Imperial College
London

MATH50005

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May-June 2021

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

Groups and Rings

Date: Monday, 17 May 2021

Time: 09:00 to 11:00

Time Allowed: 2 hours

Upload Time Allowed: 30 minutes

This paper has 4 Questions.

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

Each sheet of paper should have your CID, Question Number and Page Number on the top.

Only use 1 side of the paper.

Allow margins for marking.

Any required additional material(s) will be provided.

Credit will be given for all questions attempted.

Each question carries equal weight.

SUBMIT YOUR ANSWERS AS SEPARATE PDFs TO THE RELEVANT DROPBOXES ON BLACKBOARD INCLUDING A COMPLETED COVERSHEET WITH YOUR CID NUMBER, QUESTION NUMBERS ANSWERED AND PAGE NUMBERS PER QUESTION.

1. (a) Let G be a group and let $Z(G)$ be the centre of G.

(i) What is an alternative way of saying $Z(G) = G$?

(ii) Give an example of a group G such that $|G| = 6$ and $Z(G) \neq \{e\}$. Give an example of a group G such that $|G| = 6$ and $Z(G) = \{e\}$. (No proofs are required.)

(iii) Does there exist a group G such that $|G| > 2$ but $|Z(G)| = 2$? Give an example, or prove that such a group does not exist.

(iv) Does there exist a group G such that the index of $Z(G)$ in G is 2? Give an example, or prove that such a group does not exist.

(9 marks)

(b) (i) What can you say about the centre of a simple group?

(ii) For each integer n such that $2 \leq n \leq 11$ determine if there exists a simple group G such that $|G| = n$. (You need to justify your answer. You can use any results from the course if you state them clearly.)

(11 marks)

(Total: 20 marks)

2. (a) Let G be a finite group acting on a set X. Let $x \in X$.

(i) Give the definition of the orbit of x and the definition of the stabiliser of x in G. State (without proof) a relationship between the sizes of these.

(ii) Prove that the stabilisers of points in the same orbit are conjugate subgroups of G.

(iii) The permutation group S_8 acts on the set of elements of order 6 in S_8 by conjugation. How many orbits are there? (You need to justify your answer. You can use any results from the course if you state them clearly.)

(12 marks)

(b) Let $\mathbb{F}_2 = \{0, 1\}$ be the field with 2 elements. Let $G = \mathrm{GL}(2, \mathbb{F}_2)$ be the group of invertible (2×2)-matrices with entries in $\mathbb{F}_2$ acting on the set of column vectors $(\mathbb{F}_2)^2$.

(i) Determine the orbits of G in $(\mathbb{F}_2)^2$ and the order of the stabilisers of points in each orbit.

(ii) For $g \in G$ let $\mathrm{Fix}(g)$ be the set of vectors $v \in (\mathbb{F}_2)^2$ such that $g(v) = v$. Determine all integers n for which there is an element $g \in G$ such that $n = |\mathrm{Fix}(g)|$.

(8 marks)

(Total: 20 marks)

3. (a) Let k be a field.

(i) Give the definition of the characteristic of k.

(ii) Without quoting results from your notes, explain carefully why the characteristic of k cannot be 6.

(iii) Let $G = k^\times$ be the multiplicative group of k. Let G_{tors} be the torsion subgroup of G. Is it true that G_{tors} is always finite? Give a proof or a counter-example.

(iv) Let k be a field such that $|k^\times| = 1$. What can you say about the characteristic of k?

(9 marks)

(b) (i) Give an example of a commutative ring R and a maximal ideal of R.

(ii) Let R be an integral domain. Let $a \in R$ be an element such that aR is a maximal ideal of R. Can a be 0, an invertible element of R, an irreducible element of R, a non-zero element of R which is neither invertible nor irreducible? For each part of this question give an example or briefly explain why this is not possible.

(iii) Give a construction of a field with 125 elements. (You need to justify your solution. You can use any results from the course if you state them clearly.) (11 marks)

(Total: 20 marks)

4. (a) (i) Give an example of a prime ideal which is not maximal.

(ii) Give an example of an integral domain which is not a principal ideal domain. Justify your answer.

(iii) Do there exist a principal ideal domain R and a prime ideal $I \subset R$, $I \neq 0$, such that I is not a maximal ideal of R?

(8 marks)

(b) Let R be the ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$. For each of the following elements of R determine if it is an invertible element of R, an irreducible element of R, or neither invertible nor irreducible:

$$\text{(i) } \sqrt{2}, \quad \text{(ii) } 1+\sqrt{2}, \quad \text{(iii) } 2+\sqrt{2}, \quad \text{(iv) } 3+\sqrt{2}, \quad \text{(v) } 4+\sqrt{2}, \quad \text{(vi) } 5+\sqrt{2}.$$

Hint: Use the multiplicativity of the function $R \to \mathbb{Z}$ that sends $m + n\sqrt{2}$ to $m^2 - 2n^2$.

