Rings and Modules – Final exam

21.01.2020, 12:15-15:15

Your Name ______________________________

This examination booklet contains 6 problems on 20 pages of paper including the front cover and the empty pages.

Please, follow the instructions below!

(1) First sign the booklet on the line provided above!
(2) Calculators, books, notes, electronic devices etc. are NOT allowed.
(3) Please, mute your phone and leave it in your bag at the back of the classroom.
(4) Do all of your work in this booklet. If you need extra paper, ask the proctors to give you yellow paper. Make sure to number the yellow pages in a clear way, so that the graders cannot get confused with the correct order of the pages.
(5) You should fully justify/explain your answers. In each question, it is always stated what results you can assume without proving. Prove all relevant computations and claims that you make.
(6) The exercises do not require any involved computations or elaborate discussions – try to be coincise.
(7) You may unstaple the booklet, we are prepared to staple it back. However, it is your responsibility to put the papers in the right order.

This booklet is divided into 3 parts: Part A, Part B, Part C.
Each part contains 2 questions in total.
For each of Part A, Part B, Part C, you should choose exactly one of the two questions and solve that.
All questions carry equal weight.

In the table below, for each of the 3 parts report in the second column (the one labelled "Question #") the number corresponding to the question that you have attempted.
Only those questions whose number is reported in the table will be marked.

Part	Question #	Maximum score	Your score	
A		25		
B		25		
C		25		
	Exam	75		=E
	Homework	210		=HW
	Total	100		$=E + \frac{25}{210} * HW$

Part A

Choose one of the two following questions and solve it. Do not forget to report on the first page of the booklet which of the two questions you solved to Part A.

Question A.1 [25pt]

Let F be a field. For $n \in \mathbb{N}_{>0}$, we shall denote

$$R_n := F[X_1, \ldots, X_n],\ R'_n := F[X_1, X_1^{-1}, X_2, X_2^{-1}, \ldots, X_n, X_n^{-1}].$$

(1) Prove the following statement:

Let $\mathfrak{m} \subset R_n$ be a maximal ideal. Then the field $k = R_n/\mathfrak{m}$ is an algebraic extension of F.
[*You may assume here any result proved in the lectures, if clearly stated.*] [5pt]

(2) State and prove the weak Nullstellensatz. [5pt]

(3) For any n, describe the maximal ideals of R'_n, when $F = \mathbb{R}$.
[*You should indicate generators for each maximal ideal of R'_n.*] [5pt]

(4) Assume that F is algebraically closed.
Compute the Krull dimension of R'_n. [5pt]

(5) Assume that F is algebraically closed.
Show that any prime ideal $\mathfrak{p} \subset R'_n$ is the intersection of all maximal ideals of R'_n containing $\mathfrak{p}$. [5pt]

Solution to Question A.1

---

(1) Let $\mathfrak{m} \subseteq F[x_1, \dots, x_n] =: R$ be a maximal ideal. Then $k := F[x_1, \dots, x_n]/\mathfrak{m}$ is a field which is a quotient of a polynomial ring over the field F. Moreover, k contains F because of the (injective) ring homomorphism $F \to F[x_1, \dots, x_n]/m$. Then $\operatorname{trdeg}_F k = \dim k = 0$ by Theorem 5.9 of the course; thus, k is an algebraic extension of F.

(2) We state and prove the Weak Nullstellensatz.

Theorem 0.1. *If F is an algebraically closed field then every maximal ideal of $F[x_1, \dots, x_n]$ is of the form $\mathfrak{m}_{c_1,\dots,c_n} := (x_1 - c_1, \dots, x_n - c_n)$ for $c_1, \dots, c_n \in F$.*

Proof. The ideal $\mathfrak{m}_{c_1,\dots,c_n} = (x_1 - c_1, \dots, x_n - c_n)$ is maximal as it is the kernel of the morphism $\phi_{c_1,\dots,c_n} \colon F[x_1, \dots, x_n] \to F$ which the identity on F and sends x_i to $c_i \in F$. You can find the proof of this claim in the notes, cf. Example 7.3 in the notes.
Let $\mathfrak{m} \subseteq F[x_1, \dots, x_n] =: R$ be a maximal ideal. Then part (1) implies that $k := F[x_1, \dots, x_n]/\mathfrak{m}$ is an algebraic extension of F. But F is algebraically closed, so $k \supset F$ is the trivial extension and we can identify k with F via this embedding. Let $c_i := \overline{x_i} \in k = F$. Then $\mathfrak{m}_{c_1,\dots,c_n} \subseteq \ker(F[x_1, \dots, x_n] \to k) = \mathfrak{m}$. Since $\mathfrak{m}_{c_1,\dots,c_n}$ is maximal and $\mathfrak{m}$ is a proper ideal, we obtain $\mathfrak{m}_{c_1,\dots,c_n} = \mathfrak{m}$. ☐

(3) **Claim**. R'_n is the localization of R_n at the multiplicative system $m_n = \{c \prod_{i=1}^n x_i^{t_i},\ t_i \in \mathbb{N}, \prod_{i=1}^n t_i \neq 0, c \in F^*\}$.
Proof. As the multiplicative system is generated (multiplicatively) by the monomials $x_1, x_2, \cdots, x_n$ the conclusion follows at once. ☐

As R'_n is the localization of R_n at m_n, then it was proven in the example sheets that the maximal ideals of R'_n are the localizations of those maximal ideals of R_n that do not contain any element of m_n.
Let $\mathfrak{m} \subset R_n$ be a maximal ideal. As $F \simeq \mathbb{R}$, then $R_n/\mathfrak{m}$ is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$ by part (1).
If $R_n/\mathfrak{m} \simeq \mathbb{R}$, then we can repeat the argument given in part (2) and show that there exists $c_1, c_2, \dots, c_n \in \mathbb{R}$, such that $\mathfrak{m} = \mathfrak{m}_{c_1,c_2,\dots,c_n} = (x_1 - c_1, x_2 - c_2, \dots, x_n - c_n)$. In this case, $\mathfrak{m} \cap m_n = \emptyset$ if and only if $c_i \neq 0,\ \forall i = 1, 2, \dots, n$ by the maximality of $\mathfrak{m}$. Thus, all maximal ideal in R'_n are of the form $(x_1 - c_1, x_2 - c_2, \dots, x_n - c_n),\ (c_1, c_2, \dots, c_n),\ c_i \neq 0,\ \forall i$.
If $R_n/\mathfrak{m} \simeq \mathbb{C}$, then denoting by $\overline{x}_i \in R_n/\mathfrak{m}$ the class of x_i, it follows that x_i is a root of a monic polynomial $f_i(X)$ of degree 1 or 2 irreducible over $\mathbb{R}$, the minimal polynomial of $\overline{x}_i$ over $\mathbb{R} \subset R_n/\mathfrak{m}$ – here we are indentifying $\mathbb{R} \subset R_n/\mathfrak{m}$ with the image of the composition of homomorphisms

$$\mathbb{R} \xrightarrow{i} R_n \xrightarrow{\pi} R_n/\mathfrak{m} ,$$

where i is the inclusion of the fileds of coefficients in the polynomial ring, while π is the projection to the quotient. But then the kernel of the map π is the ideal $=(f_1(x_1), f_2(x_2), \dots, f_n(x_n))$. In this case, $\mathfrak{m} \cap m_n = \emptyset$ if and only if $f_i(X) \neq X,\ \forall i = 1, 2, \dots, n$ by the maximality of $\mathfrak{m}$. Thus, all maximal ideal in R'_n are of the form $(f_1(x_1), f_2(x_2), \dots, f_n(x_n))$, $f_i(X) \in \mathbb{R}[X]$ monic irreducible polynomial of degree 1 or 2, and $f_i(X) \neq X$, $\forall i$.

