數學傳播　32卷1期, pp. 25-47

線性代數五講——
第四講 主理想整環上的模及其分解

龔　昇・張德健

4.1. 環上的模的基本概念

A. 在第二講及第三講中, 我們討論了向量空間及其上線性變換, 在這一講及下一講中將從模的觀點來重新認識之, 這是本書的主要部份, 在這一講中, 將介紹模的定義和基本性質, 尤其是在主理想整環上的模及其分解。

若 $\mathcal{V}$ 體 $\mathbb{F}$ 上的一個向量空間, $T \in \mathcal{L}(\mathcal{V})$。對 $\mathbb{F}[x]$ 中任一多項式 $p(x)$, 對任意 $\vec{v} \in \mathcal{V}$, 可定義

$$p(x)\,\vec{v} = p(T)(\vec{v}),$$

這就是我們要討論作用在 $\mathcal{V}$ 上的線性算子。顯然對任意 $r(x)$, $s(x) \in \mathbb{F}[x]$, $\vec{u}$, $\vec{v} \in \mathcal{V}$ 有

$$\begin{aligned} r(x)\,(\vec{u}+\vec{v}) &= r(x)\,\vec{u} + r(x)\,\vec{v}, \\ (r(x)+s(x))\,\vec{u} &= r(x)\,\vec{u} + s(x)\,\vec{u}, \\ (r(x)\,s(x))\,\vec{u} &= r(x)\,(s(x)\,\vec{u}), \\ 1\,\vec{u} &= \vec{u}, \end{aligned}$$

等等。但是 $\mathbb{F}[x]$ 不是體而是環, 所以 $\mathbb{F}[x]$ 中元素對 $\mathcal{V}$ 作純量乘積, $\mathcal{V}$ 不能成爲一個向量空間。於是引入了比向量空間更爲一般的概念：模。

定義 4.1.1: 若 $\mathcal{R}$ 是有單位元的交換環, 其元素稱爲純量 (scalar)。一個 $\mathcal{R}-$模 ($\mathcal{R}-$module), 或 $\mathcal{R}$ 上的一個模 (a module over $\mathcal{R}$) 是一個非空集合 M, 有運算加法, 記作 $+$, 對 $(\vec{u},\vec{v}) \in M \times M$, 有 $\vec{u}+\vec{v} \in M$; 另一個是 $\mathcal{R}$ 與 M 的運算是純量乘積, 用毗連來表示, 對 $(r,\vec{v}) \in \mathcal{R} \times M$, 有 $r\,\vec{v} \in M$, 而且有

1. M 對加法而言是 Abel 群;
2. 對所有 r, $s \in \mathcal{R}$, $\vec{u}$, $\vec{v} \in M$ 有

a. (分配律) : $r\,(\vec{u}+\vec{v}) = r\,\vec{u} + r\,\vec{v}$, $\quad (r+s)\,\vec{u} = r\,\vec{u} + s\,\vec{v}$;

b. (結合律) : $(r\,s)\,\vec{u} = r\,(s\,\vec{u}), c. \quad 1\,\vec{u} = \vec{u}$.

顯然當 $\mathcal{R}$ 爲體, 則模爲向量空間, 即體上的模就是向量空間。當 $\mathcal{R} = \mathbb{Z}$ (整數環), 則 $\mathbb{Z}-$ 模就是 Abel 群, 故模也是 Abel 群的概念之擴充。

特別重要的是在第一講開始就說到的 $\mathcal{R} = \mathbb{F}[x]$, 若 $\mathbb{F}$ 是體, 則由定理 1.2.1, $\mathbb{F}[x]$ 是主理想整環, 於是可以定義 $\mathbb{F}[x]-$ 模, 這是我們今後要主要討論的對象。

若 $\mathcal{R}$ 是環, 則所有 $m \times n$ 的矩陣的集合 $\mathcal{M}_{m,n}(\mathcal{R})$ 是一個 $\mathcal{R}-$ 模, 其加法與數乘就是矩陣的加法與數乘。當 $\mathcal{R} = \mathbb{F}[x]$ 時, $\mathcal{M}_{m,n}(\mathbb{F}[x])$ 是矩陣元素全爲多項式的矩陣的全體, 它成爲一個 $\mathbb{F}[x]-$ 模。

另一個重要的模式環 $\mathcal{R}$ 自己可以成爲 $\mathcal{R}-$ 模。若 $\mathcal{R}$ 有單位元素的交換環, 定義數乘爲環乘法, 這就是成爲一個 $\mathcal{R}-$ 模, 我們今後會用到這個模。

在下面所討論的線性算子 $T \in \mathcal{L}(\mathcal{V})$ 作用在向量空間 $\mathcal{V}$ 上時, $\mathcal{V}$ 可以看成 $\mathbb{F}$ 上的一個向量空間, 也可以看成在 $\mathbb{F}[x]$ 上的模。

B. 一些向量空間中的概念可以推廣到模上。例如我們可定義 $\mathcal{R}-$ 模 M 的子模如下 :

若 $\mathcal{S}$ 是 $\mathcal{R}-$ 模 M 的一個部分集合, 本身是一個 $\mathcal{R}-$ 模, 稱 $\mathcal{S}$ 爲 M 的子模, S 上的運算就是 M 的運算在 S 上的限制。不難證明

$\mathcal{R}-$ 模 M 的一個非空部分集合 S 成爲子模的充分必要條件爲對任意 $r,\, s \in \mathcal{R}$, $\vec{u},\, \vec{v} \in S$ 有 $r\,\vec{u} + s\,\vec{v} \in S$。

若 $S_1,\, S_2$ 是 M 的子模, 則 $S_1 \cap S_2$ 及

$$S_1 \,+\, S_2 = \left\{\vec{w}_1 \,+ \vec{w}_2 \,:\;\; \vec{w}_1 \in S_1,\;\; \vec{w}_2 \in S_2\right\}$$

也是 M 的子模。

c. 有單位元的交換環 $\mathcal{R}$ 就是 $\mathcal{R}$ 自己上面的模, 則 $\mathcal{R}-$ 模 $\mathcal{R}$ 的子模就是環 $\mathcal{R}$ 的理想。

由子模的概念, 可以定義模的直和 : 若 M 是 $\mathcal{R}-$ 模, 稱 M 是子模 $S_1, \ldots, S_n$ 的直和 (direct sum), 若對每個 $\vec{v} \in M$ 可以唯一地(不計前後次序) 寫成是子模 S_j 中元素之和。即對任意 $\vec{v} \in M$, 有 $\vec{v}_j \in S_j$, $j = 1, \ldots, n$ 使得

$$\vec{v} = \vec{v}_1 + \cdots + \vec{v}_n = \sum_{j=1}^{n} \vec{v}_j.$$

並且若還有 $\vec{w}_j \in S_j$, $j = 1, \ldots, n$ 使得 $\vec{v} = \sum_{j=1}^{n} \vec{w}_j$, 則經過適當排列有 $\vec{w}_j = \vec{v}_j$, $j = 1, \ldots, n$。

當 M 是子模 $S_1, \ldots, S_n$ 的直和, 寫成

$$M = S_1 \oplus S_2 \oplus \ldots \oplus S_n.$$

若 $M = S \oplus S^c$, 則 S^c 爲 S 在 M 中的補集 (complement)。顯然, M 是子模 $S_1, \ldots, S_n$ 的直和若且唯若 $M = S_1 + S_2 + \cdots + S_n$ 及對每一個 $j = 1, \ldots, n$, 有

$$S_j \cap \Big(\sum_{k \neq j} S_k \Big) = \{\vec{0}\}.$$

可以定義生成集 (spanning set)如下：若 M 是 $\mathcal{R}-$ 模, S 是一個部分集合, 由 S 生成的 (spanned or generated) 子模爲 S 中元素的所有的 $\mathcal{R}-$ 線性組合, 即

$$\langle S \rangle = \mathrm{span}(S) = \big\{ r_1 \vec{v}_1 + \cdots + r_n \vec{v}_n \,:\, r_j \in \mathcal{R},\ \ \vec{v}_j \in S,\ \ j = 1, \ldots, n \big\}.$$

M 中的一個部分集合 S 稱爲生成 (spanned or generated) M, 若 $M = \langle S \rangle$, 即每一個 $\vec{v} \in M$, 可寫成

$$\vec{v} = \sum_{j=1}^{n} r_j \, \vec{v}_j,$$

這裡 $r_1, \ldots, r_n \in \mathcal{R}$, $\vec{v}_1, \ldots, \vec{v}_n \in S$。特別由一個元素生成的子模, 即 $\langle \vec{v} \rangle = \mathcal{R}\, \vec{v} = \{ r\, \vec{v} \,:\, r \in \mathcal{R} \}$, $\vec{v} \in M$, 稱爲由 $\vec{v}$ 生成的循環子模 (cyclic submodule)。這是一種十分重要的子模, 今後要不斷出現。如果 $\mathcal{R}-$ 模 M 可以由有限集合生成, 則稱 M 是有限生成的 (finitely generated)。

C. 同樣可以在模中定義部分集合的 $\mathcal{R}-$ 線性獨立、$\mathcal{R}-$ 線性相依及 $\mathcal{R}-$ 基底。若 S 是 M 的部分集合, 稱 S 爲線性獨立的 (linearly independent), 若對任意 $r_1, \ldots, r_k \in R$, $\vec{v}_1, \ldots, \vec{v}_k \in S$, 下面的齊性方程式

$$r_1 \, \vec{v}_1 + r_1 \, \vec{v}_1 + \cdots + r_k \, \vec{v}_k = \vec{0}$$

有唯一的解 $r_1 = \cdots = r_k = 0$。若集合 S 不是線性獨立的, 則稱爲線性相依。

若 M 是 $\mathcal{R}-$ 模, M 的部分集合 $\mathcal{B}$ 稱爲 M 的基底 (basis), 若 $\mathcal{B}$ 線性獨立且生成 M。

