Algebra IV - Rings and modules (MATH-311) — Final exam

25 January 2024, 9 h 15 – 12 h 15

Nom : Alexander Grothendieck

SCIPER : 42

Signature : _____

Numéro

1

Paper & pen: This booklet contains 6 exercises, on 33 pages, for a total of 100 points. Please use the space with the square grid for your answers. **Do not** write on the margins. Write all your solutions under the corresponding exercise, except if you run out of space at a given exercise. In that case, continue with your solution at the empty space left after your solution for another exercise. In this case, mark clearly where the continuation of your solution is. If even this way the booklet is not enough, then ask for additional papers from the proctors. Write your name and the exercise number clearly on the top right corner of the additional paper. At the end of your exam put the additional papers into the exam booklet under the supervision of a proctor, and sign on to the number of additional papers on the proctor's form. We provide scratch paper. You are not allowed to use your own scratch paper. Please write with a pen, NOT with a pencil.

Duration of the exam: It is not allowed to read the inside of the booklet before the exam starts. The length of the exam is 180 minutes. If you did not leave until the final 20 minutes, then please stay seated until the end of the exam, even if you finish your exam during these 20 minutes. The exams are collected by the proctors at the end of the exam, during which please remain seated.

Cheat sheet: You can use a cheat sheet, that is, two sides of an A4 paper handwritten by yourself. At the end, we collect the cheat sheets.

CAMIPRO & coats: Please prepare your CAMIPRO card on your table. Your bag and coat should be placed close to the walls of the room, NOT in the vicinity of your seat.

Results of the course: You can use all results seen during the lectures or in the exercise sessions (that is, all results in the lectures notes or on the exercise sheets), except if the given question asks exactly that result or a special case of it. If you are using such a result, please state explicitly what you are using, and why the assumptions are satisfied.

Separate points can be solved separately: You get maximum credit for solving any point of an exercise assuming the statements of the previous points, even if you did not solve (all of) those previous points.

Assumptions: all rings are with identity.

Question:	1	2	3	4	5	6	Total
Points:	16	16	18	18	18	14	100
Score:							

Exercise 1 [**16 pts**]

Consider the proof of Hilbert's basis theorem, where we proved that if a commutative ring R is Noetherian, then so is $R[x]$. We fixed an arbitrary ideal $I \subseteq R[x]$ and we wanted to show that I is finitely generated. We chose a finite generator set of the ideal

$$I_{\text{in}} = \left\{ \; a_n \in R \;\middle|\; \sum_{i=0}^{n} a_i x^i \in I \text{ such that } a_n \neq 0 \; \right\}$$

of R. We chose then $f_1, \ldots, f_r \in I$ such that their leading coefficients yielded exactly the above generator set, and such that their degrees were the same, say d. Then we also chose a generator set $f_{r+1}, \ldots, f_s$ for the R-module

$$\left\{ \; f \in I \;\middle|\; \deg f < d \; \right\}$$

Show that $f_1, \ldots, f_s$ generate I as an ideal of $R[x]$.

Solution:

Let $g \in I$, and let us show that g is generated by $f_1, \ldots, f_s$.

We show this by induction on the degree l of g. (**2 points**) If $l < d$, the result holds by definition of $f_{r+1}, \ldots, f_s$ (**3 points**). Hence, let us assume that $l \geqslant d$, and that we know the results for polynomials of degree smaller than d.

Let b be the leading coefficient of g. By definition of $f_1, \ldots, f_r$, if $a_{d,j}$ denotes the leading coefficient of f_j (with $1 \leqslant j \leqslant r$), then there exists $(\lambda_j)_{1 \leqslant j \leqslant r}$ such that

$$b = \sum_{j=1}^{r} \lambda_j a_{j,d}.$$

(**5 points**). In particular,

$$g' := g - \sum_{j=1}^{r} \lambda_j x^{l-d} f_j$$

has degree smaller than $l = \deg(g)$. Since $g \in I$ and each $f_j \in I$, also $g' \in I$. By the induction hypothesis, we deduce that $g' \in (f_1, \ldots, f_s)$. Since $g - g' \in (f_1, \ldots, f_s)$ by construction, we conclude that $g \in (f_1, \ldots, f_s)$. (**6 points**).

