UNIVERSITY OF DUBLIN

1417

TRINITY COLLEGE

FACULTY OF SCIENCE

SCHOOL OF MATHEMATICS

JS Mathematics **Trinity Term 1994**
SS Mathematics

COURSE 373

Exam Hall

Dr. M. Purser and Dr. T.G. Murphy

Answer Section A and B in separate answer books. Section A - Answer 3 out of the 6 questions. Section B - Answer 2 out of the 4 questions.

SECTION A

PLEASE INSERT Michael Purser's questions here.

SECTION B

7. Show that the multiplicative group $F^{\times} = F - \{0\}$ of a finite field F is cyclic.

Determine all the primitive elements (multiplicative generators) in $\mathbf{GF}(17)$.

8. Listing the elements of $\mathbf{GF}(8)$ in any way you wish, draw up the addition and multiplication tables for this field.

9. Define the *characteristic* of a field, and show that the characteristic of a finite field F is always a prime number.

Show that a finite field F of characteristic p contains p^n elements for some n.

Show further that the map

$$\Phi : x \mapsto x^p$$

is an automorphism of F; and show that every automorphism of F is of the form $x \mapsto \Phi^i(x)$ for some i.

Prove that each subfield $K \subset F$ is of the form

$$K = \{x \in F : \Phi^m(x) = x\}$$

for some m.

10. Show that if $f(x)$ is an irreducible polynomial of degree d over $\mathbf{GF}(p^d)$, then

$$f(x) \mid x^{p^d} - x.$$

Hence or otherwise show that if there are $N(d,p)$ prime polynomials of degree d over $\mathbf{GF}(p^n)$ then

$$\sum_{d|n} dN(d,p) = p^n.$$

Determine the number of prime polynomials of degree 6 over $\mathbf{GF}(2)$, and find one of them.