha_1, \alpha_2, \cdots, \alpha_m$ 是 $f(x)$ 在 E 中两两不同的根, 由定理 97 可知 $f(x) = q_1(x)(x - \alpha_1)$, 其中 $q_1(x) \in E[x]$. 由于 E 是交换环, 从而 $0 = f(\alpha_2) = q_1(\alpha_2)(\alpha_2 - \alpha_1)$. 由于 $\alpha_2 \neq \alpha_1$ 且 E 为整环, 从而 $q_1(\alpha_2) = 0$, 即 $q_1(x) = q_2(x)(x - \alpha_2)$, 从而 $f(x) = q_2(x)(x - \alpha_2)(x - \alpha_1)$. 由此递归可得 $f(x) = q_m(x)(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_m)$. 由于 $f(x)$ 非零, 故 $q_m(x)$ 非零, 于是 $\deg q_m(x) \geq 0$. 因此, 由引理 88 第 (3) 条可得 $\deg f(x) = m + \deg q_m(x)$, 从而 $m \leq \deg f(x)$.

多项式的根

定义 99

设 D 和 E 都是整环且 $D \subseteq E$, $\alpha \in D$, $f(x) \in D[x]$. 如果 $(x-\alpha)^m \mid f(x)$ 但是 $(x-\alpha)^{m+1} \nmid f(x)$, 则当 $m \geq 2$ 时称 α 是 $f(x)$ 的**重根**并且**重数**为 m, 当 $m = 1$ 称 α 为 $f(x)$ 的**单根**.

定义 100

设 D 是整环, $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in D[x]$, 则称

$$f'(x) = a_1 + 2a_2 x + \cdots + (n-1)a_{n-1}x^{n-2} + n a_n x^{n-1}$$

为 $f(x)$ 的**形式微商** (formal derivative).

多项式的根

定理 101

设 D 是整环, $f(x), g(x) \in D[x]$, $a \in D$, 则

(1) $(af(x))' = af'(x)$;

(2) $(f(x) + g(x))' = f'(x) + g'(x)$;

(3) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

多项式的根

定理 102

设 D 和 E 都是整环且 $D \subseteq E$, $f(x) \in D[x]$, $\alpha \in E$, 则

(1) α 为 $f(x)$ 的重根当且仅当 $f(\alpha) = f'(\alpha) = 0$;

(2) 如果 D 为域, 并且在 $D[x]$ 中 $(f, f') = 1$, 则 $f(x)$ 在 E 中没有重根.

证明: (1) 必要性. 设 α 是 $f(x)$ 的 m 重根, 其中 $m \geq 2$, 则 $f(x) = (x-\alpha)^m q(x)$, 其中 $q(x) \in E[x]$ 且 $q(\alpha) \neq 0$. 于是

$$f'(x) = m(x-\alpha)^{m-1} q(x) + (x-\alpha)^m q'(x),$$

从而 $f(\alpha) = f'(\alpha) = 0$.

证明 (续)

充分性. 当 $f(\alpha) = f'(\alpha) = 0$ 时, 显然 α 为 $f(x)$ 的根. 若 α 为 $f(x)$ 的单根, 则 $f(x) = q(x)(x - \alpha)$, 其中 $q(x) \in E[x]$ 且 $q(\alpha) \neq 0$. 此时 $f'(x) = q'(x)(x - \alpha) + q(x)$, 于是 $f'(\alpha) = q(\alpha) \neq 0$, 矛盾. 因此, α 必为 $f(x)$ 的重根.

(2) 如果 D 为域, 则由定理 91 知存在 D 上的多项式 $s(x), t(x)$ 使得

$$s(x)f(x) + t(x)f'(x) = \gcd(f(x), f'(x)) = 1.$$

如果 α 是 $f(x)$ 在 E 中的重根, 则由 (1) 可知 $f(\alpha) = f'(\alpha) = 0$. 将 $x = \alpha$ 代入上式可得矛盾 $0 = 1$, 因此 $f(x)$ 在 E 中没有重根.

多项式的根

定理 103

设 D 和 E 都是整环且 $D \subseteq E$, $f(x) \in D[x]$, $\alpha_1, \cdots, \alpha_m$ 是 $f(x)$ 在 E 中 $m \geq 1$ 个两两不同的根, 并且根 α_i 的重数为 m_i, 其中 $i \in [m]$, 则 $m_1 + \cdots + m_m \leq \deg f$.

证明: 由于 α_1 是 $f(x)$ 的 m_1 重根, 则有 $(x-\alpha_1)^{m_1} \mid f(x)$, 即有 $f(x) = q_1(x)(x-\alpha_1)^{m_1}$, 其中 $q_1(\alpha_1) \neq 0$. 由于 E 是交换环, 从而 $0 = f(\alpha_2) = q_1(\alpha_2)(\alpha_2-\alpha_1)^{m_1}$. 由于 $\alpha_2 \neq \alpha_1$ 且 E 为整环, 故 $q_1(\alpha_2) = 0$ 且 α_2 是 $q_1(x)$ 的 m_2 重根, 于是有 $q_1(x) = q_2(x)(x-\alpha_2)^{m_2}$, 从而 $f(x) = q_2(x)(x-\alpha_2)^{m_1}(x-\alpha_1)^{m_2}$. 由此递归可得 $f(x) = q_m(x)(x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}\cdots(x-\alpha_m)^{m_m}$. 由于 $f(x)$ 非零, 故 $q_m(x)$ 非零, 于是 $\deg q_m(x) \geq 0$. 因此, 由引理 88 第 (3) 条可得 $\deg f(x) = m_1 + \cdots + m_m + \deg q_m(x)$, 从而 $m_1 + \cdots + m_m \leq \deg f(x)$.

多项式的根

推论 104

设 F 是域, $f(x) \in F[x], \alpha_1, \cdots, \alpha_m$ 是 $f(x)$ 在 F 中两两不同的根, 并且根 α_i 的重数为 m_i, 其中 $i \in [m]$, 则 $m_1 + \cdots + m_m \leq \deg f$.

