GX 2044

OLLSCOIL NA hÉIREANN, GAILLIMH
NATIONAL UNIVERSITY OF IRELAND, GALWAY

SUMMER EXAMINATIONS 2004 - HONOURS

B.A. and B.Sc. EXAMINATIONS
HIGHER DIPLOMA IN MATHEMATICS

MATHEMATICS

MA416 [RING THEORY] and MA491 [FIELD THEORY]

Dr. Dave Johnson
Prof. M. Newell
Dr. J. Ward

Time allowed: **Three** hours.

Those seeking credit for one semester should answer *three* questions.
Those seeking credit for both semesters should answer *five* questions.
Please use separate answer books for each section.

SECTION A — RING THEORY

1. Let R be a commutative ring with 1.

(a) Find a formula for $(a+b)^n$ where $a, b \in R$ and n is a positive integer.

(b) Let $J(R) = \{a \in R : a^n = 0 \text{ for some integer } n\}$. Prove that $J(R)$ is an ideal in R.

(c) Prove that $1 - a$ is a unit of R, when $a \in J(R)$.

(d) Deduce that $u - a$ is a unit of R, when u is a unit of R and $a \in J(R)$.

p.t.o.

2. (a) Explain what is meant by the term "a principal ideal domain".

(b) Prove that any pair of elements a, b in a principal ideal domain R have a greatest common divisor d.

(c) When $d = 1$, prove that $a \mid c$, whenever $a \mid bc$ for $c \in R$.

3. (a) Give the defining relations for a ring homomorphism θ mapping a ring R onto a ring S.

(b) When $\theta \neq 0$ and $1 \epsilon R$, prove that $\theta(u)$ is a unit in S, when u is a unit in R.

(c) Describe all the ring homomorphisms mapping $\mathbf{Z}$ into $\mathbf{Z} \times \mathbf{Z}$.

4. Let R be the subring of complex numbers consisting of all $a + b\sqrt{-3}$, where a, b are integers.

(a) Prove that $\{1, -1\}$ is the group of units in R.

(b) Prove that 2, $1 + \sqrt{-3}$, $1 - \sqrt{-3}$ are irreducible elements of R.

(c) Deduce that R is not a unique factorization domain.

Section B – Field Theory (MA 491)

B1. (i) Explain how a field $\mathbf{K}$ may be viewed as a vector space over a sub–field $\mathbf{F}$ and hence define the degree $[\mathbf{K} : \mathbf{F}]$.
(ii) Define the term **splitting field** of a polynomial. Find quadratic factors for

$$f(x) = x^4 + 2x^3 - 8x^2 - 6x - 1$$

over $\mathbf{Z}[X]$ and hence, or otherwise show that $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is a splitting field for $f(x)$ over $\mathbf{Q}$.
(iii) Show that $\sqrt{3} \notin \mathbf{Q}(\sqrt{2})$ and deduce that $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is an extension of degree 4 over $\mathbf{Q}$. Write down a basis for $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbf{Q}$.
(iv) Prove that $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{3} - \sqrt{2})$ and find the minimum polynomial of $\sqrt{3} - \sqrt{2}$ over $\mathbf{Q}(\sqrt{3})$.

B2. (i) What is meant by a "straight–edge and compass construction"?
(ii) State Gauss' Theorem concerning the values for which the regular n–gon can be constructed by straight edge and compass.
(iii) Using the identity $\sin 3\theta = 3\sin\theta - 4\sin^3\theta$, or otherwise, **prove** that the angle $10°$ is not constructible.
(iv) Using part (ii) show that $18°$ is constructible. Deduce that the angle $n°$ is constructible $\Leftrightarrow 3|n$.
(v) Show that $\cos^{-1}\left(\frac{23}{27}\right)$ can be trisected using straight–edge and compass.

p.t.o

B3. (i) Write down the four roots of the polynomial $x^4 - 2$. Letting $r = \sqrt[4]{2}$ and $i = \sqrt{-1}$, show that a splitting field for this polynomial over $\mathbf{Q}$ is $\mathbf{Q}(r, i)$.
(ii) Let σ be the $\mathbf{Q}$–automorphism defined as $\sigma : r \to ir$; $\sigma : i \to i$, where r is the positive real fourth root of 2; and let τ be the $\mathbf{Q}$–automorphism of complex conjugation, defined as $\tau : i \to -i$; $\tau : r \to r$. Hence determine the Galois group G of $x^4 - 2$ over $\mathbf{Q}$ and establish that G is non–abelian of order 8.
(iii) Under the Galois correspondence find the (fixed) subfield corresponding to the subgroup of G of order 2 generated by σ^2.

B4. (i) Let $\mathbf{GF}(q)$ be a finite field of order q $(= p^n$, p a prime $n \geq 1)$. State the main properties of $\mathbf{GF}(q)$.
(ii) Verify that an element α in $\mathbf{GF}(9)$ which is a root of $x^2 + 2x + 2$ is a primitive element of $\mathbf{GF}(9)$, i.e. all the non–zero elements of the field are powers of α.
(iii) Describe, without proofs, the construction of a BCH–code over $\mathbf{GF}(q)$, of length $q^n - 1$ and minimum distance $\geq d$.
(iv) Hence, or otherwise, find a generator $g(x)$ for a BCH–code of length 8 and dimension 4 over $\mathbf{GF}(3)$.