一点域论

王玮

2021 年 11 月 7 日

鉴于课时限制, 这里的多数内容将作为参考阅读材料, 我们将介绍基本概念, 但会略过很多证明. 计划详细讲的内容有:

1. 商环的构造, 命题 1.12;
2. 第一个有限域的构造, 命题 2.5;
3. 多项式根的存在性命题 3.14;
4. 代数闭域的存在性定理 4.2 和代数闭包的唯一性定理 4.12;
5. 代数基本定理 5.1;
6. 有限域的唯一存在性定理 6.4.

若时间允许, 将展开上述内容所需要的某些结论的证明.

1 环

定义 1.1. 一个 **环** (ring) 是一个满足以下条件的 5-元组 $(R, 0, 1, +, \times)$:

1. R 是一个集合;
2. R 有 **零元** (记为 0_R 或 0) 和 **幺元** (记为 1_R 或 1) (故 R 非空);
3. $+_R, \times_R$ (简记为 $+, \times$) 是 R 上的二元运算且满足以下运算规则
   (a) $x + 0 = x$;
   (b) $x + (y + z) = (x + y) + z$;
   (c) $x + y = y + z$;

(d) 每个 x 对应 (唯一的) y 使得 $x+y=0$;

(e) $x\times 1=x$;

(f) $x\times(y\times z)=(x\times y)\times z$;

(g) $x\times(y+z)=(x\times y)+(x\times z)$;

(h) $(y+z)\times x=(y\times x)+(z\times x)$.

$+,\times$ 分别称为环 R 的加法、乘法. 通常不假定环的乘法满足交换律. 但我们的课程上仅考虑乘法满足交换律的环 (称为 **交换环** (commutative ring)), 即

(i) $x\times y=y\times x$.

以下环这一概念仅指交换环.

通常记 $x\times y$ 为 xy, 并且记 $(x\times y)+z$ 为 $xy+z$.

通常我们直接用 R 指代环 $(R,0,1,+,\times)$.

(d) 中断言对应于 x 的 y 记为 $-x$. 记 $x+(-y)$ 为 $x-y$.

命题 1.2. *对环 R 的任意元素 x, $-x=(-1)x$.*

例 1.3. 常见的环有: $\mathbb{Z},\mathbb{Q},\mathbb{R}$ 等. 注意: $\mathbb{N}$ 及其上的常见运算不构成一个环.

若 R 是一个环, 令 $R[X]$ 记所有如下多项式构成的集合

$$a_0+a_1X+\cdots+a_nX^n,$$

定义加法、乘法为通常的多项式加法、乘法, $0,1$ 分别为只有常数项 $0_R,1_R$ 的多项式. 则 $R[X]$ 也构成一个环, 且当 R 是交换环时 $R[X]$ 也是交换的.

若 R 是环, 令 $M_n(R)$ 记所有元素在 R 中的 $n\times n$ 方阵的集合, 即 $M_n(R)$ 中的元素如下形式

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}.$$

如同定义实矩阵的加法、乘法运算一样, 可以定义 $M_n(R)$ 上的加法、乘法运算. 零元定义为所有元素都为 0_R 的 $n\times n$ 矩阵, 幺元定义为对角线元素为 1_R、其它元素为 0_R 的 $n\times n$ 矩阵. 则 $M_n(R)$ 也构成一个环. 不过, 即使 R 是交换环, $M_n(R)$ 通常也不是交换环.

当谈论一个特定的环 R 时, 习惯用 n 或 n_R ($n \in \mathbb{N}$) 表示 R 中的幺元 1_R 连加 n-次; 类似地, -2 表示 R 中 $(-1)+(-1)$, 等等. 当 $n>0$, $a \in R$ 时, a^n 是 a 连乘 n 次所得的元素; $a^0 = 1 = 1_R$.

定义 1.4. 设 R 为环. 若存在正整数 n 使得 $n_R = 0_R$, 则称 R 的 **特征**

$$\mathrm{char}(R) = \min\{n \in \mathbb{N} : n > 0, n_R = 0_R\};$$

否则 $\mathrm{char}(R) = 0$.

易见: $\mathrm{char}(\mathbb{Z})$ 和很多大家熟悉的环的特征都为 0. 后面我们将看到特征大于 0 的环.

定义 1.5. 令 L_{ring} 记只有以下非逻辑符号的一阶语言:

- 两个常元符号 $\dot{0}, \dot{1}$;
- 两个二元函数符号 $\dot{+}, \dot{\times}$.

L_{ring} 称为 **环的一阶语言**, 或 **环的语言**.

当然每个环都是一个 L_{ring}-模型.

定义 1.6. 设 R 是一个环. R 的一个 **子环** (subring) 是指一个满足以下条件的 $S \subseteq R$,

- $0, \in S$, $1 \in S$;
- S 对加法和乘法封闭.

例 1.7. 设 R 是环而 $A \subseteq R$. 令 $-A = \{-a : a \in A\}$,

$$\langle A\rangle^R = \{a_1^{n_1} + \cdots + a_k^{n_k} + m : k \in \mathbb{N}, n_i \in \mathbb{N}, a_i \in A \cup (-A), m \in \mathbb{Z}\}.$$

容易验证 $\langle A\rangle^R$ 是 R 的最小的包含 A 的子环. (当 R 确定时, 记 $\langle A\rangle^R$ 为 $\langle A\rangle$)

定义 1.8. 设 R 是一个环. R 的一个 **理想** (ideal) 是一个满足以下条件的 R 的非空子集 I:

1. 任意 $x \in I$ 和 $y \in R$, $xy \in I$;
2. 任意 $x \in I$ 和 $y \in I$, $x + y \in I$.

