University of St Andrews

MAY 2012 EXAMINATION DIET

SCHOOL OF MATHEMATICS & STATISTICS

MODULE CODE: **MT 5826**

MODULE TITLE: Finite Fields

EXAM DURATION: $2\frac{1}{2}$ hours

EXAM INSTRUCTIONS Attempt ALL questions.

The number in square brackets shows the maximum marks obtainable for that question or part-question.

Your answers should contain the full working required to justify your solutions.

PLEASE DO NOT TURN OVER THIS EXAM PAPER UNTIL YOU ARE INSTRUCTED TO DO SO.

1. Topic of question: Groups, polynomials, rings and fields.

(a) How many subgroups of index 5 does a cyclic group of order 120 have? What is the order of these subgroups? (No proof needed, you can cite a result from the course.) **[2]**

(b) Define the term *division ring.* **[1]**

(c) Prove that every finite, commutative ring with identity and without zero divisors is a field. **[3]**

(d) Let $p \in \mathbb{N}$ be a prime and $\mathbb{F}_p = \{0, 1, \dots, p-1\}$ be the field with p elements. For which primes p is the polynomial $x^2 + x + 1$ over $\mathbb{F}_p$ irreducible? Prove your answer.

Hint: Consider $(x^2 + x + 1)(x - 1)$. **[4]**

(e) Let $\mathbb{F}_{97} = \{0, 1, \dots, 96\}$ be the field with 97 elements. For which values $a \in \mathbb{F}_{97}$ does the polynomial $f = x^{97} + x^2 + 2ax - 1$ have a multiple root?

Hint: You can use that $5 \in \mathbb{F}_{97}$ has order 96 and express the elements a as powers of 5. **[4]**

2. Topic of question: Fields, minimal polynomial, field extensions and splitting field.

(a) What is the prime field of $\mathbb{C}$? **[1]**

(b) Let F be a field, K a subfield of F and $\alpha \in F$. Show that the intersection of all subfields of F that contain both K and α is a subfield of F. **[3]**

(c) Let K be a subfield of the field F and let $a \in F$ be algebraic over K. Define the *degree of a over K*. **[1]**

(d) Let $\mathbb{F}_3 = \{0, 1, 2\}$ be the field with three elements and $f = x^3 + x^2 + 1$. Determine the splitting field of f. **[3]**

(e) Let F be any field and $g \in F[x]$ be any monic polynomial of degree 3. Prove that the degree of the splitting field of g over F is a divisor of 6. **[3]**

(f) Let F be a field and K be a subfield of F. Let $a, b \in F$ be elements of F which are algebraic over K and assume their degrees are d_a and d_b. Show that $a + b$ is algebraic over K and that its degree is at most $d_a \cdot d_b$. **[4]**

3. Topic of question: The theory of finite fields.

(a) State the main theorem about existence and uniqueness of finite fields. **[2]**

(b) How many proper subfields does $\mathbb{F}_{7^{120}}$ have? **[2]**

(c) How many fields F are there with $\mathbb{F}_{2^{30}} \subseteq F \subseteq \mathbb{F}_{2^{900}}$? **[2]**

(d) Define the *characteristic* of a ring R with identity. **[1]**

(e) Let F be a finite field. Prove that the characteristic of F is a prime number. **[3]**

(f) What is the smallest finite field (i.e. the one with the least number of elements) that contains a primitive 17-th root of unity? **[2]**

4. Topic of question: Cyclotomic fields.

(a) Let K be a field. Define the term *n-th cyclotomic field* of K. **[1]**

(b) Let $F := \mathbb{F}_5$ be the field with 5 elements. What is its 62-nd cyclotomic field? **[2]**

(c) Let K be a field of characteristic p, and $n \in \mathbb{N}$ with $p \nmid n$. As usual, let

$$Q_n(x) = \prod_{\substack{s=1 \\ \gcd(s,n)=1}}^{n} (x - \zeta^s)$$

where ζ is a primitive n-th root of unity over K.

(i) Prove $x^n - 1 = \prod_{d|n} Q_d(x)$. **[2]**

(ii) Prove $Q_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$, where μ is the Moebius function. **[2]**

(You may assert and then use, without proof, the Moebius Inversion Formula).

(d) Let K be any finite field of characteristic p. Show that there is no extension field L of K which contains a primitive p-th root of unity. **[2]**