

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May-June 2022

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

Commutative Algebra

Date: 17 May 2022

Time: 09:00 – 11:30 (BST)

Time Allowed: 2:30 hours

Upload Time Allowed: 30 minutes

This paper has 5 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 ONE PDF TO THE RELEVANT DROPBOX ON BLACKBOARD
WITH COMPLETED COVERSHEETS WITH YOUR CID NUMBER, QUESTION NUMBERS
ANSWERED AND PAGE NUMBERS PER QUESTION.**

In this examination every ring is commutative with unity. You may use any results from the course, including all lectures and problem sheets, without further justification, provided you state them clearly and correctly.

Subquestions are sequential, and **you are expected to use results of earlier subquestions in later ones**, even if you have not successfully proven the earlier claims.

1. (a) (i) State *Hilbert's Basis Theorem*. (4 marks)
- (ii) Show that if A is a Noetherian ring and B is a finitely generated \mathbb{Z} -algebra, then the ring $A \otimes_{\mathbb{Z}} B$ is Noetherian.
(Hint: It may help to recall that $A \otimes_{\mathbb{Z}} \mathbb{Z}[t_1, \dots, t_n] \cong A[t_1, \dots, t_n]$ for a ring A and indeterminates t_j .) (5 marks)
- (b) (i) State the universal property of the tensor product of modules. (4 marks)
- (ii) Show that the multiplication of a ring A induces a surjective ring homomorphism $A \otimes_{\mathbb{Z}} A \rightarrow A$. (5 marks)
- (iii) Let k be any field and $K = k(x_1, x_2, x_3, \dots)$ the field of rational functions in countably infinitely many indeterminates over k . Find an ideal \mathfrak{k} of $K \otimes_{\mathbb{Z}} K$ which is not finitely generated; you do not need to prove \mathfrak{k} is not finitely generated. (2 marks)

From this we conclude that when a ring K is Noetherian, $K \otimes_{\mathbb{Z}} K$ need not also be Noetherian.

(Total: 20 marks)

2. Recall that a ring A is called *Boolean* if $x^2 = x$ for all $x \in A$. Agree in good humor to call a ring A **Troolean** if $x^3 = x$ for all $x \in A$.
 - (a) Prove that a Boolean ring is Troolean. (2 marks)
 - (b) Recall that the *characteristic* $n \geq 0$ of A generates the kernel of the unique ring map $\mathbb{Z} \rightarrow A$. What are the possible characteristics of a Troolean ring? (4 marks)
 - (c) (i) Show that in a local ring (A, \mathfrak{m}) , the elements of $1 + \mathfrak{m}$ are units. (2 marks)
 - (ii) List all Troolean local rings up to isomorphism. (4 marks)
 - (d) Show a Troolean ring of characteristic 2 is Boolean.
(Hint: Cube $x + 1$.) (3 marks)
 - (e) (i) State the *Chinese Remainder Theorem* in its general form. (2 marks)
 - (ii) Prove that a Troolean ring is the direct product of a Boolean ring and a Troolean ring of characteristic 3. (3 marks)
- (Total: 20 marks)

3. (a) Let b and b' lie in the integral closure of an integral domain A in some larger ring C and suppose the minimal monic polynomial $p(t)$ for b' over A remains irreducible over $A[b]$.
- (i) Show that $M = A[b] \otimes_A A[b']$ and $N = A[b, b']$ are both free $A[b]$ -modules of rank equal to the degree of p . (3 marks)
 - (ii) Show that the map $f: A[b] \otimes_A A[b'] \longrightarrow A[b, b']$ induced by the multiplication of C is a surjective $A[b]$ -module homomorphism. (1 mark)
 - (iii) Let $S = A \setminus \{0\}$, so that the localization $S^{-1}A$ is the field of fractions K of A . Show the localization map $M \longrightarrow S^{-1}M$ is injective. (2 marks)
 - (iv) Show that $S^{-1}f: S^{-1}M \longrightarrow S^{-1}N$ is an isomorphism of K -vector spaces. (2 marks)
 - (v) Conclude from the commutative square that f is injective. (2 marks)

All told, we have shown $f: A[b] \otimes_A A[b'] \longrightarrow A[b, b']$ is an isomorphism.