R 的一个理想 I 是 **真理想** (proper ideal), 当且仅当 $I \neq R$.

例 1.9. 1. $\{0\}$ 和 R 是任意环 R 的两个理想, 它们称为 **平凡理想** (trivial ideals).

2. 设 R 是环, $a \in R$, 记

$$(a) = aR = \{ar : r \in R\}.$$

则 (a) 是一个理想, 称为 a 生成的 **主理想** (principal ideals).

3. $(1) = R$.

4. 在整数环 $\mathbb{Z}$ 中, 可以证明所有理想都形如 (n).

5. 设 R 是环, $a_1, \dots, a_n \in R$, 记

$$(a_1, \dots, a_n) = \{r_1 a_1 + \cdots + r_n a_n : r_1, \dots, r_n \in R\}.$$

则 $(a_1, \dots, a_n)$ 是一个理想, 称为 $a_1, \dots, a_n$ 生成的理想.

定义 1.10. 环 R 的理想 I 是 **素理想** (prime ideal), 当且仅当 I 满足以下条件

- 任意 a, b, 若 $ab \in I$ 则 $a \in I$ 或 $b \in I$.

命题 1.11. *一个正整数 n 是素数, 当且仅当 $n\mathbb{Z}$ 是 $\mathbb{Z}$ 的素理想*

设 I 是环 R 的一个理想, 定义 R 上的二元关系如下

$$x \sim_I y \Leftrightarrow x - y \in I.$$

此二元关系具有以下性质,

命题 1.12. *设 $R, I, \sim_I$ 如上.*

1. *$\sim_I$ 是一个等价关系.*

2. *$\sim_I$ 的等价类形如 $a + I = \{a + x : x \in I\}$.*

3. *任意 R 中元素 x, y 和 x', y', 若 $x + I = x' + I$ (即 $x \sim_I x'$) 且 $y + I = y' + I$ 则*

$$(x + y) + I = (x' + y') + I, \quad xy + I = x'y' + I.$$

由以上命题, 我们可以定义一个环 R', 其元素为 $\sim_I$ 的等价类 $x+I$ ($x \in R$), 加法和乘法分别如下

$$(x+I) +' (y+I) = (x+y)+I, \quad (x+I) \times' (y+I) = xy+I.$$

可以验证 $(R', 0+I, 1+I, +', \times')$ 满足定义 1.1, 并且是一个交换环 (当 R 是交换环时). R' 是一个 **商环** (quotient ring), 通常记为 R/I, 并记 $+', \times'$ 为 $+, \times$.

例 1.13. 当 $R = \mathbb{Z}$, n 是固定的正整数, $I = n\mathbb{Z}$ 时, 以上关系 $\sim_I$ 就是相对 n 的同余关系, 即

$$x \sim_I y \Leftrightarrow x \equiv y \mod n.$$

这时商环 $\mathbb{Z}/n\mathbb{Z}$ 就是我们介绍过的同余类的环. 且 $\mathrm{char}(\mathbb{Z}/n\mathbb{Z}) = n$.

2 域

注意, 定义 1.1 不要求环中乘法可逆.

定义 2.1. 一个域是一个满足以下条件的交换环 $(F, 0, 1, +, \times)$:

(j) 任意 $x \neq 0$, 存在 (唯一的) y 使得 $xy = 1$ (记此 y 为 x^{-1} 或 $1/x$).

通常用 F 指代域 $(F, 0, 1, +, \times)$.

域 F 的所有非零元素构成的集合记为 $F^\times$, 称为 F 的 **乘法群** (multiplicative group). 显然, $1 = 1_F \in F^\times$, 且 $F^\times$ 对乘法和 $x \mapsto x^{-1}$ 封闭.

例 2.2. 常见的域有: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 等.

令 $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. 容易验证 $\mathbb{Q}[\sqrt{2}]$ 构成一个域.

定义 2.3. 设 L 是一个域. L 的一个 **子域** (subfield) 是 L 的一个对乘法逆元封闭的子环 K, 即: K 是 L 的子环, 且任意非零的 $a \in K$, $a^{-1} \in K$. 这时我们也称 L 是 K 的 **扩域** (field extension).

例 2.4. $\mathbb{R}, \mathbb{C}$ 和 $\mathbb{Q}[\sqrt{2}]$ 都是 $\mathbb{Q}$ 的扩域.

设 K 是 L 的子域, 将 L 作为向量集合可以定义一个 K-线性空间, 其上的加法是 L 中的加法, 数乘运算为: 若 $a \in K$, $b \in L$, 则 ab 是 a 和 b 在

L 中的乘积. 这时, L 作为 K-线性空间的维数记为 $[L:K]$. 在上面的例子中, $[\mathbb{R}:\mathbb{Q}]$ 和 $[\mathbb{C}:\mathbb{Q}]$ 都是无穷的 (不可数的), 但

$$[\mathbb{Q}[\sqrt{2}]:\mathbb{Q}] = [\mathbb{C}:\mathbb{R}] = 2.$$

当 $[L:K] \in \mathbb{N}$ 时, 称 L 是 K 的一个 **有限扩张** (finite extension); 否则 L 是 K 的无限扩张.

命题 2.5. *一个正整数 n 是素数, 当且仅当 $\mathbb{Z}/n\mathbb{Z}$ 是域.*

证明. 注意在环 $\mathbb{Z}/n\mathbb{Z}$ 中, $(n) = n\mathbb{Z}$ 是加法零元, $1 + (n)$ 是乘法幺元.