(4) As R'_n is a localization of R_n, then $\dim(R'_n) = \dim R'$ as

$$R_n \subset R'_n \subset Frac(R_n)$$

which implies that $Frac(R'_n) = Frac(R_n)$, so that by Theorem 5.9 of the course, $\dim(R'_n) := \text{trdeg}_F Frac(R'_n) = \text{trdeg}_F Frac(R_n) =: \dim R'$.

(5) As R'_n is the localization of R_n at m_n, then it was shows in class that the prime ideals of R'_n are the extensions under localization of those prime ideals of R_n that do not contain any element of m_n. Moreover, the same argument as in (3) shows that the maximal ideal of R'_n have the form $(X_1 - a_1, X_2 - a_2, \dots, X_n - a_n)$, $a_i \in F$, $a_1 a_2 \cdot a_n \neq 0$.

Let us denote by $\pi\colon R_n \to R'_n$ the localization map. Then, we know that $\mathfrak{p}$ is the extension of a prime ideal $\mathfrak{q} \subset R_n$.

Claim. Any prime ideal $\mathfrak{q} \subset R_n$ is the intersection of all maximal ideals of R_n containing $\mathfrak{q}$.

Proof. It is clear that

$$\mathfrak{q} \subset \cap_{\mathfrak{m} \text{ maximal, } \mathfrak{m} \supseteq \mathfrak{q}} \mathfrak{m}.$$

Assume that the reverse inclusion does not hold. But then

$$\exists f \in (\cap_{\mathfrak{m} \text{ maximal, } \mathfrak{m} \supseteq \mathfrak{q}} \mathfrak{m}) \setminus \mathfrak{q}.$$

But then $f(a) = 0$, $\forall a in V(\mathfrak{q})$. On the other hand, we have shown in class that since (F is algebraically closed and) $\mathfrak{q}$ is prime, hence radical, then $\mathfrak{q} = \{g \in F[x_1, \dots, x_n] = R_n \mid g(a) = 0, \ \forall a \in V(\mathfrak{q}) \subset \mathbb{A}^n\}$. In particular, also $f \in \mathfrak{q}$ by the above observation, which gives a contradiction. $\square$

It suffices to show that the following claim. **Claim** Let $\{J_i\}_{i \in I}$ be prime ideals of R_n such that $L := \cap_{i \in I} J_i$ is prime and $L \cap m_n = \emptyset$. Then $L^e = \cap_{i \in I} J_i^e$.

Proof. $L^e \subset \cap_{i \in I} J_i^e$: let $t \in (\cap_{i \in I} J_i)^e$ then $t = r/s$, with $r \in \cap_{i \in I} J_i, s \in m_n$. Then as $r \in J_i$, $\forall i \in I$, then $r/s \in J_i^e, \forall i \in I$.

$L^e \supset \cap_{i \in I} J_i^e$: let $t \cap_{i \in I} J_i^e$, $t = r/s$, $r \in R_n$, $s \in m_n$. But then $r = st \in J_i^e$, $\forall i \in I$. If for a certain $i \in I$, $J_i \cap m_n = \emptyset$, then $J_i = J_i^{ec}$, hence $r \in J_i$. If for a certain $i \in I$, $r \notin J_i$, then $J_i^{ec} \neq J_i$ and by the primality of the J_i, then $J_i^e = (1)$, that is, $J_i \cap m_n \neq \emptyset$. As J_i is prime and m_n contains monomials in the x_k then $x_l \in J_i$ for some $l = 1, \dots, n$. This implies then that $r x_1 \cdot x_n \in J_i$, $\forall i \in I$, hence $r x_1 \cdot x_n \in L$. As $L \cap m_n = \emptyset$, then $x_1 \cdot x_n \notin L$, hence $r \in L$, so that $r/s \in L^e$. $\square$

QUESTION A.2 [25PT]

Let F be an algebraically closed field Let n, p, q be positive integers, with $p > 1, n, q > 0$.

(1) State the definition of an integral extension of rings and the definition of an integrally closed ring. [4pt]

(2) State Noether's Normalization Theorem. [4pt]

(3) Let R be the ring $R := F[X, Y, T_1, \ldots, T_n]/(X^pY^q - f(T_1, \ldots, T_n))$, where $f \in F[T_1, \ldots, T_n]$ is a non-constant polynomial.
Construct an integral extension $S \subset R$ with $S = F[Z_1, \ldots, Z_l]$ as guaranteed by Noether's Normalization Theorem.
What is the meaning of the integer l? [9pt]

(4) Show that in each entry of the list below the ring R is a domain and compute the integral closure:
(a) $R = F[x, y]/(x^2 - y^3)$
(b) $R = F[x, y, z]/(x^2 - yz^2)$
(c) $R = F[x, y, z]/(x^2 - yz)$
[8pt]

Solution to Question A.2

(1) This is Definition 5.11 in the notes.
(2) This is Theorem 5.18 in the notes.
(3) Let R be the ring $R := F[X, Y, T_1, \dots, T_n]/(X^pY^q - f(T_1, \dots, T_n))$, where $f \in F[T_1, \dots, T_n]$ is a non-constant polynomial. Take the following change of coordinates

$$A := X, \quad B = Y - X, \quad C_i = T_i, \forall i = 1, 2, \dots, n,$$

so that $B+A = Y$ With respect to this new set of coordinate, the polynomial $X^pY^q - f(T_1, \dots, T_n)$ becomes

$$A^p(B + A)^q - f(C_1, \dots, C_n) = A^{p+q} + \sum_{i=i}^{q} \binom{q}{i} B^i A^{p+q-1} - f(C_1, \dots, C_n)$$

and

$$\begin{aligned} R :=&F[X, Y, T_1, \dots, T_n]/(X^pY^q - f(T_1, \dots, T_n)) \\ =&F[A, B, C_1, \dots, C_n]/(A^{p+q} + \sum_{i=i}^{q} \binom{q}{i} B^i A^{p+i-1} - f(C_1, \dots, C_n))). \end{aligned}$$

