GX1599

OLLSCOIL NA hÉIREANN, GAILLIMH
THE NATIONAL UNIVERSITY OF IRELAND, GALWAY

SUMMER 1999

B.A. and B.Sc. Degree Examination
Higher Diploma in Mathematics Examination

MATHEMATICS

MA483 = MA416 [RING THEORY] — & — MA491 [FIELD THEORY]

Professor J. Wiegold
Professor T. Hurley
Dr. D. Flannery

Time allowed: *Three* hours.
Full marks for five correct solutions.

SECTION A — RING THEORY

A1. Let $n \geq 2$ be an integer.

(a) Define $R_n = \{a + b\sqrt{n} \mid a, b \in \mathbf{Z}\}$ and

$$S_n = \left\{ \begin{pmatrix} a & nb \\ b & a \end{pmatrix} \mid a, b \in \mathbf{Z} \right\}.$$

(i) Prove that R_n is a subring of $\mathbf{R}$, and that S_n is a subring of $M_2(\mathbf{Z})$.
(ii) Assuming that $\sqrt{n}$ is irrational, exhibit an isomorphism of R_n onto S_n.
(iii) Are R_2 and S_3 isomorphic? Why?

(b) (i) Prove that $\mathbf{Z}_n$ is an integral domain if and only if n is prime.
(ii) Suppose R is an integral domain. Is $R \times R$ necessarily an integral domain? Is $R[x]$ necessarily an integral domain? Justify your answers.

A2. (a) Let R be a commutative ring with 1, and I an ideal of R. Prove that R/I is a field if and only if I is a maximal ideal. State, but do not prove, the analogous result when "maximal ideal" is replaced by "prime ideal".

(b) Describe the prime and maximal ideals of
(i) $\mathbf{Z}$;
(ii) $\mathbf{Z}_6$.

(c) Suppose S is a ring with 1 such that $x^2 = x$ for all $x \in S$. Let I be a prime ideal of S. Prove that $SI \cong \mathbf{Z}_2$, and hence deduce that I is a maximal ideal of S.

p.t.o.

A3. (a) (i) Prove Gauss' Lemma.

(ii) Apply the lemma to show that $x^4 - 7x^2 + 3x + 1$ is irreducible over $\mathbf{Q}$.

(iii) Is $\mathbf{Q}[x]/\langle x^4 - 7x^2 + 3x + 1\rangle$ a field? Why?

(b) (i) State Eisenstein's Irreducibility Criterion.

(ii) Apply the criterion to prove that $1 + x + x^2 + \cdots + x^{p-1}$ is irreducible over $\mathbf{Q}$ for any prime p.

A4. (a) (i) Define the terms *Euclidean domain, unique factorisation domain*, and *principal ideal domain.*

(ii) Give an example, with justification, of a unique factorisation domain that is not a principal ideal domain.

(b) (i) Show that $3, 2 + \sqrt{-5}$ and $2 - \sqrt{-5}$ are all irreducible elements of $\mathbf{Z}[\sqrt{-5}]$.

(ii) Using (b)(i), show that $\mathbf{Z}[\sqrt{-5}]$ is not a unique factorisation domain.

(iii) Is $\mathbf{Z}[\sqrt{-5}]$ a principal ideal domain? A Euclidean domain?

p.t.o.

SECTION B — FIELD THEORY

B1. (a) Suppose $p(x)$ is an irreducible polynomial of degree n over a field F. Describe *briefly* the construction of the field $K = F[x]/ < p(x) >$. Show that $[K : F] = n$.

(b) Find the irreducible factors in $\mathbf{Q}[x]$ of $f(x) = x^4 - x^2 - 2$. Show that $f(x)$ splits into linear factors over $\mathbf{Q}(i, \sqrt{2})$. Determine $[\mathbf{Q}(i, \sqrt{2}) : \mathbf{Q}]$ and write down a basis for $\mathbf{Q}(i, \sqrt{2})$ over $\mathbf{Q}$.

(c) If u is an element algebraic over a field K and its degree over K is odd, prove $K(u) = K(u^2)$. Give an example to show that it is not always true that $K(v) = K(v^2)$, for v an algebraic element over K.

B2. (a) Explain what is meant by saying that a number $\alpha \in \mathbf{R}$ is *constructible by ruler and compass.* Prove that the set of constructible numbers is a subfield of $\mathbf{R}$.

(b) Prove that it is impossible to trisect 60^o with ruler and compass.

(c) Show that it is impossible to construct $\cos \frac{2\pi}{7}$ by ruler and compass and deduce that it is impossible to construct a regular heptagon.

B3. (a) Suppose $p = 0.97$ is the probability that a digit in an ISBN code is transmitted correctly. Compare the probability of correct transmission when no check digit is used to the probability of correct transmission when one check digit is used.

(b) Describe the Hamming $(7, 4)$ binary code. State its minimum distance and why it is a 1-error correcting code. Prove that the Hamming $(7, 4)$ code has the best information rate possible for a 4-dimensional 1-error correcting code.

(c) Suppose $\alpha \in GF(3^2)$ is a root of $x^2 - x - 1$.
Prove that α is a primitive element.
Hence, or otherwise, find a generating polynomial $g(x)$ for a BCH code of length 8 and dimension 4 over GF(3).

B4. (a) Let F be a field of characteristic $p \neq 0$.
Show that $x^{p^n} - x$ cannot have a multiple root in any extension field of F.

(b) Prove that for every positive integer n and every prime p, there exists a field with p^n elements. (Consider $x^{p^n} - x$ over $\mathbf{Z}_p[x]$. Quote but do not prove any Theorems on the existence of splitting fields for a polynomial over a field.)

(c) Suppose G is a finite group in which the equation $x^d = 1$ has at most d solutions for every divisor d of n. Prove that G is cyclic.
Deduce that, when K is a finite field, the multiplicative group $K^* = K - \{0\}$ is cyclic.
What is meant by a primitive element of K^*? Where are primitive elements of K^* used?