COURSE NOTES Spring 2025

抽象代数 II

Abstract Algebra II

Runkun Liu

Nankai University

目录

记号约定 **ii**

第一章 模 **1**
1.1 模的基本概念 1
1.1.1 模的定义与例子 1
1.1.2 子模 2
1.1.3 子模与模的生成 3
1.1.4 模同态与商模 5
1.1.5 同态集合与自同态环 6
1.2 自由模 7
1.2.1 自由模与基 7
1.2.2 自由模之间的同态 9
1.2.3 交换幺环上的矩阵 10
1.2.4 PID 上矩阵的标准型 12
1.3 有限生成模 15
1.3.1 生成元与关系 15
1.3.2 PID 上的有限生成模 16
1.3.3 PID 上的有限生成扭模 20

第二章 域 **26**
2.1 基本概念 26
2.1.1 域、特征与同态 26
2.1.2 子域与素域 27
2.1.3 扩张次数与塔式公式 28
2.2 代数扩张 29
2.2.1 代数元与最小多项式 29
2.2.2 单扩张的结构与次数 30
2.2.3 代数扩张的基本性质 32
2.2.4 补充：代数闭包与纯超越扩张 34
2.3 分裂域 35
2.3.1 分裂域的构造 35
2.3.2 分裂域的唯一性 37

附录 A 适用条件速查 **42**
A.1 主要结论的适用条件 42

记号约定

以下记号在相应章节引入。除特别说明外，R 是非零幺环，模是幺左模；涉及扭元时要求标量环为整环，涉及结构定理时要求它为主理想整环。

记号	含义
$R, \mathrm{Z}(R)$	幺环及其中心。
D	主理想整环（PID）。
F, K, E	域；写 E/F 时表示域扩张。
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$	整数、有理数、实数、复数与含 p 个元素的域（p 为素数）。
$\mathrm{Hom}_R(M,N), \mathrm{End}_R(M)$	模同态集合与模自同态环。
$\mathrm{Mat}_n(F)$	域 F 上的 $n\times n$ 矩阵环。
$\ker\varphi, \mathrm{Im}\,\varphi$	同态的核与像。
$\mathrm{rank}(A), \mathrm{rank}\,M$	矩阵的秩与 PID 上有限生成模的秩。
$\mathrm{ann}(x), \mathrm{Tor}(M)$	元素的零化子与整环上模的扭子模。
$\Delta_k(A), d_i$	行列式因子与不变因子，均在相伴意义下考虑。
M_p	被不可约元 p 的某个幂杀死的元素组成的分支。
$\mathrm{Frac}(D)$	整环 D 的分式域。
$\mathrm{Ch}(F), [E:F]$	域的特征与扩张次数。
$\mathrm{Irr}(\alpha, F)$	α 在 F 上的首一最小多项式。
$F[\alpha], F(\alpha), F(S)$	添加元素生成的子环与子域。
$\mathrm{Aut}(E), \mathrm{id}_F$	自同构群与 F 上的恒等映射。

同态的矩阵表示统一使用行坐标：若 M, N 分别有 m, n 个基向量，则矩阵为 $m\times n$，并满足

$$[\varphi(x)]_{\mathcal{C}} = [x]_{\mathcal{B}} A_\varphi.$$

矩阵环作用于列向量的例子使用其自然左作用。

定义、定理、引理、命题、推论及例共享编号，按节重新计数。例如，引理 1.3.13 的编号依次记录章号、节号和条目序号；同一节的定义、定理等环境共同计数。

第一章　模

本章围绕一个问题展开：怎样用生成元及其关系描述一个模？先建立子模、商模与同态的基本工具，再研究自由模和矩阵表示，最后在主理想整环上把关系化为标准型，得到有限生成模的结构及其唯一性。除特别说明外，R 是满足 $1 \neq 0$ 的幺环，模均为幺左 R-模；D 表示主理想整环。

1.1　模的基本概念

1.1.1　模的定义与例子

定义 1.1.1 (模). 设 R 为非零幺环，M 为交换群，有从 $R \times M$ 到 M 的映射：$(a, x) \mapsto ax$ 满足：

1. 对任意 $a, b \in R, x \in M$，有：$(a+b)x = ax + bx$.
2. 对任意 $a \in R, x, y \in M$，有：$a(x+y) = ax + ay$.
3. 对任意 $x \in M$，1 是 R 的幺元，有：$1x = x$.
4. 对任意 $a, b \in R, x \in M$，有：$a(bx) = (ab)x$.

则称 M 为一个**左 R-模**，称该映射为 R 与 M 的**纯量乘法**，类似地，可以定义右 R-模以及双 R-模，接下来主要讨论左 R-模且简称为模。

模结构的关键是环中的元素如何作用于交换群。这里 $\mathrm{End}(M)$ 指交换群 $(M, +)$ 的自同态环：加法逐点定义，乘法是映射复合。模的纯量乘法等价于一个保持幺元的**环同态**

$$R \longrightarrow \mathrm{End}(M), \qquad a \longmapsto \varphi_a, \quad \varphi_a(x) = ax.$$

事实上，四条模公理分别保证逐点加法、群同态性、保持幺元及乘法与复合相容；反过来，这样的环同态也给出满足模公理的作用。

例 1.1.2 (模的例子).

1. 域 F 上的线性空间 V 是 F-模，纯量乘法为线性空间的数乘运算；
2. 列向量空间 F^n 是矩阵环 $\mathrm{Mat}_n(F)$ 上的左模，作用为矩阵与列向量相乘;
3. 任给域 F 上的线性空间 V 和 V 上的一个线性变换 $\mathcal{A}$，V 是多项式环 $F[\lambda]$-模，纯量乘法为：$(f(\lambda), v) \mapsto f(\mathcal{A})v$;
4. 任意交换群 $(G, +)$ 是 $\mathbb{Z}$-模，纯量乘法为：$(a, x) \mapsto ax$;
5. 任意幺环 R 是 R-模，纯量乘法为 R 上的乘法;

6. 任给交换群 G，记其自同态环为 $\mathrm{End}(G)$，则 G 是 $\mathrm{End}(G)$-模，纯量乘法为：$(f,x)\mapsto f(x)$.

1.1.2 子模

研究代数结构必须研究其子结构和商结构。

定义 1.1.3 (子模). R-模 M 的一个非空子集 N 称为 M 的**子模**，若 N 在 M 的加法运算和 R 与 M 的纯量乘法运算下也成为一个 R-模。

定理 1.1.4 (子模的判定). N 是 M 的子模的充要条件是：N 是 M 作为群的子群，且对任意 $a\in R, x\in N$ 有：$ax\in N$.

证明. 必要性由子模的定义得到。反之，子群条件使 N 在加法下成为交换群，纯量乘法的封闭性使 R 对 N 的作用有定义；模公理由 M 中的相应等式限制到 N 上得到，故 N 是子模。 □

例 1.1.5 (子模的例子).

1. 线性空间 V 作为 F-模，其非空子集 W 是 V 的子模当且仅当 W 是其线性子空间；
2. 线性空间 V 作为 $F[\lambda]$-模，其非空子集 W 是 V 的子模当且仅当 W 是线性变换 $\mathcal{A}$ 的不变子空间;
3. 交换群 G 作为 $\mathbb{Z}$-模，其非空子集 H 是 G 的子模当且仅当 H 是 G 的子群;
4. 幺环 R 作为 R-模，其非空子集 I 是 R 的子模当且仅当 I 是 R 的左理想;
5. 设 M 是 R-模，任取 $x\in M$，集合 $Rx:=\{ax : a\in R\}$ 是子模。

设 M_1, M_2 是 M 的两个子模，考虑：子模的交 $M_1\cap M_2$ 与子模的和 $M_1+M_2:=\{x_1+x_2 : x_1\in M_1, x_2\in M_2\}$。

定理 1.1.6 (子模的交与和). 任意一族子模的交是子模，任意有限多的子模的和是子模。

证明. 子模的交包含零元，且对差与纯量乘法封闭，故由定理 1.1.4是子模。若 $x=\sum_i x_i$、$y=\sum_i y_i$ 属于有限和，其中 $x_i, y_i\in M_i$，则 $x-y=\sum_i(x_i-y_i)$、$ax=\sum_i ax_i$ 仍属于该和，故它也是子模。空族的交约定为 M，空和为零子模，结论同样成立。 □

有和结构就可以考虑直和结构，类似群的直和，我们分别定义内直和与外直和，然后说明二者在同构意义下没有本质区别。

定义 1.1.7 (子模的内直和). 设 $M_1, M_2, \dots, M_s$ 是 M 的子模，满足 $M=M_1+\cdots+M_s$，且对任意 $u\in M$，其表示为 $u=a_1+a_2+\cdots+a_s, a_i\in M_i$ 的方式是唯一的，则称 M 为 $M_1,\dots,M_s$ 的**内直和**，记为：$M=M_1\oplus\cdots\oplus M_s$.

定理 1.1.8 (内直和的判定). 设 $M_1,\dots,M_s$ 是 M 的子模，且 $M=M_1+\cdots+M_s$。以下条件等价：

1. $M=M_1\oplus\cdots\oplus M_s$；
2. 若 $a_i\in M_i$ 且 $a_1+\cdots+a_s=0$，则每个 $a_i=0$；
3. 对每个 i，$M_i\cap\sum_{j\neq i}M_j=\{0\}$。

证明. 两个分解相减后得到零的分解，因此 (1) 与 (2) 等价。若 (2) 成立，取 $x\in M_i\cap\sum_{j\neq i}M_j$，写成 $x=\sum_{j\neq i}a_j$，由 $x-\sum_{j\neq i}a_j=0$ 得 $x=0$。反之，若 $\sum_i a_i=0$，则 $a_i=-\sum_{j\neq i}a_j$ 属于上述交，故每个 $a_i=0$。 □

定义 1.1.9 (有限多个模的外直和). 设 $N_1,\dots,N_s$ 是 R-模，考虑笛卡尔积 $N=N_1\times N_2\times\cdots\times N_s$,在 N 上定义加法为:$(x_1,\dots,x_s)+(y_1,\dots,y_s)=(x_1+y_1,\dots,x_s+y_s)$,纯量乘法为:$(a,(x_1,\dots,x_s))\mapsto(ax_1,\dots,ax_s)$,则 N 成为一个 R-模,称为 $N_1,\dots,N_s$ 的**外直和**，记为 $N=N_1\oplus\cdots\oplus N_s$.

考虑下面的命题，与群的外直积和内直积类似，模的外直和和内直和在同构意义下也没有本质区别。

定理 1.1.10 (内直和与外直和的对应). 任给外直和 $N=N_1\oplus\cdots\oplus N_s$，考虑其子模 $N_i'=\{(0,0,\dots,x_i,0,\dots,0):x_i\in N_i\}$，则 N_i' 为 N 的子模，且 N 是 $N_1',\cdots N_s'$ 的内直和；反过来，任给内直和 $N=N_1\oplus\cdots\oplus N_s$，则 N 同构于 $N_1,\dots,N_s$ 的外直和。

证明. 外直和中的每个坐标嵌入 N_i' 对加法与纯量乘法封闭，故为子模。任意元组 $(x_1,\dots,x_s)$ 是各坐标嵌入之和；各分量由对应坐标唯一确定，所以这个和是内直和。反之，从外直和到给定内直和 N 的映射 $(x_1,\dots,x_s)\mapsto\sum_i x_i$ 是模同态。内直和的生成性使它满射，分解的唯一性使它单射，故为模同构。 □

1.1.3 子模与模的生成

我们还关心子模的生成结构。在先前我们已经看到，对任意 R-模 M，任意 $x\in M$，$Rx\subseteq M$ 是 M 的一个子模，容易验证 Rx 是 M 中包含 x 的最小的子模，于是称 Rx 为 M 中由 x 生成的子模，x 是子模 Rx 的**生成元**。类似地，我们可以将生成元的个数推广至任意多个。

定义 1.1.11 (子模的生成). 设 $S\subseteq M$ 是 R-模 M 的任意子集，定义 S 生成的子模为所有包含 S 的子模的交，即：

$$\langle S\rangle:=\bigcap\{N\subseteq M:N是M的子模，且S\subseteq N\}.$$

由定义可知，$\langle S\rangle$ 是 M 中包含 S 的最小子模。这里允许 $S=\varnothing$；由于零子模也参加取交，有 $\langle\varnothing\rangle=0$。此外，由子模的运算封闭性，容易验证下面的等价刻画。

定理 1.1.12 (子模的生成)**.** 设 $S \subseteq M$，则

$$\langle S\rangle = \left\{ \sum_{i=1}^{k} a_i x_i : k \geq 0,\ a_i \in R,\ x_i \in S \right\}.$$

即 $\langle S\rangle$ 由 S 中元素的所有有限 R-线性组合构成，约定 $k=0$ 时的空和为零。

证明. 令 L 为等号右侧的集合。它含零元；合并两个有限和、将系数取负或左乘同一个标量，所得仍是有限线性组合，故 L 是子模。由于 L 包含 S，由生成子模的最小性有 $\langle S\rangle \subseteq L$。反过来，$\langle S\rangle$ 包含 S 且对模运算封闭，因此包含每个这样的有限线性组合，即 $L \subseteq \langle S\rangle$。 □

注意到上述定理中等号右侧的式子在 S 是有限集时可以写为以下等价式子：

$$\langle S\rangle = Rx_1 + \cdots + Rx_n$$

其中 $S = \{x_1, \ldots, x_n\}$，由此引出**有限生成子模**的定义。

定义 1.1.13 (有限生成子模，有限生成模)**.** 设 N 是 R-模 M 的子模，若存在有限集 $S = \{x_1, \ldots, x_n\}$（允许 $n = 0$）满足：

$$N = \langle \{x_1, \ldots, x_n\}\rangle = Rx_1 + \cdots + Rx_n$$

则称 N 为 M 的**有限生成子模**，进一步，若 $M = N$，则 M 称为**有限生成模**，特别地，可以由一个元素生成的子模（模）被称为**循环子模（模）**。

注意，有限生成模的子模未必是有限生成的，例如域 k 上无限多个变量的多项式环 $R = k[x_1, x_2, \cdots]$，R 作为 R-模是由 1 生成的，故有限生成，但考虑其理想 $I = \langle x_1, x_2, \cdots\rangle$，则 I 作为 R 的子模并不是有限生成的。

定义 1.1.14 (诺特模与左诺特环)**.** 若 R-模 M 的任意子模均有限生成，则称 M 为**诺特模（Noether 模）**。若 R 作为左 R-模是诺特模，则称 R 为**左诺特环**；等价地，R 的每个左理想都有限生成。

定义 1.1.14中的条件也可以用子模升链表述。

定理 1.1.15 (诺特模的升链条件)**.** 以下命题等价：

1. M 的任意子模有限生成;
2. M 的任意子模升链 $N_1 \subseteq N_2 \subseteq \cdots$ 必然稳定，即存在 N_k 使得 $N_k = N_{k+1} = \cdots$.

证明. ($\Rightarrow$) 取任意子模升链 $N_1 \subseteq N_2 \subseteq \cdots$，令 $N = \bigcup_{k=1}^{\infty} N_k$。升链保证 N 是子模，因而 N 有限生成。若 $N = 0$，则升链各项均为零，结论成立。否则取 $N = Rx_1 + \cdots + Rx_r$，其中 $r \geq 1$。每个 x_i 属于某个 N_{k_i}；取 $k = \max\{k_1, \ldots, k_r\}$，则全部生成元均在 N_k 中，故 $N = N_k = N_{k+1} = \cdots$，即升链最终稳定。

($\Leftarrow$) 若 M 的任意子模升链均稳定，取 M 的任意子模 N，假设 N 不是有限生成的，则归纳地选取 x_k：任取 $x_1 \in N \setminus \{0\}$，记 $N_1 = Rx_1$，然后选取 $x_2 \in N \setminus N_1$，记 $N_2 = Rx_1 + Rx_2$，不断这样进行下去，注意这里是 N 非有限生成保证了每一步中的 $N \setminus N_k$ 非空，于是我们得到子模严格升链 $N_1 \subsetneqq N_2 \subsetneqq \cdots$，则与任意升链最终稳定的条件矛盾，即 M 的任意子模 N 有限生成。 □

例 1.1.16 (有限生成模的例子).

1. 考虑 $M = \mathbb{Z}^3$ 作为 $\mathbb{Z}$-模，其子模 $N := \{(a,b,c) : a+b+c = 0\}$ 是有限生成的，生成元为：$(1,0,-1), (1,-1,0)$;
2. 考虑左诺特环 R 作为左 R-模，由定义 1.1.14，其任意子模有限生成;
3. 考虑多项式环 $R[x]$ 作为 R-模，则对任意自然数 n，$R[x]$ 中次数不大于 n 的全体多项式集合 $R[x]_n$ 作为子模是有限生成的，其生成元为：$1, x, x^2, \ldots, x^n$;
4. 考虑域上多项式环 $k[x]$，取任意次数为 $n \geq 1$ 的多项式 $f(x) \in k[x]$，则商环 $k[x]/(f(x))$ 作为 k-模是有限生成的，其生成元为：$\overline{1}, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{n-1}$.

1.1.4 模同态与商模

为了比较不同的模，先定义保持模运算的映射；随后通过商去子模构造商模，并用同态的核描述它。

定义 1.1.17 (模同态，模同构). 设 M_1, M_2 为两个 R-模，若映射 $\varphi : M_1 \to M_2$ 满足：$x, y \in M_1, \varphi(x+y) = \varphi(x) + \varphi(y)$，$a \in R, x \in M_1, \varphi(ax) = a\varphi(x)$，则称 φ 为**模同态**，满足条件的满（单）射称为满（单）模同态，双射称为**模同构**，记作 $M_1 \cong M_2$.