由此易見

a. 模 M 的部分集合 $\mathcal{B}$ 是一組基底若且唯若對每個 $\vec{v} \in M$ 有唯一的部分集合 $\{\vec{v}_1, \ldots, \vec{v}_n\}$ 及非零純量 $\alpha_1, \ldots, \alpha_n \in R$, 使得

$$\vec{v} = \sum_{j=1}^{n} \alpha_j \, \vec{v}_j.$$

b. 若 $\mathcal{B}$ 是 M 的基底, 則 $\mathcal{B}$ 是 M 的極小生成集合, 是極大線性獨立集合。

對於向量空間, 有線性變換; 對於模則有同態的概念。

定義 4.1.2: 若 M, N 爲 $\mathcal{R}-$ 模, 映射 $T : M \to N$ 稱爲 $\mathcal{R}-$ 同態 (homomorphism), 若對所有 r, $s \in R$, $\vec{u}$, $\vec{v} \in M$, 有

$$T(r\,\vec{u} + s\,\vec{v}) = r\,T(\vec{u}) + s\,T(\vec{v}).$$

所有從 M 到 N 的 $R-$ 同態記作 $\mathrm{Hom}_{\mathcal{R}}(M, N)$。

顯然 $R-$ 同態是線性變換的推廣。我們稱 M 到 M 的 $\mathcal{R}-$ 同態爲自同態 (endomorphism); 稱單射的同態爲單同態 (monomorphism); 稱滿射的同態爲滿同態 (epimorphism); 稱雙射的同態爲同構 (isomorphism)。

若 $T \in \mathrm{Hom}_{\mathcal{R}}(M, N)$, 定義 T 的核與像爲

$$\ker(T) = \{\vec{v} \in M : T(\vec{v}) = \vec{0}\}, \quad \mathrm{Im}(T) = \{\vec{w} \in N : \exists \vec{v} \in M, \text{ such that } T(\vec{v}) = \vec{w}\},$$

它們分別是 M 及 N 的子模。

由於不是所有的模都有 $\mathcal{R}-$ 基底, 故有以下的定義 :

定義 4.1.3: $\mathcal{R}-$ 模 M 稱爲自由的 (free), 若 M 有 $\mathcal{R}-$ 基底。若 $\mathcal{B}$ 是 M 的基底, 稱 M 在 $\mathcal{B}$ 上自由。M 的基底的基數 (cardinality) 稱爲 M 的秩 (rank), 記作 $\mathrm{rank}(M)$。

下來證明這樣的定義是有意義的

D. 若 M 是 $\mathcal{R}-$ 模, S 是它的子模, 稱

$$\vec{v} + S = \{\vec{v} + \vec{s} : \ \vec{s} \in S\}, \qquad \vec{v} \in M$$

爲 S 在 M 中的一個陪集, 所有 S 在 M 中的陪集作成的集合記作 M/S。這是一個 $R-$ 模, 其運算定義爲

$$(\vec{v} + S) + (\vec{u} + S) = \vec{v} + \vec{u} + S, \qquad r\,(\vec{v} + S) = r\,\vec{v} + S,$$

而 M/S 的零元素爲 $\vec{s} + S = \vec{0} + S = S$。這個 $\mathcal{R}-$ 模稱爲 M 關於 S 的商模 (quotient module)。

現在來證明: 若 M 是自由模, 則 M 的任意兩個基底有相同的基數。有了這個結果, 自由模 M 的秩才有意義。爲此, 要建立一些環的結果。

若 $\mathcal{R}$ 是有單位元素的交換環, $\mathcal{Q}$ 是 $\mathcal{R}$ 的理想, $\mathcal{Q}$ 在 $\mathcal{R}$ 中的陪集的集合 $\mathcal{R}/\mathcal{Q}$ 作爲一個環, 稱爲 $\mathcal{R}$ 關於 $\mathcal{Q}$ 的 商環 (quotient ring), 其加法與乘法定義爲

$$(a + \mathcal{Q}) + (b + \mathcal{Q}) = a + b + \mathcal{Q}, \qquad (a + \mathcal{Q})\,(b + \mathcal{Q}) = ab + \mathcal{Q}, \quad \forall\ a, b \in \mathcal{R}$$

要證明乘法有意義, 就要證明

$$b+\mathcal{Q}=b'+\mathcal{Q}\ \Rightarrow\ ab+\mathcal{Q}=ab'+\mathcal{Q},$$

也就是

$$b-b'\ \in\mathcal{Q}\ \Rightarrow\ a\,(b-b')\in\mathcal{Q},$$

由於 $\mathcal{Q}$ 是理想, 故上式成立。現在我們來證明下面的結果, 以說明極大理想的重要性。

引理 4.1.1: 若 $\mathcal{R}$ 是有單位元素的交換環, 商環 $\mathcal{R}/\mathcal{Q}$ 是體若且唯若當 $\mathcal{Q}$ 是極大理想 (即不存在 $\mathcal{R}$ 的理想 $\mathcal{I}$, 使得 $\mathcal{Q}\subsetneq\mathcal{I}\subsetneq\mathcal{R}$)。

證明: 若 $\mathcal{R}/\mathcal{Q}$ 是體, 且 $\mathcal{Q}$ 不是極大理想, 則存在理想 $\mathcal{I}$ 滿足 $\mathcal{Q}\subsetneq\mathcal{I}\subsetneq\mathcal{R}$。設 $i\in\mathcal{I}-\mathcal{Q}$, 考慮由 i 及 $\mathcal{Q}$ 生成的理想 :

$$\mathcal{K}=\langle i,\mathcal{Q}\rangle\ \subseteq\mathcal{I}.$$

由於 $i\notin\mathcal{Q}$, 故 $i+\mathcal{Q}\neq 0$。由於 $\mathcal{R}/\mathcal{Q}$ 是體, 故 $i+\mathcal{Q}$ 有反元素存在, 稱之爲 $i'+\mathcal{Q}$, 即

$$(i+\mathcal{Q})\,(i'+\mathcal{Q})=i\,i'+\mathcal{Q}=1+\mathcal{Q}.$$

所以 $1-i\,i'\in\mathcal{Q}\subseteq\mathcal{K}$。但 $i\,i'\in\mathcal{K}$, 故 $1\in\mathcal{K}$, 這便導出故 $\mathcal{K}=\mathcal{R}$。但 $\mathcal{K}\subseteq\mathcal{I}$, $\mathcal{I}$ 是 $\mathcal{R}$ 的眞部分集合, 這個矛盾導出 $\mathcal{Q}$ 是極大理想。

反之, 若 $\mathcal{Q}$ 是極大理想, $0\neq r+\mathcal{Q}$, 則 $r\notin\mathcal{Q}$, 故 $\mathcal{I}=\langle r,\mathcal{Q}\rangle$ 是嚴格地包含 $\mathcal{Q}$。因爲 $\mathcal{Q}$ 是極大理想, 故 $\mathcal{I}=\mathcal{R}$。這導出 $1\in\mathcal{I}$, 故有 $s\in\mathcal{R}$ 使得 $1=sr+i$ 對某個 $i\in\mathcal{Q}$ 成立。故

$$(s+\mathcal{Q})\,(r+\mathcal{Q})=sr+\mathcal{Q}=(1-i)+\mathcal{Q}=1+\mathcal{Q}.$$

即 $(r+\mathcal{Q})^{-1}=s+\mathcal{Q}$。所以 $\mathcal{R}/\mathcal{Q}$ 是體。定理因而證畢。

引理 4.1.2: 任意有單位元的交換環 $\mathcal{R}$ 一定有極大理想。

證明: 若 $\mathcal{R}$ 不是零環, 則一定有眞理想, 例如 $\{0\}$。若 I 爲 $\mathcal{R}$ 所有眞理想的集合, 則 I 爲非空集合, 若

$$\mathcal{Q}_1\ \subset\ \mathcal{Q}_1\ \subset\ \ldots$$

是 $\mathcal{R}$ 中眞理想鏈, 則 $\mathcal{I}=\cup_j\mathcal{Q}_j$ 也是一個理想。因爲 $1\notin\mathcal{I}$, 故 $I\in\mathcal{I}$。因此 I 中任何鏈都有上界, 由 Zorn 引理, I 有極大元素 (對照 2.1 節中向量空間與其基底存在1性的證明)。這證明了 $\mathcal{R}$ 有極大理想, 引理證畢。

定理 4.1.1: 若 M 是自由 $\mathcal{R}-$ 模, 則 M 的任意二個基底有相同的基數。

證明: 由引理4.1.2, $\mathcal{R}$ 有極大理想 $\mathcal{Q}$, 再由引理4.1.1知 $\mathcal{R}/\mathcal{Q}$ 是一個體。令

$$\mathcal{Q}\,M = \big\{a_1\vec{v}_1 + \cdots + a_n\vec{v}_n :\ a_j \in \mathcal{Q},\ \vec{v}_j \in M,\ \ j = 1, \ldots, n\big\},$$

