HONOURS MSci AND HONOURS MMath EXAMINATION

MATHEMATICS AND STATISTICS

Paper MT5826 : Finite Fields

May 2008

Time allowed : Two and a half hours

Attempt ALL FOUR questions

1. (a) Define the term *principal ideal domain*. [1]

(b) Prove that for a field F, the polynomial ring $F[x]$ is a principal ideal domain. [3]

(c) Let F be a field. Define what it means for a polynomial $p \in F[x]$ to be *reducible over* F. [1]

(d) Find *one* irreducible polynomial over $\mathbb{F}_3$ of degree 4. [4]

(e) State (giving justification) whether the following are fields:

(i) $\mathbb{F}_2[x]/(x^4 + x^2 + x + 1)$; (ii) $\mathbb{F}_5[x]/(x^3 + x + 1)$. [2]

(f) Calculate the multiplicative order of the element $x^2 + (x^3 + x + 1)$ in the field $\mathbb{F}_2[x]/(x^3 + x + 1)$. [2]

2. (a) Let F be a field and $f \in F[x]$ a polynomial. Prove that $\alpha \in F$ is a root of f if and only if $x - \alpha$ divides f. [2]

(b) Prove: if K is a field of characteristic zero, $f \in K[x]$ is a non-zero irreducible polynomial and F is any extension field of K, then f has no multiple roots in F. [3]

(c) Let F, K be fields. Let $\alpha \in F$ be algebraic over K and let g be the minimal polynomial of α over K. Prove that $K[x]/(g)$ is isomorphic to $K(\alpha)$. [3]

(d) Consider the irreducible polynomials $f(x) = x^2+x+1$ and $g(x) = x^2+x+2$ in $\mathbb{F}_5[x]$. Let $L = \mathbb{F}_5[x]/(f)$.

(i) Show that L is the splitting field for f over $\mathbb{F}_5$.

(ii) Show that L is also a splitting field for g over $\mathbb{F}_5$. Find a root of g in L. [4]

(e) State in full (without proof) the theorem about the 'Subfield Criterion for Finite Fields'. [2]

3. (a) Define a *primitive element* of a finite field $\mathbb{F}_q$. [1]

(b) How many elements that are not primitive does $\mathbb{F}_9$ contain? [3]

(c) Express all primitive elements of $\mathbb{F}_9$ as powers of one primitive element $\zeta \in \mathbb{F}_9$. [2]

(d) State the Moebius Inversion Formula (additive version only!). [2]

(e) Use the Moebius Inversion Formula to derive a formula for the number $N_q(d)$ of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree d. You can use the following formula without proof:

$$q^n = \sum_{d|n} dN_q(d) \quad \text{for all } n \in \mathbb{N}. \qquad [2]$$

(f) How many irreducible polynomials of degree 4 are there in $\mathbb{F}_9[x]$? (Note that in this part (f) we want to count not only the monic ones but all irreducible polynomials!) Prove your answer! [3]

4. (a) Prove that if F is a finite field containing a subfield K with q elements, then F has q^m elements where $m = [F : K]$. [2]

(b) Let $q = p^k$ for some prime p and some $k \in \mathbb{N}$ that is even. Define the *conjugates* of $\alpha \in \mathbb{F}_q$ with respect to $\mathbb{F}_{p^2}$. [1]

(c) Let $\alpha \in \mathbb{F}_{27}$ be a root of $f(x) = x^3+2x+1 \in \mathbb{F}_3[x]$. Calculate the conjugates of α with respect to $\mathbb{F}_3$. Express them as polynomials in α of degree less than 3. [3]

(d) Let F be a finite extension of a finite field K, and $\alpha \in F$. Define the *trace* $\mathrm{Tr}_{F/K}(\alpha)$ and the *norm* $N_{F/K}(\alpha)$ of α over K. [2]

(e) Prove that for the situation in (d) the following holds: $N_{F/K}(\alpha) = 0$ if and only if $\alpha = 0$. [2]