有了子模，就可以在商群上定义相应的模结构。

定义 1.1.18 (商模). 设 N 是 R-模 M 的子模，则考虑商群 M/N，在其上定义纯量乘法：$(a, x+N) \mapsto ax+N$，则 M/N 成为一个 R-模，称为 M 对 N 的**商模**。

这个作用与代表元的选取无关：若 $x+N = y+N$，则 $x-y \in N$，从而 $a(x-y) \in N$，故 $ax+N = ay+N$。模公理由 M 中的相应等式传到商群上得到。自然映射 $\pi : M \to M/N$ 是满模同态，其核为 N。

定理 1.1.19 (模同态基本定理). 设 $\varphi : M_1 \to M_2$ 是满模同态，则：

1. $M_1/\ker\varphi \cong M_2$，同构由 $x + \ker\varphi \mapsto \varphi(x)$ 给出;
2. $N \mapsto \varphi(N)$ 与 $L \mapsto \varphi^{-1}(L)$ 互为逆，建立 M_1 中包含 $\ker\varphi$ 的子模与 M_2 的子模之间的一一对应;
3. 若 $\ker\varphi \subseteq N_1 \subseteq M_1$，则 $M_1/N_1 \cong M_2/\varphi(N_1)$。

证明. (1) 若两个陪集相等，其代表元之差在核中，故映射良定义。该映射是满模同态，且只有零陪集映为零，因而是同构。

(2) 由满射性有 $\varphi(\varphi^{-1}(L)) = L$。若 $N \supseteq \ker\varphi$，则 $x \in \varphi^{-1}(\varphi(N))$ 时存在 $n \in N$ 使得 $\varphi(x) = \varphi(n)$，于是 $x - n \in \ker\varphi \subseteq N$，故 $x \in N$。

(3) 满模同态 $x \mapsto \varphi(x) + \varphi(N_1)$ 的核恰为 N_1，应用 (1) 即可。对非满同态，相应结论是 $M_1/\ker\varphi \cong \operatorname{Im}\varphi$。 □

1.1.5 同态集合与自同态环

模同态已在定义 1.1.17中引入。下面讨论同态集合上的加法与纯量乘法，再讨论自同态的复合。

定义 1.1.20 (同态集合)**.** 设 M 和 N 是两个模，记所有从 M 到 N 的群同态构成的集合为 $\operatorname{Hom}(M,N)$，所有 M 到 N 的模同态构成的集合为 $\operatorname{Hom}_R(M,N)$.

命题 1.1.21 (同态集合的加法)**.** 显然 $\operatorname{Hom}_R(M,N)$ 是 $\operatorname{Hom}(M,N)$ 的子集。在 $\operatorname{Hom}(M,N)$ 上定义运算加法：$(f+g)x = f(x)+g(x)$，则容易验证 $(\operatorname{Hom}(M,N),+)$ 是一个交换群，且 $\operatorname{Hom}_R(M,N)$ 是其子群。

既然 $\operatorname{Hom}_R(M,N)$ 已经是一个交换群，那我们自然想要看看在这上面有没有某个模结构，例如它是否能成为一个 R-模。最自然的尝试是沿用 N 中的纯量乘法，定义

$$(af)(x) = af(x), \qquad a \in R,\ f \in \operatorname{Hom}_R(M,N).$$

我们试着验证这是否给出了一个 R-模。首先，这个定义必须真的是从 $R \times \operatorname{Hom}_R(M,N)$ 到 $\operatorname{Hom}_R(M,N)$ 的映射；也就是说，af 不能只是一个从 M 到 N 的映射，它还必须是 R-模同态。加法的相容性由 N 的模公理得到，剩下需要检查的是对标量的相容性。任取 $b \in R, x \in M$，一方面，由 f 是模同态以及 N 的模公理，有

$$(af)(bx) = af(bx) = a\big(bf(x)\big) = (ab)f(x).$$

另一方面，若 af 是模同态，它应当满足

$$(af)(bx) = b(af)(x) = (ba)f(x).$$

因此，这个尝试能否成立，关键就在于对所有 b, x 是否有

$$(ab - ba)f(x) = 0.$$

这里不能一般地交换 a 与 b 的次序。若 R 是交换环，上述障碍就消失了，于是我们得到下面的结论；这是一个保证该作用成立的充分条件，不是从这个计算就能推出的必要条件。

定理 1.1.22 (交换环上同态集合的模结构)**.** 设 R 为交换幺环，则 $\operatorname{Hom}_R(M,N)$ 在上述纯量乘法下成为一个 R-模。

对于一般的幺环，我们可以考虑其中能够与所有元素交换的部分，即环的中心。这样不必要求整个环交换，只需把上面尝试中的标量限制在这个子环中。

定义 1.1.23 (环的中心). 幺环 R 的**中心**为

$$\mathrm{Z}(R) = \{a \in R : ab = ba \text{ 对所有} b \in R\}.$$

它是 R 的交换幺子环。

中心中的元素与所有标量交换，因此同样的作用仍成立。

定理 1.1.24 (同态集合上的中心作用). 设 R 为幺环，则 $\mathrm{Hom}_R(M, N)$ 在上述纯量乘法下成为一个 $\mathrm{Z}(R)$-模。

当 $N = M$ 时，自同态可以复合；逐点加法与复合满足环公理，恒等映射是幺元。于是 $\mathrm{Hom}_R(M, M)$ 成为一个幺环。

定义 1.1.25 (自同态环). 上述幺环记为 $\mathrm{End}_R(M)$，称为 R-模 M 的**自同态环**。

1.2 自由模

先前已经提到过，域 F 上的线性空间 V 可以看作是 F-模，所以模论也被称为“环上的线性代数”。有限维线性空间具有许多非常良好的性质，例如有一组基 $v_1, \ldots, v_n$，使每个向量有唯一的基展开，并且

$$V = Fv_1 \oplus \cdots \oplus Fv_n.$$

我们想试着在模上面也做类似的事情，得到类似的性质或结论。但一般幺环与域的性质相差很大：它可能不交换，可能有零因子，也可能有非平凡理想，因此一般的模未必能像线性空间那样选出一组基。我们先考虑一类能够保留这种基结构的模；后面会看到，它们同构于 R^n，可以作为线性空间在模上的一种推广，这就是**自由模**。本节及后文的自由模均指**具有有限基的自由模**；一般自由模允许无限基，但这里不展开。

1.2.1 自由模与基

定义 1.2.1 (自由模的泛性质). 设 R 是非零幺环，M 是 R-模。若存在 $u_1, \ldots, u_n \in M$，使得对任意 R-模 N 及任意 $v_1, \ldots, v_n \in N$，存在唯一的模同态 $\varphi : M \to N$ 满足 $\varphi(u_i) = v_i$，则称 M 为**有限生成自由模**，$u_1, \ldots, u_n$ 为它的一组**基**。零模对应 $n = 0$ 及空基。在证明基的大小唯一之前，只说这组基有 n 个元素；对一般非交换环，不能预先把 n 视为模的不变量。

上述定义被称为自由模的“泛性质”。它首先告诉我们：给定基向量的像，就能唯一决定一个模同态。粗略地讲，当我们试图用 n 个元素生成一个 R-模时，一个具有 n 个基向量的自由模就是能够得到的“最大”的模。这里的“最大”并不是说它包含所有其他模，而是指：任给由 $v_1, \ldots, v_n$ 生成的 R-模 N，泛性质都给出一个把 u_i 映为 v_i 的模同态；因为 v_i 生成 N，这个同态必为满射。换句话说，任何由 n 个元素生成的模，都可以由这样的自由模再商去某些关系得到。

定理 1.2.2 (同构保持自由性与基)**.** 设 M_1, M_2 都是 R-模, 且 M_1 为自由模, $u_1, \dots, u_n$ 是它的一组基，若存在 $\varphi : M_1 \to M_2$ 为模同构，则 M_2 也是 R 上的自由模，且 $\varphi(u_1), \dots, \varphi(u_n)$ 是 M_2 的一组基。

证明. 对任意 R-模 N 及 $v_1, \dots, v_n \in N$, 由泛性质取唯一的 $\psi : M_1 \to N$ 满足 $\psi(u_i) = v_i$。则 $\psi \circ \varphi^{-1} : M_2 \to N$ 将 $\varphi(u_i)$ 送到 v_i。任何另一满足这些条件的同态与 φ 复合后都等于 ψ，故它也等于 $\psi \circ \varphi^{-1}$。因此 $\varphi(u_i)$ 满足自由模的泛性质。 □

我们也可以从另一个角度来理解自由模的“最大”或“自由”。在用若干元素生成代数结构时，我们往往会关心生成元之间的关系，也就是是否存在非平凡的线性关系。如果生成元之间已经有一条关系，那么指定它们的像时也必须保持这条关系，因而不能任意指定；而泛性质恰好允许我们任意指定基向量的像。因此，自由模的这组基向量之间没有任何非平凡关系的束缚，这也是它被称为“自由模”的原因。下面将这一理解写成线性无关的严格刻画。[1]

定理 1.2.3 (泛性质与基的等价刻画)**.** 设 $u_1, \dots, u_n \in M$。它们满足定义 1.2.1中的泛性质，当且仅当它们生成 M 且 R-线性无关，即

$$\sum_{i=1}^{n} a_i u_i = 0 \quad \Longrightarrow \quad a_1 = \cdots = a_n = 0.$$

等价地，每个 $x \in M$ 都能唯一写成 $x = \sum_i a_i u_i$。

证明. 先设泛性质成立，令 $L = \sum_i Ru_i$。自然映射 $M \to M/L$ 与零映射都把每个 u_i 送到零；由唯一性它们相等，因此 $M = L$。再将 u_i 指定映到 R^n 的第 i 个标准基向量 e_i。若 $\sum_i a_i u_i = 0$，应用所得模同态即得 $\sum_i a_i e_i = 0$，故每个 $a_i = 0$。

反之，若每个 x 具有唯一表达式 $x = \sum_i a_i u_i$，对任意指定的 $v_i \in N$，定义 $\varphi(x) = \sum_i a_i v_i$。唯一表达式保证良定义，并直接保证加法与纯量乘法相容；任何满足要求的同态都必须取此值，故它唯一。 □

于是，自由模的研究可以归结为标准模 R^n。

定理 1.2.4 (自由模的结构)**.** 一个 R-模 M 有一组含 n 个元素的基，当且仅当 $M \cong R^n$。

证明. 若 $u_1, \dots, u_n$ 为一组基，则

$$\varphi : R^n \to M, \qquad (a_1, \dots, a_n) \mapsto \sum_i a_i u_i$$

由生成性为满射，由线性无关性为单射，因而是模同构。反之，将 R^n 的标准基经同构送到 M，由定理 1.2.3即可得到 M 的一组基。 □

推论 1.2.5 (自由模的有限直和)**.** 若 M, N 分别有含 m, n 个元素的基，则 $M \oplus N$ 有一组含 $m + n$ 个元素的基。

[1] 进一步研究生成元之间的关系，可以引出 syzygy 模与自由消解；本章用同态的核记录这些关系，不展开这些旁支概念。

证明. 将 M 与 N 的基分别嵌入直和的两个分量，由定理 1.2.3即得一组基；也可直接用 $M \oplus N \cong R^m \oplus R^n \cong R^{m+n}$。 □

需要注意的是，我们目前还不知道一个自由模的基所含元素的个数是否唯一，因此还不能直接把这个数看作模的不变量。事实上，一般非交换幺环上的同一个自由模确实可能有大小不同的基。不过，后面我们会看到，若 R 是非零交换幺环，就可以保证有限基的大小唯一，届时才把它定义为这个自由模的秩。

1.2.2 自由模之间的同态

由定理 1.2.4可以看出，对自由模的讨论可以归结为对 R^n 的讨论。而研究 R^m 与 R^n 之间的同态时，我们又可以试着用矩阵来表示同态：选定两组基，把定义域的每个基向量的像在陪域的基下展开，再将这些系数排成矩阵。这样，对自由模之间同态的讨论就进一步归结为对环上矩阵的讨论。

定义 1.2.6 (模同态的矩阵表示). 设 M, N 为左 R-模，分别取有序基 $\mathcal{B} = (u_1, \dots, u_m)$ 与 $\mathcal{C} = (v_1, \dots, v_n)$。对 $\varphi : M \to N$，写

$$\varphi(u_i) = \sum_{j=1}^{n} a_{ij} v_j, \qquad A_\varphi = (a_{ij}) \in R^{m\times n}.$$

称 A_φ 为 φ 在这两组基下的**矩阵表示**。本章统一使用**行坐标**：若 $x = \sum_i x_i u_i$，则

$$[\varphi(x)]_{\mathcal{C}} = [x]_{\mathcal{B}} A_\varphi.$$

标量都写在基向量左边，因此该约定也适用于非交换环。

记矩阵表示的映射为

$$\Phi : \mathrm{Hom}_R(M, N) \longrightarrow R^{m\times n}, \qquad \varphi \longmapsto A_\varphi.$$

它与原来的同态 φ 是不同的映射。

定理 1.2.7 (矩阵表示的双射). 固定上述两组基后，Φ 是一个双射。

证明. 同态由基向量的像唯一决定，故 Φ 是单射。反之，任意矩阵 (a_{ij}) 指定 $u_i \mapsto \sum_j a_{ij} v_j$；由自由模的泛性质，这一指定唯一延拓为模同态，故 Φ 是满射。 □

但到目前为止，我们只建立了 $\mathrm{Hom}_R(M, N)$ 与 $R^{m\times n}$ 之间的一个双射，还没有考虑它们之间的代数结构是否相容。先前已经知道 $\mathrm{Hom}_R(M, N)$ 是 $\mathrm{Z}(R)$-模，所以自然可以借助这个双射，把同态的加法与纯量乘法传到矩阵空间上。任取 $\varphi, \psi \in \mathrm{Hom}_R(M, N)$ 及 $z \in \mathrm{Z}(R)$，定义

$$A_\varphi + A_\psi := A_{\varphi+\psi},$$
$$zA_\varphi := A_{z\varphi}.$$

由基向量的像展开可知，这些运算恰好就是我们熟悉的逐项运算：

$$(b_{ij}) + (c_{ij}) = (b_{ij} + c_{ij}),$$
$$z(b_{ij}) = (zb_{ij}).$$

因此，矩阵表示不仅把同态与矩阵一一对应起来，还保持加法和中心的纯量作用。

推论 1.2.8 (矩阵表示与中心作用)**.** $\Phi : \mathrm{Hom}_R(M,N) \to R^{m\times n}$ 是 $\mathrm{Z}(R)$-模同构。这里不能一般地推出它是秩为 mn 的自由 $\mathrm{Z}(R)$-模，因为 R 作为 $\mathrm{Z}(R)$-模未必自由，也未必具有秩 1。

推论 1.2.9 (交换环上的同态模)**.** 若 R 是交换幺环，则 Φ 是 R-模同构，且 $\mathrm{Hom}_R(M,N)$ 是具有 mn 个基向量的自由 R-模。

矩阵表示还要与同态的复合及基的选取相容。下面仍使用行坐标，不要求 R 交换。

命题 1.2.10 (矩阵表示的复合与换基)**.** 沿用定义 1.2.6的记号，则：

1. 设 L 是有序基为 $\mathcal{D}$ 的自由左 R-模，$\psi : N \to L$ 为模同态，则在这三组基下
$$A_{\psi\circ\varphi} = A_\varphi A_\psi.$$
2. 设 $\mathcal{B}' = (u'_1,\dots,u'_m)$、$\mathcal{C}' = (v'_1,\dots,v'_n)$ 是新基，且
$$u'_i = \sum_{j=1}^{m} p_{ij}u_j, \qquad v'_i = \sum_{j=1}^{n} q_{ij}v_j,$$
其中 $P=(p_{ij})$、$Q=(q_{ij})$ 均可逆。记 A'_φ 为新基下的矩阵，则
$$A'_\varphi = PA_\varphi Q^{-1}.$$

证明. (1) 对任意 $x \in M$，行坐标满足
$$[\psi(\varphi(x))]_{\mathcal{D}} = [\varphi(x)]_{\mathcal{C}} A_\psi = [x]_{\mathcal{B}} A_\varphi A_\psi,$$
故复合的矩阵为 $A_\varphi A_\psi$。

(2) 新基向量在旧基下的坐标分别是 P, Q 的各行，因而
$$[x]_{\mathcal{B}} = [x]_{\mathcal{B}'}P, \qquad [y]_{\mathcal{C}} = [y]_{\mathcal{C}'}Q.$$
取 $y=\varphi(x)$，代入 $[y]_{\mathcal{C}} = [x]_{\mathcal{B}}A_\varphi$ 并右乘 Q^{-1}，得到
$$[\varphi(x)]_{\mathcal{C}'} = [x]_{\mathcal{B}'}PA_\varphi Q^{-1}.$$
由矩阵表示的唯一性得所述公式。这里没有交换任何乘积因子的顺序。 □