則 $\mathcal{Q}\,M$ 是 M 的一個子模, 稱爲商模 $M/\mathcal{Q}\,M$。現在來證明 $M/\mathcal{Q}\,M$ 是體 $\mathcal{R}/\mathcal{Q}$ 上的一個向量空間, 爲此定義其數乘爲

$$(r + \mathcal{Q})(\vec{u} + \mathcal{Q}\,M) = r\,\vec{u} + \mathcal{Q}\,M,$$

這裡 $r \in \mathcal{R}$ 及 $\vec{u} \in M$。我們先要驗證這樣定義的數乘是有意義的, 換句話說, 我們要證明若 $r\,r' \in \mathcal{R}$, $\vec{u}\,\vec{u}' \in M$, 且

$$r + \mathcal{Q} = r' + \mathcal{Q},$$

及

$$\vec{u} + \mathcal{Q}\,M = \vec{u}' + \mathcal{Q}\,M$$

則

$$r\,\vec{u} + \mathcal{Q}\,M = r'\,\vec{u}' + \mathcal{Q}\,M.$$

也就是要證明若 $r - r' \in \mathcal{Q}$, $\vec{u} - \vec{u}' \in \mathcal{Q}\,M$, 則 $r\,\vec{u} - r'\,\vec{u}' \in \mathcal{Q}\,M$。

由於 $r - r' \in \mathcal{Q}$, $\vec{u} - \vec{u}' \in \mathcal{Q}\,M$, 則 $(r - r')\,\vec{u}' \in \mathcal{Q}\,M$ 及 $r\,(\vec{u} - \vec{u}') \in \mathcal{Q}\,M$。於是

$$(r - r')\,\vec{u}' + r\,(\vec{u} - \vec{u}') \ = r\,\vec{u} - r'\,\vec{u}' \in \mathcal{Q}\,M.$$

因此, 這樣定義的數乘是有意義的。可以直接驗證：這樣定義的數乘滿足在定義1.3.1(向量空間的定義) 中數乘滿足的四個條件, 而 $M/\mathcal{Q}\,M$ 顯然對加法成 Abel 群。故 $M/\mathcal{Q}\,M$ 的確是體 $\mathcal{R}/\mathcal{Q}$ 上的一個向量空間。

若 $\mathcal{B}$ 是自由 $\mathcal{R}-$ 模 M 上的一組基底, 且 $\vec{b}_j$, $\vec{b}_k \in \mathcal{B}$, $j \neq k$, 則 $\vec{b}_j + \mathcal{Q}\,M$ 與 $\vec{b}_k + \mathcal{Q}\,M$ 是不相同的。這可證明如下: 若

$$\vec{b}_j + \mathcal{Q}\,M = \vec{b}_k + \mathcal{Q}\,M, \qquad j \neq k$$

成立, 則 $\vec{b}_j - \vec{b}_k \in \mathcal{Q}\,M$, 故

$$\vec{b}_j - \vec{b}_k = a_1\,\vec{v}_1 + \cdot + a_n\,\vec{v}_n,$$

這裡 $a_k \in \mathcal{Q}$, $\vec{v}_k \in M$, $k = 1, \ldots, n$。由於每個 $\vec{v}_k$ 都是 $\mathcal{B}$ 中元素的線性組合。假設 $\vec{v}_k$ 中 $\vec{b}_j$ 的係數爲 α_k, 比較上式兩邊的 $\vec{b}_j$ 係數, 得到

$$1 = a_1\,\alpha_1 + \cdot + a_n\,\alpha_n,$$

而 $\alpha_k + \mathcal{Q}$, $k = 1, \ldots, n$, 故上式右邊屬於 $\mathcal{Q}$, 即 $1 \in \mathcal{Q}$, 這與 $\mathcal{Q}$ 是極大理想互相矛盾。所以, 當 $j \neq k$, $\vec{b}_j + \mathcal{Q}\,M$ 與 $\vec{b}_k + \mathcal{Q}\,M$ 是不相同的。因此

$$\mathcal{B}' = \left\{ \vec{b} + \mathcal{Q}\,M \,:\, \vec{b} \in \mathcal{B} \right\}$$

與 M 的基底 $\mathcal{B}$ 有相同的基數。

繼續來證明 $\mathcal{B}'$ 是 $\mathcal{R}/\mathcal{Q}$ 上的一個向量空間 $M/\mathcal{Q}\,M$ 的一組基底。由於 $\mathcal{B}$ 生成 M, 故 $\mathcal{B}'$ 生成 $M/\mathcal{Q}\,M$。要先證 $\mathcal{B}'$ 線性獨立。若

$$\sum_{j=1}^{n} (\alpha_j + \mathcal{Q})\,(\vec{b}_j + \mathcal{Q}\,M) = \vec{0},$$

則 $\sum_{j=1}^{n} (\alpha_j\,\vec{b}_j + \mathcal{Q}\,M) = \vec{0}$, 也就是 $\sum_{j=1}^{n} \alpha_j\,\vec{b}_j \in \mathcal{Q}\,M$, 於是

$$\sum_{j=1}^{n} \alpha_j\,\vec{b}_j = \sum_{j=1}^{n} a_j\,\vec{b}_j,$$

這裡 $a_j \in \mathcal{Q}$, $j = 1, \ldots, n$。兩邊相等導出 $\alpha_j \in \mathcal{Q}$, $j = 1, \ldots, n$。於是 $\alpha_j + \mathcal{Q} = 0$, 即 $\mathcal{R}/\mathcal{Q}$ 中的零元素, $j = 1, \ldots, n$。故 $\mathcal{B}'$ 爲線性獨立。因此, $\mathcal{B}'$ 的確是向量空間 $M/\mathcal{Q}\,M$ 的一組基底。而 $\mathcal{B}$ 的基數 $= \dim\,(M/\mathcal{Q}\,M)$, 不依賴於 $\mathcal{B}$ 的選取。

定理2.1.1告訴我們, 體 $\mathbb{F}$ 上兩個向量空間同構若且唯若它們的維數相同。在模的情形, 有如下定理。

定理 4.1.2: 兩個自由 $\mathcal{R}-$ 模同構若且唯若它們有相同的秩。

證明: 若 M 與 N 爲兩個自由 $\mathcal{R}-$ 模。假設 $M \approx N$ 則從 M 到 N 的任意同構映射 T 將 M 的一組基底映爲 N 的一組基底。由於 T 是雙射, 故 $\mathrm{rank}(M) = \mathrm{rank}(N)$。反之, 若 $\mathrm{rank}(M) = \mathrm{rank}(N)$ 而 $\mathcal{B}$ 是 M 的一組基底, $\mathcal{C}$ 是 N 的一組基底, 則由於 $\mathcal{B}$ 與 $\mathcal{C}$ 的基數相同, 故有雙射 $T : \mathcal{B} \to \mathcal{C}$, 這個映射可線性擴充到整個 M 到整個 N 上的同構, 所以, $M \approx N$。

當 $\mathcal{R}-$ 模 M 的秩數 n 爲有限時, 易見 $M \approx \mathbb{R}^n$。

E. 由於有限生成 $\mathcal{R}-$ 模 M 的子模未必是有限生成的, 因此, 要討論在什麼條件下有限生成 $\mathcal{R}-$ 模 M 的子模也是有限生成的便成爲一個有趣的問題。這個條件就是我們下面要講的升鏈條件。

定義 4.1.4: 一個 $\mathcal{R}-$ 模 M 稱爲滿足子模的升鏈條件 (ascending chain condition), 如果對 M 的任何子模序列

$$S_1 \subset S_2 \subset S_3 \subset \cdots$$

存在指標 k, 使得 $S_k = S_{k+1} = S_{k+2} = \cdots$。子模升鏈條件記爲 a.c.c.。

定理 4.1.3: $\mathcal{R}-$ 模 M 的每個子模是有限生成的若且唯若 M 滿足子模的升鏈條件。

定理中的模稱爲 Noether 模 (Noetherian module)。

證明: 若 M 的所有的子模都是有限生成, 而 M 有無窮上升子模序列

$$S_1 \subset S_2 \subset S_3 \subset \cdots$$

易見 $S = \cup_j S_j$ 也是 M 的子模, 故 S 也是有限生成的。若 $S = \langle \vec{u}_1, \ldots, \vec{u}_n \rangle$, $\vec{u}_j \in M$, $j = 1, \ldots, n$。由於 $\vec{u}_j \in S$, 故有指標 k_j, 使得 $\vec{u}_j \in S_{k_j}$。令 $k = \max\{k_1, \ldots, k_n\}$, 則

$$\vec{u}_j \in S_k, \qquad j = 1, \ldots, n.$$

因此

$$S = \langle \vec{u}_1, \ldots, \vec{u}_n \rangle \subset S_k \subset S_{k+1} \subset S_{k+2} \subset \cdots \subset S.$$

這表明上升子模序列 $S_1 \subset S_2 \subset S_3 \subset \ldots$ 從 S_k 起是相同的。

反之, 若 M 滿足子模的升鏈條件且 S 是 M 的子模。取 $\vec{u}_1 \in S$, 考慮子模 $S_1 = \langle \vec{u}_1 \rangle \subset S$, 若 $S_1 = S$, 則 S 就是有限生成。若 $S_1 \neq S$, 於是有 $\vec{u}_2 \in S \setminus S_1$。令 $S_2 = \langle \vec{u}_1, \vec{u}_2 \rangle$。若 $S_2 = S$, 則 S 就是有限生成。若 $S_2 \neq S$, 於是有 $\vec{u}_3 \in S \setminus S_2$。考慮子模 $S_3 = \langle \vec{u}_1, \vec{u}_2\, \vec{u}_3 \rangle$。一直這樣進行下去, 就得到一個子模上升鏈

$$\langle \vec{u}_1 \rangle \subset \langle \vec{u}_1, \vec{u}_2 \rangle \subset \langle \vec{u}_1, \vec{u}_2\, \vec{u}_3 \rangle \subset \cdots S.$$

如果這樣的子模沒有一個等於 S, 就得到一個子模的無窮上升序列, 前一個爲後一個所眞包含, 這與 M 滿足子模的升鏈條件相互矛盾。故有某個 n, 使得 $S = \langle \vec{u}_1, \ldots \vec{u}_n \rangle$, 換句話說, S 是有限生成。定理因而證畢。

