國立交通大學應用數學研究所博士班資格考試

科目：代數

2012 年 9 月 21 日

1. (% 20) Let $\mathbb{F}_q$ be a finite field of q elements where q is a power of a prime p.

   (a) Let n be a positive integer and let $G = \mathrm{SL}(n, \mathbb{F}_q) = \{A \in M_{n\times n}(\mathbb{F}_q) \mid \det A = 1\}$. Compute the order $|G|$ of the group G and give a Sylow p-subgroup of G.

   (b) In the case where $n = 2$, i.e. $G = \mathrm{SL}(2, \mathbb{F}_q)$, determine the number of Sylow p-subgroups of G.

2. (% 20) Let X be a finite set whose cardinality is $r = |X| \geq 1$. Let G be a finite group acting on X. The action of $g \in G$ on $w \in X$ is denoted by $g \cdot w$. Assume that the action is transitive (meaning that for any two elements $x, y \in X$ there exists a $g \in G$ such that $y = g \cdot x$).

   (a) Fix an $x \in X$ and let $H = G_x := \{g \in G \mid g \cdot x = x\}$ be the stabilizer of x. Prove that the action of G is *effective* (i.e. for every nontrivial element $g \in G$ there exist an element $y \in X$ such that $g \cdot y \neq y$) if and only if H does not contain any nontrivial normal subgroup of G.

   (b) Assume that $|G| \nmid r!$. Prove that G is not a simple group.

3. (% 15)

   (a) Let $\mathbb{Z}[i] = \{x + yi \mid x, y \in \mathbb{Z}\}$ be the ring of Gaussian integers where $i = \sqrt{-1}$. Let p be a prime number such that $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. Show that the ideal $(a + bi) = \{(a + bi)w \mid w \in \mathbb{Z}[i]\}$ is a prime ideal of $\mathbb{Z}[i]$.

   (b) It is known that $\mathbb{Z}[x]$, the polynomial ring with coefficients in $\mathbb{Z}$, is not a principal ideal domain. Prove this fact by constructing a non-principal prime ideal of $\mathbb{Z}[x]$. You need to explain your answer.

4. (% 15) Let K be a field and let L be a finite extension field of K. Let $\alpha \in L$ and let $f_\alpha(x) \in K[x]$ be the minimal polynomial of α over K. Here we require that $f_\alpha(x)$ is a monic polynomial.

   (a) Prove or disprove that the degree $\deg(f_\alpha)$ of $f_\alpha(x)$ is a divisor of the degree $[\mathrm{L} : \mathrm{K}]$ of L over K.

(b) Let $R \subset K$ be a UFD (unique factorization domain) and let $\{w_1, \ldots, w_n\}$ be a basis for L over K where $n = [L : K]$. Suppose that

$$\alpha w_j = \sum_{i=1}^{n} a_{ij} w_i, \; a_{ij} \in R \quad \text{for all } 1 \leq i \leq n \text{ and } 1 \leq j \leq n.$$

Show that $f_\alpha(x) = x^d + c_1 x^{d-1} + \cdots + c_{d-1} x + c_d$ for some integer $d \geq 1$ and $c_1, \ldots, c_d \in R$.

5. (% 10) Let D be a Euclidean domain and let $M \neq \{0\}$ be a finitely generated D-module. Assume that M has no nontrivial torsion D-submodule. That is,

$$\{m \in M \mid \alpha \cdot m = 0 \text{ for some nonzero } \alpha \in D\} = \{0\}.$$

Prove or disprove that M has a basis over D. By a basis of M it means a subset $\{m_1, \ldots, m_n\}$ of M such that for every $m \in M$, it can be written *uniquely* as a linear combination of $m_1, \ldots, m_n$ with coefficients in D. That is,

$$m = \sum_{i=1}^{n} \alpha_i m_i \quad \text{with } \alpha_i \in D \text{ for } i = 1, \ldots, n,$$

where $\alpha_1, \ldots, \alpha_n$ are uniquely determined by m.

6. (% 20)

(a) Find integers a, b such that the Galois group of the cubic polynomial $f(x) = x^3 + ax + b$ over $\mathbb{Q}$ is (i) a cyclic group of order 3; (ii) isomorphic to S_3 (the symmetric group of degree 3). (Note: the Galois group of $f(x)$ over $\mathbb{Q}$ means the Galois group of the splitting field of $f(x)$ over $\mathbb{Q}$.)

(b) Let $\mathbb{F}_{17}$ be a finite field of 17 elements. Assume that the cubic polynomial $f(x) = x^3 + ax + b$ is a polynomial with coefficients in $\mathbb{F}_{17}$ (i.e. $f(x) \in \mathbb{F}_{17}[x]$). Can you find $a, b \in \mathbb{F}_{17}$ such that the Galois group of $f(x)$ over $\mathbb{F}_{17}$ is isomorphic to S_3 ?