- (b) (i) Identify $\mathbb{Q}[x]/(x^2 + 3)$ and $\mathbb{Q}[t]/(t^2 + 1)$ as subfields of the integral closure $\overline{\mathbb{Q}}$ of \mathbb{Q} in \mathbb{C} . (2 marks)
- (ii) Using part (a)(i) or otherwise, identify $\mathbb{Q}[x]/(x^2 + 3) \otimes_{\mathbb{Q}} \mathbb{Q}[t]/(t^2 + 1)$ with another subfield $K < \overline{\mathbb{Q}}$. (1 mark)
- (iii) Show K contains the primitive third roots of unity (i.e., the roots of $\frac{y^3 - 1}{y - 1} = y^2 + y + 1$). (2 marks)
- (iv) Show $K = \mathbb{Q}[\varepsilon]$ for ε a primitive twelfth root of unity (meaning we have $\varepsilon^{12} = 1$ but $\varepsilon^n \neq 1$ for positive $n < 12$). (3 marks)
- (v) Show $K \cong \mathbb{Q}[z]/(z^4 - z^2 + 1)$. (2 marks)
(Hint: Note that $z^{12} - 1 = (z^6 + 1)(z^6 - 1)$ and $z^6 + 1 = (z^4 - z^2 + 1)(z^2 + 1)$.)

All told, we have shown that $\mathbb{Q}[x]/(x^2 + 3) \otimes_{\mathbb{Q}} \mathbb{Q}[t]/(t^2 + 1)$ is isomorphic to $\mathbb{Q}[z]/(z^4 - z^2 + 1)$.
(Total: 20 marks)

4. (a) State the definition of a *Dedekind domain*. (4 marks)
- (b) Write $A = \mathbb{Z}[\sqrt{-13}]$.
- (i) Prove or disprove: A is a Dedekind domain. (2 marks)
 - (ii) Find two distinct irreducible factorizations of 14 in A . (4 marks)
 - (iii) Find a prime ideal \mathfrak{p} of A lying over $(7) \triangleleft \mathbb{Z}$. (6 marks)
 - (iv) Is there any prime ideal of A strictly between (0) and \mathfrak{p} ? (4 marks)
- (Total: 20 marks)

5. (a) State *Hensel's Lemma*. (5 marks)

Recall that, as a consequence, if (A, \mathfrak{m}) is a complete local ring and $f(t) \in A[t]$ is a monic polynomial such that the reduction $\bar{f}(t) \in (A/\mathfrak{m})[t]$ admits a simple root \bar{a} in A/\mathfrak{m} , then $f(t)$ admits a simple root $a \in A$.

Recall that \mathbb{Z}_p is a complete discrete valuation ring.

- (b) If $p \neq 2$ is a prime, show that if there exists $u \in \mathbb{Z}_p^\times$ such that $1 + u^2 \in (p)$, then -1 is a square in \mathbb{F}_p and \mathbb{Z}_p . (5 marks)

- (c) Show that for all $u \in \mathbb{Z}_7^\times$, the element $1 + u^2$ is a unit of \mathbb{Z}_7 .

(*Hint: The squares of \mathbb{F}_7 are 0, 1, 2, 4.*) (5 marks)

- (e) It can be shown that $A = \mathbb{Z}_7[t]/(t^2 + 1)$ is a complete discrete valuation ring with unique maximal ideal (7) and is a free module of rank 2 over \mathbb{Z}_7 with basis given by 1 and the class $i = \sqrt{-1}$ of t . Assuming all this, show that 3 and 5 are squares in A .

(*Hint: Show -4 and -2 are squares in $\mathbb{F}_{49} = \mathbb{F}_7[t]/(t^2 + 1)$.*) (5 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2022

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

MATH70061/97053

Commutative Algebra (Solutions)

Setter's signature

.....

Checker's signature

.....