which immediately show that R is integral over the subring $F[B, C_1, \dots, C_n]$, as by the above observations $R = F[B, C_1, \dots, C_n][A]$ and A satisfies the monic equation $S^{p+q} + \sum_{i=i}^{q} \binom{q}{i} B^i S^{p+i-1} - f(C_1, \dots, C_n) = 0$ in the indeterminate S.
Alternatively, one can construct an integral extension $S \subset R$ with $S = F[Z_1, \dots, Z_l]$ following the proof of Noether's Normalization Theorem.
When R is a domain, then the integer l is the transcendence degree of the field of fractions of R. [9pt]
(4) (a) $R = F[x, y]/(x^2 - y^3)$
To prove R is a domain, it suffices to show that (x^2-y^3) is irreducible, as $F[x, y]$ is a UFD. Considering the isomorphism $F[x, y] \simeq F[y][X]$ where the latter is the ring of polynomials in the variable X with coefficients in $F[y]$, then the only possibilty for $(X^2 - y^3)$ to be irreducible is that it is a product of two polynomials of degree 1 in X,

$$\begin{gathered} X^2 - y^3 = p_1(X, y)p_2(X, y), \\ p_1(X, y) = a_1(y)X + b_1(y), \quad p_2(X, y) = a_2(y)X + b_2(y). \end{gathered}$$

But then,

$$a_1(y) \cdot a_2(y) = 1, \quad b_1(y) + b_2(y) = 0, \quad b_1(y) \cdot b_2(y) = y^3,$$

which is impossible as it would imply that $-b_1(y)^2 = y^3$.
To compute the integral closure of R, let us denote by Q the field of fractions of R. We will denote by $\overline{x}, \overline{y}$ the classes of x, y in R, respectively. Then $\frac{\overline{x}}{\overline{y}} \in Q$ and

$$\left(\frac{\overline{x}}{\overline{y}}\right)^2 = \frac{\overline{x}^2}{\overline{y}^2} = \frac{\overline{y}^3}{\overline{y}^2} = \overline{y},$$

that is, $\frac{\overline{x}}{\overline{y}}$ is a solution to the monic polynomial $T^2 - \overline{y} \in R[T]$. Thus $\frac{\overline{x}}{\overline{y}} \in \overline{R}$, where $\overline{R}$ denotes the integral closure of R. Moreover,

$$\left(\frac{\overline{x}}{\overline{y}}\right)^3 = \frac{\overline{x}^3}{\overline{y}^3} = \frac{\overline{x}^3}{\overline{x}^2} = \overline{x},$$

so that $F\left[\frac{\overline{x}}{\overline{y}}\right] \supseteq R$, in particular Q is also the field of fractions of the ring $F\left[\frac{\overline{x}}{\overline{y}}\right]$.

Finally, we claim that $F\left[\frac{\overline{x}}{\overline{y}}\right] \subseteq Q$ is integrally closed. Indeed, it suffices that to prove that $F\left[\frac{\overline{x}}{\overline{y}}\right] \simeq F[T]$, where T is just a free variable. As Q is the field of fraction of $F\left[\frac{\overline{x}}{\overline{y}}\right]$, then using the above isomorphism $Q \simeq F(T)$ and we have seen that $F[T] \subseteq F(T)$ is integrally closed. To prove that there exists an isomorphism $F\left[\frac{\overline{x}}{\overline{y}}\right] \simeq F[T]$, let us notice that $F[\overline{x}] \subset R \subset F\left[\frac{\overline{x}}{\overline{y}}\right]$ and $F[\overline{x}] \simeq F[U]$, where U is just a free variable. This follows since we have the projection to the quotient map (restricted to $F[x]$)

$$F[x] \hookrightarrow F[x,y] \twoheadrightarrow R := F[x,y]/(x^2 - y^3)$$

which is injective since $F[x] \cap (x^2 - y^3) = (0)$. But then this implies that the dimension of $F\left[\frac{\overline{x}}{\overline{y}}\right]$ as a $\mathbb{Z}$-module is ∞ (as the dimension of $F\left[\overline{x}\right]$ is ∞), so that $F\left[\frac{\overline{x}}{\overline{y}}\right]$ is isomorphic to a polynomial ring.

(b) $R = F[x,y,z]/(x^2 - yz^2)$.
To prove R is a domain, it suffices to show that $(x^2 - yz^2)$ is irreducible, as $F[x,y,z]$ is a UFD. Considering the isomorphism $F[x,y,z] \simeq F[y,z][X]$ where the latter is the ring of polynomials in the variable X with coefficients in $F[y,z]$, then the irreducibility of $X^2 - yz^2$ follows from Eisenstein's criterion, as y does not divide the leading coefficient of the polynomial, which is 1, y divides the coefficient of the linear term in X, which is 0, and y divides the constant term with respect to the variable X, yz^2, while y^2 does not divide yz^2.
To compute the integral closure of R, let us denote by Q the field of fractions of R. We will denote by $\overline{x}, \overline{y}, \overline{z}$ the classes of x, y, z in R, respectively. Then $\frac{\overline{x}}{\overline{z}} \in Q$ and

$$\left(\frac{\overline{x}}{\overline{z}}\right)^2 = \frac{\overline{x}^2}{\overline{z}^2} = \frac{\overline{yz}^2}{\overline{z}^2} = \overline{y},$$

that is, $\frac{\overline{x}}{\overline{z}}$ is a solution to the monic polynomial $T^2 - \overline{y} \in R[T]$. Thus $\frac{\overline{x}}{\overline{z}} \in \overline{R}$, where $\overline{R}$ denotes the integral closure of R. Thus $F\left[\frac{\overline{x}}{\overline{z}}, \overline{z}\right] \supset R$ since $\frac{\overline{x}}{\overline{z}} \cdot \overline{z} = \overline{z}$. In particular Q is also the field of fractions of the ring $F\left[\frac{\overline{x}}{\overline{z}}, \overline{z}\right]$.
Finally, we claim that $F\left[\frac{\overline{x}}{\overline{z}}, \overline{z}\right] \subseteq Q$ is integrally closed. Indeed, it suffices that to prove that $F\left[\frac{\overline{x}}{\overline{z}}, \overline{z}\right] \simeq F[T,V]$, where S is just a free variable. As Q is the field of fraction of $F\left[\frac{\overline{x}}{\overline{z}}, \overline{z}\right]$, then using the above isomorphism $Q \simeq F(T,V)$ and we have seen that $F[T,V] \subseteq F(T,V)$ is integrally closed. To prove that there exists an isomorphism $F\left[\frac{\overline{x}}{\overline{z}}, \overline{z}\right] \simeq F[T,V]$, let us notice that $F[\overline{x}, \overline{z}] \subset R \subset F\left[\frac{\overline{x}}{\overline{z}}, \overline{z}\right]$ and $F[\overline{x}, \overline{z}]$, where

