The University of Waikato
Department of Mathematics

Test 2 (**6:10pm**, 3 June, 2009)

MATH310A *Algebra and Number Theory* (2009)

The test is scheduled to last **90 minutes**. There are six questions each worth 18 marks: attempt any five. Total marks: 90 (one mark per minute!).

If you complete six questions then I will mark your FIRST FIVE and that will determine your mark. (Of course, these may not be your best five).

Throughout, let $\mathbb{N} = \{1, 2, 3, \ldots\}$ be the natural numbers, let $\mathbb{Z}$ be the ring of integers, let $\mathbb{R}$ be the field of real numbers and let $\mathbb{C}$ be the complex number field.

1. (a) **[5 marks.]** Prove from first principles (which means from the definition of a ring), that in any ring R, $0a = 0$ for all $a \in R$.You may assume all the usual properties of abelian groups.

   (b) **[6 marks.]** Let A be an abelian group. Prove that A is a ring if we define $a \cdot b = 0$ for all $a, b \in A$. (This means showing the laws involving multiplication are all satisfied.)

   (c) **[3 marks.]** Show that the cancellation law

   $$a \neq 0,\ ab = ac \ \Rightarrow\ b = c$$

   holds for all elements a, b, c of an integral domain R.

   (d) **[4 marks.]** Show that if $a, b \in R$, a ring with identity 1, and a, b have inverses $a', b' \in R$ respectively, then ab has inverse $b'a'$.

2. (a) **[2+2+6+3 marks.]**

   i. Let $\mathbb{F}$ be a field. What is the definition of an irreducible polynomial in $\mathbb{F}[x]$?

   ii. State the Factor Theorem for polynomials over a field.

   iii. Hence show that a polynomial of degree 3 has no zeros if it is irreducible.

   iv. Hence show the following polynomial in $\mathbb{Z}_3[x]$ is not irreducible:

   $$p(x) = x^3 + x^2 + x + 2.$$

   (b) **[1+3+1 marks.]**

   i. If $\mathbb{F}$ is a field, what is the largest number of zeros a polynomial of degree n can have?

   ii. Give three examples of degree 2 polynomials in $\mathbb{Z}_3[x]$ having each possible number of zeros.

   iii. Give an example of a polynomial in $R[x]$ for some choice of commutative ring R, having degree n but with more than n zeros.

TURN OVER

3. (a) **[5 marks.]** Let R be a ring with I an ideal of R. Then I is a subgroup of the abelian group $(R, +)$, and so R/I is a factor group. Show multiplication on the cosets given by

$$(a + I) \cdot (b + I) := ab + I$$

for all $a + I, b + I \in R/I$ is well-defined.

(b) **[5 marks.]** In $\mathbb{Z}[i]$, show that the subset $S = \{m + ni : m, n \text{ even integers}\}$ is an ideal.

(c) **[3 marks.]** With S as above, show that in $\mathbb{Z}[i]/S$,

$$((2 + 3i) + S) \cdot ((1 - i) + S) = (1 + 3i) + S.$$

(d) **[4 marks.]** How many elements does $\mathbb{Z}[i]/S$ have? List them.

(e) **[1 mark.]** $\mathbb{Z}[i]$ is a PID. Write down an element $a \in \mathbb{Z}[i]$ such that $S =< a >$ – no proof needed.

4. (a) **[3 marks.]** Let $\psi : R \to S$ be a homomorphism from ring R to ring S. Show that $ker(\psi)$ is an ideal of R. (You may assume it is a subgroup under addition.)