由於環 $\mathcal{R}$ 是自己上的模, 且模 $\mathcal{R}$ 的子模就是環 $\mathcal{R}$ 的理想, 故定義4.1.4及定理4.1.3成爲如下定義:

定義 4.1.5: 環 $\mathcal{R}$ 成爲滿足理想的升鏈條件, 若對 $\mathcal{R}$ 的任意上升理想序列

$$\mathcal{Q}_1 \subset \mathcal{Q}_2 \subset \mathcal{Q}_3 \subset \cdots$$

一定存在指標 k, 使得 $\mathcal{Q}_k = \mathcal{Q}_{k+1} = \mathcal{Q}_{k+2} = \cdots$。

在1.2節中證明了主理想環一定滿足升鏈條件。

定理 4.1.4: 環 $\mathcal{R}$ 的每個理想是有限生成若且唯若 $\mathcal{R}$ 滿足理想的升鏈條件。

定理中的環成爲Noether 環 (Noetherian ring)。下面要證明一條重要的定理。

定理 4.1.5: 若 $\mathcal{R}$ 是 Noether 環, 則任意有限生成的 $\mathcal{R}-$ 模是 Noether 模。

這條定理說, 若 $\mathcal{R}$ 是 Noether 環, 即每個理想是有限生成的, 則有限生成的 $\mathcal{R}-$ 模的每個子模也是有限生成的。這就給出了條件使有限生成的子模依然是有限生成的。

證明: 若 M 是有限生成的 $\mathcal{R}-$ 模, $M = \langle \vec{u}_1, \ldots \vec{u}_n \rangle$。考慮滿射同態 $T : \mathcal{R}^n \to M$ 定義爲

$$T(\alpha_1, \alpha_2, \ldots, \alpha_n) = \sum_{j=1}^{n} \alpha_j \vec{u}_j, \quad \alpha_j \in \mathcal{R}, \;\; j = 1, \ldots, n.$$

若 S 是 M 的一個子模, 則

$$T^{-1}(S) = \left\{ \vec{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{R}^n : \;\; T(\vec{\alpha}) \in S \right\}$$

是 $\mathcal{R}^n$ 的一個子模, 且 $T(T^{-1}(S)) = S$。假設 $\mathcal{R}^n$ 只有有限生成子模, 則 $T^{-1}(S)$ 是有限生成的, $T^{-1}(S) = \langle \vec{\beta}_1, \vec{\beta}_2, \ldots, \vec{\beta}_k \rangle$。於是若 $\vec{w} \in S$, 則有 $\vec{\beta} \in T^{-1}(S)$, 使得 $\vec{w} = T(\vec{\beta})$。由於

$$\vec{\beta} = \gamma_1 \vec{\beta}_1 + \gamma_2 \vec{\beta}_2 + \cdots + \gamma_k \vec{\beta}_k, \quad \gamma_j \in \mathcal{R}, \;\; j = 1, \ldots, k,$$

故

$$\vec{w} = T(\vec{\beta}) = \gamma_1 T(\vec{\beta}_1) + \gamma_2 T(\vec{\beta}_2) + \cdots + \gamma_k T(\vec{\beta}_k).$$

於是 S 由 $\{T(\vec{\beta}_1), T(\vec{\beta}_2), \ldots, T(\vec{\beta}_k)\}$ 所有限生成。所以餘下要證明的只是 $\mathcal{R}^n$ 的每一個子模都是有限生成的。

當 $n = 1$ 時這是對的, 因爲 $\mathcal{R}$ 是 Noether 環。假設對所有 $1 \leq k < n$, $\mathcal{R}^k$ 只有有限生成的子模; 若 S 是 $\mathcal{R}^n$ 的子模, 令

$$S_1 = \left\{ \vec{\alpha} \in S : \;\; \vec{\alpha} = (s_1, s_2, \ldots, s_{n-1}, 0), \;\; s_j \in \mathcal{R} \right\}$$

及

$$S_2 = \left\{ (0, 0, \ldots, 0, s_n), \;\; (s_1, s_2, \ldots, s_{n-1}, s_n) \in S, \;\; s_1, \ldots, s_n \in \mathcal{R} \right\}$$

於是 S_1 同構於 $\mathcal{R}^{n-1}$ 的一個子模 (只要將 S_1 的每個元素的最後一個座標去掉)。由數學歸納法的假設, S_1 是有限生成的。令 $S_1 = \langle \mathcal{B} \rangle$, 而 $\mathcal{B} = \{\vec{\nu}_1, \ldots, \vec{\nu}_k\}$, $0 \leq k \leq n-1$ (若 S_1 爲空集合, 則 $\mathcal{B}$ 爲空集合而 $k = 0$)。

同樣 S_2 同構於 $\mathcal{R}$ 的一個子模 (即理想), 因此是有限生成的。若 S_2 是平凡的, 則 S 的每個元素的最後一個座標爲 0, 故 $S = S_1$ 是有限生成的。若 S_2 是非平凡的, 而由 $(0, 0, \ldots, 0, b_n)$, $b_n \neq 0$ 所生成; 在 S 中有 $\vec{b} = (b_1, b_2, \ldots, b_{n-1}, b_n) \in S$, 則 $\mathcal{B}' = \{\vec{b}\} \cup \mathcal{B}$ 生

成 S。這是因爲：若 $\vec{\alpha} = (s_1, \ldots, s_n) \in S$, 則 $(0, \ldots, 0, s_n) \in S_2$, 故有 $\gamma \in \mathcal{R}$, 使得 $(0, \ldots, 0, s_n) = \gamma(0, \ldots, 0, b_n)$, 即 $s_n = \gamma b_n$, 因此 $\vec{\alpha} - \gamma\vec{b} \in S_1$, 於是 $\vec{\alpha} \in \gamma\vec{b} + S_1$, 這就是 $\mathcal{B}'$ 生成 S。定理因而證畢。

因爲定理4.1.5的關係, 導致我們去研究那些環是 Noether 環。

我們在此證明: 有單位元的交換環 $\mathcal{R}$ 是體若且唯若當它只有理想 $\{0\}$ 及 $\mathcal{R}$, 而無其它理想。因此, 由定理4.1.4, 體當然是 Noether 的, 當 $\mathcal{R}$ 是主理想整環時, 由於所有的理想都是主理想; 因此, 主理想整環也是 Noether 的。下面給出十分重要的 Hilbert 定理。這是一個十分有用的基本定理。

定理4.1.6 (Hilbert **基本定理**): 若環 $\mathcal{R}$ 是 Noether 環, 則多項式環 $\mathcal{R}[x]$ 也是 Noether 環。

證明: 要證的是 $\mathcal{R}[x]$ 的任意一個理想 $\mathcal{Q}$ 是有限生成的。令 L_j 爲 $\mathcal{Q}$ 中所有 j 次多項式最高項的係數及 $\mathcal{R}$ 中的零元素所成的集合, $j = 0, 1, \ldots$。不難看出 L_j 都是 $\mathcal{R}$ 的理想, 這是因爲對 $a, b \in L_j$, $a \neq 0$, $b \neq 0$, 存在 j 次多項式

$$f(x) = a\,x^j + \cdots \in \mathcal{Q}, \qquad g(x) = b\,x^j + \cdots \in \mathcal{Q}.$$

於是

$$f(x) - g(x) = (a - b)\,x^j + \cdots$$

必屬於 $\mathcal{Q}$。若 $a - b \neq 0$, 則 $a - b \in L_j$; 若 $a - b = 0$, 但由於 $0 \in L_j$, 則必有 $a - b \in L_j$。對於任一個 $c \in \mathcal{R}$, $c\,f(x) = c\,a\,x^j + \cdots \in \mathcal{Q}$。若 $c\,a \neq 0$, 則 $c\,a \in L_j$; 若 $c\,a = 0$, 但由於 $0 \in L_j$, 則必有 $c\,a \in L_j$; 所以 L_j 是 $\mathcal{R}$ 中的一個理想。若 $f(x) = a\,x^j + \cdots \in \mathcal{Q}$, 由於 $\mathcal{Q}$ 是 $\mathcal{R}[x]$ 的一個理想,

$$x\,f(x) = a\,x^{j+1} + \cdots \in \mathcal{Q}.$$

因此, 若 $a \in L_j$, 則 $a \in L_{j+1}$, 於是得到一個理想升鏈

$$L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots.$$

因爲 $\mathcal{R}$ 是 Noether 環, 故存在 d 使得

$$L_d = L_{d+1} = L_{d+2} = \cdots = L.$$

其中 $L = \cup_{j \geq 0} L_j$。因爲 $\mathcal{R}$ 是 Noether 環, 所以每個 L_j, $j = 0, 1, \ldots, d$ 都是有限生成的。設 $L_j = \langle a_j^{(1)}, \ldots, a_j^{(k_j)} \rangle$, $j = 0, 1, \ldots, d$。從而由 L_j 的定義知道, 有 $\mathcal{Q}$ 的多項式 $f_j^{(1)}, \ldots, f_j^{(k_j)}$, 使得 $f_j^{(\ell)}$ 的首項係數爲 $a_j^{(\ell)}$, $\ell = 1, \ldots, k_j$。

我們可以證明: $S = \{f_0^{(1)}, \ldots, f_0^{(k_0)}, f_1^{(1)}, \ldots, f_1^{(k_1)}, \ldots, f_d^{(1)}, \ldots, f_d^{(k_d)}\}$ 是理想 $\mathcal{Q}$ 的生成集。

