IMPERIAL

MATH70061

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

Commutative Algebra

Date: Monday, May 20, 2024

Time: 14:00 – 16:30 (BST)

Time Allowed: 2.5 hours

This paper has 5 Questions.

Please Answer All Questions in 1 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. Let k be a field and $f_1, \ldots, f_n \in k[X_1, \ldots, X_n]$. Let $I \subset k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ be the ideal

$$I = (Y_1 - f_1, \ldots, Y_n - f_n)$$

(a) Show that $I \cap k[X_1, \ldots, X_n] = (0)$.
[Hint: Use a monomial order with $Y_1 > \ldots Y_n > X_1 > \ldots > X_n$.] (6 marks)

Recall that the map $\phi_f : k^n \to k^n$ defined by

$$(a_1, \ldots, a_n) \to (f_1(a_1, \ldots, a_n), \ldots, f_n(a_1, \ldots, a_n))$$

is said to be **invertible** if there exists polynomials $g_1, g_2, \ldots, g_n \in k[Y_1, \ldots, Y_n]$ such that $g_i(f_1, \ldots, f_n) = X_i$ for $1 \leq i \leq n$.

(b) Consider a monomial order $\leq$ on $k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ such that $X_i > Y_j$ for all $1 \leq i, j \leq n$. Show that if $G = \{X_1 - g_1, , \ldots, X_n - g_n\}$ for $g_i \in k[Y_1, \ldots, Y_n]$ is the reduced Gröbner basis of I with respect to $\leq$ then ϕ_f is invertible. (4 marks)

(c) Conversely, suppose that ϕ_f is invertible.

(i) Show that $X_i - g_i \in I$ for all i.

(ii) Show that $I \cap k[Y_1, \ldots, Y_n] = (0)$.

(iii) Deduce that $G = \{X_1 - g_1, \ldots, X_n - g_n\}$ is the reduced Gröbner basis of I with respect to $\leq$.

(10 marks)

(Total: 20 marks)

2. (a) Define the **Krull dimension** of a ring. (2 marks)

Recall that we denote by $R[[t]]$ the formal power series ring in the variable t over R, and $\mathcal{N}(R)$ and $\mathcal{N}(R[[t]])$ the nilradicals of R and $R[[t]]$ respectively.

(b) Assume that R is Noetherian. Show that

$$\mathcal{N}(R[[t]]) = \{\sum_{n=0}^{\infty} a_n t^n \in R[[t]] : a_n \in \mathcal{N}(R) \text{ for every } n\}.$$

(6 marks)

(c) Assume that $R = k$ is a field. Show that every non-zero element of $k[[t]]$ is of the form $t^n u$ for some $n \in \mathbb{Z}_{\geq 0}$ and an invertible element $u \in k[[t]]^*$. Deduce that the only prime ideals of $k[[t]]$ are (0) and (t). (6 marks)

(d) Assume that R is an Artinian ring. Show that the Krull dimension of $R[[t]]$ is one.
[Hint: use the previous parts.] (6 marks)

(Total: 20 marks)

3. (a) Show that an ideal $I \subset \mathbb{C}[X_1, \ldots, X_n]$ contains a monomial if and only if every point of $\mathcal{V}(I)$ has at least one co-ordinate equal to zero, that is, if $(a_1, \ldots, a_n) \in \mathcal{V}(I)$, then $a_i = 0$ for at least one i. (6 marks)

(b) (i) Let $F, G \in \mathbb{C}[X_1, \ldots, X_n]$ be square-free polynomials, i.e, there is no polynomial $P \in \mathbb{C}[X_1, \ldots, X_n]$ such that P^2 divides F or G. Suppose that $\mathcal{V}(F) = \mathcal{V}(G)$, then show that $F = cG$ for some $c \in \mathbb{C} \setminus \{0\}$. (7 marks)

(ii) Construct a square-free polynomial F in $\mathbb{R}[X, Y]$ such that $\mathcal{V}(F) = \mathcal{V}(G)$ for $G = X^2 + Y^2 - 1$ but $F \neq cG$ for some $c \in \mathbb{R} \setminus \{0\}$.