第四章 域的扩张

§4.1 域上的线性空间

§4.2 扩域和代数扩张

§4.3 多项式的分裂域

§4.4 有限域

§4.1 域上的线性空间

- 线性空间的定义
- 线性子空间
- 线性组合
- 线性空间的基
- 线性空间的维数

线性空间的定义

定义 105

设 V 是一个带有加法 (记作 “$+$”) 运算的非空集合, F 是一个域. 如果 V 关于加法运算构成一个交换群, 并且对每个 $k \in F, v \in V$, 在 V 中可唯一地确定一个元素 kv (称为 k 与 v 的标量乘法). 进一步, 若对任意 $k, l \in F, u, v \in V$ 满足下述条件:

(1) $(kl)v = k(lv)$;

(2) $(k + l)v = kv + lv$;

(3) $k(u + v) = ku + kv$;

(4) $1v = v$,

则称 V 为域 F 上的一个**向量空间** (vector space) 或**线性空间** (linear space). 向量空间中的元素称为**向量** (vector), 域中的元素称为**标量**或**纯量** (scalar), 域 F 称为向量空间的**基域**.

例

例 106

集合 $F^n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in F\}$ 是域 F 上的向量空间, 其加法运算和标量乘法运算分别为

$$(a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) = (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n),$$
$$k(a_1, a_2, \cdots, a_n) = (ka_1, ka_2, \cdots, ka_n).$$

例 107

域 F 上的所有 2×2 矩阵的集合 $\mathbb{M}_2(F)$ 关于如下矩阵的加法和标量乘法运算构成 F 上的向量空间:

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} + \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} = \begin{pmatrix} a_1 + b_1 & a_2 + b_2 \\ a_3 + b_3 & a_4 + b_4 \end{pmatrix},$$
$$k \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} = \begin{pmatrix} ka_1 & ka_2 \\ ka_3 & ka_4 \end{pmatrix}.$$

例

例 108

设 p 是素数, 则 $\mathbb{Z}_p$ 是一个域. 系数在 $\mathbb{Z}_p$ 上的一元多项式环 $\mathbb{Z}_p[x]$ 关于通常多项式的加法和标量乘法构成有限域 $\mathbb{Z}_p$ 上的一个向量空间.

例 109

复数域 $\mathbb{C}$ 是实数域 $\mathbb{R}$ 上的向量空间, 运算是通常的复数的加法和乘法运算.

例 110

设 E 是域, F 是 E 的子域, 那么 E 是 F 上的向量空间. 向量空间的运算就是域 E 中的运算.

线性子空间

定义 111

设 V 是域 F 上的向量空间, U 是 V 的非空子集. 如果 U 关于 V 的运算也构成 F 上的向量空间, 则称 U 为 V 的子空间.

例 112

集合 $\left\{a_0 + a_1 x + a_2 x^2 \mid a_0, a_1, a_2 \in \mathbb{Z}_5\right\}$ 是 $\mathbb{Z}_5$ 上的由所有系数在域 $\mathbb{Z}_5$ 上的多项式组成的向量空间 $\mathbb{Z}_5[x]$ 的子空间.

线性组合

定义 113

设 V 是域 F 上的向量空间, $v_1, v_2, \cdots, v_n$ 是 V 中的向量 (它们不必互不相同), 那么子集

$$\langle v_1, v_2, \cdots, v_n \rangle = \{a_1 v_1 + a_2 v_2 + \cdots + a_n v_n \mid a_1, a_2, \cdots, a_n \in F\}$$

称为 V 的由 $v_1, v_2, \cdots, v_n$ **张成的子空间**. 形如 $a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$ 的元素称为 $v_1, v_2, \cdots, v_n$ 的**线性组合**. 如果 $\langle v_1, v_2, \cdots, v_n \rangle = V$, 那么称 $v_1, v_2, \cdots, v_n$ 张成 V. 一般地, 设 B 是 V 的任一非空子集, 如果 V 中任一元素都是B 中有限多个元素的线性组合, 则称 B 张成 V.

线性相关和无关

定义 114

设 $v_1, v_2, \cdots, v_n$ 是域 F 上向量空间 V 的一组向量, 如果存在不全为零的元素 $k_1, k_2, \cdots, k_n \in F$, 使得

$$k_1 v_1 + k_2 v_2 + \cdots + k_n v_n = 0,$$

则称向量组 $v_1, v_2, \cdots, v_n$ 在 F 上**线性相关** (linearly dependent). 如果一个向量组在 F 上不是线性相关的, 则称这个向量组在 F 上**线性无关** (linearly independent).

例 115

设 $F = \mathbb{Z}_2 = \{0, 1\}$, 则 F^3 中的向量组 $\{(1,0,0), (1,1,0), (1,1,1)\}$ 在 F 上是线性无关的. 因为假设存在 $a, b, c \in F$, 使得
$a(1,0,0) + b(1,1,0) + c(1,1,1) = (0,0,0)$, 那么
$(a+b+c, b+c, c) = (0,0,0)$, 于是 $a = b = c = 0$.

线性空间的基

定义 116

设 V 是 F 上的向量空间, B 是 V 的一个非空子集. 如果 B 中任一有限子集都在 F 上线性无关, 且 B 张成 V, 则称 B 为 V 的**基**.

注 116.1

可以用集合论的方法证明每个向量空间都有基. 以有限多个元素为基的向量空间 *(包括零空间)* 称为**有限维向量空间** *(finite dimensional vector space)*, 否则称为**无限维向量空间** *(infinite dimensional vector space)*.

线性空间的基

定理 117

如果 $\{u_1, u_2, \cdots, u_m\}$ 和 $\{w_1, w_2, \cdots, w_n\}$ 都是域 F 上向是空间 V 的基, 那么 $m = n$.

证明: 假设 $m \neq n$. 不妨设 $m < n$. 由于 $u_1, u_2, \cdots, u_m$ 张成 V, 所以可设 $w_1 = k_1u_1 + \cdots + k_mu_m$, 且这些 $k_i \in F$ 不全为零, 对 $u_1, u_2, \cdots, u_m$ 的顺序适当重排后可设 $k_1 \neq 0$, 则 $w_1, u_2, \cdots, u_m$ 张成 V. 又可设 $w_2 = l_1w_1 + l_2u_2 + \cdots + l_mu_m$, 则 $l_2, \cdots, l_m$ 中至少有一个不为零, 不妨设 $l_2 \neq 0$, 则 $w_1, w_2, u_3, \cdots, u_m$ 张成 V. 继续这样去, 最后可得 $w_1, w_2, \cdots, w_m$ 张成 V, 从而可推出 w_{m+1} 是 $w_1, w_2, \cdots, w_m$ 的线性组合, 与已知条件矛盾.

线性空间的维数

定义 118

如果一个向量空间 V 具有一个含 n 个元素的基, 则称 V 的**维数** (dimension) 是 n, 零空间 $\{0\}$ 称为是由空集张成的, 并规定它的维数是 0 , 无限维向量空间的维数规定为无穷大 $+\infty$. 域 F 上向量空间 V 的维数记作 $\dim_F V$.