当 $n = pq$, 且 p 和 q 都小于 n 时,

$$(p + (n)) \times (q + (n)) = pq + (n) = (n).$$

当 n 是素数时, 所有正的 $m < n$ 都与 n 互素. 根据 Bézout 定理, 存在 u, v 使得

$$mu + nv = 1,$$

故

$$(m + (n)) \times (u + (n)) = mu + (n) = 1 + (n).$$

□

定义 2.6. 一个环 R 是一个 **整环** (domain), 当且仅当其中任意一对非零元的乘积都非零, 即, 任意 $a, b \in R$, 若 $ab = 0$ 则 $a = 0$ 或 $b = 0$.

例 2.7.

- $\mathbb{Z}$ 是整环.
- 当正整数 n 是合数时, $\mathbb{Z}/(n)$ 不是整环.
- 所有域都是整环.

设 D 是整环, 令

$$D' = \{(a, b) \in D^2 : b \neq 0\}.$$

定义 D' 上的等价关系 $\sim$ 如下

$$(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 b_2 = a_2 b_1.$$

(a,b) 代表的等价类记为 $[a,b]$. 令 Q 为所有 $\sim$-等价类的集合. 记 $0_Q=[0,1]$, $1_Q=[1,1]$, 定义

$$[a_1,b_1]+_Q[a_2,b_2]=[a_1b_2+a_2b_1,b_1b_2],\quad [a_1,b_1]\times_Q[a_2,b_2]=[a_1a_2,b_1b_2].$$

容易验证 $+_Q,\times_Q$ 是 Q 上的二元运算.

命题 2.8. *以上 $(Q,0_Q,1_Q,+_Q,\times_Q)$ 是一个域, 称为 D 的* **分式域** *(fraction field).*

例 2.9. 设 K 是域而 $A\subseteq K$. 例 1.7 中定义了 K 中最小的包含 A 的子环 $\langle A\rangle$. 参考 [3], $\langle A\rangle$ 的分式域为 $[A]^K$, 即

$$[A]^K=\{ab^{-1}:a\in\langle A\rangle,0\neq b\in\langle A\rangle\}.$$

则 $[A]^K$ 是 K 中最小的包含 A 的子域. (当 K 确定时, 记 $[A]^K$ 为 $[A]$).

当 $K=\mathbb{R}$ 时,

$$[1]^K=[\mathbb{Z}]^K=\mathbb{Q}.$$

3 多项式

设 K 是一个域.

$K[X]$ 是所有以 X 为变元的、系数来自 K 的多项式 (polynomial) 的集合, 其中的元素形如

$$a_nX^n+\cdots+a_1X+a_0.$$

多项式的加法、乘法运算与实多项式的对应运算一致. 以下"多项式"指 $K[X]$ 的元素.

一个 **n-次**多项式是指一个形如 $f(X)=a_nX^n+\cdots+a_1X+a_0$ 且 $a_n\neq 0$ 的多项式, 这时记 $\deg f=n$. 上述 n-次多项式是 **首一的** (monic) 当且仅当 $a_n=1$. 系数全为零的多项式记为 0, 约定 $\deg 0=-\infty$. 多项式的次数有一些简单性质

$$\deg fg=\deg f+\deg g,\quad \deg(f+g)\leq\max\{\deg f,\deg g\}.$$

命题 3.1 (带余除法)**.** *若 $f(X)\in K[X]$, $g(X)\in K[X]$, 则存在唯一的一对多项式 $q(X),r(X)$ 满足*

$$f(X)=g(X)q(X)+r(X)$$

且 $\deg r<\deg g$.

在命题 3.1 中, 若 $r=0$, 则称 g **整除** f, 记为 $g|f$.

命题 3.2 (最大公因式)**.** *若 $f,g\in K[X]$ 且它们的次数都大于 0, 则存在唯一的首一多项式 h 满足*

1. *$h|f$, $h|g$;*
2. *任意多项式 h', 若 $h'|f$ 且 $h'|g$, 则 $h'|h$.*

命题 3.2 中的 h 称为 f 和 g 的**最大公因式** (greatest common divisor), 记为 $\gcd(f,g)$.

定理 3.3 (Bézout)**.** *若 $f,g\in K[X]$ 且它们的次数都大于 0, 则存在多项式 u,v 使得*

$$\gcd(f,g)=fu+gv.$$

命题 3.2 和定理 3.3 都可以用命题 3.1 和辗转相除法证明. 分析辗转相除法还可以得到以下结论.

命题 3.4. *设 K 是域, L 是 K 的扩域. 若 $f(X),g(X)\in K[X]$ 且在 $L[X]$ 中有最大公因式 $h(X)$. 则 $h(X)\in K[X]$ 且 $h(X)$ 是 $f(X),g(X)$ 在 $K[X]$ 中的最大公因式.*

例 3.5. 若 $f_1,\ldots,f_n$ 是 n 个多项式, 则以下集合是一个理想

$$\{f_1g_1+\cdots+f_ng_n : g_1,\ldots,g_n\in K[X]\},$$

记为 $(f_1,\ldots,f_n)$. 运用最大公因式的存在性, 可以证明

$$(f_1,f_2)=(\gcd(f_1,f_2)).$$

不难定义多个多项式 $f_1,\ldots,f_n$ 的最大公因式 $\gcd(f_1,\ldots,f_n)$. 可以进一步得到

$$(f_1,\ldots,f_n)=(\gcd(f_1,\ldots,f_n)).$$

定理 3.6 (主理想)**.** *$K[X]$ 的所有理想都是主理想, 即形如 (f).*

作为定理 3.6 的特例, 若 $f_1,\ldots,f_n$ 是 n 个多项式, 则唯一存在首一多项式 g 使得 $(g)=(f_1,\ldots,f_n)$. 容易验证 g 整除每一个 f_i, 且任意同时整除每一个 f_i 的多项式 h 都能整除 g. 因此, g 称为 $f_1,\ldots,f_n$ 的 **最大公因式**, 记 $g=\gcd(f_1,\ldots,f_n)$.