U is just a free variable. The latter claim follows since we have the projection to the quotient map (restricted to $F[x,z]$)

$$F[x,z] \hookrightarrow F[x,y,z] \twoheadrightarrow R := F[x,y,z]/(x^2 - yz^2)$$

which is injective since $F[x,z] \cap (x^2 - yz^2) = (0)$. But then this implies that $F\left[\frac{\overline{x}}{\overline{z}}, \overline{z}\right]$ is not finitely generated as a $F[\overline{z}]$-module (as$F\left[\overline{x}, \overline{z}\right]$ is not finitely generated as a $F[\overline{z}]$-module), so that $F[\overline{z}]\left[\frac{\overline{x}}{\overline{z}}\right]$ is isomorphic to a free polynomial ring in 2 variables.

(c) $R = F[x,y,z]/(x^2 - yz)$.
To prove R is a domain, it suffices to show that $(x^2 - yz)$ is irreducible, as $F[x,y,z]$ is a UFD. Considering the isomorphism $F[x,y,z] \simeq F[y,z][X]$ where the latter is the ring of polynomials in the variable X with coefficients in $F[y,z]$, then the irreducibility of $X^2 - yz$ follows from Eisenstein's criterion, as y does not divide the leading coefficient of the polynomial, which is 1, y divides the coefficient of the linear term in X, which is 0, and y divides the constant term with respect to the variable X, yz^2, while y^2 does not divide yz^2.

[8pt]

Part B

Choose one of the two following questions and solve it. Do not forget to report on the first page of the booklet which of the two questions you solved to Part B.

Question B.1 [25pt]

Let R be a commutative ring with unit. Let n, q, k be positive integers. We denote by $\mathrm{Mat}_k(R)$ the free R-module of $k \times k$ matrices with coefficients in R.

(1) State the Fundamental Theorem of PIDs and the Smith normal form reduction theorem. [5pt]

(2) For the following matrices, either compute, when possible, their Smith normal form or explain why they cannot be reduced to Smith Normal form:

(a) $A \in \mathrm{Mat}_n(\mathbb{R}[X])$ and all entries of A are equal to the polynomial

$$f(X) = 2020X^{2019} + 2019X^{2018} + 2018X^{2017} + 2017X^{2016} + \cdots + 3X^2 + 2X + 1.$$

(b) $B = \begin{pmatrix} 2 & 0 \\ X & 0 \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z}[X])$

(c) C is the same matrix as in (a), but this time you should consider it as a matrix with coefficients in $\mathbb{Z}[X]$.

[10pt]

(3) Give an example of a $\mathbb{Z}$-module M which is not finitely generated and for which there exists an endomorphism $f\colon M \to M$ which cannot be put in Smith normal form. [5pt]

(4) Let $R = \mathbb{Q}$ and let $f_{\min}(X) = (X-1)^2(X^3-3)$, $g(X) = (X-1)^4(X^3-3)$. How many different conjugation classes are there in $\mathrm{Mat}_7(R)$ of matrices with minimal polynomial $f_{\min}(X)$ and characteristic polynomial $g(X)$?

[*Recall for an endomorphism $\psi\colon V \to V$ of a $\mathbb{Q}$-vector space the minimal polynomial of ψ is the monic generator of the kernel of the ring homorphism*

$$\begin{aligned} \mathbb{Q}[X] &\to \mathrm{End}_{\mathbb{Q}}(V) \\ 0 &\mapsto 0 \\ 1 &\mapsto 1 \\ X &\mapsto \psi. \end{aligned}$$

] [5pt]

Solution to Question B.1

---

(1) The Fundamental Theorem of PIDs is Theorem 4.13 in the notes.
Smith normal form reduction theorem is Theorem 4.5 in the notes. [5pt]

(2) (a) We consider the matrix $A \in \mathrm{Mat}_n(\mathbb{R}[X])$ as an endomorphism a of the free module $M := \oplus_{i=1}^n \mathbb{R}[X]$. Let $e_i,\ i = 1, \dots, n$ denote the standard basis of this free module. Then with respect to this basis $a(e_i) = \sum_{j=1}^n f(X)e_j$. But then for any $i, k = 1, 2, \dots, n$,

$$a(e_i - e_k) = a(e_i) - a(e_k) = 0.$$

Claim. The following is a basis of M

$$g_i = -e_{i+1} + e_i,\ i = 1, \dots, n-1,\ g_n = \frac{\sum_{i=1}^n e_i}{n}.$$

Proof. To show that $\{g_1, \dots, g_n\}$ are linearly independent in M, let us notice that $0 \neq g_n \in Im(a)$, while $g_i \in \ker(a),\ i = 1, \dots, n-1$, and

$$0 = \sum_{i=1}^{n-1} \lambda_i g_i = (\lambda_1, \lambda_2 - \lambda_1, \lambda_3 - \lambda_2, \dots, \underbrace{\lambda_i - \lambda_{i-1}}_{i\text{-th position}}, \dots, -\lambda_{n-1})$$

if and only if $\lambda_i = 0,\ \forall i = 1, \dots, n-1$. To conclude the proof, then it suffices to consider the change of basis matrix from the basis $\{g_i\}$ to the basis $\{e_i\}$ which is as follows

$$S = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \frac{1}{n} \\ -1 & 1 & 0 & 0 & 0 & \frac{1}{n} \\ 0 & -1 & 1 & 0 & 0 & \frac{1}{n} \\ 0 & 0 & -1 & \ddots & 0 & \vdots \\ 0 & 0 & 0 & 0 & 1 & \frac{1}{n} \\ 0 & 0 & 0 & 0 & -1 & \frac{1}{n} \end{pmatrix}.$$

By the above reasoning, we know $\det(S) \neq 0$. On the other hand, as all the entries of S are in $\mathbb{R}$, then $\det(S) \in \mathbb{R}$, but any non-zero element of $\mathbb{R}$ is invertible in $\mathbb{R}[X]$, which concludes our proof. □

With respect to the basis then as

$$a(g_1) = 0,\ i = 1, \dots, n-1,\ a(g_n) = f(X)g_n,$$

so that the matrix of a in this basis is given by

$$\left(\begin{array}{c|c} f(X) & 0_{1,n-1} \\ \hline 0_{n-1,1} & 0_{n-1,n-1} \end{array}\right)$$

which is exactly in Smith normal form.