例 119

例 106 中的域 F 上的向量空间 F^n 是 n 维的,

$$
\begin{aligned}
e_1 &= (1, 0, \cdots, 0), \\
e_2 &= (0, 1, \cdots, 0), \\
&\cdots\cdots \\
e_n &= (0, 0, \cdots, 1)
\end{aligned}
$$

是 F^n 的一个基. 而例 112 中的向量空间 $\mathbb{Z}_p[x]$ 是 $\mathbb{Z}_p$ 上的无限维向量空间, $\{x^n \mid n \geq 0\}$ 是 $\mathbb{Z}_p[x]$ 的一个基.

§4.1 域上的线性空间

- 线性空间的定义
- 线性子空间
- 线性组合
- 线性空间的基
- 线性空间的维数

§4.2 扩域和代数扩张

- 扩域和子域
- 域的扩张
- 维数定理
- 域的构造例子
- 域论基本定理
- 代数扩张

扩域和子域

定义 120

设 F 和 E 是两个域. 如果 $F \subseteq E$, 并且 F 中的运算就是 E 的运算在 F 上的限制, 则称 E 为域 F 的**扩域** (extension field), 而称 F 为 E 的**子域**.

扩域和子域

定理 121

设 E 是域, F 是 E 的子域, S 为 E 的一个非空子集. 令

$$F(S) = \bigcap_{L \in \Sigma} L,$$

其中

$$\Sigma = \{L \mid L \text{ 为 } E \text{ 的子域且 } F \cup S \subseteq L\},$$

则 $F(S)$ 是 E 的包含 F 和 S 的最小子域. 此时称 $F(S)$ 为 E 的添加集合 S 于 F 的子域.

证明: 显然, Σ 非空. 由于 E 中加法子群和乘法子群的交仍为 E 的加法子群和乘法子群, 因此 E 的子域的交仍是 E 的子域, 于是 $F(S)$ 是 E 的子域. 又因为 $F \cup S \subseteq F(S)$, 从而 $F(S) \in \Sigma$, 于是 $F(S)$ 是 E 的包含 F 和 S 的最小子域.

扩域和子域

定理 122

设 E 是 F 的扩域, S_1 与 S_2 是 E 的两个非空子集, 则

$$F(S_1)(S_2) = F(S_1 \cup S_2) = F(S_2)(S_1).$$

证明: 因为 $F \cup S_1 \cup S_2 \subseteq F(S_1)(S_2)$, 而 $F(S_1 \cup S_2)$ 为 E 的包含 F 及 $S_1 \cup S_2$ 的最小子域, 所以

$$F(S_1 \cup S_2) \subseteq F(S_1)(S_2).$$

又因为 $F \cup S_1 \subseteq F(S_1 \cup S_2)$, 所以 $F(S_1) \subseteq F(S_1 \cup S_2)$. 又有 $S_2 \subseteq F(S_1 \cup S_2)$, 所以 $F(S_1) \cup S_2 \subseteq F(S_1 \cup S_2)$. 而 $F(S_1)(S_2)$ 为 E 的含 $F(S_1)$ 与 S_2 的最小子域, 所以

$$F(S_1)(S_2) \subseteq F(S_1 \cup S_2).$$

从而

$$F(S_1)(S_2) = F(S_1 \cup S_2).$$

同理可证 $F(S_2)(S_1) = F(S_1 \cup S_2)$. 从而可得定理结论.

扩域和子域

注 122.1

设 E 是 F 的扩域, 则在 F 中添加 E 中的集合 S 时有如下结论:

(1) 若 $S=\{a\}$, 其中 $a\in E$, 记 $F(\{a\})=F(a)$, 并称 $F(a)$ 为 F 的**单扩域**或**单扩张** *(simple extension)*. 考虑 $F(a)$ 包含 E 中哪些元素: 首先, 因为 $a\in F(a)$, 有 $a^k\in F(a)$ $(k\in\mathbb{N})$, 所以对任意的 $f(x)\in F[x], f(a)\in F(a)$. 又对任意的 $g(x)\in F[x]$, 如果 $g(a)\neq 0$, 则 $\frac{1}{g(a)}\in F(a)$. 从而 $\widetilde{F}=\left\{\frac{f(a)}{g(a)}\mid f(x),g(x)\in F[x],g(a)\neq 0\right\}\subseteq F(a)$. 由域的定义直接验证可知, $\widetilde{F}$ 是一个域, 且 $F\subseteq\widetilde{F}, a\in\widetilde{F}$, 从而 $\widetilde{F}=F(a)$, 即

$$F(a)=\left\{\frac{f(a)}{g(a)}\mid f(x),g(x)\in F[x],g(a)\neq 0\right\}.$$

(2) 设 $S=\{a_1,a_2,\cdots,a_s\}$, 其中 $a_i\in E$ $(i\in[s])$, 记 $F(S)=F\left(a_1,a_2,\cdots,a_s\right)$. 记 $F\left(a_1,a_2,\cdots,a_s\right)$ 为 F 的添加 E 的元素 $a_1,a_2,\cdots,a_s$ 所得的扩域. 由定理 *122* 知

$$F\left(a_1,a_2,\cdots,a_s\right)=F\left(a_1\right)\left(a_2\right)\cdots\left(a_s\right).$$

域的扩张

定义 123

设 E 是 F 的扩域. 如果 E 作为 F 上的向量空间是有限维的, 则称 E 是 F 的**有限扩域**或**有限扩张** (finite extension), 否则称 E 为 F 的**无限扩域**或**无限扩张** (infinite extension). E 在 F 上的维数 $\dim_F E$ 称为 E 关于 F 的**扩张次数** (degree of extension), 记作 $[E:F]$, 即

$$[E:F]=\dim_F(E).$$

例 124

复数域 $\mathbb{C}$ 作为实数域 $\mathbb{R}$ 上的向量空间有基 $1,\mathrm{i}$, 所以 $[\mathbb{C}:\mathbb{R}]=2$. 而 $\mathbb{C}$ 是有理数域 $\mathbb{Q}$ 的无限扩张.

例 125

因为 $1,\pi,\pi^2,\cdots,\pi^n,\cdots$ 在 $\mathbb{Q}$ 上线性无关, 所以 $\mathbb{Q}(\pi)$ 在 $\mathbb{Q}$ 上的弦张次数是 $[\mathbb{Q}(\pi):\mathbb{Q}]=+\infty$.