因此，左乘可逆矩阵改变定义域的基；右乘可逆矩阵 Q 时，陪域的基按 Q^{-1} 变换。后面将用这一对应解释 Smith 标准型如何简化生成元之间的关系。

1.2.3 交换幺环上的矩阵

上一节中我们已经知道，对自由模间同态的讨论可以归结为对环上矩阵的讨论。这一节转而研究交换幺环上的矩阵，看看高等代数中熟悉的哪些性质仍然成立。本小节假设 R 是非零交换幺环。行列式的基本恒等式仍然成立，但不能把域上的结论全部照搬过来；特别是矩阵可逆的条件必须用“行列式是单位”，不能仅用“行列式非零”。

定义 1.2.11 (行列式). 对 $A=(a_{ij})\in R^{n\times n}$，定义

$$\det A=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)a_{1\sigma(1)}\cdots a_{n\sigma(n)}.$$

约定 0×0 矩阵的行列式为 1。

交换幺环上矩阵的行列式的性质与域上矩阵的行列式的性质基本一致，如交换两行（列）符号变号，某一行（列）加到另一行（列）上不改变行列式的值，可用代数余子式按行（列）展开，矩阵相乘的行列式等于矩阵的行列式相乘，等等。

利用矩阵表示与行列式的性质，我们现在可以回到先前留下的问题：同一个自由模的两组有限基，所含元素的个数是否一定相同？下面先借助极大理想把这个问题化为域上线性空间的维数问题，再给出用补零方阵和行列式得到矛盾的另一条证明路线。

定理 1.2.12 (交换幺环上自由模的秩唯一). 设 R 是非零交换幺环。若 $R^m\cong R^n$，则 $m=n$。因此有限生成自由 R-模的基的大小唯一。

证明. 取 R 的一个极大理想 $\mathfrak{m}$。模同构将 $\mathfrak{m}R^m$ 映到 $\mathfrak{m}R^n$，因而诱导

$$R^m/\mathfrak{m}R^m\cong R^n/\mathfrak{m}R^n.$$

这是域 $R/\mathfrak{m}$ 上的线性空间同构，即 $(R/\mathfrak{m})^m\cong(R/\mathfrak{m})^n$，由维数唯一性得 $m=n$。 □

另一证明（行列式方法）. 用行坐标表示同构及其逆，得到 $A\in R^{m\times n}$ 与 $B\in R^{n\times m}$，满足 $AB=I_m$、$BA=I_n$。若 $m<n$，在 A 下方补零行，在 B 右侧补零列，得到两个 n 阶方阵

$$\widetilde{A}=\begin{pmatrix}A\\0\end{pmatrix},\qquad \widetilde{B}=\begin{pmatrix}B & 0\end{pmatrix}.$$

它们满足 $\widetilde{B}\widetilde{A}=BA=I_n$，但 $\widetilde{A}$ 有零行，所以

$$0=\det\widetilde{B}\,\det\widetilde{A}=\det(\widetilde{B}\widetilde{A})=\det I_n=1,$$

与 R 非零矛盾。故 $m\geq n$；交换 m,n 同理得 $n\geq m$，于是 $m=n$。 □

定义 1.2.13 (有限生成自由模的秩). 设 R 是非零交换幺环，M 是有限生成自由 R-模。称任意一组基所含的元素个数为 M 的**秩**，记为 $\operatorname{rank}M$。定理 1.2.12保证它与基的选择无关；零模的秩为零。

推论 1.2.14 (标准自由模的同构判定). 对非零交换幺环 R，有 $R^m\cong R^n$ 当且仅当 $m=n$。

类似域上矩阵，可以定义代数余子式与伴随矩阵。

定义 1.2.15 (余子式与代数余子式). 任取方阵 $A\in R^{n\times n}$，则去掉第 i 行和第 j 列后得到的 $(n-1)$ 阶方阵的行列式 M_{ij} 定义为 a_{ij} 的**余子式**，$A_{ij}:=(-1)^{i+j}M_{ij}$ 为 a_{ij} 的**代数余子式**。

完全类似域上矩阵的情形，矩阵的行列式可以利用代数余子式进行行（列）展开。

定理 1.2.16 (代数余子式恒等式)**.** 沿用上述记号，对任意 $1 \le i, k \le n$，有

$$\sum_{j=1}^{n} a_{ij} A_{kj} = \delta_{ik} \det A, \qquad \sum_{j=1}^{n} a_{ji} A_{jk} = \delta_{ik} \det A,$$

其中 $\delta_{ik} = 1 \ (i = k)$，$\delta_{ik} = 0 \ (i \neq k)$。

证明. 当 $i = k$ 时，两式分别是按第 i 行及第 i 列的行列式展开。当 $i \neq k$ 时，将第 k 行替换为第 i 行，新矩阵有两行相同，故行列式为零；按替换后的第 k 行展开，其余子式不变，得到第一式。对列作同样的替换与展开，得到第二式。 □

定义 1.2.17 (伴随矩阵)**.** 沿用定义中代数余子式 A_{ij} 的记号，定义 A 的**伴随矩阵**为

$$A^* = (A_{ji})_{1 \le i,j \le n}.$$

即先组成代数余子式矩阵，再取转置。

由定理 1.2.16，易得如下结论。

定理 1.2.18 (伴随矩阵恒等式)**.** 沿用上述记号，有：

$$AA^* = A^*A = (\det A) I_n.$$

证明. 乘积 AA^* 的第 (i, k) 项为 $\sum_j a_{ij} A_{kj}$，由定理 1.2.16等于 $\delta_{ik} \det A$。对 A^*A 同理。 □

定义 1.2.19 (可逆矩阵)**.** 考虑 $R^{n \times n}$ 上的环结构，其中的可逆元称为**可逆矩阵**。

利用定理 1.2.18，可逆矩阵有如下性质。

推论 1.2.20 (可逆矩阵的行列式判定)**.** 沿用上述记号，有：

1. A 可逆当且仅当 $\det A$ 为 R 中单位;
2. 若 A 可逆，则 $A^{-1} = (\det A)^{-1} A^*$.

证明. 若 A 可逆,则 $\det A \det A^{-1} = 1$,故 $\det A$ 是单位。若 $\det A$ 是单位,由定理 1.2.18可知 $(\det A)^{-1} A^*$ 是 A 的双侧逆。 □

1.2.4 PID 上矩阵的标准型

以下将环的条件加强为主理想整环 D。我们的目标是通过可逆的行、列变换，将任意矩阵化为标准型。后面将把矩阵的列、行看作生成元与关系的坐标，用这种标准型简化模的结构。

定义 1.2.21 (等价矩阵)**.** 设 D 是主理想整环，则称 D 上的两个同型的 $m \times n$ 矩阵 A, B 是**等价**的，若存在可逆矩阵 $P \in D^{m \times m}$，$Q \in D^{n \times n}$，使得：$A = PBQ$.

域上的矩阵都等价于非零对角元全为 1 的标准型。在一般主理想整环上，这一结论未必成立；非零对角元还可能是非单位。下面用满足整除链的对角元给出相应的标准型。

定理 1.2.22 (PID 上矩阵的标准型)**.** 设 D 是主理想整环，$A \in D^{m\times n}$。存在可逆矩阵 P, Q 使得 PAQ 为 $m \times n$ 对角形矩阵，非零对角元为

$$d_1, \dots, d_r, \qquad d_i \mid d_{i+1} \quad (1 \le i < r),$$

其余元素全为零。其中 $r \le \min\{m, n\}$。这称为 A 的 **Smith 标准型**。

证明. 思路是先把一个非零元素移到左上角，再利用最大公因子使它整除全部矩阵元素，最后对剩余子矩阵归纳。关键在于：当左上角元素不能整除所选元素时，取最大公因子会使它生成的主理想严格增大，因此可用理想升链的稳定性证明过程终止。

若 $A = 0$，结论显然。否则将一个非零元素移到左上角，记为 a。若第一列某个元素 b 不被 a 整除，取 $g = \gcd(a, b)$ 及 $u, v \in D$ 满足 $ua + vb = g$。用可逆的两行变换

$$\begin{pmatrix} u & v \\ -b/g & a/g \end{pmatrix}, \qquad \det \begin{pmatrix} u & v \\ -b/g & a/g \end{pmatrix} = 1,$$

可把这两个位置的元素 $(a, b)^{\mathsf{T}}$ 化为 $(g, 0)^{\mathsf{T}}$。此时 $(a) \subsetneq (g)$。对第一行中不被 a 整除的元素，作对应的列变换。

当第一行、第一列的元素都被 a 整除时，用减去倍数的方法消去其余元素，得到

$$\begin{pmatrix} a & 0 \\ 0 & B \end{pmatrix}.$$

若 B 中存在元素 b 不被 a 整除，先将 b 所在行加到第一行，使第一行出现 b，再用上述列变换将左上角元素改为 $\gcd(a, b)$；其生成的理想又严格增大，然后重新消去第一行与第一列。

这个过程必定终止。事实上，PID 中任意理想升链稳定：升链的并仍是理想，设其生成元为 c；c 属于升链中的某一项，则此项已经等于整个并。因此，不可能有无限多个严格增大的左上角元素理想。终止时 a 整除 B 的每个元素。对 B 按较小的矩阵大小归纳，得到满足整除链的对角元；归纳中的行、列变换仍保持各元素为 a 的倍数，故 a 整除下一个非零对角元，结论成立。 □

借助对行列式因子的讨论，我们可以得到标准型在相伴意义下的唯一性。

定义 1.2.23 (子矩阵与子式)**.** 任取矩阵 A，考虑其中的行 $i_1 < i_2 < \cdots < i_k$，以及列 $j_1 < j_2 < \cdots < j_l$，这些行列相交位置的元素构成一个新的 $k \times l$ 矩阵，称为 A 的一个**子矩阵**。将任意一个 $k \times k$ 子矩阵的行列式称为 A 的一个 k **阶子式**，若其由行 $i_1 < i_2 < \cdots < i_k$，列 $j_1 < j_2 < \cdots < j_k$ 相交位置的元素构成，则将其记为：

$$A \begin{pmatrix} i_1 & \cdots & i_k \\ j_1 & \cdots & j_k \end{pmatrix}.$$

定义 1.2.24 (矩阵的秩)**.** 设 $A \in D^{m\times n}$。若 $A = 0$，定义 $\operatorname{rank}(A) = 0$；否则定义 $\operatorname{rank}(A)$ 为存在非零子式的最大阶数。等价地，它是将 A 视为分式域 $\operatorname{Frac}(D)$ 上的矩阵时的秩。

定义 1.2.25 (行列式因子). 对 $A \in D^{m\times n}$ 及 $1 \le k \le \min\{m,n\}$，定义所有 k 阶子式的最大公因子为 A 的 k **阶行列式因子** $\Delta_k(A)$，它在相伴意义下确定。约定 $\Delta_0(A) = 1$；当所有 k 阶子式均为零时，约定 $\Delta_k(A) = 0$。

类似域上矩阵的情形，两个等价矩阵的秩与行列式因子在一定意义下相等。

定理 1.2.26 (等价变换保持秩与行列式因子). 任取两个等价矩阵 A, B，则：

1. $\operatorname{rank}(A) = \operatorname{rank}(B)$;
2. $\Delta_k(A) \sim \Delta_k(B)$，这里的 $\sim$ 表示相伴。

证明. 先考虑 $B = PA$。B 的每一行都是 A 各行的 D-线性组合。对任意 k 阶子式按行列式的多重线性展开，含有重复行的项为零；其余各项是 A 的某个 k 阶子式乘以 D 中的一个系数。因此 $\Delta_k(A)$ 整除 $\Delta_k(B)$。对右乘 Q 作相同的列展开，结论仍成立。再利用 $A = P^{-1}BQ^{-1}$ 得到反方向的整除，故行列式因子相伴。各阶子式是否全为零也保持不变，所以秩相等。 □

最后由上述讨论可得 PID 上矩阵标准型的唯一性。

定理 1.2.27 (标准型的唯一性). 设 A 的 Smith 标准型的非零对角元为 $d_1, \dots, d_r$，且 $d_i \mid d_{i+1}$。则 $r = \operatorname{rank}(A)$，并且

$$\Delta_i(A) \sim d_1 \cdots d_i, \qquad d_i \sim \frac{\Delta_i(A)}{\Delta_{i-1}(A)} \quad (1 \le i \le r).$$

因此标准型在各对角元相伴的意义下唯一。

证明. 由定理 1.2.26，只需计算标准型的子式。其非零 i 阶子式是 i 个不同非零对角元的乘积。若所选指标为 $j_1 < \cdots < j_i$，则 $j_k \ge k$，由整除链知 $d_1 \cdots d_i$ 整除 $d_{j_1} \cdots d_{j_i}$；而选前 i 个对角元时，子式正好是 $d_1 \cdots d_i$。故最大公因子与此乘积相伴，进而得到商的公式及唯一性。 □

定义 1.2.28 (矩阵的不变因子). 设 A 是 PID D 上的矩阵。称其 Smith 标准型中按整除链排列的非零对角元 $d_1, \dots, d_r$ 为 A 的**不变因子**。它们允许为单位，并由定理 1.2.27在相伴意义下唯一确定；$A = 0$ 时序列为空。

例 1.2.29 (对角矩阵的整除链调整). 取 $A = \operatorname{diag}(2, 3)$。虽然它已经是对角矩阵，但 $2 \nmid 3$，还未满足 Smith 标准型的整除链。记 R_i, C_i 分别为第 i 行、第 i 列，作如下

可逆的整数行、列变换：

$$\begin{pmatrix}2&0\\0&3\end{pmatrix}\xrightarrow{R_1\leftarrow R_1+R_2}\begin{pmatrix}2&3\\0&3\end{pmatrix}\xrightarrow{C_2\leftarrow C_2-C_1}\begin{pmatrix}2&1\\0&3\end{pmatrix}$$
$$\xrightarrow{C_1\leftrightarrow C_2}\begin{pmatrix}1&2\\3&0\end{pmatrix}\xrightarrow{R_2\leftarrow R_2-3R_1}\begin{pmatrix}1&2\\0&-6\end{pmatrix}$$
$$\xrightarrow{C_2\leftarrow C_2-2C_1}\begin{pmatrix}1&0\\0&-6\end{pmatrix}\xrightarrow{R_2\leftarrow -R_2}\begin{pmatrix}1&0\\0&6\end{pmatrix}.$$

因此标准型为 $\mathrm{diag}(1,6)$。也可用定理 1.2.27核对：$\Delta_1(A)=\gcd(2,3)=1$、$\Delta_2(A)=6$，故不变因子为 $1,6$。这里第一因子由最大公因子决定，不能直接把原来的 $2,3$ 作为不变因子。

例 1.2.30 (贯穿例子：整数矩阵的标准型)**.** 取

$$A=\begin{pmatrix}2&4&0\\0&6&0\\0&0&0\end{pmatrix}.$$

将第二列减去第一列的两倍，得到 $\mathrm{diag}(2,6,0)$。因此 $\mathrm{rank}(A)=2$，$\Delta_1=2$、$\Delta_2=12$，不变因子为 $2,6$。下一节将用同一个矩阵描述一个模的关系，再解释这些数决定了怎样的商模。

1.3 有限生成模

1.3.1 生成元与关系

有限生成模已在定义 1.1.13中引入。以下先说明如何用自由模中的一个子模记录生成元之间的全部关系，再利用 PID 的性质简化这些关系。

先前在说明自由模的结构时，设 M 的一组基为 $x_1,\dots,x_n$，我们利用了这样一个满同态：

$$\varphi:R^n\to M,\qquad (a_1,\dots,a_n)\mapsto\sum_i a_ix_i.$$

由于基向量线性无关，这时 $\ker\varphi=0$，所以 $M\cong R^n/\ker\varphi=R^n$。而对于任何有限生成模 M，只要选定一组生成元 $x_1,\dots,x_n$，我们都可以做完全相同的事情。区别在于，这组生成元未必线性无关，因而核可能不再为零。我们先保留这个核，再用模同态基本定理描述 M。

定理 1.3.1 (有限生成模的结构)**.** 对任意一个有限生成模 M，其一组生成元为 $\{x_1,x_2,\dots,x_n\}$，则其同构于一个自由模商去一个子模：

$$M\cong R^n/K,$$

其中子模 K 为满同态：

$$\varphi : R^n \longrightarrow M$$
$$(a_1, \ldots, a_n) \longmapsto a_1x_1 + \cdots + a_nx_n.$$

的核 $\ker\varphi = \{(a_1, \ldots, a_n) \in R^n : \sum_{k=1}^{n} a_kx_k = 0\}$.

