环 上 的 模

下文中的环均指含幺的交换环.

1. 模的定义. 设 A 是环. 所谓 A **模** (A-module) 是指二元组 (M,φ), 其中 M 是阿贝尔群 (群运算用加法表示), φ 为映射 (称为**数量积**或**纯量积**),

$$\varphi\colon A\times M\to M,\quad (a,x)\mapsto a\star x$$

(无歧义时常简记为 $a\cdot x$ 或毗连 ax), 满足如下性质:

(1) 对所有 $x\in M$, 有 $1\cdot x=x$;
(2) 对所有 $a,b\in A$, $x\in M$, 有 $a\cdot(b\cdot x)=(ab)\cdot x$;
(3) 对所有 $a,b\in A$, $x\in M$, 有 $(a+b)\cdot x=a\cdot x+b\cdot x$;
(4) 对所有 $a\in A$, $x,y\in M$, 有 $a\cdot(x+y)=a\cdot x+a\cdot y$.

令 M_1 与 M_2 为 A 模. 映射 $\varphi: M_1\to M_2$ 叫做 A **模同态** (或A **线性映射**), 如果

(1) φ 是阿贝尔群同态,
(2) 对一切 $a\in A$, $x\in M$, 有 $\varphi(ax)=a\varphi(x)$.

如果 A 模同态 φ 是双射, 则称它为 A 模间的**同构**.

令 M 是 A 模. 它的子集 N 叫做 M 的 A **子模** (submodule), 如果 N 是 M 的加法子群, 并且对一切 $a\in A$, $x\in N$, 有 $ax\in N$.

2. 模的例子.

(1) 最平凡的模是零模, 它只有一个元素 0. 对任何 A 模 M, 存在唯一的同态 $0\to M$, 以及唯一的同态 $M\to 0$, 前者是将 0 送到 0 的映射, 后者将一切元素送到 0. 任何两个模 M 和 N, 复合同态 $M\to 0\to N$ 叫做**零同态**.
(2) 阿贝尔群与 $\mathbb{Z}$ 模是等价的概念. 若 k 是域, 则 k 模与 k 上的线性空间是等价的概念.
(3) 考虑一切分量属于 A 的列向量 $(a_1,\ldots,a_n)^{\mathrm{T}}$ 构成的集合 A^n. 则在显然的 "数乘" 与 "加法" 运算下, A^n 构成一个 A 模. 一般将同构于 A^n 的 A 模称作**秩为 n 的自由 A 模** (free A-module).
(4) 令 $k[\lambda]$ 是域 k 上的一元多项式环. 令 V 是秩为 n 的 k 模. 令 $T: V\to V$ 为 V 上一 k 线性映射. 则 V 可以通过 T 看作 $k[\lambda]$ 模. 如果 $f\in k[\lambda]$, $v\in V$, 定义

$$f(\lambda)\star v=f(T)(v).$$

Date: 创建日期: 2020 年 11 月 8 日. 编译日期: 2021 年 12 月 13 日.

假设 (V_1, T_1) 和 (V_2, T_2) 是两个线性空间以及分别作用于它们之上的两个线性映射. 如上所述, 它们决定了 $k[\lambda]$ 模 M_1, M_2. 则模同态 $\varphi : M_1 \to M_2$ 包含了如下信息: 第一, 有阿贝尔群同态 $\varphi : M_1 \to M_2$, 第二, 它要尊重 $k[\lambda]$ 结构, 即 $\varphi(f(\lambda)v) = f(\lambda)\varphi(v)$. 这第二个条件意味着, 首先, $\varphi(cv) = c\varphi(v)$ $(c \in k)$, 即 φ 是 k 线性映射; 其次 $\varphi(\lambda v) = \lambda\varphi(v)$, 转换成线性映射的语言, 即是说 $\varphi(T_1(v)) = T_2\varphi(v)$.

所以, φ 是 $k[\lambda]$ 模同构的必要且充分条件是, φ 首先是线性空间的同构, 然后 $\varphi \circ T_1 = T_2 \circ \varphi$. 如果用矩阵 P 来表示 k 线性映射 φ, 则 φ 是 $k[\lambda]$ 模的必要且充分条件是 $\mathsf{PT}_1 = \mathsf{T}_2\mathsf{P}$, 即方阵 T_1 与 T_2 通过矩阵 P 相似.