维数定理

定理 126

设 K 是域 E 的有限扩域, E 是域 F 的有限扩域, 则 K 是域 F 的有限扩域, 且

$$[K:F]=[K:E]\cdot[E:F].$$

证明: 设 $X=\{x_1,x_2,\cdots,x_n\}$ 是 K 在 E 上的基, $Y=\{y_1,y_2,\cdots,y_m\}$ 是 E 在 F 上的基, 则只要证明

$$YX=\{y_jx_i\mid 1\leqslant j\leqslant m,1\leqslant i\leqslant n\}$$

是 K 在 F 上的基.

设 $a\in K$, 则存在 $b_1,b_2,\cdots,b_n\in E$, 使得

$$a=b_1x_1+b_2x_2+\cdots+b_nx_n.$$

又对每个 $i\in[n]$, 存在元素 $c_{i1},c_{i2},\cdots,c_{im}\in F$, 使得

$$b_i=c_{i1}y_1+c_{i2}y_2+\cdots+c_{im}y_m.$$

证明 (续)

于是

$$a = \sum_{i=1}^{n} b_i x_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} c_{ij} y_j \right) x_i = \sum_{i,j} c_{ij} \left(y_j x_i \right).$$

这就证明了 YX 在 F 上张成 K.

以下证明 YX 在 F 上线性无关. 假设存在 $c_{ij} \in F, 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m$ 使得

$$0 = \sum_{i,j} c_{ij} \left(y_j x_i \right) = \sum_{i} \sum_{j} \left(c_{ij} y_j \right) x_i,$$

那么因为每个 $c_{ij} y_j \in E$, 而 X 是 K 在 E 上的基, 所以对任意 $i \in [n]$ 有

$$\sum_{j} c_{ij} y_j = 0.$$

注意到每个 $c_{ij} \in F$, 且 Y 是 E 在 F 上的基, 因此每个 $c_{ij} = 0$. 这就证明了 YX 在 F 上线性无关, 于是 YX 是 K 在 F 上的基.

域的构造例子

引理 127

设 F 是任一有限域, 则对任意正整数 n 均存在 F 上的 n 次不可约多项式.

定理 128

设 F 是任一有限域, $f(x) \in F[x]$ 是一个首 1 的 n 次不可约多项式. 令

$$F[x]_{f(x)} = \{g(x) \in F[x] \mid \deg(g) < \deg(f) = n\}$$

并在 $F[x]_{f(x)}$ 中定义加法运算 $g(x) \oplus h(x) = g(x) + h(x)$ 和乘法运算 $g(x) \odot h(x) = g(x)h(x) \pmod{f(x)}$, 则 $F[x]_{f(x)}$ 是一个域.

证明

显然 $F[x]_{f(x)}$ 关于加法运算 "$\oplus$" 构成交换群, 关于乘法运算 "$\odot$" 满足结合律并有单位元 1. 要证明 $F[x]_{f(x)}$ 是一个域只需证明对任意非零多项式 $g(x) \in F[x]_{f(x)}$ 有乘法逆即可. 由定理 91 可得存在 $s(x), t(x) \in F[x]$ 使得

$$s(x)f(x) + t(x)g(x) = \gcd(f(x), g(x)),$$

从而对任意 $u(x) \in F[x]$ 有

$$[s(x) + u(x)g(x)]f(x) + [t(x) - u(x)f(x)]g(x) = \gcd(f(x), g(x)).$$

因此由带余除法可知必有 $u'(x) \in F[x]$ 使得
$\deg[t(x) - u'(x)f(x)] < \deg(f) = n$. 令 $t'(x) = t(x) - u'(x)f(x)$, 由 $\gcd(g(x), f(x)) = 1$ 立即可得 $t'(x) \odot g(x) = 1$, 即 $g(x)$ 可逆. 因此 $F[x]_{f(x)}$ 是一个域.

域论基本定理

定理 129 (域论基本定理, Kronecker(1887))

设 F 是域, $p(x)$ 是 $F[x]$ 中次数大于零的不可约多项式, 那么存在 F 的扩域使得 $p(x)$ 在此扩域中有根.

证明: 只需构造 F 的一个扩域 $\bar{E}$ 使得 $p(x)$ 在 $\bar{E}$ 中有根即可. 先取 E 为 $F[x]/\langle p(x)\rangle$, 由定理 87 和定理 73 知 E 是一个域. 由于

$$\phi : \ F \longrightarrow E$$

$$a \longmapsto a + \langle p(x)\rangle$$

是单射且保持两个运算, 故 E 中有一个同构于 F 的子域.

证明 (续)

显然, $F \cap E = \emptyset$. 于是由环的扩张定理可知存在 F 的扩环 $\bar{E}$ 以及环同构

$$\tilde{\phi} : \bar{E} \cong E$$

使得 $\tilde{\phi}|_F = \phi$. 由于 E 是域, 因此 $\bar{E}$ 也是域. 设 $\alpha \in \bar{E}$ 使得 $\tilde{\phi}(\alpha) = x + \langle p(x) \rangle$. 由于

$$\tilde{\phi}(p(\alpha)) = p(x + \langle p(x) \rangle) = p(x) + \langle p(x) \rangle = 0 + \langle p(x) \rangle,$$

所以 $p(\alpha) = 0$. 故 α 为 $p(x)$ 在 $\bar{E}$ 中的根.

例

注 129.1

由于 $\bar{E}$ 是 E 中用 $a\,(a \in F)$ 取代 $a + \langle p(x) \rangle$ 而得到的 F 的扩域, 即 $\bar{E}$ 是将 F 嵌入 E 而得到扩域, 所以不妨就将 $\bar{E}$ 就看成是 E, 而认为 E 包含 F. 以后, 凡是遇到类似的情况, 都将以此观点来看待 F 的扩域.

例 130

设 $f(x) = x^5 + 2x^2 + 2x + 2 \in \mathbb{Z}_3[x]$, 则 $f(x)$ 在 $\mathbb{Z}_3$ 上的不可约分解形式为 $\left(x^2 + 1\right)\left(x^3 + 2x + 2\right)$. 因此, 为求包含 $f(x)$ 根的 $\mathbb{Z}_3$ 的扩域 E, 可取 $E = \mathbb{Z}_3[x] / \left\langle x^2 + 1 \right\rangle$ (这是一个有 9 个元素的域) 或者取 $E = \mathbb{Z}_3[x] / \left\langle x^3 + 2x + 2 \right\rangle$ (这是一个有 27 个元素的域).