证明. 对上述满同态应用定理 1.1.19即可。 □

由上述定理，自由模 R^n 的结构是确定的，所以在选定生成元后，M 的结构就由关系子模 $K = \ker\varphi$ 决定。注意到，一个系数向量 $(a_1, \ldots, a_n)$ 属于核，恰好意味着

$$a_1x_1 + \cdots + a_nx_n = 0.$$

所以 K 不是随意引入的子模，而是包含了这组生成元之间全部 R-线性关系的集合。由此可以看出，**生成元以及生成元之间的全部关系决定了一个有限生成模的结构**。

我们也可以在这里再一次体会自由模的“自由性”：当所选生成元是一组基时，它们之间没有非平凡关系，所以 $K = 0$；若这组生成元有非平凡关系，就需要将这些关系商掉，才能得到 M。这里要区分“模是自由的”与“所选生成元是一组基”。即使 M 本身自由，也可以选取有关系的生成元，例如 $\mathbb{Z}$ 由 $2, 3$ 生成，但有 $3 \cdot 2 - 2 \cdot 3 = 0$，相应的 $\mathbb{Z}^2 \to \mathbb{Z}$ 的核并不为零。因此，不能把“核不为零”直接等同于“模不自由”；它首先说明的是所选生成元之间有关系。

1.3.2 PID 上的有限生成模

这一小节将环的条件加强为主理想整环 D，研究其上有限生成模的结构。首先，在先前我们已经看到，一个有限生成模必定同构于一个自由模商去一个子模。具体地，若 M 由 $x_1, \ldots, x_n$ 生成，则由定理 1.3.1有 $M \cong D^n/K$。由此看出，要搞清楚 M 的结构，首先要搞清楚自由模 D^n 的子模 K 的结构。如果 K 也有有限基，我们就能用一个有限矩阵记录这些关系，再试着通过变换基把它们简化。这说明为什么下面首先研究自由模的子模。

定理 1.3.2 (PID 上自由模子模的结构). 设 $K \subseteq D^n$ 为子模，其中 D 是主理想整环。则 K 为有限生成自由模，且 $\operatorname{rank} K \leq n$。

证明. 对 n 归纳。$n = 0$ 时显然。$n = 1$ 时，K 是 D 的理想，故 $K = Dd$；若 $d \neq 0$，则 $a \mapsto ad$ 是 $D \to K$ 的同构，否则 $K = 0$。

设 $n \geq 2$，取第一坐标投影 $\pi : D^n \to D$。若 $\pi(K) = 0$，则 $K \subseteq \ker\pi \cong D^{n-1}$，由归纳假设得结论。若 $\pi(K) = Dd$ 且 $d \neq 0$，取 $v \in K$ 满足 $\pi(v) = d$，并令 $K_0 = K \cap \ker\pi$。每个 $x \in K$ 满足 $\pi(x) = ad$，于是 $x - av \in K_0$，故 $K = Dv + K_0$。若 $av \in K_0$，投影后有 $ad = 0$；由于 D 为整环且 $d \neq 0$，必有 $a = 0$。因此

$$K = Dv \oplus K_0.$$

其中 $Dv \cong D$，而 K_0 由归纳假设是秩不超过 $n - 1$ 的自由模，故 K 是秩不超过 n 的自由模。 □

引理 1.3.3 (直和的商)**.** 设 M_1, M_2 为 M 的子模，且 $M_1 + M_2 = M_1 \oplus M_2$，$N_1 \subseteq M_1$ 与 $N_2 \subseteq M_2$ 为子模，则有：

$$(M_1 \oplus M_2)/(N_1 \oplus N_2) \cong (M_1/N_1) \oplus (M_2/N_2).$$

证明. 定义满模同态

$$M_1 \oplus M_2 \longrightarrow (M_1/N_1) \oplus (M_2/N_2), \qquad m_1 + m_2 \longmapsto (m_1 + N_1, m_2 + N_2).$$

内直和保证 m_1, m_2 唯一，因此映射良定义；其核为 $N_1 \oplus N_2$。应用定理 1.1.19即可。有限多个直和项的情形同理。 □

我们已经知道 $M \cong D^n/K$，而 K 也是自由模。分别写出两组基后，有

$$D^n = Du_1 \oplus \cdots \oplus Du_n, \qquad K = Dv_1 \oplus \cdots \oplus Dv_m, \qquad m \le n.$$

我们希望借助引理 1.3.3，把商模逐项拆开来研究。但任意选出的两组基之间未必有 $Dv_i \subseteq Du_i$，所以此时还不能直接写出 Du_i/Dv_i。那么接下来可以做的事情，就是在 D^n 与 K 中找到两组合适的基，使每个 v_i 只涉及对应的一个 u_i，也就是 $v_i = d_i u_i$。如果能做到这一点，我们就得到

$$D^n/K \cong \bigoplus_{i=1}^{m} Du_i/D(d_i u_i) \oplus \bigoplus_{j=m+1}^{n} Du_j,$$

原来混在一起的关系便分别只约束一个生成元。上一节的矩阵标准型正是帮助我们找出这种基的工具，下面把这个思路写成定理。

定理 1.3.4 (与子模相适配的基)**.** 设 $K \subseteq D^n$ 为子模，$\operatorname{rank} K = m$。存在 D^n 的一组基 $u_1, \dots, u_n$ 及 K 的一组基 $v_1, \dots, v_m$，使得

$$v_i = d_i u_i \quad (1 \le i \le m), \qquad 0 \ne d_i \in D, \quad d_i \mid d_{i+1} \quad (1 \le i < m).$$

证明. 由定理 1.3.2, K 有含 $m \le n$ 个元素的基。取 K 与 D^n 的任意基，嵌入 $\iota : K \to D^n$ 的行坐标矩阵为 $m \times n$ 矩阵 A。由定理 1.2.22，取可逆矩阵 P, Q 使 PAQ 为 Smith 标准型。按命题 1.2.10，将定义域的基按 P 变换，将陪域的基按 Q^{-1} 变换，新矩阵恰为 PAQ。这个标准型必须有 m 个非零对角元：否则某个定义域基向量映为零，与 ι 是单射矛盾。因此新基满足 $v_i = d_i u_i$，且 d_i 满足整除链。 □

为了将 PID 上有限生成模的结构叙述更清楚，还需要引入模中元素的**零化子**的概念。

定义 1.3.5 (零化子，扭元与扭模)**.** 设 M 是交换幺环 R 上的模，对 $x \in M$ 定义其**零化子**

$$\operatorname{ann}(x) = \{a \in R : ax = 0\},$$

这是 R 的理想。以下关于扭元的讨论假设 R 是**整环**。若存在 $0 \neq a \in R$ 使得 $ax = 0$，称 x 为**扭元**；零元也属于扭元。定义

$$\operatorname{Tor}(M) = \{x \in M : \exists 0 \neq a \in R,\ ax = 0\}.$$

若 $\operatorname{Tor}(M) = 0$，称 M 为**无扭模**；若 $\operatorname{Tor}(M) = M$，称 M 为**扭模**。非零元素 x 满足 $\operatorname{ann}(x) = 0$ 时，也称 x 为自由元。

$\operatorname{Tor}(M)$ 是子模：若 $ax = 0$、$by = 0$ 且 $a, b \neq 0$，则 $ab(x - y) = 0$；整环条件保证 $ab \neq 0$。对 $r \in R$，有 $a(rx) = r(ax) = 0$，故它也对纯量乘法封闭。若允许零因子，上述定义未必给出子模。例如 $M = R = \mathbb{Z}/6\mathbb{Z}$ 时，$\overline{2}, \overline{3}$ 都被非零元素杀死，但它们的和 $\overline{5}$ 是单位，不被非零元素杀死。

例 1.3.6 (无扭不等于自由)**.** 整环上的自由模必为无扭模。反之一般不成立：$\mathbb{Q}$ 作为 $\mathbb{Z}$-模是无扭模，却不是自由模。若它有一组基，取其中任意基向量 b，由 $b/2 \in \mathbb{Q}$ 及基展开，等式 $b = 2(b/2)$ 将要求 b 的坐标 1 是某个整数的两倍，矛盾。

综合以上的分析，我们可以得出最终的结论，即 PID 上的有限生成模结构定理。

定理 1.3.7 (PID 上有限生成模结构定理)**.** 设 M 是主理想整环 D 上的有限生成模。则存在 $r, s \geq 0$ 及非零非单位 $d_1, \ldots, d_s$，满足 $d_i \mid d_{i+1}$，使得

$$M \cong D^r \oplus \bigoplus_{i=1}^{s} D/(d_i).$$

等价地，M 可写为有限多个非零循环子模的内直和，先列出扭循环项，再列出自由循环项，各生成元的零化子形成下降链。零模对应 $r = s = 0$。

证明. 先把关系子模的基与自由模的基适配，再逐项取商：每个关系 $d_i u_i$ 只约束对应的一个生成元，其余生成元给出自由部分。

由定理 1.3.1，写 $M \cong D^n/K$；由定理 1.3.4，可取

$$D^n = \bigoplus_{i=1}^{n} Du_i, \qquad K = \bigoplus_{i=1}^{m} D(d_i u_i), \qquad d_i \mid d_{i+1}.$$

由于 $D(d_i u_i) \subseteq Du_i$，引理 1.3.3给出

$$D^n/K \cong \bigoplus_{i=1}^{m} Du_i/D(d_i u_i) \oplus \bigoplus_{j=m+1}^{n} Du_j.$$

映射 $D \to Du_i/D(d_i u_i)$、$a \mapsto au_i + D(d_i u_i)$ 的核为 (d_i)，故该商同构于 $D/(d_i)$。当 d_i 为单位时，这一商为零，将这些项删去；剩下的非单位仍满足整除链，重编号后即得所述形式，且 $r = n - m$。将各直和项的循环生成元通过同构送入 M，便得到内直和表述。它们的零化子依次为 $(d_1) \supseteq \cdots \supseteq (d_s) \supseteq 0$，而自由循环项的零化子为零。 □

PID 上有限生成模结构定理告诉我们，一个这样的模可以写成若干循环子模的直和。我们再看这个分解中两类循环项的意义：对扭循环项 $D/(d_i)$，它的生成元 $1+(d_i)$ 满足

$$d_i\big(1+(d_i)\big)=0+(d_i).$$

因此，每个这样的循环项都是扭模；有限多个扭循环项的直和仍为扭模，因为各个 d_i 的乘积能杀死全部这些项。另一方面，剩下的 r 个循环项都同构于 D，它们的直和是自由模 D^r，秩为 r。所以，这个结构定理把 M 分成了“受非零关系约束的部分”与“没有关系约束的自由部分”。前面的构造也给出了它们的来路：生成元给出自由模，关系给出子模，标准型将关系分离为逐个生成元的关系。由此，我们定义分解中的秩与不变因子；至于这些数据是否与分解的选择无关，还需要继续证明。

定义 1.3.8 (PID 上有限生成模的秩与不变因子)**.** 设 M 有定理 1.3.7中的分解

$$M\cong D^r\oplus\bigoplus_{i=1}^{s}D/(d_i),\qquad 0\neq d_1\mid\cdots\mid d_s,$$

其中各 d_i 均非单位。称 r 为 M 的**秩**，称 $d_1,\dots,d_s$ 为 M 的**不变因子**，后者在相伴意义下考虑。它们的唯一性将在定理 1.3.21中证明。

回顾先前 PID 上矩阵的标准型，对角线上的非零元素 $d_1,\dots,d_r$ 被称为矩阵的不变因子；这里我们又定义了模的不变因子。为什么两种不同的对象使用了同一个名称？它们的联系就在于：矩阵可以记录一个模的生成元之间的关系，而矩阵的标准型把这些关系逐个分离。下面先用已经算过的矩阵观察这个联系，再从两个方向说明一般情形。

例 1.3.9 (贯穿例子：从矩阵到商模)**.** 继续例 1.2.30。使用行坐标，把 A 看作同态 $\mathbb{Z}^3\to\mathbb{Z}^3$、$x\mapsto xA$ 的矩阵。其像为

$$K=\mathbb{Z}(2,4,0)+\mathbb{Z}(0,6,0).$$

定义 $M=\mathbb{Z}^3/K$。前面的列变换对应陪域的基变换，将 K 变为由 $(2,0,0)$ 与 $(0,6,0)$ 生成的子模，故

$$M\cong\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}.$$

因此 M 的秩为 1，不变因子为 $2,6$。

一方面，任给 PID 上的有限生成模 $M\cong D^n/K$，关系子模 K 由定理 1.3.2有有限基。考虑嵌入映射 $\iota:K\to D^n$ 的矩阵；按照定理 1.3.4的过程，将它化为 Smith 标准型，便得到 $v_i=d_iu_i$ 这样的逐项关系。因此，这个关系矩阵的非零不变因子中，*删去单位后*剩下的因子，正是模的不变因子。单位关系把一个生成元全部商掉，不留下非零循环项；这一点也解释了为什么矩阵的不变因子允许为单位，而模的不变因子在规范分解中不允许为单位。

另一方面，任给一个 PID 上的矩阵 $A\in D^{m\times n}$，使用本章的行坐标约定，它确定同态

$$\varphi:D^m\longrightarrow D^n,\qquad x\longmapsto xA.$$

设 A 的 Smith 标准型有 $r = \operatorname{rank}(A)$ 个非零对角元 $d_1, \dots, d_r$。选择相应的新基 $w_1, \dots, w_m$ 与 $u_1, \dots, u_n$，同态便有

$$\varphi(w_i) = \begin{cases} d_i u_i, & 1 \le i \le r, \\ 0, & r < i \le m. \end{cases}$$

因此，其像正好是 $D(d_1u_1) \oplus \cdots \oplus D(d_ru_r)$，于是

$$\begin{aligned} D^n / \operatorname{Im}\varphi &= \left(\bigoplus_{i=1}^{n} Du_i \right) / \left(\bigoplus_{i=1}^{r} D(d_i u_i) \right) \\ &\cong \left(\bigoplus_{i=1}^{r} Du_i / D(d_i u_i) \right) \oplus \left(\bigoplus_{j=r+1}^{n} Du_j \right) \\ &\cong \left(\bigoplus_{i=1}^{r} D/(d_i) \right) \oplus D^{n-r}. \end{aligned}$$

这就由矩阵构造出了一个有限生成模，并直接读出了它的自由秩与循环关系。仍然要删去其中 d_i 为单位时对应的零商模，剩下的 d_i 才是这个模的不变因子。

推论 1.3.10 (有限生成无扭模的自由性)**.** PID 上有限生成的无扭模必为自由模。

证明. 在定理 1.3.7的分解中，每个非零 $D/(d_i)$ 都是扭模。若 M 无扭，这些项均不能出现，因此 $M \cong D^r$，为自由模。 □

上述推论中主理想整环与有限生成的条件均不能直接删去。

例 1.3.11 (删去有限生成或 PID 条件的反例)**.** 两个条件都不能直接删去。

1. $R = \mathbb{Z}[x]$ 的理想 $I = (2, x)$ 是有限生成无扭 R-模，却不是自由模。若它自由，任意两个非零元素 $a, b \in I$ 都有关系 $ba - ab = 0$，故基至多有一个元素，从而 I 必须是主理想。若 $I = (f)$，则 $f \mid 2$ 且 $f \mid x$，迫使 f 为单位，然而 I 是真理想：代入 $x = 0$ 再模 2 的同态将 I 送到零。因此矛盾。

2. $\mathbb{Q}$ 作为 $\mathbb{Z}$-模无扭，但不有限生成，也不自由。有限个有理数的整数线性组合，其分母均被某个固定正整数整除，不能得到全部有理数；不自由性见例 1.3.6。

1.3.3 PID 上的有限生成扭模

上一小节中我们已经知道 PID 上有限生成模的结构，现在希望进一步证明这种结构在适当意义下是唯一的。具体地，我们想证明自由部分的秩与不变因子序列都是由模本身决定的，其中因子在相伴意义下考虑。这一小节先通过研究有限生成扭模来确定因子数据的唯一性，最后再处理自由部分的秩，从而完成整个结构定理的唯一性证明。

有限维线性空间作为特殊的 PID 上有限生成模具有许多良好的结构性质，于是证明上述唯一性的大体思路就是将模上的问题转化到线性空间上来讨论。注意到以下观察可以帮助我们将一般 PID 上的模转化为域上的线性空间。

命题 1.3.12 (被不可约元杀死的模与线性空间)**.** 设 N 为一个 D-模，D 是主理想整环，且存在 $p \in D$，对任意 $u \in N$ 满足：

$$pu = 0,$$

则 N 可以成为一个 $D/(p)$-模，而若 p 是 D 中的不可约元素，其生成的理想 (p) 为一个极大理想，故 $D/(p)$ 是一个域，于是 N 成为一个域 $D/(p)$ 上的线性空间。

证明. 对 $\overline{a} \in D/(p)$ 及 $u \in N$，定义 $\overline{a}\,u = au$。若 $a - b \in (p)$，则 $(a-b)u = 0$，故作用良定义。若 p 不可约，PID 中 (p) 是极大理想，因此 $D/(p)$ 是域，N 即为其上的线性空间。 □

通过上述观察可以看出，我们接下来要做的事情就是把 M 分解为一列零化子是由 p 或 p^k 生成的循环模，其中 p 是 D 中的不可约元素。借助下面的引理可以帮助我们进行上述分解。

引理 1.3.13 (互素零化子的分解)**.** 设 D 为主理想整环，$u \in M$ 满足 $\operatorname{ann}(u) = (ab)$，其中 $a, b \neq 0$ 且互素。则存在 $u_1, u_2 \in Du$ 使得

$$Du = Du_1 \oplus Du_2, \qquad \operatorname{ann}(u_1) = (a), \quad \operatorname{ann}(u_2) = (b).$$

证明. 取 $r, s \in D$ 满足 $ra + sb = 1$，令 $u_1 = sbu$、$u_2 = rau$，则 $u = u_1 + u_2$。显然 $au_1 = 0$。若 $cu_1 = 0$，则 $ab \mid csb$，消去 $b \neq 0$ 得到 $a \mid cs$。由 $sb \equiv 1 \pmod{a}$ 知 s 在 $D/(a)$ 中可逆，故 $a \mid c$；因此 $\operatorname{ann}(u_1) = (a)$。对 u_2 同理。若 $x \in Du_1 \cap Du_2$，则 $ax = bx = 0$，从而 $x = (ra + sb)x = 0$，所以和为直和。 □

