國立交通大學應用數學研究所博士班資格考試

科目：代數

2010 年 9 月 16 日

1. Let S_n denote the group of permutations on the set $\{1, 2, \ldots, n\}$ of n letters. In the following, we fix a prime number p.

   (a) (10 %) Determine the number of p-Sylow subgroups of S_p.

   (b) (15 %) Now consider the group S_{p^2} of permutations on $\{1, 2, \ldots, p^2\}$. Let $A = \{\tau \in S_{p^2} \mid \tau(i) = i \text{ for } i > p\}$ and let Q be the subgroup of A generated by the cycle $(1, 2, \ldots, p)$. Define $\sigma \in S_{p^2}$ by the formula

   $$\sigma(j) = \begin{cases} j + p & \text{if } j + p \leq p^2, \\ j + p - p^2 & \text{if } j + p > p^2 \end{cases}$$

   where $j = 1, 2, \ldots, p^2$ and let $T = Q\,(\sigma Q \sigma^{-1}) \cdots (\sigma^{p-1} Q \sigma^{-(p-1)})$. Show that T is a subgroup of S_{p^2} and the subgroup generated by T and σ is a p-Sylow subgroup of S_{p^2}.

2. By definition, a finite field is a field with finitely many elements. Let $\mathbb{F}_q$ denote a finite field with q elements.

   (a) (5 %) Prove that $q = p^f$ for some prime number p with integer $f \geq 1$.

   (b) (5 %) Construct a finite field of $q = 125$ elements.

3. (10 %) For a given positive integer n, the reduction of a polynomial $h(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ is the polynomial $\tilde{h}(x) = \sum_{i=0}^{n} \tilde{a}_i x^i$ where $\tilde{a}_i \equiv a_i \pmod{n}$ is the reduction of integer a_i modulo n. Thus, $\tilde{h}(x) \in \mathbb{Z}_n[x]$ where $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$. Let $f(x)$ be a non-constant, monic polynomial with integer coefficients. Assume that $f(x)$ is a separable polynomial (i.e., all roots of $f(x)$ are simple). Prove or disprove that for all but finitely many prime numbers p, the reduction $\tilde{f}$ of f modulo p is still a separable polynomial.

4. Let $\mathfrak{a} = (n, f(x))$ be the ideal of $\mathbb{Z}[x]$ generated by a positive integer n and a non-constant, monic polynomial $f(x) \in \mathbb{Z}[x]$.

   (a) (10 %) Give a necessary and sufficient condition on n and $f(x)$ so that $\mathfrak{a}$ is a maximal ideal of $\mathbb{Z}[x]$. You need to prove your assertion.

   (b) (10 %) Prove or disprove that $\mathfrak{a}$, as a $\mathbb{Z}[x]$-module, is free over $\mathbb{Z}[x]$.

5. Let K be a field and let n be a positive integer. Define

$$\Phi_n(x) := \prod_{d|n} \left(x^d - 1\right)^{\mu(n/d)} \in K(x)$$

where $\mu(m)$ is the Möbius μ function defined by $\mu(1) = 1, \mu(m) = 0$ if m is not square free, and $\mu(p_1 p_2 \cdots p_l) = (-1)^l$ where $p_1, \ldots, p_l$ are distinct prime numbers.

(a) (5 %) Show that for all positive integer n, $\Phi_n(x)$ is in fact a polynomial of degree $\phi(n)$ over K where ϕ is the Euler phi-function. (You only need to prove this result under the assumption that K is a field of characteristic 0.)

(b) (10 %) Suppose that $K = \mathbb{F}_p$ a finite field of p elements. Assume that n is a positive integer relatively prime to p. Let r be the smallest positive integer such that $p^r \equiv 1 \pmod{n}$. Prove that

$$\Phi_n(x) = g_1(x) \cdots g_m(x)$$

where $g_1(x), \ldots, g_m(x)$ are distinct irreducible polynomials of $\mathbb{F}_p[x]$ such that $\deg g_1(x) = \ldots = \deg g_m(x) = r$ and $m = \phi(n)/r$.

6. Let k be a field and let $k[t]$ be the ring of polynomials in t with coefficients in k. Let M be a $k[t]$-module.

(a) (10 %) Let $\widetilde{M}$ be the sum of all $k[t]$-submodule V such that $\dim_k V < \infty$. Prove that $\widetilde{M} = M_{\text{tor}}$ where M_{tor} denotes the torsion $k[t]$-submodule of M.

(b) (10 %) Suppose that M_{tor} is a direct sum of cyclic modules $N_1, \ldots, N_4$ whose annhilators are the ideals generated by the polynomials $p_1(t)^{l_1}, p_1(t)^{l_2} p_2(t)^{m_1}, p_1(t)^{l_3} p_3(t)^{n_1}$ and $p_2(t)^{m_2} p_3(t)^{n_2}$ with $l_1 \leq l_2 \leq l_3$, $m_1 \geq m_2$ and $n_1 \leq n_2$. Here $p_1(t), p_2(t), p_3(t)$ are distinct irreducible polynomials. Compute the invariants of M_{tor}. (The invariants of a finitely generated torsion module N is a decreasing sequence of ideals $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_r$ of $k[t]$ such that $N \simeq \oplus_{i=1}^r k[t]/\mathfrak{q}_i$.)