(b) $\ker(B) = \mathbb{Z}[X](0, 1)$, while $Im(B) = \mathbb{Z}[X](2, X)$. Hence, the only possibility to have a Smith normal form for the matrix B would be that we have a basis $\{g_1, g_2\}$ of $\mathbb{Z}[X]^2$ such that (up to permuting the order of the g_i) the span of g_1 contains $\mathbb{Z}[X](2, X)$ and the span of g_2 contains $\mathbb{Z}[X](0, 1)$. But this forces $g_1 = (2, X)$ as $gcd(2, X) = 1$ and

$g_2 = (0,1)$. But the change of basis matrix from the basis $\{g_1, g_2\}$ to the basis $\{e_1, e_2\}$ would be

$$S = \begin{pmatrix} 2 & 0 \\ X & 1 \end{pmatrix},$$

which is not invertible, since $\det(S) = 2$ and 2 is not invertible in $\mathbb{Z}[X]$.

(c) Take $n = 2$ and let us use the same notation as in part (a). Then $ker(a) = \mathbb{Z}[X](e_1 - e_2)$ and $Im(a) = \mathbb{Z}[X][f(X)(e_1 + e_2)]$. Hence, the only possibility to have a Smith normal form for the matrix C would be that we have a basis $\{g_1, g_2\}$ of $\mathbb{Z}[X]^2$ such that (up to permuting the order of the g_i) the span of g_1 contains $\mathbb{Z}[X](e_1 - e_2)$ and the span of g_2 contains $\mathbb{Z}[X][f(X)(e_1 + e_2)]$. But this forces $g_1 = e_1 - e_2$ and $g_2 = h(X)(e_1 + e_2)$, with $h(X)|f(X)$. But the change of basis matrix from the basis $\{g_1, g_2\}$ to the basis $\{e_1, e_2\}$ would be

$$S = \begin{pmatrix} 1 & h(X) \\ -1 & h(X) \end{pmatrix},$$

which is not invertible, since $\det(S) = 2h(X)$ and 2 is not invertible in $\mathbb{Z}[X]$.

[10pt]

(3) Let M be the $\mathbb{Z}$-module defined as

$$M := \bigoplus_{i=0}^{\infty} \mathbb{Z}.$$

The module M is the collection of all sequences of integers, $(a_i)_{i\in\mathbb{N}},\ a_i \in \mathbb{Z}$, which only have a finite number of non-zero elements. The elements $e_i \in M,\ i \in \mathbb{N}$, where e_i is the sequence that has 1 in the i-th spot and 0 elsewhere, form a basis of M. The module M is equipped with the following family of endomorphisms

$$s_k \colon M \to M, \quad k \in \mathbb{N}_{>0}$$
$$s_k(e_i) = e_{i+k}.$$

For any $k > 0$, s_k is injective since, by definition of s_k, the elements $s_k(e_i)$ are linearly independent as they are part of a basis of M.

Claim. For any $0 \neq (a_i)_{i\in\mathbb{N}} \in M$, then $s_k((a_i))$ is never parallel to (a_i).

Proof. In fact if j is the largest index such that $a_j \neq 0$ in (a_i), then $j + k$ is the is the largest index such that $s_k(a_i)$ has a non-zero entry, which proves our claim. $\square$

But this implies that s_k, $k > 0$, can never be put in Smith normal form since $s_k \neq 0$ but we cannot find any eigenvector of s_k.

(4) Let A be a matrix satisfying the conditions of the exercise. As $g(X) = (X-1)^4(X^3-3)$, we know that 1 is an eigenvalue of A of algebraic multiplicity $= 4$. Then, up to similarity, A contains a 4×4 diagonal block of the form

$$\left(\begin{array}{c|cccc} B & 0 & 0 & 0 & 0 \\ \hline 0 & 1 & * & * & * \\ 0 & 0 & 1 & * & * \\ 0 & 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 & 1 \end{array}\right),$$

where B is a 3×3 matrix. As $f_{min}(A) = 0$ then

$$\begin{pmatrix} 1 & * & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & 1 \end{pmatrix}^2 - \mathrm{Id} = 0.$$

But then the Jordan normal form theorem implies that A is similar to one of the following 2 matrices (which are not similar)

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

On the other hand, the matrix B must satisfy the equation B and you have seen in the exercises that if an $n \times n$ matrix S satisfies a degree n polynomial $g(X) \in \mathbb{Q}[X]$ irreducible over $\mathbb{Q}$, $g(X) = X^n + \sum_{i=0}^{n-1} a_i X^i$ then S is similar to the matrix

$$\begin{pmatrix} 0 & 0 & 0 & 0 & -a_0 \\ 1 & 0 & 0 & 0 & -a_1 \\ 0 & 1 & \ddots & 0 & \vdots \\ 0 & 0 & 1 & 0 & -a_{n-2} \\ 0 & 0 & 0 & 1 & -a_{n-1} \end{pmatrix}.$$

Hence, B is similar to the matrix,

$$\begin{pmatrix} 0 & 0 & 3 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

and so the only possibilities for the classes of similitude of A are

$$\begin{pmatrix} 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Question B.2 [25pt]

Let R be a commutative ring with unit.

(1) Define the notion of a primary ideal $I \subset R$.
Show that the radical ideal $\sqrt{I}$ of a primary ideal $I \subset R$ is prime.
State the theorem on the existence of minimal primary decompositions for ideals in a noetherian ring. What can be said in regards to the uniqueness such decompositions? [5pt]

(2) Let R be a PID. Show that R is Noetherian.
Is R Artinian? Either show that the stament holds or provide a counterexample.
[*For the first part of the question you cannot use the implication* PID $\Rightarrow$ UFD.] [4pt]

(3) Let R be a PID. Let $f \in R$ be a non-zero element and define $R' = R/(f)$.
Provide a justified answer to the following questions:
   (a) Characterize those $f \in R$ for which R' is a domain.
   (b) Is R' Artinian?
   (c) Compute the radical ideal $\sqrt{0} \subset R'$.

   Answer questions (a-d) when R is a UFD instead of a PID. [4pt]

(4) Let R be a UFD and let $I \subset R$ be a principal ideal.
Show that there exists a unique minimal primary decomposition of I.
Show that the uniqueness does not hold if I is not assumed to be principal. [5pt]

(5) Show that if $I = \sqrt{I}$ is a radical ideal and $ab \in I$, then $I = \sqrt{I + (a)} \cap \sqrt{I + (b)}$. [7pt]

Solution to Question B.2

(1) See Definition 7.32, Proposition 7.34, Theorem 7.52 and 7.54 in the notes.