例

例 131

设 $f(x)=x^2+1\in\mathbb{Q}[x]$, 则在 $E=\mathbb{Q}[x]/\left\langle x^2+1\right\rangle$ 中有

$$\begin{aligned} f\left(x+\left\langle x^2+1\right\rangle\right) &= \left(x+\left\langle x^2+1\right\rangle\right)^2+1 \\ &= x^2+\left\langle x^2+1\right\rangle+1 \\ &= x^2+1+\left\langle x^2+1\right\rangle \\ &= \left\langle x^2+1\right\rangle. \end{aligned}$$

我们知道, 多项式 x^2+1 以复数 i 作为其一个根, 但这里想强调的是仅用有理数就构造出了一个域, 这个域包含有理数集以及多项式 x^2+1 的根. 这里根本不需要任何复数的知识.

代数扩张

定义 132

设 E 为域 F 的扩域, $\alpha \in E$, 如果存在 F 上的非零多项式 $f(x)$, 使得 $f(\alpha) = 0$, 则称 α 为 F 上的一个**代数元** (algebraic element). 如果 α 不是 F 上的代数元, 那么称 α 为 F 上的一个**超越元** (transcendental element). 如果 F 的扩域 E 中的每个元素都是 F 上的代数元, 则称 E 是 F 的**代数扩张** (algebraic extension). 如果 E 不是 F 的代数扩张, 则称 E 为 F 的**超越扩张** (transcendental extension).

注 132.1

有理数域上的代数元称为代数数, 不是代数数的数称为超越数.

§4.2 扩域和代数扩张

- 扩域和子域
- 域的扩张
- 维数定理
- 域的构造例子
- 域论基本定理
- 代数扩张

§4.3 多项式的分裂域

- 分裂域的定义
- 分裂域的形式
- 分裂域的存在性
- 分裂域的唯一性

分裂域的定义

定义 133

设 E 是 F 的扩域. $f(x)$ 为 F 上的一个非常数多项式. 如果 $f(x)$ 能分解成 $E[x]$ 中一次因式的乘积, 则称 $f(x)$ 在 E 上是**分裂**的. 如果 $f(x)$ 在 E 上是分裂的, 但 $f(x)$ 在 E 的任一包含 F 的真子域上都不分裂, 则称 E 为多项式 $f(x)$ 在 F 上的**分裂域** (splitting field).

例 134

仍考虑前面提到的多项式 $f(x) = x^2 + 1 \in \mathbb{Q}[x]$. 因为 $x^2 + 1 = (x + \mathrm{i})(x - \mathrm{i})$, 所以 $f(x)$ 在 $\mathbb{C}$ 中是分裂的, 但它在 $\mathbb{Q}$ 上的分裂域却是 $\mathbb{Q}(\mathrm{i})$, 而 $x^2 + 1$ 在 $\mathbb{R}$ 上的分裂域是 $\mathbb{C}$.

分裂域的形式

定理 135

设 $f(x) \in F[x], E$ 是 F 的扩域, 且在 E 上有

$$f(x) = b\,(x - a_1)\,(x - a_2) \cdots (x - a_n)\,,\ b \neq 0,$$

则 E 为 $f(x)$ 在 F 上的分裂域的充分必要条件是

$$E = F\,(a_1, a_2, \cdots, a_n)\,.$$

分裂域的存在性

定理 136

设 $f(x)$ 为域 F 上的一个非常数多项式, 则存在 F 的扩域 E, 使 E 为 $f(x)$ 在 F 上的分裂域.

证明: 对 $n = \deg f(x)$ 应用数学归纳法.

如果 $n = 1$, 那么 $f(x)$ 已经是一次的, 所以 F 本身就是 $f(x)$ 在其上的分裂域. 假设对所有的域及所有次数小于 n 的多项式结论都成立, 则由定理 154, 存在 F 的扩域 E', 使 $f(x)$ 在 E' 中至少有一个根, 设为 a_1, 则在 $E'[x]$ 中有 $f(x) = (x - a_1)\, g(x), g(x) \in E'[x]$. 因为 $\deg g(x) < \deg f(x)$, 由归纳假设知, 存在多项式 $g(x)$ 在 E' 上的分裂域 K, 使在 $K[x]$ 中有

$$g(x) = b\,(x - a_2)\,(x - a_3) \cdots (x - a_n)\,, \quad b \neq 0.$$

令

$$E = F\,(a_1, a_2, \cdots, a_n)\,,$$

则由定理 135 知 E 就是 $f(x)$ 在 F 上的分裂域. 由数学归纳法知结论成立.

例

例 137

考虑 $\mathbb{Z}_3[x]$ 中的不可约多项式 $f(x)=x^2+x+2$. 由于在 $\mathbb{Z}_3[\mathrm{i}]=\{a+b\mathrm{i}\mid a,b\in\mathbb{Z}_3\}$ 上有

$$f(x)=[x-(1+\mathrm{i})][x-(1-\mathrm{i})].$$

所以 $\mathbb{Z}_3[\mathrm{i}]$ 就是 $f(x)$ 在 $\mathbb{Z}_3$ 上的分裂域. 另一方面, 由定理 154 的证明知 $E=\mathbb{Z}_3[x]/\left\langle x^2+x+2\right\rangle$ 中的元素 $x+\left\langle x^2+x+2\right\rangle$ 是 $f(x)$ 的根, 易验证 $2x+2+\left\langle x^2+x+2\right\rangle\in E$ 是另一个根. 于是 $f(x)$ 在 E 中分裂. 又因为 E 只有 9 个元素, 可得 $[E:\mathbb{Z}_3]=2$, 所以 E 也是 $f(x)$ 在 $\mathbb{Z}_3$ 上的分裂域. 于是找到了 $f(x)$ 在 $\mathbb{Z}_3$ 上的两个分裂域, 一个是 $\mathbb{Z}_3[\mathrm{i}]$, 另一个是 $\mathbb{Z}_3[x]/\left\langle x^2+x+2\right\rangle$. 将陪集 $1+\left\langle x^2+x+2\right\rangle$ 与 $\mathbb{Z}_3$ 中的 1 等同, 并将陪集 $x+\left\langle x^2+x+2\right\rangle$ 记作 β. 于是,

$$E=\{0,1,2,\beta,2\beta,\beta+1,2\beta+1,\beta+2,2\beta+2\}.$$

并且有

$$x^2+x+2=(x-\beta)[x-(2\beta+2)]=(x-\beta)(x+\beta+1).$$

分裂域的唯一性

定理 138

设 ϕ 是域 F 到 F' 的同构, $f(x)$ 是 F 上的非常数多项式. 如果 E 是 $f(x)$ 在 F 上的分裂域, E' 是 $\phi(f(x))$ 在 F' 上的分裂域, 那么存在从 E 到 E' 的同构, 且该同构在 F 上与 ϕ 一致.

