

1. 设  $P \in \mathbb{Z}[x]$ ,  $d(P)$  表示集合  $\{P(a) : a \in \mathbb{Z}\}$  中元的最大公因子. 如果  $P$  是  $k$  次本原多项式, 证明  $d(P)$  整除  $k!$ .

2. 对任意  $A, B \in M_n(\mathbb{C})$ , 定义  $\varphi(A, B) = \text{Tr}(AB)$ . 如果  $\{X_i\}_{1 \leq i \leq n^2}$  是线性空间  $M_n(\mathbb{C})$  的一组基. 证明存在另一组基  $\{X_i'\}_{1 \leq i \leq n^2}$  满足

$$(a) \quad \varphi(X_i, X_j') = \delta_{i,j}$$

$$(b) \quad \forall A \in M_n(\mathbb{C}), \quad \sum_{i=1}^{n^2} X_i A X_i' = \text{Tr}(A) I_n$$