# 臺灣大學數學系
# 102 學年度下學期博士班資格考試題
## 科目：代數 2014.02.20

**NOTATIONS :**

$\mathbb{F}_p$, the finite field with $p$ elements, $p$ a prime.
$\mathrm{Mat}_n(k)$, the ring of $n \times n$ matrices with entries from a commutative ring $k$.
$K[X_1, X_2, \ldots, X_n]$, polynomial ring in variables $X_1, X_2, \ldots, X_n$ over field $K$.

(1) (20%) Let $A$ be a square matrix with integral entries :

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \cdots & \cdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \in \mathrm{Mat}_n(\mathbb{Z})$$

For integral row vector $\mathbf{x} = (x_1, x_2, \cdots, x_n) \in \mathbb{Z}^n$, let $f_A(\mathbf{x}) := \mathbf{x} \cdot A \in \mathbb{Z}^n$.

Show that $f_A(\mathbb{Z}^n)$ is an additive subgroup of finite index inside $\mathbb{Z}^n$ if and only if $\det(A) \neq 0$. If that is the case, prove also that the absolute value of $\det(A)$ equals to the index $(\mathbb{Z}^n : f_A(\mathbb{Z}^n))$.

(2) (15%)Let $P(X) \in \mathbb{R}[X]$ be a non-constant polynomial without multiple roots. Let $A_0 := P(X), A_1(X) := P'(X)$, i.e. the derivative of $P(X)$. Define a polynomial remainder sequence $A_i(X), 1 \leq i \leq k$:

$$A_{i-1} := Q_i A_i - A_{i+1},$$

with $Q_i(X) \in \mathbb{R}[X]$, $\deg A_{i+1} < \deg A_i$, and $A_{k+1}$ being a constant polynomial. Set $\ell_i :=$ leading coefficient of $A_i$, and $d_i := \deg A_i$. Prove that the number of real roots of $P(X)$ is exactly $s - r$, where $r$ is the number of sign changes in the sequence $\ell_0, \ell_1 \ldots, \ell_{k+1}$, and $s$ is the number of sign changes in the sequence $(-1)^{d_0}\ell_0, (-1)^{d_1}\ell_1, \ldots, (-1)^{d_{k+1}}\ell_{k+1}$.

(3) (20%) Let $G$ be a finite group. Denote by $\mathbb{Q}[G]$ the group algebra of $G$ over the field $\mathbb{Q}$, this algebra has a vector space basis over $\mathbb{Q}$ indexed by elements of $G$. Each element of $\mathbb{Q}[G]$ can be written uniquely as formal sum:

$$\sum_{s \in G} a_s s,$$

with $a_s \in \mathbb{Q}$. Multiplication in $\mathbb{Q}[G]$ extends that in $G$.

Let $p$ be a prime number, and consider $G := \mathbb{Z}/p\mathbb{Z}$ the cyclic group of order $p$. Let $I \subset \mathbb{Q}[G]$ be the ideal generated by the element $\sum_{s \in G} s$. Prove that :

$$\mathbb{Q}[\mathbb{Z}/p\mathbb{Z}]/I \cong \mathbb{Q}(e^{2\pi i/p}).$$

(4) (15%) Show that the set of all maximal ideals in $\mathbb{C}[X_1, X_2, \ldots, X_n]$ is in natural one-to-one correspondence with the set of points of $\mathbb{C}^n$.

(5) (15%) Let $p$ be a prime number. Compute the Galois group of the polynomial $X^p - 2$ over $\mathbb{Q}$ .

(6) (15%) Let $G$ be a finite abelian group, $\mathbb{Q}/\mathbb{Z}$ denote the additive group of $\mathbb{Q}$ modulo $\mathbb{Z}$. Suppose that there is a non-degenerate pairing $B$ which is alternating, i.e $B : G \times G \to \mathbb{Q}/\mathbb{Z}$ is $\mathbb{Z}$-bilinear satisfying $B(x, y) = -B(y, x)$ for all $x, y \in G$, and if $B(x, G) = 0$ then $x$ must be 0. Show that the order of $G$ must be a square.