Editor's signature

.....

1. (a) (i) If A is a Noetherian ring, then the polynomial ring $A[t]$ in one indeterminate over A is again Noetherian. [4, A]
(ii) Finite generation of B implies the existence of a surjective homomorphism $\mathbb{Z}[t_1, \dots, t_n] \rightarrow B$. One then has a surjective homomorphism $A \otimes \mathbb{Z}[t_1, \dots, t_n] \rightarrow A \otimes B$, but the domain is isomorphic to $A[t_1, \dots, t_n]$, which is Noetherian by the Hilbert basis theorem since we have assumed A is. As a quotient of a Noetherian ring is again Noetherian, it follows $A \otimes B$ is Noetherian. [5, C]
unseen ↓
- (b) (i) The tensor product $M \otimes_A N$ of two A -modules is the initial A -module receiving an A -bilinear map from $M \times N$, in the sense that there is such a map $t: M \times N \rightarrow M \otimes_A N$ and if P is an A -module and $\beta: M \times N \rightarrow P$ an A -bilinear map, then there exists a unique A -linear $\bar{\beta}: M \otimes_A N \rightarrow P$ such that $\beta = \bar{\beta} \circ t$. [4, A]
seen ↓
- (ii) Since the ring multiplication $\mu: A \times A \rightarrow A$ is \mathbb{Z} -bilinear by distributivity, it factors uniquely as $t: A \times A \rightarrow A \otimes A$ followed by a \mathbb{Z} -linear map $\bar{\mu}: A \otimes A \rightarrow A$. Since $1 \cdot a = a$ for each $a \in A$, we see $\mu = \bar{\mu} \circ t$ is surjective, and this implies $\bar{\mu}$ is surjective as well. Since pure tensors $a \otimes a'$ generate $A \otimes A$, to see $\bar{\mu}$ is a ring homomorphism one need only observe it sends $ab \otimes a'b' = (a \otimes a')(b \otimes b')$ to $aba'b' = aa'bb' = \bar{\mu}(a \otimes a')\bar{\mu}(b \otimes b')$. [5, B]
unseen ↓
- (iii) The kernel \mathfrak{k} of $\bar{\mu}: K \otimes K \rightarrow K$ is an ideal containing (generated by, but we do not need this) the elements $1 \otimes x_n - x_n \otimes 1$ for all integers $n \geq 1$. Since every element of $K \otimes K$ by definition can be written as an expression in only finitely many x_n , no finite set of elements of \mathfrak{k} will suffice to generate all of them. (I do not intend them to give a fully rigorous argument.) [2, D]
2. (a) If $x^2 = x$, then $x^3 = x^2 \cdot x = x \cdot x = x$. [2, A]
unseen ↓
- (b) Note that $2 = 2^3 = 8$ in A , so that $6 = 0$. Thus all characteristics divide 6. One can check manually that for $n \in \{1, 2, 3, 6\}$ and all $x \in \mathbb{Z}/n\mathbb{Z}$ one has $x^3 = x$. [4, B]
- (c) (i) Let $x \in \mathfrak{m}$. If $1 + x$ were not a unit, then it would lie in some maximal ideal, but \mathfrak{m} is the only option. Then we would have $1 + x$ and x both in \mathfrak{m} , and hence $1 \in \mathfrak{m}$, a contradiction. [2, A]
seen ↓
- (ii) Let x be an element of the unique maximal ideal. Then $x \pm 1$ are units, and since $0 = x(x-1)(x+1)$, it follows $x = 0$. Thus the maximal ideal is (0) , so A is a field, and hence is \mathbb{F}_2 or \mathbb{F}_3 . [4, D]
unseen ↓
- (e) For all $x \in A$ one has $x + 1 = (x + 1)^3 = x^3 + x^2 + x + 1 = x^2 + 1$ and hence $x = x^2$. [3, A]
- (f) (i) Let A be a ring and \mathfrak{a}_j finitely many pairwise coprime ideals. Then $\bigcap \mathfrak{a}_j = \prod \mathfrak{a}_j$ and the natural map $A \rightarrow \prod A/\mathfrak{a}_j$ induces an isomorphism $A/\bigcap \mathfrak{a}_j \rightarrow \prod A/\mathfrak{a}_j$. [2, A]
seen ↓
- (ii) Apply the Chinese Remainder Theorem to the coprime ideals (2) and (3) , whose product is $(6) = (0)$, to obtain an isomorphism $A \rightarrow A/(2) \times A/(3)$. [3, B]
meth seen ↓