(2) To show noetherianity of R, we have to show that R satisfies the ACC. Let

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \ldots$$

be an ascending chain of ideals. Then,

$$I = \cup_{k=1}^{\infty} I_k$$

is an ideal. Since R is a PID, then $I = (f)$ and $f \in I_{n_0}$, $n_0 \in \mathbb{N}$. But then $I = I_{n_0}$, since $I \supset I_{n_0}$, but since $f \in I_{n_0}$ also $I \subset I_{n_0}$, hence $I_{n_0} = I_{n_0+k}$, $\forall k \geq 0$ which show that the ascending chain is eventually constant.
A PID is not necessarily Artinian. Take $\mathbb{Z}$ which is a PID, but it contains the infinite descending chain of ideals

$$(2) \supset (4) \supset (8) \supset \cdots \supset (2^i) \supset \ldots.$$

(3) (a) R' is a domain if and only if f' is irreducible, that is, if $g|f'$ then $g = cf'$, c invertible in R. This does not change if R is a UFD rather than a PID.

(b) The ideal of R' are in 1-1 correspondence with the ideals of R which contains (f). Hence if we have a descending chain of ideals of R'

$$I'_1 \supset I'_2 \supset \cdots \supset I'_n \supset \ldots$$

this corresponds to a descending chain of ideals of R

$$I_1 \supset I_2 \supset \cdots \supset I_n \supset \ldots$$

containing (f). But then, since R is PID, then $I_i = (f_i)$ and $f_i|f_{i+1}|f$. But since PID $\Rightarrow$ UFD this gives a contradiction, since it would imply that f has infinitely many distinct non-trivial divisors.
If R is UFD, consider the case $R = \mathbb{Z}[X]$, which we know is UFD, and take $f = X$ Then $R' = \mathbb{Z}$ and we have seen that $\mathbb{Z}$ is not Artinian.

(c) The radical ideal $\sqrt{(0)} \subset R'$ is the image of the ideal $\sqrt{(f)} \subset R$ under the quotient map $R \to R'$. On the other hand $\sqrt{(f)} := \{x \in R \mid \exists n \in \mathbb{N}_{>0} \text{ s.t. } x^n \in (f)\}$. An element $y \in R$ belongs to (f) when $f|y$. As R is a UFD, then writing the decomposition of f

$$f = \prod_{i=1}^{n} f_i^{n_i}, n_i \in \mathbb{N}_{>0},$$

then we see that an element $x \in R$ such that $x^n \in (f)$ must be divisible by all the irreducibles f_i dividing f. On the other hand, taking $n := \max n_i$, it follows that if $f_i|x$, $\forall i$, then $f|x^n$. Hence, $\sqrt{(f)} = (\prod_{i=1}^{n} f_i)$.
We have not really used that R is PID, just that it is a UFD.

(4) Let $f \in R$ be irreducible. Then $\mathfrak{p} = (f)$ is prime. Also, $\forall n \in \mathbb{N}_{>0}$, $J_n := (f^n)$ is $\mathfrak{p}$-primary. To prove this, take $x, y \in R$ such that $xy \in J_n$ and assume that $x \notin J_n$. Then $f^n \not| x$ and $f^n | xy$ which implies that $f|y$ so that $y^n \in J_n$.
Let $I = (g)$ and write

$$g = \prod_{i=1}^{n} g_i^{n_i}, n_i \in \mathbb{N}_{>0}$$

its decomposition. Then

$$I = \cap_{i=1}^{n} (g_i^{n_i})$$

is a unique minimal primary decomposition, since:

(a) the prime ideals (g_i) are the associated primes of I: in fact, for $j = 1, \ldots, n$, $(g_j) = Ann([g_j^{n_j - 1} \prod_{i=1, i\neq j}^{n} g_i^{n_i}])$.

(b) the ideals (g_i) are minimal: in fact, g_i is irreducible.

For the non-uniqueness of the primary decomposition for non-principal ideals, we saw, for example, Example 7.55 in the notes.

(5) We have to show that

$$I \subset \sqrt{I + (a)} \cap \sqrt{I + (b)}, \quad \text{and} \quad I \supset \sqrt{I + (a)} \cap \sqrt{I + (b)}.$$

$\subset$. Since $I \subset I + (a)$, $I \subset I + (b)$, a fortiori also $I \subset \sqrt{I + (a)}$, $I \subset \sqrt{I + (b)}$, which implies $I \subset \sqrt{I + (a)} \cap \sqrt{I + (b)}$.

$\supset$. Let $x \in \sqrt{I + (a)} \cap \sqrt{I + (b)}$. Then $x \in \sqrt{I + (a)}$ and $x \in \sqrt{I + (b)}$. Hence, there exists n, m such that

$$x^n = i_1 + f_1 a, \quad x^m = i_2 + f_2 b, \quad i_1, i_2 \in I, \; f_1, f_2 \in R.$$

Thus

$$x^{n+m} = (i_1 + f_1 a)(i_2 + f_2 b) = j_1 + cab, \quad j_1 \in I, c \in R.$$

This implies that $x^{n+m} \in I$ as $ab \in I$, but as I is radical, this implies that $x \in I$.

Part C

Choose one of the two following questions and solve it. Do not forget to report on the first page of the booklet which of the two questions you solved to Part C.

In this section you can assume the following result:
Let Q be an R-module. If $Q_{\mathfrak{m}} = 0$, for any maximal ideal $\mathfrak{m} \subset R$, then $Q = 0$.

Question C.1 [25pt]

Let R be a commutative ring with unit.

(1) Define what it means for a subset $T \subset R$ to be a multiplicatively closed subset of R. Define the localization $T^{-1}R$ of R at T and the natural homomorphism $R \to T^{-1}R$. [6pt]

(2) Let $\mathfrak{p} \subset R$ be a prime ideal. Define the localization $R_{\mathfrak{p}}$ of R at $\mathfrak{p}$. When is the natural homomorphism $R \to R_{\mathfrak{p}}$ injective? [5pt]

(3) Show that if for every prime $\mathfrak{p} \subset R$, $R_{\mathfrak{p}}$ contains no nilpotent element then R contains no nilpotent element. [7pt]

(4) Assume that R is a domain. Let M be an R-module.
recall that the submodule $\mathrm{Tor}(M) \subset M$ of torsion elements of M is defined as

$$\mathrm{Tor}(M) = \{m \in M \mid \exists r \in R \setminus \{0\} \text{ such that } rm = 0\}.$$

Let S be a multiplicatively closed subset of R. Show that $\mathrm{Tor}(S^{-1}M) = S^{-1}(\mathrm{Tor}(M))$, where $S^{-1}(\mathrm{Tor}(M))$ denotes the submodule generated by the image of $\mathrm{Tor}(M)$ in $S^{-1}M$.
Show that for an R-module M the following are equivalent:
(a) M is torsion-free;
(b) $M_{\mathfrak{p}}$ is torsion-free, for all prime ideals $\mathfrak{p} \subset R$;
(c) $M_{\mathfrak{m}}$ is torsion-free, for all maximal ideals $\mathfrak{m} \subset R$;
[7pt]

QUESTION C.2 [25PT]

Let R be a commutative ring with unit. Let M, N be R-modules.