Exercise 2 [**16 pts**]

Let

$$0 \longrightarrow E^\bullet \xrightarrow{\alpha^\bullet} F^\bullet \xrightarrow{\beta^\bullet} G^\bullet \longrightarrow 0$$

be a short exact sequence of co-chain complexes, that is, $\alpha^\bullet$ and $\beta^\bullet$ are co-chain morphisms such that

$$0 \longrightarrow E^i \xrightarrow{\alpha^i} F^i \xrightarrow{\beta^i} G^i \longrightarrow 0$$

is exact for every $i \in \mathbb{Z}$. Let $e^i : E^i \to E^{i+1}$, $f^i : F^i \to F^{i+1}$ and $g^i : G^i \to G^{i+1}$ be the structure homomorphisms of $E^\bullet$, $F^\bullet$ and $G^\bullet$, respectively.

Show that the following sequence is exact for any $i \in \mathbb{Z}$:

$$H^i(E^\bullet) \xrightarrow{H^i(\alpha^\bullet)} H^i(F^\bullet) \xrightarrow{H^i(\beta^\bullet)} H^i(G^\bullet) \tag{1}$$

[*Remark: you can use without proof that H^i is functorial, that is, that $H^i(\beta^\bullet \circ \alpha^\bullet) = H^i(\beta^\bullet) \circ H^i(\alpha^\bullet)$.*]

Solution:

Throughout, the image of an element a in some quotient is denoted $\overline{a}$.

Fix some $i \in \mathbb{Z}$. Since H^i is functorial, we know that

$$H^i(\beta^\bullet) \circ H^i(\alpha^\bullet) = H^i(\beta^\bullet \circ \alpha^\bullet) = H^i(0) = 0,$$

where the second equality holds by definition of a cochain complex. Hence,

$$\mathrm{im}(H^i(\alpha^\bullet)) \subseteq \ker(H^i(\beta^\bullet)).$$

(3 points)

To conclude the exercise, let us show the other inclusion, so let $\overline{y} \in \ker(H^i(\beta^\bullet))$, with $y \in \ker(\beta^i)$. Then we obtain that $\beta^i(y) = g^i(z)$ for some $z \in G^{i-1}$ (**1 point**). By exactness, β^{i-1} is surjective, so there exists $y' \in F^{i-1}$ such that $\beta^{i-1}(y') = z$. (**2 points**) Since the diagram

$$\begin{array}{ccc} F^{i-1} & \xrightarrow{\beta^{i-1}} & G^{i-1} \\ {\scriptstyle f^{i-1}}\downarrow & & \downarrow{\scriptstyle g^{i-1}} \\ F^i & \xrightarrow[\beta^i]{} & G^i \end{array}$$

commutes, we know that $\beta^i(f^{i-1}(y')) = g^{i-1}(z) = \beta^i(y)$, so $y - f^{i-1}(y') \in \ker(\beta^i)$. (**3 points**) By exactness, there exists $x \in E^i$ such that $\alpha^i(x) = y - f^{i-1}(y')$. (**1 point**) Since the diagram

$$\begin{array}{ccc} E^i & \xrightarrow{\alpha^i} & F^i \\ {\scriptstyle e^i}\downarrow & & \downarrow{\scriptstyle f^i} \\ E^{i+1} & \xrightarrow[\alpha^{i+1}]{} & F^{i+1} \end{array}$$

commutes and $f^i(y - f^{i-1}(y')) = 0$, then $\alpha^{i+1}(e^i(x)) = 0$. Since α^{i+1} is injective by assumption, we deduce that $e^i(x) = 0$. In other words, $x \in \ker(e^i)$, so we can consider $\overline{x} \in H^i(E^\bullet)$. (**4 points**) Since $\alpha^i(x) = y - f^{i-1}(y')$, we conclude that by definition,

$$\overline{y} = H^i(\alpha^\bullet)(\overline{x}) + \overline{f^{i-1}(y')} = H^i(\alpha^\bullet)(\overline{x}) \in \mathrm{im}(H^i(\alpha^\bullet)),$$

where the second equality holds by definition of $H^i(F^\bullet)$. Hence, $\ker(H^i(\beta^\bullet)) = \mathrm{im}(H^i(\alpha^\bullet))$, which is exactly what we had to prove. (**2 points**)