设 $f \in K[X]$ 的次数大于 0. 若存在多项式 g, h 使得 $f = gh$ 且 $\deg f > \max\{\deg g, \deg h\}$, 则 f 是 **可约的** (reducible); 否则 f 是 **不可约的** (irreducible).

例 3.7.

- 任意一次多项式都不可约.
- 在 $\mathbb{Q}[X]$ 中, 当 $k > 0$ 时 $X^k - 2$ 是不可约多项式.
- 在 $\mathbb{R}[X]$ 中, $X^2 - 2$ 是可约多项式, $X^2 + 1$ 是不可约多项式. $\mathbb{R}[X]$ 中次数 > 2 的多项式都可约.
- 在 $\mathbb{C}[X]$ 中, 一个多项式不可约, 当且仅当它是一次多项式, 即形如 $X - a$.

定理 3.8 (唯一不可约分解)**.** *任意非零多项式 f 都对应一组 $a, p_1, \ldots, p_k$ 和 $n_1, \ldots, n_k$, 使得*

1. $f = ap_1^{n_1} \cdots p_k^{n_k}$,
2. $0 \neq a \in K$,
3. p_i *都是各不相同的首一不可约多项式,*
4. n_i *都是正整数.*

并且, 若 $b, q_1, \ldots, q_\ell$ 和 $m_1, \ldots, m_\ell$ 也满足以上四个条件, 则 $a = b$, $k = \ell$, 且存在双射 $\sigma : \{1, \ldots, k\} \to \{1, \ldots, k\}$ 使得 $q_i = p_{\sigma(i)}$, $m_i = n_{\sigma(i)}$.

与命题 2.5 类似, 利用 Bézout 定理 3.3 可得

命题 3.9. *$f(X) \in K[X]$ 不可约, 当且仅当 $K[X]/(f)$ 是域.*

K 可以看作 $K[X]/(f)$ 的一个子环, 因为可以定义环单同态

$$i : K \to K[X]/(f), \quad i(a) = a + (f).$$

这样, $f(X) = \sum_{k=0}^{n} a_k X^k \in K[X]$ 也可以看作 $(K[X]/(f))[X]$ 中的如下多项式

$$\sum_{k=0}^{n} (a_k + (f)) X^k.$$

定义 3.10. 设 K 是域同时是环 R 的子环, $f(X) \in K[X]$. $a \in R$ 是 $f(X)$ 的 **根** (root), 当且仅当 $f(a) = 0$.

命题 3.11. *若 $f(X)\in K[X]$ 在环 $R\supseteq K$ 中有不同的根 $a_1,\dots,a_n$, 则 $\prod_{i=1}^n(X-a_i)|f(X)$. 因此, n-次多项式最多有 n 个不同的根 (在任何环中).*

由以上命题, 可定义: $a\in R$ 是 $f(X)\in K[X]$ 的 **n-重根**, 当且仅当 $(X-a)^n|f(X)$ 但 $(X-a)^{n+1}\nmid f(X)$, 这时 n 称为 a 作为 $f(X)$ 的根的 **重数** (multiplicity). **单根** (simple root) 指 1-重根. 在代数中, “$f(X)$ 在 R 中有 n 个根”, 通常指: $f(X)$ 在 R 中有 n_1-重根 a_1, ..., n_r-重根 a_r, $a_1,\dots,a_r$ 各不相同且 $n_1+\cdots+n_r=n$.

命题 3.12. *设 $f(X)\in K[X]$. 则在 $K[X]/(f)$ 中, $X+(f)$ 是 $f(X)$ 的根.*

证明. 设 $f(X)=a_0+a_1X+\cdots+a_nX^n$, 在 $K[X]/(f)$ 中, $f(X)$ 的系数分别是 $a_0+(f),a_1+(f),\dots,a_n+(f)$. 则

$$\begin{aligned} f(X+(f)) &= \sum_{k=0}^n(a_k+(f))(X+(f))^k=\sum_{k=0}^n(a_kX^k+(f)) \\ &= \sum_{k=0}^n a_kX^k+(f)=(f). \end{aligned}$$

□

注释 3.13. 以上命题的证明中 X 扮演了两个角色: 一个作为变元符号, 一个作为 $K[X]$ 中的元素 (一次单项式 X). 为了厘清这两个角色, 我们考察以下一阶语言: 给 K 中每个元素 a 添加一个常元符号 c_a 到环的语言 L_R 中, 所得的语言记为 $L_{R,K}$. 定义以 K 为论域的 $L_{R,K}$-模型 (K,I) 如下:

- $I(\dot{0}),I(\dot{1}),I(\dot{+}),I(\dot{\times})$ 分别解释为 K 中的零元、幺元、加法和乘法;
- $I(c_a)=a$.

$K[X]$ 中的多项式 $a_0+a_1X+\cdots+a_kX^k$ 都可以看作 $L_{R,K}$-项

$$c_{a_0}\dot{+}c_{a_1}x\dot{+}\cdots\dot{+}c_{a_k}x^k.$$

因此 $K[X]$ 是 $L_{R,K}$-项的集合, 以它为论域定义 L_R 的解释就构成一个 L_R-模型 (即一个环).

