MATH50005

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May 2024

This paper is also taken for the relevant examination for the
Associateship of the Royal College of Science

Groups and Rings

Date: Friday, May 17, 2024

Time: 10:00 – 12:00 (BST)

Time Allowed: 2 hours

This paper has 4 Questions.

Please Answer Each Question in a Separate Answer Booklet

Candidates should start their solutions to each question on a new sheet of paper.

Supplementary books may only be used after the relevant main book(s) are full.

Any required additional material(s) will be provided.

Allow margins for marking.

Credit will be given for all questions attempted.

Each question carries equal weight.

DO NOT OPEN THIS PAPER UNTIL THE INVIGILATOR TELLS YOU TO

1. (a) (i) Give the definition of an *action* of a group G on a set X. (1 mark)

(ii) Give the definition of a *faithful* action. (1 mark)

(iii) Give the definition of a *transitive* action. (1 mark)

(iv) Let G be a finite group acting on a finite set X. You are asked to give a proof or a counterexample to each of the following statements. (You can use all results from the course if you state them clearly.)

(1) Suppose that an element $g \in G$ has no fixed point in X. Can we conclude that G acts faithfully on X? Can we conclude that G acts transitively on X? (3 marks)

(2) Suppose that G acts transitively on X. Can we conclude that there is an element $g \in G$ that has no fixed point in X? (2 marks)

(b) Let S_n be the group of permutations of $\{1, \dots, n\}$.

(i) What is the maximal order of a cyclic subgroup of S_8? (Justify your answer.) (5 marks)

(ii) Let X be the set of subgroups $G \subset S_4$ such that $|G| = 4$. The group S_4 acts on X by conjugation, i.e., a permutation $\sigma \in S_4$ sends a subgroup G to $\sigma G \sigma^{-1}$. How many S_4-orbits are there in X? (Justify your answer. You can use all results from the course if you state them clearly.) (7 marks)

(Total: 20 marks)

2. (a) (i) Give the definition of the *Smith normal form*. (2 marks)

(ii) State the main theorem concerning the Smith normal form of a matrix. (No proof is required.) (1 mark)

(iii) Reduce the matrix

$$\begin{pmatrix} 0 & 6 & 2 \\ 2 & 0 & 4 \end{pmatrix}$$

to the Smith normal form. (4 marks)

(iv) Using your result in part (iii), or otherwise, determine the quotient group of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ by the subgroup generated by the rows of the matrix in (iii). (3 marks)

(b) (i) Give the definition of a *simple group*. (1 mark)

(ii) Let G be a group with $2p$ elements, where p is a prime number. Prove that G is not a simple group. (You can use all results from the course if you state them clearly.) (4 marks)

(iii) Let G be a group with p^n elements, where p is a prime number and $n \geq 2$. Prove that G is not a simple group. (You can use all results from the course if you state them clearly.) (5 marks)

(Total: 20 marks)

3. (a) Let k be a field. Let $f(t) \in k[t]$ be an irreducible polynomial. Briefly explain why there exists a finite field extension $k \subset K$ such that $f(t)$ has a root in K. (No proofs are required.) (2 marks)

In parts (b), (c), (d), (e) you are asked to justify your solution. You can use all results from the course if you state them clearly.

(b) Give a construction of fields with 3, 9 and 27 elements. (4 marks)

(c) Let k be a field with 27 elements. What are the positive integers n such that the multiplicative group $k^\times$ has an element of order n? (3 marks)

(d) Let K be a field with subfields $k_1 \subset K$ and $k_2 \subset K$ such that $|k_1| = 9$ and $|k_2| = 27$. What can you say about $k_1 \cap k_2$? (5 marks)

(e) Let p be a prime number and let n be a positive integer. Prove that a field with p^{2n} elements contains a unique subfield with p^2 elements. (6 marks)

(Total: 20 marks)

4. (a) (i) Give the definition of an *integral domain*. (1 mark)

(ii) Prove that $R = \{a + b\sqrt{5} | a, b \in \mathbb{Z}\}$ is an integral domain. (1 mark)