Exercise 3 [**18 pts**]

(1) Show that if $0 \neq f \in \mathbb{R}[x]$ is an irreducible element, then either

- $f = x - c$ for some $c \in \mathbb{R}$, or
- $f = (x-c)^2 + a$ for some $a, c \in \mathbb{R}$ with $a > 0$.

(2) Show that up to isomorphisms of rings, there are three (non-isomorphic) possibilities for $\mathbb{R}[x]_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime ideal of $\mathbb{R}[x]$.

Solution:

(1) Note that if $z \in \mathbb{C}$ is a root of f, then so is its conjugate $\overline{z}$, since f has real coefficients. Since $\mathbb{C}$ is algrebaically closed, we can write

$$f = \prod_i (x - c_i) \prod_j (x - d_j)(x - \overline{d_j}),$$

where the c_i's are real numbers, and the d_j are complex numbers. Since each $(x-d_j)(x-\overline{d_j})$ is a real polynomial of degree 2 and f is irreducible, we conclude that $\deg(f) \in \{1, 2\}$. (**2 points**)

- If f has degree 1, then $f = x - c$ for some $c \in \mathbb{R}$.
- If f has degree 2, let us write $f = x^2 + bx + c$. Then we have

$$f = \left(x - \frac{-b}{2}\right)^2 - \left(c - \frac{b^2}{4}\right).$$

Let $b' := \frac{-b}{2}$ and $c' := c - \frac{b^2}{4}$. Then $f = (x-b')^2 + c'$. Since f is irreducible, it cannot have any root. This immediately shows that $c' > 0$ (any positive number has a square root over the real numbers). (**2 points**)

(2) Let $\mathfrak{p}$ be a prime ideal. Since $\mathbb{R}[x]$ is a PID, $\mathfrak{p}$ is generated by a monic irreducible element, say f. (**1 point**)

If $f = 0$, then by definition $\mathbb{R}[x]_{\mathfrak{p}} = \mathbb{R}(x)$, which is a field. On the other hand, if $f \neq 0$ (and hence, we know by the first point that f has degree 1 or 2), then we know from the course (more precisely, the correspondence between prime ideals in a localization and prime ideals of the ring avoiding the elements we give inverses to) that $f\mathbb{R}[x]_{(f)}$ is a non-trivial (maximal) ideal of $\mathbb{R}[x]_{(f)}$. In particular, $\mathbb{R}[x]_{(f)} \ncong \mathbb{R}(x)$ since it is not a field. (**2 points**)

Assume that $\deg(f) = 1$, i.e. $f = x - c$. Let us show that $\mathbb{R}[x]_{(f)} \cong \mathbb{R}[x]_{(x)}$. Consider the isomorphism $\mathbb{R}[x] \to \mathbb{R}[x]$ given by sending x to $x - c$ (its inverse is given by $x \mapsto x + c$). Then the image of the prime ideal (x) is $(x - c)$, so our isomorphism induces an isomorphism

$$\mathbb{R}[x]_{(x)} \cong \mathbb{R}[x]_{(x-c)}.$$

(**2 points**)