推论 139

设 F 是域, $f(x) \in F[x]$, 那么 $f(x)$ 在 F 上的任何两个分裂域都是同构的.

证明: 假设 E 和 E' 都是 $f(x)$ 在 F 上的分裂域, 则在上述定理中取 ϕ 为 F 的恒等映射即得结果.

§4.4 有限域

- 有限域的乘法群
- 本原元
- 极小多项式
- 极小多项式的不可约性
- 极小多项式的次数
- 有限域的扩张
- 本原多项式
- 有限域上的域论基本定理
- 有限域的唯一性

有限域的乘法群

定理 140

设 E/F 是任一有 q 个元素的有限域, 则 $E^* = E \setminus \{0\}$ 中每个元素 α 均满足 $\alpha^{q-1} = 1$, 即 E^* 中的每个元素均是 $x^{q-1} - 1 \in F[x]$ 的根, 并且

$$x^{q-1} - x = \prod_{\alpha \in E^*} (x - \alpha).$$

证明: 由于 E^* 中每个元素的阶都是 $q-1$ 的因子, 于是对 E^* 中任意元素 α 均有 $\alpha^{q-1} = 1$, 即 E^* 中的每个元素均是 $x^{q-1} - 1 \in F[x]$ 的根. 由于 $x^{q-1} - 1 \in F[x]$ 最多有 $q-1$ 个根, 因此 $x^{q-1} - 1 = \prod_{\alpha \in E^*}(x - \alpha)$.

推论 141 (费马小定理)

设 E/F 是一个含 q 个元素的有限域, 则 E 中每个元素 α 均满足 $\alpha^q = \alpha$, 即 E 中的每个元素均是 $x^q - x \in F[x]$ 的根, 因此 $x^q - x = \prod_{\alpha \in E}(x - \alpha)$.

引理 142

设 G 是有限交换群, $\alpha, \beta \in G$, $\operatorname{ord}\alpha = r$, $\operatorname{ord}\beta = s$. 若 $(r, s) = 1$, 则 $\operatorname{ord}\alpha\beta = rs$.

证明: 设 $\operatorname{ord}\alpha\beta = d$, 则 $1 = \left((\alpha\beta)^d\right)^s = (\alpha\beta)^{ds} = \alpha^{ds}\beta^{ds} = \alpha^{ds}(\beta^s)^d = \alpha^{ds}$, 于是 $r \mid ds$. 由于 $(r, s) = 1$, 所以 $r \mid d$. 同理考虑 $\left((\alpha\beta)^d\right)^r = 1$ 可得 $s \mid d$. 由 $(r, s) = 1$ 可知 $rs \mid d$, 又由 $(\alpha\beta)^{rs} = (\alpha^r)^s (\beta^s)^r = 1$ 可知 $d \mid rs$, 因此有 $rs = d$.

有限域的乘法群

引理 143

设 F 是任一域, $x^m-1, x^n-1 \in F[x]$, 其中 m, n 为正整数. 若 $m \mid n$, 则 $(x^m-1) \mid (x^n-1)$.

证明: 不妨设 $n = tm$, 则有
$x^n - 1 = (x^m-1)(x^{n-m} + x^{n-2m} + x^{n-3m} + \cdots + x^{n-tm})$. 于是
$(x^m-1) \mid (x^n-1)$.

有限域的乘法群

定理 144

设 E/F 是一个有 q 个元素的有限域, 则其乘法群是循环群.

证明: 将 $q-1$ 作因子分解可得

$$q-1=p_1^{c_1}p_2^{c_2}\cdots p_s^{c_s},$$

其中 $p_1,\cdots,p_s$ 为不同的素数, $c_i\geq 1$ 对任意 $i\in[s]$. 由定理 140 我们知道 E^* 中的全部 $q-1$ 个非零元素是多项式 $x^{q-1}-1$ 的全部根.

证明 (续)

现在证明对每个 $i \in [s]$, E^* 中均有一个阶为 $p_i^{c_i}$ 的元素. 由于 $p_i^{c_i} \mid q-1$, 因此多项式 $x^{p_i^{c_i}} - 1$ 是 $x^{q-1} - 1$ 的因式, 于是 $x^{p_i^{c_i}} - 1$ 的全部根都是 $x^{q-1} - 1$ 的根, 即根都在 E^* 之中. 由于 $x^{q-1} - 1$ 没有重根, 所以 $f_i(x) = x^{p_i^{c_i}} - 1$ 也没有重根, 即 $f_i(x)$ 在 E^* 中有 $p_i^{c_i}$ 个不同的根. 由于 $p_i^{c_i-1} \mid p_i^{c_i}$, 因此多项式 $g_i(x) = x^{p_i^{c_i-1}} - 1$ 整除 $f_i(x)$, 于是 $g_i(x)$ 也有 $p_i^{c_i-1}$ 个不同的根, 并且这些根都是 $f_i(x)$ 的根. 注意到 $f_i(x)$ 有 $p_i^{c_i}$ 个根, 因此存在 $\alpha_i \in E^*$ 使得 α_i 是 $f_i(x)$ 的根但不是 $g_i(x)$ 的根. 即 $\alpha_i^{p_i^{c_i}} = 1$ 但是 $\alpha_i^{p_i^{c_i-1}} \neq 1$. 所以 α_i 的阶为 $p_i^{c_i}$. 于是, 对每个 $i \in [s]$, E^* 中均有一个阶为 $p_i^{c_i}$ 的元素 α_i. 令 $\alpha = \alpha_1\alpha_2\cdots\alpha_s$, 则由引理 142 可知 α 的阶为 $p_1^{c_1}\cdots p_s^{c_s} = q-1$. 因此 E^* 为循环群.

本原元

定义 145

有限域的乘法群的生成元称为该有限域的本原元.

推论 146

设 F 是一个有 q 个元素的有限域, 那么 F 共有 $\varphi(q-1)$ 个本原元.

极小多项式

定义 147

设 E/F, 则对任意 $\alpha \in E$, 我们称 $F[x]$ 中满足 $g(\alpha) = 0$ 的次数最小的首一多项式

$$g(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n$$

为 α 在 F 上的**极小多项式**.

引理 148

设 E/F, $\alpha \in E$, $g(x) \in F[x]$ 是 α 的极小多项式. 若有 $g'(x) \in F[x]$ 使得 $g'(\alpha) = 0$, 则 $g(x) \mid g'(x)$.