对任意非零非单位 $d \in D$，在相伴意义下写 $d \sim p_1^{k_1} \cdots p_m^{k_m}$，其中 p_i 互不相伴且不可约，$k_i \geq 1$。反复使用引理 1.3.13，可将零化子为 (d) 的循环模分解为零化子分别为 $(p_i^{k_i})$ 的循环模的直和。

推论 1.3.14 (循环扭模的素幂分解)**.** 设 $\operatorname{ann}(u) = (d)$，其中 $d \neq 0$ 且非单位。在相伴意义下写

$$d \sim p_1^{k_1} \cdots p_m^{k_m},$$

其中 p_i 互不相伴且不可约，$k_i \geq 1$。则 $Du = \bigoplus_{i=1}^{m} Du_i$，其中 $\operatorname{ann}(u_i) = (p_i^{k_i})$。

证明. 不同不可约元的幂互素，对引理 1.3.13按因子个数归纳即可。 □

下面定义 p-分支与 p-模。

定义 1.3.15 (p 分支与 p-模)**.** 设 M 为 PID D 上的有限生成扭模，$p \in D$ 为不可约元素。定义它的 **p-分支**

$$M_p = \{x \in M : \exists k \geq 0,\ p^k x = 0\}.$$

若 $M = M_p$，称 M 为 **p-模**。相伴的不可约元给出相同的分支。

容易验证下述关于 p-分支的性质。

定理 1.3.16 (分支的基本性质)**.** 对上述 M 及不可约元 p，有：

1. M_p 是子模，且 $u \in M_p$ 当且仅当 $\operatorname{ann}(u) = (p^k)$ 对某个 $k \geq 0$ 成立；$k = 0$ 恰对应 $u = 0$；
2. 若 p, q 互不相伴且不可约，则 $M_p \cap M_q = 0$。

证明. 若 $p^a x = 0$、$p^b y = 0$，取 $k = \max\{a, b\}$ 即可得到 $p^k(x - y) = 0$；标量倍也被相同的幂杀死，故 M_p 是子模。若 $u \neq 0$ 且 $p^k u = 0$，写 $\operatorname{ann}(u) = (d)$，则 $d \mid p^k$，因此 d 与某个 p^j 相伴，反方向显然。对 $u = 0$，零化子为 $D = (1)$。若 $x \in M_p \cap M_q$，则 $p^a x = q^b x = 0$。由于 p^a, q^b 互素，用 Bézout 等式即可得 $x = 0$。 □

有上述准备后，我们可以将 PID 上任意一个有限生成扭模分解为一系列 p-分支的直和。

定理 1.3.17 (PID 上有限生成扭模的 p-分支分解)**.** 设 M 为 PID 上的有限生成扭模。存在有限个互不相伴的不可约元 $p_1, \ldots, p_m$，使得

$$M = M_{p_1} \oplus \cdots \oplus M_{p_m}, \qquad M_{p_i} \neq 0.$$

其它不可约元的分支均为零。各非零分支是由 M 本身定义的子模，因此这个分解及所用不可约元的相伴类唯一。零模对应空直和。

证明. 由定理 1.3.7，M 是有限多个非零循环扭模的直和。把每个循环项的零化子分解为不可约元的幂，再反复使用引理 1.3.13，得到各项的素幂分解。合并被同一个 p_j 的幂杀死的各项，记所得子模为 N_j，则 $M = \bigoplus_j N_j$，且存在 $e_j \geq 1$ 满足 $p_j^{e_j} N_j = 0$。

证明 $N_j = M_{p_j}$。包含 $N_j \subseteq M_{p_j}$ 显然。若 $x \in M_{p_j}$，写 $x = \sum_l x_l$、$x_l \in N_l$，并取 k 使 $p_j^k x = 0$。直和性给出每个 $p_j^k x_l = 0$。当 $l \neq j$ 时，p_j^k 与 $p_l^{e_l}$ 互素，且二者都杀死 x_l，由 Bézout 等式得 $x_l = 0$。故 $x = x_j \in N_j$。相同论证表明未出现在分解中的不可约元 p 满足 $M_p = 0$。因此非零分支及对应的相伴类都由 M 内在确定。 □

上面已经证明了有限生成扭模的 p-分支分解，而各分支本身是由模内在定义的子模，因此这一步的分解是唯一的。于是，对任意一个有限生成扭模，我们只要分别确定每个 p-分支的因子数据，就能确定整个扭模的因子数据。但目前还不知道一个 p-模能否用不同的素幂指数分解成循环项，所以接下来的关键就是证明这些指数唯一。我们会再次把问题转到线性空间上来讨论。一般有限生成模还可能有自由部分，不能直接说它也完全由这些分支组成；自由秩的问题留到最后处理。

定理 1.3.18 (PID 上 p-模分解的唯一性)**.** 设 M 为有限生成 p-模，且有两种非零循环子模分解

$$M = \bigoplus_{i=1}^{s} Dy_i = \bigoplus_{j=1}^{t} Dz_j,$$

其中 $\operatorname{ann}(y_i) = (p^{m_i})$、$\operatorname{ann}(z_j) = (p^{n_j})$，且

$$1 \leq m_1 \leq \cdots \leq m_s, \qquad 1 \leq n_1 \leq \cdots \leq n_t.$$

则 $s = t$，且 $m_i = n_i$。

证明. 关键是从 M 本身构造线性空间层，使其维数记录每个素幂指数的出现次数；这样得到的数据就不依赖某次分解的选择。

由 p-模的定义，各个循环项的零化子都是 p 的幂；我们只需从模本身确定循环项的个数与这些幂的指数。取任意 $k \geq 0$，考虑 $p^k M = \{p^k x : x \in M\}$。这些都是 M 的子模，并且组成下降链

$$M \supseteq pM \supseteq p^2 M \supseteq \cdots .$$

如果取相邻两层的商 $N_k = p^k M / p^{k+1} M$，就有 $pN_k = 0$。这正好满足命题 1.3.12的条件，所以 N_k 成为域 $D/(p)$ 上的线性空间。由于 M 有限生成，N_k 也是有限维的；我们便可以利用维数不依赖基或分解的性质。把上述直和分解传到 N_k，得到

$$N_k \cong \bigoplus_i D(p^k y_i)/D(p^{k+1} y_i).$$

若 $k \geq m_i$，这一项为零；若 $k < m_i$，则映射

$$D \to D(p^k y_i)/D(p^{k+1} y_i), \quad a \mapsto a p^k y_i + D(p^{k+1} y_i)$$

的核恰为 (p)：若 $a p^k y_i = b p^{k+1} y_i$，则 $p^{m_i} \mid p^k(a - bp)$，故 $p \mid a$；反之显然。因此该项同构于 $D/(p)$，维数为 1。于是

$$c_k := \dim_{D/(p)} N_k = \#\{i : m_i > k\} = \#\{j : n_j > k\}.$$

N_k 由 M 本身定义，故这些维数不依赖分解。$c_0 = s = t$，且 $c_k - c_{k+1}$ 恰为指数等于 $k+1$ 的循环项个数，因此两个指数序列相同。 □

在证明了 PID 上 p-模关于其不变因子分解的唯一性后，考虑 PID 上有限生成扭模 M 的 p-分支分解，可以对 M 进行如下分解并定义初等因子。

定义 1.3.19 (初等因子). 设 M 为 PID 上的有限生成扭模。先作唯一的非零分支分解 $M = \bigoplus_p M_p$，再将每个 M_p 写为非零循环项的直和

$$M_p \cong \bigoplus_{i=1}^{s_p} D/(p^{k_{p,i}}), \qquad 1 \leq k_{p,1} \leq \cdots \leq k_{p,s_p}.$$

所有 $p^{k_{p,i}}$ 构成的多重集称为 M 的**初等因子**。由定理 1.3.17和 1.3.18，它在相伴意义下唯一；其中每个因子的重数也必须保留。对一般的 PID 上有限生成模，约定其初等因子为扭子模 $\mathrm{Tor}(M)$ 的初等因子。

容易看出，对于 p-模来说其初等因子就是不变因子，故对于一般的 PID 上有限生成扭模 M，考虑其 p-分支分解，将其每个 p-分支作为 p-模的不变因子收集起来就是 M 的全部初等因子。

下面的定理给出初等因子与不变因子的关系，不变因子显然可以完全决定初等因子，另一方面，初等因子也可以完全决定不变因子。

定理 1.3.20 (不变因子与初等因子的转换). PID 上有限生成扭模的不变因子序列与初等因子多重集互相决定，均在相伴意义下考虑。

证明. 给定不变因子，将各 d_i 分解为不可约元的幂，并用引理 1.3.13分解 $D/(d_i)$，即可得到初等因子。

反过来，我们只需证明初等因子可以唯一决定不变因子；下面的过程也说明怎样具体算出这些不变因子。将属于同一个不可约元相伴类的初等因子放在同一行，并按指数递增排列，得到

$$\begin{aligned} &p_1^{k_{1,1}}, \dots, p_1^{k_{1,s_1}}, \\ &p_2^{k_{2,1}}, \dots, p_2^{k_{2,s_2}}, \\ &\vdots \\ &p_t^{k_{t,1}}, \dots, p_t^{k_{t,s_t}}. \end{aligned}$$

这里 $p_1, \dots, p_t$ 互不相伴，且每行指数递增。设 $s = \max\{s_1, \dots, s_t\}$。先把每行中指数最大的那个初等因子相乘，得到最后一个不变因子

$$d_s = p_1^{k_{1,s_1}} \cdots p_t^{k_{t,s_t}}.$$

然后删去这些已经用过的初等因子，再把剩下每行中指数最大的因子相乘，得到 d_{s-1}。如果某一行已经没有剩余因子，就把这一行的贡献看作 1；不断这样进行下去，直到得到 $d_1, \dots, d_s$。

把这个过程一次写出，就是将较短的指数行在左边补零至长度 s。记补齐后的指数为 $e_{p,i}$，则

$$d_i = \prod_p p^{e_{p,i}} \quad (1 \le i \le s).$$

这说明为什么要在左边补零：最大的指数始终对应最后一个不变因子，随后由右向左取出剩余的因子。由于每行指数递增，有 $d_i \mid d_{i+1}$；某一行长度为 s，所以各 d_i 都非单位。每一列中的不同素幂互素，由引理 1.3.13可以再将 $D/(d_i)$ 拆开，恰好得到给定的全部初等因子。任何满足整除链的非单位不变因子序列，其每个 p 的正指数必须按这个次序排列且靠右放置，故它只能由上述方式得到。因此转换唯一。若 $M = 0$，两组因子均为空。 □

由此我们可以得到最终的结论。

定理 1.3.21 (PID 上有限生成模结构的唯一性)**.** 若 PID 上有限生成模 M 有两种规范分解

$$M \cong D^r \oplus \bigoplus_{i=1}^{s} D/(d_i) \cong D^{r'} \oplus \bigoplus_{j=1}^{s'} D/(d'_j),$$

其中各 d_i, d'_j 非零非单位，并分别满足整除链，则

$$r = r', \qquad s = s', \qquad d_i \sim d'_i.$$

等价地，非零循环子模内直和分解，在零化子下降链的条件下，其项数与对应的零化子唯一。

证明. 先用内在定义的扭子模分开自由部分与扭部分：商模确定自由秩，扭子模的分支及各层维数确定初等因子，再由转换定理恢复不变因子。

在任意上述分解中，自由部分无扭，循环商项均为扭模。因此 M 中全部扭元构成的内在子模 $\mathrm{Tor}(M)$ 恰对应循环商项的直和，且

$$M/\mathrm{Tor}(M) \cong D^r \cong D^{r'}.$$

由定理 1.2.12得 $r = r'$。再对 $\mathrm{Tor}(M)$ 使用定理 1.3.17、1.3.18，得到唯一的初等因子多重集；由定理 1.3.20得到 $s = s'$ 且 $d_i \sim d_i'$。这分别完成自由部分与扭部分的唯一性证明。 □

推论 1.3.22 (PID 上有限生成模的同构判定)**.** 设 M_1, M_2 是 PID 上的有限生成模，则以下命题等价：

1. $M_1 \cong M_2$；
2. M_1, M_2 有相同的秩和不变因子；
3. M_1, M_2 有相同的秩和初等因子。

证明. 模同构保持扭子模及自由商模，故由定理 1.3.21得到相同的秩与因子。反之，相同的这些数据给出相同的规范分解，因此两模同构。 □

注 (结构数据唯一与分解的选择)*.* 定理 1.3.21确定的是自由秩与因子数据；$\mathrm{Tor}(M)$ 及其非零 p-分支也是内在定义的子模，但自由补模和具体循环子模可以有不同选择。例如令 $M = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$，取

$$T = 0 \oplus \mathbb{Z}/2\mathbb{Z}, \qquad U = \mathbb{Z}(1, \overline{0}), \qquad U' = \mathbb{Z}(1, \overline{1}).$$

则 $U \neq U'$，而 $M = U \oplus T = U' \oplus T$：任意 $(a, \overline{b})$ 可写成 $a(1, \overline{1}) + (0, \overline{b} - \overline{a})$，且 U' 与 T 的交为零。两种分解的自由秩都是 1，不变因子都是 2。

例 1.3.23 (贯穿例子：初等因子与分支)**.** 例 1.3.9中的 M 满足

$$\mathrm{Tor}(M) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/3\mathbb{Z}.$$

故初等因子为 $2, 2, 3$；注意 2 出现两次。2-分支为 $(\mathbb{Z}/2\mathbb{Z})^2$，3-分支为 $\mathbb{Z}/3\mathbb{Z}$。从初等因子恢复不变因子时，两行素幂指数分别为 $(1, 1)$ 与 $(0, 1)$，逐列相乘得到 $2, 6$。自由部分 $\mathbb{Z}$ 则给出秩 1。

第二章　域

本章从域的基本性质出发，把“添加元素”与“对多项式环取商”联系起来，继而用最小多项式计算扩张次数，再逐次添加多项式的根，构造并比较分裂域。

2.1　基本概念

2.1.1　域、特征与同态

定义 2.1.1 (域). 若 F 是非零整环，且每个非零元素均可逆，则称 F 为**域**。

在环论中我们已经知道域没有非平凡理想，具体地我们有如下定理。

定理 2.1.2 (域的理想刻画). 非零交换幺环 F 是域，当且仅当它的理想只有 0 与 F。

证明. 若 F 为域且理想 I 含有 $0 \neq a$，则 $1 = a^{-1}a \in I$，故 $I = F$。反之，若 $0 \neq a \in F$，则非零理想 (a) 只能等于 F，于是存在 $b \in F$ 使 $ba = 1$，因此 a 可逆。 □

由上述定理及理想对应定理，非零交换幺环 R 对极大理想 I 取商得到域 R/I，因为商环没有非平凡理想。这是构造域的一个基本办法。

例 2.1.3 (通过构造商环得到域的例子).

1. 设 p 为素数，则 $p\mathbb{Z}$ 是 $\mathbb{Z}$ 的极大理想，故 $\mathbb{Z}/p\mathbb{Z}$ 是一个含有 p 个元素的域，记为 $\mathbb{F}_p$，这是**有限域**（亦称 Galois 域）的一个例子；
2. 考虑域 F 及整环 $F[x]$，设 $f(x) \in F[x]$ 不可约，则 $(f(x))$ 是 $F[x]$ 的一个极大理想，故 $F[x]/(f(x))$ 是一个域。

环论中对环的特征的讨论同样可以放到域中讨论。

定义 2.1.4 (域的特征). 若存在正整数 n 满足 $n1 = 0$，定义域 F 的**特征**为

$$\mathrm{Ch}(F) = \min\{n \geq 1 : n1 = 0\};$$

否则定义 $\mathrm{Ch}(F) = 0$。域的特征是**零或素数**。

证明. 若特征为正整数 n，则 $n \neq 1$。若 $n = ab$ 且 $1 < a, b < n$，则 $(a1)(b1) = n1 = 0$，但由 n 的最小性 $a1, b1$ 均非零，与域无零因子矛盾。故 n 为素数。 □

将环同态与环同构的概念在域上考虑即可得到域同态与同构的概念。

定义 2.1.5 (域同态与域同构). 设 E, F 是域，映射 $\varphi : E \to F$ 称为**域同态**，若 φ 是环同态，且 $\varphi(1_E) = 1_F$. 若域同态 φ 是双射，称 φ 为**域同构**。

可以看出，域同态相较于允许不保持幺元的环同态，多了一个“将幺元送到幺元”的要求。但对两个域之间的非零环同态，这个性质并不是额外强加的，而是自然成立的。

考虑非零环同态 $\varphi: E \to F$，任取 $\alpha \in \varphi(E)$，写 $\alpha = \varphi(\beta)$，则

$$\alpha\varphi(1_E) = \varphi(\beta 1_E) = \varphi(\beta) = \alpha,$$
$$\varphi(1_E)\alpha = \varphi(1_E\beta) = \varphi(\beta) = \alpha.$$

所以 $\varphi(1_E)$ 是像中的幺元。由于 φ 非零，可以取 $\alpha \neq 0$；在 F 中消去 α，就得到 $\varphi(1_E) = 1_F$。因此，定义中保持幺元的条件也就是明确排除了零映射。

定理 2.1.6 (域同态的单射性)**.** 域同态一定是单射。

证明. 任取域同态 $\varphi: E \to F$，它也是一个环同态，环论中我们知道 $\ker\varphi$ 是 E 的一个理想，由于 E 是域，它的理想只有 $\{0\}$ 和 E，由 $\varphi(1_E) = 1_F$ 知 $\ker\varphi \neq E$，则有：$\ker\varphi = \{0\}$，则 φ 是单射。 □

定义 2.1.7 (域同态集合与自同构群)**.** 记全体 E 到 F 的域同态构成的集合为 $\mathrm{Hom}(E, F)$。从域 E 到自身的域同态称为**自同态**，其中的双射称为**自同构**。E 的全体自同构在映射复合下组成的群称为它的**自同构群**，记为 $\mathrm{Aut}(E)$。

复合仍是域自同构，恒等映射是单位元，自同构的逆仍保持域运算，因而 $\mathrm{Aut}(E)$ 确实是群。

例 2.1.8 (Frobenius 同态)**.** 设 F 为特征 $p > 0$ 的域。映射

$$\mathrm{Fr}: F \to F, \qquad a \mapsto a^p$$

称为 **Frobenius 同态**。由特征 p 下 $(a+b)^p = a^p + b^p$，它保持加法；它也保持乘法与幺元，故为域同态。当 F 有限时，由定理 2.1.6，它是单射，从而是自同构；在 $\mathbb{F}_p$ 上它恰为恒等映射。

2.1.2 子域与素域

定义 2.1.9 (子域)**.** 设 E 是域，$F \subseteq E$ 是 E 的子集，若 F 在 E 的运算下也成为一个域，则称 F 是 E 的**子域**，E 是 F 的**扩张**，记作 E/F.