Assume that $\deg(f) = 2$, i.e. $f = (x-c)^2 + a$ with $a > 0$, and let us show that $\mathbb{R}[x]_{(f)} \cong \mathbb{R}[x]_{(x^2+1)}$. Again, consider the isomorphism $\psi\colon \mathbb{R}[x] \to \mathbb{R}[x]$ given by sending x to $\sqrt{a}(x + c)$ (its inverse is given by $x \mapsto \frac{x}{\sqrt{a}} - c$). Then the image of f is exactly $a(x^2+1)$, so $\psi((f)) = (a(x^2+1)) = (x^2+1)$. Thus, ψ indeed induces an isomorphism $\mathbb{R}[x]_{(f)} \cong \mathbb{R}[x]_{(x^2+1)}$. (**4 points**)

To conclude the exercise, we are left to show that $\mathbb{R}[x]_{(x)} \ncong \mathbb{R}[x]_{(x^2+1)}$. Assume by contradiction that they were isomorphic, and let $\mathfrak{m}_1$ (resp. $\mathfrak{m}_2$) denote unique the maximal ideal of $\mathbb{R}[x]_{(x)}$ (resp. $\mathbb{R}[x]_{(x^2+1)}$)). Since an isomorphism must preserve maximal ideals, we would conclude that also

$$\mathbb{R}[x]_{(x)} \Big/ \mathfrak{m}_1 \cong \mathbb{R}[x]_{(x)} \Big/ \mathfrak{m}_2.$$

We will show that $\mathbb{R}[x]_{(x)} \Big/ \mathfrak{m}_1 \cong \mathbb{R}$, while $\mathbb{R}[x]_{(x)} \Big/ \mathfrak{m}_2 \cong \mathbb{C}$, which immediately concludes since $\mathbb{R} \ncong \mathbb{C}$ (one is algebraically closed, and the other is not).

- *Proof that* $\mathbb{R}[x]_{(x)} \Big/ \mathfrak{m}_1 \cong \mathbb{R}$*:*

  As we already said, $\mathfrak{m}_1 = x\mathbb{R}[x]_{(x)}$. We know by Exercise 6.4 of sheet 11 that

  $$\mathbb{R}[x]_{(x)} \Big/ x\mathbb{R}[x]_{(x)} \cong \mathrm{Frac}\left(\mathbb{R}[x] \Big/ x\mathbb{R}[x]\right) \cong \mathrm{Frac}(\mathbb{R}) \cong \mathbb{R}.$$

- *Proof that* $\mathbb{R}[x]_{(x^2+1)} \Big/ \mathfrak{m}_1 \cong \mathbb{C}$*:*

  As before, $\mathfrak{m}_2 = (x^2+1)\mathbb{R}[x]_{(x^2+1)}$, so

  $$\mathbb{R}[x]_{(x^2+1)} \Big/ (x^2+1)\mathbb{R}[x]_{(x^2+1)} \cong \mathrm{Frac}\left(\mathbb{R}[x] \Big/ (x^2+1)\mathbb{R}[x]\right) \cong \mathrm{Frac}(\mathbb{C}) \cong \mathbb{C}.$$

(**5 points**)

Exercise 4 [**18 pts**]

Consider the following situation:

- k *is an algebraically closed field,*
- $a, b \in k$ *are arbitrary elements,*
- $R = k[x, y]$*,*
- M *is the* R*-module* $R/(x, y)$*,*
- L *is the* R*-module* $R/(x - a, y - b)$*,*
- Q *is an arbitrary finite length* R*-module.*

(1) Compute $\mathrm{Tor}_i^R(L, M)$ for an arbitrary $i \in \mathbb{Z}$. Your answer should depend on the value of $(a, b) \in k^2$.

(2) Show that $\mathrm{Tor}_i^R(Q, M)$ is of finite length over R.

