EPFL - Fall 2023 | Prof. Zs. Patakfalvi
Rings and modules | **Exercises**
Sheet 1 - Solutions

Exercise 1. Answer the following questions. Provide an explanation by a proof or a counterexample.

(1) Suppose that R is a Noetherian ring. Let $S \subset R$ be a subring. Is it true that S is Noetherian?
(2) Let R be a commutative Artinian ring. Is every prime ideal of R maximal?

Proof. (1) It is not necessarily true that S is Noetherian. A counterexample is given by an inclusion of any non-Noetherian integral domain (e.g., $k[x_1, x_2, \ldots]$) into its fraction field (clearly Noetherian).

(2) Let $\mathfrak{p}$ be a prime ideal of R. Since there exists a correspondence between ideals in $R/\mathfrak{p}$ and ideals in R containing $\mathfrak{p}$, we know that $R/\mathfrak{p}$ is an Artinian integral domain. Let $x \in R/\mathfrak{p}$ be a non-zero element. The sequence of ideals $((x^n))_{n\geq 0}$ is decreasing and hence by Artinianity it stabilizes, which means that $x^n = ux^{n+1}$ for some $u \in R/\mathfrak{p}$ and $n \in \mathbb{N}$. Since $R/\mathfrak{p}$ is a domain, and we have $x^n(1-ux) = 0$ and thus $ux = 1$, which proves that x is invertible. So every non-zero element of $R/\mathfrak{p}$ is invertible, and thus $R/\mathfrak{p}$ is a field. Therefore $\mathfrak{p}$ is maximal inside R.

□

Exercise 2. (1) A simple module is a module that has only trivial submodules. Show that any simple module is cyclic.

(2) Let $m \in M$ be an element. We define the annihilator of m by

$$\mathrm{Ann}_R(m) = \{\, r \in R \mid rm = 0 \,\}$$

We only write $\mathrm{Ann}(m)$ if it the base ring is clear from the context.

Show that $\mathrm{Ann}(m)$ is a left ideal of R and that the cyclic module Rm is isomorphic to the module $R/\mathrm{Ann}(m)$.

(3) Let M be a simple $k[x]$-module. Prove that $M \cong k[x]/(f)$ where f is an irreducible polynomial in $k[x]$ and (f) denotes the ideal generated by f.

(4) Which of the following $\mathbb{Z}$-modules are simple?
   (a) $\mathbb{Z}$
   (b) $\mathbb{Z}/6\mathbb{Z}$
   (c) $\mathbb{Z}/7\mathbb{Z}$

Proof. (1) If $M = 0$ then $M = R \cdot 0$ and the assertion is true. Otherwise let $m \in M \setminus \{0\}$. Then Rm is a left submodule of M. Since $Rm \neq 0$ and M is simple we conclude that $Rm = M$.

(2) We define a homomorphism of left R-modulues $\Phi_m : {}_R R \to Rm$ by $\Phi_m(r) = rm$. The kernel of Φ_m is by definition the set of elements $r \in R$ such that $rm = 0$, i.e., $\ker(\Phi_m) = \mathrm{Ann}(m)$. This proves that $\mathrm{Ann}(m)$ is a left ideal of R and that $Rm \cong R/\mathrm{Ann}(m)$.

(3) By (1) and (2), M is isomorphic to $k[x]/\mathrm{Ann}(m)$ for some $m \in M$. Let $\mathrm{Ann}(m) = (f)$ for some $f \in k[x]$ (recall that $k[x]$ is a PID); we need to prove that f is irreducible. To this end let g divide f, then $k[x] \cdot (g + (f))$ is a left $k[x]$-submodule of $k[x]/(f)$.

Since by assumption $M \cong k[x]/(f)$ is simple we must have that $k[x] \cdot (g + (f)) = 0$ or $k[x] \cdot (g + (f)) = k[x]/(f)$, which implies that either f divides g or $(f, g) = (1)$. As g divides f, this means that either $g = f$ or $g = 1$ (up to multiplication by a unit). Thus f is irreducible.

(4) Notice that the $\mathbb{Z}$-submodules of $\mathbb{Z}/n\mathbb{Z}$ are exactly the ideals of $\mathbb{Z}/n\mathbb{Z}$ seen as a ring. Hence $\mathbb{Z}/n\mathbb{Z}$ is a simple $\mathbb{Z}$-module if and only if it has no non-zero proper ideals. As you know a commutative ring has no non-zero proper ideals if and only if it is a field, in particular only (c) gives a simple $\mathbb{Z}$-module.

□

Exercise 3. Let R be a ring, M a left R-module and $m \in M$.

(1) In the previous exercise you proved that $\mathrm{Ann}(m)$ is a left ideal of R. Give an example to show that $\mathrm{Ann}(m)$ might *not* be a two sided ideal of R.

(2) Define the *annihilator* of M to be

$$\mathrm{Ann}_R(M) = \{ r \in R \mid rM = 0 \} = \{ r \in R \mid \forall m \in M : rm = 0 \}$$

Prove that $\mathrm{Ann}(M)$ is a two sided ideal of R.

(3) Let $\phi : S \to R$ be a surjective homomorphism of rings and M a module over S. Show that we can endow an R-module structure given by $r \cdot m = s \cdot m$ for any $s \in \phi^{-1}(r)$ and $m \in M$ if and only if $\ker \phi \subseteq \mathrm{Ann}(M)$.

(4) For example, let $S = k[x]$ and $M = k[x]$ (with the standard action). Then M/f^2M is a $k[x]/(f^2)$-module for any $0 \neq f \in k[x]$. In addition, if f is not invertible, then M/f^2M is not a $k[x]/(f)$-module.

Proof. (1) We need to consider a non-commutative ring R to create an example, since left and right ideals coincide in commutative rings. The first example of a non-commutative ring R that comes to mind will suffice. That is, let R be the ring of 2×2 matrices over some field k. To keep things as simple as possible we consider R as a left R-module by left multiplication. Let $0 \neq a \in k$, we will calculate the annihilator of $m_a = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}$. Hence we are interested in solving the matrix equation

$$\begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \cdot \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

The solutions are exactly the matrices with $b_{11} = b_{21} = 0$, and thus $\mathrm{Ann}(m_a) = \left\{ \begin{bmatrix} 0 & b \\ 0 & c \end{bmatrix} \mid b, c \in k \right\}$. This is not a right ideal of R because multiplying such an element from the right with an arbitrary matrix in R does in general not give a matrix of this form. For example multiplication from the right with $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ gives b in the top left corner of the matrix, so this top left entry is non-zero whenever b is.

(2) Let $r, s \in \mathrm{Ann}(M)$ and $l \in R$. Then $l(r + s)m = l(rm + sm) = 0$ and $(r + s)lm = r(lm) + s(lm) = 0$.

(3) Assume first $\ker(\phi) \subseteq \mathrm{Ann}(M)$, and let $r \in R$, $m \in M$ and s, $s' \in \phi^{-1}(r)$. Then $s - s' \in \ker(\phi)$, so by assumption

$$0 = (s - s')m = sm - s'm$$

so that $sm = s'm$. Thus, at least the map $R \times M \to M$ sending $(r, m) \to r \cdot m$ is well-defined. The module axioms are then straight-forward to see (one could also argue as in the proof of Exercice 3.2) Now assume that the action is well defined. Then in particular for any $s \in \ker(\phi) = \phi^{-1}(0)$ and $m \in M$,

$$sm = 0$$

In other words $\ker(\phi) \subseteq \mathrm{Ann}(M)$.

(4) Clearly, $f^2 \in \mathrm{Ann}(M/f^2M)$, so by the previous point we get that M/f^2M is an $k[x]/(f^2)$-module via the above procedure.

Assume now that $f \neq 0$ is not invertible, and assume by contradiction that M/f^2M in an $R/(f)$-module via the above procedure. Then by the previous point, $f \in \mathrm{Ann}(M/f^2M)$, so in particular

$$f = f \cdot 1 \in f^2M = f^2k[x]$$

so there exists $c \in k[x]$ such that $cf^2 = f$. Since R is a domain, we get

$$cf = 1$$

which contradicts the fact that f is not invertible.

□

Exercise 4. Let $I \subseteq R$ be an ideal.

(1) Show that

$$IM = \left\{ \sum_{i=1}^{d} r_i m_i \;\middle|\; 1 \leq d \in \mathbb{Z},\ r_i \in I,\ m_i \in M \right\}$$

is an R-submodule of M.

(2) Show that M/IM is an R/I-module with scalar multiplication given by

$$(x + I)(y + IM) = xy + IM.$$

From now, let $R = k[x, y]$, let M be the R-submodule generated by the element $(x, y) \in R \oplus R = N$, and let I be the maximal ideal $I = Rx + Ry$ of R. Note that $R/I \cong k$ via the homomorphism $R \to k$ that evaluates x and y to 0.

(3) Show that $M \subseteq IN$ and hence $I(N/M) = IN/M$ as R-submodules of N/M.

(4) Show that L/IL is a two dimensional vector-space over k, where $L = N/M$

[Hint: use point (3) and the third isomorphism theorem]

Now, we change a little bit our setup, and we redefine M:

(5) Let M be the submodule generated by the two elements $(x, 0)$ and $(0, y)$ of $R \oplus R = N$. Is $N/M \cong R$?

[Hint: look at $\mathrm{Ann}(N/M)$.]

Proof. (1) We need to prove that IM is an additive subgroup and that it is stable under multiplication by elements of R. By comparing definitions (i.e. that of IM above and that of a subgroup generated by a subset), IM is in fact the subgroup of M generated

by the set $\{rm \mid r \in I,\ m \in M\}$, so IM is an additive subgroup of M. On the other hand, we have for all $r \in R$ that

$$r \cdot (IM) = \left\{ \sum_{i=1}^{d} \underbrace{r r_i}_{\in I} m_i \;\middle|\; 1 \leq d \in \mathbb{Z},\ r_i \in I,\ m_i \in M \right\} \subseteq IM$$

as I is a left ideal. Thus $IM \leq_R M$.

(2) One can prove this by simple (but tedious) verification of well-definedness and of all the axioms. But let us give a more conceptual proof. An abelian group M has a left R-module structure if and only if we have a ring morphism $\lambda : R \to \mathrm{End}_{\mathrm{Ab}}(M)$ (where the multiplication law on the latter is given by composition): if M is an R-module then we can define $\lambda(r) \in \mathrm{End}_{\mathrm{Ab}}(M)$ to be left multiplication by r, and conversely if $\lambda : R \to \mathrm{End}_{\mathrm{Ab}}(M)$ is a ring morphism then $r.m := \lambda(r)(m)$ endows M with the structure of an R-module.
Now let $\lambda : R \to \mathrm{End}_{\mathrm{Ab}}\left({}^{M}\!/_{IM}\right)$ be the ring morphism corresponding to the R-module structure on ${}^{M}\!/_{IM}$. If $r \in I$, then multiplication by r on ${}^{M}\!/_{IM}$ is the zero map, and thus $r \in \ker(\lambda)$. As thus $I \subseteq \ker(\lambda)$, we obtain an induced ring morphism $\overline{\lambda} : {}^{R}\!/_{I} \to \mathrm{End}_{\mathrm{Ab}}\left({}^{M}\!/_{IM}\right)$, given by $\overline{\lambda}(r + I) = \lambda(r)$ for all $r \in R$. Hence, $\overline{\lambda}$ endows ${}^{M}\!/_{IM}$ with the structure of an ${}^{R}\!/_{I}$-module, given explicitly by

$$(x + I)(y + IM) = \overline{\lambda}(x + I)(y + IM) = \lambda(x)(y + IM) = xy + IM.$$

(3) Let $m \in M$ be arbitrary, then there exists a polynomial $f \in R$ such that $m = (xf, yf)$. Thus $m = x \cdot (f, 0) + y \cdot (0, f) \in IN$, and so we obtain $M \subseteq IN$. In particular, ${}^{IN}\!/_{M}$ is a well-defined R-submodule of ${}^{N}\!/_{M}$. To conclude, notice that

$$\begin{aligned} I\left({}^{N}\!/_{M}\right) &= \left\{ \sum_{i=1}^{d} r_i(n_i + M) \;\middle|\; 1 \leq d \in \mathbb{Z},\ r_i \in I,\ n_i \in N \right\} \\ &= \left\{ \underbrace{\left(\sum_{i=1}^{d} r_i n_i \right)}_{\in IN} + M \;\middle|\; 1 \leq d \in \mathbb{Z},\ r_i \in I,\ n_i \in N \right\} \\ &= \left\{ \textstyle\sum_{i=1}^{d} r_i n_i \;\middle|\; 1 \leq d \in \mathbb{Z},\ r_i \in I,\ n_i \in N \right\} \Big/ M = {}^{IN}\!/_{M}. \end{aligned}$$

(4) By (3) we have

$$L/_{IL} \overset{(3)}{=} \left({}^{N}\!/_{M}\right)\Big/\left({}^{IN}\!/_{M}\right) \cong {}^{N}\!/_{IN}$$

by the third isomorphism theorem. Now observe that the map

$$\begin{aligned} N &\to {}^{R}\!/_{I} \oplus {}^{R}\!/_{I} \\ (f, g) &\mapsto (f + I, g + I) \end{aligned}$$

is surjective and has kernel IN (verify it!). Thus, as by the remark above (3) we have ${}^{R}\!/_{I} \cong k$ (can you describe the R-module structure on k given by this isomorphism?), we obtain by the first isomorphism theorem that ${}^{N}\!/_{IN} \cong k \oplus k$.

(5) Let $(f,g) \in N$ be arbitrary. Then $xy(f,g) = fy(x,0) + gx(0,y) \in M$, and thus $xy((f,g)+M) = 0$ inside ${}^{N}\!/_{M}$. As $(f,g) \in N$ was arbitrary, we obtain $xy \in \mathrm{Ann}({}^{N}\!/_{M})$. On the other hand, as R is a domain, we have $\mathrm{Ann}({}_{R}R) = (0)$. As the annihilator is preserved under R-module isomorphisms, we thus have ${}^{N}\!/_{M} \ncong R$.

□

Exercise 5. Let

$$0 \to M \to N \to {}^{N}\!/_{M} \to 0$$

be a short exact sequence of R-modules. For each of the following assertions either prove that the assertion holds or provide a counterexample.

(1) If M and ${}^{N}\!/_{M}$ are finitely generated, then N is too.
(2) Conversely, if N is finitely generated, then ${}^{N}\!/_{M}$ is finitely generated too.
(3) If N is finitely generated, then M is finitely generated too.

Proof. (1) As M is finitely generated, we can find a subset $\{m_1, \ldots, m_k\} \subseteq M$ generating M as an R-module, and as ${}^{N}\!/_{M}$ is finitely generated we can find a subset $\{n_1 + M, \ldots, n_l + M\} \subseteq {}^{N}\!/_{M}$ generating ${}^{N}\!/_{M}$ as an R-module.
We claim that N is generated by $\{m_1, \ldots, m_k, n_1, \ldots, n_l\}$. Given $n \in N$, we can write $n + M = \sum_{j=1}^{l} s_j(n_j + M)$ for some $s_j \in R$, and so $n - \sum_{j=1}^{l} s_j n_j \in M$. But then there exist $r_i \in R$ such that $n - \sum_{j=1}^{l} s_j n_j = \sum_{i=1}^{k} r_i m_i$. This exhibits n as an R-linear combination of the m_i's and n_j's and so N is generated by these elements.

(2) The statement is true. Suppose $\{n_1, \ldots n_k\}$ generate N, then in fact $\{n_1 + M, \ldots, n_k + M\}$ generates N/M. Indeed any $n + M \in N/M$ can be written as

$$n + M = \left(\sum_{i=1}^{k} r_i n_i\right) + M = \sum_{i=1}^{k} r_i(n_i + M)$$

and thus $n + M$ is an R-linear combination of the $n_i + M$'s.

(3) This statement is not true. Take $R = \mathbb{C}[x_1, x_2, \ldots]$, the polynomial ring in infinitely many variables. (An element of R is by definition a polynomial in finitely many of the variables $x_1, x_2, \ldots$, and addition and multiplication are then exactly what one would think it is).

Let N be R viewed as a module over itself, and take the submodule M to be generated by $\{x_1, x_2, \ldots\}$. This is a proper submodule, as it does not contain the constants $\mathbb{C} \subset N$. Any element of M is a polynomial $f(x_1, \ldots, x_i)$ with no constant term. Given a finite set of such polynomials $\{f_i\} \subset M$, there is an integer I such that any element contained in $\langle\{f_i\}\rangle$ can be written as a linear combination of monomials, each of which has positive degree in some x_i with $i < I$. So this span cannot be equal to all of M, as it does not contain x_n for $n \gg 0$.

Note: the statement in (3) is true for modules over an important class of rings called Noetherian rings. These include many common rings such as fields k, $\mathbb{Z}$, and $k[x_1, \ldots, x_n]$. So $\mathbb{C}[x_1, x_2, \ldots]$ is an example of a non-Noetherian ring.

□

Exercise 6. (1) Let

$$0 \to M \to N \to N/M \to 0$$

be a short exact sequence of R-modules. For each of the following assertions either prove that the assertion holds or provide a counterexample.

- If N is free, then N/M is free.
- If N is free, then M is free.
- If M and N/M are free, then N is free.

(2) Let $R = \mathbb{Z}$. Is $\mathbb{Z}[x]/(x^2+1)\mathbb{Z}[x]$ a free R-module? How about $\mathbb{Z}[x]/(2x^2)\mathbb{Z}[x]$? Is $\mathbb{Q}$ a free R-module? Is it finitely generated?

Proof. A module is free if it is isomorphic to $\bigoplus_I R$ for some (possibly infinite) indexing set I.

Digression:

Definition 1. A subset $\{m_i\} \subset M$ is a basis for M if:

- It spans M: every $m \in M$ can be written as $m = \sum r_i m_i$ for some $r_i \in R$.
- It is linearly independent: if $\sum r_i m_i = 0$ for $r_i \in R$ then $r_i = 0$ for each i.

Lemma 1. *The module M is free if and only if it has a basis.*

Proof. Assume M is free, so $M \cong \bigoplus_I R$. We can define a basis $\{e_i\}_I$ for M where e_i is 1 in its i^{th} position and zero elsewhere. It is straightforward that these span and are linearly independent. Conversely suppose we have a module M which has a basis $\{e_i\}_{i\in I}$. Define $\phi : \oplus_I R \to M$ by extending linearly from $\phi((\delta_{i,j})_{j\in I}) = e_i$ for each $i \in I$. This is surjective, because any $m \in M$ can be written as a linear combination of the e_i and each of these is in the image. It is injective, because if not there is some non-zero element of $\oplus_I R$ killed by ϕ. But this gives a non-trivial linear dependence among the e_i in M. □

Now we return to the solution.

(1)
- This is false: a counterexample is given by $R = \mathbb{Z}$, $N = \mathbb{Z}$, $M = 2\cdot\mathbb{Z}$, for then $N/M \cong \mathbb{Z}/2\mathbb{Z}$.
- This is also false: a counterexample is $R = \mathbb{Z}/4\mathbb{Z}$, $N = \mathbb{Z}/4\mathbb{Z}$ and $M = 2\cdot\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$. This has too few elements to be a free $\mathbb{Z}/4\mathbb{Z}$-module.
- This is true. Suppose M has basis $\{m_1, \ldots, m_k\}$ and N/M has basis $\{n_1 + M, \ldots, n_l + M\}$. We claim that $\{m_1, \ldots, m_k, n_1, \ldots, n_l\}$ is a basis for N. They span by the argument in Exercise 4.1. For linear independence: suppose $\sum s_j n_j + \sum r_i m_i = 0$. This implies $\sum s_j(n_j + M) = 0$ in N/M and so the s_j's are all zero by the linear independence of the $n_j + M$'s. But then $\sum r_i m_i = 0$ is a linear dependence for a basis of M, forcing also the r_i's to be zero as well.

(2)
- $\mathbb{Z}[x]/(x^2+1)\mathbb{Z}[x]$ is a free $\mathbb{Z}$-module, with basis $\{1, x\}$ (it is isomorphic to $\mathbb{Z}[i]$).
- $\mathbb{Z}[x]/(2x^2)\mathbb{Z}[x]$ is not free since x^n is a torsion element for all $n \geq 2$ (as $x^n \notin (2x^2)$ but $2x^n \in (2x^2)$).
- $\mathbb{Q}$ is not a free $\mathbb{Z}$ module. Indeed, any two elements of $\mathbb{Q}$ are $\mathbb{Z}$-linearily dependet: if $a/b, c/d \in \mathbb{Q}$ then either both are equal to zero, or $cb(a/b) - ad(c/d) = 0$ is a non-trivial $\mathbb{Z}$-linear relation. Thus if $\mathbb{Q}$ was a free $\mathbb{Z}$-module, then it must be generated by a single element, which is impossible. For example, this can be seen by the second part of the question:

$\mathbb{Q}$ is not finitely generated over $\mathbb{Z}$ since if $\{\frac{p_1}{q_1}, \dots, \frac{p_n}{q_n}\}$ is a generating set, let $q = q_1 \cdots q_n$. Then $\frac{1}{q+1}$ does not lie in the $\mathbb{Z}$-span of $\{\frac{p_1}{q_1}, \dots, \frac{p_n}{q_n}\}$.

□

Optional exercise. Not on the exam. Suggested if you are seriously interested in algebra.

Exercise 7. Let k be a field. In this exercise we understand the non-commutative ring $\mathcal{D}_k(k[x])$ of *differential operators* on $k[x]$ over k. Let $\mathcal{D}$ be the sub-algebra of $\mathcal{D}_k(k[x])$ generated by the elements $\frac{\partial}{\partial x}$ and x, where $\frac{\partial}{\partial x}$ sends a polynomial $p(x)$ to its algebraic derivative with respect to x and the element $x \in \mathrm{End}_k(k[x])$ is multiplication by x. We have seen in "Anneaux et corps" (sheet 3 ex. 9 and sheet 4 ex. 6) that $\mathcal{D}_k(k[x]) = \mathcal{D}$ when $\mathrm{char}\, k = 0$ (it is not true for $\mathrm{char}\, k > 0$, can you find an element?).

It was also shown that the elements $x^i \left(\frac{\partial}{\partial x}\right)^j$ generate $\mathcal{D}$ as a k-vectorspace for $(i, j) \in \mathbb{N}^2$. Additionally it was shown that $\mathcal{D}$ has no two sided non-trivial ideals, or equivalently $\mathcal{D}$ is simple, if $\mathrm{char}\, k = 0$.

(1) Show that a basis of $\mathcal{D}$ as a k-vector space is given by the elements $x^i \left(\frac{\partial}{\partial x}\right)^j$, where $(i, j) \in \mathbb{N}^2$ if $\mathrm{char}\, k = 0$, and $i \in \mathbb{N}$ and $j \in \{0, 1, \dots, p-1\}$ if $\mathrm{char}\, k = p > 0$.

(2) Now we change the perspective and consider a quotient of the free k-algebra on two generators $\mathcal{D}^{form} = k\langle u, v\rangle/(uv - vu - 1)$. Prove that in $\mathcal{D}^{form}$ we have the identity

$$uP(v) = \frac{\partial}{\partial v} P(v) + P(v)u$$

for all polynomials $P(v) \in k[v]$. Use this to prove that $\mathcal{D}^{form}$ is generated as a k-vector space by $\{v^j u^i \mid (i, j) \in \mathbb{N}^2\}$.

(3) Show that there are well defined ring homomorphisms ϕ and ψ from $\mathcal{D}^{form}$ to $\mathrm{End}_k(k[x])$, such that $\phi(u) = \frac{\partial}{\partial x}$ and $\phi(v) = x$, as well as $\psi(u) = x$ and $\psi(v) = -\frac{\partial}{\partial x}$. Show that ϕ and ψ are surjective onto $\mathcal{D}$, and define an isomorphism betwenn $\mathcal{D}$ and $\mathcal{D}^{form}$ if and only if $\mathrm{char}(k) = 0$.

(4) Determine the submodules of $k[x]$ as a left $\mathcal{D}$-module (with left $\mathcal{D}$-module structure given by the inclusion $\mathcal{D} \subset \mathrm{End}_k(k[x])$) in the case when $\mathrm{char}\, k = 0$.

(5) Determine the left submodules of $k[x]$ as a $\mathcal{D}$-module, if $\mathrm{char}\, k = 2$.

Proof. (1) As mentioned above, the fact that $\{x^i \left(\frac{\partial}{\partial x}\right)^j \mid i, j \in \mathbb{Z}_{\geq 0}\}$ is a generating set of $\mathcal{D}$ over k was already shown in "Anneaux et corps". Now notice that if $\mathrm{char}(k) = p > 0$ then $\left(\frac{\partial}{\partial x}\right)^j = 0$ for all $j \geq p$ (repeatedly taking derivatives more than p times will produce a factor divisible by p in front of every monomial). Thus if we let $\Omega = \mathbb{Z}^2_{\geq 0}$ if $\mathrm{char}(k) = 0$ and $\Omega = \mathbb{Z}_{\geq 0} \times \{0, \dots, p-1\}$ if $\mathrm{char}(k) = p > 0$, we obtain that already $\mathcal{B} = \{x^i \left(\frac{\partial}{\partial x}\right)^j \mid (i, j) \in \Omega\}$ generates $\mathcal{D}$.

Now we need to prove that the elements of $\mathcal{B}$ are k-linearily independent. Let $\lambda_\bullet : \Omega \to k$ be a set of finitely many non-zero coefficients in k such that $\sum_{(i,j)\in\Omega} \lambda_{i,j} x^i \left(\frac{\partial}{\partial x}\right)^j = 0$. In particular, if we evaluate the expression on the LHS at 1 we obtain $\sum_{(i,0)\in\Omega} \lambda_{i,0} x^i = 0$ as element of $k[x]$, and thus $\lambda_{i,0} = 0$ for all i. Suppose we have proven $\lambda_{i,j} = 0$ for all i and all $j < J$ for some $J > 0$ (satisfying $J \leq p-1$ if $\mathrm{char}(k) = p > 0$). Then we have $\sum_{(i,j)\in\Omega,\ j\geq J} \lambda_{i,j} x^i \left(\frac{\partial}{\partial x}\right)^j = 0$, and evaluating the LHS at x^J shows that $\lambda_{i,J} = 0$ for all i. By induction, we conclude that $\lambda_{i,j} = 0$ for all $(i,j) \in \Omega$. Thus $\mathcal{B}$ is a basis of $\mathcal{D}$.