3. (a) (i) The module structure is given by $q(b) \cdot (r(b) \otimes s(b')) := q(b)r(b) \otimes s(b')$ for M and by the inclusion $A[b] \hookrightarrow A[b, b'] = N$ for N . To see M is free of rank $d = \deg p$, note that $A[b'] \cong A[t]/(p(t))$ is free of rank d as an A -module, so $M \cong A[b] \otimes_A A^{\oplus d} \cong (A[b] \otimes_A A)^{\oplus d} \cong A[b]^{\oplus d}$. To see N is free of rank d , note that $p(t)$ is still irreducible over $A[b]$, it is the minimal polynomial for b' over $A[b]$, so that $N = A[b, b'] \cong A[b][t]/(p(t))$ is free of rank d over $A[b]$. [3, A]
unseen ↓
- (ii) It is clear f is an $A[b]$ -module homomorphism because $q(b) \cdot (r(b) \otimes s(b')) = q(b)r(b) \otimes s(b')$ is sent to $q(b)r(b)s(b')$ for each $q(b) \in A[b]$. It is surjective because any $\sum a_{ij}b^i(b')^j$ for $a_{ij} \in A$ is the f -image of $\sum_j (\sum_i a_{ij}b^i \otimes (b')^j)$. [1, B]
sim. seen ↓
- (iii) Because M is a free $A[b]$ -module and $A[b]$ is a free A -module, no nonzero element of M is annihilated by multiplication with an element of S , so $M \rightarrow S^{-1}M$ is injective. [2, A]
seen ↓
- (iv) Because M and N have the same finite rank as A -modules, it follows $S^{-1}M$ and $S^{-1}N$ have the same dimension as K -vector spaces. Since f is surjective, by the exactness of localization, $S^{-1}f$ is surjective. But a surjection between finite-dimensional vector spaces of equal dimension is an isomorphism. [2, D]
unseen ↓
- (v) As the diagram [2, D]

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow & & \downarrow i \\ S^{-1}M & \xrightarrow[S^{-1}f]{\sim} & S^{-1}N \end{array}$$

is commutative and the lower path is a composite of injective maps, the upper composite $i \circ f$ is also injective. But this implies f is injective. We already knew f is surjective, so it is an isomorphism.

- (b) (i) We have $\mathbb{Q}[x]/(x^2 + 3) \cong \mathbb{Q}[i\sqrt{3}]$ and $\mathbb{Q}[t]/(t^2 + 1) \cong \mathbb{Q}[i]$. [2, B]
- (ii) Since $x^2 + 3$ has no root in $\mathbb{Q}[i]$ (or since $t^2 + 1$ has no root in $\mathbb{Q}[i\sqrt{3}]$), part (b) gives [1, B]
unseen ↓
- $$\mathbb{Q}[x]/(x^2 + 3) \otimes_{\mathbb{Q}} \mathbb{Q}[t]/(t^2 + 1) \cong \mathbb{Q}[i\sqrt{3}, i] = K.$$
- (iii) The quadratic formula shows the roots of $y^2 + y + 1$ are $\zeta_{\pm} := \frac{1}{2}(1 \pm i\sqrt{3})$, which already lie in $\mathbb{Q}[i\sqrt{3}] < K$. [2, A]
- (iv) Choosing $\varepsilon = e^{2\pi i/12}$, one has $\zeta_+ = \varepsilon^4$ and $-i = \varepsilon^9$, so $\varepsilon = -i\zeta_+$ lies in K . On the other hand, $\mathbb{Q}[\varepsilon]$ evidently contains both $\varepsilon^4 = \zeta_+$ and $\varepsilon^3 = i$. Alternatively, it is not hard to see directly or by an argument using symmetries of the plane that $\varepsilon = \frac{1}{2}(\sqrt{3} + i)$. [3, C]
- (v) From the factorization one sees the roots of $z^4 - z^2 + 1$ are precisely those twelfth roots of unity which are neither sixth nor fourth roots, which is to say the primitive twelfth roots of unity, so $\mathbb{Q}[\varepsilon] \cong \mathbb{Q}[z]/(z^4 - z^2 + 1)$. [2, B]