Solution:

(1) As we have seen in Example 5.3.9 in the lecture notes, a free resolution of L is given by

$$R \xrightarrow{\cdot((y-b),-(x-a))} R^{\oplus 2} \xrightarrow{\cdot(x-a)+\cdot(y-b)} R$$

where the morphism $R \to L$ is the quotient map, the first map sends r to $(r(y-b), -(x-a))$ and the second map sends (f, g) to $(x - a)f + (y - b)g$. (**2 points**)

Tensoring by M gives the sequence

$$M \xrightarrow{\cdot((y-b),-(x-a))} M^{\oplus 2} \xrightarrow{\cdot(x-a)+\cdot(y-b)} M.$$

(**1 point**)

Since x and y act as 0 on M, this sequence is exactly

$$M \xrightarrow{\cdot(-b,a)} M^{\oplus 2} \xrightarrow{\cdot(-a)+\cdot(b)} M.$$

If $a = b = 0$, then we immediately obtain that

$$\begin{cases} \mathrm{Tor}_0^R(L, M) = M; \\ \mathrm{Tor}_1^R(L, M) = M^{\oplus 2}; \\ \mathrm{Tor}_2^R(L, M) = M. \end{cases}$$

(**2 points**)

Now, assume that $(a, b) \neq (0, 0)$. By the same argument as in Exercise 7.4 of sheet 4, we know that $\mathrm{Tor}_i(\cdot f, M) = \cdot f$ for any $f \in R$. From this we see that $\mathrm{Tor}_i^R(L, M)$ is $(x - a)$ and $(y - b)$-torsion. Since it is a subquotient of $M^{\oplus i}$ is it also x and y-torsion, so $\mathrm{Ann}(\mathrm{Tor}_i^R(L, M)) \supseteq (x - a, y - b, x, y)$. Since $(a, b) \neq (0, 0)$, this ideal is the while ring R, meaning that $\mathrm{Tor}_i^R(L, M) = 0$ for every $i \geqslant 0$.

(**3 points**)

(2) We show this by induction on the length of Q. If Q has length 0, then $Q = 0$ and the statement is immediate. (**1 point**)

If Q has length 1, this means that it is a simple R-module. Let $a \in Q$ be any element. Then Q is generated by a, to there exists as isomorphism $Q \cong R/I$ for some ideal I. Since Q is simple, we deduce from the correspondence theorem that I is a maximal ideal. It must then be of them form $(x-a, y-b)$ for some $a, b \in R$ by the Nullstellensatz. The result then follows from the previous point. (**4 points**)

Finally, assume that Q has length at least 2, and consider a short exact sequence

$$0 \to Q' \to Q \to L \to 0,$$

where L is simple (this exists by definition of finite length module).

By the induced long exact sequence in homology, we have exact sequences

$$\cdots \to \mathrm{Tor}_i^R(Q', M) \to \mathrm{Tor}_i^R(Q, M) \to \mathrm{Tor}_i^R(L, M) \to \dots.$$

In particular, for each $i \geqslant 0$, we have an exact sequence

$$0 \to A \to \mathrm{Tor}_i^R(Q, M) \to B \to 0,$$

where A is a quotient of $\mathrm{Tor}_i^R(Q', M)$ and B is a submodule of $\mathrm{Tor}_i^R(L, M)$. Since these two Tor_i-modules are finite length by the induction hypothesis and our work before, both A and B also have finite length. Thus, $\mathrm{Tor}_i^R(L, M)$ also has finite length. (**5 points**)

Exercise 5 [**18 pts**]

Consider the following situation:

- k *is a field,*
- $R = k[x,y]\Big/(xy)$,
- *for* $a, b \in k$ *such that* $(a,b) \neq (0,0)$*, let* $\eta_{a,b} : k[t] \to R$ *be the* k*-algebra homomorphism given by* $t \mapsto ax + by$ *(where* $ax + by$ *denotes the element* $ax + by + (xy) \in R$*).*

Without proof you can admit that $\eta_{a,b}$ *is injective (for example, it is easy to see that the elements* $(ax + by)^i \in R$ *are* k*-linearly independent).*

Show that $\eta_{a,b}$ yields an integral extension if and only if $a \neq 0$ and $b \neq 0$.

Solution:

Assume first that $a \neq 0$ and $b \neq 0$, and let us show that $\eta_{a,b}$ is an integral extension.