证明: 由极小多项式的定义可知 $\deg g'(x) \geq \deg g(x)$. 由带余除法可得 $g'(x) = h(x)g(x) + r(x)$, 其中 $\deg r(x) < \deg g(x)$. 令 $x = \alpha$ 可得 $0 = 0 + r(\alpha)$, 于是 $r(x)$ 是一个次数更低的且以 α 为根的多项式, 这与 $g(x)$ 是极小多项式矛盾, 从而 $r(x) = 0$. 因此 $g(x) \mid g'(x)$.

极小多项式的不可约性

定理 149

设 E/F, 则对任意 $\alpha \in E$, 其在 F 上的极小多项式唯一存在, 并且是 F 上的不可约多项式.

证明: 设 E 中有 q^n 个元素, 则由推论 141 可知 E 中任一元素 α 均是 F 上的多项式 $x^{q^n} - x$ 的根. 因此 α 一定满足 F 上的一个首项系数为 1 的次数最低的多项式. 这证明了 α 在 F 上存在一个极小多项式.

现证明唯一性. 假设 $g_1(x)$ 和 $g_2(x)$ 都是 α 在 F 上的极小多项式, 则由引理 148 可得 $g_1(x) \mid g_2(x)$ 和 $g_2(x) \mid g_1(x)$. 由 $g_1(x)$ 和 $g_2(x)$ 最高项系数为 1 立即可得 $g_1(x) = g_2(x)$.

现证明不可约性. 如果 $g(x) = g_1(x)g_2(x)$, 其中 $\deg g_1(x) > 0$, $\deg g_1(x) > 0$. 于是由 $g(\alpha) = g_1(\alpha)g_2(\alpha) = 0$ 可知 $g_1(\alpha) = 0$ 或 $g_2(\alpha) = 0$, 这与 $g(x)$ 是 α 的极小多项式矛盾, 从而 $g(x)$ 不可约.

极小多项式的次数

定理 150

设 E/F, 其中 $|F| = q$, $|E| = q^n$, 则任意 $\alpha \in E$ 在 F 上的极小多项式次数不超过 n.

证明: 由于 E 是 F 上的 n 维线性空间, 则 $n+1$ 个元素 $1, \alpha, \alpha^2, \cdots, \alpha^n$ 在 F 上必定线性相关, 即存在 F 上不全为 0 的 $n+1$ 个元素 $a_0, a_1, \cdots, a_n$ 使得 $\sum_{i=0}^{n} a_i \alpha^i = 0$. 因此, $\sum_{i=0}^{n} a_i \alpha^i$ 是 F 上以 α 为根且次数不超过 n 的多项式. 从而定理得证.

域的扩张

定理 151

设 E/F, $|F| = q$, $|E| = q^n$, $f(x) = a_0 + a_1 x + \cdots + a_m x^m \in F[x]$ 为 F 上的 m 次不可约多项式. 若 $\alpha \in E$ 是 $f(x)$ 的一个根, 则

$$F_0 = \{c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1} \mid c_0, c_1, \cdots, c_{m-1} \in F\}$$

是 E 的子域且 $|F_0| = q^m$.

本原多项式

定义 152

设 E/F, 我们称 $F[x]$ 中以 E 的本原元为根的极小多项式为E/F 上的**本原多项式**.

定理 153

设 E/F, 其中 $|F| = q$, $|E| = q^n$, 则 E/F 上本原多项式的次数为 n.

证明: 设 α 是 E 的本原多项式, 其极小多项式次数为 d, 则由定理 151 知

$$F_0 = \{c_0 + c_1\alpha + \cdots + c_{d-1}\alpha^{d-1} \mid c_0, c_1, \cdots, c_{d-1} \in F\}$$

是 E 的子域且 $|F_0| = q^d$. 由于 F_0 包含 α, 因此 $F_0 = E$, 于是 $d = n$.

域论基本定理

定理 154

设 F 是一个有限域, $|F| = q$. 若 $f(x) \in F[x]$ 是一个首 1 的 n 次不可约多项式, 则存在 F 的一个阶为 q^n 的扩域 E 使得 $f(x)$ 在 E 中有根, 并且该根在 F 上的极小多项式是 $f(x)$.

证明: 设 $f(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1} + x^n \in F[x]$ 是不可约多项式, 由定理 128 知有限域 $F[x]_{f(x)}$ 是 F 的一个有 q^n 个元素的扩域, 且其限制在 F 上时即为 F 中的运算. 显然, 此时未定元 x 即为 $f(x)$ 在有限域 $F[x]_{f(x)}$ 中的根. 进一步, 由引理 148 以及 $f(x)$ 是不可约多项式直接可得 x 在 F 上的极小多项式是 $f(x)$.

不可约多项式的性质

定理 155

设 E/F, 其中 $|F| = q$, $|E| = q^n$. 若 $f(x) \in \mathbb{F}[x]$ 是一个 m 次不可约多项式, 则 $f(x) \mid (x^{q^n} - x)$ 当且仅当 $m \mid n$.

证明: 必要性. 由定理 154 知 $f(x)$ 在 F 的某个扩域中一定有根, 设其中的一个根为 α. 于是有 $(x - \alpha) \mid f(x)$, 因此 $(x - \alpha) \mid (x^{q^n} - x)$, 即 α 是 $x^{q^n} - x$ 的一个根. 由推论 141 知 E 中的全部元素恰为 $x^{q^n} - x$ 的全部根, 因此 $\alpha \in E$. 由定理 151 知

$$F_0 = \{c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1} \mid c_0, c_1, \cdots, c_{m-1} \in F\}$$

是 E 的子域且 $|F_0| = q^m$, 于是 $[F_0 : F] = m$. 由于 $[E : F] = n$, 则由定理 126 知 $m \mid n$.

证明 (续)

充分性. 由定理 154 知 $f(x)$ 在 F 的一个阶为 q^m 的扩域中有根, 记这个扩域为 F_0, 其中一个根为 α. 由 $\alpha \in F_0$ 可得 $\alpha^{q^m} = \alpha$, 于是 $\alpha^{q^{2m}} = (\alpha^{q^m})^{q^m} = \alpha^{q^m} = \alpha$, $\alpha^{q^{3m}} = \alpha, \cdots, \alpha^{q^{tm}} = \alpha$, 其中 $n = tm$. 因此 α 是 $x^{q^n} - x$ 的一个根. 由定理 154 知 $f(x)$ 是 α 在 F 上的极小多项式, 于是由引理 148 立即可得 $f(x) \mid x^{q^n} - x$.