(2) Inside $\mathcal{D}^{form}$, we can use the relation $uv - vu - 1 = 0$ to swap the u's and v's in any given monomial. Let us make this precise. By induction on j, one proves

$$uv^j = \frac{\partial}{\partial v} v^j + v^j u$$

inside $\mathcal{D}^{form}$ (i.e. modulo $uv - vu - 1$). The formula in question then follows by k-linearity. Multiplying the formula by powers of u, it then follows also more generally that

$$u^i P(v) = \sum_{k=0}^{i} \left(\frac{\partial}{\partial v}\right)^k (P(v)) \cdot u^{i-k}.$$

In particular, we have a formula to replace any monomial $u^i v^j$ by an expression where in all monomials v is to the left of u. By using this iteratively, moving all v's to the left, one can express every element of $\mathcal{D}^{form}$ as a sum of monomials of the form $v^j u^i$. That is, $\mathcal{B}^{form} := \{v^j u^i \mid i,j \in \mathbb{Z}_{\geq 0}\}$ is a generating set of $\mathcal{D}^{form}$ as a k-vector space.

(3) By the universal property of the free k-algebra on two generators, there exists a k-algebra morphism $\Phi : k\langle u, v\rangle \to \mathrm{End}_k(k[x])$ mapping $u \mapsto \frac{\partial}{\partial x}$ and $v \mapsto x$. To show that Φ factors through $\mathcal{D}^{form}$, it suffices to prove that $uv - vu - 1$ is in the kernel of Φ. This amounts to proving that for all $f \in k[x]$ we have $\frac{\partial}{\partial x}(xf(x)) = f(x) + x\frac{\partial}{\partial x} f(x)$, which follows from the (algebraic) Leibnitz-rule. Therefore, we obtain the well-defined $\phi : \mathcal{D}^{form} \to \mathrm{End}_k(k[x])$ mapping $u \mapsto \frac{\partial}{\partial x}$ and $v \mapsto x$.

Now as $\mathcal{D}$ contains $\frac{\partial}{\partial x}$ and x, the image of ϕ is contained in $\mathcal{D}$. On the other hand, as every element of $\mathcal{B}$ is attained by ϕ (evaluating at $v^i u^j$), we obtain that the image is exactly $\mathcal{D}$, i.e. ϕ is surjective onto $\mathcal{D}$.

By repeating the same argument for $\Psi : k\langle u, v\rangle \to \mathrm{End}_k(k[x])$ mapping $u \mapsto x$ and $v \mapsto -\frac{\partial}{\partial x}$, we obtain also the desired map $\psi : \mathcal{D}^{form} \to \mathrm{End}_k(k[x])$, surjective onto $\mathcal{D}$.

Now finally we investigate when the surjective morphism $\phi : \mathcal{D}^{form} \to \mathcal{D}$ is also injective. If $\mathrm{char}(k) = p > 0$ then u^p is mapped to $\left(\frac{\partial}{\partial x}\right)^p$, which as we have seen is equal to 0 inside $\mathcal{D}$. To conclude that ϕ isn't injective, it remains to show that u^p isn't equal to 0 inside $\mathcal{D}^{form}$. This can be seen via ψ, because $\psi(u^p)$ is the k-endomorphism of $k[x]$ given by multiplication with x^p, which is not the zero map. So u^p is non-zero inside $\mathcal{D}^{form}$, and hence ϕ is not injective. The same argument, replacing u and v, shows that ψ is not injective either.

It remains to consider the case where $\mathrm{char}(k) = 0$. We have seen that $\mathcal{B}^{form} := \{v^j u^i \mid i,j \in \mathbb{Z}_{\geq 0}\}$ generates $\mathcal{D}^{form}$ over k, and in characteristic zero $\mathcal{B} = \{x^i \left(\frac{\partial}{\partial x}\right)^j \mid i,j \in \mathbb{Z}_{\geq 0}\}$ is a k-basis of $\mathcal{D}$. But then ϕ induces a bijection between $\mathcal{B}^{form}$ and $\mathcal{B}$, and thus

we obtain that $\mathcal{B}^{form}$ is also linearily independent, and thus a k-basis. Therefore ϕ induces a bijection between two bases, and is thus a vector-space isomorphism. In particular, ϕ is injective, and hence $\mathcal{D}^{form} \cong \mathcal{D}$ in characteristic zero. The argument for ψ is completely analogous.

(4) We claim that $k[x]$ is a simple $\mathcal{D}$-module. First note that $k[x]$ is generated as a $\mathcal{D}$-module by the element $1 \in k[x]$, because for any $f(x) \in k[x]$, the k-endomorphism of $k[x]$ given by multiplcation with $f(x)$ is an element of $\mathcal{D}$, and the image of 1 under this endomorphism is $f(x)$. Hence any element of $k[x]$ can be obtained by letting some element of $\mathcal{D}$ act on 1, i.e. 1 generates $k[x]$ as a $\mathcal{D}$-module. Now suppose N is a non-zero $\mathcal{D}$-submodule of $k[x]$. We will show that $1 \in N$. As N is non-zero, it contains some non-zero element $f(x) = \sum_{i=0}^{n} a_i x^i$ (where $a_n \neq 0$). We need to find a differential operator D such that $D(f) = 1$. In fact, $D = \frac{1}{a_n n!}(\frac{\partial}{\partial x})^n$ will do it (here we use that $\mathrm{char}(k) = 0$).

(5) The first thing to note is that

$$\frac{\partial}{\partial x}(x^2) = 2x = 0.$$

Similarly $\frac{\partial}{\partial x}(x^{2n}) = 0$ any $n \in \mathbb{N}$.
Now let N be a non-zero $\mathcal{D}$-submodule of $k[x]$, and notice that N is generated by a single element. Indeed, the ring $\mathcal{D}$ contains a copy of $k[x]$ as a subring (by viewing an element p of $k[x]$ as the k-endomorphism of $k[x]$ given by left multiplication by p), and the induced $k[x]$-module structure on $k[x]$ is the natural one. Thus N is also a $k[x]$-submodule of $k[x]$, i.e. an ideal. But $k[x]$ is a PID, so N is generated by some f as a $k[x]$-module. In fact, we can take f to be the monic polynomial of minimal degree inside N (there is a unique one). As $N \neq 0$ we have $f \neq 0$, and as the derivative of f is has degree strictly smaller than f and is inside N (as N is a $\mathcal{D}$-module), we must have $\frac{\partial}{\partial x} f(x) = 0$. This means that $f(x) = \sum_{i=1}^{2n} a_i x^{2i}$ for some $a_0, \ldots, a_n \in k$ with $a_n = 1$. Finally, we show that $\mathcal{D} \cdot f = k[x] \cdot f$ as k-subspaces of $k[x]$; it suffices to show that the LHS is included in the RHS. As both sides are k-vector spaces, it suffices to prove that $\mathcal{B} \cdot f \subseteq k[x] \cdot f$. This is true as $\left(x^i \left(\frac{\partial}{\partial x}\right)^j\right) \cdot f(x) = 0$ if $j \geq 1$, and $x^i f(x) \in k[x] \cdot f$ for all $i \geq 0$.
Therefore, we conclude that the $\mathcal{D}$-submodules of $k[x]$ are exactly the subsets of the form $k[x] \cdot f$ with f monic and only having terms of even degree. Notice also that any two distinct such f give distinct submodules.

□

Remark 0.1. Let k be a field of characteristic $p > 0$. We describe an element $\partial \in \mathcal{D}_k(k[x])$ which is not in the sub-algebra generated by $\frac{\partial}{\partial x}$ and x. Given $i \geq 0$, define

$$\partial(x^i) = \begin{cases} 0 \text{ if } i < p \\ \frac{n(n-1)\ldots(n-p+1)}{p} x^{n-p} \text{ if } i \geq p \end{cases}$$

(by $\frac{n(n-1)\ldots(n-p+1)}{p}$ we mean the image of $\frac{n(n-1)\ldots(n-p+1)}{p} \in \mathbb{Z}$ via the canonical ring morphism $\mathbb{Z} \to k$ sending 1 to 1).

Note that in characteristic 0, this operator is simply

$$\frac{1}{p}\left(\frac{\partial}{\partial x}\right)^p$$

Anyways, an immediate computation shows that

$$[\partial, x] = \left(\frac{\partial}{\partial x}\right)^{p-1}$$

so ∂ is indeed a differential operator. To see that it is not generated by $\frac{\partial}{\partial x}$ and x (i.e. $\partial \notin \mathcal{D}$), note that $(x^p) \subseteq k[x]$ is always a sub-$\mathcal{D}$-module, while $\partial(x^p) = (p-1)! \notin (x^p)$. In fact, as in characteristic zero, $k[x]$ is a simple $\mathcal{D}_k(k[x]))$-module!.

EPFL - Fall 2023 Prof. Zs. Patakfalvi
Rings and modules **Exercises**
Sheet 2 - Solutions

There was one bonus exercise on this problem sheet. The exercise was denoted by the symbol ♠ next to the exercise number.

Exercise 1. Show that the following holds for an R-module M of finite length $l(M)$ (i.e., an R-module M that admits a composition series of finite length).

(1) If there is a short exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

of R-modules, then $l(M) = l(M') + l(M'')$.
(2) If $N <_R M$ is a proper submodule then $l(N) < l(M)$.
(3) Use (2) to show that any strict chain of submodules in M (not necessary a maximal chain, i.e. not necessarily a composition series) has length smaller than or equal to $l(M)$. Conclude that a module M is of finite length if and only if M is both Noetherian and Artinian.

Proof. (1) The solution has two steps: first we prove that both M' and M'' have finite length, and then we prove the formula.

For the first step, let $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_t = M$ be a composition series of M (in particular $t = l(M)$). Up to isomorphism (of short exact sequences), we can view M' as an actual submodule of M and $M'' = M/M'$ as the actual quotient of M by M'. Now for $0 \leq i \leq t$, define $M_i' = M' \cap M_i$ and $M_i'' = (M_i + M')/M'$; we would like to understand the quotients of consecutive terms.

On the one hand, we have a natural map $M_{i+1}' \hookrightarrow M_{i+1} \twoheadrightarrow M_{i+1}/M_i$, and the kernel of this composition is exactly M_i'. Hence we obtain an induced inclusion $M_{i+1}'/M_i' \hookrightarrow M_{i+1}/M_i$. As the latter is simple, we obtain that M_{i+1}'/M_i' is either trivial or simple.

On the other hand, we have by the third isomorphism theorem that $M_{i+1}''/M_i'' \cong (M_{i+1} + M)/(M_i + M)$. Then, we have a natural map $M_{i+1} \hookrightarrow M_{i+1} + M \twoheadrightarrow (M_{i+1} + M)/(M_i + M)$, and the composed arrow is easily seen to be surjective. Also, M_i is included in the kernel of the composition, so we obtain an induced surjective map $M_{i+1}/M_i \twoheadrightarrow (M_{i+1} + M)/(M_i + M) \cong M_{i+1}''/M_i''$. As M_{i+1}/M_i is simple, we obtain that M_{i+1}''/M_i'' is either trivial or simple.

In conclusion, the quotients of consecutive terms both in $M_0' \subseteq \cdots \subseteq M_t'$ and $M_0'' \subseteq \cdots \subseteq M_t''$ are all either simple or trivial. So by deleting some of the modules in the sequence, we will obtain composition series both for M' and M''. Hence M' and M'' have finite length (and length smaller than or equal to t).

Now for the second step, by the one-to-one correspondence of submodules of M'' and submodules of M containing M' it is clear that a composition series for M' can be extended to a composition series for M by adding the preimage of a composition series

of M''. This gives a composition series for M of length $l(M')+l(M'')$. Therefore, since by the Jordan Holder Theorem $l(M)$ is the length of *any* composition series, we obtain $l(M') + l(M'') = l(M)$.

(2) Follows directly from the argument above.

(3) Let $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = M$ be a strict chain of length n. Then by (2) we have $l(M) > l(M_{n-1}) > \cdots > l(M_0) = 0$, hence $l(M) \geq n$. Since every chain of M is of finite length bounded by $l(M)$, M is both Noetherian and Artinian. The implication in the other direction was discussed in Remark 3.2.4 of the lecture notes.

□

Exercise 2. Let R be a ring and let M be a finitely generated module over R. Let $f : M \to M$ be an R-module homomorphism.

(1) Suppose that R is a Noetherian ring.
   (i) Does injectivity of f implies surjectivity?
   (ii) Does surjectivity of f implies injectivity?
   (iii) What happens if R is not necessarily Noetherian?
   Hint: For one of the directions, try to reduce to the Noetherian case by considering the $\mathbb{Z}$-subalgebra of R generated by finitely many suitable elements.

(2) Suppose that M is a module of finite length, show that f is injective if and only if f is surjective.

Proof. (1) (i) Let R be a ring with $a \in R$ neither a unit nor a zero divisor, then multiplication by a is an injective but not surjective morphism $m_a : R \to R$.

(ii) Suppose that M is a finitely generated module over a Noetherian ring, then M is Noetherian. Let $f : M \to M$ be a surjective morphism. For all k we have containments $\ker(f^k) \subset \ker(f^{k+1})$. Therefore, there exists a positive integer m such that $\ker(f^{m+1}) = \ker(f^m)$. In particular, $f : \mathrm{im}(f^m) \to M$ is injective, but by surjectivity $\mathrm{im}(f^m) = M$, therefore f is injective.

(iii) Amazingly, the statement remains true even if R is not Noetherian. Let e_i for $1 \leq i \leq n$ be generators of M as an R-module. Let $f(e_i) = \sum_{i=1}^n a_{ij} e_j$ for all i. By surjectivity there exists b_{jk} such that $e_j = \sum_{k=1}^n b_{jk} f(e_k)$ for all j. Suppose that $m \in \ker(f)$ with $m = \sum_i m_i e_i$. Let $\mathbb{Z}[a_{ij}, b_{ij}, m_k] \to R$ be the natural inclusion morphism, where $\mathbb{Z}[a_{ij}, b_{ij}, m_k]$ is the $\mathbb{Z}$-subalgebra of R generated by the a_{ij}'s, b_{ij}'s and m_k's. There is therefore an induced structure of $R' = \mathbb{Z}[a_{ij}, b_{ij}, m_k]$-module on M. Let M' be the R'-submodule generated by e_i for $1 \leq i \leq n$. By definition of M' the morphism f induces a morphism $f' : M' \to M'$, it is surjective since $e_i = f(\sum_k b_{ik} e_k)$. As now R' is Noetherian (it is a finitely generated $\mathbb{Z}$-algebra), we obtain by the previous point that the element $m \in \ker(f')$ is zero. As $m \in \ker(f)$ was arbitrary, we conclude that f is injective.

(2) Consider the short exact sequence

$$0 \longrightarrow \ker(f) \longrightarrow M \longrightarrow \mathrm{im}(f) \longrightarrow 0 \ .$$

By Exercise 1.1, we have $l(M) = l(\ker(f)) + l(\mathrm{im}(f))$. Since the zero module is the only module of length zero, f being surjective implies that $\ker(f) = 0$. Conversely, if f is injective, then $l(M) = l(\mathrm{im}(f))$, hence $l(\mathrm{im}(f))$ can not be a proper submodule of M by the same exercise, i.e. $M = \mathrm{im}(f)$.

□

Exercise 3. This exercise is about *semi-simple* modules.

Definition 1. A module M over a ring R is semi-simple, if it is a finite sum of its simple submodules. That is, $M = \sum_{i=1}^{d} M_i$, where $M_i \leq_R M$ are simple. A ring R is semi-simple if it is semi-simple as a left R-module.

(1) Prove that M is semi-simple if and only if $M = \bigoplus M_i$ for finitely many simple $M_i \leq_R M$, i.e., prove that if $M = \sum_{i=1}^{d} M_i$ where $d \in \mathbb{N}$ is minimal with this property, then $M_i \cap \sum_{j \neq i} M_j = 0$ for all i.

(2) In this exercise we prove Maschke's theorem. Let G be a finite group, and k a field such that $(|G|, \mathrm{char}(k)) = 1$. Then $k[G]$ is semi-simple.
   (i) For any ring R, any R-module M and any submodule N show that $M = N \oplus L$ for some submodule L if and only if there exists an element $\phi \in \mathrm{Hom}_R(M, N)$ such that $\phi(n) = n$ for all $n \in N$. *Hint: Use the universal property of direct sums.*
   (ii) Let M be any $k[G]$-module which has finite dimension over k. Show that for any submodule N there exists an element $\phi \in \mathrm{Hom}_{k[G]}(M, N)$ such that $\phi(n) = n$ for all $n \in N$. *Hint: Take $\xi \in \mathrm{Hom}_k(M, N)$ such that $\xi(n) = n$ for all $n \in N$. Show that ϕ defined by $\phi(x) = \frac{1}{|G|} \sum_{g \in G} g\xi(g^{-1}x)$ is $k[G]$-linear.*
   (iii) Conclude the proof.

(3) Under the same hypotheses as before, prove that $k[G]$ has finite length over itself.

Proof. (1) The $\Leftarrow$ direction is immediate from Definition 1. So, we prove direction $\Rightarrow$.

Let us start with an arbitrary finite collection of simple submodules M_i of M (given by Definition 1), such that $\sum_{i=1}^{d} M_i = M$. We may further also assume that d is minimal with this property.

We have that $\sum_{i=1}^{d} M_i \cong \bigoplus_{i=1}^{d} M_i$ if and only if for all $1 \leq i \leq d$ we have $M_i \cap \sum_{j \neq i} M_j = 0$. If this is the case, we are ready, so we may assume the contrary. By reindexing, we may assume then that $M_1 \cap \sum_{j=2}^{d} M_j \neq 0$. However, since $M_1 \cap \left(\sum_{i=2}^{d} M_i\right)$ is then a non-zero submodule of M_1, and therefore it equals M_1. Hence, $M_1 \subseteq \sum_{i=2}^{d} M_i$, and then $M = \sum_{i=2}^{d} M_i$. This contradicts the choice of d, and also concludes our proof.

(2) We prove Maschke's theorem:
   (i) We will show that $M = \ker(\phi) \oplus N$. To this end let $i_N : N \hookrightarrow M$ and $i_{\ker(\phi)} : \ker(\phi) \hookrightarrow M$ denote the inclusion of the two submodules. By the universal property of direct sums there exists a unique morphism $i_{\ker(\phi)} + i_N = \psi : \ker(\phi) \oplus N \to M$, it is injective since $N \cap \ker(\phi) = 0$. We show that ψ is surjective. Let $m \in M$, let $\phi(m) = n$, we have $m - n \in \ker(\phi)$, say $m - n = l$. Hence $m = \psi(l, n)$ where $l \in \ker(\phi)$ and $n \in N$.
   (ii) We prove that for every $k[G]$-module M, which is finite dimensional over k, and every submodule $N \leq_{k[G]} M$, there is a direct complement. By the previous exercise, to prove our goal, we have to find $\phi \in \mathrm{Hom}_{k[G]}(M, N)$, such that $\phi|_N = \mathrm{Id}_N$. Let us start with a k-vector space projection $\xi \in \mathrm{Hom}_k(M, N)$, such that $\xi|_N = \mathrm{Id}_N$. Such projection exists by linear algebra. Then, define for every $x \in M$,

$$\phi(x) = \frac{1}{|G|} \sum_{g \in G} g\xi(g^{-1}x)$$

(here we use that $(|G|, \mathrm{char}(k)) = 1$). We claim that ϕ is as desired. Indeed, if $x \in N$, then $g^{-1}x \in N$, and hence $\xi(g^{-1}x) = g^{-1}x$, for all $g \in G$. So,

$$\phi(x) = \frac{1}{|G|}\sum_{g\in G} g\xi(g^{-1}x) = \frac{1}{|G|}\sum_{g\in G} gg^{-1}x = \frac{1}{|G|}|G|x = x.$$

Furthermore, ϕ is $k[G]$-linear. Indeed, since it is k-linear, only the compatibility with $h \in G$ has to be shown, which is done by the next computation (here $h \in G$ arbitrary):

$$\phi(hx) = \frac{1}{|G|}\sum_{g\in G} g\xi(g^{-1}hx) = \frac{1}{|G|}\sum_{f\in G} hf\xi(f^{-1}x) = h\phi(x)$$

(iii) Since $k[G]$ is finite dimensional over k. Let $N \subset k[G]$ be a submodule. By the above there exists a submodule L such that $N \oplus L = k[G]$. We repeat the argument for N and L until $k[G] = \oplus M_i$ where every submodule is simple (note that this process has to be done only finitely many times, because any finitely generated $k[G]$-module is in particular a finite dimensional k-vector space since G is finite).

(3) By (1) and (2) we know that $k[G] = \bigoplus_{i=1}^{d} M_i$ for finitely many simple submodules M_i. Then the modules $N_j = \bigoplus_{i=1}^{j} M_i$ for $0 \le j \le d$ yield a decomposition series, showing that $k[G]$ has length d.

□

Exercise 4. (1) Let R be a PID, and let $f \in R$ be a product of $n \ge 0$ prime elements. Prove that the length of $R/(f)$ as an R-module is equal to n.

(2) Let $f \in \mathbb{R}[x]$ be a nonzero polynomial with exactly $n \ge 0$ non-real roots (counted with multiplicity). Prove that

$$\dim_{\mathbb{R}}\left(\mathbb{R}[x]/(f)\right) - \mathrm{length}_{\mathbb{R}[x]}\left(\mathbb{R}[x]/(f)\right) = n/2$$

(3) Let M be a $\mathbb{Z}$-module. Prove that M has finite length if and only if it is finite (as a set).

(4) Give an example of a ring and a module over this ring which has finite length but infinitely many submodules.

Proof. (1) We prove the assertion by induction on n; for $n = 0$ it clearly holds, and for $n = 1$ it holds since primes in a PID are maximal, and thus the quotient of R by a prime is simple.

So assume that we have shown the assertion for some $n \ge 1$, and let f be a product of $n+1$ primes. Let p be a prime dividing f and write $f = pg$ where g is a product of n primes. Then we have a natural surjection $R/(f) \twoheadrightarrow R/(g)$ of R-modules, and let K be the kernel. It is straightforward to see that $K = R\cdot(g+(f))$. Now we have a short exact sequence

$$0 \to \mathrm{Ann}_R(g+(f)) \to R \xrightarrow{\cdot(g+(f))} K \to 0.$$

Finally, one can easily verify that $\mathrm{Ann}_R(g+(f)) = (p)$, and thus $K \cong R/(p)$. As we then have a short exact sequence

$$0 \to R/(p) \to R/(f) \to R/(g) \to 0,$$

it follows from Exercise 1.1 and the induction hypothesis that $R/(f)$ has length $n+1$.

(2) The dimension of $\mathbb{R}[x]/(f)$ as an $\mathbb{R}$-vector space is $d = \deg f$. Furhtermore, as $\mathbb{R} \subseteq \mathbb{C}$ is a field extension of degree 2, the irreducible polynomials of $\mathbb{R}[x]$ are the linear polynomials and the quadratic polynomials having no real roots. Therefore, if m is the number of real roots of f counted with multiplicity, one can see that f is the product of exactly $m + n/2$ irreducible polynomials. Hence by the previous exercise we obtain that the length of $\mathbb{R}[x]/(f)$ is equal to $m + n/2$. As $d = m + n$, we obtain

$$\dim_{\mathbb{R}}\left(\mathbb{R}[x]/(f)\right) - \text{length}_{\mathbb{R}[x]}\left(\mathbb{R}[x]/(f)\right) = m + n - (m + n/2) = n/2.$$

(3) If M is finite as a set then M has finite length as there are only finitely many submodules. Conversely, if M has finite length, then by Exercise 1 it is in particular Noetherian, so finitely generated. By the classification of finitely generated $\mathbb{Z}$-modules, we have an isomorphism $M \cong \mathbb{Z}^{\oplus r} \oplus F$ for some finite $\mathbb{Z}$-module F and $r \geq 0$. If by contradiction $r \geq 1$, then M contains a copy of $\mathbb{Z}$ as a submodule, so again by Exercise 1 we obtain that $\mathbb{Z}$ has finite length. This is not true, e.g. as $\mathbb{Z}$ is not Artinian. Hence $r = 0$ and $M \cong F$ is finite.

(4) It suffices to take an infinite field k and a finite dimensional k-vector space V of dimension greater than or equal to 2. It is clearly of finite length, and if $v_1, v_2 \in V$ are linearly independent, then $\{k \cdot (v_1 + \lambda v_2)\}_{\lambda \in k}$ is an infinite family of distinct subspaces. □

Exercise 5. Let $n, m > 0$ be integers, let k be a field and let $R := k[x, y]$. Show that the R-module

$$M := k[x, y]/(x^n, y^m)$$

has length nm.
Hint: Exercise 1 can be useful to decompose this computation into easier ones, allowing some induction argument.

Proof. First let us show the following: for any $d \geq 0$, the module

$$N_d := k[x, y]/(x, y^d)$$

has length d.
Set

$$S := k[x, y]/(x)$$

and $\pi : R \to S$ the quotient map. By Exercise 2.3 on sheet 1, we can define an S-module structure on N_d such that for all $r \in R$ and $n \in N_d$, $r \cdot n = \pi(r) \cdot n$.
With this in mind, it is immediate that S-submodules of N_d are the same as R-submodules of N_d, so in particular its length is unchanged.
Now, $S \cong k[y]$ by setting $x = 0$, and through this isomorphism we see that N_d corresponds to

$$k[y]/(y^d)$$

so we know by Exercise 4.1 that its length is d.

Now, let us compute the length of

$$N_{n,m} := k[x, y]/(x^n, y^m)$$

is nm. If $n = 1$, this was already worked out before, so assume $n \geq 2$. Consider the morphism $\phi : k[x,y] \to N_{n,m}$ given by sending 1 to $x^{n-1} + (x^n, y^m)$. Note that the sequence

$$k[x,y] \xrightarrow{\phi} N_{n,m} \to N_{n-1,m} \to 0$$

is exact where $N_{n,m} \to N_{n-1,m}$ is the usual quotient map, so we obtain a short exact sequence

$$0 \to k[x,y]\Big/\ker(\phi) \to N_{n,m} \to N_{n-1,m} \to 0$$

Let us understand $\ker(\phi)$. Clearly, $(x, y^m) \subseteq \ker(\phi)$, and given $a \in \ker(\phi)$, we get that by definition there exists $b, c \in k[x,y]$ such that

$$x^{n-1}a = x^n b + y^m c$$

In particular x^{n-1} divides $y^m c$, so since x and y are coprime ($k[x,y]$ is a UFD) we get that x^{n-1} divides c (write $c = x^{n-1}c'$). Thus,

$$a = xb + y^m c'$$

or in other words $a \in (x, y^m)$.

Hence we have proven that $\ker(\phi) = (x, y^m)$, so we finally have a short exact sequence

$$0 \to N_{1,m} \to N_{n,m} \to N_{n-1,m} \to 0$$

which by induction on n gives us

$$l(N_{n,m}) = l(N_{n-1,m}) + l(N_{1,m}) = (n-1)m + m = nm.$$

□

Exercise 6. ♠ Let $p > 0$ be a prime number. Compute the length of

$$\mathbb{Z}[x]\Big/(p^2, x^2 - p),$$

as a module over the ring $\mathbb{Z}[x]$.