爲此, 設 $f \in \mathcal{Q}$, $\deg(f) = n$。對 n 用數學歸納法。若 $n < d$, 則 $a_n = \sum_{1\le i\le k_n} r_i\, a_n^{(i)}$, $r_i \in \mathcal{R}$。於是多項式

$$h = f - \sum_{1\le i\le k_n} r_i\, f_n^{(i)}$$

的次數小於 n, 從而由數學歸納法的假設知 h 可由 S 中的元素生成, 進而 f 可由 S 中的元素生成。

若 $n \ge d$, 則 $a_n \in L_n = L_d$, 故 $a_n = \sum_{1\le i\le k_d} r_i\, a_d^{(i)}$, $r_i \in \mathcal{R}$。於是多項式

$$h = f - \sum_{1\le i\le k_d} r_i\, x^{n-d} f_d^{(i)}$$

的次數小於 n, 從而由數學歸納法的假設知 h 可由 S 中的元素生成, 進而 f 可由 S 中的元素生成。定理因而證畢。

4.2. 主理想整環上的模

A. 在上一節中給出了有單位元的交換環 $\mathcal{R}$ 上的模的定義以及它的一些性質。當環 $\mathcal{R}$ 爲體時, 模就是向量空間, 至於向量空間中的部分基本概念與定理, 有些可以移植到模上來。例如子空間、商空間、直和、生成集合、線性獨立、基底、維數、線性變換、核與像等等, 到了模理論中有相對應的名詞與定義。例如, 與子空間、商空間、維數與線性變換相對應的爲子模、商模、秩與模同態等。但是模與向量空間, 從表面上看, 只是建立在環與體上的差別, 但相互之間卻存在著本質上的差異。這裡舉出一些事實, 而不加以證明。

1. 存在這樣的模, 它沒有線性獨立的元素。當然就沒有基底。這就是爲什麼要引入自由模的原因。
2. 存在這樣的模, 它的子模無補集。
3. 存在這樣的有限生成模, 其子模不是有限生成的。這就是爲什麼引入 Noether 模的原因。
4. 存在這樣的模, 它的線性相依集合 S 中的任一元素不能用 S 中其它元素的線性組合來表示。
5. 存在這樣的模, 其極小生成集合不是模的基底, 其極大線性獨立集合不是模的基底。
6. 存在這樣的自由模, 其子模不自由, 其商模不自由。
7. 若 $\mathcal{V}$ 是體 $\mathbb{F}$ 上的向量空間, $\alpha \in \mathbb{F}$, $\vec{v} \in \mathcal{V}$, $\alpha \ne 0$ 及 $\vec{v} \ne \vec{0}$, 則 $\alpha\,\vec{v} \ne \vec{0}$。但在模的情形, 這不再永遠成立。

8. 存在這樣的自由模, 有線性獨立集合不包在基底中, 有生成集合不包有基底。

由於在一般的有單位元的交換環 $\mathcal{R}$ 上的模有種種不很理想的性質, 這才導致了我們專門來討論主理想環上的模的理論。這是因爲主理想環有很多很好的性質, 這就導出了在其上的模也有很多很好的性質, 因而情況大爲改觀。例如上述 (6) 中, 在主理想整環上自由模的子模也是自由的, 等等。這一講中針對著理想整環上的模進行研究之後, 在下一講中以此來考慮向量空間中的一些問題, 我們便可以得到一系列重要的結果。

B. 現在我們來證明下面的定理：

定理 4.2.1: 主理想整環 $\mathcal{R}$ 上自由模 M 的任意子模 S 也是自由的, 且 $\operatorname{rank}(S) \leq \operatorname{rank}(M)$。

證明: 我們只證明模的秩是有限的情形, 儘管秩爲無限時這也成立。由定理 4.1.2 知, 若 $\operatorname{rank}(M) = n$, 則 $M \approx \mathcal{R}^n$。因此, 我們直接來討論 $\mathcal{R}^n$ 即可。現在對 n 用數學歸納法。

當 $n = 1$ 時, $M = \mathcal{R}$, $\mathcal{R}$ 的任意子模 S 就是 $\mathcal{R}$ 的理想。由於 $\mathcal{R}$ 是主理想環, 即 $S = \langle a \rangle$。設 $S \neq \{0\}$。因 $\mathcal{R}$ 是整環, 故對所有 $r \neq 0$, 我們知道 $ra \neq 0$。因此, 映射

$$\sigma : \mathcal{R} \to S, \qquad \sigma(r) = ra$$

是 $\mathcal{R}$ 到 S 的同構, 故 S 是自由的。

假設當 $k < n$ 時, $\mathcal{R}^k$ 的子模是自由的。令 S 是 $\mathcal{R}^k$ 的一個子模。考慮

$$S_1 = \{\alpha \in S : s_1, \ldots, s_{n-1} \in \mathcal{R}, \ \alpha = (s_1, \ldots, s_{n-1}, 0)\}$$

及

$$S_2 = \{(0, \ldots, 0, s_n) : s_1, \ldots, s_{n-1} \in \mathcal{R}, \ \alpha = (s_1, \ldots, s_{n-1}, s_n) \in S\}.$$

因爲 S_1 同構於 $\mathcal{R}^{n-1}$ 的一個部分集合, 由數學歸納法的假設, 這是自由的。設 $\mathcal{B} = \{\alpha_1, \ldots, \alpha_k\}$ 是 S_1 的基底, 其中 $k \leq n-1$ (若 S_1 是平凡的, 則 $\mathcal{B}$ 是空集合)。

同樣, S_2 同構於 $\mathcal{R}$ 的一個子模 (理想)。若 S_2 是平凡的, 則 S 中每個元素的最後座標是 0, 故 $S = S_1$ 是自由的。若 S_2 非平凡, 則有秩 1, 基底爲 $\{(0, \ldots, 0, t_n), \ t_n \neq 0\}$, 且 $\beta = (t_1, \ldots, t_{n-1}, t_n) \in S$。現在我們來證明 $\mathcal{B}' = \{\beta\} \cup \mathcal{B}$ 是 S 的基底。先證 $\mathcal{B}'$ 是線性獨立的。若有 $b, a_1, \ldots, a_k \in \mathcal{R}$ 使得

$$b\,\beta + a_1\alpha_1 + \cdots + a_k\alpha_k = 0,$$

則

$$b\,\beta = -\big(a_1\alpha_1 + \cdots + a_k\alpha_k\big).$$

比較兩邊的最後座標, 我們得到 $b\,t_n = 0$, 所以 $b = 0$。而由 $\alpha_1, \ldots, \alpha_k$ 的線性獨立導出 $a_j = 0, j = 1, \ldots, k$, 故 $\mathcal{B}'$ 是線性獨立的。其次, 若 $\alpha = (s_1, \ldots, s_n) \in S$, 則 $(0, \ldots, 0, s_n) \in S_2$, 所以 $(0, \ldots, 0, s_n) = b\,(0, \ldots, 0, t_n)$, $b \in \mathcal{R}$, 即 $s_n = b\,t_n$。於是 $\alpha - b\,\beta \in S_1$, 也就是 $\alpha = b\,\beta + S_1$, 因此 $\mathcal{B}'$ 生成 S; 故 S 是自由的。這就證明了定理。

在 A 的第 7 點中我們提到, 體 $\mathbb{F}$ 上的向量空間 $\mathcal{V}$, 若 $a \neq 0$, $a \in \mathbb{F}$, $\vec{v} \neq \vec{0}$, $\vec{v} \in \mathcal{V}$, 則 $a\,\vec{v} \neq \vec{0}$, 但在模的情形, 這不一定成立。於是有下面的定義 :

定義 4.2.1: 若 $\mathcal{R}$ 是整環, M 是 $\mathcal{R}$ 的模。對 $v \in M$, 如果有非零的 $a \in \mathcal{R}$ 使得 $a\,v = 0$, 則稱 v 是 M 的一個撓元素 (torsion element)。一個模如果不包含撓元素則稱爲 無撓的 (torsion free)。如果模的所有元素是撓元素, 則稱 M 是 撓模 (torsion module)。

若 M 爲模, 其所有撓元素所組成的集合記作 M_{tor}, 不難看出這是 M 的一個子模, 且 M/M_{tor} 是一個無撓模。這可證明如下 : 若 $a, b \in M_{tor}$, 則有 $\alpha, \beta \in \mathcal{R}$, $\alpha \neq 0$ 及 $\beta \neq 0$ 使得 $\alpha\,a = 0$ 及 $\beta\,b = 0$。於是對任意的 $r, s \in \mathcal{R}$, 我們有 $\alpha\,\beta\,(r\,a + s\,b) = 0$, 即 $r\,a + s\,b \in M_{tor}$。由 4.1 節第 2 項中 (1) 知, M_{tor} 是一個子模。現在我們再證 M/M_{tor} 是一個無撓模。若 $a + M_{tor}$ 是 M/M_{tor} 中的一個撓元素, 則存在 $r \in \mathcal{R}$, $r \neq 0$, 使得 $r(a + M_{tor}) = 0$, 即 $ra \in M_{tor}$ 。於是有 $s \in \mathcal{R}$, $s \neq 0$, 使得 $s(r\,a) = (s\,r)\,a = 0$, 且 $s\,r \neq 0$, 故 $a \in M_{tor}$, 於是 M/M_{tor} 中的撓元素是零, 即 M/M_{tor} 爲無撓模。