有限域的唯一性

定理 156

两个阶相同的有限域 E/F 和 E'/F' 的素域 F 和 F' 同构, 从而 E 和 E' 同构.

证明: 设 E 和 E' 的阶都为 p^n, p 是一个素数. 那么它们的素域 F 和 F' 都是 p 个元素的. 设而 0 和 $0'$ 分别是 F 和 F' 的零元, 1 和 $1'$ 分别是 F 和 F' 的单位元, 那么

$$F = \{0, 1, 21, \cdots, (p-1)1\},$$
$$F' = \{0', 1', 21', \cdots, (p-1)1'\}.$$

显然

$$\sigma : F \mapsto F', \quad ke \mapsto ke' \quad (0 \leqslant k \leqslant p-1)$$

就是从 F 到 F' 的一个同构.

证明 (续)

设 ξ 是 F 的一个本原元, $f(x)=f_0+f_1x+\cdots+f_{n-1}x^{n-1}+x^n\in F[x]$ 是 ξ 在 F 上的极小多项式. 令

$$g(x)=f_0'+f_1'x+\cdots+f_{n-1}'x^{n-1}+x^n, f_i'\in F',$$

其中 $\sigma(f_i)=f_i', i=0,1,2,\cdots,n-1$. 因为 $f(x)$ 是 F 上的不可约多项式, 易证 $g(x)$ 是 F' 上的不可约多项式. 注意到 $\deg g(x)=n$, 由定理 155 可得

$$g(x)\mid\left(x^{p^n}-x\right),$$

从而存在 $h(x)\in F'$ 使得 $x^{p^n}-x=g(x)h(x)$, 其中 $\deg g(x)=p^n-n$.

证明 (续)

由于 E' 中全部元素都是 $x^{p^n}-x$ 的根, 因此 $g(x)$ 在 E' 中有根, 不妨设一个根为 ξ'. 由于 $g(x)$ 是首项系数为 1 的 F' 上的不可约多项式, 所以 $g(x)$ 就是 ξ' 在 F' 上的极小多项式. 由定理 151 可得

$$E'=\left\{a'_0+a'_1\xi'+\cdots+a'_{n-1}\xi'^{n-1}\mid a'_0,a'_1,\cdots,a'_{n-1}\in\Pi'\right\}.$$

容易验证映射

$$\sum_{i=0}^{n-1}a_i\xi^i\mapsto\sum_{i=0}^{n-1}\sigma\left(a_i\right)\xi'^i\quad(a_i\in F)$$

是从 E 到 E' 的一个同构映射.

共轭元

注 156.1

从现在起, 我们用 $\mathbb{F}_q$ 或 $\mathbb{GF}(q)$ 表示含有 q 个元素的有限域.

定义 157

设 $\mathbb{F}_{q^n}/\mathbb{F}_q$ 且 $\alpha \in \mathbb{F}_{q^n}$, 则元素 $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$ 称为 α 关于 $\mathbb{F}_q$ 的**共轭元**.

不可约多项式的性质

定理 158

设 $f(x)=\sum_{i=0}^{n-1} f_i x^i + x^n \in \mathbb{F}_q[x]$ 是 n 次首 1 不可约多项式, 则 f 在 $\mathbb{F}_{q^n}$ 中恰有 n 个单根, 并且这 n 个根关于 $\mathbb{F}_q$ 共轭.

证明: 由定理 154 和定理 156 可知 $f(x)$ 在 $\mathbb{F}_{q^n}$ 中有根. 记其中的一个根为 α, 则 $f(x)$ 为 α 在 F 上的极小多项式. 下面证明如果 $\alpha \in \mathbb{F}_{q^n}$ 是 f 的一个根, 则 α^q 也是. 注意到

$$\begin{aligned} f\left(\alpha^q\right) &= f_0 + f_1\alpha^q + f_2\alpha^{2q} + \cdots + f_{n-1}\alpha^{(n-1)q} + \alpha^{nq} \\ &= f_0^q + f_1^q\alpha^q + f_2^q\alpha^{2q} + \cdots + f_{n-1}^q\alpha^{(n-1)q} + \alpha^{nq} \\ &= \left(f_0 + f_1\alpha + f_2\alpha^2 + \cdots + f_{n-1}\alpha^{n-1} + \alpha^n\right)^q \\ &= (f(\alpha))^q = 0. \end{aligned}$$

证明 (续)

因此, 元素 $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$ 都是 f 的根. 下面证明这些元素互不相同. 假设存在整数 j 和 k 使得 $\alpha^{q^j} = \alpha^{q^k}$, 其中 $0 \leq j < k \leq n-1$. 等式两边取 q^{n-k} 次幂可得

$$\alpha^{q^{n-k+j}} = \alpha^{q^n} = \alpha.$$

由引理 148 可得 $f(x) \mid x^{q^{n-k+j}} - x$. 于是由定理 155 可得 $n \mid n-k+j$. 但是 $0 < n-k+j < n$, 矛盾. 因此 $\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}$ 均是 f 的单根.

定理 159

对任意 $\alpha \in \mathbb{F}_{q^m}$, 令 $f(x)$ 是 α 在 $\mathbb{F}_q$ 上的极小多项式, e 是使 $\alpha^{q^e} = \alpha$ 的最小非负整数, 则

$$f(x) = \prod_{i=0}^{e-1} \left(x - \alpha^{q^i}\right).$$

证明: 首先证明多项式 $f(x) = \prod_{i=0}^{e-1}(x - \alpha^{q^i})$ 在 $\mathbb{F}_q$ 上. 令 $f(x) = \sum_{i=0}^{e} f_i x^i$, 则 $(f(x))^q = \prod_{i=0}^{e-1}(x - \alpha^{q^i})^q = \prod_{i=0}^{e-1}(x^q - \alpha^{q^{i+1}}) = \prod_{i=0}^{e-1}(x^q - \alpha^{q^i}) = f(x^q)$. 于是 $(f(x))^q = \sum_{i=0}^{e} f_i x^{qi}$. 另一方面, $(f(x))^q = (\sum_{i=0}^{e} f_i x^i)^q = \sum_{i=0}^{e} f_i^q x^{qi}$. 因此有 $f_i = f_i^q$, 于是 $f_i \in \mathbb{F}_q$, 故 $f(x) = \prod_{i=0}^{e-1}(x - \alpha^{q^i}) \in \mathbb{F}_q[x]$. 进一步, 由定理 149 和定理 158 可知 $f(x)$ 是 α 在 $\mathbb{F}_q$ 上的极小多项式.