(12 marks)

(Total: 20 marks)

1. (a) *Let G be a group and let $Z(G)$ be the centre of G.*

(i) *What is an alternative way of saying $Z(G) = G$?*

1, A

We have $Z(G) = \{g \in G | gh = hg \text{ for any } h \in G\}$. Thus $Z(G) = G$ if and only if G is abelian.

seen ⇓

(ii) *Give an example of a group G such that $|G| = 6$ and $Z(G) \neq \{e\}$. Give an example of a group G such that $|G| = 6$ and $Z(G) = \{e\}$. (No proofs are required.)*

2, A

Examples are: the cyclic group C_6 for the first question and the symmetric group S_3 for the second question.

seen ⇓

(iii) *Does there exist a group G such that $|G| > 2$ but $|Z(G)| = 2$? Give an example, or prove that such a group does not exist.*

3, B

Yes. Examples include the dihedral group D_8 and $C_2 \times S_3$. Indeed, the centre of $C_2 \times S_3$ is $C_2 \times \{e\}$, because the centre of S_3 is trivial.

sim. seen ⇓

(iv) *Does there exist a group G such that the index of $Z(G)$ in G is 2? Give an example, or prove that such a group does not exist.*

3, C

No. For any $g \in G$, $g \notin Z(G)$, the group G is generated by $Z(G)$ and g. Since g commutes with $Z(G)$ and g, we must have $G = Z(G)$, a contradiction.

sim. seen ⇓

(b) (i) *What can you say about the centre of a simple group? (No proof is required.)*

1, A

If a group G is simple then $Z(G) = \{e\}$ or $Z(G) = G$.

seen ⇓

(ii) *For each integer n such that $2 \leq n \leq 11$ determine if there exists a simple group G such that $|G| = n$. (You need to justify your answer. You can use any results from the course if you state them clearly.)*

5, A

5, D

If $n = p$ is prime ($n = 2, 3, 5, 7, 11$), then the cyclic group C_p is simple. (All subgroups of a cyclic group of order n are cyclic of order dividing n.) If $n = 2p$, where p is prime, then by Cauchy's theorem every group of order $2p$ contains a cyclic subgroup of order p, which has index 2, hence is normal. Thus the groups of orders $n = 4, 6, 10$ are not simple. Finally, let $n = p^m$, where p is a prime and $m \geq 2$ ($n = 8, 9$). By lectures, the centre $Z(G)$ of any group G of order p^m is not equal to $\{e\}$. If G is non-abelian, then $Z(G) \neq G$ hence G is not simple. Now assume that G is abelian. Any element of G generates a subgroup isomorphic to C_{p^a} for some $a \geq 1$, which contains a subgroup isomorphic to C_p. This is obviously a proper normal subgroup of G, so G is not simple.

unseen ⇓

2. (a) *Let G be a finite group acting on a set X. Let $x \in X$.*

(i) *Give the definition of the orbit of x and the definition of the stabiliser of x in G. State (without proof) a relationship between the sizes of these.*

3, A

The orbit of x is $G(x) = \{g(x) | g \in G\}$. The stabiliser of x is $St_G(x) = \{g \in G | g(x) = x\}$. We have $|G(x)| \cdot |St_G(x)| = |G|$.

seen ⇓

(ii) *Prove that the stabilisers of points in the same orbit are conjugate subgroups of G.*

3, A

If $h \in G$ is such that $h(x) = x$, then $(ghg^{-1})(g(x)) = g(h(x)) = g(x)$. We obtain that $gSt_G(x)g^{-1} \subset St_G(g(x))$. This holds for any $g \in G$ and any $x \in X$. Thus the inclusion will remain true if we replace x by $g(x)$ and g by g^{-1}. Then we obtain $g^{-1}St_G(g(x))g \subset St_G(x)$. Hence $St(g(x)) \subset gSt(x)g^{-1}$, so we are done.

seen ⇓

(iii) *The permutation group S_8 acts on the set of elements of order 6 in S_8 by conjugation. How many orbits are there? (You need to justify your answer. You can use any results from the course if you state them clearly.)*

6, B

By lectures, the conjugacy classes in S_n bijectively correspond to cycle shapes. The cycle shapes of permutations of order 6 in S_8 are as follows:

sim. seen ⇓

$$(6), (6)(2), (3)(2), (3)(3)(2), (3)(2)(2).$$

Thus there are 5 orbits.