对于一般的域同态 $\varphi: E \to F$，由于 $E \cong \mathrm{Im}\,\varphi$，故我们可以把 E 看作 F 的子域，F 是 E 的扩张。

比较同一基域的两个扩张时，还要指定映射在基域上的行为。

定义 2.1.10 (基域上的同态与同构)**.** 设 E, E' 都是 F 的扩域。若域同态 $\sigma: E \to E'$ 满足 $\sigma|_F = \mathrm{id}_F$，称它为 F**-同态**；若它还是双射，称为 F**-同构**。当 $E' = E$ 时，F-同构也称为 F**-自同构**。

定理 2.1.11 (子域的交)**.** 任意一族子域的交还是子域。

证明. 在固定域 E 中，各子域都含 $0, 1$，且对加减乘及非零元素取逆封闭，因此它们的交也满足这些条件，故为子域。空族的交约定为 E。 □

类似子环的生成，我们有子域的生成。

定义 2.1.12 (子域的生成). 设 E 是域，$S \subseteq E$ 是 E 的子集，则定义由 S 生成的域为：

$$C(S) := \bigcap \{F : S \subseteq F \subseteq E \text{且} F \text{为} E \text{的子域}\}.$$

交中的域都包含 S，所以 $C(S)$ 是 E 中包含 S 的最小子域。这里允许 $S = \varnothing$；其生成的子域就是后面的素域。考虑 S 生成的含幺子环，再加入非零元素的逆，就得到这个子域。

定理 2.1.13 (生成子域与分式域). 设 $S \subseteq E$，则 $C(S)$ 是 E 中由 S 生成的含幺子环的分式域。

证明. 一方面，任意 E 中含 S 的子域包含 S 生成的子环，也就包含其分式域，故所有子域的交包含该分式域；另一方面，该分式域是 E 中包含 S 的子域，故分式域包含所有子域的交。 □

定义 2.1.14 (素域). 考虑 E 所有子域的交，这仍是一个子域，称其为 E 的**素域**，于是任意一个域都有素域作为子域，或者说任何一个域都是其素域的扩张。

定理 2.1.15 (素域的生成). 设 E 是域，其素域为 1 生成的子域 $C(1)$.

证明. 每个子域都包含 1，所以都包含由 1 生成的子域 $C(1)$。另一方面，$C(1)$ 本身也是 E 的子域，因此全部子域的交恰为 $C(1)$。 □

定理 2.1.16 (素域的结构). 任何一个域 E 的素域一定同构于 $\mathbb{F}_p$ 或 $\mathbb{Q}$。且：

1. E 的素域同构于 $\mathbb{F}_p$ 当且仅当 $\mathrm{Ch}(E) = p$；
2. E 的素域同构于 $\mathbb{Q}$ 当且仅当 $\mathrm{Ch}(E) = 0$.

证明. 当 $\mathrm{Ch}(E) = p$ 时，容易验证 1 生成的子环同构于 $\mathbb{Z}/p\mathbb{Z}$，则 1 生成的子域同构于 $\mathbb{Z}/p\mathbb{Z}$ 的分式域 $\mathbb{F}_p$；当 $\mathrm{Ch}(E) = 0$ 时，容易验证 1 生成的子环同构于 $\mathbb{Z}$，则其生成的子域同构于 $\mathbb{Z}$ 的分式域 $\mathbb{Q}$. □

定理 2.1.17 (域同态固定素域). 设 E, F 都是素域 K 的扩张，任取域同态 $\varphi : E \to F$，必有：$\varphi|_K = \mathrm{id}_K$.

证明. 由域同态满足 $\varphi(1_E) = 1_F$ 以及素域由 1 生成即得。 □

2.1.3 扩张次数与塔式公式

把扩域看成基域上的线性空间，就能用维数衡量扩张的大小，并在逐次扩张时计算总次数。

定理 2.1.18 (扩域作为线性空间). 设 E 是 F 的扩张，则 E 是 F-线性空间。

证明. 以 E 中的加法作为向量加法，以 F 与 E 中的乘法作为数乘。线性空间公理由域的运算律得到。 □

定义 2.1.19 (域的扩张次数). 设 E 为 F 的扩张，E 作为 F-线性空间的维数称为 E 对 F 的**扩张次数**，记为 $[E:F]$，若 $[E:F]<\infty$，则称 E/F 为**有限扩张**，否则称为**无限扩张**。当 E 是 F 的有限扩张，称 E 作为 F-线性空间的一组基为 E 的一组 F-基。

例 2.1.20 (二次扩张与基).

1. $\mathbb{C}$ 是 $\mathbb{R}$ 的二次扩张，且 $1, i$ 是 $\mathbb{C}$ 的一组 $\mathbb{R}$-基；
2. $\mathbb{Q}(\sqrt{2})$ 是 $\mathbb{Q}$ 的二次扩张，且 $1, \sqrt{2}$ 是 $\mathbb{Q}(\sqrt{2})$ 的一组 $\mathbb{Q}$-基；

定义 2.1.21 (中间域). 设 E/F 是域扩张。若 K 是 E 的子域且 $F \subseteq K \subseteq E$，称 K 为 E/F 的**中间域**。

定理 2.1.22 (扩张次数的塔式公式). 设 E/K，K/F 都是有限扩张，则 E/F 也是有限扩张，且有：

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

证明. 设 $u_1, \dots, u_m$ 是 E 的一组 K-基，$v_1, \dots, v_n$ 是 K 的一组 F-基。每个 $x \in E$ 可写成 $\sum_i a_i u_i$，再将每个 $a_i \in K$ 写为 $\sum_j b_{ij} v_j$，故所有 $u_i v_j$ 生成 E 作为 F-线性空间。若 $\sum_{i,j} b_{ij} u_i v_j = 0$、$b_{ij} \in F$，先利用 u_i 在 K 上线性无关，得每个 $\sum_j b_{ij} v_j = 0$；再利用 v_j 在 F 上线性无关，得全部 $b_{ij} = 0$。因此这 mn 个元素为一组 F-基，故 $[E:F] = mn$。 □

2.2 代数扩张

从生成的角度看域扩张 E/F，可以把它理解为向 F 中添加了一些元素，再用域运算生成得到的。自然的问题是，这些新加入的元素与 F 中原来的元素是否有某种非平凡关系。更具体地，对一个新元素 α，我们能否用 F 中的系数，通过有限次加法和乘法得到一个非平凡的等式？也就是说，能否找到这样的关系：

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0, \qquad a_i \in F, \quad a_i \text{ 不全为零.}$$

如果可以，那么 α 就是 $F[x]$ 中某个非零多项式的根。这里排除零多项式，是因为它在任何元素处都取值为零，不能表达新元素满足了什么关系。下面先用一个取值映射把这些关系记录下来，再严格定义代数元与超越元。

2.2.1 代数元与最小多项式

首先设有域扩张 E/F，设 $\alpha \in E$，考虑将多项式在 α 处取值的映射：

$$\begin{aligned} \varphi_\alpha : F[x] &\longrightarrow E \\ f(x) &\longmapsto f(\alpha) \end{aligned}$$

这是一个环同态，于是其核 $\ker \varphi_\alpha$ 是 $F[x]$ 的一个理想。

定义 2.2.1 (零化多项式). 设 $\varphi_\alpha : F[x] \to E$、$f \mapsto f(\alpha)$。若 $0 \neq f \in \ker \varphi_\alpha$，则称 f 为 α 在 F 上的一个**零化多项式**。

由于 F 是一个域，故 $F[x]$ 是一个主理想整环，也是一个欧几里得整环，于是我们知道理想 $\ker \varphi_\alpha$ 是一个主理想，于是显然有以下定理：

定理 2.2.2 (取值映射的核). 存在 $f_\alpha \in F[x]$ 使 $\ker \varphi_\alpha = (f_\alpha)$。若核非零，要求 f_α 首一，则它唯一；若核为零，取 $f_\alpha = 0$。

证明. $F[x]$ 是 PID，故该核有生成元；核非零时，将任意非零生成元除以其首项系数即可得到首一生成元。同一非零主理想的两个生成元相伴，而 $F[x]$ 的单位是非零常数，因此首一生成元唯一。核为零时用 0 生成即可。 □

定义 2.2.3 (代数元). 若 $\ker \varphi_\alpha \neq 0$，即存在非零 $f \in F[x]$ 使 $f(\alpha) = 0$，称 α 为 F 上的**代数元**。将该核的唯一首一生成元 f_α 称为 α 在 F 上的**最小多项式**，记为 $\mathrm{Irr}(\alpha, F)$。其次数称为 α 在 F 上的次数，记为 $\deg(\alpha, F)$。

定义 2.2.4 (超越元). 若 $\ker \varphi_\alpha = 0$，即没有非零 F 系数多项式在 α 处为零，称 α 为 F 上的**超越元**。

由上述定义容易看出：

定理 2.2.5 (一次代数元). 对 F 上的代数元 α，$\alpha \in F \Leftrightarrow \deg(\alpha, F) = 1$.

证明. 若 $\alpha \in F$，则 $x - \alpha$ 零化 α，而非零常数不能零化它，故最小多项式次数为 1。反之，首一的一次最小多项式可写为 $x - a$、$a \in F$，代入 α 得 $\alpha = a \in F$。 □

定理 2.2.6 (最小多项式的不可约性). 设 α 是 F 上的代数元，则其最小多项式不可约。更一般地，首一多项式 $g \in F[x]$ 是 α 的最小多项式，当且仅当 $g(\alpha) = 0$ 且 g 不可约。

证明. 若 $f_\alpha = gh$ 且 g, h 次数均较小，则 $g(\alpha)h(\alpha) = 0$。由于 E 是域，必有一个因子在 α 处为零，与 f_α 为非零核中最小次数的多项式矛盾。反之，若 $g(\alpha) = 0$，则 $f_\alpha \mid g$；g 不可约且二者首一，迫使 $g = f_\alpha$。 □

2.2.2 单扩张的结构与次数

由定理 2.2.6，代数元 α 的最小多项式 f_α 在 F 上不可约。于是 (f_α) 是 $F[x]$ 中的极大理想，商环 $F[x]/(f_\alpha)$ 是域，而且常数陪集给出 F 在其中的嵌入。这样，我们就又通过构造商环得到了一个域扩张。接下来换一个角度：如果把域扩张看作向 F 中添加元素，那么这个商环构造实际上添加了怎样的元素？我们将它与添加 α 生成的域联系起来，再看扩张的大小怎样由最小多项式的次数决定。

定义 2.2.7 (单扩张). 设 E/F 是域扩张，任取 $\alpha \in E$，记

$$F(\alpha) = C(F \cup \{\alpha\})$$

为 E 中 $F \cup \{\alpha\}$ 生成的子域，称为 α 在 F 上生成的子域，我们称 $F(\alpha)/F$ 为 F 的**单扩张**，若 α 是代数元，称 $F(\alpha)/F$ 为**单代数扩张**，若 α 是超越元，称 $F(\alpha)/F$ 为**单超越扩张**。

若 $\alpha \in E$ 是 F 上的代数元，考虑以下交换图：

$$\begin{array}{ccc} F[x] & \xrightarrow{\varphi_\alpha} & E \\ \downarrow{\scriptstyle \pi_\alpha} & \nearrow{\scriptstyle \overline{\varphi_\alpha}} & \\ F[x]/(f_\alpha) & & \end{array} \tag{2.1}$$

交换图 2.1中的商环 $F[x]/(f_\alpha)$ 是域，诱导映射 $\overline{\varphi_\alpha}$ 保持幺元，因而为单射，其像也是域。这个像恰为 $F[\alpha]$；它包含 F 与 α，所以 $F[\alpha]$ 已经是由它们生成的子域，即：

$$F(\alpha) = F[\alpha].$$

综上我们有以下定理：

定理 2.2.8 (单扩张与多项式商环). 设 E/F 为域扩张，任取 $\alpha \in E$，若 α 是代数元，则：

$$F(\alpha) \cong F[x]/(f_\alpha).$$

若 α 是超越元，则：

$$F(\alpha) \cong F(x).$$

其中 $F(x) = \mathrm{Frac}(F[x])$ 是有理函数域。

证明. 对于代数元的情形，考虑对 φ_α 使用环同态基本定理，有：$F[\alpha] \cong F[x]/(f_\alpha)$，又由 $F[\alpha] = F(\alpha)$ 即得：$F(\alpha) \cong F[x]/(f_\alpha)$。

对于超越元的情形，同理有环同构：$F[\alpha] \cong F[x]$，于是二者的分式域同构：$F(\alpha) \cong F(x)$。 □

在得到域扩张 $F(\alpha)/F$ 后，我们会关心扩张次数 $[F(\alpha) : F]$ 的大小，下面的定理给出了扩张次数与 α 在 F 上次数的关系。

定理 2.2.9 (单代数扩张的次数与基). 设 $\alpha \in E$ 为 F 上的代数元，则 $F(\alpha)$ 为 F 的有限扩张且满足：

$$[F(\alpha) : F] = \deg(\alpha, F) = \deg f_\alpha(x).$$

证明. 设 $n = \deg f_\alpha$。由定理 2.2.8，每个元素可由 $F[x]/(f_\alpha)$ 中的陪集表示。用带余除法可将代表多项式唯一化为次数小于 n 的余式，因此

$$1, \alpha, \ldots, \alpha^{n-1}$$

生成 $F(\alpha)$ 作为 F-线性空间。若 $\sum_{i=0}^{n-1} a_i \alpha^i = 0$ 且系数不全为零，则得到次数小于 n 的非零零化多项式，与最小性矛盾。故上述 n 个元素线性无关，是一组基，扩张次数为 n。 □

2.2.3 代数扩张的基本性质

以上讨论了添加单个元素得到的扩张。下面考虑任意多个代数元及由它们生成的域。

定义 2.2.10 (代数扩张). 设 E/F 是域扩张，若任取 $\alpha \in E$ 都是 F 上的代数元，则称 E 为 F 的**代数扩张**。

定义 2.2.7中的单扩张只添加一个元素；现在考虑由多个元素生成的扩张。

定义 2.2.11 (扩域的生成). 设有域扩张 E/F，任给集合 $S \subseteq E$，我们称 $C(F \cup S)$ 为 S 在 F 上生成的域，记作 $F(S)$。

注意到这里 S 的势可以是任意的，可以是有限也可以是无限，下面的定理给出 S 生成的域与 S 的有限子集生成的域之间的关系。

定理 2.2.12 (无限生成域的有限子集表达). 设有域扩张 E/F，任给集合 $S \subseteq E$，有：

$$F(S) = \bigcup \{F(S') : S' \subseteq S, |S'| < \infty\}.$$

证明. 记右侧的并为 L。每个 $F(S')$ 都包含于 $F(S)$，故 $L \subseteq F(S)$。反之，L 包含 $F \cup S$，而且 L 是子域：若 $x \in F(S_1)$、$y \in F(S_2)$，则 x, y 同属于 $F(S_1 \cup S_2)$，其中 $S_1 \cup S_2$ 仍有限；加减乘除的结果也在该域中（除法要求 $y \neq 0$）。因此 L 是包含 $F \cup S$ 的子域，由 $F(S)$ 的最小性知 $F(S) \subseteq L$。 □

除了关心 S 的势，我们还关心添加元素的顺序是否影响生成的域的结构，例如考虑 $\alpha_1, \alpha_2 \in E$，我们可以直接将 α_1, α_2 一起添加到 F 中，生成域 $F(\alpha_1, \alpha_2)$，也可以先向 F 中添加 α_1 生成 $F(\alpha_1)$，再向域 $F(\alpha_1)$ 中添加 α_2，生成域 $F(\alpha_1)(\alpha_2)$，即 $F(\alpha_1, \alpha_2)$ 与 $F(\alpha_1)(\alpha_2)$ 是否是相同的，一般地，我们有如下定理：

定理 2.2.13 (逐次添加与同时添加). 设 $S_1, S_2 \subseteq E$，则

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

证明. 右侧是包含 $F \cup S_1 \cup S_2$ 的子域，因此包含左侧。反之，左侧包含 $F(S_1)$ 及 S_2，因此包含右侧。 □

于是当我们将 F 扩张为 $F(\alpha_1, \ldots, \alpha_n)$ 时，我们可以分 n 次进行，每次只考虑一个元素的单扩张。

于是由上述讨论我们知道，如果向 F 中添加有限个代数元得到域扩张 E，那么由定理 2.2.9及塔式公式 2.1.22，E 一定是 F 的有限次扩张，那么反过来，我们想知道是否任意有限次扩张 E 都是 F 的代数扩张，事实上由下面的定理我们知道结论是肯定的。