(5) 将环 A 看作秩为 1 的自由模. 则它的子模与 A 的理想是同一概念.
(6) 命 $\mathscr{C}^\infty(D)$ 为 n 维空间中光滑曲面 D (或一可微流形) 上的光滑函数构成的环. 命 E 为 n 维空间中与 D 相切的光滑向量场的全体 (或流形上的某光滑向量丛的光滑截面的全体) 构成的集合. 则 E 为 $\mathscr{C}^\infty(D)$ 上的模.
(7) 令 $\varphi : A \to B$ 为一环同态. 则 B 可通过法则 $a \star b = \varphi(a)b$ 看作 A 模.
(8) 若 $\varphi : M \to M'$ 为 A 模同态. 则**同态核** $\mathrm{Ker}(\varphi) = \{x \in M : \varphi(x) = 0\}$ 为 M 的子模; **同态像** $\mathrm{Im}(\varphi) = \{y \in M' : \exists x \in M, \varphi(x) = y\}$ 为 M' 的子模.
(9) 令 $\mathrm{Hom}_A(M, N)$ 为一切从 A 模 M 到 A 模 N 的 A 线性映射的全体. 则 $\mathrm{Hom}_A(M, N)$ 自然地是 A 模. 特别地, 当 $N = A$ 时, 称 $\mathrm{Hom}_A(M, A)$ 为 M 的**对偶模**, 记为 $M^\vee$.

3. 商模与同态基本定理. 令 N 为 A 模 M 的子模. 则商群 M/N 可以自然地被赋予 A 模结构如下: $a(x + N) = ax + N$. 容易验证这个定义是良好的. 称这个具备这个模结构的 M/N 为 M 关于 N 的**商模**.

同态基本定理. — 若 $\varphi : M \to M'$ 为 A 模同态. 令 $\pi : M \to M/N$ 为投影同态 $\pi(x) := x + N$.

(1) 若 $N \subset \mathrm{Ker}(\varphi)$ 存在唯一同态 $\overline{\varphi} : M/N \to M'$, 使得 $\overline{\varphi} \circ \pi = \varphi$.
(2) 若 $N = \mathrm{Ker}(\varphi)$, 则 $\overline{\varphi}$ 诱导了同构 $M/\mathrm{Ker}(\varphi) \simeq \mathrm{Im}(\varphi)$.
(3) M 的包含 N 的子模与 M/N 的子模通过下列映射一一对应:

$$S \longmapsto \pi(S),$$

$$\pi^{-1}(T) \longleftarrow\!\shortmid T.$$

若 S 与 $T = \pi(S)$ 对应, 则 $S/N \simeq T$.

4. 模的运算. 理想的许多运算可以推广到模上. 令 M 是 A 模, M_i 是由指标集 I 参数化的一族 M 的子模. 则他们的**和** $\sum_{i\in I} M_i$ 是由所有有限和 $\sum x_i$ 构成的子集, 其中 $x_i \in M_i$, $x_i = 0$ 对除了有限多个 $i \in I$ 成立. 容易验证, $\sum_{i\in I} M_i$ 是 M 的子模. 此外,

$\bigcap_{i\in I} M_i$ 也是 M 的子模. 应用同态基本定理, 可以证明如下同构:

$$(M_1+M_2)/M_1 \cong M_2/(M_1\cap M_2). \quad \square$$

设 $\varphi: A\to B$ 为环同态, M 是 B 模. 则可将 M 通过如下方式看作 A 模: $a\star x := \varphi(a)x$. 这种将 B 模看作 A 模的方法叫做 "**纯量的收缩** (contraction of scalars)". 比如, 通过典则同态 $\mathbb{Z}\to B$ 而将 B 模看作 $\mathbb{Z}$ 模, 即是 "忘掉" M 的 B 模结构, 而只把它当作阿贝尔群; 在线性代数中, 可以将 n 维复线性空间看作 $2n$ 维实线性空间, 就是将纯量环 $\mathbb{C}$ 收缩到了纯量环 $\mathbb{R}$. 类似地, 将例 2 第四款中的模的纯量通过 $k\to k[t]$ 而收缩到 k 上, 得到的便是 k 线性空间 V 自己.