给定多项式 $f\in K[X]$, 可以定义 $K[X]$ 上的等价关系. $K[X]/(f)$ 就是对应的等价类的集合; 以它为论域, 可以定义 $L_{R,K}$-的解释 J, 其中 $J(c_a)=a+(f)$. 将 f 看作 $L_{R,K}$-项 $t(x)$, 以上命题说明

$$(K[X]/(f),J)\models\exists x(t(x)\approx\dot{0}).$$

以上两个命题可得出,

命题 3.14. *设 K 是域而 $f \in K[X]$, 且 $\deg f > 0$. 则存在 K 的扩域 K' 和 $a \in K'$ 使得 $f(a) = 0$.*

证明. 设 $f \in K[X]$, $\deg f > 0$. 由唯一不可约分解定理 3.8, 取 f 的一个不可约因式 $p(X)$.

令 $L = K[X]/(p(X))$. 由命题 3.9 知 L 是一个域. 由命题 3.12 知 $p(X)$ 在 L 中有根.

定义 $\sigma : K \to L$ 为

$$\sigma(a) = a + (p(X)),$$

即: σ 将 K 的元素 a 映射为 $K[X]$ 中零次多项式 a 的等价类 $a + (p(X))$. 容易验证 σ 是单同态, 即 L_{ring}-模型 K 至 $K[X]/(p(X))$ 的嵌入映射. 由此嵌入映射, 我们就可以仿照 [3, 引理 1.4.3] 的证明, 构造 K 的扩域 K', 使之与 $K[X]/(p(X))$ 同构. □

设 $f(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$. 定义 $f(X)$ 的 **形式导式** (formal derivative) 为

$$f'(X) = \sum_{i=1}^{n} i a_i X^{i-1} = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}.$$

显然 $f'(X) \in K[X]$.

定理 3.15. *设 K 是域, $f(X) \in K[X]$. 则以下等价*

1. *存在 K 的扩域 L 使得 $f(X)$ 在 L 中有重根 (即 L 中有 a 使得 $(X-a)^2 | f(X)$).*
2. *$(f, f') = 1$.*

由定理 3.15 及命题 3.4 可知, 一个 K-多项式能否有重根, 只与 $K[X]$ 有关.

4 代数闭域

定义 4.1. 一个域 K 是 **代数闭域**, 当且仅当任意 $f(X) \in K[X]$ 都在 K 中有根, 即存在 $a \in K$ 使得 $f(a) = 0$.

定理 4.2. *任意域都有代数闭的扩域.*

我们需要以下引理,

引理 4.3. *设 K 是一个域. 则存在 K 的一个扩域 K', 使得 $|K'| \leq \max\{|K|, \omega\}$, 且任意 $f(X) \in K[X]$ 在 K' 中有根.*

证明. 我们只证明 $|K| \leq \omega$ 的情况. 这时 $K[X]$ 可数, 故可以列举其中多项式如下:

$$f_0(X), f_1(X), \ldots, f_n(X), \ldots$$

令 $K_0 = K$. 设 K_n 是 K 的扩域且 $|K_n| \leq \omega$. 若 $f_n(X) \in K[X] \subseteq K_n[X]$ 在 K_n 中有根, 则令 $K_{n+1} = K_n$. 否则, 由命题 3.14, 取 K_n 的扩域 K_{n+1} 使得 $f(X)$ 在 K_{n+1} 中有根; 注意由命题 3.14 的证明及 3.12 知, K_{n+1} 同构于 $K_n[X]$ 的一个商, 因此

$$|K_{n+1}| \leq |K_n[X]| \leq \max\{|K_n|, \omega\} \leq \omega.$$

最后, 令 $K' = \bigcup_{n\in\mathbb{N}} K_n$. □

证明定理 4.2. 设 K 是一个域. 同样我们只证明 $|K| \leq \omega$ 的情况.

由引理 4.3, 我们可构造域的序列 $(K_n)_{n\in\mathbb{N}}$, 使得

- $K_0 = K$;
- $|K_n| \leq \omega$;
- $K_n \subseteq K_{n+1}$;
- 若 $f(X) \in K_n[X]$ 则 $f(X)$ 在 K_{n+1} 中有根.

最后, 令 $K' = \bigcup_{n\in\mathbb{N}} K_n$. □

定义 4.4. 设 k 是域, K 是 k 的扩域. $a \in K$ 是 **k-代数的** (algebraic over k), 当且仅当存在 $f(X) \in k[X]$ 使得 $f(a) = 0$.

$a \in K$ 是 **k-超越的** (transcendental over k), 当且仅当 a 不是 k-代数的.

我们可以将代数/超越元的概念推广至 K 的一般子集上. 设 $S \subseteq K$. $b \in k$ 是 **S-代数的** (**S-超越的**), 当且仅当 b 是 $[S]^K$-代数的 ($[S]^K$-超越的). 记

$$(S^{\text{alg}})^K = \{a \in K : a \text{ 是} S\text{-代数的}\},$$

称为 S 在 K 中的 **代数闭包** (algebraic closure).

k 的扩域 K 是一个 **代数扩域** (algebraic extension), 当且仅当 $K = (k^{\mathrm{alg}})^K$, 即所有 $a \in K$ 都是 k-代数的.

在 $\mathbb{C}$ 或 $\mathbb{R}$ 中, $\mathbb{Q}$-超越元简称为 **超越数**, 其它数称为 **代数数**. 由康托的定理 $|\mathbb{Q}| < |\mathbb{R}| = |\mathbb{C}|$ 可知, "多数" 实数或复数是超越数. 但要证明具体的实数是超越数并不容易. 根据 Lindemann-Weierstrass 定理, e 和 π 是超越数.

定义 4.5. 设 k, K 如上. 若 $a \in K$ 是 k-代数的, 则有次数最小的首一多项式 $f(X) \in k[X]$ 使得 $f(a) = 0$, 称之为 a 的 **k-最小多项式** (minimal polynomial).