Proof. Let $M := \mathbb{Z}[x]/(p^2, x^2 - p)$, and consider the quotient map

$$\pi\colon \mathbb{Z}[x]\Big/(p^2, x^2 - p) \to \mathbb{Z}[x]\Big/(p, x^2 - p).$$

Note that the latter module is isomorphic to

$$N := (\mathbb{Z}/p\mathbb{Z}[x])\Big/(x^2),$$

and since the $\mathbb{Z}[x]$-action this module factors through an action of $\mathbb{Z}/p\mathbb{Z}[x]$, let us compute the length of N as a $\mathbb{Z}/p[x]$-module. Since this ring is a PID, we deduce by Exercise 4.(1) that the length of N is 2.

Let us compute $\ker(\pi)$. By the third isomorphism theorem,

$$\ker(\pi) = (p, x^2 - p)\Big/(p^2, (x^2 - p)),$$

so in particular it is generated by $\overline{p}$ (i.e. the class of p in the quotient). hence, we have a surjection

$$\theta\colon \mathbb{Z}[x] \to \ker(\pi),$$

sending 1 to $\overline{p}$.

Let us understand $\ker(\theta)$. It is immediate to see that $(p, x^2 - p) \subseteq \ker(\theta)$. On the other hand, if $f(x) \in \ker(\theta)$, then $pf(x) = p^2 a(x) + (x^2 - p)b(x)$ for some $a(x), b(x) \in \mathbb{Z}[x]$. In

particular, p divides $(x^2 - p)b(x)$, so since p is prime, p divides $b(x)$. Write $b(x) = pb'(x)$. Then

$$f(x) = pa(x) + (x^2 - p)b'(x) \in (p, x^2 - b).$$

Thus,

$$(p, x^2 - p) = \ker(\theta).$$

In other words,

$$\ker(\pi) \cong \mathbb{Z}[x]\Big/(p, x^2 - p) \cong N.$$

In other words, we have a short exact sequence

$$0 \to N \to M \to N \to 0,$$

so by additivity of the length,

$$\text{length}(M) = 2\,\text{length}(N) = 4.$$

□

Exercise 7. Let R be a Noetherian ring. Are the following rings Noetherian? Are they Artinian?

(1) $R[x, \frac{1}{x}] := \{\sum_{i=-m}^{n} a_i x^i : a_i \in R, m, n \in \mathbb{N}\}$.
(2) $R[x_1, x_2, x_3, ...]$.
(3) $R[[x]]$, the ring of formal power series[1] with coefficients in R.
Hint: For an ideal I and each $n \in \mathbb{N}$, let $I_n := \{a_n : \exists \sum_{i=n}^{\infty} a_i x^i \in I\}$. Then adapt the proof of the Hilbert basis theorem.
(4) $C^0(\mathbb{R})$, the ring of continuous functions $\mathbb{R} \to \mathbb{R}$ with pointwise operations.
(5) $\mathbb{R}[x]\Big/\big((x-1)^2 x\big)$.

Proof. (1) We will show that $R[x, \frac{1}{x}]$ is isomorphic to a quotient of a polynomial ring. It then follows that it is Noetherian by the Hilbert basis theorem (as Noetherianity is preserved under quotients).
The isomorphism in question comes from the R-algebra homomorphism

$$\phi : R[u, v] \to R[x, \frac{1}{x}]$$
$$u \mapsto x,\ v \mapsto \frac{1}{x},$$

which exists by the universal property of $R[u, v]$. This is surjective as any element of $R[x, 1/x]$ can be written as some polynomial in x and $\frac{1}{x}$ by definition. Thus it has some kernel I, and hence $R[x, \frac{1}{x}] \cong R[u, v]/I$ is Noetherian.

As a side note, we can go further, and identify the kernel $\ker \phi = I$ to be the ideal $(uv - 1)$. For it is clear that $uv - 1 \in I$, and suppose that $g \in \ker \phi$. Then we can use elements of $(uv-1)$ to cancel mixed terms, and so write $g = g_1 + g_2$ where $g_1 \in (uv-1)$ and $g_2 = \sum_{i \geq 0} a_i u^i + \sum_{j>0} b_j v^j$ for some $a_i, b_j \in R$. But it is clear that g_2 cannot be in $\ker \phi$ unless all of its coefficients are zero. So $g = g_1 \in (uv - 1)$.

[1] $R[[x]] = \{\sum_{i=0}^{\infty} a_i x^i : a_i \in R\}$, where multiplication and addition are defined formally, as what you think they should be. These are purely formal objects: there is no requirement for any kind of convergence.

Take $R \neq 0$ to be any Noetherian ring. There is an infinite descending chain of ideals in $R[x, x^{-1}]$ given by $(x+1) \supsetneq ((x+1)^2) \supseteq ((x+1)^3) \supseteq \ldots$. We need to prove that the containment is strict. To this end suppose that there exists a $k > 0$ such that $((x+1)^k) = ((x+1)^{k+1})$. Then there exists $f \in k[x, x^{-1}]$ such that $(x+1)^k = f(x, x^{-1})(x+1)^{k+1}$. Write $f(x, x^{-1}) = \sum_{m \leq i \leq n} a_i x^i$ with $m \leq n$ integers and $a_m, a_n \neq 0$. Then there is a term of degree $k+n+1$ with coefficient $a_n \neq 0$ on the right-hand side, and thus $m \leq n < 0$ as the left-hand side has only terms of degree less than or equal to k. But then there is a non-zero term of degree $m < 0$ on the right-hand side corresponding to $a_m x^m$. This is not possible, since the left-hand side has no non-zero term with negative degree. We conclude that $f = 0$, but this amounts to a contradiction since $(x+1)^k \neq 0$ since it has non-zero coefficients corresponding to the terms x^k and 1. Hence $R[x, \frac{1}{x}]$ isn't Artinian.

(2) $R[x_1, x_2, \ldots]$ is not Noetherian, as the ideal $(x_1, x_2, \ldots)$ cannot be finitely generated. It is not Artinian (for any choice of $R \neq 0$), since it contains the strictly descending chain $(x_1) \supsetneq (x_1^2) \supsetneq (x_1^3) \supsetneq \ldots$.

(3) $R[[x]]$ is not Artinian (for any choice of $R \neq 0$), since it contains the strictly descending chain $(x) \supsetneq (x^2) \supsetneq (x^3) \supsetneq \ldots$.

$R[[x]]$ is Noetherian, and the proof is a variant of the proof of the Hilbert basis theorem.

To this end suppose I is an ideal of $R[[x]]$. For each integer $n \geq 0$, let

$$I_n := \{a_n : \exists \sum_{i=n}^{\infty} a_i x^i \in I\}.$$

For each n, this is an ideal of R, and by multiplying each power series by x we see that $I_n \subseteq I_{n+1}$ for each n. So by the ascending chain condition, there is M such that $I_n = I_{n+1}$ for all $n \geq M$.

Also, for each $i \leq M$, I_i is finitely generated, so we may fix a finite set $\{a_{i,j}\}_{0 \leq j \leq N}$ of generators for I_i (we take always the same number N of generators by repeating elements if needed). For each $0 \leq i \leq M$ and $0 \leq j \leq N$, fix $f_{i,j} \in I$ such that

$$f_{i,j} = a_{i,j} x^i + \text{ higher order},$$

which exsits by construction of I_i.

We claim that the the ideal J generated by the set $\{f_{i,j}\}_{\substack{0 \leq i \leq M \\ 0 \leq j \leq N}}$ is equal to I. Let $g = \sum_{k=0}^{\infty} b_k x^k \in I$. By construction of I_0, we can find an element $h_0 \in J$ having the same term of order 0 as g: there exists an R-linear combination of $a_{0,0}, \ldots, a_{0,N}$ equal to b_0, and taking h_0 to be the same R-linear combination of $f_{0,0}, \ldots, f_{0,N}$ will do. Similarly, we can find an element $h_1 \in J$ having the same term of order 1 as $g - h_0$. Iterating this procedure, we construct an element $h = h_0 + \cdots + h_{M-1} \in J$ such that $g - h$ has no terms of degree strictly smaller than M.

Now we proceed similarly, but with a slight modification. As before, we can find coefficients $c_{0,0}, \ldots, c_{0,N} \in R$ such that $l_0 = c_{0,0} f_{M,0} + \cdots + c_{0,N} f_{M,N}$ has the same term of order M as $g - h$. Then, we can find $c_{1,0}, \ldots, c_{1,N} \in R$ such that $l_1 = c_{1,0} x f_{M,0} + \cdots + c_{1,N} x f_{M,N}$ (we added a factor x in there to make things of the correct order; in the next step we will need a factor x^2 and so on) has same term of order $M+1$ as $g - h - l_0$. We iterate this procedure indefinitely, and for $0 \leq j \leq N$ define the power

series $c_j = \sum_{k\geq 0} c_{k,j}x^k$, as well as $l = c_0 f_{M,0} + \cdots + c_N f_{M,N} \in J$. One can then show by comparing coefficients that $g - h - l = 0$. As $h, l \in J$, we conclude $g \in J$, and as $g \in I$ was arbitrary, we obtain $I = J$. Hence I is finitely generated, and thus $R[[x]]$ is Noetherian.

(4) $C^0(\mathbb{R})$ is neither Artinian nor Noetherian. To this end define $I_n = \{f \in C(\mathbb{R}) : f(x) = 0 \text{ for all } x \geq n\}$, where $n \in \mathbb{Z}$. It is clear that $I_n \subset I_{n+1}$. We need to show that the containment is strict. To this end, define for example the continuous function f by $f(x) = 0$ for all $x \geq n+1$ and $f(x) = x - (n+1)$ for all $x \leq n+1$, this is a well-defined continuous function $f \in I_{n+1} \setminus I_n$. So $(I_n)_{n\in\mathbb{Z}}$ is a strictly increasing sequence of ideals indexed by $\mathbb{Z}$, showing that $C^0(\mathbb{R})$ is neither Artinian nor Noetherian.

(5) The most efficient solution is the following: it suffices to notice that the dimension of $\mathbb{R}[x]/\left((x-1)^2 x\right)$ as an $\mathbb{R}$-vector space is equal to 3 (the degree of the polynomial), so in particular it is finite. As ideals of $\mathbb{R}[x]/\left((x-1)^2 x\right)$ are in particular $\mathbb{R}$-subspaces, and finite dimensional vector spaces obviously satisfy the ascending and descending chain conditions, we obtain that $\mathbb{R}[x]/\left((x-1)^2 x\right)$ is both Artinian an Noetherian.

□

EPFL - Fall 2023 | Prof. Zs. Patakfalvi
Rings and modules | **Exercises**
Sheet 3 - Solutions

Exercise 1. Computing a presentation of an R module M means explicitly determining an exact sequence of the form $R^{\oplus t} \xrightarrow{\eta} R^{\oplus s} \xrightarrow{\varepsilon} M \longrightarrow 0$. Do the following computations.

(1) Compute a presentation of the $\mathbb{Z}$-module
$$M := \mathbb{Z}(2,9) + \mathbb{Z}(4,3) + \mathbb{Z}(6,8) \subseteq \mathbb{Z} \oplus \mathbb{Z}.$$

(2) Let $R = \mathrm{Mat}_{2\times 2}(\mathbb{Z})$ be the ring of 2×2-matrices over $\mathbb{Z}$. Compute a presentation of the left R-module
$$M := R\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} + R\begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix} \subseteq R.$$

Proof. (1) We define a surjective morphism $\varepsilon : \mathbb{Z}^3 \to M$ by $e_1 \mapsto (2,9)$, $e_2 \mapsto (4,3)$, $e_3 \mapsto (6,8)$. Then we calculate generators of the kernel:
(a_1, a_2, a_3) is mapped to zero if and only if the following two equations are satisfied:
$$2a_1 + 4a_2 + 6a_3 = 0$$
$$9a_1 + 3a_2 + 8a_3 = 0$$
From the first equation we find $a_1 = -2a_2 - 3a_3$. Substituing for a_1 in the second equation gives us $15a_2 = -19a_3$. This implies that $a_2 = -19t$, $a_3 = 15t$ for $t \in \mathbb{Z}$. This gives that $a_1 = -2(-19t) - 3(15t) = -7t$. We conclude that a presentation is given by
$$\mathbb{Z} \xrightarrow{\eta} \mathbb{Z}^3 \xrightarrow{\varepsilon} M \to 0$$
where the first map is $\eta : t \mapsto (-7t, -19t, 15t)$

(2) We define a surjective morphism $\varepsilon : R^2 \to M$ by
$$e_1 \mapsto \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix},\ e_2 \mapsto \begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix}$$
and we are interested in calculating generators of the kernel. I.e., we calculate the solution set of the matrix equation
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} 0 & 3 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 2a + 2\beta & 3\alpha \\ 2c + 2\delta & 3\gamma \end{pmatrix} = 0$$
Hence the kernel consits of the elements $\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right)$ such that $a = -\beta$, $c = -\delta$, $\alpha = \gamma = 0$. I.e., the elements of the form
$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} 0 & -a \\ 0 & -c \end{pmatrix}\right).$$
Thus, the map $\eta : R \to R^2$ defined by
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}\right)$$
gives a presentation $R^{\oplus t} \xrightarrow{\eta} R^{\oplus s} \xrightarrow{\varepsilon} M \to 0$ of M.

□

Exercise 2. Do the following:

(1) Calculate the Smith normal form of the following matrix over $\mathbb{Z}$.

$$\begin{pmatrix} 1 & 9 & 1 \\ -2 & -6 & 0 \\ 2 & -8 & 2 \\ -1 & 1 & 5 \end{pmatrix}$$

(2) (i) Find a direct sum of cyclic $\mathbb{Z}$-modules isomorphic to the $\mathbb{Z}$-module M with generators e_1, e_2, e_3, e_4 and relations

$$\begin{gathered} e_1 - 2e_2 + 2e_3 - e_4 = 0 \\ 9e_1 - 6e_2 - 8e_3 + e_4 = 0 \\ e_1 + 2e_3 + 5e_4 = 0 \end{gathered}$$

[*Hint/Remark:* By definition, M is the quotient of the free $\mathbb{Z}$-module on 4 generators $\bigoplus_{i=1}^{4} \mathbb{Z}e_i$ by the submodule generated by $e_1 - 2e_2 + 2e_3 - e_4$, $9e_1 - 6e_2 - 8e_3 + e_4$ and $e_1 + 2e_3 + 5e_4$. Notice that in the quotient, $e_1, \ldots, e_4$ then satisfy exactly these relations.]

(ii) Explicitly give 'nice' generators of M, in terms of the original generators e_1, e_2, e_3, e_4. Here, $f_1, \ldots, f_s$ are 'nice' generators if the relations they satisfy are generated by relations of the form $m_i f_i = 0$, where $m_1, \ldots, m_s \in \mathbb{Z}$ are integers.

Proof. (1) We follow the algorithm for using row and column operations to produce the Smith normal form of a matrix.

Step 1a: Ensure that the $(1,1)^{\text{th}}$ entry is the principal generator for the ideal generated by the entries of the first row and column. In this case it is already true, so we move on.

Step 1b: Use that property to remove all other entries in the first column by adding a multiple of the first row to subsequent rows. Then remove all other entries in the first row by adding a multiple of the first column to later columns:

$$\begin{pmatrix} 1 & 9 & 1 \\ -2 & -6 & 0 \\ 2 & -8 & 2 \\ -1 & 1 & 5 \end{pmatrix} \to \begin{pmatrix} 1 & 9 & 1 \\ 0 & 12 & 2 \\ 0 & -26 & 0 \\ 0 & 10 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 12 & 2 \\ 0 & -26 & 0 \\ 0 & 10 & 6 \end{pmatrix}$$

Step 2a: Ensure the $(2,2)^{\text{th}}$ entry is the principal generator for the ideal generated by the second row and column. In this case we must swap the second and third columns.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 12 & 2 \\ 0 & -26 & 0 \\ 0 & 10 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 12 \\ 0 & 0 & -26 \\ 0 & 6 & 10 \end{pmatrix}$$

Step 2b: Remove other non-zero entries in the second row and column.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 12 \\ 0 & 0 & -26 \\ 0 & 6 & 10 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 12 \\ 0 & 0 & -26 \\ 0 & 0 & -26 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -26 \\ 0 & 0 & -26 \end{pmatrix}$$

Step 3: Tidy up the resulting matrix to obtain Smith normal form:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -26 \\ 0 & 0 & -26 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -26 \\ 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 26 \\ 0 & 0 & 0 \end{pmatrix}$$

(2) (i) In terms of the generators $e_1, \ldots, e_4$ of M given in the exercise the surjection $\mathbb{Z}^4 \to M$ defined by these generators has kernel K spanned by

$$\begin{pmatrix} 1 \\ -2 \\ 2 \\ -1 \end{pmatrix}, \begin{pmatrix} 9 \\ -6 \\ -8 \\ 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 \\ 0 \\ 2 \\ 5 \end{pmatrix}.$$

So K is the image of the linear map $\mathbb{Z}^3 \to \mathbb{Z}^4$ given by the matrix

$$\begin{pmatrix} 1 & 9 & 1 \\ -2 & -6 & 0 \\ 2 & -8 & 2 \\ -1 & 1 & 5 \end{pmatrix}$$

As discussed in section 4.1 of the lecture notes, multiplying a matrix to the left and right with invertible matrices doesn't change the isomorphism type of the cokernel. Hence M is isomorphic to the cokernel of the Smith normal form of the above matrix, i.e.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 26 \\ 0 & 0 & 0 \end{pmatrix}$$

The cokernel of this matrix is $\overbrace{\mathbb{Z}/\mathbb{Z}}^{=0} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z} \oplus \mathbb{Z}$, so we obtain

$$M \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z} \oplus \mathbb{Z}.$$

(ii) We want to find the elements of M which correspond to the canonical generators of $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z} \oplus \mathbb{Z}$ (i.e. the vectors with precisely one component equal to 1 and 0's everywhere else). Write

$$A := \begin{pmatrix} 1 & 9 & 1 \\ -2 & -6 & 0 \\ 2 & -8 & 2 \\ -1 & 1 & 5 \end{pmatrix}, \quad D := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 26 \\ 0 & 0 & 0 \end{pmatrix}$$

We have found invertible matrices $P \in \mathrm{GL}_4(\mathbb{Z})$ and $Q \in \mathrm{GL}_3(\mathbb{Z})$ such that

$$PAQ = D$$

We can rephrase this as a commutative diagram

$$\begin{array}{ccc} \mathbb{Z}^3 & \xrightarrow{f_A} & \mathbb{Z}^4 \\ {\scriptstyle f_Q}\uparrow & & \downarrow{\scriptstyle f_P} \\ \mathbb{Z}^3 & \xrightarrow[f_D]{} & \mathbb{Z}^4 \end{array}$$

where f_B denotes the linear map associated to the matrix B. We then have that f_P induces an isomorphism

$$\overline{f_P} : M = \operatorname{coker}(f_A) \to \operatorname{coker}(f_D)$$

However, it is clear that a nice basis for $\operatorname{coker}(f_D)$ is given by the classes of $(e_2, \dots, e_4)$, so a nice basis for $M = \operatorname{coker}(f_A)$ is given by the classes of

$$(f_{P^{-1}}(e_2), f_{P^{-1}}(e_3), f_{P^{-1}}(e_4))$$

Thus, we simply have to compute P^{-1} (i.e. the inverse of the operations we did on the rows) and take the last three columns of this matrix as this nice basis. Thus we have to find P, and for this we need to keep track of the *line* operations we performed on A to find the Smith normal form. By revisiting the solution of (1), this gives

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -3 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ -2 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

so

$$P^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 3 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ -1 & 3 & 1 & 1 \end{pmatrix}.$$

Thus, a nice basis is given by the images of $f_1 := e_2 + 3e_4$, $f_2 := e_3 + e_4$ and $f_3 = e_4$. In M, they satisfy the relations $2f_1 = 0$, $26f_2 = 0$ (and f_3 satifies no non-trivial relation).

□

Exercise 3. Let $R = \mathbb{Q}[x]$. Find a direct sum of cyclic R-modules isomorphic to the R-module with generators e_1, e_2 and relations

$$x^2 e_1 + (x+1)e_2 = 0$$
$$(x^3 + 2x + 1)e_1 + (x^2 - 1)e_2 = 0$$

.

Proof. As before, we get a homomorphism $R^2 \to M$ with kernel K, which is given by the image of the map $R^2 \to R^2$ defined by the matrix

$$\begin{pmatrix} x^2 & x^3 + 2x + 1 \\ x + 1 & x^2 - 1 \end{pmatrix}$$

We put this into Smith normal form. We have that the ideal $(x^2, x+1) = 1$ and $1 \times x^2 + (1-x)(1+x) = 1$. The first step in the algorithm therefore tells us to multiply from the left by the matrix

$$\begin{pmatrix} 1 & 1-x \\ -(x+1) & x^2 \end{pmatrix}.$$

We get

$$\begin{pmatrix} 1 & 1-x \\ -(x+1) & x^2 \end{pmatrix}\begin{pmatrix} x^2 & x^3+2x+1 \\ x+1 & x^2-1 \end{pmatrix} = \begin{pmatrix} 1 & 3x+x^2 \\ 0 & -(3x^2+3x+x^3+1) \end{pmatrix}$$

By an elementary column operation this gives:

$$\begin{pmatrix} 1 & 0 \\ 0 & -(x+1)^3 \end{pmatrix}$$

So this means that there is a different set of generators f_1 and f_2 of M that satisfies the relations: $f_1 = 0$ and $(x+1)^3 f_2 = 0$, hence:

$$M \cong \mathbb{Q}[x]\Big/(x+1)^3$$

□

Exercise 4. Give an example of an infinitely generated $\mathbb{Z}$-module which is *not* an (infinite) direct sum of copies of $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ for various choices of n.

Proof. We claim that an example is given by $\mathbb{Q}$ as a $\mathbb{Z}$-module. Indeed, assume for sake the of contradiction that $\mathbb{Q} \cong \mathbb{Z}^{\oplus I} \oplus \bigoplus_i \mathbb{Z}/n_i$ for some set I and some $n_i \geq 2$. Since $\mathbb{Q}$ is torsion-free we see that the sum of $\mathbb{Z}/n_i$ is empty. To prove that $\mathbb{Q}$ is not a free module, we observe that every two cyclic (isomorphic to $\mathbb{Z}$) submodules of $\mathbb{Q}$ intersect. Indeed, let p_1/q_1 and p_2/q_2 be two rational number belonging to two different cyclic modules. Then $p_1p_2 = q_1p_2 \cdot p_1/q_1 = p_1q_2 \cdot p_2/q_2$ is an element in the intersection. Therefore, if $\mathbb{Q}$ is free, then it must be generated by a single element, i.e. $\mathbb{Q} \cong \mathbb{Z}$, which of course is a contradiction.

An other way to show that $\mathbb{Q} \ncong \mathbb{Z}^{\oplus I}$ for any I, is to notice that the endomorphism $(\cdot 2) : a \mapsto 2a$ is surjective on $\mathbb{Q}$, but not on $\mathbb{Z}^{\oplus I}$.

□

Exercise 5. Let $R = \mathbb{Z}[x]$ and consider the matrix $A = \begin{pmatrix} 2 & x \\ 0 & 0 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(R)$.

(1) Show that A is not equivalent to a diagonal matrix. The equivalence that we consider here is the one introduced in the lectures, that is, up to left or right multiplication by an invertible matrix.
(2) Show that the cokernel of the map $A : R^{\oplus 2} \to R^{\oplus 2}$ is isomorphic to a direct sum of cyclic R-modules, but is not isomorphic to an R-module of the form $R^{\oplus m} \oplus \bigoplus_{i=1}^{n} R/(a_i)$ where $a_1, \ldots, a_n \in R \setminus \{0\}$.
(3) Show that $(2, x)$ is not isomorphic to a direct sum of cyclic R-modules.

Proof. (1) We will show that A is not equivalent to a diagonal matrix. Suppose that $A' = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ is equivalent to A. Then $\mathrm{rank}(A') = \mathrm{rank}(A) = 1$ and therefore $\lambda_i = 0$

for $i = 1$ or $i = 2$. By multiplying from the left and the right by the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, we may assume that $\lambda_2 = 0$ (and denote $\lambda = \lambda_1$ from now on). Then there exists invertible matrices $S = \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix}$ and $T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix}$ such that $SA = A'T$, i.e.

$$\begin{pmatrix} 2s_{11} & xs_{11} \\ 2s_{21} & xs_{21} \end{pmatrix} = \begin{pmatrix} \lambda t_{11} & \lambda t_{12} \\ 0 & 0 \end{pmatrix}$$

Since $\mathbb{Z}[x]$ is a UFD, the equality $2s_{11} = \lambda t_{11}$ and $xs_{11} = \lambda t_{12}$ implies that there exists some $t' \in \mathbb{Z}[x]$ such that $t_{11} = 2t'$ and $t_{12} = xt'$. Since the units of $\mathbb{Z}[x]$ are precisely ± 1, we obtain $\pm 1 = \det(T) = t_{11}t_{22} - t_{12}t_{21} = 2t't_{22} - xt't_{21}$. This implies that the ideal $(2, x)$ contains 1, a contradiction.

(2) Let M be the cokernel of $A : \mathbb{Z}[x]^2 \to \mathbb{Z}[x]^2$. It is straightforward to see that $M \cong \mathbb{Z}[x]/(2,x) \oplus \mathbb{Z}[x]$, which is a direct sum of cyclic R-modules. Suppose by contradiction that there exist $a_1, ..., a_n \in \mathbb{Z}[x] \setminus \{0\}$ and $m \geq 0$ such that

$$\mathbb{Z}[x]/(2,x) \oplus \mathbb{Z}[x] \cong (\mathbb{Z}[x])^{\oplus m} \oplus \bigoplus_{i=1}^{n} \mathbb{Z}[x]/(a_i).$$

Then the torsion-submodules of the LHS and RHS must be isomorphic, i.e.

$$\mathbb{Z}[x]/(2,x) \cong \bigoplus_{i=1}^{n} \mathbb{Z}[x]/(a_i).$$

But thus the annihilators of the LHS and the RHS must agree. For the LHS the annihilator is $(2, x)$, while for the RHS it is $\bigcap_{i=1}^{n}(a_i)$. But as $\mathbb{Z}[x]$ is a UFD, the latter is a principal ideal (generated by the least common multiple of the a_i's), while the former isn't principal. This is the desired contradiction.

(3) Suppose by contradiction that $\varphi : (2, x) \xrightarrow{\cong} \bigoplus_{i \in I} M_i$ is an isomorphism, where $\{M_i\}_{i \in I}$ is a family of cyclic R-modules. For all $i \in I$, let $f_i \in (2, x)$ be such that $\varphi(f_i)$ is a generator of M_i. Then $f_i f_j$ is in the intersection $\varphi^{-1}(M_i) \cap \varphi^{-1}(M_j)$, while the intersection $M_i \cap M_j$ inside $\bigoplus_{i=1}^{n} M_i$ is equal to 0. Therefore all but one of the M_i's must be trivial. But then $(2, x)$ is principal, which is a contradiction as well.