4. (a) A *Dedekind domain* is a normal, Noetherian integral domain of Krull dimension 1. [4, A]
seen ↓
- (b) (i) We showed in the Week 7 problem sheet that the integral closure of \mathbb{Z} in $K = \mathbb{Q}(\sqrt{n})$ (the *ring of integers* \mathcal{O}_K) is $\mathbb{Z}[\sqrt{n}]$ for n square-free and congruent to 2 or 3 (mod 4) and is $\mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right]$ for $n \equiv 1 \pmod{4}$. Since $-13 \equiv 3 \pmod{4}$, we see A is the ring of integers of $\mathbb{Q}(\sqrt{-13})$, and we know rings of integers of number fields are (the motivating) examples of Dedekind domains. [2, B]
meth seen ↓
- (ii) Evidently $14 = 2 \cdot 7$, and only slightly less obviously, $14 = (1 + \sqrt{-13})(1 - \sqrt{-13})$. To see these are irreducible, we note the squares $|z|^2$ of the moduli of $z = 2, 7, 1 \pm \sqrt{-13}$ are respectively 4, 49, 14, and since $|a + b\sqrt{-13}|^2 = a^2 + 13b^2$, there are no z with $|z|^2$ equal to 2 or 7. [4, C]
sim. seen ↓
- (iii) Note that $\mathfrak{p}_{\pm} = (7, 1 \pm \sqrt{-13})$ contain $(7) \triangleleft \mathbb{Z}$, and $(a + b\sqrt{-13}) \cdot (1 \pm \sqrt{-13})$ lies in \mathbb{Z} if and only if $b \mp a = 0$, in which case the product is $14a$. To see these ideals are prime, note they are the kernels of homomorphisms $\mathbb{Z}[\sqrt{-13}] \rightarrow \mathbb{F}_7$ taking $-13 \mapsto \mp 1$; such homomorphisms exist because they descend from maps $\mathbb{Z}[x] \rightarrow \mathbb{F}_7$ taking $x \mapsto \mp 1$ and hence $x^2 + 13 \mapsto 0$. [6, D]
- (iv) Since A is a Dedekind domain, there are no chains of primes of length > 1 , and hence no intermediate primes between 0 and \mathfrak{p}_{\pm} . [4, A]
seen ↓

5. (a) Let (A, \mathfrak{m}) be a complete local ring. If the reduction $\bar{f} \in (A/\mathfrak{m})[t]$ of a monic polynomial $f \in A[t]$ admits a factorization $\bar{g}\bar{h}$ into coprime monic polynomials $\bar{g}, \bar{h} \in (A/\mathfrak{m})[t]$, then f admits a factorization gh into monic polynomials $g, h \in A[t]$ whose respective reductions are \bar{g}, \bar{h} and which have the same degrees. [5, M]
seen ↓
- (b) If $1+u^2 \in (p)$, then $1+\bar{u}^2 = 0$ in \mathbb{F}_p , so $(t-\bar{u})(t+\bar{u}) = t^2 + 1$ in $\mathbb{F}_p[t]$. If $p \neq 2$, then $\bar{u} \neq -\bar{u}$, so -1 admits a square root in \mathbb{Z}_p by Hensel's lemma, which applies because \mathbb{Z}_p is a complete discrete valuation ring. [5, M]
meth seen ↓
- (c) If $1+u^2$ were a nonunit of \mathbb{Z}_7 , then it would lie in the unique maximal ideal (7) , so by part (b) we would know $-1 = 6$ is a square of \mathbb{F}_7 . But it is easy to verify manually that the respective squares of $0, \pm 1, \pm 2, \pm 3$ are $0, 1, 4, 2$, so this is not so. We conclude $1+u^2$ is a unit. [5, M]
unseen ↓
- (d) By Hensel's lemma, it is enough to see 3 and 5 are squares in the field $\mathbb{Z}_7[i]/(7) \cong \mathbb{Z}_7[t]/(7, t^2 + 1) \cong \mathbb{F}_7[t]/(t^2 + 1) = \mathbb{F}_{49}$. For this, we note $t^2 = -1$, so $(\pm 2t)^2 = -4 = 3$ and $(\pm 3t)^2 = -9 = 5$. [5, M]