注意: 同一个域 K 可能是两个域 k_1 和 k_2 的扩域, 其中同一个元素 a 可能既是 k_1-代数元又是 k_2-代数元, 这时相对不同域 a 可能有不同的最小多项式. 比如: 当 $K = \mathbb{R}$ 时, 取 $k_1 = \mathbb{Q}[\sqrt{2}]$ 和 $k_2 = \mathbb{Q}[\sqrt[3]{2}]$ (参加以下定理 4.7), 则 $a = \sqrt[6]{2}$ 是 k_i-代数元, 其 k_1-最小多项式为 $X^3 - \sqrt{2}$, k_2-最小多项式为 $X^2 - \sqrt[3]{2}$.

命题 4.6. *设 $a \in K \supset k$ 是 k-代数的. 设 $h(X) \in k[X]$ 是 a 的最小多项式.*

(1) $h(X)$ 是不可约的.

(2) 若 $f(X) \in k[X]$ 且 $f(a) = 0$, 则 $h(X) | f(X)$. 故代数元的最小多项式是唯一的.

证明. (1) 可由定理 3.8 得到.

(2) 可由命题 3.2 得到. □

我们有如下的代数元判别定理.

定理 4.7 ([4], 定理 5.4)**.** *设 K 是 k 的扩域, $a \in K$. 则以下命题等价:*

1. a 是 k-代数的.

2. $k[a] = \{f(a) : f(X) \in k[X]\}$ 是有限维 k-线性空间.

3. $k[a]$ 是域.

设 $f(X) = b_0 + b_1 X + \cdots + b_n X^n \in k[X]$, $a \in K \supset k$. 严格来说, 以上 $f(a)$ 应该记作 $f(a)^K$, 表示其中的加法、乘法是域 K 上的加法、乘法. 这时 $k[a]$ 应该记作 $k[a]^K$. 若将 K 和 k 看作 L_{ring}-模型, k 是 K 的子模型, $k[a]^K$ 是在 K 中构造的、包含 $k \cup \{a\}$ 的最小子模型.

推论 4.8. 若 $a \in K \supset k$ 是 k-代数的, $b \in K$ 是 $k[a]$-代数的, 则 b 也是 k-代数的.

证明. 用定理 4.7 之 2. □

命题 4.9. 设 k 有两个扩域 K, L, $a \in K, b \in L$. 设 a 是 k-代数的且有最小多项式 $f(X)$. 若 $f(b) = 0$ 则 $k[a] \cong k[b]$.

证明. 只要验证以下映射是同构映射

$$\sigma : k[a] \to k[b], \quad \sigma(f(a)) = f(b).$$

□

命题 4.10. 若 K 是域, $\emptyset \neq S \subseteq K$. 设 $A = (S^{\text{alg}})^K$. 则 $A = (A^{\text{alg}})^K$.

证明. 设 $b \in (A^{\text{alg}})^K$, 则有 $a_0, \ldots, a_n \in A$ 及 $f(X) = \sum_{i=0}^n a_i X^i$ 使得 $f(b) = 0$.

令 $k_0 = [S]$, $k_1 = k_0[a_0]$, $k_{i+1} = k_i[a_i]$ $(i < n)$. 则 k_n 是域, $f(X) \in k_n[X]$. 故 b 是 k_n-代数的.

多次运用推论 4.8 可知 b 是 k_0-代数的, 即 S-代数的. □

命题 4.11. 若 K 是域, $\emptyset \neq S \subseteq K$. 则 $(S^{\text{alg}})^K$ 是域.

证明. 令 $k = [S]^K$.

若 $0 \neq a, b \in (k^{\text{alg}})^K$, 则 $b \in (k[a]^{\text{alg}})^K$. 由定理 4.7 知, $k_1 = k[a]$ 和 $k_2 = k_1[b]$ 都是域. 由于 $a, b \in k_2$, 故 $a^{-1}, a+b, ab$ 都在 $k_2 \subseteq (k^{\text{alg}})^K$ 中. □

定理 4.12. 若 k 是域, K 和 L 都是 k 的代数闭扩域. 则 $(k^{\text{alg}})^K \cong (k^{\text{alg}})^L$.

证明. 这里只处理 $|k| \leq \omega$ 的情况. 这时 $k[X]$ 可数, 因此 $(k^{\text{alg}})^K$ 和 $(k^{\text{alg}})^L$ 都至多可数. 因此可分别枚举 $(k^{\text{alg}})^K$ 和 $(k^{\text{alg}})^L$ 的元素如下

$$a_0, a_1, \ldots \in (k^{\text{alg}})^K, \quad b_0, b_1, \ldots, \in (k^{\text{alg}})^L.$$

令 $E_0 = F_0 = k$, $\sigma_0 : E_0 \to F_0$ 为恒等映射 $\sigma_0(a) = a$.

设 E_{2n}, F_{2n}, σ_{2n} 满足:

- 若 $i < 2n$ 则 $a_i \in E_{2n}$, $b_i \in F_{2n}$;
- E_{2n}, F_{2n} 是 k 的扩域;

- $k \subseteq E_{2n} \subseteq (k^{\mathrm{alg}})^K$, $k \subseteq F_{2n} \subseteq (k^{\mathrm{alg}})^L$;
- $\sigma_0 \subseteq \sigma_{2n} : E_{2n} \to F_{2n}$ 是同构映射.

a_n 是 k-代数的, 因此也是 E_{2n}-代数的, 故有最小多项式 $f(X) \in E_{2n}[X]$ 使得 $f(a_n) = 0$. 设 $f(X) = c_0 + c_1 X + \cdots + c_m X^m$. 令 $g(X) = \sigma_{2n}(c_0) + \sigma_{2n}(c_1)X + \cdots + \sigma_{2n}(c_m)X^m$, 则 $g(X) \in F_{2n}[X]$. 由于 L 是代数闭域, 故存在 $b_{n'} \in (k^{\mathrm{alg}})^L$ 使得 $g(b_{n'}) = 0$ (当然在 L 中计算). 由命题 4.9 (的证明) 知, σ_{2n} 可以扩展为同构映射 $\sigma_{2n+1} : E_{2n}[a_n] \to F_{2n}[b_{n'}]$.