令 $\mathfrak{a}$ 为 A 的理想. 定义

$$\mathfrak{a}M = \left\{\sum_{i=1}^{n} a_i x_i \in M : n\in\mathbb{N}, a_i\in\mathfrak{a}, x_i\in M\right\}.$$

则 $\mathfrak{a}M$ 为 M 的子模. 注意到商模 $M/\mathfrak{a}M$ 可以自然地看作 $A/\mathfrak{a}$ 模. $A/\mathfrak{a}$ 模 $M/\mathfrak{a}M$ 是一个常见操作 "**纯量的扩张** (extension of scalars)" 的特例. 考虑多项式环 $\mathbb{R}[t]$ 上的自由模 $M=\mathbb{R}[t]^n$, 以及理想 (t^2+1). 则 $M/(t^2+1)M$ 就是向量空间 $\mathbb{C}^n$.

令 I 是指标集. 设有 A 模 M_i, $i\in I$. 则读者可自己定义乘积模 $\prod_{i\in I} M_i$. 诸 M_i 的 (外) **直和** $\bigoplus_{i\in I} M_i$ 则是指一切

$$(m_i : i\in I) \in \prod_{i\in I} M_i,$$

其中 $m_i\neq 0$ 仅对有限个 i 成立, 构成的 $\prod_{i\in I} M_i$ 的子模. 将 $(m_i : i\in I)$ 改记为形式线性组合 $\sum_{i\in I} m_i$, 用以彰显它是直和中的元素. 如果指标集有限, 则乘积模与直和没有区别.

5. 矩阵与行列式. 可以考虑分量属于环 A 的 $m\times n$ 矩阵的全体 $\mathrm{M}_{m\times n}(A)$. 对任何这样的矩阵 $\mathsf{T}=(a_{ij})$, 可以定义自由模之间的同态

$$A^n\to A^m, \quad x\mapsto \mathsf{T}x.$$

反之, 任何从 A^n 到 A^m 的同态都具有这样的形态. n 阶方阵 T 叫做**可逆**的, 如果存在方阵 S 使得 $\mathsf{ST}=\mathsf{TS}=\mathsf{Id}_n$. 可逆 n 阶方阵的全体构成群, 记作 $\mathrm{GL}_n(A)$. 显然可逆方阵定义的自由模 A^n 上的同态是同构.

我们也可以对方阵 $\mathsf{T}=(a_{ij})\in\mathrm{M}_n(A)$ 定义它的**行列式**

$$\det\mathsf{T} = \sum_{\sigma\in\mathfrak{S}_n} (-1)^{\mathrm{sgn}(\sigma)} a_{1\sigma(1)}\cdots a_{n\sigma(n)} \in A.$$

可以验证, $\det\mathsf{T}_1\mathsf{T}_2 = \det\mathsf{T}_1\det\mathsf{T}_2$. 方阵 T 可逆的必要且充分条件是 $\det\mathsf{T}$ 是 A 中的单位, 因为 Cramer 法则给出了计算逆的公式

$$\mathsf{T}^{-1} = (\det\mathsf{T})^{-1}\mathrm{adj}(\mathsf{T})$$

其中 $\mathrm{adj}(\mathsf{T})$ 是方阵 T 的经典伴随方阵.

群 $\mathrm{GL}_n(A)$ 具有很多元素. 比如三类初等方阵: 对任何 $a \in A$, $i \neq j$, $\mathsf{Id}_n + ae_{ij}$ 是可逆的; 对 $u \in \mathbb{G}_{\mathrm{m}}(A)$, $\mathsf{Id}_n + (u-1)e_{ii}$ 是可逆的; 置换矩阵是可逆的.

6. 自由模与基. 令 M 为 A 模. 元素 $v_1, \ldots, v_n \in M$ 被称为 M 的**基**, 如果

- $v_1, \ldots, v_n$ "A **线性无关**", 即若 $a_1v_1 + \cdots + a_nv_n = 0$, 则 $a_1 = \cdots = a_n = 0$;
- $v_1, \ldots, v_n$ "**线性生成**了 M", 即对任何 $x \in M$, 存在 $x_1, \ldots, x_n \in A$, 使 $x = x_1v_1 + \cdots + x_nv_n$.