(b) **[5+6+4 marks.]** Let $\mathbb{F}$ be a field. Recall we can make the Cartesian product $\mathbb{F} \times \mathbb{F}$ a ring if we define, for all $(a, b), (c, d) \in \mathbb{F} \times \mathbb{F}$,

$$\begin{aligned} (a, b) + (c, d) &= (a + c, b + d), \\ (a, b) \cdot (c, d) &= (ac, bd). \end{aligned}$$

Define $f : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ by setting

$$f((a, b)) = b \text{ for all } (a, b) \in \mathbb{F} \times \mathbb{F}.$$

i. Show that f is a homomorphism.

ii. Use the Homomorphism Theorem for rings (= first isomorphism for rings) to deduce that the subset $\{(a, 0) : a \in \mathbb{F}\}$ is a maximal ideal of $\mathbb{F} \times \mathbb{F}$.

iii. Let I be an ideal of $\mathbb{F} \times \mathbb{F}$ containing at least one element (α, β) for which neither α nor β is zero. Show $I = \mathbb{F} \times \mathbb{F}$.

CONTINUED

5. In an integral domain R, recall that $a, b \in R$ are said to be *associates* if $a = \alpha b$ for some unit $\alpha \in R$. It may be useful to observe that if $\alpha, \beta \in R$ are units, so are $\alpha\beta$ (inverse is $\alpha^{-1}\beta^{-1}$) and α^{-1} itself (inverse is α).

   (a) **[6 marks.]** Prove that the binary relation $\approx$ defined on R and given by

   $$a \approx b \Leftrightarrow \ a \text{ and } b \text{ are associates}$$

   is an equivalence relation on R.
   (Recall this means you must show it is reflexive, symmetric and transitive. So for all $a, b, c \in R$: (i) $a \approx a$; (ii) if $a \approx b$ then $b \approx a$; and (iii) if $a \approx b$ and $b \approx c$ then $a \approx c$.)

   (b) **[3 marks.]** Show also that if $a, b, c, d \in R$, with $a \approx b$ and $c \approx d$, then $ac \approx bd$.

   (c) **[3 marks.]** However, give an example to show that if $a, b, c, d \in R$, with $a \approx b$ and $c \approx d$, then it need not be the case that $a + c \approx b + d$. (*Hint:* first pick R, then a, b, c, d, to give the counterexample.)

   (d) **[2 marks.]** For any $a \in R$, show that the equivalence class under $\approx$ containing a is the set

   $$S_a = \{\alpha a : \alpha \text{ a unit in } R\}.$$

   (e) **[4 marks.]** Letting $R = \mathbb{Z}[i]$, find the equivalence class under $\approx$ containing $2 + i$. List the elements in the form $a + bi$, $a, b \in \mathbb{Z}$. (*Hint:* there are only four units in $\mathbb{Z}[i]$.)

6. (a) **[4+6 marks.]** Let R be a ring. Define the operation $* : R \times R \to R$ by setting

   $$a * b := ab + ba,$$

   for all $a, b \in R$. This operation is easily seen to be commutative, even if the original ring product is not.

   i. Show that $*$ distributes over $+$: for all $a, b, c \in R$,

   $$a * (b + c) = (a * b) + (a * c).$$

   (The other distributive law holds automatically because $*$ is commutative!)

   ii. Not all the ring laws work though: examples can be found to show $*$ is not associative. However, show that the following limited form of associativity does hold: for all $a, b \in R$,

   $$(a * b) * (a * a) = a * (b * (a * a)) \text{ } \textit{(Jordan identity).}$$

   (b) **[8 marks.]** Given a ring R, its *opposite ring* R^{op} is defined from R by retaining the same definition of $+$, but by defining a new product $a \circ b := ba$ for all $a, b \in R$. It is routine to check that $(R^{op}, +, \circ)$ is a ring too.
   Obviously if R is commutative, then $R = R^{op}$. However, R and R^{op} can be isomorphic at other times. Show that the ring $M_n(\mathbb{R})$ of all $n \times n$ matrices over the reals $\mathbb{R}$ is isomorphic to its opposite, with an isomorphism $f : M_n(\mathbb{R}) \to M_n(\mathbb{R})$ being given by $f(A) = A^t$ for all $A \in M_n(\mathbb{R})$, where A^t denotes the transpose of A. (Thus, prove this f is an isomprphism!)
   (*Hint:* recall the following useful properties of transpose: $(A + B)^t = A^t + B^t$, $(AB)^T = B^t A^t$, and $(A^T)^T = A$ for all $A, B \in M_n(\mathbb{R})$.)