(7 marks)

(Total: 20 marks)

4. (a) Let R be a ring such that for any element $r \in R$, there exists some $n \in \mathbb{N}$ (depending on r) such that $r^n = r$. Show that $\dim R = 0$. (7 marks)

(b) Prove that a PID (principal ideal domain) has dimension 0 or 1. Give an example of an integral domain of dimension 1 that is not a PID. Prove your assertions. (6 marks)

(c) Suppose $A \subset B$ are rings and B is integral over A. Show that for any prime ideal $\mathfrak{p} \subset A$ the set $\{\mathfrak{q} \in \mathrm{Spec} B : \mathfrak{q} \cap A = \mathfrak{p}\}$ is finite.

[*Hint: First replace A by $A/\mathfrak{p}$ and B by $B/\mathfrak{p}B$ and then invert non-zero elements of A.*]
(7 marks)

(Total: 20 marks)

5. (a) Define what it means for a ring to be a **valuation ring**. (2 marks)

(b) Suppose R is a valuation ring with field of fractions K. Show that any subring R' of K with $R \subset R' \subset K$ is isomorphic to $R_{\mathfrak{p}}$, the localisation of R at a prime ideal $\mathfrak{p}$.

(9 marks)

(c) Prove that in a valuation ring, any radical ideal is prime.

(9 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2024

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

MATH70061

Commutative Algebra (Solutions)

Setter's signature	Checker's signature	Editor's signature
Yankı Lekili	. . . .	. . . .

1. (a) Consider a monomial order such that $Y_1 > \ldots > Y_n > X_1 > \ldots > X_n$. Then, setting $g_i = Y_i - f_i$, we see that $LT(g_i) = Y_i$, hence $S(g_i, g_j) = Y_j(Y_i - f_i) - Y_i(Y_j - f_j) = Y_i f_j - Y_j f_i$, therefore, division by $g_1, \ldots, g_n$ is given by

$$S(g_i, g_j) = Y_j g_i - Y_i g_j$$

hence the remainder is zero. This proves that $\{g_1, \ldots, g_n\}$ is a Gröbner basis for I. Now, ideal membership property says that $f \in I$ if and only if division by remainder of f by $\{g_1, \ldots, g_n\}$ is zero. However, if $f \in k[X_1, \ldots, X_n]$, the since $LT(g_i) = Y_i$ does not divide any term of f for any i, we conclude that $f \notin I$. $\boxed{6, \text{A}}$

(b) If $G = \{X_1 - g_1, \ldots, X_n - g_n\}$ is a Gröbner basis for I, in particular, $X_i - g_i \in I$, therefore, there exist $q_{ij} \in k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ such that

$$X_i - g_i = \sum_{j=1}^{n} q_{ij}(Y_j - f_j)$$

Now, substituting $Y_i = f_i(X_1, \ldots, X_n)$ gives that $X_i = g_i(f_1, \ldots, g_n)$ which shows that ϕ_f is invertible. $\boxed{4, \text{A}}$

(c) (i) $g_i(f_1, \ldots, f_n) - g_i(Y_1, \ldots, Y_n) \in I$ since $Y_i - f_i \in I$. Therefore, $X_i - g_i = g_i(f_1, \ldots, f_n) - g_i \in I$. $\boxed{2, \text{A}}$

(ii) Suppose there exist $h \in I \cap k[Y_1, \ldots, Y_n]$. Since $Y_i - f_i \in I$, we have $h(f_1, \ldots, f_n) - h \in I$. Therefore, $h(f_1, \ldots, f_n) \in I$ (as $h \in I$). This implies $h(f_1, \ldots, f_n) \in I \cap k[X_1, \ldots, X_n]$. Thus, by part (a), we get $h(f_1, \ldots, f_n) = 0$. This is impossible if ϕ_f is invertible unless $h = 0$, since that implies $k[f_1, \ldots, f_n] = k[X_1, \ldots, X_n]$. In particular, $f_1, \ldots, f_n$ are algebraically independent. $\boxed{4, \text{A}}$