容易验证, M 是秩为 n 的自由模的必要且充分条件是 M 具有一个 n 个元素构成的基. 显然, 如果 $(v_1, \ldots, v_n) \in M$ 是 M 的一组基, $\mathsf{P} \in \mathrm{GL}_n(A)$, 则

$$(w_1, \ldots, w_n) = (v_1, \ldots, v_n)\mathsf{P}$$

仍然是 M 的一组基. 且任何 M 的基都具有这种形态. 可以验证, A^n 同构于 A^m 的必要且充分条件是 $m = n$. 如果矩阵 T 给出了 A^n 到 A^m 的同态, 则如果进行基变换, 则相应矩阵表示为 PTQ^{-1}.

并非所有 A 模都是自由的. 比如有限阿贝尔群都不是自由的. 例 2 第四款中描述的模也都不是自由的. 一个模被称为**循环模** (cyclic module), 如果它作为模同构于 $A/\mathfrak{a}$, 其中 $\mathfrak{a}$ 是 A 的理想. 除非 $\mathfrak{a} = (0)$, 循环模都不是自由的.

7. 有限生成模. A 模 M 叫做**有限生成** (finitely generated) A 模, 如果存在满同态

$$A^n \to M.$$

M 是有限生成的等价于存在 $v_1, \ldots, v_n \in M$ 使得第 6 段第二款中的性质成立, 即任何 $v \in M$ 都是 $v_1, \ldots, v_n$ 的 A **线性组合** (A-linear combination). 此时, 称这里的 $v_1, \ldots, v_n$ **(线性地) 生成了** M, 或把 $v_1, \ldots, v_n$ 叫做 M 的一组 (关于 A 的) **生成元** (generator). 我们先前证明过有限生成 $\mathbb{Z}$ 模的结构定理: 任何有限生成阿贝尔群可以写成直和 $F \oplus T$, 其中 F 是有限秩的自由阿贝尔群, T 是有限个循环模的直和. 今后将会证明, 类似的性质对例 2 第四款中的模也成立.

如果 A 的理想作为 A 模是有限生成的, 就叫它是**有限生成的理想**. 一个理想是有限生成的必要充分条件是它具有形态 $(a_1, \ldots, a_n)$, 其中 $a_i \in A$.

先前证明过, 有限生成 $\mathbb{Z}$ 模的子模仍然是有限生成的. 此性质的证明依赖于归纳法以及我们对 $\mathbb{Z}$ 的子模的认识. 对于一般的环, 有限生成模的子模未必有限生成. 事实上, 无限个变量的多项式环

$$\mathbb{C}[x_1, x_2, x_3, \ldots]$$

的理想 $(x_1, x_2, x_3, \ldots)$ 就不是有限生成的.

证. 设这个理想为有限生成的, 且以 $f_1, \ldots, f_r$ 为生成元, 我们来推导矛盾. 由于 $f_1, \ldots, f_r$ 只含有有限个变量, 可假设变量 x_N 不出现在 $f_1, \ldots, f_r$ 中. 设 $x_N = \sum_{i=1}^r h_i(x) f_i(x)$.

由于 h_i 是多项式, 它们只含有限个变量. 因此, 上面的等式在有限个变量的多项式环 $\mathbb{C}[x_1,\ldots,x_n]$ 中成立.

由于 $f_1,\ldots,f_r$ 在 $\mathbb{C}[x_1,x_2,\ldots]$ 中不生成单位理想, 它们在 $\mathbb{C}[x_1,\ldots,x_n]$ 中也必然不生成单位理想. 希尔伯特零点定理推出一定存在 $\zeta=(\zeta_1,\ldots,\zeta_n)\in\mathbb{C}^n$, 使得 $f_i(\zeta)=0$ 对任何 i 都成立. 由于 f_i 中不含变量 x_N, $f_i(\zeta)$ 是否等于 0 与 ζ_N 取什么值无关. 因此无妨设 $\zeta_N=1$. 在等式

$$x_N=\sum_{i=1}^r h_i(x)f_i(x)$$

中将 x_i 取值为 ζ_i, 就得到了 $1=0$, 因而产生了矛盾. □

此处所举例子具有某种 "无限" 的品性. 在赋予环某种 "有限性质" 之后, 即可保证有限生成模的子模仍然为有限生成的. 为此, 我们引入 "诺特环" 这一概念.