(b) *Let $\mathbb{F}_2 = \{0, 1\}$ be the field with 2 elements. Let $G = \mathrm{GL}(2, \mathbb{F}_2)$ be the group of invertible (2×2)-matrices with entries in $\mathbb{F}_2$ acting on the set of column vectors $(\mathbb{F}_2)^2$.*

(i) *Determine the orbits of G in $(\mathbb{F}_2)^2$ and the order of the stabilisers of points in each orbit.*

3, B

By linear algebra, the orbits are $\{0\}$ and $(\mathbb{F}_2)^2 \setminus \{0\}$. The stabiliser of 0 is all of G, which has 6 elements. The stabiliser of any non-zero vector in $(\mathbb{F}_2)^2$ has 2 elements, e.g. by the orbit-stabiliser theorem.

unseen ⇓

(ii) *For $g \in G$ let $\mathrm{Fix}(g)$ be the set of vectors $v \in (\mathbb{F}_2)^2$ such that $g(v) = v$. Determine all integers n for which there is an element $g \in G$ such that $n = |\mathrm{Fix}(g)|$.*

5, D

The element $e \in G$ acts as the identity, so has 4 fixed points. By linear algebra, it is the only element of G that fixes two different non-zero vectors in $(\mathbb{F}_2)^2$, so every other element of G can fix at most one non-zero vector. By Jordan's theorem applied to the 3-element orbit $(\mathbb{F}_2)^2 \setminus \{0\}$, exactly three elements of G have $|\mathrm{Fix}(g)| = 2$, so the remaining two elements of G have $|\mathrm{Fix}(g)| = 1$. (A solution based on the isomorphism $G \cong S_3$, identifying the 3-element orbit with $\{1, 2, 3\}$, is also fine.)

unseen ⇓

3. (a) *Let k be a field.*

(i) *Give the definition of the characteristic of k.* [1, A]

For a positive integer n we denote by $n \cdot 1 \in k$ be the sum of n copies of $1 \in k$. If $n \cdot 1 \neq 0$ for any n, then $\mathrm{char}(k)$ is 0. If n is the smallest positive integer such that $n \cdot 1 = 0 \in k$, then $\mathrm{char}(k)$ is n. [seen ⇓]

(ii) *Without quoting results from your notes, explain carefully why the characteristic of k cannot be 6.* [2, A]

Assume that $\mathrm{char}(k) = 6$. Then $a = 2 \cdot 1$ and $b = 3 \cdot 1$ are non-zero elements of k such that $ab = 0$. This is a contradiction, because k is a field hence every non-zero element of k is invertible, so k has no zero-divisors. [seen ⇓]

(iii) *Let $G = k^\times$ be the multiplicative group of k. Let G_{tors} be the torsion subgroup of G. Is it true that G_{tors} is always finite? Give a proof or a counter-example.* [3, A]

No. Let $k = \mathbb{C}$. Then $(k^\times)_{\mathrm{tors}}$ consists of all complex roots of unity, of which there are infinitely many. [unseen ⇓]

(iv) *Let k be a field such that $|k^\times| = 1$. What can you say about the characteristic of k ?* [3, B]

The characteristic of k is 2. Otherwise, -1 and 1 are two different elements of k, so $k^\times$ contains more than one element. [unseen ⇓]

(b) (i) *Give an example of a commutative ring R and a maximal ideal of R.* [1, A]

The zero ideal of a field is such an example. [seen ⇓]

(ii) *Let R be an integral domain. Let $a \in R$ be an element such that aR is a maximal ideal of R. Can a be 0, an invertible element of R, an irreducible element of R, a non-zero element of R which is neither invertible nor irreducible? For each part of this question give an example or briefly explain why this is not possible.* [4, A]

Yes. $\{0\}$ is a maximal ideal of a field. [seen ⇓]

No. If $a \in R^\times$, then $aR = R$, but maximal ideals are proper ideals of R.

Yes. 2 is an irreducible element of $\mathbb{Z}$ which generates a maximal ideal.

No. If $a = bc$, where $b, c \neq 0$ and $b, c \notin R^\times$, then $aR \subsetneq bR \subsetneq R$, so aR is not maximal.

