MATH 203301

This question paper consists of 4 printed pages, each of which is identified by the reference MATH 203301

Only approved basic scientific calculators may be used

UNIVERSITY OF LEEDS
Resit Examination for the Module MATH 2033
(May/June 2011)

Rings, Polynomials and Fields

Time allowed : 2 hours

Do not answer more than **four** questions
All questions carry equal marks

1. (i) Explain what is meant by the *set* $\mathbb{Z}[\sqrt{2}]$. Explain briefly how this set may be made into a ring.

(ii) Show that if $x \in \mathbb{Z}[\sqrt{2}]$ obeys $x = a + b\sqrt{2}$ with $a, b \in \mathbb{Z}$ then a and b are uniquely determined. (You may assume here that $\sqrt{2}$ is irrational.)

(iii) Carefully state the definition of the norm $N(\alpha)$ of an element $\alpha \in \mathbb{Z}[\sqrt{d}]$ (for $d \in \mathbb{Z}$ not square).

(iv) Carefully state the definition of a unit in a ring.

(v) Show that $\mathbb{Z}[\sqrt{-2}]$ has exactly two units; and that $\mathbb{Z}[\sqrt{2}]$ has infinitely many units.

(vi) Determine, giving reasons, which of the following inclusions of sets extend to inclusions of subrings:

(a) $\{0, 1\} \subseteq \mathbb{Z}$.

(b) $T \subseteq \mathbb{Q}$, where $T = \{x \in \mathbb{Q} : \; x = n/m$ for some $n, m \in \mathbb{Z}$ with $m \neq 0$ and $|m| < 17\}$.

(c) $U \subseteq M_2(\mathbb{Z})$, where $M_2(\mathbb{Z})$ is the ring of 2×2 matrices with integer entries; and

$$U = \{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \; : \; a, b \in \mathbb{Z} \}$$

(d) $U' \subseteq M_2(\mathbb{Z})$, where

$$U' = \{ \begin{pmatrix} a & b \\ c & a \end{pmatrix} \; : \; a, b, c \in \mathbb{Z} \}$$

(continued...)

2. Recall that a ring is, in particular, an abelian group; and that an ideal in a ring is also an abelian group. In this question we look at simple properties of ideals, starting with their properties as abelian groups.

(i) Show that the intersection of two subgroups of a group is a group.

(ii) Consider the abelian group $(\mathbb{Z}, +, 0)$. Explain the meaning of the notations $2\mathbb{Z}$ and $3\mathbb{Z}$ describing subsets of $\mathbb{Z}$. Show that these subsets form subgroups of $\mathbb{Z}$; and determine their intersection.

(iii) Let R be an abelian group, and S a subset of R. Write $\langle S\rangle$ for the intersection of all subgroups of R containing S. Show that $\langle S\rangle$ contains

(a) the identity element of R (as an abelian group);

(b) the inverses of all the elements of S;

(c) all finite sums of elements of S and their inverses.

(iv) Show that the intersection of two ideals in a ring R is an ideal in R.

(v) Let $S = \{s_1, s_2, ..., s_n\}$ be a subset of a ring R. Write (S) for the intersection of all ideals of R containing S. Show that

$$(S) = \langle\{rar' \mid r, r' \in R;\ a \in S\}\rangle$$

(vi) If R is a commutative ring, show that the set $aR = \{ar \ : \ r \in R\}$ is an ideal in R.

(vii) Let I be a non-trivial ideal in $\mathbb{Z}$ and let d be the smallest positive element in I.

(1) Show that $d\mathbb{Z} \subseteq I$.

(2) Show that there is no element $d' \in I \setminus d\mathbb{Z}$.

Hence prove that every ideal in $\mathbb{Z}$ is of the form $a\mathbb{Z}$ for some $a \in \mathbb{Z}$.

(continued. . .)

3. (i) Let R and S be rings. Define the notion of a *(ring) homomorphism* $\theta : R \to S$.

(ii) Suppose that $\theta : R \to S$ is a ring homomorphism. Show that $\theta(-a) = -\theta(a)$ for all $a \in R$.

(iii) Determine which of the following mappings are homomorphisms:

(1) $\theta : \mathbb{Z}[\sqrt{3}] \to \mathbb{Z}[\sqrt{3}]$ defined by $\theta(a + b\sqrt{3}) = a - b\sqrt{3}$ for $a, b \in \mathbb{Z}$.