定理 2.2.14 (有限扩张必为代数扩张)**.** 若 E 为 F 的一个有限次扩张，则 E 是 F 的一个代数扩张。

证明. 设 $[E:F]=n$，任取 $\alpha\in E$。线性空间 E 中的 $n+1$ 个元素 $1,\alpha,\dots,\alpha^n$ 必线性相关，因此存在不全为零的 $a_0,\dots,a_n\in F$ 使

$$a_0+a_1\alpha+\cdots+a_n\alpha^n=0.$$

故 α 是非零多项式 $\sum_{i=0}^{n}a_ix^i$ 的根，是代数元。 □

根据上述结论，我们可以得到域扩张 E/F 上 F 的代数元具有某种封闭性：

定理 2.2.15 (代数元对域运算的封闭性)**.** 设 $\alpha,\beta\in E$ 是 F 上的代数元，则 $\alpha+\beta$、$\alpha-\beta$ 及 $\alpha\beta$ 也为 F 上的代数元；当 $\beta\neq 0$ 时，$\alpha\beta^{-1}$ 也为代数元。

证明. α 在 F 上代数，β 也在 $F(\alpha)$ 上代数，因为原来的非零 F 系数零化多项式仍可视为 $F(\alpha)$ 系数多项式。由定理 2.2.9及 2.1.22，$F(\alpha,\beta)/F$ 为有限扩张，故为代数扩张。上述各运算结果在这个域内，其中逆要求 $\beta\neq 0$，所以结论成立。 □

综合上述所有讨论，我们有如下结论：

定理 2.2.16 (有限生成代数扩张的有限性)**.** 设有域扩张 E/F，取 $\alpha_1,\dots,\alpha_n\in E$，设 $K=F(\alpha_1,\dots,\alpha_n)$，则以下三个叙述等价：

(i) K 为 F 的代数扩张；

(ii) $\alpha_1,\dots,\alpha_n$ 都是 F 上的代数元；

(iii) K 为 F 的有限扩张。

证明. (i) 立即推出 (ii)。若 (ii) 成立，依次添加 $\alpha_1,\dots,\alpha_n$，每一步均为有限单代数扩张；由塔式公式得到 (iii)。(iii) 由定理 2.2.14推出 (i)。 □

有限个代数元生成有限扩张。添加无限多个代数元时，生成的域一般未必有限，但其中每个元素只涉及有限多个生成元，所以仍是代数扩张。

推论 2.2.17 (任意多个代数元生成代数扩张)**.** 若 $S\subseteq E$ 的每个元素都在 F 上代数，则 $F(S)/F$ 为代数扩张。

证明. 由定理 2.2.12，每个 $x\in F(S)$ 都属于某个有限子集 S' 生成的域 $F(S')$。由定理 2.2.16，该域是 F 的有限扩张，故 x 在 F 上代数。 □

在扩张次数有限时，我们容易证明代数扩张具有传递性，即：若扩张 K/E 与 E/F 都是代数扩张，则 K/F 也是代数扩张，对于次数无限时事实上也有相同的结论。

定理 2.2.18 (代数扩张的传递性)**.** 若扩张 K/E 与 E/F 都是代数扩张，则 K/F 也是代数扩张。

证明. 中间域 E/F 可能无限，但一个零化多项式只涉及有限多个系数。先将这些系数收集到一个有限扩张中，就能回到有限扩张的塔式公式。

任取 $\alpha \in K$，取非零多项式 $\sum_{i=0}^{n} a_i x^i \in E[x]$ 使 $\sum_i a_i \alpha^i = 0$。令 $L = F(a_0, \ldots, a_n)$。各 a_i 在 F 上代数，由定理 2.2.16，L/F 有限；α 在 L 上代数，所以 $L(\alpha)/L$ 也有限。由塔式公式，$L(\alpha)/F$ 有限，进而 α 在 F 上代数。由 α 的任意性得结论。 □

2.2.4 补充：代数闭包与纯超越扩张

下面区分给定扩域中的代数闭包与纯超越扩张。这些概念不参与下一节分裂域的构造与唯一性证明。

由代数扩张的传递性，我们知道逐次添加代数元不会产生新的超越元；即使添加任意多个代数元，每个生成的元素也只涉及有限多个生成元。于是我们可以问：能否把所有代数元收集起来，得到一个“最大”的代数扩张？这里首先固定一个扩域 E/F，只收集 E 中在 F 上代数的元素；不能把来自未指定扩域的元素直接放在一起。由定理 2.2.15，这些元素对域运算封闭，所以已经构成一个子域 E_0，并且 E_0/F 是代数扩张。它包含 E 中每个代数于 F 的元素，因此在这个固定的 E 中确实是最大的代数中间域。下面的定义指的正是这种相对的构造。

定义 2.2.19 (给定扩域中的代数闭包)**.** 设 E/F 是域扩张，令

$$E_0 = \{\alpha \in E : \alpha \text{ 在} F \text{ 上代数}\}.$$

称 E_0 为 F **在** E **中的代数闭包**。它是 E 的子域，且 E_0/F 是代数扩张。

这个定义依赖给定的扩域 E，不能因此断言 E_0 是代数闭域。例如 $E = F = \mathbb{Q}$ 时有 $E_0 = \mathbb{Q}$。通常所说的“F 的代数闭包”还要求该扩域本身代数闭，即其中每个非常数多项式都有根；这里尚未证明这种扩域的存在性。此外，若 $\alpha \in E$ 在 E_0 上代数，由传递性它在 F 上也代数，故 $\alpha \in E_0$。所以 $E \setminus E_0$ 中的元素在 E_0 上超越。这个结论并不等同于纯超越扩张。

定义 2.2.20 (纯超越扩张)**.** 若存在 $S \subseteq E$，使 $E = F(S)$，且 S 在 F 上**代数无关**，则称 E/F 为**纯超越扩张**。这里代数无关指：对 S 中任意有限个不同元素 $s_1, \ldots, s_n$，不存在非零多项式 $f \in F[x_1, \ldots, x_n]$ 满足 $f(s_1, \ldots, s_n) = 0$。

例如，α 在 F 上超越时，$F(\alpha)/F$ 为纯超越扩张。不能用“E 中的所有元素都是超越元”定义它，因为 $F \subseteq E$，而 F 中的元素均在 F 上代数。[1]

[1] 更一般的超越基等内容不在这里展开。

2.3 分裂域

2.3.1 分裂域的构造

在先前的讨论中，我们可以看出代数元与域上多项式的根有密切联系。由定义知道，如果 E/F 是代数扩张，那么 E 中的每个元素都是某个非零 F 系数多项式的根。那么反过来，是否每个非常数的 F 系数多项式都在 E 中有根呢？一般来说，这个结论并不成立。例如 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 是代数扩张，但 x^2-3 在其中没有根：若 $(a+b\sqrt{2})^2=3$ 且 $a,b\in\mathbb{Q}$，则 $2ab=0$，分别得到 $a^2=3$ 或 $b^2=3/2$，均无有理解。于是我们的问题可以变为：任意取定一个非常数多项式 $f\in F[x]$，能否找到某个域扩张 E/F，使 f 在 E 中至少有一个根？**Kronecker 构造**给出了肯定的回答。

定理 2.3.1 (Kronecker 构造)**.** 设 F 为域，任取 $f(x)\in F[x]$，且 $\deg f(x)>0$，存在一个域扩张 E/F，使得 $f(x)$ 在 E 中有根。

证明. 由 $F[x]$ 是 PID，可以把 f 分解成不可约因子的乘积。要使 f 有一个根，只需使其中一个不可约因子 $p\in F[x]$ 有根，所以我们先将问题归结为不可约多项式的情形。由于 (p) 是极大理想，$E=F[x]/(p)$ 是域。常数陪集给出嵌入 $F\hookrightarrow E$：非零常数不属于 (p)。令 $\alpha=\overline{x}$，则 $p(\alpha)=\overline{p(x)}=0$，故 $f(\alpha)=0$。 □

这个构造我们并不陌生。先前已经知道，若 α 是 F 上的代数元，最小多项式为 f_α，那么

$$F[x]/(f_\alpha)\cong F(\alpha).$$

这个同构告诉我们：向 F 中添加代数元 α，与把 $F[x]$ 商掉它的最小多项式所生成的理想，得到的是同构的域。所以，如果我们希望一个不可约多项式 $p\in F[x]$ 在某个扩域中有根，就可以反过来做：直接构造 $F[x]/(p)$。在这个域中，$\overline{x}$ 满足 $p(\overline{x})=0$，这就相当于向 F 添加了 p 的一个根，而不必事先知道这个根在哪里。若在另一扩域中已有 p 的根 α，对应的同构为

$$\begin{aligned}\Phi: F[x]/(p) &\longrightarrow F(\alpha),\\ g(x)+(p) &\longmapsto g(\alpha).\end{aligned}$$

于是 $\Phi(\overline{x})=\alpha$，也就是说，抽象商域中的 $\overline{x}$ 正好对应我们熟悉的那个根。

由 Kronecker 构造，任意非常数多项式 f 都在某个扩域中有一根 α_1，于是可以在这个新域中写出 $f=(x-\alpha_1)f_1$。如果 f_1 仍非常数，就对它继续做相同的事情，在进一步的扩域中找到根 α_2，再写 $f_1=(x-\alpha_2)f_2$。不断这样进行下去，每次都使剩余因子的次数减少 1，所以经过有限步，所有线性因子都能得到。这说明，一个根的构造已经足够：重复它就能找到使原多项式完全分裂的扩域。

定理 2.3.2 (多项式分裂扩域的存在性)**.** 设 $0\neq f\in F[x]$ 且 $\deg f=n>0$。存在域扩张 E/F 使

$$f(x)=a\prod_{i=1}^{n}(x-\alpha_i),\qquad a\in F^*,\quad \alpha_i\in E.$$

根允许重复。

证明. 对 n 归纳。$n=1$ 时根已经在 F 中。一般情况下，由定理 2.3.1，先在某个有限扩域 F_1 中找到一根 α_1，写 $f=(x-\alpha_1)f_1$，其中 $f_1\in F_1[x]$ 的次数为 $n-1$。对 f_1 应用归纳假设，即可在 F_1 的某个扩域中将它分裂，从而 f 也分裂。 □

于是我们自然地引出**分裂**与**分裂域**的概念。

定义 2.3.3 (分裂). 设有域扩张 E/F，任取 $f(x)\in F[x]$，且 $\deg f(x)=n>0$，若存在 $a\in F^*,\alpha_1,\dots,\alpha_n\in E$，使得：

$$f(x)=a(x-\alpha_1)...(x-\alpha_n)$$

则称 $f(x)$ 在 E 中**分裂**。

定义 2.3.4 (分裂域). 设 E/F 为域扩张，$f\in F[x]$ 为非常数多项式，且 $f=a\prod_{i=1}^{n}(x-\alpha_i)$ 在 E 中分裂。若 $E=F(\alpha_1,\dots,\alpha_n)$，称 E 为 f 在 F 上的**分裂域**，称 E/F 为**分裂域扩张**。

例 2.3.5 (从最小多项式到分裂域). 取 $F=\mathbb{Q}$、$\alpha=\sqrt{2}$。其最小多项式为 x^2-2，因此

$$\mathbb{Q}(\sqrt{2})\cong\mathbb{Q}[x]/(x^2-2),\qquad[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2.$$

它有基 $1,\sqrt{2}$，且 x^2-2 的两个根 $\sqrt{2},-\sqrt{2}$ 都在其中，故这个单扩张已经是该多项式的分裂域。

例 2.3.6 (x^3-2 的分裂域). 取 $f(x)=x^3-2\in\mathbb{Q}[x]$，令 $\alpha=\sqrt[3]{2}$ 为正实根。若最简分数 a/b 为有理根，则 $a^3=2b^3$ 先迫使 a 为偶数，再迫使 b 为偶数，矛盾。三次多项式可约必有一次因子，因此 f 不可约。由定理 2.2.9，

$$[\mathbb{Q}(\alpha):\mathbb{Q}]=3.$$

令 $\omega=(-1+\sqrt{-3})/2\in\mathbb{C}$，则 $\omega^2+\omega+1=0$、$\omega^3=1$ 且 $\omega\neq1$。于是

$$x^3-2=(x-\alpha)(x-\alpha\omega)(x-\alpha\omega^2).$$

$\mathbb{Q}(\alpha)\subseteq\mathbb{R}$，而 $\alpha\omega,\alpha\omega^2$ 非实，故第一次添加根所得的域还不能使 f 分裂。再令 $K=\mathbb{Q}(\alpha,\omega)$，三个根均在 K 中。反过来，由 $\omega=(\alpha\omega)/\alpha$，有 $K=\mathbb{Q}(\alpha,\alpha\omega,\alpha\omega^2)$，所以 K 恰为 f 的分裂域。
ω 满足二次多项式 x^2+x+1，但不属于实域 $\mathbb{Q}(\alpha)$，故 $[K:\mathbb{Q}(\alpha)]=2$。塔式公式 2.1.22给出

$$[K:\mathbb{Q}]=[K:\mathbb{Q}(\alpha)]\,[\mathbb{Q}(\alpha):\mathbb{Q}]=2\cdot3=6.$$

结合两层扩张的基，K 的一组 $\mathbb{Q}$-基为

$$1,\ \alpha,\ \alpha^2,\ \omega,\ \alpha\omega,\ \alpha^2\omega.$$

第一次扩张获得一个实根，第二次扩张补齐另外两个根。

由定义可以看出，使 f 分裂的扩域未必就是 f 的分裂域：它还可能含有使 f 分裂并不需要的其他元素。由定理 2.3.2，先找到使 f 分裂的扩域，再取其中由全部根生成的子域，就得到一个分裂域。我们希望进一步说明，它是使 f 分裂的“最小”的扩张。这个最小性首先是在一个固定的分裂扩域 K 中讨论的：若某个中间域 H 已经使 f 分裂，那么 f 在 K 中的全部根都必须属于 H，因而它们生成的分裂域 E 也包含在 H 中。为什么在不同子域中写出的全部根不会变成另一套根？一种思路是比较两种线性因子分解，并利用 $K[x]$ 中的唯一分解性。下面把这一论证写明。

定理 2.3.7 (固定扩域中分裂域的最小性)**.** 设 $f \in F[x]$ 非常数并在 K 中分裂。令 $E \subseteq K$ 为 f 的全部根在 F 上生成的子域，则

$$E = \bigcap \{H : F \subseteq H \subseteq K,\ H \text{ 是子域且} f \text{ 在} H \text{ 中分裂}\}.$$

证明. 设 $f = a\prod_{i=1}^{n}(x-\alpha_i)$ 在 E 中分裂。若它也在 $H \subseteq K$ 中分裂，写 $f = b\prod_{i=1}^{n}(x-\beta_i)$，其中 $\beta_i \in H$。这两式也是 $K[x]$ 中的分解。由于 $K[x]$ 是 PID，唯一分解性说明两组一次因子在相伴及置换意义下相同。每个 $x-\alpha_i$、$x-\beta_i$ 都是首一的，所以相伴时实际相等；适当重排后，有 $\alpha_i = \beta_i$，从而每个 $\alpha_i \in H$。于是 $E = F(\alpha_1, \ldots, \alpha_n) \subseteq H$。而 E 本身也使 f 分裂，属于取交的子域族，所以交恰为 E。也可以把 f 在 H 中的分解代入任意一个 K 中的根，利用域中无零因子直接得到这个根等于某个 β_i；这给出了同一包含关系的另一种简短验证。 □

由 Kronecker 构造的过程可以得到以下分裂域的性质。

定理 2.3.8 (分裂域的次数与基域扩大)**.** 设 E/F 是非常数多项式 $f \in F[x]$ 的分裂域，$\deg f = n$，则：

1. $[E : F] \leq n!$；
2. 若 $F \subseteq K \subseteq E$，则 E 也是 $f \in K[x]$ 在 K 上的分裂域。

证明. (1) 按重数列出全部根 $\alpha_1, \ldots, \alpha_n$，令 $F_i = F(\alpha_1, \ldots, \alpha_i)$。在 $F_{i-1}[x]$ 中除去前 $i-1$ 个已知线性因子后，余下多项式次数为 $n-i+1$，且以 α_i 为根。所以 α_i 在 F_{i-1} 上的最小多项式次数不超过 $n-i+1$。由塔式公式，

$$[E : F] = \prod_{i=1}^{n}[F_i : F_{i-1}] \leq \prod_{i=1}^{n}(n-i+1) = n!.$$

(2)f 在 E 中分裂，而且

$$F(\alpha_1, \ldots, \alpha_n) = E \subseteq K(\alpha_1, \ldots, \alpha_n) \subseteq E.$$

故 $K(\alpha_1, \ldots, \alpha_n) = E$，满足分裂域的生成条件。 □

2.3.2 分裂域的唯一性

上一小节中我们已经得到了分裂域的存在性。这一小节主要研究唯一性：对 $f \in F[x]$ 的两个分裂域 $E, \bar{E}$，是否一定存在固定 F 的同构 $E \to \bar{E}$？我们试着借助同态的逐步延拓来构造这样的同构。