其次, 不難看出主理想整環上任意自由模是無撓的, 但反之不眞; 不過我們有如下的定理。

定理 4.2.2: 主理想整環上模 M 如果是無撓的, 且是有限生成的, 則模是自由的。

證明: 由於 M 是有限生成的, 故有 $\vec{0} \neq \vec{v}_j \in M$, $j = 1, \ldots, n$, 使得 $M = \langle \vec{v}_1, \ldots, \vec{v}_n \rangle$。在這些生成元素中取極大線性獨立部分集合 $S = \{\vec{u}_1, \ldots, \vec{u}_k\}$, 將 M 的生成元素重新寫成

$$M = \langle \vec{u}_1, \ldots, \vec{u}_k, \vec{v}_1, \ldots, \vec{v}_{n-k} \rangle.$$

於是對每個 $\vec{v}_i$, $i = 1, \ldots, n-k$, 集合 $\{\vec{u}_1, \ldots, \vec{u}_k, \vec{v}_j\}$ 是線性相依的。所以對每個 $\vec{v}_i$, 存在 $0 \neq \alpha_i$ 及 $\beta_1^{(i)}, \ldots, \beta_k^{(i)}$ 使得

$$\alpha_i\,\vec{v}_i + \beta_1^{(i)}\,\vec{u}_1 + \cdots + \beta_k^{(i)}\,\vec{u}_k = \vec{0}.$$

令 $\alpha = \alpha_1 \cdots \alpha_{n-k}$, 則 $\alpha\,\vec{v}_i \in \mathrm{span}(S)$, $i = 1, \ldots, n-k$。於是

$$\alpha\,M = \{\alpha\,\vec{v} : \vec{v} \in M\}$$

是 $\mathrm{span}(S)$ 的一個子模。但 $\mathrm{span}(S)$ 是自由模, 其基底爲 S, 故由定理 4.2.1, $\alpha\,M$ 也是自由的。考慮映射

$$\Phi\,(\vec{v}) = \alpha\,\vec{v}$$

是一個映成同態, 由於 M 是無撓的, 所以 Φ 也是一對一的, 所以 $M \approx \alpha M$, 故得知 M 是自由的, 定理因而證畢。

4.3. 主理想整環上的有限生成模的分解定理

有了以前這些準備之後, 要進入本講的主題, 給出主理想整環上有限生成模的分解定理。這需要三個步驟來建立起這些重要的定理。

1. 第一步, 將主理想整環上有限生成模分解爲撓模與自由模之直和。

定理 4.3.1: 若 M 是主理想整環 $\mathcal{R}$ 上的有限生成模, 則

$$M = M_{tor} \oplus M_{free},$$

這裡 M_{free} 是一個自由 $\mathcal{R}-$ 模。並且這種分解是唯一的, 即若還有分解 $M = T \oplus N$, 其中 T 是 M 的無撓子模, N 是 M 的自由子模, 則 $T \equiv M_{tor}$, $N \equiv M_{free}$。

證明: 由於商模 M/M_{tor} 是無撓的以及當 M 是有限生成時, M/M_{tor} 也是有限生成的, 故由定理4.2.2知 M/M_{tor} 是自由模。

有了定理 4.3.1 要討論主理想整環有限生成模的分解, 只要討論主理想整環上有限生成撓模的分解。

2. 第二步, 將主理想整環上有限生成撓模分解爲准素子模的直和。在 2.2 節中, 我們曾引入了向量空間零化子的概念。現將此概念擴充到模上。

定義 4.3.1: 若 M 是一個 $\mathcal{R}-$ 模, $v \in M$ 的零化子 爲

$$\mathrm{ann}(v) = \big\{r \in \mathcal{R} : \ rv = 0\big\},$$

M 的 零化子爲

$$\mathrm{ann}(M) = \big\{r \in \mathcal{R} : \ rM = \{0\}\big\},$$

這裡 $rM = \big\{rv : \ v \in M\big\}$.

顯然 $\mathrm{ann}(v)$ 及 $\mathrm{ann}(M)$ 是 $\mathcal{R}$ 中的裡想。

若 M 是主理想整環上有限生成的撓模, $\mathrm{ann}(v)$ 生成元稱爲 v 的 階 (order), $\mathrm{ann}(M)$ 的生成元稱爲 M 的階。顯然, 若 μ, ν 是 M (或 $v \in M$) 的兩個階, 則它們是相伴的 (associate), 即存在某個可逆元 $u \in \mathcal{R}$ 使得

$$\mathrm{ann}(M) = \langle\mu\rangle = \langle\nu\rangle \ \Rightarrow \ \mu = u\nu.$$

故 M 的階, 除去乘以可逆元外, 是唯一確定的。μ, ν 除去乘以可逆元外, 由定理 1.2.3 有相同的素元 (prime element) 乘積分解。

定義 4.3.2: 模 M 稱爲准素模 (prime module), 若其零化子爲 $\mathrm{ann}(M) = \langle p^e \rangle$。這裡 p 是素元, $e \in \mathbb{N}$。換句話說, 若 M 的階是某個素元的正次方, 則 M 是一個准素模。

顯然, 主理想整環上有限生成的撓模 M 是一個准素模若且唯若當 M 中每個元素的階是一個固定的素元的冪。

分解定理的第二步是將撓模 M 分解爲准素子模的直和。

定理 4.3.2 (**准素模唯一分解定理**): 若 M 是一個主理想整環上非零有限生成的撓模, 階爲

$$\mu = p_1^{e_1} \cdots p_n^{e_n},$$

這裡 p_j, $j = 1, \ldots, n$, 爲互不相伴的素元, 則 M 可分解爲直和

$$M = M_{p_1} \oplus \cdots \oplus M_{p_n},$$

這裡

$$M_{p_j} = \big\{ v \in M : \ \ p_j^{e_j} v = 0 \big\}$$

爲准素子模, 階爲 $p_j^{e_j}$, $j = 1, \ldots, n$。尤有進者, 這樣的分解是唯一的, 也就是說, 若還有分解

$$M = N_1 \oplus \cdots \oplus N_m,$$

其中 N_k 是階爲 $q_k^{f_k}$ 的准素模, 則 $m = n$, 且可適當安排下標 j 使得 $N_j = M_{p_j}$, q_j 與 p_j 相伴, $e_j = f_j$, $j = 1, \ldots, n$。

證明: 假設 $\mu = pq$, 且 p, q 的最大公因子 $\gcd(p, q) = 1$。考慮集合

$$M_p = \big\{ v \in M : \ \ pv = 0 \big\},$$

以及

$$M_q = \big\{ v \in M : \ \ qv = 0 \big\}.$$

我們現在要證明 $M = M_p \oplus M_q$ 以及 M_p 與 M_q 分別有零化子 $\langle p \rangle$ 與 $\langle q \rangle$。

由於 p 與 q 互質, 所以理想 $\langle p, q \rangle$ 由 $\gcd(p, q) = 1$ 生成 (證明與命題 1.2.1 之證明相同), 故 $1 \in \langle p, q \rangle$。因此存在 $a, b \in \mathcal{R}$ 使得

$$ap + bq = 1.$$

若 $v \in M_p \oplus M_q$, 則 $pv = qv = 0$。故

$$v = 1 \cdot v \ = \ (ap + bq) \cdot v = 0.$$

因此, $M_p \cap M_q = \{0\}$。

對任意 $v \in M$, 我們有

$$v = 1 \cdot v \ = \ apv + bqv,$$

而 $q(apv) = a(pq)v = a\mu v = 0$, 故 $apv \in M_q$; 同樣 $bqv \in M_p$。因此, $M = M_p \oplus M_q$。若 $rM_p = 0$, 則對任意 $v = v_1 + v_2 \in M_p \oplus M_q = M$, 有

$$rqv = rq \cdot (v_1 + v_2) \ = \ rqv_1 + rqv_2 = 0,$$

因此, $rq \in \text{ann}(M)$; 這導出 $\mu = pq \big| rq$, 即 $p \big| r$。這說明 $\text{ann}(M_p) = \langle p \rangle$。同理可證 $\text{ann}(M_q) = \langle q \rangle$。

若 μ 是素元的乘積

$$\mu = p_1^{e_1} \cdots p_n^{e_n},$$

由上面的證明知道有 $M = M_{p_1^{e_1}} \oplus N$, 這裡 N 爲具有零化子 $\langle \mu / p_1^{e_1} \rangle$ 的子模; 重複這個步驟, 記 $M_{p_j^{e_j}}$ 爲 M_{p_j}, $j = 1, \ldots, n$, 就得到定理中的分解。

至於分解的唯一性, 注意到由 $M = N_1 \oplus N_2 \oplus \cdots \oplus N_m$ 知 $\text{ann}(M) = \langle q_1^{f_1}, \ldots, q_n^{f_n} \rangle$, 因此 $q_1^{f_1} \cdots q_n^{f_n}$ 與 $p_1^{e_1} \cdots p_n^{e_n}$ 相伴。由定理1.2.3, 知 $\mathcal{R}$ 是唯一因子分解環, 所以 $n = m$, 且可適當安排下標 j 使得 $N_j = M_{p_j}$, q_j 與 p_j 相伴, $e_j = f_j$, $j = 1, \ldots, n$, 從而

$$N_j = \left\{ v \in M : \ q_j^{f_j} v = 0 \right\} = \left\{ v \in M : \ p_j^{e_j} v = 0 \right\} = M_{p_j},$$

$j = 1, \ldots, n$, 定理的證明於是完畢。

3. 第三步由定理4.3.2知, 下一步就應該對定理4.3.2中那些准素子模 M_{p_j}, $j = 1, \ldots, n$, 進行分解。

定理 4.3.3 (**循環分解定理**): 若 M 是主理想整環 $\mathcal{R}$ 上非零准素有限生成撓模, 其階爲 p^e, 則 M 可分解爲循環子模的直和:

$$M = \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_n. \tag{4.3.1}$$

$\mathcal{C}_j$ 爲有階 p^{e_j} 的循環子模, $j = 1, \ldots, n$, 且滿足

$$e = e_1 \ \geq \ e_2 \ \geq \ \ldots \ \geq \ e_n \ \geq \ 1,$$

或等價於

$$p \,\big|\, p^{e_n}, \quad p^{e_n} \,\big|\, p^{e_{n-1}}, \ \ldots\ , p^{e_2} \,\big|\, p^{e_1}. \tag{4.3.2}$$