□

Exercise 6. Set $M = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and let $\alpha : M \to M$ be an isomorphism.

(1) Show that $\alpha(0 \times \mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$, show in general that if N is an R-module then an automorphism ϕ of N takes $\mathrm{Tors}(N)$ to $\mathrm{Tors}(N)$ bijectively.

(2) Show that $\alpha(\mathbb{Z} \times 0)$ is not equal necessarily to $\mathbb{Z} \times 0$

[*Remark:* The torsion submodule $\mathrm{Tors}_R(M)$ of an R-module M (or simply $\mathrm{Tors}(M)$ if the ring is clear from the context) was used to prove the unicity of the decomposition of a finitely generated module over a PID into cyclic modules given by Theorem 4.3.3 of the lecture notes.]

Proof. (1) Since $\mathrm{Tors}(\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) = 0 \times \mathbb{Z}/2\mathbb{Z}$ it is sufficient to show the general statement that an automorphism ϕ of N takes $\mathrm{Tors}(N)$ to $\mathrm{Tors}(N)$ bijectively. To this end, suppose $rn = 0$, then $0 = r\phi(n)$ and hence $\phi(\mathrm{Tors}(N)) \subset \mathrm{Tors}(N)$, converserly, suppose $r\phi(n) = 0$, then $rn \in \mathrm{Ker}(\phi)$, but ϕ is injective hence $rn = 0$.

(2) Let $(1,0) \mapsto (1,1)$

□

Exercise 7. Show that an exact sequence

$$0 \longrightarrow M \longrightarrow N \longrightarrow L \longrightarrow 0$$

of R-modules induces an exact sequence

$$0 \longrightarrow \mathrm{Tors}(M) \longrightarrow \mathrm{Tors}(N) \longrightarrow \mathrm{Tors}(L) \ ,$$

but not necessarily an exact sequence

$$0 \longrightarrow \mathrm{Tors}(M) \longrightarrow \mathrm{Tors}(N) \longrightarrow \mathrm{Tors}(L) \longrightarrow 0 \ .$$

Proof. It is clear that any homomorphism ϕ takes torsion to torsion, hence the sequence is well defined. Since restriction of an injection obviously is injective it is sufficient to check exactness in the middle.
Let $f : M \to N$ and $g : N \to L$ be the morphisms in question. Since $g \circ f = 0$, the same is true for the restriction to any submodules. Let $n \in \mathrm{Ker}(\mathrm{Tors}(g))$, there exists an $m \in M$ such that $f(m) = n$, we need to show that $m \in \mathrm{Tors}(M)$. Since there exists $r \in R$ not zero-divisor such that $0 = rn = f(rm)$ we have $rm \in \mathrm{Ker}(f)$, but f is injective. Hence $rm = 0$ and $m \in \mathrm{Tors}(M)$.

We have a surjection of $\mathbb{Z}$-modules $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, but it does not induce a surjection on torsion submodules. □

Exercise 8. Let $M \in \mathrm{Mat}(n \times n, k)$ for a field k. Show that there is a basis with respect to which M is block diagonal with blocks of the form

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

Hint: M acts naturally on some n-dimensional k-vector space V. Consider V as a $k[x]$-module via $f \cdot v = f(M)(v)$ and use the classification of finitely generated modules over a PID.

Proof. As k is a field, $k[x]$ is a PID. Also, V is finite dimensional over k, so it is finitely generated (by a k-basis) over $k[x]$. Therefore the structure theorem says that $V \cong k[x]^{\oplus l} \oplus \bigoplus_{i=0}^{m} k[x]/(f_i)$ for some monic polynomials f_i of degree d_i. As V is finite dimensional over $k \subset k[x]$, and $k[x]$ itself is not, we see that $l = 0$. Decompose V into $\oplus_{i=0}^{m} V_i$ where $V_i \cong k[x]/(f_i)$, noting that V_i is d_i-dimensional as a k-vector space. Note that M preserves each V_i as it is a sub-$k[x]$-module of V. Thus if we choose a basis of V which is a union of bases of the V_i, the matrix of ϕ is block diagonal with blocks corresponding to the V_i. We now show that if we choose these bases in a particular way, we get the required form.

The action of M on V_i corresponds under this isomorphism to the k-linear map "multiplication by x" on $k[x]/(f_i)$. We choose the basis of V_i to be the elements which correspond via the isomorphism to the elements $\{1, x, ..., x^{d_i-1}\}$ of $k[x]/(f_i)$. It is clear that these span, and are linearly independent. If we define a_i by $f_i(x) = x^{d_i} - \sum_{j=0}^{d_i-1} a_j x^j$ then the matrix of the linear map given by multiplication by x on $k[x]/(f_i)$ has the required form. □

EPFL - Fall 2023	Prof. Zs. Patakfalvi
Rings and modules	**Exercises**
Sheet 4 - Solutions	

There was one bonus exercise on this problem sheet. The exercise was denoted by the symbol ♠ next to the exercise number.

Exercise 1. Let R be a commutative ring, and let M be an R-module.

(1) Show that $\mathrm{Hom}_R(M, -)$ is *left exact.* That is, for any short exact sequence of R-modules

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0 \ ,$$

there is an induced exact sequence

$$0 \longrightarrow \mathrm{Hom}_R(M, N') \longrightarrow \mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(M, N'') \ .$$

(2) Give an example of a ring R and an R-module M such that $\mathrm{Hom}_R(M, -)$ is not *right exact.* That is, give an example of a surjection of R-modules $N \twoheadrightarrow N''$ such that the induced morphism $\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N'')$ is not surjective.

Proof. (1) Suppose that

$$0 \longrightarrow N' \xrightarrow{i} N \xrightarrow{s} N'' \longrightarrow 0 \ ,$$

is exact. We want to show that

$$0 \longrightarrow \mathrm{Hom}_R(M, N') \xrightarrow{i\circ -} \mathrm{Hom}_R(M, N) \xrightarrow{s\circ -} \mathrm{Hom}_R(M, N'') \ ,$$

is exact. Let $\phi \in \mathrm{Hom}_R(M, N')$ and suppose it is mapped to 0, i.e. $i \circ \phi : M \to N'$ is the zero morphism. Since i is injective this implies that $\phi = 0$. So we get exactness at $\mathrm{Hom}_R(M, N')$. To check exactness in the middle, observe that since $s \circ i = 0$ we have the containment $\mathrm{im}(i \circ -) \subset \ker(s \circ -)$. Let $\phi \in \mathrm{Hom}_R(M, N)$ be such that $s \circ \phi : M \to N''$ is the zero morphism. Then $\phi(M) \subset \ker(s) = i(N')$, and therefore ϕ factors through $i : N' \to N$.

(2) Let $R = \mathbb{Z}$. Consider the surjection $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ and let $M = \mathbb{Z}/2\mathbb{Z}$. The induced morphism

$$\mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}\right) \to \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}\right)$$

can not be surjective since the first group is zero, but the other is not.

□

Exercise 2. Let $R = k[x, y]$ where k is a field. Extend the complex below to a free resolution $F_\bullet$ of the R-module $k \cong R/(x, y)$. Then compute $\mathrm{Ext}^i_{F_\bullet}(k, R)$ for each i, and note that you get the same as for the resolutions in Example 5.3.9 in the printed course notes.

$$R \oplus R \oplus R \longrightarrow R \longrightarrow k \longrightarrow 0$$

The first morphism is defined by sending a basis to the following elements:

$$(1, 0, 0) \mapsto x, (0, 1, 0) \mapsto y, (0, 0, 1) \mapsto x + y$$

and the second morphism is the natural surjection $R \to k$.

[*Remark:* This is an example of the fact that the Ext-modules $\mathrm{Ext}^i_{F_\bullet}(M, N)$ don't depend on the free resolution $F_\bullet$ of M.]

Proof. The kernel of the first map is the set of those $(a,b,c) \in R^{\oplus 3}$ such that $0 = ax + by + c(x+y) = (a+c)x + (b+c)y$. As R is UFD this means that $a + c = yd$ and $b + c = -xd$ for some $d \in R$. That is, we have $a = yd - c$ and $b = -xd - c$. Equivalently $a = yd - e$ and $b = -xd - e$ and $c = e$ (where e and d are arbitrary elements of R). From here one can read off the following extension to a free resolution:

$$0 \longrightarrow R \oplus R \longrightarrow R \oplus R \oplus R \longrightarrow R \longrightarrow k \longrightarrow 0$$

$$(1,0,0) \longmapsto x$$

$$(0,1,0) \longmapsto y$$

$$(0,0,1) \longmapsto x + y$$

$$(1,0) \longmapsto (1,1,-1)$$

$$(0,1) \longmapsto (y,-x,0)$$

Upon applying $\mathrm{Hom}_R(\_, R)$ to the projective resolution determined by the complex above (removing k) and identifying $R^{\oplus n} \cong \mathrm{Hom}_R(R^{\oplus n}, R)$, we get

$$0 \longleftarrow R \oplus R \longleftarrow R \oplus R \oplus R \longleftarrow R \longleftarrow 0$$

$$(x,y,x+y) \longmapsfrom 1$$

$$(1,y) \longmapsfrom (1,0,0)$$

$$(1,-x) \longmapsfrom (0,1,0)$$

$$(-1,0) \longmapsfrom (0,0,1)$$

(Notice that on the level of matrices, the morphisms here are obtained from the morphisms above by transposing the matrix.) We calculate the cohomology of this complex, The first map is injective, hence $H^0 = 0$, i.e., $\mathrm{Ext}^0_{F_\bullet}(k,R) = 0$. The solution to the system

$$\begin{aligned} r_1 + r_2 - r_3 &= 0 \\ r_1 y - r_2 x &= 0 \end{aligned}$$

can easily seen to be $r_1 = rx, r_2 = ry, r_3 = r(x+y)$ for some $r \in R$. Therefore the above complex is exact in degree one and $\mathrm{Ext}^1_{F_\bullet}(k,R) = 0$. Finally, the image of the last map is $R \oplus (x,y)$ (because $r_1 y - r_2 x$ runs through (x,y) for r_1, r_2 running through R and we can use r_3 to get any element in the first coordinate). Thus the co-kernel is $(R \oplus R)\big/(R \oplus (x,y)) \cong R/(x,y) \cong k$. Therefore, $\mathrm{Ext}^2_{F_\bullet}(k,R) = k$. This agrees with the values for these groups given by the resolutions in Example 5.3.9 in the printed course notes. □

Exercise 3. Let $0 \to M \xrightarrow{i} Z \xrightarrow{p} N \to 0$ be a short exact sequence of R-modules.

(1) A *section* of p is a morphism $s\colon N \to Z$ such that $p \circ s = \mathrm{id}_N$. Show that p admits a section if and only if there exists an isomorphism $\Phi : M \oplus N \xrightarrow{\cong} Z$ and a commuting diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{i} & Z & \xrightarrow{p} & N & \longrightarrow & 0 \\ & & \| & & \uparrow{\scriptstyle \Phi} & & \| & & \\ 0 & \longrightarrow & M & \xrightarrow{e} & M \oplus N & \xrightarrow{\pi} & N & \longrightarrow & 0 \end{array}$$

(2) A *section* of i is a morphism $q\colon Z \to M$ such that $q \circ i = \mathrm{id}_M$. Show that i admits a section if and only if there exists an isomorphism $\Psi : Z \xrightarrow{\cong} M \oplus N$ and a commuting diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{i} & Z & \xrightarrow{p} & N & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \Psi} & & \| & & \\ 0 & \longrightarrow & M & \xrightarrow{e} & M \oplus N & \xrightarrow{\pi} & N & \longrightarrow & 0 \end{array}$$

We say that a short exact sequence satisfying any of these conditions is split exact.

Proof. (1) Suppose that we have a commuting diagram as the one described in the exercise. Define $s : N \to Z$ by $N \xrightarrow{e_N} M \oplus N \overset{\Phi}{\cong} Z$ where e_N is the canonical inclusion. We need to check that $p \circ s$ is equal to the identity on N. By the commutativity of the diagram $p = \pi \circ \Phi^{-1}$ and hence $p \circ s = \pi \circ \Phi^{-1} \circ \Phi \circ e_N = \pi \circ e_N = \mathrm{id}_N$.
Conversely, suppose that $s : N \to Z$ is a section of p. Define $\Phi : M \oplus N \to Z$ by $\Phi(m,n) = i(m) + s(n)$. Then for any $z \in Z$, let $n = p(z)$. Now $z - s(n)$ is in $\ker p = \mathrm{im}\, i$, so let m be a preimage under i. Then

$$\Phi(m,n) = i(m) + s(n) = z - s(n) + s(n) = z,$$

so as $z \in Z$ was arbitrary, Φ is surjective. On the other hand, if $\Phi(m,n) = 0$, then $0 = p \circ \Phi(m,n) = n$ and thus $i(m) = 0$ which also gives $m = 0$. Hence Φ is an isomorphism. As also $\Phi \circ e = i$ and $p \circ \Phi = \pi$, the diagram commutes.

(2) If the diagram exists we can define q as the composition $Z \overset{\Psi}{\cong} M \oplus N \xrightarrow{\pi_M} M$ where π_M is the canonical projection. We need to check that $q \circ i$ is equal to the identity on M. By the commutativity of the diagram $i = \Psi^{-1} \circ e$ and hence $q \circ i = \pi_M \circ \Psi \circ \Psi^{-1} \circ e = \pi_M \circ e = \mathrm{id}_M$.
Conversely, suppose that $q : Z \to M$ is a section of i. Now define $\Psi : Z \to M \oplus N$ by $\Psi(z) = (q(z), p(z))$. Let $(m,n) \in M \oplus N$ be arbitrary, then by surjectivity of p there

exists $z \in Z$ such that $p(z) = n$. As $q \circ i = \mathrm{id}_M$ and $p \circ i = 0$ we then have

$$\Psi(z + i(m - q(z))) = (q(z + i(m - q(z))), p(z + i(m - q(z)))) = (q(z) + m - q(z), n) = (m, n).$$

Hence Ψ is surjective. On the other hand, if we suppose $\Psi(z) = 0$, then in particular $z \in \ker p = \mathrm{im}\, i$, so we can write $z = i(m)$ for some $m \in M$. But then $0 = q(z) = m$, so in fact $m = 0$ and thus $z = 0$. Hence Ψ is an isomorphism. As $\Psi \circ i = e$ and $\pi \circ \Psi = p$, we then obtain that the diagram commutes.

□

Exercise 4. ♠ Let R be a commutative ring. The *projective dimension* of an R-module M is the smallest integer $n \geq 0$ such that there exists a projective resolution

$$0 \to P_n \to P_{n-1} \to \cdots \to P_0$$

of M. We write $\mathrm{projdim}(M) = n$, and if no finite projective resolution exists, this number is by definition ∞.

As this exercise shows, Ext-groups help us find this number.

(1) Show that an R-module M is projective if and only for any R-module N, $\mathrm{Ext}^i(M, N) = 0$ for all $i > 0$.
Hint: Using long exact sequence of Ext*-groups (see Theorem 5.5.6 in the notes) can be useful.*

(2) More generally, show that if $M \neq 0$, then M has projective dimension $n \geq 0$ if and only if the two following conditions hold:
- for all R-module N, $\mathrm{Ext}^i(M, N) = 0$ for all $i > n$;
- there exists an R-module M' such that $\mathrm{Ext}^n(M, M') \neq 0$.

(3) As an example, show that the $k[x, y]$-module $M := k[x, y]/(x, y)$ has projective dimension 2.
Note that it would be a mess to show directly that for any surjection $f : P \to M$ from a projective module P, $\ker(f)$ *is not projective!*

Proof. (1) It is immediate by the definition of Ext-groups that if M is projective, then $\mathrm{Ext}^i(M, N) = 0$ for any R-module N. On the other hand, assume that the above vanishing of Ext-groups hold, and consider a short exact sequence

$$0 \to K \xrightarrow{a} R^n \xrightarrow{b} M \to 0$$

for some $n \geq 0$ (in other words, choose generators of M).

Applying the functor $\mathrm{Hom}(-, K)$, applying the long exact sequence and using that $\mathrm{Ext}^1(M, K) = 0$ gives

$$0 \to \mathrm{Hom}(M, K) \to \mathrm{Hom}(R^n, K) \to \mathrm{Hom}(K, K) \to 0,$$

so in particular $\mathrm{Hom}(R^n, K) \to \mathrm{Hom}(K, K)$ is surjective. Let $f : R^n \to K$ be a morphism sent to $id : K \to K$. By definition, $f \circ a = id$, so our exact sequence is split. By Exercise 3 of this sheet, we conclude the existence of an isomorphism $R^n \cong M \oplus K$. In particular, M is projective (it is a direct summand of a free module).

(2) Note that if M has projective dimension n, then again by definition of the Ext-groups, $\mathrm{Ext}^i(M, N) = 0$ for all $i > n$. Let us shôw by induction on n that there exists some R-module M' such that $\mathrm{Ext}^n(M, M') \neq 0$.

If $n = 0$, then we can take $M' = M$. Furthermore, note that in the proof, we only used the vanishing of all groups Ext^1 to deduce that M was projective, so we also know

the result for $n = 1$. Thus, assume that $n \geq 2$, and that we know the result for $n - 1$. By definition, there exists a short exact sequence

$$0 \to K \to P_0 \to M \to 0$$

such that K has projective dimension $n - 1$ and P_0 is projective. Indeed, if

$$0 \to P_n \to P_{n-1} \to \cdots \to P_1 \xrightarrow{f} P_0$$

is a projective resolution of minimal length of M, then $K = \text{Image}(f)$ works. Note that $K \neq 0$, as otherwise M would be projective, contradicting $n \geq 1$.

By the induction assumption, there exists K' such that $\text{Ext}^{n-1}(K, K') \neq 0$. Applying $\text{Hom}(-, K')$ to our exact sequence and taking the long exact sequence in Ext-groups gives

$$\cdots \to \text{Ext}^{n-1}(P_0, K') \to \text{Ext}^{n-1}(K, K') \to \text{Ext}^n(M, K') \to \text{Ext}^n(P_0, K') \to \dots$$

Since $n \geq 2$, we know that $\text{Ext}^n(P_0, K') = 0 = \text{Ext}^{n-1}(P_0, K')$ by the previous point, so we conclude this part of the proof.

Now, assume that the two conditions in the bullet hold for an R-module M, and let us show that M has projective dimension n. Again, if $n = 0$, the result holds by the first point, so assume that we know the result for $n - 1$, and again consider a short exact sequence

$$0 \to K \to P_0 \to M \to 0$$

with P_0 projective. For any R-module M' and $i > 0$, we know by the first point that $\text{Ext}^i(P_0, M') = 0$ so the long exact sequence in Ext-groups gives isomorphisms

$$\text{Ext}^i(K, M') \cong \text{Ext}^{i+1}(M, M')$$

for any $i \geq 1$. Thus, by induction, K has projective dimension at most $n-1$, so M has projective dimension at most n. However, since $\text{Ext}^n(M, M') \neq 0$ for some R-module M', we know by what we already proved that the projective dimension of M is at least n, concluding the proof.

(3) By Example 5.3.9 in the lecture notes, we know that there exists a projective resolution of M of length 2, so the projective dimension of M is at most 2. However, we know by the same example that

$$\text{Ext}^2(M, k[x, y]) \neq 0,$$

so we are done by the previous point.

□

Exercise 5. Consider the ring $\mathbb{Z}[\sqrt{-5}]$.

(1) Is the ideal $(2, 1 + \sqrt{-5})$ a free $\mathbb{Z}[\sqrt{-5}]$-module?
[*Hint:* Consider the element $6 \in \mathbb{Z}[\sqrt{-5}]$.]

(2) Prove that $(2, 1 + \sqrt{-5})$ is a projective $\mathbb{Z}[\sqrt{-5}]$-module.
[*Hint*: Prove that $(2, 1+\sqrt{-5})$ is projective by showing that it is a direct summand of a free module. To do this, define the obvious surjection $p : \mathbb{Z}[\sqrt{-5}]^2 \to (2, 1 + \sqrt{-5})$ and examine the assignment $s : (2, 1+\sqrt{-5}) \to \mathbb{Z}[\sqrt{-5}]^2$ defined by $s(x) = 2xe_1 - \frac{1-\sqrt{-5}}{2}xe_2$.]

Proof. (1) The $\mathbb{Z}[\sqrt{-5}]$-module $I = (2, 1+\sqrt{-5})$ is not free. Suppose the contrary, then $I \cong \mathbb{Z}[\sqrt{-5}]^{\oplus\Omega}$ for some index set Ω. As I can be generated by 2 elements, we must have $|\Omega| \leq 2$ (to see this, try to prove that a generating set of $R^{\oplus n}$ always contains at least n elements (Hint: you know this for fields, so try to reduce to this case by dividing by a maximal ideal)).
Suppose that $|\Omega| = 2$. Then we have a surjection $\mathbb{Z}[x]^{\oplus 2} \twoheadrightarrow I \cong \mathbb{Z}[x]^{\oplus 2}$ given by mapping $(1,0)$ to 2 and $(0,1)$ to $1+\sqrt{-5}$. But then by Exercise 4 on Sheet 2, this surjection must be an isomorphism, which contradicts the fact that $(3, -1+\sqrt{-5}) \in \mathbb{Z}[x]^{\oplus 2}$ is mapped to 0.
So we must have $|\Omega| = 1$. We first show that $1 \notin I$ by proving that for all elements $a + b\sqrt{-5} \in I$ we have that $a \equiv b \bmod 2$. We calculate $(r_1 + r_2\sqrt{-5})(1+\sqrt{-5}) = r_1 - 5r_2 + (r_1 + r_2)\sqrt{-5}$. We have that $r_1 - 5r_2 \equiv r_1 + r_2 \bmod 2$. Obviously $a \equiv b \bmod 2$ for all elements $a + b\sqrt{-5} \in (2)$ hence it is sufficient to note that if $r_1 + r_2\sqrt{-5}$ and $s_1 + s_2\sqrt{-5}$ are such that $r_1 \cong r_2 \bmod 2$ and $s_1 \cong s_2 \bmod 2$ then $(r_1 + r_2\sqrt{-5}) + (s_1 + s_2\sqrt{-5}) = r_1 + s_1 + (r_2 + s_2)\sqrt{-5}$ satisfies $s_1 + r_1 \cong s_2 + r_2 \bmod 2$.
Now suppose that $(a + b\sqrt{-5}) = I$. For any $\alpha = \alpha_1 + \alpha_2\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ write $N(\alpha) = \alpha\bar{\alpha} \in \mathbb{Z}$ where $\bar{\alpha} = \alpha_1 - \alpha_2\sqrt{-5}$. Then N is multiplicative, so $N(a + b\sqrt{-5}) = a^2 + 5b^2$ divides $N(2) = 4$ and $N(1+\sqrt{-5}) = 6$. This implies $N(a + b\sqrt{-5})$ is either one or two. The equation $a^2 + 5b^2 = 2$ is easily seen to have no integer solutions. If $N(a + b\sqrt{-5}) = 1$ then $1 \in I$ which we have already proven not to be the case, hence the claim follows.

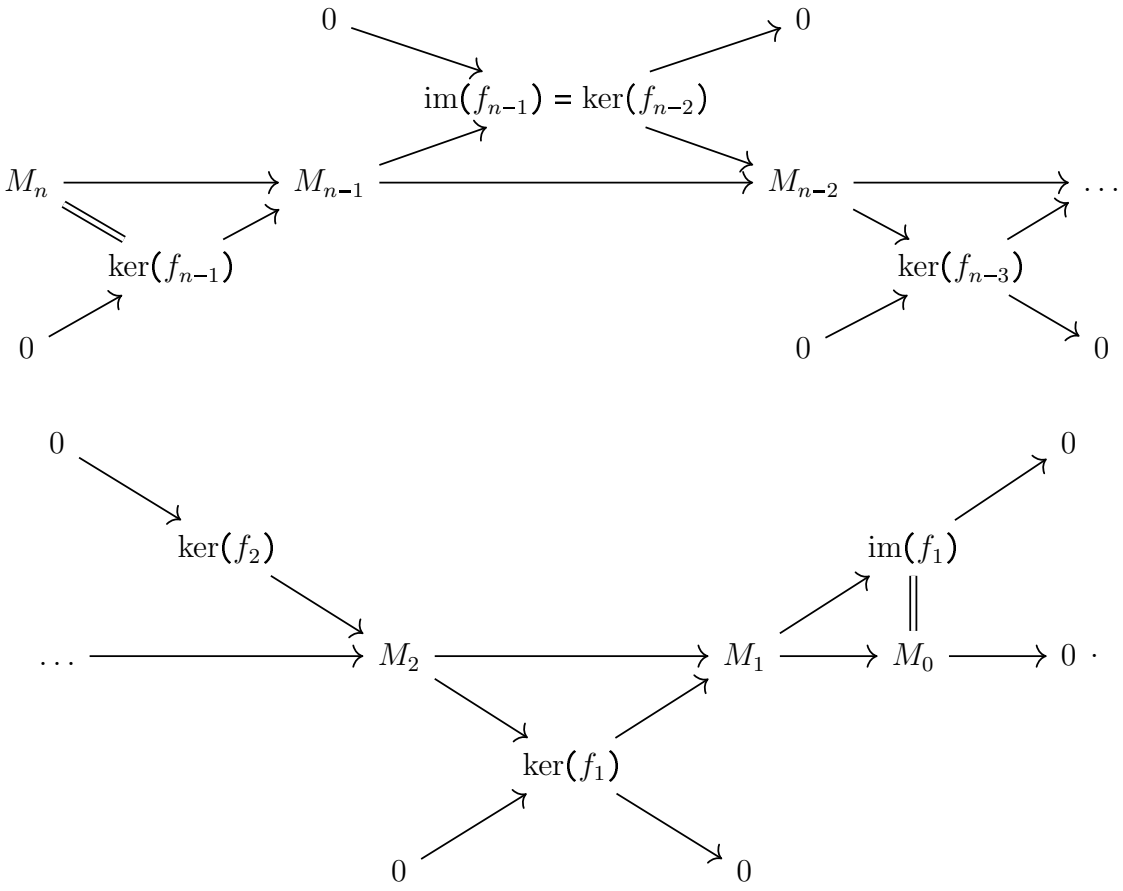
(2) Following the suggestion in the exercise we define $p : \mathbb{Z}[\sqrt{-5}]^2 \to (2, 1+\sqrt{-5})$ by mapping the canonical basis e_1, e_2 to $e_1 \mapsto 2$ and $e_2 \mapsto 1+\sqrt{-5}$. If we can prove that p admits a section s we are done by Exercise 3 on this sheet.
Claim: for all $x \in I$ we have that $\frac{1-\sqrt{-5}}{2}x \in \mathbb{Z}[\sqrt{-5}]$.
Proof of claim: write $x = r_1 2 + r_2(1+\sqrt{-5})$, then $\frac{1-\sqrt{-5}}{2}x = (1-\sqrt{-5})r_1 + 3r_2$. Hence the assignment s given in the hint is well-defined. Moreover, we have that $p(s(x)) = p(2xe_1 - \frac{1-\sqrt{-5}}{2}xe_2) = 4x - 3x = x$.