8. 诺特模与诺特环的定义. 设 A 为环. 设 M 为 A 模. 我们称 M 为**诺特**[1]的 (Noetherian), 如果 M 满足下述诺特的**升链条件** (ascending chain condition, ACC): 若 $M_1\subseteq M_2\subseteq M_3\subseteq\cdots$ 为 M 的一系列子模. 则存在充分大的 n, 使得 $M_n=M_{n+1}=\cdots$. 若自由模 A 为诺特的, 则称环 A 为**诺特环**.

引理. *A 模 M 为诺特模的必要且充分条件是任何 M 的子模都是有限生成的.*

证. 设 M 的任意子模都是有限生成的. 令 $M_1\subseteq M_2\subseteq\cdots$ 为 M 的子模的升链. 容易验证, $\bigcup_{n=1}^\infty M_n=N$ 为 M 的子模. 因为 N 是有限生成的, 可以选定一组生成元 $w_1,\ldots,w_m\in N$. 因为每个 w_i 都属于某一个 M_i, 故存在充分大的 n, 使得 $w_i\in M_n$ 成立. 由此可知

$$M_n=M_{n+1}=\cdots=N.$$

反之, 设 M 为诺特模. 令 N 为 M 的子模. 如果 $N=\{0\}$, 则命题为平凡. 如不然, 取 $v_1\in N$. 如果 $\varphi_1:A\to N$, $a\mapsto av_1$ 为满射, 则命题已证. 如果不然, 必存在 $v_2\in N$, 使得同态 $\varphi_2:A^2\to N,(a,b)\mapsto av_1+bv_2$ 与 φ_1 有不同的像. 长此以往, 就得到了一系列同态 φ_n, 且

$$\mathrm{Im}(\varphi_1)\subseteq\mathrm{Im}(\varphi_2)\subseteq\cdots.$$

由于 M 为诺特, 上述升链必然稳定. 因此必有 n, 使得 φ_n 为满射. 因此 N 为有限生成. □

类似于诺特模的定义, 也可以定义 A 模的子模的**降链条件** (descending chain condition, DCC). A 模叫做**阿廷**[2]的 (Artinian), 如果它满足降链条件. A 叫做 **阿廷环**, 如果秩为一的自由 A 模 A 为阿廷模.

[1]埃米 · 诺特 (Amalie Emmy Noether, 1882 年 3 月 23 日 – 1935 年 4 月 14 日), 德国数学家. 她被爱因斯坦和维纳誉为人类历史上最伟大的女科学家.

[2]埃米尔 · 阿廷 (Emil Artin, 1898 年 3 月 3 日 – 1962 年 12 月 20 日), 是生于奥匈帝国的数学家. 他与诺特一起被认为是抽象代数学科的奠基人. 他也是当代数论的主要开拓者.

9. 一些例子.

(1) 显然, 主理想整环是诺特环, 域是诺特环. 特别地, $\mathbb{Z}$ 是诺特环. 但 $\mathbb{Z}$ 不是阿廷环. $\mathbb{Z}/n\mathbb{Z}$ 既是阿廷环也是诺特环. 我们稍后将证明**希尔伯特**[3]**基定理** (Hilbert's basis theorem), 它断言任何诺特环上的多项式环仍然是诺特环. 因此, 初等代数中常见的环都是诺特环.

(2) 实数上的可微函数环 $\mathscr{C}^\infty(\mathbb{R})$ 或连续函数环 $\mathscr{C}(\mathbb{R})$ 都不是诺特环.

(3) 令 A 是环. 则无限个变量的多项式环 $A[x_1, x_2, \ldots]$ 既不是阿廷环也不是诺特环. 一个理想的无限严格升链由

$$(x_1) \subsetneqq (x_1, x_2) \subsetneqq \cdots$$

给出. [理由: 如果 $x_n \in (x_1, \ldots, x_{n-1})$, 则 $x_n = \sum_{i=1}^{n-1} h_i(x)x_i$, 令 $x_i = 0$ 便推出 $x_n = 0$, 矛盾.] 一个理想的无限严格降链由 $(x_1) \supsetneqq (x_1^2) \supsetneqq \cdots$ 给出.