设 $E = F(\alpha_1, \ldots, \alpha_n)$。我们希望构造 $\sigma : E \to \bar{E}$，自然先令 $\sigma|_F = \mathrm{id}_F$。这样一来，$\sigma$ 就完全由 $\alpha_1, \ldots, \alpha_n$ 的像决定了；但这些像必须保持原来元素之间的代数关系，不能任意指定。同时确定 n 个元素的像比较困难，所以我们需要逐个考虑。先选定 α_1 的一个合适的像 $\bar{\alpha}_1$，尝试建立

$$\sigma_1 : F_1 = F(\alpha_1) \longrightarrow \bar{F}_1 = F(\bar{\alpha}_1)$$

之间的同构；然后再选 α_2 的像 $\bar{\alpha}_2$，尝试把 σ_1 延拓成

$$\sigma_2 : F_2 = F_1(\alpha_2) \longrightarrow \bar{F}_2 = \bar{F}_1(\bar{\alpha}_2)$$

之间的同构。不断这样进行下去，就能逐步得到从 E 到 $\bar{E}$ 的嵌入。最后还要证明，它的像确实是整个 $\bar{E}$，才能得到所求同构。把 $F_0 = \bar{F}_0 = F$，$\sigma_0 = \mathrm{id}_F$，以及各步的像 $\bar{F}_i = \sigma_i(F_i)$ 写在一起，就是交换图 2.2所示的过程。

$$\begin{array}{ccccccccc} F_0 = F & \hookrightarrow & F_1 & \hookrightarrow & F_2 & \hookrightarrow & \cdots & \hookrightarrow & F_n = E \\ \downarrow{\scriptstyle \mathrm{id}_F} & & \downarrow{\scriptstyle \sigma_1} & & \downarrow{\scriptstyle \sigma_2} & & & & \downarrow{\scriptstyle \sigma_n = \sigma} \\ \bar{F}_0 = F & \hookrightarrow & \bar{F}_1 & \hookrightarrow & \bar{F}_2 & \hookrightarrow & \cdots & \hookrightarrow & \bar{F}_n \end{array} \tag{2.2}$$

由上述讨论可以看出，这个过程的关键问题是：如何将 F_i 到 $\bar{F}_i$ 的同构 σ_i，延拓为 $F_{i+1} = F_i(\alpha_{i+1})$ 到 $\bar{F}_{i+1}$ 的同构 σ_{i+1}？这里“延拓”的意思是保留已经确定的映射，即

$$\sigma_{i+1}|_{F_i} = \sigma_i.$$

它不是把整个 F_i 上的映射重新指定为恒等映射。为解决这一步，我们先给出两个有用的引理：先把已有同构作用到多项式系数上，再利用商域构造向添加一个根后的域延拓。

引理 2.3.9 (系数同构在多项式环上的延拓)**.** 设 $\varphi : K \to \bar{K}$ 为域同构。对 $f(x) = \sum_{k=0}^{n} a_k x^k \in K[x]$，定义

$$\bar{f}(x) = \varphi_* f(x) := \sum_{k=0}^{n} \varphi(a_k) x^k \in \bar{K}[x].$$

则 $\varphi_* : K[x] \to \bar{K}[x]$ 为环同构，保持次数，并且 f 不可约当且仅当 $\bar{f}$ 不可约。

证明. 逐项作用的 φ_* 保持加法与乘法，其逆为 $(\varphi^{-1})_*$，且非零首项系数仍非零，故保持次数。若 f 有非平凡因式分解，应用 φ_* 即得 $\bar{f}$ 的非平凡分解；对逆映射作相同讨论，得到反方向。 □

引理 2.3.10 (单代数扩张同构的延拓)**.** 沿用引理 2.3.9的记号，设 $p \in K[x]$ 不可约，α 为 p 的根，$\bar{\alpha}$ 为 $\bar{p}$ 的根，则：

1. 存在域同构 $\eta : K[x]/(p) \to \bar{K}[x]/(\bar{p})$，在常数子域上等于 φ；
2. 存在唯一的域同构 $\sigma : K(\alpha) \to \bar{K}(\bar{\alpha})$，满足 $\sigma|_K = \varphi$ 且 $\sigma(\alpha) = \bar{\alpha}$；
3. 若域同态 $\psi : K(\alpha) \to L$ 满足 $\psi|_K = \varphi$，其中 L 包含 $\bar{K}$，则 $\psi(\alpha)$ 是 $\bar{p}$ 的根。

证明. (1) 系数同构 φ_* 将理想 (p) 映到 $(\bar{p})$，故它诱导

$$\eta : g + (p) \longmapsto \varphi_* g + (\bar{p}).$$

由逆系数同构可知 η 为同构。记 $\pi, \bar{\pi}$ 为自然商映射，则 $\bar{\pi} \circ \varphi_* = \eta \circ \pi$，如交换图 2.3所示：

$$\begin{array}{ccc} K[x] & \xrightarrow{\varphi_*} & \bar{K}[x] \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \bar{\pi}} \\ K[x]/(p) & \xrightarrow{\eta} & \bar{K}[x]/(\bar{p}) \end{array} \tag{2.3}$$

(2) 取值同构 $K[x]/(p) \to K(\alpha)$ 与 $\bar{K}[x]/(\bar{p}) \to \bar{K}(\bar{\alpha})$ 都将 $\bar{x}$ 送到相应根。把它们与 η 复合，得到要求的 σ；根的像由这个复合自动确定，不是另行指定。由于 K 与 α 生成整个域，满足这两个条件的同态唯一。

(3) 写 $p = \sum_{k=0}^{n} a_k x^k$，则

$$0 = \psi(p(\alpha)) = \sum_{k=0}^{n} \varphi(a_k)\psi(\alpha)^k = \bar{p}(\psi(\alpha)).$$

□

利用以上引理，我们可以得到以下定理。

定理 2.3.11 (单代数扩张的同态计数)**.** 设 $\sigma : K \to \bar{K}$ 为域同构，$K(\alpha)/K$ 为单代数扩张，$p = \mathrm{Irr}(\alpha, K)$，且 $\bar{p} = \sigma_* p$。若 $\bar{E}/\bar{K}$ 是使 $\bar{p}$ 分裂的扩域，则满足 $\varphi|_K = \sigma$ 的域同态 $\varphi : K(\alpha) \to \bar{E}$ 与 $\bar{p}$ 在 $\bar{E}$ 中的不同根一一对应，对应由 $\varphi \mapsto \varphi(\alpha)$ 给出。因此这样的域同态个数至多为 $[K(\alpha) : K]$，等号成立当且仅当 $\bar{p}$ 没有重根。

证明. 由引理 2.3.10(3)，每个同态把 α 送到 $\bar{p}$ 的一根；同态由这个像唯一确定。反之，对每个根 $\beta \in \bar{E}$，引理 2.3.10(2) 给出同构 $K(\alpha) \to \bar{K}(\beta)$，再与嵌入 $\bar{K}(\beta) \hookrightarrow \bar{E}$ 复合，即得到一个延拓。故同态个数恰为不同根个数，至多为 $\deg \bar{p} = \deg p = [K(\alpha) : K]$；恰好达到此数，当且仅当全部根互不相同。

令 $\iota_K : K \hookrightarrow K(\alpha)$ 与 $\iota_{\bar{K}} : \bar{K} \hookrightarrow \bar{E}$ 为包含映射。延拓条件 $\varphi|_K = \sigma$ 可写为交换图 2.4：

$$\begin{array}{ccc} K & \xrightarrow{\iota_{\bar{K}} \circ \sigma} & \bar{E} \\ {\scriptstyle \iota_K}\downarrow & \nearrow_{\varphi} & \\ K(\alpha) & & \end{array} \tag{2.4}$$

□

同态数能否达到扩张次数，取决于相关多项式有无重根。下面先给出一个可计算的判别。

定义 2.3.12 (多项式的形式导数). 对 $f(x)=\sum_{k=0}^{n}a_kx^k\in F[x]$，定义它的**形式导数**为

$$f'(x)=\sum_{k=1}^{n}ka_kx^{k-1},$$

其中 k 按 $k1_F$ 理解；常数多项式的导数为零。这是系数上的代数运算，并且逐项相乘可验证乘积法则 $(fg)'=f'g+fg'$。

引理 2.3.13 (重根的形式导数判别). 设 $f\in F[x]$ 非常数，E/F 是使 f 分裂的扩域。则以下条件等价：

1. f 在 E 中有重根；
2. f 与 f' 在 E 中有共同根；
3. $\gcd(f,f')$ 是非常数多项式。

这里最大公因子取首一代表。因此 f 无重根当且仅当 $\gcd(f,f')=1$。

证明. 若 $\alpha\in E$ 是 f 的根，写 $f=(x-\alpha)^rg$，其中 $r\geq 1$ 且 $g(\alpha)\neq 0$。由乘积法则，

$$f'=r(x-\alpha)^{r-1}g+(x-\alpha)^rg'.$$

当 $r=1$ 时，$f'(\alpha)=g(\alpha)\neq 0$；当 $r\geq 2$ 时，$f'(\alpha)=0$。这在任意特征下都成立，故 (1) 与 (2) 等价。

若 $\gcd(f,f')=1$，Bézout 等式给出 $u,v\in F[x]$ 使 $uf+vf'=1$，在共同根处取值会得到 $0=1$，故 (2) 不成立。若最大公因子非常数，它整除 f，所以也在 E 中分裂并有根；这个根同时是 f 与 f' 的根。因此 (2) 与 (3) 等价。 □

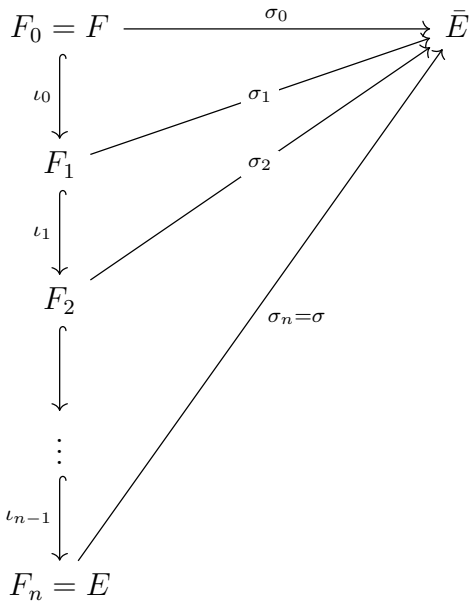
由同态延拓与以上重根判别，可以得到分裂域扩张的唯一性及同构个数。

定理 2.3.14 (分裂域的唯一性). 设 $f\in F[x]$ 非常数，$E,\bar{E}$ 为 f 的两个分裂域。存在域同构 $\sigma:E\to\bar{E}$ 满足 $\sigma|_F=\mathrm{id}_F$。这样的 F-同构个数至多为 $[E:F]$；等号成立当且仅当 f 的每个不可约因式都没有重根。这里指不可约因式自身没有重根，允许 f 含有某个因式的高次幂。

证明. 先逐次添加根并延拓基域上的映射，得到 $E\to\bar{E}$ 的嵌入；再利用两个域都由全部根生成这一点证明满射。各步映像的最小多项式还控制可选的不同根数，从而给出同构个数及等号条件。

存在性：按重数列出 f 在 E 中的根，写 $E=F(\alpha_1,\dots,\alpha_n)$，令 $F_0=F$、$F_i=F_{i-1}(\alpha_i)$。从 $\sigma_0=\mathrm{id}_F$ 出发，假设已构造 $\sigma_{i-1}:F_{i-1}\to\bar{E}$。$\alpha_i$ 在 F_{i-1} 上的最小多项式 p_i 整除 f；将其系数经 σ_{i-1} 映到 $\bar{E}$，得到的多项式仍整除 f，因为 σ_{i-1} 固定 F。由于 f 在 $\bar{E}$ 中分裂，这个多项式也在 $\bar{E}$ 中分裂。对 F_{i-1} 与其像之间的同构应用定理 2.3.11，便得到延拓 $\sigma_i:F_i\to\bar{E}$。

这些延拓都指向同一个扩域 $\bar{E}$, 并且在已有子域上的限制保持不变, 如交换图 2.5所示；其中 ι_i 为包含映射：



(2.5)

最终得到 F-嵌入 $\sigma : E \to \bar{E}$，还需证明满射。将 $f = a\prod_i(x-\alpha_i)$ 经 σ 映到 $\bar{E}[x]$，得到 $f = a\prod_i(x-\sigma(\alpha_i))$。因此 $\bar{E}$ 中 f 的每个根都等于某个 $\sigma(\alpha_i)$，其全部根生成的域 $\bar{E}$ 包含于 $\sigma(E)$。故 $\sigma(E) = \bar{E}$，σ 为同构。

个数上界：对每个已给定的 σ_{i-1}，定理 2.3.11说明它的延拓数至多为 $[F_i : F_{i-1}]$。逐步相乘，并用塔式公式，得到

$$\#\{\sigma : E \xrightarrow{\sim} \bar{E} : \sigma|_F = \mathrm{id}_F\} \le \prod_{i=1}^{n}[F_i : F_{i-1}] = [E : F].$$

等号条件：若 f 的每个不可约因式没有重根，则每个 p_i 整除某个这样的因式，所以 p_i 也没有重根。由引理 2.3.13，有 $\gcd(p_i, p_i') = 1$。系数同构与形式导数交换，故将 Bézout 等式经系数映射后，仍得到映像多项式与其导数的 Bézout 等式；再由该引理，相应的映像多项式也无重根。于是每个已给定的同态恰有 $[F_i : F_{i-1}]$ 个延拓，上界成为等号。

反之，若某个不可约因式 q 有重根，可先选 α_1 为 q 的一根。则 p_1 为 q 的首一相伴多项式，第一步的不同根个数严格小于 $[F_1 : F]$；后续每一步的延拓数仍不超过相应扩张次数，故总数严格小于 $[E : F]$。 □

注 (分裂域唯一与同构映射的选择). 定理 2.3.14所说的唯一，是指任何两个分裂域之间存在固定基域 F 的同构（定义 2.1.10）；这样的同构可以有多种选择。例如 $\mathbb{Q}(\sqrt{2})$ 有两个不同的 $\mathbb{Q}$-自同构：

$$a + b\sqrt{2} \longmapsto a + b\sqrt{2}, \qquad a + b\sqrt{2} \longmapsto a - b\sqrt{2} \quad (a, b \in \mathbb{Q}).$$

它们分别将 $\sqrt{2}$ 映到 $\pm\sqrt{2}$。由引理 2.3.10，在基域上的映射和生成元的像指定以后，延拓才是唯一的。

附录 A　适用条件速查

A.1　主要结论的适用条件

表 A.1列出常用结论的假设与结果；第一列链接到完整陈述和证明。模均指幺左模，D 表示 PID，F, K, E 表示域。

表 A.1　主要结论的适用条件

结论与正文位置	适用条件	可得结论
模与矩阵		
同态集合的标量结构 定理 1.1.24、1.1.22	R 为幺环；M, N 为 R-模	$\mathrm{Hom}_R(M,N)$ 为 $\mathrm{Z}(R)$-模；R 交换时为 R-模。
同态的矩阵表示 定义 1.2.6、命题 1.2.10	R 为幺环；M, N 为有限生成自由模并选定有序基	使用行坐标；复合的矩阵满足 $A_{\psi\circ\varphi} = A_\varphi A_\psi$。
自由模的秩唯一 定理 1.2.12	R 为非零交换幺环；M 为有限生成自由模	基的大小与选择无关；$R^m \cong R^n$ 推出 $m = n$。
方阵可逆性 推论 1.2.20	R 为非零交换幺环；A 为 R 上的方阵	A 可逆当且仅当 $\det A$ 为单位。
扭元集合是子模 定义 1.3.5后的说明	R 为交换整环；M 为 R-模	$\mathrm{Tor}(M)$ 为子模；此处不要求 M 有限生成。
自由模的子模 定理 1.3.2	D 为 PID；$K \subseteq D^n$ 为子模，n 有限	K 有限生成且自由，$\mathrm{rank}\, K \le n$。
Smith 标准型 定理 1.2.22、1.2.27	D 为 PID；$A \in D^{m\times n}$	对角元满足整除链；非零不变因子在相伴意义下唯一。
有限生成模的结构 定理 1.3.7、1.3.21	D 为 PID；M 为有限生成 D-模	$M \cong D^r \oplus \bigoplus_i D/(d_i)$；$r$ 唯一，规范因子在相伴意义下唯一。
无扭模的自由性 推论 1.3.10	D 为 PID；M 有限生成且无扭	M 为自由模。
域扩张		
塔式公式 定理 2.1.22	$F \subseteq K \subseteq E$；$E/K$ 与 K/F 均有限	$[E:F] = [E:K][K:F]$。
有限扩张的代数性 定理 2.2.14	E/F 为有限扩张	E 中每个元素都在 F 上代数。
有限生成代数扩张 定理 2.2.16	$E = F(\alpha_1, \ldots, \alpha_n)$；各 α_i 在 F 上代数	$[E:F] < \infty$。
分裂域的存在与唯一 定理 2.3.2、2.3.8、2.3.14	$f \in F[x]$ 非常数，$\deg f = n$	分裂域存在且在 F-同构意义下唯一；其次数至多为 $n!$。
分裂域的自同构数 定理 2.3.14	E/F 为 f 的分裂域；f 的每个不可约因式自身无重根	固定 F 的自同构数为 $[E:F]$；去掉无重根条件时仅有上界。