University of St Andrews

MAY 2010 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 does a cyclic group of order 12 have? What are the orders of these subgroups? (No proof needed, you can cite a result from the course.) **[2]**

(b) Define the term *integral domain.* **[1]**

(c) Prove that every finite integral domain is a field. **[3]**

(d) Let $\mathbb{F}_2 = \{0, 1\}$ be the field with 2 elements. Find (giving justification) all *irreducible* polynomials of $\mathbb{F}_2[x]$ of degree less than or equal to 3. **[3]**

(e) Let $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ be the field with 7 elements. Determine the set

$$\left\{a \in \mathbb{F}_7 \mid x^3 + x + a \text{ is irreducible in } \mathbb{F}_7[x]\right\}.$$ **[4]**

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

(a) Let F be a field and let K and L be subfields of F. Show that $K \cap L$ is also a subfield of F. **[2]**

(b) Define the term *prime subfield of a field F*. Define what it means that *the field L is a prime field.* Let F be an arbitrary field and let L be the prime subfield of F. Prove that L is a prime field. **[3]**

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

(d) In the situation of part (c), show that the minimal polynomial of a over K is an irreducible polynomial in $K[x]$. Is the same minimal polynomial irreducible as a polynomial in $F[x]$? **[2]**

(e) Let $f = x^3 + x + 1 \in \mathbb{F}_2[x]$. How many elements does the splitting field of f over $\mathbb{F}_2$ have? Prove your answer.

[**Hint:** Show that f is irreducible over $\mathbb{F}_2$. Then use that $\mathbb{F}_8 \cong \mathbb{F}_2[a]/(a^3+a+1)$ and that f as a polynomial in $\mathbb{F}_8[x]$ is divisible by $(x - a)$.] **[4]**

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

(a) Let F be a finite field of characteristic p. Let

$$S := \{0 \cdot 1_F, 1 \cdot 1_F, \dots, (p-1) \cdot 1_F\}$$

be the set of integer multiples of the identity 1_F of F. Prove that S is a subfield of F. Conclude that S is the prime subfield of F. **[4]**

(b) Prove that the cardinality of every finite field is a prime power. **[2]**

(c) Let $p \in \mathbb{N} \setminus \{0\}$ be a prime. What is the multiplicative order of a *primitive element* of the field $\mathbb{F}_{p^k}$ of p^k elements? **[1]**

(d) Let $p \in \mathbb{N} \setminus \{0\}$ be a prime and let $a, b \in \mathbb{N} \setminus \{0\}$. Prove that if $\mathbb{F}_{p^a}$ is a subfield of $\mathbb{F}_{p^b}$ then a divides b. **[2]**

(e) Let $p \in \mathbb{N} \setminus \{0\}$ be a prime and let $n \in \mathbb{N} \setminus \{0, 1\}$. In this question you will prove that there is a field with $q := p^n$ elements. Let S be a splitting field of $x^q - x \in \mathbb{F}_p[x]$.

(i) Show that $x^q - x$ has q different roots in S. **[2]**

(ii) Show that $R := \{a \in S \mid a^q = a\}$ is a subfield of S. **[3]**

(iii) Show that $x^q - x$ splits over R and thus that $R = S$. **[2]**

(iv) Show that $|S| = q$. **[2]**

4. Topic of question: Cyclotomic fields.

(a) Define the terms *n-th cyclotomic field over the field K* and a *primitive n-th root of unity over K*. **[2]**

(b) How many elements does the third cyclotomic field over the field $\mathbb{F}_5$ have? How many elements does the third cyclotomic field over the field $\mathbb{F}_{13}$ have? **[3]**

(c) Let $f = x^4 + x + 1 \in \mathbb{F}_2[x]$, this is irreducible (do not prove this!). Thus $\mathbb{F}_{16} = \mathbb{F}_2[x]/(f)$. Let α be a root of f in $\mathbb{F}_{16}$. Describe the conjugates of α with respect to $\mathbb{F}_2$ as polynomials in α of degree less than 4. **[2]**