(4) 根据对应定理, 诺特环的商环仍然是诺特环. 但是诺特环的子环不一定是诺特环. 比如无穷个变量的多项式环 $\mathbb{Q}[x_1, x_2, \ldots]$ 是为其分式域的子环.

(5) 令 p 为素数. 令 G 为 $\mathbb{Z}$ 模 $\mathbb{Q}/\mathbb{Z}$ 中一切阶为 p 的方幂的元素的全体. 则 G 是阿廷 $\mathbb{Z}$ 模, 但不是诺特的.

(6) 诺特环上的有限秩的自由模是诺特的 (证明与 $\mathbb{Z}$ 模的情形类似). 诺特模的商模是诺特的. 因此诺特环上的有限生成模是诺特的. 因此, 诺特环上的有限生成模与诺特模这两个概念是一致的.

(7) 可以证明, 阿廷环都是诺特环 (证明略复杂, 我们在这门课中不进行讨论), 但是我们已经看到阿廷模未必是诺特模.

10. 有限生成模的表现. 现在我们来讨论如何研究诺特环 A 上的有限生成模. 首先, 如果 M 是有限生成模, 则我们知道存在满同态

$$d_0 : A^{n_0} \to M.$$

由于 $\mathrm{Ker}(\varphi)$ 是 A^{n_0} 的子模, 而 A^{n_0} 是诺特的, 因此存在满同态 $\psi : A^{n_1} \to \mathrm{Ker}(\varphi)$. 我们可以将 ψ 与包含同态 $\mathrm{Ker}(\varphi) \hookrightarrow A^{n_0}$ 复合到一起, 得到同态 $d_1 : A^{n_1} \to A^{n_0}$, 由此我们的到了序列

$$A^{n_1} \xrightarrow{d_1} A^{n_0} \xrightarrow{d_0} M \to 0 \qquad (*)$$

其中 $\mathrm{Ker}(d_0) = \mathrm{Im}(d_1)$. 根据同态基本定理, M 的同构类完全由同态 d_1 决定. 而 d_1 可以由一个分量在 A 中的矩阵 T_1 表出. 这个矩阵叫做模 M 的**表现矩阵** (presentation matrix). 我们先前研究有限生成 $\mathbb{Z}$ 模的时候, 矩阵 T_1 起到了关键作用: 我们说明了如

[3]大卫 · 希尔伯特 (David Hilbert, 1862 年 1 月 23 日 – 1943 年 2 月 14 日), 德国数学家, 是 19 世纪末和 20 世纪前期最具影响力的学者之一. 他因发明了大量的思想观念 (例如不变量理论, 公理化几何, 希尔伯特空间) 而被尊为伟大的数学家.

果合适地选取基，可以使得 d_1 的矩阵表示变得简单 (Smith 标准形)，从而获得了关于 M 结构的定理. 式子 $(*)$ 叫做 M 的**表现** (presentation).

例. 在线性代数中学习 Jordan 标准形理论时学过如下结论 "两方阵 $\mathsf{T}_1, \mathsf{T}_2$ 相似，当且仅当 λ 方阵 $\lambda\mathsf{Id} - \mathsf{T}_1$, $\lambda\mathsf{Id} - \mathsf{T}_2$ 相抵". 接下来给出这个断言的模论解释. 考虑 n 维 k 模 k^n 和一个分量取值于 k 的 n 阶方阵 T. 则我们可以利用例 2 第四款的方法得到一个 $k[\lambda]$ 模，记为 M. 我们断言：

方阵 $\lambda\mathsf{Id}_n - \mathsf{T} \in \mathrm{M}_n(k[\lambda])$ 是 M 的一个表现矩阵.

作为习题，读者可以尝试用这个断言推出上述线性代数课程中的结论.