(iii) Since any element in $I \cap k[Y_1, \ldots, Y_n] = (0)$, for any non-zero $f \in I$, $LT(f)$ is divisible by some $LT(X_i - g_i) = X_i$. Hence, $h_i = X_i - g_i$ generate the initial ideal of I. Moreover, as in part (a) but now for a monomial order with $X_1 > \ldots > X_n > Y_1 \ldots > Y_n$, we can see that the division with remainder of $S(h_i, h_j)$ by $\{h_1, \ldots, h_n\}$ is zero, hence $\{h_1, \ldots, h_n\}$ is a Gröbner basis for I (the fact that it is reduced is clear). $\boxed{4, \text{A}}$

2. (a) For a ring A, the **Krull dimension** is defined to be

$$\dim A := \dim \mathrm{Spec}(A) = \sup\{n \geq 0 : \exists\ \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \ldots \subsetneq \mathfrak{p}_n \subsetneq A \text{ with } \mathfrak{p}_i \text{ prime ideal }\}$$

$\boxed{2,\ \mathrm{A}}$

(b) Let $f(X) = \sum_{n=0}^{\infty} a_n X^n \in R[[X]]$. Consider the ideal of R generated by a_i, by the Noetherian hypothesis, this can be generated by only finitely many of the a_i, say, $a_n \in (a_1, \ldots, a_s)$ for all n. Then, we can write $a_n = \sum_{i=1}^{s} c_{ni} a_i$ for all n, hence

$$f(X) = \sum_{n=0}^{\infty} a_n X^n = \sum_{n=0}^{\infty} (\sum_{i=0}^{s} c_{ni} a_i) X^n = \sum_{i=0}^{s} a_i f_i(X)$$

where $f_i(X) = \sum_{n=0}^{\infty} c_{ni} X^n$. Thus, if a_i are nilpotent in R, then $a_i f_i(X)$ are nilpotent in $R[[X]]$, and so $f(X)$ which is a finite sum of nilpotent elements is nilpotent (by binomial expansion).

Conversely, suppose $f(X)$ is nilpotent, so $f(X)^N = 0$ for some N, then $0 = f(X)^N = a_0^N + X(\ldots)$, hence $a_0^N = 0$. Suppose by induction that $a_0, \ldots, a_k$ are nilpotent, then $p_k(X) = \sum_{n=0}^{k} a_n X^n$ is nilpotent (by binomial expansion) and so $f(X) - p_k(X) = a_{k+1} X^{k+1} + \ldots$ is nilpotent, which implies that a_{k+1} is nilpotent.

$\boxed{6,\ \mathrm{B}}$

(c) We claim that $f(X) = a_0 + a_1 X + a_2 X^2 + \ldots$ is invertible if and only if a_0 is nonzero. If it exists, we can write $f^{-1}(X) = b_0 + b_1 X + b_2 X^2 + \ldots$, then $a_0 b_0 = 1$. We have

$$\begin{aligned} 1 &= (a_0 + a_1 X + a_2 X^2 + \ldots)(b_0 + b_1 X + b_2 X^2 + \ldots) \\ &= a_0 b_0 + (a_1 b_0 + a_0 b_1) X + \ldots \end{aligned}$$

This can be solved for $b_0, b_1, \ldots$ successively from $a_0 b_0 = 1$, $a_1 b_0 + a_0 b_1 = 0$,...etc. which establishes our claim.

Now, given an arbitrary $f(X) = a_0 + a_1 X + a_2 X^2 + \ldots$ let n be the smallest non-zero a_i, then we can write $f(X) = X^n (a_n + a_{n+1} X + \ldots)$ which is $X^n u(X)$ for some invertible $u(X)$ from what we showed above.