(2) $\psi : \mathbb{Z} \to \mathbb{Z}[\sqrt{7}]$ defined by $\psi(a) = a\sqrt{7}$ for $a \in \mathbb{Z}$.

(3) $\phi : M_3(\mathbb{Z}[\sqrt{2}]) \to M_2(\mathbb{Z}[\sqrt{2}])$ defined by

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \mapsto \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

(recall that $M_n(R)$ is the ring of $n \times n$ matrices over a ring R).

(iv) Let I be an ideal in a ring R. Define a relation ρ_I on R by $(r, r') \in \rho_I$ if $r - r' \in I$. Show that ρ_I is an equivalence relation, and hence explain what is meant by the *factor ring* R/I.

(v) Give the multiplication table for the ring $\mathbb{Z}/3\mathbb{Z}$.

4. (i) Consider a polynomial $f \in \mathbb{Q}[x]$. For $r \in \mathbb{Q}$ we understand by $f(r) \in \mathbb{Q}$ the *evaluation* of f obtained by substituting r for x in f. Show that the set $A = \{f \in \mathbb{Q}[x] \ : \ f(3) = 1\}$ is not an ideal in $\mathbb{Q}[x]$.

(ii) Explain why the polynomial $x^4 - 5$ is irreducible over $\mathbb{Q}$, quoting or naming any theorem you use. Write the polynomial $x^4 - 5$ as a product of irreducible polynomials in $\mathbb{C}[x]$. Similarly, write the polynomial as a product of irreducible polynomials in $\mathbb{R}[x]$.

(iii) Determine, giving reasons, which of the following polynomials are irreducible over $\mathbb{Q}$:

(a) $x^3 + 12x + 4$.

(b) $x^4 + 8x^2 + 7$.

(c) $6x^4 + 10x^3 + 30x^2 + 10x + 27$.

(iv) Give the definition of a *primitive polynomial* in $\mathbb{Z}[x]$, and explain why the notion of a primitive polynomial applies to polynomials in $\mathbb{Z}[x]$ and not to polynomials in $\mathbb{Q}[x]$.

(v) Show that if p, p' are irreducible in $\mathbb{Q}[x]$ then $pp' + 1$ contains an irreducible factor that is an associate neither of p nor of p'. (You may assume that $\mathbb{Q}[x]$ is a Unique Factorisation Domain.) Extend your argument to show that $\mathbb{Q}[x]$ has infinitely many associate-classes of irreducibles.

(vi) Write down the Maclaurin series for $f(x) = \frac{1}{1-x}$. The polynomial $1 - x$ is irreducible in $\mathbb{Q}[x]$ and so in particular not a unit. Why does the existence of the Maclaurin series not contradict this assertion?

(continued...)

5. (i) Explain briefly what is meant by the notation $\mathbb{Q}(\sqrt{5})$.

(ii) Let $K \supseteq F$ be a field extension. Define what it means for an element $\alpha \in K$ to be *algebraic* over F.

(iii) Give an example of a number in $\mathbb{R} \setminus \mathbb{Q}$ that is algebraic over $\mathbb{Q}$. Take care to show explicitly that your number does *not* lie in $\mathbb{Q}$.

(iv) If α is algebraic over F, prove that there is a unique monic irreducible polynomial $m(x) \in F[x]$ which has α as a root (its *minimal polynomial*).

(v) Define the term *basis* of a vector space over a field F.

(vi) Determine a basis of $\mathbb{Q}(\sqrt{3-\sqrt{7}})$ over $\mathbb{Q}$.

(vii) Let $K \supseteq F$ be a field extension. Explain what is meant by the notation $[K : F]$.

(viii) Compute $[\mathbb{Q}(\sqrt{3-\sqrt{7}}) : \mathbb{Q}]$ and $[\mathbb{Q}(\sqrt{3-\sqrt{7}}) : \mathbb{Q}(\sqrt{7})]$, carefully explaining any assumptions you make, and theorems you use.

(ix) Let $\mathbb{Z}_2$ denote the field of order 2. Show that $x^2 + x + 1 \in \mathbb{Z}_2[x]$ is irreducible.

END