□

Exercise 6. Prove the following.

(1) If $0 \longrightarrow M_n \longrightarrow \ldots \longrightarrow M_0 \longrightarrow 0$ is an exact sequence of finitely generated modules over an Artinian and Noetherian ring R, then $0 = \sum_{i=0}^{n}(-1)^i \operatorname{length} M_i$.
(2) Let $R = k[\varepsilon]$ denote (as usual) the quotient $k[x]/(x^2)$ where k is a field (and ε is the class of x). Let M be the R-module $R/(\varepsilon)$. Show that M has no finite resolution by finitely generated free modules.
(3) In general if R is Artinian and Noetherian, and $\operatorname{length} R \nmid \operatorname{length} M$, prove that M has no finite resolution by finitely generated free modules.
(4) Prove that over a PID every finitely generated module has a finite free resolution.

Proof. (1) This follows from the additivity of lengths proven in a previous exercise (Exercise 2.4) after slicing the long exact sequence into short exact sequences. Since $\ker(f_i) = \operatorname{im}(f_{i+1})$ for $1 \leq i \leq n-1$ we get an exact commuting diagram as follow:



By the additivity of lengths on short exact sequences, we have $\mathrm{length}(M_0) = \mathrm{length}(M_1) - \mathrm{length}(\ker(f_1))$ and $\mathrm{length}(\ker(f_i)) = \mathrm{length}(M_{i+1}) - \mathrm{length}(\ker(f_{i+1}))$ for $1 \leq i \leq n-2$. Finally $\mathrm{length}(\ker(f_{n-1}) = \mathrm{length}(M_n)$. These equations combined yield then the formula.

(2) Suppose that

$$0 \longrightarrow R^{\oplus n_k} \xrightarrow{f_k} \ldots \xrightarrow{f_2} R^{\oplus n_1} \xrightarrow{f_1} k \longrightarrow 0$$

is a finite length free resolution of k. Then by the previous exercise and by Example 3.2.9 of the lecture notes we have $1 = \sum_{i=1}^{k} (-1)^{i+1} 2n_i$, but this is impossible since the right-hand side is an even number.

(3) Suppose that

$$0 \longrightarrow R^{\oplus n_k} \xrightarrow{f_k} \ldots \xrightarrow{f_2} R^{\oplus n_1} \xrightarrow{f_1} M \longrightarrow 0$$

is a finite length free resolution of M. Then by the previous exercise we have $\mathrm{length}(M) = \sum_{i=1}^{k} (-1)^{i+1} \mathrm{length}(R) n_i$. Since $\mathrm{length}(R)$ divides the right hand side the result follows.

(4) This follows from the structure theorem for finitely generated modules over principal ideal domains. Let $R^{\oplus s} \twoheadrightarrow M$ be a surjection, which exists as M is finitely generated. As R is Noetherian, the kernel K is finitely generated too. But then as R is a domain,

K can't have non-trivial torsion elements. From the classification of finitely generated modules, we conclude that $K \cong R^{\oplus t}$ for some t. Hence we obtain an exact sequence

$$0 \to R^{\oplus t} \to R^{\oplus s} \to M \to 0$$

which is thus a finite free resolution of M.

□

Exercise 7. In this exercise R is an integral domain which is not a field; in particular it is commutative. Recall the definition of an R-module M being divisible: for all $m \in M$ and $r \in R \setminus \{0\}$ there exists an $n \in M$ such that $rn = m$. In other words, M is divisible if and only if multiplication by r on M is surjective for every $r \in R \setminus \{0\}$.

(1) Show that a non-trivial free R-module is not divisible.
(2) Show that $\mathbb{Q}$ is not a projective $\mathbb{Z}$-module, or in general $\mathrm{Frac}(R)$ is not a projective R-module.
[*Hint:* Define the notion of submodule of divisible elements, and refine (1) by showing that it is trivial for free R-modules.]
(3) From now on, let M, N be R-modules. Let $P_\bullet$ be a projective resolution of M and let $\psi : N \to N$ be the R-module homomorphism corresponding to multiplication by a fixed $r \in R$. Show that ψ induces a co-chain morphism $\mathrm{Hom}_R(P_\bullet, N) \to \mathrm{Hom}_R(P_\bullet, N)$. By passing to cohomology, one obtains a map $\mathrm{Ext}^i_R(M, \psi) : \mathrm{Ext}^i_R(M, N) \to \mathrm{Ext}^i_R(M, N)$. Show that $\mathrm{Ext}^i_R(M, \psi)$ is still just multiplication by r on $\mathrm{Ext}^i_R(M, N)$. In particular, it is independent of the projective resolution.
[*Remark:* One can in fact perform an analogous construction for *any* R-module homomorphism $\psi : N \to L$, and thus obtain a map $\mathrm{Ext}^i_R(M, \psi) : \mathrm{Ext}^i_R(M, N) \to \mathrm{Ext}^i_R(M, L)$, which as in Remark 5.4.26 of the printed course notes is independent of the projective resolution. This makes also $\mathrm{Ext}^i_R(M, -)$ a functor, while in the course we only saw that $\mathrm{Ext}^i_R(-, N)$ is a functor.]
(4) Fix $r \in R$, and let $\phi : M \to M$ be the multiplication by r. Show that $\mathrm{Ext}^i_R(\phi, N)$, as in Definition 5.4.25 of the course notes, is also just the multiplication by r on $\mathrm{Ext}^i_R(M, N)$.
(5) Show that, despite $\mathrm{Frac}(R)$ being not a projective R-module, if N is an R-module such that $\mathrm{Ann}(N) \neq 0$, then $\mathrm{Ext}^i_R(\mathrm{Frac}(R), N) = 0$ for all $i \geq 0$ (note that for P projective, $\mathrm{Ext}^i_R(P, N) = 0$ for all $i > 0$ by definition).

Proof. (1) In view of the hint in the second point, for an R-module M we define

$$\mathrm{Div}(M) := \{m \in M \mid \forall r \in R \setminus \{0\}\ \exists n \in N : \ rn = m\}.$$

One checks easily that this is in fact a submodule of M, and by definition it is clear that M is divisible if and only if $M = \mathrm{Div}(M)$. Now consider a free module $R^{\oplus\Omega}$ where Ω is non-empty. As R is not a field, there exists $r \in R \setminus \{0\}$ which is not a unit. Let $(x_\alpha)_{\alpha\in\Omega} \in \mathrm{Div}(R^{\oplus\Omega})$ and suppose that there is an $\beta \in \Omega$ such that $x_\beta \neq 0$. By definition, we find (y_α) such that $rx_\beta \cdot (y_\alpha) = (x_\alpha)$. In particular we obtain $rx_\beta y_\beta = x_\beta$, which implies that r is a unit, contradiction. Thus $\mathrm{Div}(R^{\oplus\Omega}) = 0$.
(2) We directly prove the general statement. If by contradiction $\mathrm{Frac}(R)$ is projective, then it is a direct summand of a free module F. But then as $\mathrm{Frac}(R)$ is divisible, it injects into $\mathrm{Div}(F)$, which by (1) is trivial. This is a contradiction.

(3) Consider the diagram

$$\begin{array}{ccccccccc}
\cdots & \longleftarrow & \mathrm{Hom}_R(P_2,N) & \xleftarrow{-\circ p_2} & \mathrm{Hom}_R(P_1,N) & \xleftarrow{-\circ p_1} & \mathrm{Hom}_R(P_0,N) & \longleftarrow & 0 \\
 & & \downarrow{\scriptstyle \psi\circ -} & & \downarrow{\scriptstyle \psi\circ -} & & \downarrow{\scriptstyle \psi\circ -} & & \\
\cdots & \longleftarrow & \mathrm{Hom}_R(P_2,N) & \xleftarrow[-\circ p_2]{} & \mathrm{Hom}_R(P_1,N) & \xleftarrow[-\circ p_1]{} & \mathrm{Hom}_R(P_0,N) & \longleftarrow & 0
\end{array}$$

It commutes because post-composition commutes with pre-composition. Notice also that $\psi \circ -$ is just multiplication by r on $\mathrm{Hom}_R(P_i, N)$. Now to get the maps induced on cohomology, we restrict and corestrict to the kernels of the horizontal maps, and then quotient out the images of the horizontal maps. Under all of these operations, multiplication by r remains multiplication by r. Hence the induced map $\mathrm{Ext}^i_R(M, \psi)$ is multiplication by r on $\mathrm{Ext}^i_R(M, N)$.

(4) We follow the construction of $\mathrm{Ext}^i_R(\phi, N)$ as in Definition 5.4.25 of the printed course notes. In a first step, we have to lift the map $\phi : M \to M$ to a chain morphism $\Phi_\bullet : P_\bullet \to P_\bullet$, as in Theorem 5.4.20 of the course notes. Notice that the diagram

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & P_2 & \xrightarrow{p_2} & P_1 & \xrightarrow{p_1} & P_0 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle r\times} & & \downarrow{\scriptstyle r\times} & & \downarrow{\scriptstyle r\times} & & \\
\cdots & \longrightarrow & P_2 & \xrightarrow[p_2]{} & P_1 & \xrightarrow[p_1]{} & P_0 & \longrightarrow & 0
\end{array}$$

where vertical arrows are multiplication by r, commutes, because multiplication by r commutes with any R-module homomorphism by definition. As in the previous point, this then also induces multiplication by r on homology, so it induces the map $\phi : M \to M$ (recall that M is the 0-th homology module of $P_\bullet$). Therefore, if $\Phi_\bullet$ is multiplication by r on every module of the sequence, then this is a lift of ϕ as in Theorem 5.4.20.

The next step is to apply $\mathrm{Hom}_R(-, N)$ to the entire diagram above. This will reverse all arrows, and the vertical arrows will be pre-composition with multiplication by r. But as again multiplication by r commutes with any R-module homomorphism, the vertical arrows will again be multiplication by r. As in the previous point, the induced morphism on cohomology is then also just multiplication by r. Hence $\mathrm{Ext}^i_R(\phi, N)$ is multiplication by r on $\mathrm{Ext}^i_R(M, N)$.

(5) Let $r \in \mathrm{Ann}(N) \setminus \{0\}$. Let $\phi : \mathrm{Frac}(R) \to \mathrm{Frac}(R)$ be multiplication by r, then this is an automorphism of $\mathrm{Frac}(R)$. As functors preserve isomorphisms (explained at the end), $\mathrm{Ext}^i_R(\phi, N)$ is still an automorphism, and by the previous point it is multiplication by r on $\mathrm{Ext}^i_R(\mathrm{Frac}(R), N)$.

On the other hand, let $\psi : N \to N$ be multiplication by r. As $r \in \mathrm{Ann}(N)$, this coincides with multiplication by 0. By point (3), we then obtain that multiplication by r on $\mathrm{Ext}^i_R(\mathrm{Frac}(R), N)$ coincides with multiplication by 0 on $\mathrm{Ext}^i_R(\mathrm{Frac}(R), N)$. But above we obtained that multiplication by r is an automorphism. Therefore, we conclude $\mathrm{Ext}^i_R(\mathrm{Frac}(R), N) = 0$ for all $i \geq 0$.

Now we explain what is meant by 'functors preserve isomorphisms'. In fact, one can verify that $\mathrm{Ext}^i_R(\mathrm{id}_M, N) = \mathrm{id}_{\mathrm{Ext}^i_R(M,N)}$ and $\mathrm{Ext}^i_R(\alpha \circ \alpha', N) = \mathrm{Ext}^i_R(\alpha', N) \circ \mathrm{Ext}^i_R(\alpha, N)$ for any M, N, and any R-module homomorphisms $\alpha : M \to M'$ and $\alpha' : M' \to M''$. This is in fact part of the definition of a (contravariant) functor.

Now let $\alpha : M \to M'$ be an isomorphism, with inverse $\alpha' : M' \to M$. Then we have

$$\mathrm{id}_{\mathrm{Ext}^i_R(M,N)} = \mathrm{Ext}^i_R(\alpha' \circ \alpha, N) = \mathrm{Ext}^i_R(\alpha, N) \circ \mathrm{Ext}^i_R(\alpha', N)$$

and

$$\mathrm{id}_{\mathrm{Ext}^i_R(M',N)} = \mathrm{Ext}^i_R(\alpha \circ \alpha', N) = \mathrm{Ext}^i_R(\alpha', N) \circ \mathrm{Ext}^i_R(\alpha, N).$$

Hence $\mathrm{Ext}^i_R(\alpha, N) : \mathrm{Ext}^i_R(M', N) \to \mathrm{Ext}^i_R(M, N)$ is an isomorphism with inverse $\mathrm{Ext}^i_R(\alpha, N)$. So functors preserve isomorphisms.

□

EPFL - Fall 2023	Prof. Zs. Patakfalvi
Rings and modules	**Exercises**
Sheet 5 - Solutions	

Exercise 1. For two short exact sequences

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

and

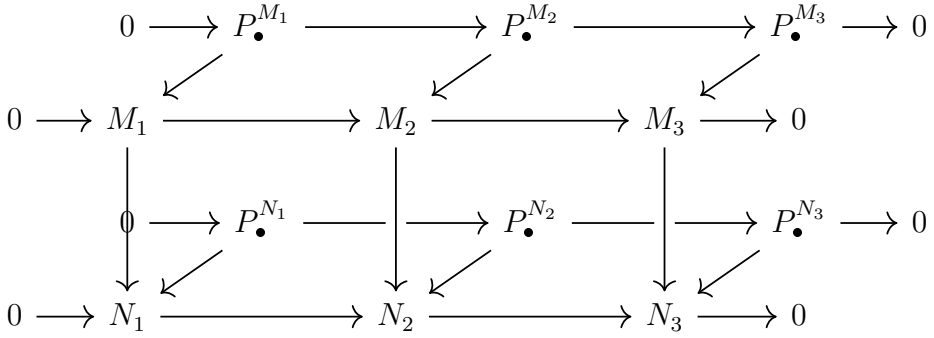
$$0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0$$

we say that there is a map between them if there exists morphisms $f_i : M_i \to N_i$, for $1 \leq i \leq 3$ and a commuting diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0. \end{array}$$

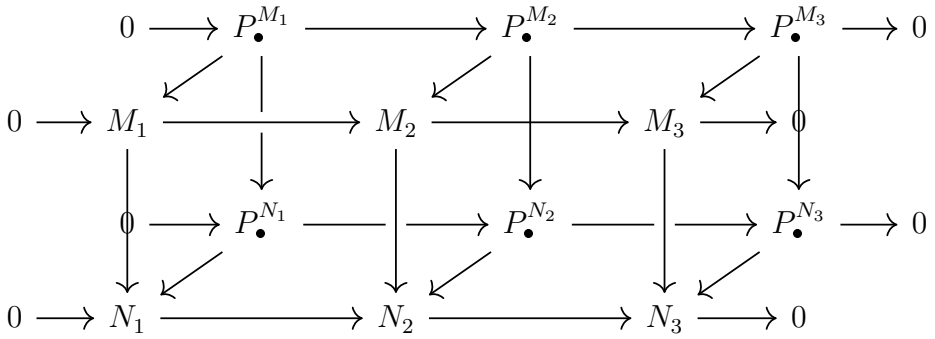
Show that whenever there is a map between two short exact sequences, then there is an induced map between long exact sequences of Ext-modules, making the suitable diagram commute.

Proof. By applying the *Horseshoe Lemma* 5.5.5 in the lecture notes there exists projective resolutions $P_\bullet^{M_i}$ of M_i and $P_\bullet^{N_i}$ of N_i for $i = 1, 2, 3$ and a commuting three dimensional diagram:



By Theorem 5.4.20 in the Lecture notes we can extend this diagram, by extending $f_i : M_i \to N_i$ to a (unique up to homotopy) morphism of chain complexes $f_\bullet : P_\bullet^{M_i} \to P_\bullet^{N_i}$ for

$i = 1, 2, 3$. Therefore we have a three dimensional diagram commuting up to homotopy:



Let K be some R-module, we can apply $\mathrm{Hom}_R(-, K)$ to the above diagram, then we get a diagram which commutes up to homotopy by Remark 5.4.15 and with the backside of the diagram still having exact rows as explained in (5.6.i) in the proof of Theorem 5.5.6. If we take cohomology we get an induced morphism $f_{i,j} : \mathrm{Ext}^j(M_i, K) \to \mathrm{Ext}^i(N_i, K)$ for every $j \geq 0$ and $i = 1, 2, 3$ which commutes with the horizontal morphisms in the diagram by Proposition 5.4.17. We want to show that these morphisms commute with the connecting homomorphism (denoted δ_M and δ_N respectively) appearing in the long exact sequence Prop 4.5.1, i.e., from what has been said above we have a diagram :

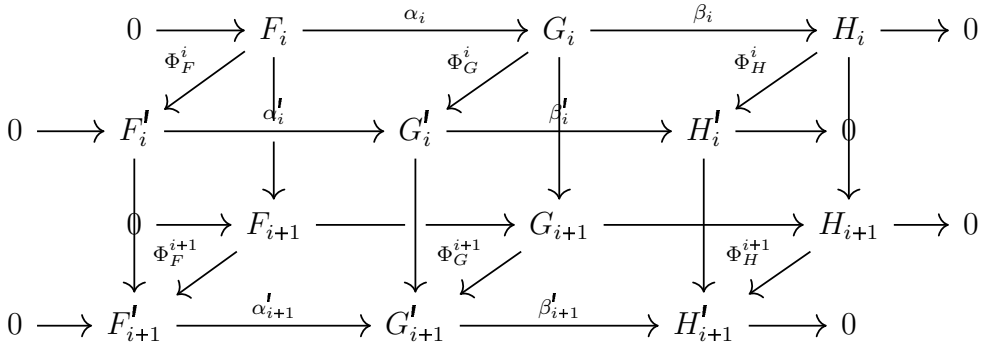
$$\begin{array}{ccccccc} \mathrm{Ext}^{i-1}(M_1, K) & \xrightarrow{\delta_M} & \mathrm{Ext}^i(M_3, K) & \longrightarrow & \mathrm{Ext}^i(M_2, K) & \longrightarrow & \mathrm{Ext}^i(M_1, K) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \mathrm{Ext}^{i-1}(N_1, K) & \xrightarrow{\delta_N} & \mathrm{Ext}^i(N_3, K) & \longrightarrow & \mathrm{Ext}^i(N_2, K) & \longrightarrow & \mathrm{Ext}^i(N_1, K) \end{array},$$

where only the commutativity of the first square needs to be checked. I.e we are checking that the long exact sequence of cohomology (Proposition 5.5.1) is *functorial*. To this end we revisit the set up of Proposition 5.5.1. We use the notation in Proposition 5.5.1 to make it easier for the reader. To this end suppose we have a commutative diagram between cocomplexes, with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F_\bullet & \xrightarrow{\alpha_\bullet} & G_\bullet & \xrightarrow{\beta_\bullet} & H_\bullet & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \Phi_F} & & \downarrow{\scriptstyle \Phi_G} & & \downarrow{\scriptstyle \Phi_H} & & \\ 0 & \longrightarrow & F'_\bullet & \xrightarrow{\alpha'_\bullet} & G'_\bullet & \xrightarrow{\beta'_\bullet} & H'_\bullet & \longrightarrow & 0 \end{array}.$$

Where the structure morphism of the complexes are denoted f_i, g_i, h_i and f'_i, g'_i, h'_i respectively (as in Proposition 4.5.1). We want to check that the morphisms $\delta_i : H^i(H_\bullet) \to H^{i+1}(F_\bullet)$, $\delta'_i : H^i(H'_\bullet) \to H^{i+1}(F'_\bullet)$ constructed in Proposition 4.5.1 commutes with the morphisms induced by Φ_F, Φ_H. To this end let $x \in H^i(H_\bullet)$, and let $\bar{x} \in H_i$ be a lift of x. Let $y \in G_i$ be a preimage under β_i of x then $\Phi^i_G(y) \in G'_i$ is a preimage under β'_i of $\Phi^i_H(\bar{x})$.

The situation is illustrated by the following diagram:



Let now $z \in F_{i+1}$ be such that $\alpha_{i+1}(z) = g_i(y)$ (so that $\delta_i(x)$ is the class of z inside $H^{i+1}(F_\bullet)$). It is sufficient to show that $\alpha'_{i+1}(\Phi_F^{i+1}(z)) = g'_i(\Phi_G^i(y))$. This follows by some easy diagram chasing as follow: We have $\alpha'_{i+1}(\Phi_F^{i+1}(z)) = \Phi_G^{i+1}(\alpha_{i+1}(z))$, but by definition we have $\alpha_{i+1}(z) = g_i(y)$. By the commutativity of the diagram $\Phi_G^{i+1}(g_i(y)) = g'_i(\Phi_G^i(y))$. Let now $x' \in H^i(H'_\bullet)$ be the image of x under the morphism induced by Φ_H. As $\alpha'_{i+1}(\Phi_F^{i+1}(z)) = g'_i(\Phi_G^i(y))$ and $\Phi_G^i(y)$ is a preimage under β'_i of $\Phi_H^i(\bar{x})$, which is a lift of x' to H'_i, we obtain that $\delta'_i(x')$ is equal to the class of $\Phi_F^{i+1}(z)$ inside $H^{i+1}(F'_\bullet)$. The latter is by definition equal to the image of $\delta_i(x)$ under the morphism induced by Φ_F, which concludes the proof. □

Exercise 2. In this exercise we prove the the two *4-lemmas*. To this end, suppose that we have a commuting diagram with exact rows:

$$\begin{array}{ccccccc} A & \xrightarrow{f_1} & B & \xrightarrow{f_2} & C & \xrightarrow{f_3} & D \\ \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle d} \\ A' & \xrightarrow{f'_1} & B' & \xrightarrow{f'_2} & C' & \xrightarrow{f'_3} & D' \end{array}$$

(1) Show that if a and c are epimorphisms (i.e. surjective) and d is a monomorphism (i.e. injective) then b is an epimorphism.
(2) Show that if b and d are monomorphisms and a is an epimorphism then c is a monomorphism.

Proof. (1) Let $\beta' \in B'$, we want to show that there exists $\beta \in B$ such that $b(\beta) = \beta'$. To this end, since c is surjective there exists $\gamma \in C$ such that $c(\gamma) = f'_2(\beta')$. By commutativity we get $df_3(\gamma) = f'_3c(\gamma) = f'_3f'_2(\beta')$. By exactness of the rows $f'_3f'_2(\beta') = 0$ and hence $f_3(\gamma) \in \ker(d)$. By assumption $\ker(d) = 0$ and hence (using exactness of the rows) $\gamma \in \mathrm{im}(f_2)$. Let $\beta_1 \in B$ be such that $f_2(\beta_1) = \gamma$. We have $f'_2(b(\beta_1) - \beta') = 0$, by commutativity and definition of β_1 and γ. By exactness of the lower row there therefore exists $\alpha' \in A'$ such that $f'_1(\alpha') = b(\beta_1) - \beta'$. By assumption a is surjective, so let $\alpha \in A$ be such that $a(\alpha) = \alpha'$. We have $bf_1(\alpha) = b(\beta_1) - \beta'$ by commutativity. Let $\beta = \beta_1 - f_1(\alpha)$, then $b(\beta) = b(\beta) - b(\beta) + \beta' = \beta'$. We conclude that b is an epimorphism.
(2) Let $\gamma \in C$ be such that $c(\gamma) = 0$; we want to show that $\gamma = 0$. By commutativity we have $df_3(\gamma) = f'_3c(\gamma) = 0$, and by injectivity of d it follows that $f_3(\gamma) = 0$. By exactness of the rows we get $\gamma \in \mathrm{im}(f_2)$, so let $\beta \in B$ be such that $f_2(\beta) = \gamma$. Now

again by commutativity we have $f_2'b(\beta) = cf_2(\beta) = 0$ and thus by exactness of the rows there exists $\alpha' \in A'$ such that $f_1'(\alpha') = b(\beta)$. Then by surjectivity of a we can also take $\alpha \in A$ with $a(\alpha) = \alpha'$. Thus we get by commutativity $bf_1(\alpha) = f_1'a(\alpha) = b(\beta)$, and by injectivity of b it follows that $f_1(\alpha) = \beta$. But thus $\gamma = f_2(\beta) = f_2f_1(\alpha)$, which by exactness gives $\gamma = 0$. Hence γ is a monomorphism.

□

Exercise 3. Prove the following.

(1) Show that any finitely generated module over a semi-simple ring is semi-simple
(2) Show that any finitely generated module over a semi-simple ring is projective
(3) Deduce that any finitely generated module over $k[G]$ is projective, if $\operatorname{char} k \nmid |G|$
(4) What are the Ext-groups then for finitely generated $k[G]$-modules?

Proof. (1) Let $\phi : R^{\oplus k} \to M$ be a surjection. Since R is semi-simple so is $R^{\oplus k}$. Write $R^{\oplus k} = \bigoplus_{i=1}^{s} I_i$, where each of the I_i are simple submodules (see Exercise 3 of Sheet 2). Let $\phi(I_i) = M_i$, by surjectivity, $M = \sum_i M_i$. We will prove that M_i is simple or trivial. As $\phi|_{I_i}$ is a surjection $I_i \twoheadrightarrow M_i$, we have that M_i is isomorphic to I_i/K_i where K_i is the kernel of $\phi|_{I_i}$. But as I_i is simple we have either $K_i = 0$ or $K_i = I_i$, which proves that either $M_i = 0$ or $M_i \cong I_i$. Hence M is a sum of simple submodules and thus semi-simple.

(2) Let R be a semi-simple ring and P a finitely generated R-module. Let $p : R^{\oplus n} \twoheadrightarrow P$ be a surjection of R-modules, and let K be the kernel of p. Write $R^{\oplus n} = \bigoplus_{i\in A} I_i$ as a direct sum of simple submodules, and let $B \subseteq A$ be a maximal subset such that

$$K \cap \bigoplus_{i\in B} I_i = 0$$

We claim that $K + \bigoplus_{i\in B} I_i = R^{\oplus n}$. If it was not the case, there would exist some $j \notin B$ such that $I_j \nsubseteq K + \bigoplus_{i\in B} I_i$. But since I_j is simple, $I_j \cap K + \bigoplus_{i\in B} I_i = 0$, contradicting the maximality of B.