Since R is generated by x and y as a $k[t]$-algebra (even as a k-algebra), it is enough to show that both x and y are integral over $k[t]$. (**3 points**) By symmetry, we only show that x is integral over $k[t]$. For example, a monic equation that x satisfies over $k[t]$ is

$$x^2 - \frac{x}{a}\eta_{a,b}(t) = x^2 - \frac{x}{a}(ax + by) = 0.$$

(**6 points**)

Now, assume that $\eta_{a,b}$ is an integral extension, and let us show that both $a \neq 0$ and $b \neq 0$. Again by symmetry, we will only show that $a \neq 0$, so let assume by contradiction that $a = 0$. By assumption, there exists an equation of the form

$$x^n = \sum_{i=0}^{n-1} x^i \eta_{a,b}(f_i)$$

for some $f_i \in k[t]$. In other words, we have that

$$x^n = \sum_{i=0}^{n-1} x^i f_i(by) \mod xy.$$

Evaluating y at 0 (which we can do modulo xy, since y divides xy) shows that as polynomials in $k[x]$, we have

$$x^n = \sum_{i=0}^{n-1} x^i f_i(0).$$

Since the elements $f_i(0)$ are constants, this is impossible. (**9 points**)

Exercise 6 [**14 pts**]

Consider $R = \mathrm{Mat}(3, \mathbb{C})$ *and the subring*

$$S = \left\{ \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \in R \;\middle|\; a, b, c, d, e, f \in \mathbb{C} \right\} \subseteq R$$

You do not have to show that S *is a subring of* R*. Let* $M = \mathbb{C}^3$ *be the* 3*-dimensional complex vectorspace, the elements of which we regard as column vectors. Then multiplication on the left turns* M *into a (left) module both over* S *and* R*. That is, the module structures are given by the multiplication* $A \cdot v = Av$ *for every* $A \in R$ *or* $A \in S$ *and for every* $v \in M$ *(you do not have to verify this).*

Note that scalar multiples of the identity matrix give $\mathbb{C}$ *as a subring of both* S *and* R*. Hence every* R *and* S *module is also automatically a* $\mathbb{C}$*-vectorspace.*

(1) Show that every non-zero S-submodule $N \subseteq M$ contains the S-submodule

$$M_1 = \left\{ \begin{pmatrix} a \\ 0 \\ 0 \end{pmatrix} \;\middle|\; a \in \mathbb{C} \right\}$$

(You do not have to verify that M_1 is an S-submodule)

(2) Conclude that M is not a semi-simple S-module.

(3) Show that M is a simple R-module.

Solution:

(1) Let $a \in \mathbb{C}$. By assumption, there is a non-zero vector

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

in N. We will work case by case.

If $x \neq 0$, then we are done since

$$N \ni \begin{pmatrix} \frac{a}{x} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a \\ 0 \\ 0 \end{pmatrix}.$$

If $y \neq 0$, then we are done since

$$N \ni \begin{pmatrix} 0 & \frac{a}{y} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a \\ 0 \\ 0 \end{pmatrix}.$$

If $z \neq 0$, then we are done since

$$N \ni \begin{pmatrix} 0 & 0 & \frac{a}{z} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a \\ 0 \\ 0 \end{pmatrix}.$$

(**6 points**)

(2) If by contradiction M was a semi-simple S-module, then we could write it as $M = N_1 \oplus \cdots \oplus N_r$ for some non-zero simple S-submodules N_i. Since for all i,

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \in N_i$$

by the first point, we deduce that necessarily, $r = 1$. (**2 points**) But then, this would mean that M is a simple S-module, which cannot be true since $M_1 \subseteq M$ is a non-zero proper S-submodule. (**2 points**)

(3) Let $N \subseteq M$ be a non-zero R-submodule. Our goal is to show that $N = M$. Since it is also an S-submodule (recall that $S \subseteq R$), we know by the first point that

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \in N.$$

Now, let

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} \in M$$

be any element. Then

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} a & 0 & 0 \\ b & 0 & 0 \\ c & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \in N.$$

Thus, $N = M$, whence M is indeed simple as an R-module. (**4 points**)