Given a prime ideal $\mathfrak{p} \subset k[[X]]$, if it is not (0) then it has a non-zero element $X^n u(X)$ for some unit $u(X)$ then multiplying with the inverse of $u(X)$ we see that X^n is in the ideal, and now since $\mathfrak{p}$ is prime, this implies that X is in $\mathfrak{p}$. Now the ideal $(X) \subset \mathfrak{p}$ and (X) is maximal since its complement consists of elements of the form $X^n u(X)$ for $n = 0$, hence are invertible. Thus, $(X) = \mathfrak{p}$ as required. $\boxed{6,\ \mathrm{B}}$

(d) Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ be the maximal ideals of R. Since these are all prime ideals of R as R is Artinian, we know that $\mathcal{N}(R) = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_s$. On the other hand, the ideal $\mathfrak{m}_i[[X]]$ are prime in $R[[X]]$. To see this, note that the quotient $R[[X]]/\mathfrak{m}_i[[X]] \simeq (R/\mathfrak{m}_i)[[X]]$ is an integral domain. Moreover, by part b), we have that $\mathcal{N}(R[[X]]) = \mathfrak{m}_1[[X]] \cap \ldots \cap \mathfrak{m}_r[[X]]$.

Since nilradical is intersection of all primes, and the prime ideals $\mathfrak{m}_i[[X]]$ do not contain each other, it follows that $\mathfrak{m}_i[[X]]$ are minimal prime ideals in $R[[X]]$. Finally, note that the prime ideals in $R[[X]]$ that contain $\mathfrak{m}_i[[X]]$ are in one-to-one correspondence with the prime ideals of $(R/\mathfrak{m}_i)[[X]]$ which we know from part c) are either (0) or (X). It follows that the chains of prime ideals $\mathfrak{m}_i[[X]] \subset \mathfrak{m}_i[[X]]+(X)$ are maximal length chains and they are all maximal length chains of prime ideals, so Krull dimension of $R[[X]]$ is 1. $\boxed{6, \text{C}}$

3. (a) If I contains $f = X_1^{i_1} X_2^{i_2} \ldots X_n^{i_n}$ then f has to vanish at all points of $\mathcal{V}(I)$ but the vanishing locus of $f(a_1, \ldots, a_n) = 0$ implies $a_i = 0$ for some i. Conversely, suppose that for every $(a_1, \ldots, a_n) \in \mathcal{V}(I)$, $a_i = 0$ for at least one i. Then, this implies that $X_1 X_2 \ldots X_n \in \mathcal{I}(\mathcal{V}(I))$. By the Nullstellensatz, then $X_1 X_2 \ldots X_n \in \sqrt{I}$, hence $(X_1 X_2 \ldots X_n)^N \in I$ for some N. $\boxed{5, \text{A}}$

(b) (i) Since $\mathbb{C}[X_1, \ldots, X_n]$ is a UFD, we can write $F = F_1 F_2 \ldots F_s$ and $G = G_1 G_2 \ldots G_r$ with F_i and G_j are irreducible and $F_i \neq F_j$ (resp. $G_i \neq G_j$)for any $i \neq j$ by the assumption that F and G are square-free. Now, $\mathcal{V}(F) = \mathcal{V}(G)$ implies that G vanishes at all points of $\mathcal{V}(F_i)$, hence $G \in \mathcal{I}(\mathcal{V}(G_i))$ which, by Nullstellensatz, means $G \in \sqrt{(F_i)}$. But, F_i is irreducible, hence (F_i) is prime, hence radical. So, $G \in (F_i)$ which means F_i divides G, therefore $F_i = G_j$ for some j. It follows that the irreducible factors of F and G coincide, hence $F = cG$ for some unit $c \in \mathbb{C}$. $\boxed{5, \text{B}}$

(ii) Consider the square-free polynomial $F = (X^2 + Y^2 - 1)(X^2 + Y^2 + 1)$. Then $\mathcal{V}(F) = \mathcal{V}(G)$ for $G = X^2 + Y^2 - 1$ but F and G have different degree, hence it can't be that $F = cG$ for some $c \in \mathbb{R} \setminus \{0\}$. $\boxed{5, \text{B}}$