Thus, $K + \bigoplus_{i\in B} I_i = R^{\oplus n}$, and hence the restriction of $R^{\oplus n} \to P$ induces an isomorphism

$$P \cong \bigoplus_{i\in B} I_i$$

On the other hand, we also proved that

$$R^{\oplus n} \cong K \oplus \bigoplus_{i\in B} I_i$$

so P is a direct summand of the free module $R^{\oplus n}$ (and hence projective).

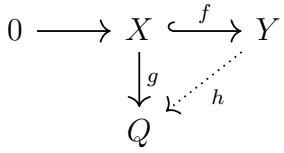
[*Remark:* The technique used in the proof actually comes from a general statement: a finitely generated module M over some ring R is semi-simple if and only if every submodule $N \leq_R M$ admits a complement, i.e. a submdule $N' \leq_R M$ such that $M = N \oplus N'$. This can be useful, so it may be worth remembering it.]

(3) We saw in Exercise 3 on Sheet 2 that $k[G]$ is semi-simple if $\operatorname{char} k \nmid |G|$, hence this follows from the previous point.

(4) In class (Corollary 5.4.24 in the printed course notes) we proved that $\operatorname{Ext}^i_R(P, N) = 0$ for all $i > 0$ whenever P is a projective R-module.

□

Exercise 4. In this exercise we define injective modules and prove *Baer's criterion*. Let R be a (not necessarily commutative) ring; any R-module and any R-morphism appearing in this exercise will be a left R-module resp. a morphism of left R-modules.
We say that an R-module Q is injective if it satisfies the following universal property: Whenever we have an injective R-morphism $f : X \hookrightarrow Y$ and an R-morphism $g : X \to Q$, then there exists an R-morphism $h : Y \to Q$ making the following diagram commute:



We will prove the following:

Theorem (Baer's Criterion)**.** *Suppose that the left R-module Q has the property that if I is any left ideal of R and $f : I \to Q$ is an R-morphism, there exists an R-morphism $F : R \to Q$ extending f. Then Q is an injective R-module.*

We will prove *Baer's criterion* in several steps. Assume that the R-module Q satisfies Baer's criterion.

(1) Let X, Y be R-modules, and assume that Y is *cyclic* (generated by $b \in Y$). Let $f : X \hookrightarrow Y$ be an injective R-morphism. Show that for every R-morphism $g : X \to Q$, there exists an R-morphism $h : Y \to Q$ making the appropriate diagram commute.
[*Hint:* Identify X with a submodule of Y and consider the subset I of R defined by $I = \{r \in R : rb \in X\}$.]

(2) Let X, Y be left R-modules with an injective R-morphism $f : X \hookrightarrow Y$ (we identify X with its image under f). Let $b \in Y$ be arbitrary. With a similar approach as in the previous point, prove that any R-morphism $g : X \to Q$ can be extended to an R-morphism $h : X + Rb \to Q$ making the appropriate diagram commute.

(3) Use *Zorn's Lemma* to conclude the proof.

Axiom 1 (Zorn's Lemma / Axiom of Choice)**.** If $(\mathcal{P}, \leq)$ is a partially ordered set with the property that every totally ordered subset (often called a chain) has an upper bound, then there exists a maximal $M \in \mathcal{P}$. (that is, for $N \in \mathcal{P}$, we have $M \nleq N$)

[*Hint:* Try to think of what it means for one partial extension of $g : X \to Q$ to be smaller than another.]

Proof. (1) Let $I = \{r \in R | rb \in X\}$ where we consider $Ra \subseteq Rb$ via f; it is straightforward to check that this is an ideal. Then the map $l : I \to Q$ defined by $l(r) = g(rb)$ is a homomorphism, so we can extend to $L : R \to Q$, by the hypothesis. Define $h : Rb \to Q$ by $h(rb) = L(r)$. This is well-defined because if $rb = r'b$, then $r - r' \in I$ and thus $L(r-r') = g((r-r')b) = 0$. Also, it is straightforward to check that h is an R-morphism extending g, so we are done.

(2) As above, let $I = \{r \in R | rb \in X\}$ and extend $l : I \to Q$ defined by $l(r) = g(rb)$ to $L : R \to Q$. Then we can define $h : X + Rb \to Q$ by $h(x + rb) = g(x) + L(r)$. To show that this is well-defined, assume that $x + rb = x' + r'b$. Then $(r - r')b = x' - x \in X$ and thus $r - r' \in I$, which implies

$$g(x - x') + L(r - r') = g(x - x') + g(r(b - b')) = 0.$$

Furthermore, it is straightforward to check that h is an R-morphism extending g, so we are done.

(3) Say that $X \subset Y$ and $g : X \to Q$ is a homomorphism. Consider the set

$$\mathcal{P} = \{(X', g') \mid X \subseteq X' \subseteq Y,\ g' : X' \to Y,\ g|_X = g\}.$$

We can define a partial order $\leq$ on $\mathcal{P}$ as follows: $(X', g') \leq (X'', g'')$ if and only if $X' \subseteq X''$ and $g''|'_X = g'$. Then if $\{(X'_i, g'_i)\}_{i\in\Omega}$ is a totally ordered subset indexed by some set Ω, we can form $\cup_{i\in\Omega} f_i : \bigcup_{i\in\Omega} A_i \to Q$, which then is an upper bound to the chain. Hence there exists a maximal $h : X' \to Q$, by Zorn's Lemma.
Now if we have some $b \in Y - X'$, we can extend h to $X' + Rb$, by the previous point. This contradicts the maximality of h, so we must have $X' = Y$, and we are done.

□

Exercise 5. Use Baer's Criterion to show that $\mathbb{Q}$ is an injective $\mathbb{Z}$-module.

Proof. Let I be an ideal of $\mathbb{Z}$, then $I = n\mathbb{Z}$ some $n \in \mathbb{Z}$. Let $g : n\mathbb{Z} \to \mathbb{Q}$ be a group homomorphism. If $n = 0$ then the zero map from $\mathbb{Z}$ to $\mathbb{Q}$ extends g. Otherwise suppose $g(n) = \frac{a}{b}$. We can extend f by $h : \mathbb{Z} \to \mathbb{Q}$ defined by $h(k) = \frac{ka}{nb}$ for all k. □

Exercise 6. [1]

(1) Set $k = \mathbb{F}_p$ and $G = \mathbb{Z}/p\mathbb{Z}$. Find all the submodules (i.e. ideals) of $R = k[G]$.
[*Hint:* To understand $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ in terms of more common rings, it might be a good idea to look for ring morphisms $\mathbb{F}_p[x] \to \mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ and investigate both kernel and image.]

(2) For $p = 2$, let x denote a generator of G and set $M = (x + 1) \subseteq k[G]$. Compute $\mathrm{Ext}^i_R(M, M)$ for all $i \geq 0$.

Proof. (1) We define a k-algebra morphism (i.e. a ring morphism that is also k-linear) $\Phi : k[x] \to k[G]$ by mapping $x \mapsto \delta_g$, where $\delta_\bullet$ is defined as in the hint and $g \in G$ is a generator (such a morphism always exists by the universal property of $k[x]$). Then notice that

$$\Phi(x^p - 1) = (\delta_g)^p - 1 = \delta_{g^p} - 1 = \delta_{e_G} - 1 = 0$$

and thus $(x^p - 1) \subseteq \mathrm{Ker}\,\Phi$. Thus we obtain a k-algebra map $\phi : k[x]/(x^p - 1) \to k[G]$. Now as the image contains $\{\delta_{g^i}\}_{0\leq i<p}$ which is a k-basis of $k[G]$, we get that ϕ is a surjective map of k-vector spaces of dimension p. Hence ϕ is an isomorphism.
Now the ideals of $k[x]/(x^p - 1)$ are in one-to-one correspondence with the ideals I of $k[x]$ containing $x^p - 1$. Notice that $x^p - 1 = (x - 1)^p$ as we are in characteristic p, and thus as $k[x]$ is a PID we obtain that the ideals of $k[x]$ containing $x^p - 1$ are exactly $I_i = ((x - 1)^i)$ for $0 \leq i \leq p$. Translating this to $k[G]$, we obtain that the ideals of $k[G]$ are precisely $\Phi(I_i) = ((\delta_g - 1)^i)$ for $0 \leq i \leq p$.

(2) Denote $R = k[G]$. The map $R \to M$ mapping $r \in R$ to $r(x+1)$ is clearly surjective. To compute the kernel, suppose that $r(x + 1) = 0$. By the isomorphism ϕ of the previous point, we can view this as an equation inside $k[x]/(x^2 - 1)$. As $x^2 - 1 = (x + 1)^2 = 0$,

[1] as modules over $k[G]$ correspond to representations of G over k, we see that something is really wrong for $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$ compared to the case of exercise 3.

we see that the solutions to the equation are precisely the multiples of $x+1$. That is, the kernel of $R \twoheadrightarrow M$ is again M. Hence we get a free resolution

$$\cdots \to R \to R \to R \to M \twoheadrightarrow 0$$

where all the arrows are just multiplication by $x+1$. Dropping the M from the sequence and applying $\mathrm{Hom}_R(-, M)$, and under the identification $\mathrm{Hom}_R(R, M) \cong M$, we obtain the sequence

$$\cdots \leftarrow M \leftarrow M \leftarrow M \leftarrow 0$$

where again every map is multiplication by $x+1$. But as $(x+1)^2 = 0$ in M, every map is equal to 0, and thus all cohomology groups are equal to M. Thus $\mathrm{Ext}^i_R(M, M) = M$ for all $i \geq 0$.

□

EPFL - Fall 2023 Prof. Zs. Patakfalvi
Rings and modules **Exercises**
Sheet 6 - Solutions

There was one bonus exercise on this problem sheet. The exercise was denoted by the symbol ♠ next to the exercise number.

Exercise 1. Let $R = k[x, y]$ be the polynomial ring in two variables over an algebraically closed field k. Recall that an ideal $\mathfrak{m}$ in a ring R is maximal if it is not properly contained in any other proper ideal of R. In this exercise you can use freely the Theorem below, which will be proven later in the course.

Theorem (The weak Nullstellensatz in two variables)**.** *Let k be an algebraically closed field. Every maximal ideal $\mathfrak{m}$ in the ring $k[x, y]$ is of the form $\mathfrak{m} = (x - a, y - b)$ for some $a, b \in k$.*

Show the following:

(1) If M is a finite length module over R, then the quotients of its composition series are of the form $R/(x - a, y - b)$.

(2) If M is a module such that $\mathrm{Ann}(M) \supseteq (x - a, y - b)$, then $\mathrm{Ann}(\mathrm{Ext}^i(M, N)) \supseteq (x - a, y - b)$ for every R-module N.
[*Hint*: Consider the multiplication by $x - a$ resp. $y - b$ on M and the induced maps on $\mathrm{Ext}^i_R(M, N)$. Recall also Exercise 7 of Sheet 4.]

(3) If N is any finitely generated module over R, then $\mathrm{Ext}^i\left(R/(x - a, y - b), N\right)$ has finite length.
[*Hint*: Use the previous point.]

(4) For every finite length module M and for every finitely generated module N over R, $\mathrm{Ext}^i_R(M, N)$ has finite length.
[*Hint*: Use the long exact sequence for a compostion series.]

Proof. (1) Let $0 = M_0 < M_1 < \cdots < M_n = M$ be a composition series. Since $Q_i := M_i/M_{i-1}$ is simple we have $Q_i \cong R/\mathrm{Ann}(Q_i)$ by Exercise 1 on Sheet 1. As thus R-submodules of Q_i correspond to ideals of R containing $\mathrm{Ann}(Q_i)$, we obtain that $\mathrm{Ann}(Q_i)$ is maximal. Hence, we conclude by the weak Nullstellensatz.

(2) By Exercise 7.4 of Sheet 4, multiplication by $r \in R$ on M induces multiplication by r on $\mathrm{Ext}^i(M, N)$. Hence if $r \in \mathrm{Ann}(M)$, multiplication by r is equal to multiplication by 0 on M, and hence multiplication by r is equal to multiplication by 0 on $\mathrm{Ext}^i(M, N)$, and thus $r \in \mathrm{Ann}(\mathrm{Ext}^i(M, N))$. Hence we obtain $\mathrm{Ann}(M) \subseteq \mathrm{Ann}(\mathrm{Ext}^i(M, N))$ which is enough to conclude.

(3) By the previous point $\mathrm{Ext}^i\left(R/(x - a, y - b), N\right)$ has a natural structure as $R/(x - a, y - b) \cong k$ module, and the R-submodules are precisely the k-submodules. It is therefore sufficient to prove that $\mathrm{Ext}^i\left(R/(x - a, y - b), N\right)$ has finite length over k, i.e. is a finite dimensional k-vectorspace. To achieve this, we will show that $\mathrm{Ext}^i\left(R/(x - a, y - b), N\right)$ is a finitely generated R-module. Let $P_\bullet \to R/(x - a, y - b)$ be a free resolution. Since R is a Noetherian ring every submodule of R^n is finitely generated, hence we may assume each P_i is finitely generated. Observe that $\mathrm{Hom}_R(R^n, N) \cong N^n$ is finitely generated for every $n \geq 0$. Again using that R is Noetherian any submodule or quotient of a finitely generated module is finitely generated, therefore we

conclude that $\mathrm{Ext}^i\left(R/(x-a,y-b),N\right)$ is a finitely generated R-module. This implies that $\mathrm{Ext}^i\left(R/(x-a,y-b),N\right)$ is a finitely generated $R/(x-a,y-b)$-module and hence a finite dimensional k-vectorspace.

(4) We prove this by induction following the hint. To this end let $0 = M_0 < M_1 \cdots < M_n = M$ be a composition series, we note that since M_1 is simple we have that $M_1 \cong R/(x-a,y-b)$ and thus $\mathrm{Ext}^i_R(M_1,N)$ is of finite length by the previous point. We have a short exact sequence

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_2/M_1 \longrightarrow 0$$

which induces an exact sequence

$$\cdots \longrightarrow \mathrm{Ext}^i_R\left(M_2/M_1,N\right) \longrightarrow \mathrm{Ext}^i_R(M_2,N) \longrightarrow \mathrm{Ext}^i_R(M_1,N) \longrightarrow \cdots .$$

By passing to the kernel on the left and the image on the right (since being of finite length is stable under quotients and submodules) we can assume that $\mathrm{Ext}^i_R(M_2,N)$ is the middle term in a short exact sequence with kernel and image of finite length, but then it follows that $\mathrm{Ext}^i_R(M_2,N)$ is of finite length. We can now repeat the argument for M_3 and so on and so forth. By induction, this proves that $\mathrm{Ext}^i_R(M,N) = \mathrm{Ext}^i_R(M_n,N)$ has finite length for all $i \geq 0$.

□

Exercise 2. Let $R = k[x,y]$ be as in the previous exercise (k is algebraically closed). We say that a finite length module is supported at $(x-a,y-b)$ if only $R/(x-a,y-b)$ appears as quotients in the composition series. Show that if M is a finite length module supported at $(x-a,y-b)$, then $\mathrm{Ext}^i_R\left(M, R/(x-a',y-b')\right) = 0$ for all $(a',b') \neq (a,b)$.

Proof. We first show that $\mathrm{Ext}^i_R\left(R/(x-a,y-b), R/(x-a',y-b')\right) = 0$ for all $i \geq 0$. By a similar argument as in Exercise 1 of this sheet (by using points (3) and (4) of Exercise 6 on Sheet 4) we have that both $(x-a,y-b)$ and $(x-a',y-b')$ are included in the annihilator of $\mathrm{Ext}^i_R\left(R/(x-a,y-b), R/(x-a',y-b')\right)$. Therefore, the ideal $(x-a,y-b)+(x-a',y-b') = R$ is in the annihilator of $\mathrm{Ext}^i_R\left(R/(x-a,y-b), R/(x-a',y-b')\right)$, which implies $\mathrm{Ext}^i_R(R/(x-a,y-b), R/(x-a',y-b')) = 0$.
Let $0 = M_0 < M_1 \cdots < M_n = M$ be a composition series. Denote $N = R/(x-a',y-b')$. We can now conclude by first looking at the short exact sequence

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_2/M_1 \longrightarrow 0$$

which induces an exact sequence

$$\cdots \longrightarrow \mathrm{Ext}^i_R\left(M_2/M_1,N\right) \longrightarrow \mathrm{Ext}^i_R(M_2,N) \longrightarrow \mathrm{Ext}^i_R(M_1,N) \longrightarrow \cdots .$$

From here we see that $\mathrm{Ext}^i_R(M_2,N) = 0$, since the other two modules are trivial by what has already been proven. We continue, upon replacing M_1 with M_2 and M_2 with M_3, we can conclude in an analog way that $\mathrm{Ext}^i_R(M_3,N) = 0$. We continue step by step, to conclude by induction that $\mathrm{Ext}^i_R\left(M, R/(x-a',y-b')\right) = \mathrm{Ext}^i_R\left(M_n, R/(x-a',y-b')\right) = 0$. □

Exercise 3. Show using the long exact sequence of cohomology that if $\mathrm{Ext}^1_R(M,N) = 0$, then every extension $0 \longrightarrow N \longrightarrow K \longrightarrow M \longrightarrow 0$ splits.

Proof. Denote by i the injection $i : N \to K$. By the long exact sequence of Ext-modules, we obtain that

$$0 \longrightarrow \mathrm{Hom}_R(M,N) \longrightarrow \mathrm{Hom}_R(K,N) \xrightarrow{-\circ i} \mathrm{Hom}_R(N,N) \longrightarrow 0$$

is exact. In particular, there exists $q \in \mathrm{Hom}_R(K,N)$ such that $q \circ i = \mathrm{id}_N$. Thus by Exercise 3 on Sheet 4, the sequence splits. □

Exercise 4. ♠ Let R the a commutative ring, and let M be an R-module. Define an $R[x]$-module $M[x]$ by the following datum:

- as an abelian group, $M[x] := \bigoplus_{j\geq 0} Mx^j$;
- R acts component-wise, and x acts as usual (i.e. $x \cdot (mx^j) = mx^{j+1}$);

(informally, $M[x]$ corresponds to polynomials with coefficients on M). Furthermore, for any R-module N, we see N as an $R[x]$-module by letting x act as 0.

Fix two R-modules M and N, and prove the following points:

(1) Show that $\mathrm{Hom}_{R[x]}(M[x],N) \cong \mathrm{Hom}_R(M,N)$ as R-modules.
(2) Show that if M is a projective R-module, then $M[x]$ is a projective $R[x]$-module.
(3) Deduce from the two previous points that for all $i \geq 0$,
$$\mathrm{Ext}^i_{R[x]}(M[x],N) \cong \mathrm{Ext}^i_R(M,N)$$
as R-modules.
(4) Show that for all $i \geq 0$, we have a short exact sequence
$$0 \to \mathrm{Ext}^i_R(M,N) \to \mathrm{Ext}^{i+1}_{R[x]}(M,N) \to \mathrm{Ext}^{i+1}_R(M,N) \to 0$$
of R-modules.
Hint: Use an adequate long exact sequence in Ext*-groups.*
(5) Conclude that $\mathrm{projdim}_{R[x]}(M) = \mathrm{projdim}_R(M) + 1$.
(6) What is the projective dimension of the $k[x_1,\dots,x_n]$-module
$$k[x_1,\dots,x_n]\Big/(x_1,\dots,x_n)?$$

Proof. (1) If $f\colon M \to N$ is a morphism as R-modules, we have an induced morphism $f_x\colon M[x] \to N$, defined as

$$f_x\left(\sum_j m_j x^j\right) = \sum_j x^j f(m_j).$$

It is straight-forward to check that f_x is a morphism of $R[x]$-modules.

Conversely, given $g\colon M[x] \to N$ a morphism of $R[x]$-modules, define $g|_M\colon M \to N$ as

$$g|_M(m) = g(mx^0).$$

Again, it is straight-forward to check that this defines a morphism of R-modules, and one readily sees that these two operations are inverses of each other.

Hence, we have a bijection $\mathrm{Hom}_R(M,N) \cong \mathrm{Hom}_{R[x]}(M[x],N)$, and checking that it is R-linear is again straightforward.

(2) We use the same notations as in the previous point. Consider a diagram of $R[x]$-modules

$$\begin{array}{ccc} & & N \\ & & \downarrow \psi \\ M[x] & \xrightarrow{g} & N', \end{array}$$

where ψ is a surjection. Then by the previous point, we have a diagram of R-modules

$$\begin{array}{ccc} & & N \\ & & \downarrow \psi \\ M & \xrightarrow{g|_M} & N', \end{array}$$

so by projectivity of M, there exists a morphism $f\colon M \to N$ such that the diagram

$$\begin{array}{ccc} & \overset{f}{\nearrow} & N \\ & & \downarrow \psi \\ M & \xrightarrow{g|_M} & N' \end{array}$$

commutes. But then, again by the previous point, the diagram

$$\begin{array}{ccc} & \overset{f_x}{\nearrow} & N \\ & & \downarrow \psi \\ M[x] & \xrightarrow{g} & N' \end{array}$$

also commutes. Thus, $M[x]$ is a projective $R[x]$-module.

(3) Let $P_\bullet \to M$ be a projective resolution of M. Then by the previous point, $P_\bullet[x] \to M[x]$ is also a projective resolution (checking exactness is straightforward, since for any R-module M', $M'[x]$ is simply an countable direct sum of copies of M' as an R-module). Hence,

$$\mathrm{Ext}^i_{R[x]}(M[x], N) = H^i(\mathrm{Hom}_{R[x]}(P_\bullet[x], N)) \cong H^i(\mathrm{Hom}_R(P_\bullet, N)) = \mathrm{Ext}^i(M, N).$$

(4) Consider the short exact sequence

$$0 \to M[x] \xrightarrow{x} M[x] \to M \to 0$$

of $R[x]$-modules, where the first map denotes multiplication by x, and M is seen as an $R[x]$-module by letting x act as zero on M. Applying the long exact sequence in Ext-groups, we obtain

$$\begin{array}{l} \ldots \longrightarrow \mathrm{Ext}^i_{R[x]}(M[x], N) \xrightarrow{\delta^i_x} \mathrm{Ext}^i_{R[x]}(M[x], N) \longrightarrow \mathrm{Ext}^i_{R[x]}(M, N) \\ \qquad \longrightarrow \mathrm{Ext}^{i+1}_{R[x]}(M[x], N) \longrightarrow \mathrm{Ext}^{i+1}_{R[x]}(M[x], N) \xrightarrow{\delta^{i+1}_x} \ldots \end{array}$$

where $\delta^j_x\colon \mathrm{Ext}^j_{R[x]}(M[x], N) \to \mathrm{Ext}^j_{R[x]}(M[x], N)$ denotes the map induced by applying $\mathrm{Ext}^j_{R[x]}(-, N)$ to the multiplication by x on $M[x]$. Combining parts 3 and 4 of Exercise 7 in sheet 4, we see that δ^j_x also comes from applying $\mathrm{Ext}^j_{R[x]}(M[x], -)$ to the

multiplication by x on N. However, x acts as zero on N, so $\delta_x^j = 0$ for all $j \geq 0$. Thus, we have short exact sequences

$$0 \to \mathrm{Ext}^i_{R[x]}(M,N) \to \mathrm{Ext}^{i+1}_{R[x]}(M[x],N) \to \mathrm{Ext}^{i+1}_{R[x]}(M[x],N) \to 0.$$

We then conclude by te previous point.

(5) This is immediate from Exercise 4.2 on sheet 4.

(6) We show this by induction on n. If $n = 0$, this is immediate, so assume that the result holds for $n-1$ (with $n \geq 1$). Let $R = k[x_1,\ldots,x_{n-1}]$ and $M = k[x_1,\ldots,x_{n-1}]/(x_1,\ldots,x_{n-1})$. Then as previously, we can see M as an $R[x_n]$-module by letting x_n act as zero, so by the previous point and induction,

$$\mathrm{projdim}_{R[x_n]}(M) = n - 1 + 1 = n.$$

Note that M, as an $R[x_n] = k[x_1,\ldots,x_n]$-module, is isomorphic to

$$k[x_1,\ldots,x_n]\Big/(x_1,\ldots,x_n),$$

so the proof is complete.

□

Exercise 5. Let $R = k[x,y]$ and consider the R-module $M = k[x,y]\Big/(x,y)$. Consider the free resolution:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & P_2 = R & \xrightarrow{f_2} & R \oplus R = P_1 & \xrightarrow{f_1} & R = P_0 & \xrightarrow{f_0} & M & \longrightarrow & 0 \\ & & 1 & \longmapsto & (y,-x) & & & & & & \\ & & & & (1,0) & \longmapsto & x & & & & \\ & & & & (0,1) & \longmapsto & y & & & & \end{array}$$

Set $M = N$. Consider

(1) $\phi_1 : P_1 \to N$ given by $\phi_1(a,b) = f_0(a)$,
(2) $\phi_2 : P_1 \to N$ given by $\phi_2(a,b) = f_0(b)$.

Determine the isomorphism classes of the middle module of the Yoneda extension associated to the classes of ϕ_1, ϕ_2 inside $\mathrm{Ext}^1_R(M,N)$ in Theorem 5.6.6 in the course notes.

[*Note*: these modules are $\mathrm{coker}\left(P_1 \xrightarrow{(\phi_i,f_1)} N \oplus P_0\right)$ for $i = 1,2$ as in the sequence 6.5.i in Notation 5.6.5 in the course notes.]

Proof.
The cokernel in question is the cokernel of the map $R \oplus R \to k \oplus R$ where (a,b) goes to $(a(0,0), ax + by)$. Let's investigate the elements in the image of this map, we have $(a(0,0), ax+by) = a(1,x) + b(0,y)$. Therefore, the image is the submodule $M := R(1,x) + R(0,y)$. We can describe this pretty concretely: we have

$$M = \{(a, ax + p) \mid a \in k,\ p \in (x^2, y)\}.$$

We use $\overline{\bullet}$ to denote the class of an element in a quotient. By our description of M, every element $\overline{(a,f)}$ of $k \oplus R\big/M$ can be written as $\overline{(0, f_{00} + (f_{10} - a)x)}$ where f_{ij} denotes the coefficient of $x^i y^j$ inside f (any term of higher order can be killed by $p \in (x^2,y)$). From this description it is straightforward to see that $\overline{(0,1)}$ and $\overline{(0,x)}$ form a k-basis of $k \oplus R\big/M$.

Below we present three different solutions showing that this cokernel is isomorphic as an R-module to $R/(x^2, y)$.