證明: 先來證明在 M 中一定存在一個元素 v_1, 使得

$$\mathrm{ann}(v_1) = \mathrm{ann}(M) = \langle p^e \rangle.$$

如果這樣的 $v \in M$ 不存在, 那麼對所有的 $\mathrm{ann}(v) = \langle p^k \rangle$, 而 $k < e$。故 $p^{e-1} \in \mathrm{ann}(M)$, 這導出 $p^e \,\big|\, p^{e-1}$, 因而矛盾。

如果能證循環子模 $\langle v_1 \rangle$ 是 M 分解中的一個被加項, 即

$$M = \langle v_1 \rangle \oplus S_1, \tag{4.3.3}$$

這裡 S_1 是 M 中的某個子模, 於是 S_1 也是一個在 $\mathcal{R}$ 上的有限生成准素撓模, 以至可以重複這個步驟, 得到

$$M = \langle v_1 \rangle \oplus \langle v_2 \rangle \oplus S_2.$$

這裡 $\mathrm{ann}(v_2) = \langle p^{e_2} \rangle$, 而 $e_2 \le e_1$。這樣一直進行下去, 我們便得到一個上升子模序列

$$\langle v_1 \rangle \ \subset\ \langle v_1 \rangle \oplus \langle v_2 \rangle \ \subset\ \ldots.$$

由於 $\mathcal{R}$ 是主理想整環, 故 $\mathcal{R}$ 是 Noether 環。由於 M 是有限生成的, 根據定理 4.1.5, M 是 Noether 模, 由定理 4.1.4, M 滿足升鏈條件, 於是上述子模鏈到有限步停止。這就證明了 M 可以分解爲循環子模 $\langle v_j \rangle$, $j = 1, \ldots, n$ 的直和, 其相應的階爲 p^{e_j}, $j = 1, \ldots, n$, 且 $e = e_j \ge e_2 \ge \cdots \ge e_n \ge 1$。現在來證明 M 可以分解爲 $M = \langle v_1 \rangle \oplus S_1$。由於 M 是有限生成的, 故有 $M = \langle v_1, u_1, \ldots, u_k \rangle$。對 k 進行歸納法。若 $k = 0$, 則只要令 $S_1 = \{0\}$ 即可; 若結論對 k 成立, 設

$$M = \langle v_1, u_1, \ldots, u_k, u \rangle.$$

由歸納法的假設

$$\langle v_1, u_1, \ldots, u_k \rangle = \langle v_1 \rangle \oplus S_0.$$

而 S_0 是一個子模。

將 $u - \alpha v_1$, $\alpha \in \mathcal{R}$ 替代 u, 不會影響生成模 M, 即

$$\langle v_1, u_1, \ldots, u_k, u - \alpha v_1 \rangle = \langle v_1, u_1, \ldots, u_k, u \rangle = M.$$

於是可以找到 $\alpha \in \mathcal{R}$ 使得

$$\langle v_1 \rangle \cap \langle u - \alpha v_1, S_0 \rangle = \{0\},$$

這樣就得到

$$M = \langle v_1 \rangle \oplus \langle u - \alpha v_1, S_0 \rangle = \langle v_1 \rangle \oplus S_1.$$

我們令 $S_1 = \langle u - \alpha v_1, S_0 \rangle$ 就可以了。$\langle u - \alpha v_1, S_0 \rangle$ 中的元素形爲 $r(u - \alpha v_1) + s_0$, 於是 $\langle v_1 \rangle \cap \langle u - \alpha v_1, S_0 \rangle = \{0\}$, 等價於對任何 $r \in \mathcal{R}$, $s_0 \in S_0$, 有

$$r(u - \alpha v_1) + s_0 \in \langle v_1 \rangle \ \Rightarrow \ r(u - \alpha v_1) + s_0 = 0,$$

這也等價於

$$r(u - \alpha v_1) + s_0 \in \langle v_1 \rangle \oplus S_0 \ \Rightarrow \ r(u - \alpha v_1) \ \in \ S_0.$$

即

$$ru \in \langle v_1 \rangle \oplus S_1 \ \Rightarrow \ r(u - \alpha v_1) \in S_0, \tag{4.3.4}$$

不難證明

$$\mathcal{I} = \left\{ r \in \mathcal{R} : \ \ ru \in \langle v_1 \rangle \oplus S_0 \right\}$$

是 $\mathcal{R}$ 的一個理想, 故爲主理想, 因此, $\mathcal{I} = \langle a \rangle$。但是

$$p^e u = 0 \in \langle v_1 \rangle \oplus S_0,$$

故 $p^e \in \langle a \rangle$, 這導出 $a \big| p^e$, 所以我們有 $f \leq e$, 使得 $a = p^f$。於是存在 $q \in \mathcal{R}$ 對下式成立 :

$$ru \in \langle v_1 \rangle \oplus S_0 \ \Rightarrow \ r \in \mathcal{I} \ \Rightarrow \ r = qp^f,$$

因此

$$r(u - \alpha v_1) = qp^f(u - \alpha v_1).$$

所以我們可以找到 $\alpha \in \mathcal{R}$ 使得

$$p^f(u - \alpha v_1) \in S_0, \tag{4.3.5}$$

則 (4.3.4)得證。由於 $p^f \in \mathcal{I}$, 所以 $p^f u \in \langle v_1 \rangle \oplus S_0$ 可寫爲

$$p^f u = tv_1 + s_0, \tag{4.3.6}$$

這裡 $t \in \mathcal{R}$, $s_0 \in S_0$。於是 (4.3.5)成爲

$$tv_1 + s_0 - \alpha p^f v_1 \in S_0 \ \Rightarrow \ (t - \alpha p^f)v_1 \in S_0.$$

上式成立若且唯若 $t - \alpha p^f = 0$, 即若且唯若 $p^f \big| t$。

由 (4.3.6), 我們得到

$$0 = p^{e-f}p^f u = p^{e-f}tv_1 + p^{e-f}s_0.$$

由於 $\langle v_1\rangle \cap S_0 = \{0\}$, 故 $p^{e-f}tv_1 = 0$。由於 v_1 的階爲 p^e, 所以 $p^e \big| p^{e-f}t$, 也就是 $p^e \big| t$, 這正是我們所需要的。於是 (4.3.3)得證, 從而 (4.3.1)得證。

式子 (4.3.2)可由 (4.3.1)推導出來。事實上, 由於

$$p^e \in \mathrm{ann}(M) \subset \mathrm{ann}(\mathcal{C}_j), \quad j = 1, \ldots, n,$$

故若 $\mathrm{ann}(\mathcal{C}_j) = \langle \alpha_j \rangle$, 則 $\alpha_j \big| p^e$。於是 $\alpha_j = p^{e_j}$, $e_j \leq e$, $j = 1, \ldots, n$。對 e_j 排列, 我們便得到 (4.3.2)。定理因而證畢。

從證明的過程來看, 可以看出這樣的分解不是唯一的。雖然如此, 除去乘上可逆元, 階 p^{e_j} 是唯一決定的。素元 p 也是唯一決定的。因爲它要除盡 M 的階 p^e。於是我們有如下的唯一性定理。

定理 4.3.4 (**循環分解唯一定理**): 若 M 是主理想整環 $\mathcal{R}$ 上一個非零的有限生成撓模, 其階爲 p^e。若 M 可分解爲

$$M = \mathcal{C}_1 \oplus \mathcal{C}_2 \oplus \cdots \oplus \mathcal{C}_n,$$

這裡 $\mathcal{C}_j$ 是階爲 p^{e_j} 的非零循環子模, 且 $e_1 \geq e_2 \geq \ldots \geq e_n \geq 1$。

若 M 還可分解爲

$$M = \mathcal{D}_1 \oplus \mathcal{D}_2 \oplus \cdots \oplus \mathcal{D}_m,$$

這裡 $\mathcal{D}_j$ 是階爲 p^{f_j} 的非零循環子模, 且 $f_1 \geq f_2 \geq \ldots \geq f_m \geq 1$, 則 $m = n$ 及

$$e_1 = f_1,\ e_2 = f_2, \ldots,\ e_n = f_n.$$

爲了證明這個唯一性定理, 我們要用到以下這些易證的結果。設 $\mathcal{R}$ 是主理想整環

(1) 在2.3節中第三條關於向量空間的同構定理都可以推廣到主理想整環 $\mathcal{R}$ 上的 $\mathcal{R}-$ 模中來。例如：$\mathcal{R}-$ 模中的第一同構定理爲：若 M 與 N 爲主理想整環 $\mathcal{R}$ 上的兩個 $\mathcal{R}-$ 模, 映射 $\tau \in \mathrm{Hom}_{\mathcal{R}}(M, N)$, 則

$$M/\ker(\tau) \approx \mathrm{Im}(\tau).$$

(2) 若 $\langle v\rangle$ 是一循環 $\mathcal{R}$ 模, $\mathrm{ann}(v) = \langle a\rangle$, 則映射

$$\tau : \mathcal{R} \to \langle v\rangle, \quad \tau(r) = rv, \quad r \in \mathcal{R}$$

是滿射同態, 其核爲 $\langle a\rangle$, 故由 (1) 中的第一同構定理, 我們有

$$\langle v\rangle \approx \mathcal{R}/\langle a\rangle.$$

若 a 是素元, 則 $\langle a\rangle$ 是 $\mathcal{R}$ 中極大理想, 故由引理 4.1.1, $\mathcal{R}/\langle a\rangle$ 是一個域。