(iii) *Give a construction of a field with 125 elements. (You need to justify your solution. You can use any results from the course if you state them clearly.)* [6, D]

Let k be the field $\mathbb{Z}/5$. We search for an irreducible polynomial of degree 3. Each of the binomials $t^3 + a$, where $a \in k$, has a root in k, so we try a polynomial with three non-zero terms. The polynomial $t^3 + t + 1$ has no roots in k, hence by a result from lectures it is irreducible in $k[t]$. By part (ii) the ideal $(t^3 + t + 1)k[t]$ is maximal, hence $F = k[t]/(t^3 + t + 1)k[t]$ is a field. Each coset has a polynomial of degree at most 2 as a unique representative, so F has 125 elements. The addition and multiplication in F come from addition and multiplication of polynomials of degree at most 2 modulo $t^3 + t + 1$. [meth seen ⇓]

4. (a) (i) *Give an example of a prime ideal which is not maximal.*

1, A

The zero ideal of $\mathbb{Z}$ is such an example.

seen ⇓

(ii) *Give an example of an integral domain which is not a principal ideal domain. Justify your answer.*

3, A

$\mathbb{Z}[t]$ is not a principal ideal domain. The ideal of all polynomials with integer coefficients and even constant term is not principal. Indeed, a generator must be an integer dividing 2 but not equal to 1, so it must be 2. But our ideal contains t, which is not a multiple of 2, so it is not the principal ideal generated by 2.

unseen ⇓

Alternatively, in lectures it was proved that the ring R of polynomials in t with coefficients in $\mathbb{Q}$ and the constant term in $\mathbb{Z}$ is not a UFD. By a theorem from lectures, every PID is a UFD, hence R is not a PID.

(iii) *Do there exist a principal ideal domain R and a prime ideal $I \subset R$, $I \neq 0$, such that I is not a maximal ideal of R?*

4, B

No, every non-zero prime ideal of a PID is maximal. Our prime ideal is aR for some $a \in R$, $a \neq 0$. If aR is not maximal, then $aR \subsetneq bR$ for some $b \in R$, $b \notin R^\times$. Hence $a = bc$. We have $b \notin aR$, as otherwise $aR = bR$. We have $c \notin aR$, as otherwise $bR = R$, using that $a \neq 0$ and R is an integral domain. This contradicts the assumption that the ideal aR is prime.

unseen ⇓

(b) *Let R be the ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$. For each of the following elements of R determine if it is an invertible element of R, an irreducible element of R, or neither invertible nor irreducible:*

(i) $\sqrt{2}$, (ii) $1 + \sqrt{2}$, (iii) $2 + \sqrt{2}$, (iv) $3 + \sqrt{2}$, (v) $4 + \sqrt{2}$, (vi) $5 + \sqrt{2}$.

Hint*: Use the multiplicativity of the function $R \to \mathbb{Z}$ that sends $m + n\sqrt{2}$ to $m^2 - 2n^2$.*

meth seen ⇓

We note that $m^2 - 2n^2 = \pm 1$ if and only if $m + n\sqrt{2} \in R^\times$. Hence $1 + \sqrt{2} \in R^\times$.

2, A

Next we note that if $m^2 - 2n^2 = \pm p$, where p is a prime, then $m + n\sqrt{2}$ is an irreducible element of R. (Indeed, if $m + n\sqrt{2} = xy$ for some $x, y \in R \setminus R^\times$ then $m^2 - 2n^2$ is a product of two integers none of which is ± 1.) Hence $\sqrt{2}$, $2 + \sqrt{2}$, $3 + \sqrt{2}$, $5 + \sqrt{2}$ are irreducibles. Finally, $4 + \sqrt{2} = \sqrt{2}(1 + 2\sqrt{2})$, where both factors are irreducible, thus $4 + \sqrt{2}$ is neither irreducible nor invertible.

10, C

If your module is taught across multiple year levels, you might have received this form for each level of the module. You are only required to fill this out once for each question.

Please record below, some brief but non-trivial comments for students about how well (or otherwise) the questions were answered. For example, you may wish to comment on common errors and misconceptions, or areas where students have done well. These comments should note any errors in and corrections to the paper. These comments will be made available to students via the MathsCentral Blackboard site and should not contain any information which identifies individual candidates. Any comments which should be kept confidential should be included as confidential comments for the Exam Board and Externals. If you would like to add formulas, please include a sperate pdf file with your email.

ExamModuleCode	QuestionNumber	Comments for Students
MATH50005	1	Part (b) (ii) with different level of details, some of you used the fact that the smalest nonabelian group has order 60, which is probably OK, I accepted such proofs
MATH50005	2	For the part (b) some students assume that G contains all two by two matrices, which is wrong, only non-singular matrices should be considered. I did not give any credit in this case.
MATH50005	3	Common mistake is characteristic 0 in (a) (iv).
MATH50005	4	Some of you did not attempte (a) (iii), not sure why. The question (b) was done case be case by many of you, while the model solution offer more general argument.