(1) *Fast and slick.* We use $\overline{\bullet}$ to denote the class of an element in a quotient. Consider the element $\overline{(1,1)} \in k \oplus R/M$, we have $y\overline{(1,1)} = \overline{(0,y)} = 0$ and hence $y \in \mathrm{Ann}\left(R \cdot \overline{(1,1)}\right)$. Similarly $x^2\overline{(1,1)} = \overline{(0,x^2)} = \overline{x(1,x)} = 0$ while $x\overline{(1,1)} = \overline{(0,x)} \neq 0$, hence $(x^2, y) = \mathrm{Ann}\left(R \cdot \overline{(1,1)}\right)$. We therefore have an isomorphism $R/(x^2, y) \to R \cdot \overline{(1,1)}$ defined by $1 \mapsto \overline{(1,1)}$. We claim that in fact $R \cdot \overline{(1,1)} = k \oplus R/M$. Indeed, we have $\overline{(1,1)} = \overline{(0, 1-x)}$ and $x\overline{(1,1)} = \overline{(0,x)}$, so $R \cdot \overline{(1,1)}$ contains the k-basis $\overline{(0,1)}$ and $\overline{(0,x)}$ of $k \oplus R/M$.

(2) *Explicit construction of the inverse of the isomorphism above.* We define a morphism $k \oplus R/M \to R/(x^2, y)$ by showing that there is a well-defined morphism of R-modules $k \oplus R \to R/(x^2, y)$ such that $(1, x)$ and $(0, y)$ are in the kernel. To this end, consider the morphism $R \to R/(x^2, y)$ defined by $f \mapsto f\overline{x}$; as x and y are in the kernel, this induces an R-module homomorphism $k \to R/(x^2, y)$ defined by $a \mapsto \overline{ax}$. We also have the R-morphism $R \to R/(x^2, y)$ given by $f \mapsto f \cdot \overline{(1-x)}$, and one sees $f \cdot \overline{(1-x)} = \overline{f - f_0 x}$. Hence we obtain an R-morphism $k \oplus R \to R/(x^2, y)$ given by $(a, f) \mapsto \overline{f - (a - f_0)x}$. As $(1, x)$ and $(0, y)$ are mapped to 0, this induces an R-morphism $k \oplus R/M \to R/(x^2, y)$, given by $\overline{(a,f)} \mapsto \overline{f - (a - f_0)x}$.
Now this is surjective as $\overline{(1,1)}$ is mapped to $\overline{1}$ which is a generator. But both sides are k-vector spaces of dimension 2, and thus it is bijective, so in fact an isomorphism of R-modules.
Remark: We could also have used $\overline{(a,f)} \mapsto \overline{f - ax}$, but this is not the inverse of the isomorphism in (1); it corresponds instead to the isomorphism $R/(x^2, y) \to k \oplus R/M$ defined by $\overline{1} \to \overline{(0,1)}$.

(3) *Hands on approach.* There is a natural isomorphism of R-modules from $k \oplus R/M$ to $k \oplus k[x]/k[x] \cdot (1, x)$ defined by mapping the variable y to zero (the R-module structure of the latter is given by y acting trivially). Over k, the module $k \oplus k[x]/k[x] \cdot (1, x)$ can easily be seen to have a basis given by $(-1, 0), (1, 1)$. Recall that multiplication by x on first coordinate is zero, hence $x(1,1) = (0, x) \equiv (-1, 0)$ modulo $(1, x)$ and $x^2(1,1) = (0, x^2) = x(1, x)$ and hence zero modulo $(1, x)$. Therefore, $k \oplus k[x]/k[x] \cdot (1, x)$ has a natural structure of $k[x]/x^2 = k[\epsilon]$-module. Define a $k[\epsilon]$-modules morphism $k[\epsilon] \to k \oplus k[x]/k[x] \cdot (1, x)$ by mapping $1 \mapsto \overline{(1,1)}$, we check that $\epsilon \mapsto x\overline{(1,1)} = \overline{(-1,0)}$. In particular, it is surjective as the image contains a k-basis. Since the dimension over k is two for both modules it is an isomorphism. Now adding y's to each side and quotienting it out so that nothing changes, the above isomorphism gives an isomorphism of R-modules composition $k[x,y]/(x^2, y) \to k \oplus k[x,y]/R(1,x) + R(0,y)$, defined by $\overline{1} \to \overline{(1,1)}$.

Interchanging the variables x and y in the above argument, we find the module associated to $[\phi_2]$ is $k[x,y]/(x, y^2)$.

[*Remark:* From the above, we have that the extension corresponding to $[\phi_1]$ is given by

$$0 \to k \to k[x,y]/(x^2,y) \to k \to 0,$$

where the first morphism sends $1 \mapsto -x$ and the second $x \mapsto 0$. Similarly, the extension corresponding to $[\phi_2]$ is given by

$$0 \to k \to k[x,y]/(x,y^2) \to k \to 0,$$

where the first morphism sends $1 \mapsto -y$ and the second $y \mapsto 0$. These are not isomorphic as elements of $\mathrm{Ext}^1_R(k,k)$ since there is no R-linear isomorphism from $k[x,y]/(x,y^2)$ to $k[x,y]/(x^2,y)$. Indeed, for any such f, $f(y) = yf(1) = 0$ (they are however the same as extensions of k-algebras, by mapping $x \mapsto y$).] □

Exercise 6. Let $R = k[x,y]$.

(1) Show that $\mathrm{Ext}^1\left((x,y), R/(x,y)\right) \neq 0$.
(2) Construct a finitely generated module M such that $\mathrm{Tors}(M) \subseteq M$ is not a direct summand.

[*Note:* For M finitely generated over a PID R, $\mathrm{Tors}(M) \subseteq M$ is always a direct summand by the fundamental theorem for finitely generated modules over PIDs.]

Proof. (1) Identify $k = R/(x,y)$ as usual. As seen on several occasions in this course, we have a projective resolution

$$0 \to R \to R \oplus R \to (x,y) \to 0$$

where the morphisms are given by $r \mapsto (-ry, rx)$ and $(r_1, r_2) \mapsto r_1x + r_2y$, respectively. To calculate $\mathrm{Ext}^1((x,y),k)$ we apply $\mathrm{Hom}(-,k)$ and calculate the cohomology in degree one of the corresponding complex. That is, the cokernel of $k \oplus k \to k$ given by $(r_1, r_2) \mapsto -r_1y + r_2x = 0$. Here we used that multiplication by x and y are zero. In particular we obtain

$$\mathrm{Ext}^1((x,y),k) = k \neq 0.$$

(2) We prove the following more general statement:

Lemma 0.1. *Let R be a domain, N a torsion module (i.e. for all $n \in N$, there exists a non-zero $r \in R$ such that $rn = 0$) and L a torsion-free module. Let*

$$0 \to N \to M \to L \to 0$$

be a non-split short exact sequence. Then $\mathrm{Tors}(M) \subseteq M$ is not a direct summand.

Proof. We may assume $N \subseteq M$ and $L = M/N$ (this is just to make notations simpler). First, note that $\mathrm{Tors}(M) = N$. Indeed, since N is torsion, $N \subseteq \mathrm{Tors}(M)$. Conversely, given $m \in \mathrm{Tors}(M)$, let $r \in R$ be non-zero such that $rm = 0$. Then $r\pi(m) = 0$, where $\pi : M \to M/N$ denotes the quotient map. Since L is torsion-free, $\pi(m) = 0$, so $r \in N$.

Now, assume $N = \mathrm{Tors}(M)$ was a direct summand. Then there would exist a morphism $M \to N$ such that the composition $N \subseteq M \to M$ is the identity, or in other words there exists a section of $N \subseteq M$ (see Exercise 3 on sheet 4). By this same exercise, this implies that the sequence

$$0 \to N \to M \to M/N \to 0$$

is split, which is a contradiction with our hypotheses. □

To conclude, we have found that $\mathrm{Ext}^1((x,y),k) \neq 0$ so there exists a non-split extension

$$0 \to k \to M \to (x,y) \to 0$$

We are done by the previous lemma.

□

Exercise 7. Throughout this exercise, R will be a ring and M, N will be R-modules. We will now see another way to compute the Ext-modules than the one we saw in the lectures (one may say a 'dual' way). To do so, we need the following Lemma, which you may use without proof.

Lemma 1. *For every R-module N there exists an injective R-module homomorphism $N \to I$ where I is an injective R-module.*

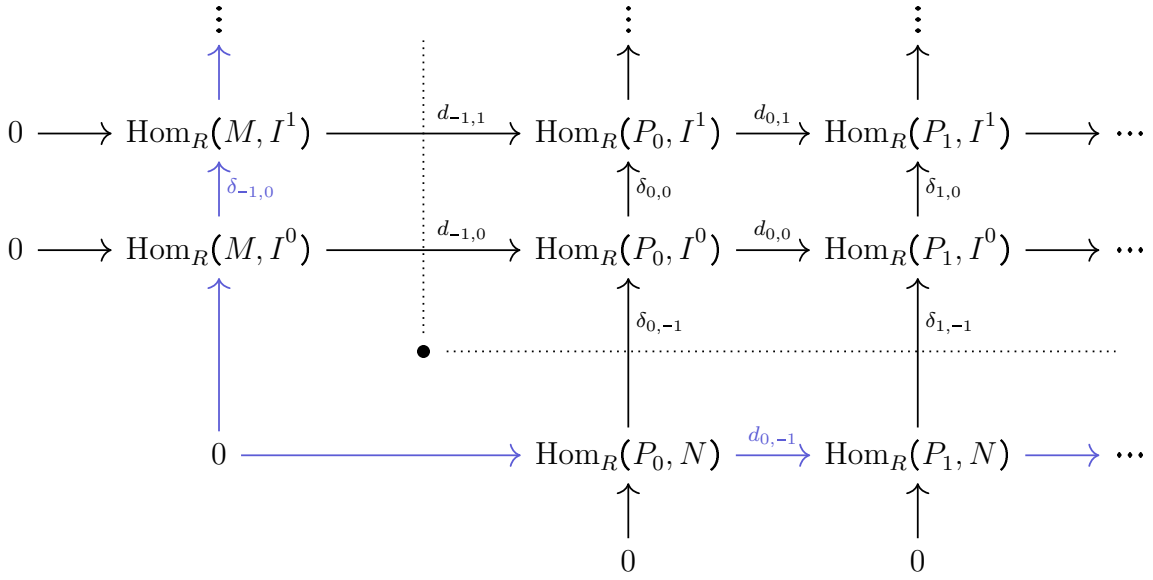
(1) Using the above Lemma, show that any R-module N admits an injective resolution. That is, there exists an exact sequence

$$0 \longrightarrow N \xrightarrow{i^{-1}} I^0 \xrightarrow{i^0} I^1 \longrightarrow \cdots$$

where I^b is an injective R-module for all $b \geq 0$ (the numbers in superscript are just indices, *not* exponents of any sort).

(2) Show that an R-module I is injective if and only if $\mathrm{Hom}_R(-, I)$ is exact.
[*Reminder:* By Lemma 5.2.2 of the lecture notes $\mathrm{Hom}_R(-, I)$ is always left exact.]

(3) Fix a projective resolution $P_\bullet \twoheadrightarrow M$ and an injective resolution $N \hookrightarrow I^\bullet$. Consider the commutative diagram



where $d_{a,b} = - \circ p_{a+1}$ and $\delta_{a,b} = i^b \circ -$ for all $a, b \geq -1$. Briefly justify that this is indeed commutative, and that all columns and lines of the diagram which are not blue are exact.

(4) Show that $H^0(\mathrm{Hom}_R(M, I^\bullet)) \cong H^0(\mathrm{Hom}_R(P_\bullet, N))$.
[*Hint:* Show that their images inside $\mathrm{Hom}_R(P_0, I^0)$ coincide.]

(5) Show that $H^1(\mathrm{Hom}_R(M, I^\bullet)) \cong H^1(\mathrm{Hom}_R(P_\bullet, N))$.
[*Hint:* Let $C^0 := \mathrm{Hom}_R(P_0, I^0)$ and $C^1 = \mathrm{Hom}_R(P_1, I^0) \oplus \mathrm{Hom}_R(P_0, I^1)$, and let $\Delta^0 : C^0 \to C^1$ be the map sending $x \in C^0$ to $(d_{0,0}(x), \delta_{0,0}(x)) \in C^1$. Show that the cohomology groups in question both embed into $\mathrm{coker}(\Delta^0)$ and that their images therein coincide.]

[*Remark:* One can generalize the above results and prove that in fact $H^i(\mathrm{Hom}_R(M, I^\bullet)) \cong H^i(\mathrm{Hom}_R(P_\bullet, N))$ for all $i \geq 0$, and thus the Ext-modules may also be computed by using an injective resolution of the second module. To do so, one defines the modules $C^m := \bigoplus_{a+b=m} \mathrm{Hom}_R(P_a, I^b)$ and connecting maps $\Delta^m : C^m \to C^{m+1}$ similar to Δ^0, where one replaces $\delta_{a,b}$ by $(-1)^a \delta_{a,b}$ to ensure $\Delta^{m+1} \circ \Delta^m = 0$. We thus obtain a complex $C^\bullet$, and one can then prove that $H^i(\mathrm{Hom}_R(M, I^\bullet))$ and $H^i(\mathrm{Hom}_R(P_\bullet, N))$ embed into $H^i(C^\bullet)$ with equal image.]

Proof. (1) By the Lemma, there exists an injective map $i^{-1} : N \hookrightarrow I^0$ with I^0 injective. Denote $I^{-1} = N$ for convenience. For $b \geq 1$, let I^b be an injective module such that there exists an injective map $\mathrm{coker}(I^{b-2} \xrightarrow{i^{b-2}} I^{b-1}) \hookrightarrow I^b$, and let i^{b-1} be the composition $I^{b-1} \to \mathrm{coker}(I^{b-2} \xrightarrow{i^{b-2}} I^{b-1}) \hookrightarrow I^b$. Then it is straightforward to verify that

$$0 \longrightarrow N \xrightarrow{i^{-1}} I^0 \xrightarrow{i^0} I^1 \longrightarrow \cdots$$

is an injective resolution.

(2) Suppose that I is injective, and let

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

be an exact sequence of R-modules. To verify that

$$0 \longrightarrow \mathrm{Hom}_R(C, I) \xrightarrow{-\circ\beta} \mathrm{Hom}_R(B, I) \xrightarrow{-\circ\alpha} \mathrm{Hom}_R(A, I) \longrightarrow 0$$

is exact, it suffices to verify that $- \circ \alpha$ is surjective, as $\mathrm{Hom}_R(-, I)$ is left exact by Lemma 5.2.2. So let $\phi \in \mathrm{Hom}_R(A, I)$ be arbitrary. Then we have a diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & A & \xhookrightarrow{\alpha} & B \\ & & \downarrow{\scriptstyle \phi} & & \\ & & I & & \end{array}$$

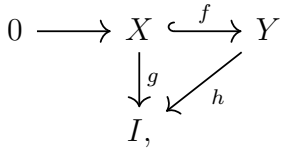
and thus by definition of I being injective, there exists $\psi : B \to I$ making the diagram commute. This precisely means $(- \circ \alpha)(\psi) = \phi$, so $- \circ \alpha$ is surjective.

Conversely, suppose that $\mathrm{Hom}_R(-, I)$ is exact, and suppose that we have a diagram of R-modules

$$\begin{array}{ccccc} 0 & \longrightarrow & X & \xhookrightarrow{f} & Y \\ & & \downarrow{\scriptstyle g} & & \\ & & I. & & \end{array}$$

Then as $\mathrm{Hom}_R(-, I)$ is exact, the map $- \circ f : \mathrm{Hom}_R(Y, I) \to \mathrm{Hom}_R(X, I)$ is surjective. In particular, there exists $h : Y \to I$ such that $h \circ f = g$, and thus a commutative

diagram



which proves that I is injective.

(3) Exactness of the non-blue rows follows as they are obtained from applying the exact functor $\mathrm{Hom}_R(-, I^b)$ to the exact sequence $P_\bullet \to M \to 0$, and exactness of the non-blue columns follows as they are obtained from applying the exact functor $\mathrm{Hom}_R(P_a, -)$ to the exact sequence $0 \to N \to I^\bullet$. The diagram commutes as vertical arrows are given by post-composition and horizontal arrows are given by pre-composition, and these two operations commute by associativity of composition.

(4) Let $\phi_{0,-1} \in \mathrm{Ker}(d_{0,-1})$ be arbitrary. Then by commutativity we have $d_{0,0} \circ \delta_{0,-1}(\phi_{0,-1}) = 0$, and so by exactness there exists $\phi_{-1,0} \in \mathrm{Hom}_R(M, I^0)$ such that $d_{-1,0}(\phi_{-1,0}) = \delta_{0,-1}(\phi_{0,-1})$. This shows that $d_{-1,0}(H^0(\mathrm{Hom}_R(P_\bullet, N))) \subseteq \delta_{0,-1}(H^0(\mathrm{Hom}_R(M, I_\bullet)))$, and a completely symmetric argument yields also the reverse inclusion. We conclude by injectivity of $d_{-1,0}$ and $\delta_{0,-1}$.

(5) We employ the notations of the Hint. To construct a map $H^1(\mathrm{Hom}_R(P_\bullet, N)) \to \mathrm{coker}(\Delta^0)$, we have to verify that if $\phi_{1,-1} \in \mathrm{im}(d_{0,-1})$, then $(\delta_{1,-1}(\phi_{1,-1}), 0) \in \mathrm{im}\,\Delta^0$. Let $\phi_{0,-1} \in \mathrm{Hom}_R(P_0, N)$ be such that $\phi_{1,-1} = d_{0,-1}(\phi_{0,-1})$. By the commutativity and exactness properties of the diagram, it is straightforward to verify that $\Delta^0(\delta_{0,-1}(\phi_{0,-1})) = (\delta_{1,-1}(\phi_{1,-1}), 0)$, and thus the latter is in the image of Δ^0. Therefore, the composition $\mathrm{Ker}(d_{1,-1}) \hookrightarrow \mathrm{Hom}_R(P_1, N) \hookrightarrow C^1 \twoheadrightarrow \mathrm{coker}(\Delta^0)$ factors through $H^1(\mathrm{Hom}_R(P_\bullet, N))$, i.e. we obtain a map $\alpha : H^1(\mathrm{Hom}_R(P_\bullet, N)) \to \mathrm{coker}(\Delta^0)$ given by mapping the class of $\phi_{1,-1} \in \mathrm{Ker}(d_{1,-1})$ to the class of $(\delta_{1,-1}(\phi_{1,-1}), 0)$.
Now we verify that α is injective. To do so, suppose that $\phi_{1,-1} \in \mathrm{Ker}(d_{1,-1})$ is such that $(\delta_{1,-1}(\phi_{1,-1}), 0) \in \mathrm{im}(\Delta^0)$; we have to show that then $\phi_{1,-1} \in \mathrm{im}(d_{0,-1})$. Let $\phi_{0,0} \in \mathrm{Hom}_R(P_0, I^0)$ be such that $\Delta^0(\phi_{0,0}) = (\delta_{1,-1}(\phi_{1,-1}), 0)$. In particular, we have $\delta_{0,0}(\phi_{0,0}) = 0$, so by exactness there exists $\phi_{0,-1} \in \mathrm{Hom}_R(P_0, N)$ such that $\phi_{0,0} = \delta_{0,-1}(\phi_{0,-1})$. Hence we obtain

$$\delta_{1,-1}(\phi_{1,-1}) = d_{0,0}(\psi_{0,0}) = d_{0,0}(\delta_{0,-1}(\phi_{0,-1})) = \delta_{1,-1}(d_{0,-1}(\phi_{0,-1})),$$

and so by injectivity of $\delta_{1,-1}$ it follows that $\phi_{1,-1} = d_{0,-1}(\phi_{0,-1})$. So $\phi_{1,-1}$ is in the image of $d_{0,-1}$, and thus α is injective.
Now by a completely symmetrical argument, there exists and injective map $\beta : H^1(\mathrm{Hom}_R(M, I^\bullet)) \to \mathrm{coker}(\Delta^0)$, mapping the class of $\phi_{-1,1} \in \mathrm{Ker}(\delta_{-1,1})$ to the class of $(0, d_{-1,1}(\psi)_{-1,1})$. So what is left to show is that the image of α is the same as the image of β. To this end, let $\phi_{1,-1} \in \mathrm{Ker}(d_{1,-1})$ be arbitrary. Then by commutativity we have $d_{1,0}(\delta_{1,-1}(\phi_{1,-1})) = 0$, and so by exactness there exists $\phi_{0,0} \in \mathrm{Hom}_R(P_0, I^0)$ with $d_{0,0}(\phi_{0,0}) = \delta_{1,-1}(\phi_{1,-1})$. Then notice that

$$d_{0,1}(\delta_{0,0}(\phi_{0,0})) = \delta_{1,0}(d_{0,0}(\phi_{0,0})) = \delta_{1,0}(\delta_{1,-1}(\phi_{1,-1})) = 0$$

and thus by exactness there exists $\phi_{-1,1} \in \mathrm{Hom}_R(M, I^1)$ such that $d_{-1,1}(\phi_{-1,1}) = \delta_{0,0}(\phi_{0,0})$. By a similar string of equations as above, we obtain $d_{-1,2}(\delta_{-1,1}(\phi_{-1,1})) = 0$,

which by injectivity of $d_{-1,2}$ gives $\phi_{-1,1} \in \mathrm{Ker}(\delta_{-1,1})$. Now we verify that $\alpha(\phi_{1,-1} + \mathrm{im}(d_{0,-1})) = \beta(-\phi_{-1,1} + \mathrm{im}(\delta_{-1,0}))$. To this end, notice that

$$\Delta^0(\phi_{0,0}) = (d_{0,0}(\phi_{0,0}), \delta_{0,0}(\phi_{0,0})) = (\delta_{1,-1}(\phi_{1,-1}), d_{-1,1}(\phi_{-1,1})) = (\delta_{1,-1}(\phi_{1,-1}), 0) - (0, d_{-1,1}(-\phi_{-1,1})).$$

Thus the classes of $(\delta_{1,-1}(\phi_{1,-1}), 0)$ and $(0, d_{-1,1}(-\phi_{-1,1}))$ inside $\mathrm{coker}(\Delta^0)$ coincide, which proves $\alpha(\phi_{1,-1} + \mathrm{im}(d_{0,-1})) = \beta(-\phi_{-1,1} + \mathrm{im}(\delta_{-1,0}))$. We hence conclude that $\mathrm{im}\,\alpha \subseteq \mathrm{im}\,\beta$. By a completely symmetrical argument we also obtain the reverse inclusion, and thus we are done.

□

EPFL - Fall 2023 | Prof. Zs. Patakfalvi
Rings and modules | **Exercises**
Sheet 7

Exercise 1. Let F be an algebraically closed field, and let I, J be ideals of $R = F[x_1, ..., x_n]$. Prove that $\sqrt{I} \subseteq \sqrt{J}$ if and only if $V(J) \subseteq V(I)$.

Proof. Suppose that $\sqrt{I} \subseteq \sqrt{J}$. Note that $V(\sqrt{J}) = V(J)$ because the power of a polynomial and the polynomial itself have the same vanishing locus. Hence, if $P \in V(J)$ then $f(P) = 0$ for all $f \in \sqrt{J}$. But then $f(P) = 0$ for all $f \in I$ because $I \subseteq \sqrt{I} \subseteq \sqrt{J}$, and so $P \in V(I)$. Thus $V(J) \subseteq V(I)$.

Now suppose that $V(J) \subseteq V(I)$. Then $I(V(I)) \subseteq I(V(J))$, since $f \in I(V(I))$ iff f vanishes on $V(I)$, but in particular then f vanishes on $V(J)$. By the Nulstellensatz this implies that $\sqrt{I} \subseteq \sqrt{J}$. □

Exercise 2. Let F be an algebraically closed field, and let I, J be ideals of $R = F[x_1, ..., x_n]$. Show that

(1) $V(I) \cup V(J) = V(I \cap J) = V(IJ)$
(2) $V(I) \cap V(J) = V(I + J)$

Proof. (1) First we show that $V(I) \cup V(J) \subseteq V(I \cap J) \subseteq V(IJ)$. As $IJ \subseteq I \cap J \subseteq I$, by the previous question $V(I) \subseteq V(I \cap J) \subseteq V(IJ)$ and so by symmetry $V(I) \cup V(J) \subseteq V(I \cap J) \subseteq V(IJ)$.

For the other inclusion, suppose conversely that there exists $P \in V(IJ) \setminus (V(I) \cup V(J))$. As P is not in $V(I) \cup V(J)$ we can find $f \in I$ such that $f(P) \neq 0$ and $g \in J$ such that $g(P) \neq 0$. But then $(fg)(P) \neq 0$ and $fg \in IJ$. This contradicts $P \in V(IJ)$.

(2) As $I \subseteq I + J$ we have $V(I + J) \subseteq V(I)$. So by symmetry $V(I + J) \subseteq V(I) \cap V(J)$.

Conversely suppose $P \in V(I) \cap V(J)$. Then $f(P) = 0$ for every $f \in I$ and $g(P) = 0$ for every $g \in J$, hence $(f + g)(P) = 0$ for every $f + g \in I + J$. Thus $P \in V(I + J)$ and we conclude $V(I + J) = V(I) \cap V(J)$

Remark: Let $(I_i)_{i \in \Sigma}$ be a collection of ideals of $R = F[x_1, \ldots, x_n]$, where Σ is an infinite indexing set. The same argument as in point (2) above shows that $\bigcap_i V(I_i) = V(\sum_i I_i)$. However, it is not true that in general $\bigcup_i V(I_i) = V(\bigcap_i I_i)$. For example, let $R = \mathbb{C}[x]$, $\Sigma = \mathbb{N}$ and $I_n = (x - n)$. Then $\bigcup_n V(x - n) = \mathbb{N}$ and $V(\bigcap_n (x - n)) = V(0) = \mathbb{C}$. □

Exercise 3. Let R be a commutative ring, and let I, J be ideals of R. In both $\mathrm{Spec}(R)$ and $\text{m-Spec}(R)$, show that

(1) $V(I) \cup V(J) = V(I \cap J) = V(IJ)$
(2) $V(I) \cap V(J) = V(I + J)$

Proof. (1) Again, since $IJ \subseteq I \cap J \subseteq I$, $V(I) \subseteq V(I \cap J) \subseteq V(IJ)$. Doing the same for J, we deduce that

$$V(I) \cup V(J) \subseteq V(I \cap J) \subseteq V(IJ)$$

so we are left to show that $V(IJ) \subseteq V(I) \subseteq V(J)$. Let $\mathfrak{p}$ be a prime ideal containing IJ, and assume by contradiction that both $I \nsubseteq \mathfrak{p}$ (let $x \in I \setminus \mathfrak{p}$) and $J \nsubseteq \mathfrak{p}$ (let $y \in I \setminus \mathfrak{p}$). Since $\mathfrak{p}$ is prime, $xy \in IJ \setminus \mathfrak{p}$, which contradicts that $IJ \subseteq \mathfrak{p}$.

(2) Since $I \subseteq I+J$, $V(I+J) \subseteq V(I)$. Doing the same for J gives $V(I+J) \subseteq V(I) \cap V(J)$. On the other hand, if $\mathfrak{p}$ contains both I and J, it contains $I+J$, so $V(I) \cap V(J) \subseteq V(I+J)$.

