MATH 247

EXAMINER: Dr. J. Woolf, EXTENSION 44052.

TIME ALLOWED: Two and a half hours

Answer all of Section A and THREE questions from Section B. The marks shown against questions, or parts of questions, indicate their relative weight. Section A carries 55% of the available marks.

SECTION A

1. Give a description of those integers n for which there is a finite field with n elements. For each of the following numbers decide if there is a finite field with that many elements and, if there is a finite field with that any elements, give an example. (You should briefly justify your answer but are NOT required to go into details.)

(i) 19,

(ii) 54,

(iii) 9. [9 marks]

2. Decide whether or not the abelian groups

$$A = \langle a, b \mid 4a + 6b, 3a + 3b \rangle \quad \text{and} \quad B = \langle a, b, c \mid a + 3c, b - 4c, 2b - 2c \rangle$$

(given in terms of generators and relations) are isomorphic. To obtain full marks you should justify your answer. [9 marks]

3. Let R be a commutative ring with identity. Say what is meant by a *unit* in R. In each of the following cases say whether the element r is a unit in the ring R. To obtain full marks you should justify your answers.

(i) $R = \mathbf{Q}$, $r = 3$,

(ii) $R = \mathbf{Z}/6\mathbf{Z}$, $r = 3$,

(iii) $R = \mathbf{Z}/8\mathbf{Z}$, $r = 3$,

(iv) $R = \mathbf{Z}[x]$, $r = x^2$,

(v) $R = \mathbf{Z}[i]$, $r = 1 - i$. [9 marks]

4. Let R be a commutative ring with identity. Say what is meant by an *irreducible* element of R. In each of the following cases say whether the polynomial $f = x^3 + x + 1$ is irreducible in the ring R. Justify your answers.

(i) $R = (\mathbf{Z}/5\mathbf{Z})[x]$,

(ii) $R = \mathbf{Q}[x]$,

(ii) $R = \mathbf{R}[x]$. [9 marks]

5. Find all the homomorphisms of abelian groups $\theta : \mathbf{Z}/12\mathbf{Z} \to \mathbf{Z}/12\mathbf{Z}$. For each homomorphism find the kernel and the image and hence decide whether or not it is an isomorphism. [9 marks]

6. Find the greatest common divisor $\gcd(\alpha, \beta)$ in $\mathbf{Z}[i]$ of $\alpha = 2 - 5i$ and $\beta = 2 + 2i$. Also find Gaussian integers $\gamma, \delta \in \mathbf{Z}[i]$ with

$$\gcd(\alpha, \beta) = \alpha\gamma + \beta\delta.$$

[10 marks]

SECTION B

7. Give the definition of a homomorphism of abelian groups. Give the definition of a homomorphism of rings. (Here 'rings' should be taken to mean commutative rings with multiplicative identity.)

For each map φ below decide whether it is (a) a homomorphism of abelian groups (where the abelian group structure is given by addition) and (b) a homomorphism of rings. You should give brief justifications of your answers.

(i) $\varphi : \mathbf{Z} \to \mathbf{Z} : m \mapsto 2m$,

(ii) $\varphi : \mathbf{Z} \to \mathbf{Z} : m \mapsto m^3$,

(iii) $\varphi : (\mathbf{Z}/3\mathbf{Z})[x] \to (\mathbf{Z}/3\mathbf{Z})[x] : f \mapsto f^3$,

(iv) $\varphi : \mathbf{Z}[x] \to \mathbf{C} : f \mapsto f(1 + i)$. [15 marks]

8. Say what is meant by a *prime ideal* of a ring R. In each case below, decide whether the ideal I of the ring R is prime or not. To obtain full marks you should justify your answers.

(i) $I = 6\mathbf{Z}$ and $R = \mathbf{Z}$,

(ii) $I = 13\mathbf{Z}$ and $R = \mathbf{Z}$,

(iii) $I = \{f \in \mathbf{Q}[x] \mid f(8) = 0\}$ and $R = \mathbf{Q}[x]$.

(iv) $I = \langle x^2 + 1 \rangle$ and $R = \mathbf{C}[x]$. [15 marks]

9. For each n below, find all the abelian groups (up to isomorphism) of size n. For each isomorphism class you find give the table of factors, and the p-primary and Smith normal form decompositions of the group.

(i) $n = 45$;

(ii) $n = 72$. [15 marks]

10. Let $R = (\mathbf{Z}/2\mathbf{Z})[x]$ and let $I \subset R$ be the ideal generated by

$$f = x^4 + x + 1.$$

Show that f is irreducible in R.

(i) Write down the number of elements in the quotient ring R/I and the number of elements in $(R/I)^*$. State the possible orders of elements in $(R/I)^*$.

(ii) Find the order of the element x in $(R/I)^*$.

(iii) Give an example of an element of each possible order in $(R/I)^*$.

[15 marks]

11. (a) State Bézout's theorem for the ring $\mathbf{Q}[x]$. Explain briefly why the quotient ring $\mathbf{Q}[x]/\langle f\rangle$ is a field if $f \in \mathbf{Q}[x]$ is irreducible. [6 marks]

(b) Use the Euclidean algorithm to find a multiplicative inverse for $x^2 + 1$ in each of the quotient rings

(a) $\mathbf{Q}[x]/\langle x^3 + x + 1\rangle$ and,

(b) $\mathbf{Q}[x]/\langle x^3 + x^2 + 1\rangle$. [9 marks]