(ii) Let R be the ring defined in part (ii). Which of the following elements of R are invertible, irreducible, or neither of the two:

$$\sqrt{5}, \quad 2+\sqrt{5}, \quad 4+\sqrt{5}, \quad 5+\sqrt{5}\,?$$

(Justify your answer.) (8 marks)

(b) (i) Give the definition of a *unique factorisation domain*. (1 mark)

(ii) Explain why the rings $\mathbb{Z}$, $\mathbb{R}[t]$, $\mathbb{Z}[\sqrt{-1}]$ are unique factorisation domains. (Justify your answer. You can use all results from the course if you state them clearly.) (4 marks)

(iii) Is $\{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$ a unique factorisation domain? (Justify your answer.)
Hint: you may consider the equality $2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. (5 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2024

This paper is also taken for the relevant examination for the Associateship.

MATH50005

Groups and Rings (Solutions)

Setter's signature	Checker's signature	Editor's signature
....	....	....

1. (a) (i) Let $S(X)$ be the group of bijections $X \to X$ with composition as the group law. An action of G on X is a homomorphism $G \to S(X)$. seen/sim.seen ⇓ 1, A

(ii) An action of a group G on a set X is faithful if the map $G \to S(X)$ is injective. 1, A

(iii) An action of G on X is transitive if there is only one G-orbit in X. Explicitly, for any $x, x' \in X$ there is an element $g \in G$ such that $x' = g(x)$. 1, A

(iv) (1) No to both questions. The subgroup $G \subset S_4$ generated by $g = (12)(34)$ does not act transitively on $\{1, 2, 3, 4\}$, but g acts without fixed point. Now let H be a group with more than one element that acts trivially on $\{1, 2, 3, 4\}$. Then $G \times H$ acts on $\{1, 2, 3, 4\}$ but this action is not faithful. 3, A

(2) Yes, by Jordan's theorem. 2, A

(b) (i) Write a generator g of a cyclic subgroup of S_8 as a product of independent cycles. Let $n_1, n_2, \ldots$ be the lengths of these cycles. The order of g equals the l.c.m. of the numbers n_i, $i = 1, 2, \ldots$. The highest order $15 = 3 \times 5$ is achieved when there are two independent cycles of orders 3 and 5. unseen ⇓ 5, B

(ii) By lectures, a group with 4 elements is isomorphic to C_4 or to $C_2 \times C_2$. A cyclic group of order 4 in S_4 is generated by a 4-cycle. All 4-cycles are conjugate in S_4, so the subgroups of S_4 isomorphic to C_4 form one orbit under conjugation. Next, a subgroup of S_4 isomorphic to $C_2 \times C_2$ is generated by two commuting permutations of order 2. If one of them is a transposition (ab), then the other one must be (cd) or $(ab)(cd)$, where $\{a, b, c, d\} = \{1, 2, 3, 4\}$, so this subgroup is generated by (ab) and (cd). After a conjugation, we can assume that $(ab) = (12)$ and $(cd) = (34)$, thus all such subgroups are conjugate. In the course we have seen that two permutations of order 2, each of which is a product of two transpositions, generate Klein's 4-group, which is a normal subgroup of S_4. Thus there are three S_4-orbits in X. 7, C

2. (a) (i) An $(m \times n)$-matrix (a_{ij}) with integer entries is in Smith normal form if $a_{ij} = 0$ for $i \neq j$; for some integer $k \geq 0$ we have $a_{ii} > 0$ for $i \leq k$ and $a_{ii} = 0$ for $i > k$; and we have divisibility $a_{11}|a_{22}|\dots|a_{kk}$.

seen ⇓

2, A

(ii) Any matrix with integer entries can be brought into Smith normal form using elementary row and column operations.