(1) Define the R-modules $\operatorname{Ext}^i_R(M,N)$. [5pt]

(2) Construct a projective resolution for an R-module M

$$\mathcal{P}\colon \quad \cdots \to P_i \to \cdots \to P_1 \to P_0 \to M \to 0,$$

where each P_j is a free R-module.
Moreover, show that if R, M are Noetherian, then each P_i can be taken to be a free and finitely generated R-module. [5pt]

(3) Let $\mathfrak{p} \subset R$ be a prime ideal. Let P be a finitely generated free R-module. Show that there is an isomorphism or $R_{\mathfrak{p}}$-modules

$$\phi_{P,N}\colon \operatorname{Hom}_R(P,N)_{\mathfrak{p}} \to \operatorname{Hom}_{R_{\mathfrak{p}}}(P_{\mathfrak{p}}, N_{\mathfrak{p}}),$$

where the module $\operatorname{Hom}_R(P,N)_{\mathfrak{p}}$ is the localization of the R-module $\operatorname{Hom}_R(P,N)$ at $\mathfrak{p}$.
[*Hint: Use the universal property of free modules.*] [5pt]

(4) Let P_1, P_2 be free R-modules and let $f\colon P_1 \to P_2$ be a homomorphism of R-modules.
Show that f induces a homorphism of $R_{\mathfrak{p}}$-modules $f_{\mathfrak{p}}\colon (P_1)_{\mathfrak{p}} \to (P_2)_{\mathfrak{p}}$.
Deduce that the following diagram commutes

$$\begin{tikzcd}
\operatorname{Hom}_R(P_2,N)_{\mathfrak{p}} \arrow[r, "\operatorname{Hom}_R(f,N)_{\mathfrak{p}}"] \arrow[d, "\phi_{P_2,N}"] & \operatorname{Hom}_R(P_1,N)_{\mathfrak{p}} \arrow[d, "\phi_{P_1,N}"] \\
\operatorname{Hom}_{R_{\mathfrak{p}}}((P_2)_{\mathfrak{p}}, N_{\mathfrak{p}}) \arrow[r, "\operatorname{Hom}_{R_{\mathfrak{p}}}(f_{\mathfrak{p}},N_{\mathfrak{p}})"] & \operatorname{Hom}_{R_{\mathfrak{p}}}((P_1)_{\mathfrak{p}}, N_{\mathfrak{p}}),
\end{tikzcd}$$

where $\operatorname{Hom}_R(f,N)_{\mathfrak{p}}$ is the localization of the morphism $\operatorname{Hom}_R(f,N)$ at $\mathfrak{p}$. [5pt]

(5) Use $(2-4)$ to show that there exists an isomorphism

$$\psi\colon \operatorname{Ext}^i_R(M,N)_{\mathfrak{p}} \to \operatorname{Ext}^i_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, N_{\mathfrak{p}}).$$

[5pt]

Question C_1

(1) $T \subset R$ is multiplicatively closed if: • $1 \in T$ • If $t, t' \in T \Rightarrow tt' \in T$ — 2 pts

Either:

• $(T^{-1}R, i)$ is the R-algebra $i : R \to T^{-1}R$ defined by the following universal property:

• $\forall r \in T$ we have $i(r) \in (T^{-1}R)^*$

• If $R \xrightarrow{\varphi} S$ is a ring homomorphism s.t $\varphi(r) \in S^*$ for $\forall r \in T$ then there $\exists!$ ring homomorphism $T^{-1}R \xrightarrow{\tilde{\varphi}} S$ such that the following diagram commutes: — 4 pts

$$\begin{tikzcd} R \arrow[r, "i"] \arrow[dr, "\varphi"'] & T^{-1}R \arrow[d, "\tilde{\varphi}"] \\ & S \end{tikzcd}$$

Or:

Alternatively, give the construction, i.e., $T \times R/\sim$ where $(t,r) \sim (t',r') \Leftrightarrow \exists\, s \in T$ s.t $s(tr' - t'r) = 0$, multiplication: $(t,r)\cdot(t',r') := (tt', rr')$ and $+ : (t,r) + (t',r') := (tt', tr' + rt')$ — 3 pts

and $i : R \longrightarrow T^{-1}R$, $r \longmapsto (1,r)$ is R-algebra. — 1 pts

Total — 6 pts

Question C1

(2) $R_p = T^{-1}R$ for $T = R-p$ which is multiplicatively closed since $\cdot\ 1 \notin P$ $\cdot$ If $r \notin P$, $s \notin P$ $\Rightarrow rs \notin P$

1

• Suppose $i : R \to R_p$ is injective then $\forall\ r \neq 0 \in R$ $i(r) \neq i(0)$ i.e., for $\forall\ s \in R-p$ $sr \neq 0$ $\Rightarrow R-p$ contains no zero divisor.

2

• Conversely, suppose every zero-divisor of R $\subset p$ and let $i(r) = 0$ then $\exists\ s \in R-p$ s.t $sr = 0$ $\Rightarrow r = 0$ since s is <u>not</u> a zero-divisor.

Conclusion: $i : R \to R_p$ is injective if $R-P$ contains no zero divisor.

2

Total: 5

Question C_1

(3)
Let $x \neq 0 \in \sqrt{0}$, then $\mathrm{ann}(x) \neq 1$

in particular, there $\exists$ a maximal ideal m, s.t $\mathrm{ann}(x) \subset m$

Consider: $i: R \longrightarrow R_m$

we have $0 = i(x^n) = i(x)^n$

hence $i(x) \in \sqrt{0_{R_m}} \Rightarrow i(x) = 0$.

Therefore, there $\exists$ $s \in R - m$ s.t

$sx = 0 \Rightarrow s \in \mathrm{ann}(x) \subset m$.

This is a contradiction.

Total 7

Question C1

4) In this exercise you may choose to consider $S^{-1}M$ as a R-module or as a $S^{-1}R$ module as you wish since $\left(\frac{r}{s}\right)\left(\frac{m}{s'}\right) = \left(\frac{0}{1}\right) \Leftrightarrow \left(\frac{r}{1}\right)\left(\frac{m}{s'}\right) = \left(\frac{0}{1}\right)$. We describe the situation by a diagram:

$$\begin{tikzcd}
Tor(M) \subset M \arrow[rr, "\ell"] \arrow[drr, bend right, "\ell|_{Tor(M)}"'] & & S^{-1}(M) \\
& & S^{-1}Tor(M) \arrow[u, phantom, "\cup"]
\end{tikzcd}$$

$\ell|_{Tor(M)}$ = canonical morphism defined by localizing $Tor(M)$ at S.

We consider $S^{-1}M$ as a R-module and compare the R-submodules $Tor(S^{-1}M) \subset S^{-1}M$ and $S^{-1}Tor(M) \subset S^{-1}M$.

