The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Spring Semester 2010–2011**

Rings and Groups **2 hours**

Answer ***all questions****.*

Question 1 is multiple choice; there is exactly one correct answer in each case. You will be awarded one mark for each correct answer and no marks for each incorrect answer. You are not required to justify your answers.

For questions 2–5 you should justify your answers carefully unless the question states otherwise.

1 Multiple choice. You should write down exactly one answer to each of the following twenty questions. **Please write down your answers in a clear list, separate from any rough work.** You are not required to justify your answers.

(i) Which of the following is the multiplicative inverse of 51 in $\mathbb{Z}_{1523}$?

(a) 1472

(b) 0.02

(c) 657

(d) -51

(ii) Which of the following rings is an integral domain?

(a) $\mathbb{Z}_{187}$

(b) $\mathbf{Mat}_7(\mathbb{Z})$

(c) $\mathbb{Z}_7[x]$

(d) $\mathbb{Z}_{38}$

(iii) Which of the following rings is not commutative?

(a) $\mathbb{Z}$

(b) $\mathbb{C}$

(c) $\mathbb{Z}_6[x]$

(d) $\mathbf{Mat}_5(\mathbb{R})$

(iv) Which of the following is a subring of $\mathbb{Z}$?

(a) $\mathbb{Z}_5$

(b) The odd numbers

(c) The even numbers

(d) $\mathbb{Z}$

(v) Which of the following is the best statement of the fact that a ring R has a multiplicative identity?

(a) $1.x = x = x.1$

(b) For all $a \in R$ there exists $e \in R$ such that $e.a = a = a.e$

(c) For all $a \in R$ there exists $b \in R$ such that $a.b = e = b.a$

(d) There exists $e \in R$ such that for all $a \in R$ $e.a = a = a.e$

(vi) Which of the following is not a ring axiom?

(a) $\forall a, b, c \in R \quad (ab)c = a(bc)$

(b) $\exists 1 \in R$ s.t. $\forall a \in R \quad a.1 = a = 1.a$

(c) $\exists 0 \in R$ s.t. $\forall a \in R \quad a + 0 = a = 0 + a$

(d) $\forall x \in R \quad -1.x = -x$

 Question 1 continued on next page

1 (continued)

(vii) Let R be a commutative ring. Which of the following statements implies that $r \in R$ is not a unit?

(a) There exists $s \neq 0 \in R$ such that $rs = 0$.

(b) For all $s \in R$, $rs = 0 \implies s = 0$.

(c) For all $s \in R$, $rs = 1$.

(d) There exists $s \in R$ such that $rs \neq 1$.

(viii) What are the units in $\mathbb{Z}[\sqrt{-17}]$?

(a) 1

(b) $1, -1$

(c) $1, -1, i, -i$

(d) There are infinitely many of them.

(ix) What are the units in $\mathbb{Z}[\sqrt{11}]$?

(a) 1

(b) $1, -1$

(c) $1, -1, i, -i$

(d) There are infinitely many of them.

(x) How many solutions are there in $\mathbb{Z}_{12}$ to the equation

$$x^2 = 1?$$

(a) none

(b) 2

(c) 4

(d) 8

(xi) In the symmetric group S_6 how many elements are there in the conjugacy class of the element $(13)(24)$?

(a) 15

(b) 45

(c) 90

(d) 180

 Question 1 continued on next page

1 (continued)

(xii) Let α be an element of the symmetric group S_9 with

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 4 & 3 & 2 & 5 & 6 & 1 & 7 & 9 \end{pmatrix}.$$

Writing α in disjoint cycle notation gives:

(a) (187)(24)(3569)

(b) (178)(24)

(c) (42)(718)

(d) (843256179)

(xiii) What is the order of D_5, the symmetry group of a regular pentagon?

(a) 5

(b) 10

(c) 20

(d) 120

(xiv) What is the order of the element a^7 in the cyclic group of order 28 generated by a?

(a) 2

(b) 4

(c) 7

(d) 28

(xv) Which of the following groups is isomorphic to the symmetric group S_3?

(a) C_3

(b) $\mathbb{Z}_6$

(c) A_4

(d) D_3

(xvi) What is the class equation of a cyclic group of order 8?