1, A

(iii)

$$\begin{pmatrix} 0 & 6 & 2 \\ 2 & 0 & 4 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 4 \\ 0 & 6 & 2 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 6 & 2 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 6 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$$

meth seen ⇓

4, B

(iv) The quotient of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ by the subgroup $(2\mathbb{Z}) \times (2\mathbb{Z}) \times \mathbb{Z}$ is isomorphic to $(\mathbb{Z}/2) \times (\mathbb{Z}/2) \times \mathbb{Z}$.

3, B

(b) (i) A group G is called simple if it has no normal subgroups other than $\{e\}$ and G.

seen/sim.seen ⇓

1, A

(ii) By Cauchy's theorem, G contains an element g of order p. The subgroup of G generated by g has index 2, so must be normal. It has p elements, so is not equal to either $\{e\}$ or G.

4, A

(iii) By lectures, a group G with p^n elements has non-trivial centre: $Z(G) \neq \{e\}$. By lectures, $Z(G)$ is a normal subgroup of G. Thus if $Z(G) \neq G$, the group G is not simple. If $Z(G) = G$, then G is abelian. Hence, by lectures, G is isomorphic to a product of cyclic groups. If this product has more than one factor, then G is not simple. A cyclic group of order p^n, $n \geq 2$, contains a subgroup isomorphic to C_p, hence it is not simple.

5, D

3. (a) In lectures we proved that the quotient ring $K = k[t]/f(t)k[t]$ is a field extension of k of degree $\deg f(t)$. Let $\tau \in K$ be the image of $t \in k[t]$ under the canonical surjective map $k[t] \to K$. In K we have $f(\tau) = 0$, so $\tau \in K$ is a root of $f(t)$. $\boxed{\text{seen} \Downarrow}$ $\boxed{2, \text{A}}$

(b) Every non-zero element in the ring $\mathbb{F}_3 := \mathbb{Z}/3$ is invertible, so this is a field. $\boxed{\text{meth seen} \Downarrow}$

The polynomial $t^2 + 1 \in \mathbb{F}_3[t]$ has no roots in $\mathbb{F}_3$, hence is irreducible. Thus $\mathbb{F}_9 := \mathbb{F}_3[t]/(t^2+1)\mathbb{F}_3[t]$ is a field with 9 elements.

The polynomial $t^3 - t + 1 \in \mathbb{F}_3[t]$ has no roots in $\mathbb{F}_3$, hence is irreducible. Thus $\mathbb{F}_{27} := \mathbb{F}_3[t]/(t^3 - t + 1)\mathbb{F}_3[t]$ is a field with 27 elements. $\boxed{4, \text{A}}$

(c) By lectures, the multiplicative group $k^\times$ is cyclic, so $k^\times \cong C_{26}$. A cyclic group C_n contains an element of order m if and only if m divides n. Thus the possible orders are $1, 2, 13, 26$. $\boxed{\text{unseen} \Downarrow}$ $\boxed{3, \text{A}}$

(d) The set $k := k_1 \cap k_2$ is closed under the field operations, so it is a subfield of K. The field k_1 is a vector space over k, so $|k_1| = |k|^n$. Thus $|k|$ is a power of 3, and hence $|k|$ is 3 or 9. The same argument with k_1 replaced by k_2 gives that $|k|$ is 3 or 27. We conclude that k is the field with 3 elements. By lectures, it is unique up to isomorphism, hence $k \cong \mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$. $\boxed{\text{unseen} \Downarrow}$ $\boxed{5, \text{C}}$

(e) Let K be a field with p^{2n} elements. As proved in lectures, the polynomial $t^{p^{2n}} - t$ is a product of $t - \alpha$, for all $\alpha \in K$. The polynomial $t^{p^2} - t$ divides $t^{p^{2n}} - t$ in $K[t]$. Indeed, $t^{p^2-1} - 1$ divides $t^{p^{2n}-1} - 1 = (t^{p^2-1})^m - 1$, where $m = (p^{2n}-1)/(p^2-1)$ is an integer. Thus $t^{p^2} - t$ has exactly p^2 roots in K. In lectures we proved that this set of roots is closed under field operations, so is a subfield of K with p^2 elements. Conversely, let $k \subset K$ be a subfield with p^2 elements. Since $k^\times$ is a cyclic group, the elements of k are roots of $t^{p^2} - t$. This proves uniqueness. $\boxed{\text{meth seen} \Downarrow}$ $\boxed{6, \text{D}}$