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: 100 of 100 marks

Total mastery marks: 20 of 20 marks

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

ExamModuleCode	QuestionNumber	Comments for Students

1.a.ii: Many people did not learn the difference between a finitely-generated ring and a polynomial ring.

1.b.i: It was common to omit the requirement that the map out of the tensor product be A-linear. This mostly resulted from quoting the sentence using the phrase "factors through" in the course notes without taking into account the preceding discussion explaining at length what such a factorization would entail.

1
1.b.ii: Many people did not show this is a ring map, or that it was surjective, settling for showing it was a well-defined group map.

1.b.iii: The answer is the kernel of the map induced by the product. The intuitive reason this cannot be finitely generated is that, for example, it includes all the $x_i(x)$ $1 - 1(x)x_i$, and these are infinite number, and, it is easy to imagine, not expressible as linear combinations of the others.

The answers given were overwhelmingly the unit ideal. The pattern was to suggest an ideal generated by pure tensors $y(x)z$. This element has inverse $y^{-1}(x)z^{-1}$ since K is a field, unless y or z is zero, so all these elements are units. A second-favorite choice was to suggest the ideal (x_1, x_2, \dots) . But the x_i are elements of K , and are not elements of $K(x)_Z K$, so these answers unfortunately suggest limited understanding of what an element of the tensor product is.

Many people assumed, for no clear reason, that all Boolean rings are quotients of $\mathbb{Z}/(6)$, despite the fact that any power $(\mathbb{Z}/2)^n$ is Boolean.

Many people showed the characteristic needed to divide 6 without showing there were examples of those characteristics.

2

Several people claimed that the answers for the integral domain and local ring questions were arbitrary quotients of polynomial rings over \mathbb{F}_2 and \mathbb{F}_3 , without noticing those did not necessarily satisfy the requirements of being an integral domain or a local ring. In fact the only answers were \mathbb{F}_2 or \mathbb{F}_3 .

In the last part of the problem, many people failed to notice the Chinese remainder theorem applied despite the fact a request for a statement of that theorem immediately preceded the question.

2.c.i.: Several confused the nilradical with the Jacobson radical.

3.a. Many people just assumed M and N were isomorphic, which is what the exercise was trying to prove.

3.a.i. Many people proved only one of M or N was free, or even tried. Several people do not seem to have learned what a free module is.

3

3.a.iii: Injectivity of $M \rightarrow S^{-1}M$ does not immediately follow from that of $A \rightarrow S^{-1}A$. For example, for $A = \mathbb{Z}$ and $M = \mathbb{Z}/2$, this doesn't work. It does work if M is a free A -module.

A separate idea that strangely came up repeatedly was that it was enough to show that the two maps to $S^{-1}A[b] \times S^{-1}A[b']$ were injective. But no one showed this. For this to be enough, one would need a flatness hypothesis no one invoked.

4

4.b.iii: People tended not to show that this ideal met Z in (7), say by noting the contraction of a prime ideal is again prime and (7) is maximal in Z .

5.b: People tended not to prove the root is simple by noting the other root, minus the first, is distinct if 2 is not equal to 0.

5

5.c: A few people had an argument attempting to use units directly rather than the preceding lemma as intended. I don't see how this argument works.