断言之证. 我们考虑映射

$$\psi : k[\lambda]^n \to k^n, \quad (f_1(\lambda), \cdots, f_n(\lambda))^{\mathrm{T}} \mapsto \sum_{i=1}^{n} f_i(\mathsf{T})e_i.$$

容易验证这个映射是 $k[\lambda]$ 模同态. 注意到，任何 $k[\lambda]^n$ 中的列向量 (下面为简便计，称它们们 "λ 向量") 可以写成 $u(\lambda) = \lambda^d u_d + \lambda^{d-1}u_{d-1} + \cdots + u_0$, 其中 $u_i \in k^n$, $u_d \neq 0$. 则 $\psi(u(\lambda)) = \sum_{i=0}^{d} \mathsf{T}^i u_0$. 我们要证明，如果 $u(\lambda) \in \mathrm{Ker}(\psi)$, 则 $u(\lambda)$ 必能够写成

$$(\dagger) \qquad (\lambda\mathsf{Id}_n - \mathsf{T})v(\lambda)$$

的形式. 为了完成证明，我们对 "首项次数" d 做归纳. 当 $d = 0$ 时，只有 $\psi(0) = 0$. 对一般的 d, 注意到形如 $(\dagger)$ 的 λ 向量落在 $\mathrm{Ker}(\psi)$ 中. 设 $\psi(u(\lambda)) = 0$, 即

$$\sum_{i=0}^{d} \mathsf{T}^i u_i = 0.$$

下需验证 $u(\lambda)$ 也具有形式 $(\dagger)$. 令

$$v_1(\lambda) = (\lambda\mathsf{Id}_n - \mathsf{T})(\lambda^{d-1}u_d + \lambda^{d-2}u_{d-1} + \cdots + u_1),$$

则 $v_1(\lambda) \in \mathrm{Ker}(\psi)$. 因此 $v_2(\lambda) = u(\lambda) - v_1(\lambda) \in \mathrm{Ker}(\psi)$. 但是 $v_2(\lambda)$ 的首项次数已经比 d 低了. 根据归纳假设，它具有形式 $(\dagger)$. 又因为具有形式 $(\dagger)$ 的 λ 向量构成了子模，$u(\lambda) = v_1(\lambda) + v_2(\lambda)$ 也形如 $(\dagger)$. 这就完成了归纳证明. □

根据结构定理，有限生成自由 $\mathbb{Z}$ 模的子模是有限生成且自由的. 因此如果 $A = \mathbb{Z}$, 在 $(*)$ 中可以假设 d_1 为单射. 对于一般的 A, d_1 有可能无法被选择为单射. 但是 $\mathrm{Ker}(d_1)$ 总是有限生成的. 因此我们可以选择满射 $A^{n_2} \to \mathrm{Ker}(d_1)$, 等等. 总之，从一个有限生成的 M 出发，我们可以得到一个序列

$$\cdots \to A^{n_k} \xrightarrow{d_k} A^{n_{k-1}} \to \cdots \to A^{n_1} \xrightarrow{d_1} A^{n_0} \xrightarrow{d_0} M \to 0$$

满足

$$(**) \qquad \boxed{\mathrm{Ker}(d_i) = \mathrm{Im}(d_{i+1})}.$$

在模论中, 序列

$$\cdots \to M_k \xrightarrow{d_k} M_{k-1} \to \cdots \to M_1 \xrightarrow{d_1} M_0 \xrightarrow{d_0} M_{-1} \to \cdots$$

叫做**正合序列** (exact sequence), 如果等式 (**) 对一切 $i \in \mathbb{Z}$ 都成立. 我们先前由通过选择 "生成元与关系" 而得到的正合序列叫做与 M 相配的**朔望** (syzygy) 序列或**自由分解** (free resolution).

11. 希尔伯特基定理. 设 A 是诺特环. 则多项式环 $A[x]$ 是诺特环.

证. 我们要证明任何 $A[x]$ 的理想都是有限生成的. 为此, 设 $\mathfrak{a}$ 是 $A[x]$ 的理想. 基本的想法是先研究 $\mathfrak{a}$ 中多项式的系数. 令 $\mathfrak{b}_m$ 是 $\mathfrak{a}$ 中次数不超过 m 的多项式的首项系数构成的集合. 则我们来验证 $\mathfrak{b}_m$ 是 A 中的理想. 事实上, 如果 $b \in \mathfrak{b}_m$, $c \in \mathfrak{b}_m$, 则存在多项式 $f(x) = bx^i + \cdots \in \mathfrak{a}$, $g(x) = cx^j + \cdots \in \mathfrak{a}$. 由于 $\mathfrak{a}$ 是理想, 我们有 $x^{m-i}f(x) + x^{m-j}g(x) = (b+c)x^m + \cdots \in \mathfrak{a}$. 因此有 $b + c \in \mathfrak{b}_m$. 如果 $a \in A$, 则 $af(x) \in \mathfrak{a}$, 故而 $ab \in \mathfrak{b}_m$. 这就验证了 $\mathfrak{b}_m$ 是理想.