(c) The ideal $I = (XZ, XW + YZ, YW)$ is not radical, because if $XZ = YW = XW + YZ = 0$, then XW and YW also vanishes, hence $XZ, YW \in \mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$ by the Nullstellensatz. We claim that $\sqrt{I} = (XZ, XW, YZ, YW)$. We have already seen, $(XZ, XW, YZ, YW) \subset \sqrt{I}$. To see the opposite inclusion. We note that

$$\mathcal{V}(I) = \{(x, y, 0, 0) \in \mathbb{C}^4 : (x, y) \in \mathbb{C}^2\} \cup \{(0, 0, z, w) \in \mathbb{C}^4 : (z, w)\}$$

So, if $f \in \mathbb{C}[X, Y, Z, W]$ such that $f \in \mathcal{I}(\mathcal{V}(I))$, then $f(X, Y, 0, 0) = 0 \in \mathbb{C}[X, Y]$ and $f(0, 0, Z, W) \in \mathbb{C}[Z, W]$. This means that every term of f is divisible by at leas one of X and Y, and at least one of Z, W. Hence, $f \in (XZ, XW, YZ, YW)$.

$\boxed{5, \text{C}}$

4. (a) We show that any prime ideal $\mathfrak{p}$ is maximal. It suffices to show that $R/\mathfrak{p}$ is a field. For any element $r \in R$, $r(r^{n-1} - 1) = 0$ for some n. Therefore, its image $\overline{r} \in R/\mathfrak{p}$ satisfies $\overline{r}(\overline{r}^{n-1} - 1) = 0$ but $R/\mathfrak{p}$ is an integral domain, therefore any non-zero element $\overline{r}$ satisfies $\overline{r}^{n-1} = 1$ for some n, hence is invertible. Thus, $R/\mathfrak{p}$ is a field and $\mathfrak{p}$ is maximal. $\boxed{6, \mathrm{C}}$

(b) Dimension of a ring is given by the supremum of heights of maximum ideals. For a PID, by Krull's height theorem, $h(\mathfrak{m}) \leq 1$ for any maximal ideal $\mathfrak{m}$. Hence, dimension of the ring can be 0 or 1.

Consider $\mathbb{Z}[\sqrt{-5}]$. This can't be a PID because PID implies UFD and we know that $21 = 3 \times 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$ and it is easy to check that each 3 is prime and does not divide any of the factors in the second factorization. On the other hand, being an integral extension of $\mathbb{Z}$, the ring $\mathbb{Z}[\sqrt{-5}]$ has dimension 1 by Cohen-Seidenberg theorem, and an integral domain since it is a subring of $\mathbb{C}$. $\boxed{7, \mathrm{B}}$

(c) We have seen in the lectures that if $A \subset B$ is an integral extension that $A/\mathfrak{p} \subset B/\mathfrak{p}B$ is also an integral extension. Moreover, prime ideals $\mathfrak{q} \subset B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$ are in bijection with prime ideals $\overline{\mathfrak{q}} \subset B/\mathfrak{p}B$ with $\overline{\mathfrak{q}} \cap A/\mathfrak{p} = (0)$. Therefore, we may assume A is an integral domain and $\mathfrak{p} = (0)$. Next, consider the multiplicative set $S = A \setminus \{0\}$. As in the proof of Cohen-Seidenberg theorem, we have a diagram

$$\begin{array}{ccc} A & \to & B \\ \downarrow_{\alpha} & & \downarrow_{\beta} \\ S^{-1}A & \to & S^{-1}B \end{array}$$

such that there is a bijection between prime ideals $\mathfrak{q} \subset B$ that contract to (0) in A and prime ideals $S^{-1}\mathfrak{q}$ in $S^{-1}B$ that contract to $(0) \in A$. But now $S^{-1}A$ is a field, and $S^{-1}B$ is a finite ring over field, so it is an Artinian ring. In particular, it has only finitely many prime (in fact, maximal) ideals. Hence, the proof is complete. $\boxed{7, \mathrm{D}}$

5. (a) A valuation ring is an integral domain R such that for all $x \in K \setminus \{0\}$, where K is the field of fractions of R, either $x \in R$ or $x^{-1} \in R$. $\boxed{2, \text{A}}$

(b) By the definition of valuation rings, R' is also a valuation ring since its field of fractions coincides with that of R. It is therefore also local. Let maximal ideal of R' be $\mathfrak{m}'$. Let $\mathfrak{p} = \mathfrak{m}' \cap R$. We claim that $R_\mathfrak{p} = R'$.