同理, 可定义 E_{2n+2}, F_{2n+2}, 和同构映射 $\sigma_{2n+2} : E_{2n+2} \to F_{2n+2}$.

最终, $\bigcup_n E_n = (k^{\mathrm{alg}})^K, \bigcup_n F_n = (k^{\mathrm{alg}})^L$, 且 $\sigma = \bigcup_n \sigma_n$ 是从 $(k^{\mathrm{alg}})^K$ 到 $(k^{\mathrm{alg}})^L$ 的同构映射. □

由定理 4.12, 可以将 k 在不同代数闭扩域中的代数闭包等同, 简记为 k^{alg}, 称为 k 的代数闭包. 由定理 4.12, 可知 k^{alg} 是 k 的最小的代数闭扩域.

定理 4.13. *若 k 是域, K 和 L 是 k 的代数闭扩域且 $|K| = |L| > \max\{|k|, \omega\}$. 则 $K \cong L$.*

证明. [3, 定理 3.1.2 和 3.3.3]. □

5 代数基本定理

这里的证明参考 [4, §5.1].

定理 5.1 (希尔伯特的代数基本定理)**.** *复数域 $\mathbb{C}$ 是代数闭域.*

我们先介绍复数域上多项式函数的两个性质. 对 $r \in \mathbb{R}$ 和 $a \in \mathbb{C}$, 令

$$D_r(a) = \{x \in \mathbb{R} : |x - a| < r\}, \quad \bar{D}_r(a) = \{x \in \mathbb{R} : |x - a| \leq r\}.$$

记 $D_r = D_r(0), \bar{D}_r = \bar{D}_r(0)$.

命题 5.2. *设 $f(X) \in \mathbb{C}[X]$, $0 < s \in \mathbb{R}$. 存在正实数 r 使得任意 $b \in \mathbb{C} - D_r$ 都满足 $|f(b)| > s$.*

证明. 当 $f(X) = 0$ 时结论显然成立.

设 $f(X) = a_n X^n + \cdots + a_1 X + a_0$, 其中 $a_n \neq 0$. 则任意 $b \in \mathbb{C}$,

$$|f(b)| = \left| a_n b^n + \sum_{i=0}^{n-1} a_i b^i \right| \geq |a_n||b|^n - \sum_{i=0}^{n-1} |a_i||b|^i.$$

上式右边是一个关于 $|b|$ 的、最高次项系数大于零的实多项式. 因此, 当 $|b|$ 足够大时, $|f(b)| > s$. □

命题 5.3. *设 r 是正实数, $f(X) \in \mathbb{C}[X]$. 则 $|f(X)|$ 在 $\bar{D}_r$ 上有最大值和最小值, 即, 存在 $x_m, x_M \in \bar{D}_r$ 使得*

$$|f(x_m)| = \min\{|f(a)| : a \in \bar{D}_r\}, \quad |f(x_M)| = \max\{|f(a)| : a \in \bar{D}_r\}.$$

命题 5.4. *设 $f(X)$ 是复系数多项式. 则 $|f(X)|$ 在 $\mathbb{C}$ 上有最小值.*

证明. 假设 $f(X)$ 是复系数多项式. 设 $s = |f(0)|$. 取正实数 r 使得任意 $a \in \mathbb{C} - \bar{D}_r$ 都满足 $|f(a)| > s$. 设 $|f(X)|$ 在 $\bar{D}_r$ 上取得最小值 $|f(x_m)|$, 则 $|f(x_m)| \leq s$, 故

$$|f(x_m)| = \min\{|f(a)| a \in \mathbb{C}\}.$$

□

证明定理 5.1. 假设 $f(X) = a_n X^n + \cdots + a_1 X + a_0$ 是复系数多项式且在复数域上没有根, $a_n \neq 0$. 设

$$|f(x_m)| = \min\{|f(a)| : a \in \mathbb{C}\}.$$

不妨设 $x_m = 0$. 则

$$s = |f(0)| = |a_0|.$$

不妨设 $a_0 = 1$. 则

$$f(X) = a_n X^n + \cdots + a_k X^k + 1 = 1 + a_k X^k \left(1 + X g(X)\right),$$

其中 $a_k \neq 0$, $g(X) \in \mathbb{C}[X]$. 令 $t \in \mathbb{R}$, 则

$$f(t(-a_k)^{-1/k}) = 1 - t^k(1 + t h(t)) = 1 - t^k - t^{k+1} h(t),$$

其中 h 是一个复系数多项式. 当 t 是充分小的正实数时,

$$\begin{aligned} |f(t(-a_k)^{-1/k})| &\leq |1 - t^k| + t^{k+1}|h(t)| \\ &= 1 - t^k + t^{k+1}|h(t)| \\ &= 1 - t^k(1 - t|h(t)|) < 1. \end{aligned}$$

这与 $|f|$ 在 0 处取得最小值的假设矛盾. □

6 有限域

在命题 2.5 中, 我们看到只有有限多个元素的域 $\mathbb{Z}/p\mathbb{Z}$ (p 是素数), 这时 $\mathrm{char}(\mathbb{Z}/p\mathbb{Z}) = p$.