注意到如果 $m < n$, 我们有 $\mathfrak{b}_m \subseteq \mathfrak{b}_n$. 这是因为如果 $b \in \mathfrak{b}_m$, 我们知道存在 $f(x) \in \mathfrak{a}$, 次数 $\leq m$, 且首项系数为 b. 因此 $x^{n-m}f(x)$ 是次数不超过 n, 且首项系数为 b 的 $\mathfrak{a}$ 中多项式. 因此我们从 $\mathfrak{a}$ 构造出了 A 中理想的升链

$$\mathfrak{b}_1 \subseteq \mathfrak{b}_2 \subseteq \cdots .$$

因为 A 是诺特环, 上面的升链必须在某一步之后不再严格上升, 即存在 n, 使得 $\mathfrak{b}_n = \mathfrak{b}_{n+1} = \cdots$. 接下来, 我们来解释为何这就推出了 $A[x]$ 是诺特的.

注意到 $A[x]$ 中次数不超过 n 的多项式的全体 $A[x]_{\leq n}$ 可以看做 A 模, 并且它是自由的, 以 $1, x, \ldots, x^n$ 为基:

$$A[x]_{\leq n} = A \cdot 1 \oplus A \cdot x \oplus \cdots \oplus A \cdot x^n.$$

同时, 由于与零次多项式数乘不改变次数, 容易验证 $\mathfrak{a} \cap A[x]_{\leq n}$ 是 $A[x]_{\leq n}$ 的 A 子模. 因为 A 是诺特的, $\mathfrak{a} \cap A[x]_{\leq n}$ 是有限生成模 (见第 8 段的引理). 于是, 存在有限个多项式

$$f_1, f_2, \cdots, f_r \in \mathfrak{a} \cap A[x]_{\leq n}$$

A 线性地生成了 $\mathfrak{a} \cap A[x]_{\leq n}$. 然后我们断言, $f_1, \ldots, f_r$ 是 $A[x]$ 模 $\mathfrak{a}$ 的一组生成元. 为此, 我们任取 $f \in \mathfrak{a}$, 设 f 的次数为 d. 我们对 d 进行归纳, 来证明 f 可以被写成 $f_1, \ldots, f_r$ 的 $A[t]$ 线性组合. 如果 $d \leq n$, 则 f 是 $f_1, \ldots, f_r$ 的 A 线性组合. 由于 A 是 $A[x]$ 的子环, 它当然也是 $f_1, \ldots, f_r$ 的 $A[x]$ 线性组合. 如果 $d > n$, 我们知道 f 的首项系数 a 落在 $\mathfrak{a}_n$ 中, 因此存在 $g \in \mathfrak{a} \cap A[x]_{\leq n}$, 使得 g 的首项系数与 f 的相等. 设 g 的次数为 $e \leq n$, 则 $f(x) - x^{d-e}g(x)$ 的次数便严格地小于 d 了. 因此归纳假设告诉我们存在 $h_1, \ldots, h_r$, 使得

$$f(x) = x^{d-e}g(x) + \sum_{i=1}^{r} h_i(x) f_i(x).$$

由于 $g(x)$ 的次数 $\leq n$, 它自己也是 $f_1, \ldots, f_r$ 的 A 线性组合. 于是上面的式子表明 $f(x)$ 是 $f_1, \ldots, f_r$ 的 $A[x]$ 线性组合. 这就结束了希尔伯特基定理的证明. $\square$

对变量的个数做归纳法, 我们由希尔伯特基定理推出任何诺特环上的有限个变量的多项式环都是诺特环. 由于主理想整环和域显然是诺特环, 以及诺特环的商环仍然是诺特环, 我们知道形如 $\mathbb{Z}[x_1, \ldots, x_n]/\mathfrak{a}$ 的环, 以及形如 $k[x_1, \ldots, x_n]/\mathfrak{a}$ (其中 k 是域) 的环都是诺特环.