1 整数矩阵及其应用

故对应于同一模之二方阵是左结合的. 反之, 二非奇异的左结合方阵对应于同一模. 故若将所有的 n 级非奇异方阵依左结合关系分类，则每一类代表一模，且不同的类所代表的模也不同. 以后凡说到 “模 $\mathfrak{M}$ 对应于方阵 A”, 此 A 即表示模 $\mathfrak{M}$ 所对应的一类方阵中的一个.

定理 1.1 模 $\mathfrak{M}$ 包有模 $\mathfrak{N}$ 的充要条件是模 $\mathfrak{M}$ 所对应的方阵右除尽模 $\mathfrak{N}$ 所对应的方阵.

证明：命模 $\mathfrak{M}$ 及 $\mathfrak{N}$ 之底分别为 $y_1, y_2, \cdots, y_n$ 及 $z_1, z_2, \cdots, z_m$. 所对应的方阵分别为 $A = (a_{ij})$ 及 $B = (b_{ij})$. 若 $\mathfrak{M}$ 包有模 $\mathfrak{N}$, 则显然此同余关系亦有反身，对称, 传递等三种性质, 故可将所有线性型依 mod $\mathfrak{M}$ 分类：属于同一类者互相同余，不同类者绝不同余.

$$y = a_1x_1 + a_2x_2 + \cdots + a_nx_n$$

如是所分成之类的数目名为 $\mathfrak{M}$ 之矩, 以 $N(\mathfrak{M})$ 记之 (其存在性还未证明). 显然 $\mathfrak{M}$ 本身即为其中之一类. 故不妨假定底已取标准形式 (4). 任一线性型... □

定理 1.2 若 $\mathfrak{M} \supseteq \mathfrak{N}$, $\mathfrak{M}, \mathfrak{N}$ 所对应的矩阵分别为 A, B, 则依 mod $\mathfrak{N}$ 将 $\mathfrak{M}$ 中的元素分类, 所得之类数为 $\frac{N(\mathfrak{N})}{N(\mathfrak{M})} = \frac{|B|}{|A|}$.

证明：由未定量 $x_1, x_2, \cdots, x_n$ 表出 $\mathfrak{D} = \{x_1, x_2, \cdots, x_n\}$ 也可由其他未定量表出. 如命

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} u_{11} & u_{12} & \cdots & u_{1n} \\ & \vdots & \cdots & \vdots \\ u_{n1} & u_{n2} & \cdots & u_{nn} \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

故由定理 5.1 可知: 对固定的 n 维模 $\mathfrak{M}$, 可经过模的换底及 $\mathfrak{D}$ 的换底, 使其对应之方阵化为对角线方阵. □

两模 $\mathfrak{M}_1$ 及 $\mathfrak{M}_2$ 的所有公共元素成一模, 此模称为 $\mathfrak{M}_1$ 与 $\mathfrak{M}_2$ 的交, 以 $\mathfrak{M}_m$ 记之. 又 $\mathfrak{M}_1$ 及 $\mathfrak{M}_2$ 中所有元素的和、差所成的集合也是一模, 此模称为 $\mathfrak{M}_1$ 与 $\mathfrak{M}_2$ 的和, 以 $\mathfrak{M}_d$ 记之.

定理 1.3 设模 $\mathfrak{M}_1$, $\mathfrak{M}_2$, $\mathfrak{M}_m$, $\mathfrak{M}_d$ 分别对应于方阵 M_1, M_2, M_m, M_d, 则 M_m 为 M_1, M_2 之最小公倍, M_d 为 M_1, M_2 之最大公约.

证明：由 $\mathfrak{M}_1 \supseteq \mathfrak{M}_m$ 及 $\mathfrak{M}_2 \supseteq \mathfrak{M}_m$ 可知:

$$M_m = A_1M_1 + A_2M_2.$$

若 $M_3 = B_1M_1 = B_2M_2$ 为 M_1, M_2 之任一公倍, $\mathfrak{M}_3$ 为 M_3 对应之模, 则

$$\mathfrak{M}_3 \subseteq \mathfrak{M}_1, \mathfrak{M}_3 \subseteq \mathfrak{M}_2,$$

因而

$$\mathfrak{M}_3 \subseteq \mathfrak{M}_m, M_3 = CM_m.$$

即 M_m 为 M_1, M_2 之最小公倍. 同样可证 M_d 为 M_1, M_2 之最大公约. □