NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

SMA4102

FACULTY OF APPLIED SCIENCES

DEPARTMENT OF APPLIED MATHEMATICS

MODERN ALGEBRA

APRIL/MAY 2002

Time : 3 hours

Candidates should attempt **ALL** questions from Section A and **ANY FOUR** questions from Section B.

SECTION A

A1. Let $\phi : G \to H$ be a homomorphism of groups. Prove that $\ker\phi$ is a subgroup of G and $\mathrm{Im}\phi$ is a subgroup of H. [6]

A2. Find the remainder when 2^{1000} is divided by 13. [5]

A3. Let G be a group such that for some fixed integer $n > 1, (ab)^n = a^n b^n$ for all $a, b \in G$. Let

$$G_n = \{a \in G : a^n = e\} \text{ and } G^n = \{a^n : a \in G\}$$

Prove that $G_n \trianglelefteq G, G^n \trianglelefteq G$ and $G/G_n \cong G^n$ [9]

A4. Let R be a commutative ring with one, and let $a \in R$. Show that if $x \equiv x'(\mathrm{mod}a)$ and $y \equiv y'(\mathrm{mod}a)$ then

$$x + y = x' + y'(\mathrm{mod}a) \text{ and } xy = x'y'(\mathrm{mod}a)$$

where $x, y, x', y' \in R$. [6]

A5. Let p be a prime and r an integer such that $0 < r < p$. Prove that the binomial coefficient $\binom{p}{r}$, is a multiple of p. Hence prove that, for each positive integer a, $a^p \equiv a (\mathrm{mod} p)$. [9]

A6. Calculate the gcd of $x^3 + 2x^2 + 4x - 7$ and $x^2 + x - 2$ in $Q[x]$. [5]

SECTION B

B7. (a) Find (4307,9271) using Euclidean algorithm. Explain briefly how you know from your working that the result obtained is the required positive g.c.d. Write (4307, 9271) in the form $4307s + 9271t$ where $t > s$

(b) Let a, b, s, t be non-zero integers such that $sa + tb = 1$. Prove, or give a counter example to, each of the following assertions: (i) $(s, t) = 1$ (ii) $(st, ab) = 1$

(c) Prove that there are infinitely many primes of the form $6k + 5$

[15]

B8. Let $\mathbf{Z}[i]$ denote the set $\{a + ib : a, b \in \mathbf{Z}\}$ of complex numbers.

(a) Defining $N : \mathbf{Z}[i] \to \mathbf{Z}$ by $N(a + ib) = a^2 + b^2$, prove that for $\alpha, \beta \in \mathbf{Z}[i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$. Deduce that if $m, n \in \mathbf{Z}$ and each is a sum of two squares then so is mn. Write 37, 89 and 3293 as sums of two squares.

(b) Prove that, given $\alpha, \beta(\neq 0)$ in $\mathbf{Z}[i]$, there exist $m, r \in \mathbf{Z}[i]$ such that $\alpha = m\beta + r$ and $0 \leq N(r) < N(\beta)$. Deduce that, in the ring $< \mathbf{Z}[i], +, \cdot >$ each ideal is a principal ideal.

(c) Assuming that each prime $p \in \mathbf{Z}$ which is of the form $4k + 1, \mathbf{Z}, k > 0$ can be expressed as a sum $p = l^2 + m^2$ of two squares, show briefly that, if $p = u^2 + v^2$ then either (i) $u = \pm l$ and $v = \pm m$ (ii) $u = \pm m$ and $v = \pm l$

[15]

[*Any facts you use concerning* $< \mathbf{Z}[i], +, \cdot >$ *should be clearly stated.*]

B9. Let $N : \mathbf{Z}[\sqrt{-5}] \to \mathbf{Z}$ be defined by

$$N(m + n\sqrt{-5}) = m^2 + 5n^2$$

Show that if $\alpha, \beta \in \mathbf{Z}[\sqrt{-5}]$,

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

Deduce that u is a unit in $\mathbf{Z}[\sqrt{-5}]$ if and only if $N(u) = \pm 1$.

By considering $(1 + \sqrt{-5})(1 - \sqrt{-5})$ show that 3 is irreducible in $\mathbf{Z}[\sqrt{-5}$ but not a prime. [15]

B10. (a) Write down, carefully the statement of the division algorithm for $\mathbf{Q}[x]$. Use it to deduce that the rational number a is a root of the polynomial $f(x)$ if and only if $x - a$ is a factor of $f(x)$ in $\mathbf{Q}[x]$. Hence factorise as far as possible in $\mathbf{Q}[x]$ the polynomial $x^3 + x^2 - 41x + 7$

(b) Prove that if β is a complex root of the polynomial $g(x) \in \mathbf{R}[x]$, then so is its complex conjugate $\bar{\beta}$.

(c) Given that $2 + i$ is a root of the polynomial $x^4 + 2x^2 - 32x + 65$ find all its roots. Hence, or otherwise, find a g.c.d of $x^4 + 2x^2 - 32x + 65$ and $3x^3 + 8x^2 + 23x - 52$ in $\mathbf{Z}[x]$.

(d) By considering $f(x + 1)$, show that

$$f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

will not factorise in $\mathbf{Z}[x]$.

[15]

B11. Define the terms group and subgroup.

(a) Let G be the set of non-zero complex numbers and let H be the subset consisting of those complex numbers with unit modulus. assuming that G is a group with respect to multiplication of complex numbers, show that H is a subgroup of G.

(b) Let G be the set of pairs (a, b) of real numbers with $a \neq 0$. Define multiplication on G by

$$(a, b)(c, d) = (ac, bc + d)$$

Prove that G is a group. Let H be the subset consisting of pairs of the form $(1, b)$. Show that H is a subgroup of G.

[15]

B12. (a) Let $< R, +, \cdot >$ and $< S, \oplus, \odot >$ be rings. Define the term homomorphism from the ring R to the ring S. Let ϕ, ψ be maps $M_2(\mathbf{Z}) \to \mathbf{Z}$ given by:

$$\phi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a + d; \qquad \psi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

Determine which if either, of these maps is a homomorphism form $< M_2(\mathbf{Z}), \oplus, \odot >$ to $< \mathbf{Z}, +, \cdot >$

(b) Explain what is meant by the kernel of the homomorphism Γ in part (a) and show that it is an ideal of $(R, +, \cdot)$.

(c) What are the kernels of the homomorphisms

(i) $f : \mathbf{Z} \to M_2(\mathbf{Z})$, $fk = \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}$ for all $k \in \mathbf{Z}$

(ii) $g :< \mathbf{Q}[x], +, \cdot > \to < \mathbf{Q}[\sqrt{2}], +, \cdot >$ given by

$$g(a_0 + a_1 x + \ldots + a_n x^n) = a_0 + a_1\sqrt{2} + \ldots + a_n(\sqrt{2})^n$$

[In the case of g a brief reason for your answers is expected.]

[15]

END OF QUESTION PAPER