4. (a) (i) A commutative ring without zero-divisors is called an integral domain. A zero-divisor is a non-zero element a such that $ab = 0$ for some $b \neq 0$. seen ⇓

1, A

(ii) R is a subset of the field $\mathbb{R}$ closed under ring operations and containing 1, so R is a commutative ring. There are no zero-divisors in $\mathbb{R}$, so there are no zero-divisors in R, so R is an integral domain. 1, A

(iii) The function $f\colon R \to \mathbb{Z}$ given by $f(a + b\sqrt{5}) = a^2 - 5b^2$ is multiplicative. We have $f(a + b\sqrt{5}) = \pm 1$ if and only if $a + b\sqrt{5} \in R^\times$. In particular, $2 + \sqrt{5}$ is invertible. It follows that if $f(a + b\sqrt{5}) = \pm p$, where p is a prime, then $a + b\sqrt{5}$ is an irreducible. In particular, $\sqrt{5}$ and $4 + \sqrt{5}$ are irreducibles. Finally, $5 + \sqrt{5} = \sqrt{5}(1 + \sqrt{5})$, where neither factor is invertible, hence $5 + \sqrt{5}$ is neither invertible nor irreducible. meth seen ⇓

8, B

(b) (i) An integral domain R is called a unique factorisation domain if every non-zero element of $R \setminus R^\times$ is a product of finitely many irreducibles, and this decomposition is unique up to changing the order of factors and multiplying the factors by elements of $R^\times$. seen ⇓

1, A

(ii) These rings are Euclidean domains (as proved in lectures and problem sheets), with the Euclidean norm of $n \in \mathbb{Z}$ defined as $|n|$, the Euclidean norm of a polynomial being its degree, and the Euclidean norm of $a + b\sqrt{-1}$ defined as $a^2 + b^2$. In lectures we proved that every Euclidean domain is a principal ideal domain, and that every principal ideal domain is a unique factorisation domain.

4, A

(iii) Let $R = \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$. Let $f\colon R \to \mathbb{Z}$ be the function $f(a + b\sqrt{-5}) = a^2 + 5b^2$. We have $a + b\sqrt{-5} \in R^\times$ if and only if $f(a + b\sqrt{-5}) = \pm 1$, which happens exactly when $a = \pm 1$ and $b = 0$. Thus $R^\times = \{\pm 1\}$. Working from the hint, we consider $2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. We have $f(2) = 4$, but since $f(a + b\sqrt{-5}) = \pm 2$ has no integer solutions, $2 \in R$ cannot be written as a product of two non-invertible elements of R, so 2 is an irreducible in R. The same argument shows that $3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are irreducibles in R. We note that they are not associates. Thus uniqueness of factorisation into a product of irreducibles fails in R, so R is not a unique factorisation domain. unseen ⇓

5, D

Review of mark distribution:

Total A marks: 32 of 32 marks
Total B marks: 20 of 20 marks
Total C marks: 12 of 12 marks
Total D marks: 16 of 16 marks
Total marks: 80 of 80 marks
Total Mastery marks: 0 of 20 marks

MATH50005 Groups and Rings

Question	Marker's comment
1	Question 1 turned out to be very hard. Many students could not give a definition of an action of a group on a set, which is bookwork, and could not answer relatively simple questions about transitive and faithful actions.
2	Q2 was easier than other questions, and was answered much better than Q1 and Q3.
3	Q3 turned out to be another hard question. Many students struggled with the structure of finite fields.
4	Most made a decent attempt at this questions. Several students failed to note that R is a subring of a field (the reals) and so cannot have zero divisors.nbsp;In part (a) (iii) many did not use the norm function. (b)(i) and (ii) were generally done well, in (b)(iii) many people did not prove that relevant elements were irreducible.