(3) 若 $p \in \mathcal{R}$ 是素元, M 是這樣的一個 $\mathcal{R}-$ 模, 使得 $pM = \{0\}$, 則 M 是 $\mathcal{R}/\langle p\rangle$ 上的一個向量空間, 其數乘定義爲 : 對所有 $v \in M$,

$$(r + \langle p\rangle) \cdot v = rv.$$

(4) 若 $p \in \mathcal{R}$ 是素元, 對於 $\mathcal{R}-$ 模 M 的任意子模 S, 集合

$$S^{(p)} = \left\{v \in S : \ pv = 0\right\}$$

是 M 的一個子模。若 $M = S \oplus T$, 則 $M^{(p)} = S^{(p)} \oplus T^{(p)}$。

定理4.3.4**的證明**: 先證 $m = n$。由 (4), 我們知道

$$M^{(p)} = C_1^{(p)} \oplus \cdots \oplus C_n^{(p)}$$

及

$$M^{(p)} = D_1^{(p)} \oplus \cdots \oplus D_m^{(p)}.$$

由於 $pM^{(p)} = \{0\}$, 故由(3), $M^{(p)}$ 是 $\mathcal{R}/\langle p\rangle$ 上的一個向量空間。由於 $C_j^{(p)}$ 及 $D_k^{(p)}$, $j = 1,\ldots,n$, $k = 1,\ldots,m$ 均爲 $M^{(p)}$ 循環子模, 故 $C_j^{(p)}$ 及 $D_k^{(p)}$, $j = 1,\ldots,n$, $k = 1,\ldots,m$ 均爲 $M^{(p)}$ 這個向量空間的一維向量子空間, 所以 $m = n$。

再證 $e_j = f_j$, $j = 1,\ldots,n$。對 e_1 進行數學歸納法。設 $e_1 = 1$, 則所有的 $e_j = 1$, $j = 1,\ldots,n$, 故 $pM = \{0\}$。這樣所有的 $f_j = 1$, $j = 1,\ldots,n$, 因爲若 $f_j > 1$, 而 $D_1 = \langle w\rangle$, 則 $pw \neq 0$, 則爲矛盾。若結論對 $e_1 \leq k-1$ 都成立, 來證明當 $e_1 = k$ 時結論也成立。假設

$$(e_1,\ldots,e_n) = (e_1,\ldots,e_s,1,\ldots,1), \quad e_s > 1$$

及

$$(f_1,\ldots,f_n) = (f_1,\ldots,f_t,1,\ldots,1), \quad f_t > 1$$

則

$$pM = pC_1 \oplus \cdots \oplus pC_s$$

及

$$pM = pD_1 \oplus \cdots \oplus pD_t.$$

易見 pC_j 是 M 的循環子模及 $\mathrm{ann}(pC_j) = \langle p^{e_j-1}\rangle$。這是因爲, 若 $C_j = \langle v_j\rangle$, 則

$$pC_j = \big\{pc : \ \ c \in C_j\big\} = \big\{prv_j : \ \ r \in \mathcal{R}\big\} = \big\{r(pv_j) : \ \ c \in \mathcal{R}\big\} = \langle pv_j\rangle,$$

而 pv_j 的階爲 p^{e_j-1}。同樣 pD_j 是 M 的循環子模及 $\mathrm{ann}(pD_j) = \langle p^{f_j-1}\rangle$。特別 $\mathrm{ann}(pC_1) = \langle p^{e_1-1}\rangle$, 由數學歸納法我們知道

$$s = t, \qquad e_1 = f_1, \ldots, e_s = f_s.$$

定理因而得證。

4. 總結以上的三步, 我們得到下面三個結論：

(1) 先將主理想整環 $\mathcal{R}$ 上的有限生成模分解爲撓模與自由模之直和 (定理4.3.1), 即

$$M = M_{tor} \oplus M_{free},$$

這裡 M_{free} 爲 M 爲一個自由模, 而 M_{tor} 爲 M 中所有撓元所組成的撓模。

(2) 若 M_{tor} 的階爲

$$\mu = p_1^{e_1} \ \ldots \ p_n^{e_n},$$

這裡 p_j, $j = 1, \ldots, n$, 是互不相伴的素元, 則有准素分解 (定理4.3.2), 即

$$M_{tor} = M_{p_1} \oplus \cdots \oplus M_{p_n},$$

這裡 M_{p_j}, $j = 1, \ldots, n$, 爲准素模, 其階爲 p^{e_j}。於是 M 有下列之分解

$$M = M_{p_1} \oplus \cdots \oplus M_{p_n} \oplus M_{free}.$$

(3) 由定理 4.3.3, 再將准素模 M_{p_j}, $j = 1, \ldots, n$, 分解爲循環子模的直和。歸納起來有這樣重要的兩個不同形式的定理。

定理4.3.5 (**主理想整環上有限生成模的循環分解定理–初等因子形式**): 若 M 是主理想整環上 $\mathcal{R}$ 上的一個非零有限生成模, 則

$$M = M_{tor} \oplus M_{free},$$

這裡 M_{tor} 爲 M 中所有撓元所組成的集合, 而 M_{tor} 爲 M 中一個自由模, 其秩由模 M 唯一決定。若 M_{tor} 有階爲

$$\mu = p_1^{e_1} \ \ldots \ p_n^{e_n},$$

這裡 p_j, $j=1,\ldots,n$, 是互不相伴的素元, 則

$$M_{tor}=M_{p_1}\oplus\cdots\oplus M_{p_n},$$

這裡

$$M_{p_j}=\big\{v\in M:\ \ p^{e_j}v=0\big\}$$

是准素模, 其階爲 p^{e_j}。每個 M_{p_j} 可以分解爲循環子模的直和

$$M_{p_j}=C_{j,1}\oplus\cdots\oplus C_{j,k_j},$$

而 $C_{j,\ell}$ 的階爲 $p_j^{e_{j,\ell}}$, $\ell=1,\ldots,k_j$, 且

$$e_j\ \geq\ e_{j,1}\ \geq\ e_{j,2}\ \geq\ \cdots e_{j,k_j}\ \geq\ 1,\quad j=1,\ldots,n.$$

將 M 的循環子模直和項 $C_{j,\ell}$ 的階 $p_j^{e_{j,\ell}}$, $\ell=1,\ldots,k_j$, $j=1,\ldots,n$, 稱爲 M 的 *初等因子* (elementary divisors)。除了乘以可逆元外, M 的初等因子由模 M 唯一決定。最終得到 M 可以分解爲循環子模及一個自由模的直和

$$M=\big(C_{1,1}\oplus\cdots\oplus C_{1,k_1}\big)\oplus\cdots\oplus\big(C_{n,1}\oplus\cdots\oplus C_{n,k_n}\big)\oplus M_{free}.\tag{4.3.7}$$

定理4.3.5的分解前面已證完。下面說明一下初等因子的唯一性。根據定理4.3.1中的唯一性部份, 不妨設 $M_{free}=\{0\}$, 令

$$D_j=D_{j,1}\oplus\cdots\oplus D_{j,\ell_k},$$

$k=1,\ldots,m$。則 D_{j,ℓ_k} 是階爲 $q_j^{f_{j,\ell_k}}$ 的准素模。於是 M 有如下兩種准素分解

$$M=D_1\oplus\cdots\oplus D_m=M_{p_1}\oplus\cdots\oplus M_{p_n}.$$

故由定理4.3.2的唯一性部份知道 $m=n$, 且不妨假設 $D_j=M_{p_j}$, $j=1,\ldots,n$, 從而 p_j 與 q_j 相伴。再由定理4.3.4知道 $k_j=\ell_j$, $f_{j,\ell}=e_{j,\ell}$, $j=1,\ldots,n$, $\ell=1,\ldots,k_j$。就證明了分解的唯一性, 即 M 的初等因子是由 M 唯一確定的。

這種分解還可以寫成另一種形式。設 S 與 T 是 M 的循環子模。若 $\mathrm{ann}(S)=\langle a\rangle$ 及 $\mathrm{ann}(T)=\langle b\rangle$, 且 $S\cap T=\{0\}$, 於是 $S\oplus T$ 也是一個子模, 且

$$\mathrm{ann}(S\oplus T)=\langle ab\rangle.$$

在 (4.3.7)中, 記

$$D_1=C_{1,1}\oplus\cdots\oplus C_{n,1},$$

則 D_1 是一個循環子模, 其階爲

$$q_1 = \prod_{j=1}^{n} p_j^{j,1}.$$

類似可以定義 $D_2, \ldots, D_m$, 這裡 $m = \max_j(k_j)$。於是我們有另一個形式的分解定理。

定理 4.3.6 (**主理想整環上有限生成模的循環分解定理–不變因子形式**): 若 M 是主理想整環上一個有限生成模, 則

$$M = D_1 \oplus \cdots \oplus D_m \oplus M_{free},$$

這裡 M_{free} 爲 M 爲一個自由模, 而 D_j 是 M 的循環子模, 其階爲 q_j, $j = 1, \ldots, m$, 而且

$$q_m \,\big|\, q_{m-1},\quad q_{m-1} \,\big|\, q_{m-2},\ \ldots\ q_2 \,\big|\, q_1.$$

純量 q_j, $j = 1, \ldots, m$, 稱爲 M 的不變因子 (invariant factor)。由定理4.3.5的初等因子的唯一性部份容易看出除去乘以可逆元, 這些不變因子由 M 所唯一決定, M_{free} 的秩由 M 所唯一決定。

—本文作者龔昇任教於中國科技大學; 張德健任教於美國 Georgetown University 數學系—