(a) $1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 = 8$

(b) $1 + 1 + 1 + 1 + 2 + 2 = 8$

(c) $1 + 1 + 2 + 2 + 2 = 8$

(d) $1 + 1 + 2 + 4 = 8$

 Question 1 continued on next page

1 (continued)

(xvii) What is the class equation of A_4?

(a) $1+3+6+6+8=24$

(b) $1+1+2+2+2=8$

(c) $1+3+4+4=12$

(d) $1+3+8=12$

(xviii) What is the order of the quotient group S_9/A_9?

(a) 2

(b) 9

(c) 18

(d) 36

(xix) Let θ be a surjective homomorphism $S_6 \longrightarrow S_4$. What is the order of the kernel of θ?

(a) 1

(b) 6

(c) 24

(d) 30

(xx) Let θ be an injective homomorphism $S_3 \longrightarrow S_4$. What is the order of the image of θ?

(a) 1

(b) 4

(c) 6

(d) 24

(20 marks)

2 (i) Is 44 a unit or a zero-divisor in $\mathbb{Z}_{1881}$? If it is a unit find its inverse, and if it is a zero-divisor find a non-zero element $b \in \mathbb{Z}_{1881}$ such that $44b \equiv 0$.
(5 marks)

(ii) Write down the units in $\mathbb{Z}_8$. Is the multiplicative group they form cyclic? Justify your answers carefully. ***(6 marks)***

(iii) Let R be a commutative ring. Prove that an element r of R cannot be both a unit and a zero-divisor. ***(4 marks)***

Additional marks for rigour and presentation. ***(5 marks)***

3 (i) Let $d \neq 1$ be a square-free integer. Define $\mathcal{N}(r)$, the norm of an element $r \in \mathbb{Z}[\sqrt{d}]$. Explain how we can use norms to identify units in $\mathbb{Z}[\sqrt{d}]$.
(4 marks)

(ii) Let d be a square-free integer and $r \in \mathbb{Z}[\sqrt{d}]$. Prove that if $\mathcal{N}(r)$ is a prime number then r is irreducible in $\mathbb{Z}[\sqrt{d}]$. You may use the fact that $\mathcal{N}(st) = \mathcal{N}(s).\mathcal{N}(t)$. ***(4 marks)***

(iii) Consider the following two factorisations of 29 in $\mathbb{Z}[i]$:

$$29 = (2 + 5i)(2 - 5i)$$

$$29 = (5 - 2i)(5 + 2i)$$

Do these two factorisations show that $\mathbb{Z}[i]$ is not a unique factorisation domain? ***(4 marks)***

(iv) Let R be a unique factorisation domain and S a subring of R. Is S necessarily a unique factorisation domain? Justify your answer briefly.
(3 marks)

Additional marks for rigour and presentation. ***(5 marks)***

4 (i) Let G be a group of order 10 with trivial centre. Find the class equation for G and find the number of elements of order 5 in G. ***(8 marks)***

(ii) Let H be a normal subgroup of a group G. Describe the quotient group G/H. (You need to specify what the elements are, how multiplication on G/H is defined, what the identity is, and what the inverse of a given element is, but you do not need to prove any of your assertions.) ***(4 marks)***

(iii) Explain how the additive group $\mathbb{Z}_n$ of the integers mod n can be constructed as a quotient group. ***(3 marks)***

Additional marks for rigour and presentation. ***(5 marks)***

5 Consider the square divided into small squares labelled 1, 2, 3, 4 and 5 as below.

1	4	3
2	5	2
3	4	1

Recall that D_4 is the group of symmetries of the square. Observe that D_4 acts on the numbered squares above inducing a homomorphism $f : D_4 \longrightarrow S_5$.

(i) Write down the effect of f on each element of D_4. ***(6 marks)***

(ii) Write down the kernel and image of the homomorphism f. Is f injective? Is f surjective? ***(4 marks)***

(iii) State, without proof, the First Isomorphism Theorem for groups. ***(2 marks)***

(iv) What does the First Isomorphism Theorem tell us in this case? ***(3 marks)***

Additional marks for rigour and presentation. ***(5 marks)***

End of Question Paper