Let $x \in R \setminus \mathfrak{p}$. Then $x \notin \mathfrak{m}'$; otherwise, $x \in R \cap \mathfrak{m}' = \mathfrak{p}$. x is thus invertible in R' so $R_\mathfrak{p} \subset R'$ as $R_\mathfrak{p}$ is the smallest subring between R and its field of fractions such that elements in $R \setminus \mathfrak{p}$ are invertible. Similarly as in the first paragraph, $R_\mathfrak{p}$ is also a valuation ring, therefore local with its maximal ideal $\mathfrak{m}_\mathfrak{p}$. Suppose there exists $x \in R' \setminus R_\mathfrak{p}$. $x \notin R_\mathfrak{p}$ so $x^{-1} \in R_\mathfrak{p}$ and x^{-1} is not invertible in $R_\mathfrak{p}$ so $x^{-1} \in \mathfrak{m}_\mathfrak{p} \subset \mathfrak{m}'$. However, $x \in R'$ so x^{-1} is invertible in R', which is a contradiction.

[A variant for the last argument: Let $x \in R' \setminus R$, then $x^{-1} \in R$. Hence, x is a unit of R', thus $x^{-1} \notin \mathfrak{m}'$ and so $x^{-1} \notin \mathfrak{p}$. Thus, $x = \frac{1}{x^{-1}} \in R_\mathfrak{p}$.] $\boxed{9, \text{D}}$

(c) Let $\sqrt{I}$ be a radical ideal in R. Suppose $ab \in \sqrt{I}$, then there exists r such that $(ab)^r \in I$. Without loss of generality, assume $\nu(a) \geq \nu(b)$. Then $\nu(a^{2r}) \geq \nu((ab)^r)$. Hence, $a^{2r} \in I$, which implies $a \in \sqrt{I}$.

[Another possible solution: Let R be a valuation ring and $I \subset R$ be a radical ideal. Suppose there exist nonzero $a, b \in R$ such that $ab \in I$ but $a \notin I$ and $b \notin I$. I is radical so $a^2 \notin I$ and $b^2 \notin I$, $(a^2) \not\subset I$ and $(b^2) \not\subset I$. Since R is a valuation ring, $I \subset (a^2)$ and $I \subset (b^2)$. $ab \in I$ so $a^2 | ab$ and $b^2 | ab$. a, b are nonzero so $a|b$, $b|a$. Then a, b differ by a unit and $a^2 \in I$, a contradiction.] $\boxed{9, \text{C}}$

Review of mark distribution:

Total A marks: 29 of 29 marks
Total B marks: 29 of 32 marks
Total C marks: 26 of 24 marks
Total D marks: 16 of 15 marks
Total marks: 100 of 100 marks
Total Mastery marks: 0 of 0 marks

MATH70061 Commutative Algebra

Question	Marker's comment
1	The first part of this question was mostly answered correctly. The second part required a simple non-trivial idea and was not perceived by all. People who got the third part did mostly answer it correctly.
2	Most people scored a good mark in this question. The difficult part was similar to one of coursework problems.
3	This was the easiest question in the exam. I am happy to see that there are several people who got a perfect score.
4	The first part was answered somewhat well. Almost everyone got the second one correctly. Almost no one got the last part fully correctly which was one of the harder problems in the exam
5	The first part was a definition and everyone got this correctly. The second and third parts were harder. There wasn't anyone who solved both completely but some people managed to give correct arguments for one of these parts.