Let $\frac{m}{s} \in Tor(S^{-1}M)$; $\exists\, r \in R - \{0\}$ & $t \in S$ s.t $trm = 0$ since R is a domain and $t \neq 0 \Rightarrow rt \neq 0 \Rightarrow m \in Tor(M)$ $\Rightarrow \frac{m}{s} \in S^{-1}Tor(M)$. Conversely, let $\frac{m}{s} \in S^{-1}Tor(M)$ then $m \in Tor(M)$ and hence $\frac{m}{s} \in Tor(S^{-1}M)$. 7

Question C2

(1) $\mathrm{Ext}^i_R(M,N)$ is defined as follows:

Take a projective resolution $P^\cdot \to M$,

$$(*) \quad \cdots \xrightarrow{p_2} P_1 \xrightarrow{p_1} P_0 \to M \to 0$$

of M; i.e., each P_i is a projective module and the sequence $(*)$ is exact.

Apply the functor $\mathrm{Hom}_R(\ ,N)$ to the ~~complex~~ $P^\cdot$, i.e.,

$$\cdots \xrightarrow{p_2} P_1 \xrightarrow{p_1} P_0 \to 0$$

to get a complex, $\mathrm{Hom}_R(P^\cdot,N)$;

$$\cdots \xleftarrow{p_2^\vee} \mathrm{Hom}_R(P_1,N) \xleftarrow{p_1^\vee} \mathrm{Hom}_R(P_0,N) \leftarrow 0$$

$$\mathrm{Ext}^i_R(M,N) := \mathrm{Ker}(p_{i+1}^\vee)/\mathrm{Im}(p_i^\vee),$$

i.e., $\mathrm{Ext}^i_R(M,N) = H^i(\mathrm{Hom}_R(P^\cdot,N))$

Total

[redacted] 5

Question C2

(2) In the first step we find a surjection from a free R-module $\bigoplus_{i\in I_0} R \xrightarrow{f_0} M$, this is always possible, take $I = M$ and $f_0(e_m) = m$.

$\ker f_0 \subset \bigoplus_{i\in I_0} R$ is a R-module, so we repeat the procedure, $\bigoplus_{i\in I_1} R \xrightarrow{f_1} \ker f_0$, we get:

$$\begin{tikzcd}
 & & \ker f_1 \arrow[dr, hook] & & \ker f_0 \arrow[dr, hook] & & \\
\arrow[r] & \bigoplus_{i\in I_2} R \arrow[ur, two heads] \arrow[rr, "f_2"] & & \bigoplus_{i\in I_1} R \arrow[ur, two heads] \arrow[rr, "f_1"] & & \bigoplus_{i\in I_0} R \arrow[r, two heads, "f_0"] & M
\end{tikzcd}$$

- If M is Noetherian $\Rightarrow$ M f.g, hence we may take $|I_0| < \infty$, $\ker f_0 \subset R^{I_0}$ and R-Noetherian, $|I_0| < \infty \Rightarrow R^{I_0}$ Noetherian, hence we can take $|I_1| < \infty$ and so on...

Total 5

Question C2

(3) By the universal property of free modules there is a R-module isomorphism:

$$\mathrm{Hom}_R\Big(\bigoplus_{i\in I} R, N\Big) \cong N^I$$
$$f \longmapsto (f(e_i))_{i\in I}$$

By the additivity of localization

$$\Big(\bigoplus_{i\in I} R\Big)_p = \bigoplus_{i\in I} R_p$$

Hence $$\mathrm{Hom}_{R_p}\Big(\big(\bigoplus_{i\in I} R\big)_p, N_p\Big) \cong (N_p)^I$$

Since $|I|<\infty$ direct product = direct sum and therefore, again by additivity of localization: $(N^I)_p = N_p{}^I$

Total points 5

Question C2 (4)

The morphism $f_p : P_{1p} \to P_{2p}$ exist by the functoriality of localization.

Let $|I_1|, |I_2| < \infty$, and:

$P_1 = \bigoplus_{i \in I_1} R \quad P_2 = \bigoplus_{i \in I_2} R$, we

unravel the diagram:

$$(\ell)_p \longmapsto (\ell \circ f)_p$$

$$\begin{tikzcd}
\mathrm{Hom}_R\left(\bigoplus_{i\in I_2} R, N\right)_p \arrow[r] \arrow[d, "\wr"] & \mathrm{Hom}_R\left(\bigoplus_{i\in I_1} R, N\right)_p \arrow[d, "\wr"] \\
(N^{I_2})_p \arrow[r] \arrow[d, "\wr"] & (N^{I_1})_p \arrow[d, "\wr"] \\
(N_p)^{I_2} \arrow[r] \arrow[d, "\wr"] & N_p^{I_1} \arrow[d, "\wr"] \\
\mathrm{Hom}_{R_p}\left(\bigoplus_{i\in I_2} R_p, N_p\right) \arrow[r, "\ell_p \circ f_p"] & \mathrm{Hom}_{R_p}\left(\bigoplus_{i\in I_1} R_p, N_p\right)
\end{tikzcd}$$

$(\ell)_p \updownarrow ((\ell(e_i))_{i\in I_2})_p \longmapsto (\ell \circ f(e_i))_{p,\, i \in I_1} \updownarrow$

$(\ell(e_i)_p)_{i \in I_2} \longmapsto (\ell \circ f(e_i)_p)_{i \in I_1}$

$$\ell_p \longmapsto \ell_p \circ f_p$$

The commutativity, is therefore clear.

$\boxed{\text{Total } 5\text{pts}}$

Question C2

Total points 5pts

(5) Let $P^\cdot \to M$ be a free resolution, since we assumed P to be f.g in (3) we assume M to be Noetherian R to be Noetherian ring.

i.e., each $P_i \in P^\cdot$ can be assumed to be finitely generated.

Since localization is an additative and exact functor:

$(P^\cdot)_p \to M_p$ is a free resolution.

Therefore, $\mathrm{Ext}^i_R(M,N)_p = H^i(P^\cdot, N)_p$

and $\mathrm{Ext}^i_{R_p}(M_p, N_p) = H^i(P^\cdot_p, N_p)$,

since by (4) the diagram below commutes

$$\begin{tikzcd}
{} \arrow[r] & \mathrm{Hom}_R(P_{i-1}, N)_p \arrow[r, "(f^\vee)_p"] \arrow[d, "\simeq"'] & \mathrm{Hom}_R(P_i, N)_p \arrow[r] \arrow[d, "\simeq"] & {} \\
{} \arrow[r] & \mathrm{Hom}_R((P_{i-1})_p, N_p) \arrow[r, "(f_p)^\vee"] & \mathrm{Hom}_{R_p}((P_i)_p, N_p) \arrow[r] & {}
\end{tikzcd}$$

this induces isom. on cohomology.