有限域 (finite field) 是只有有限多个元素的域. 以上 $\mathbb{Z}/p\mathbb{Z}$ 是有限域, 记为 $\mathbb{F}_p$.

命题 6.1. *一个域 (作为环) 的特征或是 0 或是一个素数.*

证明. 假设域 K 的特征 $\mathrm{char}(K) = n$ 是正整数且 $n = ab$, $1 < a \in \mathbb{N}$. 则 $n_K = a_K b_K = 0_K$. 因此 $a_K = 0_K$ 或 $b_K = 0_K$. 由于 $a < n$ 且 $b < n$, 这与 $\mathrm{char}(K) = n$ 矛盾. □

定理 6.2. *任何有限域的元素个数是某个素数的幂 $p^n > 1$, 且 p 是其特征.*

证明. 设 F 是有限域且 $\mathrm{char}(F) = p > 0$.

不难验证 $\{0_F, 1_F, \ldots, (p-1)_F\}$ 构成 F 的一个子域, 且同构于 $\mathbb{F}_p$, 因此可将其等同于 $\mathbb{F}_p$ 并将 F 看作 $\mathbb{F}_p$ 的一个扩域.

故 F 可看作一个 $\mathbb{F}_p$-线性空间, 向量加法是域 F 的加法, 数乘运算为: 若 $a \in \mathbb{F}_p$, $u \in F$, 则 au 是 a 和 u 在域 F 中的乘积. 由 F 有限知, F 作为 $\mathbb{F}_p$-线性空间有一个基

$$\mathcal{B} = \{u_1, \ldots, u_n\}.$$

在此基下的坐标映射是 F 与 $\mathbb{F}_p^n$ 之间的一个双射, 而 $|\mathbb{F}_p^n| = p^n$. 因此 $|F| = p^n$. □

一个域 K 的非零元素的集合通常记为 $K^\times$, 也称为 K 的乘法群. 以下引理来自 [2, Lemma 3.3.1].

引理 6.3. *若 F 是大小为 p^n 的有限域, $0 \neq a \in F$, 则 $a^{p^n} = a$.*

证明. 设 $q = p^n$, $F^\times = \{b_1, \ldots, b_{q-1}\}$. 由 $a \neq 0$ 知, $ab_i \neq ab_j$ $(i \neq j)$, 故

$$F^\times = aF^\times = \{ab_1, \ldots, ab_{q-1}\}.$$

以上所有非零元素相乘可得

$$\prod_{i=1}^{q-1} b_i = \prod_{i=1}^{q-1} ab_i = a^{q-1} \prod_{i=1}^{q-1} b_i.$$

因此 $a^{q-1} = 1$, 从而 $a^q = a$. □

定理 6.4. 对任意素数 p 和正整数 n, 存在一个刚好有 p^n 个元素的有限域. 且两个有限域同构当且仅当它们大小相同.

证明. 先证存在性, 这部分的证明参考 [1, §V.5]. 任取素数 p 和正整数 n. 设 $K = {\mathbb{F}_p}^{\mathrm{alg}}$ 是 $\mathbb{F}_p$ 的代数闭包. 令

$$F = \{a \in K : a^{p^n} - a = 0\}.$$

即, F 是多项式 $f(X) = X^{p^n} - X$ 在 K 中的所有根构成的集合.

由 $f'(X) = p^n X^{p^n-1} - 1 = -1$ (因为 $\mathrm{char}(K) = p$) 及定理 3.15 知 $f(X)$ 没有重根. 故 $|F| = p^n$.

再验证 F 是域. 显然 $0_K, 1_K \in F$.

设 $a, b \in F$, 则

$$(a+b)^{p^n} = \sum_{i=0}^{p^n} C_{p^n}^i a^i b^{p^n-i},$$

其中 $C_{p^n}^i$ 是二项式系数, 且当 $0 < i < n$ 时 p 整除 $C_{p^n}^i$. 由 $\mathrm{char}(K) = p$ 知, 上式右边等于 $a^{p^n} + b^{p^n}$; 再由 $a, b \in F$ 知, 上式等于 $a + b$, 故 $a + b \in F$. 另一方面, 显然

$$(ab)^{p^n} = a^{p^n} b^{p^n} = ab,$$

故 $ab \in F$.

容易验证 F 对减法和除法封闭, 因此 F 是域. 这就证明定理的存在性部分.

再证同构意义上的唯一性. 设 F 如上, 而 E 是另一个大小为 p^n 的有限域. 由定理 6.2 知, E 是 $\mathbb{F}_p$ 的扩域; 由定理 4.7 知, E 是 $\mathbb{F}_p$ 的代数扩域. 因此 E 的代数闭包 E^{alg}, 记为 L, 也是 $\mathbb{F}_p$ 的代数闭包. 由定理 4.12 知, 存在同构映射 $\sigma : K \to L$. 由 F 的定义知 $F = \{a \in K : a^{p^n} = a\}$, 由引理 6.3 知 $E = \{b \in L : b^{p^n} = b\}$. 因此 σ 限制在 F 上也是一个同构映射 $\sigma \restriction F : F \to E$. □

由有限域的唯一存在性, 可将大小为 p^n 的有限域等同, 记为 $\mathbb{F}_{p^n}$.

参考文献

[1] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[2] San Ling and Chaoping Xing. *Coding theory: a first course*. Cambridge University Press, Cambridge, 2004.

[3] 姚宁远. *初等模型论*. 复旦大学出版社, 2018.

[4] 莫宗坚，蓝以中，赵春来. *代数学（上）*. 高等教育出版社, 2014.