□

Exercise 4. ∘ Let R, S be commutative rings, and let $f : R \to S$ be a ring morphism. Show that there is an induced continuous map $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$.
∘ Let R be a ring and I an ideal. Show that the morphism $\mathrm{Spec}(R/I) \to \mathrm{Spec}(R)$ induced by the quotient map corresponds to the inclusion of the closed subset $V(I) \subseteq \mathrm{Spec}(R)$.

Proof. ∘ Let $\theta : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ be defined by $\theta(\mathfrak{p}) = f^{-1}(\mathfrak{p})$ (recall from basic ring theory that the preimage of a prime ideal is always prime). To show the continuity of θ, we show that the preimage of closed subsets is closed. Let $V(I) \subseteq \mathrm{Spec}(R)$ be a closed subsets: we claim that $\theta^{-1}(V(I)) = V((f(I)))$. If $\mathfrak{p} \in V((f(I)))$, then in particular $\mathfrak{p} \supseteq f(I)$, so $\theta(\mathfrak{p}) = f^{-1}(\mathfrak{p}) \supseteq I$.
Conversely, if $\mathfrak{p} \in \theta^{-1}(V(I))$, then $I \subseteq \theta(\mathfrak{p}) = f^{-1}(\mathfrak{p})$, and hence $f(I) \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is an ideal, we deduce that $(f(I)) \subseteq \mathfrak{p}$ so we conclude.
∘ This is an immediate consequence of the correspondence theorem.

□

Exercise 5. Prove that $Z = \{(u^3, u^2v, uv^2, v^3) : u, v \in \mathbb{C}\} \subset \mathbb{C}^4$ is an algebraic set (i.e. there exists an ideal I of $\mathbb{C}[x_1, x_2, x_3, x_4]$ such that $Z = V(I)$). Find $I(Z)$.
[*Hint:* Make sure you have everything!]

Proof. First we prove that Z is an algebraic set. To start, let $R = \mathbb{C}[w, x, y, z]$; by trying around a bit one finds that the polynomials $x^2 - wy$, $y^2 - xz$ and $wz - xy$ vanish on Z. So if $I := (x^2 - wy, y^2 - xz, wz - xy) \subseteq R$, then $Z \subseteq V(I)$. We are now going to prove that $Z = V(I)$, and hence that Z is algebraic. In order to do so, let $P = (x_0, x_1, x_2, x_3) \in V(I)$ be arbitrary. Now notice that

$$x_1^3 \overset{x^2-wy}{=} x_0x_1x_2 \overset{wz-xy}{=} x_0^2x_3,$$

where the polynomial over the equality sign indicates which equation is used. Similarly, we have

$$x_2^3 \overset{y^2-xz}{=} x_1x_2x_3 \overset{wz-xy}{=} x_0x_3^2.$$

Therefore, if $x_0 = 0$, then $x_1 = x_2 = 0$ as well, and hence by choosing any $v \in \mathbb{C}$ such that $v^3 = x_3$ we see that $P \in Z$. Similarly, if $x_3 = 0$ then $x_1 = x_2 = 0$ and by choosing any $u \in \mathbb{C}$ with $u^3 = x_0$ we obtain $P \in Z$. Hence we may suppose that $x_0x_3 \neq 0$.
Now let $\tilde{u}, \tilde{v} \in \mathbb{C} \setminus \{0\}$ be such that $x_0 = \tilde{u}^3$ and $x_3 = \tilde{v}^3$. By substituting this into the above two equations, we obtain that there exist $\alpha, \beta \in \mathbb{C}$ such that $\alpha^3 = \beta^3 = 1$ and

$$x_1 = \alpha\tilde{u}^2\tilde{v} \quad \text{and} \quad x_2 = \beta\tilde{u}\tilde{v}^2.$$

Now notice that

$$\tilde{u}^3\tilde{v}^3 = x_0x_3 = x_1x_2 = \alpha\beta\tilde{u}^3\tilde{v}^3$$

and so as $\tilde{u}\tilde{v} \neq 0$ we obtain $\alpha\beta = 1$. So by introducing $u = \alpha\tilde{u}$ and $v = \beta\tilde{v}$, we obtain $x_0 = u^3$, $x_1 = u^2v$, $x_2 = uv^2$ and $x_3 = v^3$. Hence $P \in Z$, so we conclude that $Z = V(I)$, and

thus Z is algebraic.

Now to finish the exercise, we are going to prove that $I = I(Z)$; by the above we already know $I \subseteq I(Z)$. Let us investigate the class $f + I$ of a polynomial $f \in R$. By using the equation $xy - wz \in I$, we may suppose that no monomial in f contains both x and y. Then by using the equations $x^3 - w^2z, y^3 - wz^2 \in I$, we may assume that no monomial in f is divisible by x^3 nor by y^3. Finally, by using the equations $x^2 - wy, y^2 - xz \in I$, we may suppose that no monomial in f is divisible by x^2 nor y^2. In conclusion, we have that for every $f \in R$ there exist $p_0, p_1, p_2 \in \mathbb{C}[w, z]$ such that

$$f + I = p_0 + xp_1 + yp_2 + I.$$

Now in order to prove the inclusion of $I(Z)$ inside I, let $f \in I(Z)$ be arbitrary. Consider the $\mathbb{C}$-algebra morphism

$$\Phi : \mathbb{C}[w, x, y, z] \to \mathbb{C}[u, v]$$
$$w \mapsto u^3,\ x \mapsto u^2v,\ y \mapsto uv^2,\ z \mapsto v^3.$$

Then as $f \in I(Z)$, we have that $\Phi(f)$ vanishes on every point of $\mathbb{C}^2$, and thus $\Phi(f) = 0$. In particular, we have $x^2 - wy, y^2 - xz, wz - xy \in \operatorname{Ker}\Phi$, and so $I \subseteq \operatorname{Ker}\Phi$. Now by the argument in the beginning of this paragraph, there exist $p_0, p_1, p_2 \in \mathbb{C}[w, z]$ and $g \in I$ such that $f = p_0 + xp_1 + yp_2 + g$. Hence, as $\Phi(f) = \Phi(g) = 0$, we obtain

$$0 = \Phi(p_0 + xp_1 + yp_2) = p_0(u^3, v^3) + u^2vp_1(u^3, v^3) + uv^2p_2(u^3, v^3)$$

inside $\mathbb{C}[u, v]$. This then shows that $p_0 = p_1 = p_2 = 0$, and thus $f = g \in I$. As $f \in I(Z)$ was arbitrary, we conclude $I(Z) \subseteq I$, and thus $I(Z) = I$.

It is quite natural to expect the dimension of an algebraic set to be equal to the dimension of the space it is embedded into minus the number of generators of its ideal, as in linear algebra. This example shows that this idea is false in general.

□

Exercise 6. Let F be an algebraically closed field, and $X \subseteq F^m$ an algebraic set with ideal $I = I(X)$. Define the coordinate ring $A(X)$ of X to be $A(X) := F[x_1, \ldots, x_m]/I$. Notice that every element of $A(X)$ naturally defines a set-map from X to F, and thus one may think of $A(X)$ as the set of global algebraic functions on X.

(1) If $X = V(I) \subseteq F^m$, and $Y = V(J) \subseteq F^n$ are algebraic sets with ideals $I = I(X)$ and $J = I(Y)$, then a morphism $f : X \to Y$ is defined to be a set-map from the points of X to the points of Y, for which the following holds: there exists a vector $(h_1, \ldots, h_n)$ of polynomials $h_i \in F[x_1, \ldots, x_m]$, such that for every $\underline{a} \in X$ we have $f(\underline{a}) = (h_1(\underline{a}), h_2(\underline{a}), \ldots, h_n(\underline{a})) \in Y$.

Show that whenever there is a morphism $f : X \to Y$ of algebraic sets as defined above, there is a unique homomorphism of F-algebras $\lambda_f : A(Y) \to A(X)$, such that

the following diagram commutes.

$$\begin{array}{ccc} F[y_1,\dots,y_n] & \xrightarrow{y_i \mapsto h_i} & F[x_1,\dots,x_m] \\ \downarrow & & \downarrow \\ A(Y) & \xrightarrow{\lambda_f} & A(X) \end{array}$$

Here the vertical arrows are the quotient maps stemming from the definition of $A(X)$ and $A(Y)$, and the top horizontal map is given by sending y_i to $h_i(x_1, ..., x_m)$.

(2) With setup as above, show that if there is a homomorphism of F-algebras $\lambda : A(Y) \to A(X)$, then there is a morphism $f : X \to Y$ such that $\lambda = \lambda_f$. Furthermore, all choices of f are the same (as set-maps from the points of X to the points of Y).

Proof. (1) Let $I = I(X)$ and $J = I(Y)$. Let ϕ be the given F-algebra homomorphism $F[y_1, ..., y_n] \to F[x_1, ..., x_m]$, sending y_j to h_j.

If the homomorphism $\lambda = \lambda_f$ exists, the diagram implies that for any $p + J \in A(Y)$ we must have $\lambda(p + J) = \phi(p) + I$. So λ is unique if it exists.

In order to show that it exists, let $\pi_X : F[x_1, \dots, x_m] \to A(X)$ and $\pi_Y : F[y_1, \dots, y_n] \to A(Y)$ be the projection maps. We want to show that $\pi_X \circ \phi$ factors through $A(Y)$, and to this end we want to show that $J \subseteq \mathrm{Ker}(\pi_X \circ \phi)$. So let $p \in J$ be arbitrary. Then $\phi(p) = p(h_1(x_1, \dots, x_m), \dots, h_n(x_1, \dots, x_m))$. Hence, if we evaluate $\phi(p)$ at a point $\underline{a} \in X$, we obtain $\phi(p)(\underline{a}) = p(h_1(\underline{a}), \dots, h_n(\underline{a})) = p(f(\underline{a}))$. But then as $f(\underline{a}) \in Y$ and $p \in J$, we obtain $\phi(p)(\underline{a}) = p(f(\underline{a})) = 0$. Hence $\phi(p)$ vanishes on every point of X, and thus $\phi(p) \in I$. Hence $p \in \mathrm{Ker}(\pi_X \circ \phi)$, and thus $J \subseteq \mathrm{Ker}(\pi_X \circ \phi)$. Therefore, there exists a morphism of F-algebras $\lambda : A(Y) \to A(X)$ such that $\pi_X \circ \phi = \lambda \circ \pi_Y$, i.e. the above diagram commutes.

(2) Now suppose we are given a homomorphism $\lambda : A(Y) \to A(X)$. For $j = 1, ..., n$, choose $h_j \in F[x_1, \dots, x_m]$ such that $\lambda(y_j + J) = h_j + I$. Let $\phi : F[y_1, \dots, y_n] \to F[x_1, \dots, x_m]$ be defined as before, i.e. y_j is mapped to h_j.
Define the morphism of algebraic sets $f : F^m \to F^n$ by $f(\underline{a}) = (h_1(\underline{a}), ..., h_m(\underline{a}))$. We must show that if $\underline{a} \in X$ then $f(\underline{a}) \in Y$. For this it is enough to show that $p(f(\underline{a})) = 0$ for all $p \in J$, by the Nullstellensatz. But as in the previous point, we have $p(f(\underline{a})) = p(h_1(\underline{a}), ..., h_m(\underline{a})) = \phi(p)(\underline{a})$. So if we can show that $\phi(p) \in I(X)$ then we are done. But now notice that by definition of $h_1, \dots, h_n$ we have $\phi(p) + I = \lambda(p + J) = 0$, so $\phi(p) \in I$. Hence $f : F^m \to F^n$ restricts and co-restricts to a morphism of algebraic sets $f : X \to Y$. By comparing with the previous point, it is then straightforward to check that $\lambda = \lambda_f$, as both send $y_j + J$ to $h_j + I$.

Now we must show that two choices of lifting h_i and h_i' of $\overline{h}_i$ result in the same map on points of X. This holds because $h_i' = h_i + p_i$ for some $p_i \in I$, as the lifting is well defined up to addition of an element of I, but p_i vanishes on all points of X. Hence $h_i(\underline{a}) = h_i'(\underline{a})$ for all $\underline{a} \in X$, so $(h_1, \dots, h_n)$ and $(h_1', \dots, h_n')$ define the same set-map. □

Exercise 7. Let F be an algebraically closed field. Let X be an algebraic set in F^n with ideal $I(X) = I$. Prove that points of F^n contained in X are naturally in bijection with maximal ideals of the coordinate ring $A(X) = F[x_1, ..., x_n]/I$.

Proof. Given a point $P = (a_1, ..., a_n) \in X$, let $\mathfrak{m}_P = (x_1 - a_1, ..., x_n - a_n)$. Since $P \in X$, we have $I \subseteq \mathfrak{m}_P$ by Exercise 1. Thus $\mathfrak{m}_P$ is a maximal ideal containing $I(X)$, and hence defines a maximal ideal $\overline{\mathfrak{m}}_P$ of $A(X) = F[x_1, ..., x_n]/I$. Conversely, a maximal ideal $\overline{\mathfrak{m}}$ of $A(X) = F[x_1, ..., x_n]/I$ is equivalent to a maximal ideal $\mathfrak{m}$ of $F[x_1, ..., x_n]$ containing I. By the Weak Nullstellensatz $\mathfrak{m} = (x_1 - a_1, ..., x_n - a_n)$, for some $a_i \in F$. The containment $I \subseteq \mathfrak{m}$ implies that $P = (a_1, ..., a_n) \in X$, and thus $\overline{\mathfrak{m}} = \overline{\mathfrak{m}}_P$. Thus the set of maximal ideals of $A(X)$ is given by $\{\overline{\mathfrak{m}}_P \mid P \in X\}$. Finally, suppose that $\overline{\mathfrak{m}}_P = \overline{\mathfrak{m}}_Q$ for $P, Q \in X$. Then necessarily $\mathfrak{m}_P = \mathfrak{m}_Q$ and thus $\{P\} = V(\mathfrak{m}_P) = V(\mathfrak{m}_Q) = \{Q\}$, and thus $P = Q$. Thus there is a bijection between X and the set of maximal ideals $A(X)$.

□

EPFL - Fall 2022	Prof. Zs. Patakfalvi
Rings and modules	**Exercises**
Sheet 8 - Solutions	17 November 2022

There was one bonus exercise on this problem sheet. The exercise was denoted by the symbol ♠ next to the exercise number.

Exercise 1. Let R be a ring and let M, K, L and N be R-modules. Assume that $\operatorname{Ext}^i_R(M,N)$, $\operatorname{Ext}^i_R(K,N)$ and $\operatorname{Ext}^i_R(L,N)$ have finite length for all $i \geq 0$, and that there exist integers s such that they are all zero for all $i > s$. Show that if

$$0 \longrightarrow K \longrightarrow M \longrightarrow L \longrightarrow 0$$

is a short exact sequence, then

$$\sum_{i=0}^{s}(-1)^i \operatorname{length}\operatorname{Ext}^i_R(M,N) = \sum_{i=0}^{s}(-1)^i \operatorname{length}\operatorname{Ext}^i_R(K,N) + \sum_{i=0}^{s}(-1)^i \operatorname{length}\operatorname{Ext}^i_R(L,N)$$

Proof. There is an induced long exact sequence on Ext^i's, since this sequence eventually terminates with all terms equal to zero this follows directly from Exercise 5.1 on Sheet 4. *Note:* Exercise 5.1 on Sheet 4 was stated for finitely generated modules M_i over an Artinian and Noetherian ring, however we only used that the M_i's where of finite length in the solution. □

Exercise 2 (Nullstellensatz for $\operatorname{Spec} R$)**.** Let R be a commutative ring. Given a closed subset $Z \subseteq \operatorname{Spec} R$, define $I(Z) := \{f \in R,\ Z \subseteq V(f)\}$. Show that $I(Z)$ is an ideal, and that for all ideals $I \subseteq \operatorname{Spec} R$,

$$I(V(I)) = \sqrt{I}$$

In particular, show that for all ideals I, J of R,

$$V(I) = V(J) \iff \sqrt{I} = \sqrt{J}$$

Proof. Throughout, the letter $\mathfrak{p}$ always denotes a prime ideal.

We will show that $I(Z)$ is an ideal by showing that if $Z = V(I)$, then $I(Z) = \sqrt{I}$, which we know to be an ideal.

Therefore, let us first prove that $I(V(I)) \subseteq \sqrt{I}$, so let $f \in I(V(I))$. By definition, $V(I) \subseteq V(f)$, hence by definition

$$f \in \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p} = \sqrt{I}$$

where the equality is Proposition 6.4.5 in the notes.

On the other hand, if $f \in \sqrt{I}$, then $f^n \in I$ for some n. Hence, $V(I) \subseteq V(f^n)$, so to conclude that $f \in I(V(I))$, we are left to show that $V(f) = V(f^n)$. Since $(f^n) \subseteq (f)$, $V(f) \subseteq V(f^n)$. Conversely, if $\mathfrak{p} \ni f^n$, then also $\mathfrak{p} \ni f$ since $\mathfrak{p}$ is prime, so $V(f^n) \subseteq V(f)$ and we are done.

In the second statement, the "left to right" implication is immediate with what we just did, and the "right to left" follows from the general fact that for any ideal I, $V(I) = V(\sqrt{I})$. This is a restatement that for all primes $\mathfrak{p}$,

$$\mathfrak{p} \supseteq I \iff \mathfrak{p} \supseteq \sqrt{I}$$

□

Exercise 3. Let R be a commutative ring and $I \subseteq R$ be a radical ideal. Show that I is prime if and only if $V(I)$ is an irreducible topological space.

Proof. We will use exercise 2 of this sheet and exercise 3 of sheet 7 without further mention.

Suppose first that I is prime, and assume that $V(I) = V(J) \cup V(K)$ with J, K radical. Then

$$I = \sqrt{I} = I(V(I)) = I(V(J) \cup V(K)) = I(V(J \cap K)) = \sqrt{J \cap K} = J \cap K$$

(the intersection of two radical ideals is radical). If by contradiction $V(J) \neq V(I)$ (or in other words $I \subsetneq J$) and $V(J) \neq V(I)$ (i.e. $I \subsetneq K$), then there exist $a \in J \setminus I$, $b \in K \setminus I$. However, $ab \in J \cap K = I$, which contradicts the fact that I is prime.

Conversely, assume $V(I)$ is an irreducible topological space, and assume by contradiction that I is not prime. Then there exist a, $b \notin I$ such that $ab \in I$. But then, $V(I) \nsubseteq V(a)$, $V(I) \nsubseteq V(b)$ and $V(I) \subseteq V(ab) = V(a) \cap V(b)$. But then, setting $Z_1 = V(a) \cap V(I)$ and $Z_2 = V(b) \cap V(I)$ gives $V(I) = Z_1 \cup Z_2$, with none of the Z_i being $V(I)$. This contradicts that $V(I)$ is irreducible. □

Exercise 4. Let $R = \mathbb{C}[x, y, z]$ and $I = (xy - z^2, x^2 - y^2) \subseteq R$. Identify $V(I) \subset \mathbb{C}^3$. Notice that this naturally breaks into smaller algebraic sets. What are the ideals of each piece?

Proof. A point $(p, q, r) \in \mathbb{C}^3$ is in $V(I)$ if and only if $pq - r^2 = 0$ and $p^2 - q^2 = (p-q)(p+q) = 0$. So either $p = q$ or $p = -q$. In the first case, the first equation becomes $0 = p^2 - r^2 = (p - r)(p + r)$ and so either $p = r$ or $p = -r$. In the second case, the first equation becomes $0 = -p^2 - r^2 = (p - ir)(p + ir)$ and so $r = ip$ or $r = -ip$. Therefore

$$V(I) = \underbrace{\{(p, p, p) : p \in \mathbb{C}\}}_{:=V_1} \cup \underbrace{\{(p, p, -p) : p \in \mathbb{C}\}}_{:=V_2} \cup \underbrace{\{(p, -p, ip) : p \in \mathbb{C}\}}_{:=V_3} \cup \underbrace{\{(p, -p, -ip) : p \in \mathbb{C}\}}_{V_4}$$

The ideals of these four pieces are $\mathfrak{p}_1 := (x-y, x-z)$, $\mathfrak{p}_2 := (x-y, x+z)$, $\mathfrak{p}_3 := (x+y, x+iz)$ and $\mathfrak{p}_4 := (x + y, x - iz)$ respectively. Notice that they are all prime (because up to a linear change of variables they are all just (x, y)), and thus V_i is irreducible for all i. Hence $V(I)$ doesn't split up further. □

Exercise 5. Let F be an algebraically closed field. Let X and Y be algebraic sets in F^n.

(1) Prove that $I(X \cup Y) = I(X) \cap I(Y)$
(2) By considering $X = V(x^2 - y)$ and $Y = V(y)$ for the ideals $(x^2 - y)$ and (y) in $F[x, y]$, show that it need not be true that $I(X \cap Y) = I(X) + I(Y)$.
(3) Prove that in general $\sqrt{I(X) + I(Y)} = I(X \cap Y)$.

Proof. (1) Suppose $f \in I(X \cup Y)$. Then $f(P) = 0$ for all $P \in X$ and all $p \in Y$. So $f \in I(X)$ and $f \in I(Y)$. Conversely, suppose $f \in I(X) \cap I(Y)$. Then $f(P) = 0$ for all $P \in X$ and all $P \in Y$. Therefore $f \in I(X \cup Y)$.

(2) $I(X) = (x^2 - y)$, $I(Y) = (y)$ and $I(X \cap Y) = I(\{(0, 0)\}) = (x, y)$. But $I(X) + I(Y) = (x^2, y)$.

(3) This follows from a question on the previous exercise sheet and the Nulstellensatz. Let $I = I(X)$ and $J = I(Y)$, so $V(I) = X$ and $V(J) = Y$. By Exercise 2 on Exercise sheet 7 we have $I(X \cap Y) = I(V(I + J))$. But by the Nulstellensatz, $I(V(I + J)) = \sqrt{I + J}$.

□

Review exercises for material from "Anneaux et corps"

Exercise 6. Show that $x^3 + y^7 \in k[x, y]$ is irreducible.
[*Hint:* Use the consequence of Gauss's theorem saying that for a unique factorisation domain R and a primitive polynomial $f \in R[t]$, we have that f is irreducible in $\mathrm{Frac}(R)[t]$ if and only if it is irreducible in $R[t]$.]

Proof. We use the hint for $R = k[y]$. It is therefore sufficient to check that $x^3 + y^7$ is irreducible in $k(y)[x]$. Suppose it is not, since the degree is three it has to have a linear term in any factorisation and hence there exists f, g coprime such that $\frac{f}{g}$ is a root of $x^3 + y^7$. We write: $\frac{f^3}{g^3} + y^7 = 0$, and hence $f^3 = -g^3 y^7$. It then follows that y^3 divides f but then also that y divides g, which contradicts coprimality.

□

Review exercises for material from "Anneaux et corps"

Exercise 7. Let $R = k[x, y, z]$. Show that $(xz^3 + yz^3 - y^2z^2 + xyz - xy)$ is a prime ideal of R.
[*Hint*: Use Eisenstein's Criterion.]

Proof. View $f = xz^3 + yz^3 - y^2z^2 + xyz - xy$ as an element of $k[x, y][z]$, so $f = (x + y)z^3 - y^2z^2 + xyz - xy$. This satisfies the hypotheses of Eisenstein's criterion for $p = y$, and so f is irreducible in R. Thus (f) is a prime ideal.

□

Review exercises for material from "Anneaux et corps"

Exercise 8. Solve the following exercises:

(1) Consider the polynomial $f = X^3Y + X^2Y^2 + Y^3 - Y^2 - X - Y + 1$ in $\mathbb{C}[X, Y]$. Write it as an element of $(\mathbb{C}[X])[Y]$, that is collect together terms according to powers of Y, and then use Eisenstein's criterion to show that f is prime in $\mathbb{C}[X, Y]$.
(2) Let F be any field. Show that the polynomial $f = X^2 + Y^2 - 1$ is irreducible in $F[X, Y]$, unless F has characteristic 2. What happens in that case?

Proof. (1) $p = X - 1$ is prime in $\mathbb{C}[X]$ and satisfies the conditions of Eisenstein's criterion for f.
(2) Eisenstein's criterion gives that $X^2 + Y^2 - 1$ is irreducible if $Y - 1 \neq Y + 1$, i.e. it is irreducible if $1 \neq -1$, i.e. unless the characteristic is 2. In characteristic 2 we have $X^2 + Y^2 - 1 = (X + Y + 1)^2$ and hence this polynomial is not irreducible.

□

Exercise 9. Show the following:

(1) Let $F \subseteq L$ be a field extension, and suppose $a_1, \ldots, a_n$ are elements of L which are algebraically independent over F. Prove that $F(a_1, \ldots, a_n)$ is isomorphic to the fraction field of the polynomial ring $F[x_1, \ldots, x_n]$.

(2) Let $F \subseteq L$ be a field extension. Show that a subset of L is a transcendence basis for L over F if and only if it is a maximal algebraically independent set. As a consequence show that a transcendence basis exists for any field extension $F \subseteq L$.

Proof. (1) Define a ring homomorphism $\phi : F[x_1, ..., x_n] \to L$ by $x_i \mapsto a_i$ and $\phi|_F = \mathrm{id}_F$. We claim this is injective. For suppose $\phi(f) = 0$ for some f. This gives a polynomial with coefficients in F satisfied by the a_i, and so by definition of algebraic independence, $f = 0$. This injectivity, along with the existence of inverses in L, means we can extend ϕ to an injective homomorphism $F(x_1, \ldots, x_n) \hookrightarrow L$. Lastly, the image is a field (as $F(x_1, \ldots, x_n)$ is) containing F and $a_1, \ldots, a_n$, and thus contains $F(a_1, \ldots, a_n)$. But as every element of the image is a rational function of the $a_1, \ldots, a_n$ with coefficients in F, we conclude that the image is precisely $F(a_1, \ldots, a_n)$. Hence $F(a_1, \ldots, a_n)$ is isomorphic to $F(x_1, \ldots, x_n)$.

(2) Suppose the set $\{a_i\}_{i \in I}$ is a transcendence basis for $L \supseteq F$, with some (perhaps infinite) indexing set I. It is algebraically independent by definition, so we need to show it is maximal subject to this. Suppose not, so there is some element a of L which such that $\{a\} \cup \{a_i\}_{i \in I}$ is algebraically independet. But by definition of transcendent basis, $L \supseteq F(\{a_i\}_{i \in I})$ is algebraic, so there is a non-zero polynomial $p \in F(\{a_i\}_{i \in I})[X]$ such that $p(a) = 0$. The coefficients of p are rational functions of the a_i's, so by multiplying through to clear denominators, we can view p as a non-zero multivariate polynomial with coefficients in F satisfied by some subset of $\{a_i\}_{i \in I}$ and a. This contradicts the choice of a.

Conversely, suppose $\{a_i\}_{i \in I}$ is a maximal algebraically independent set. We need to show that $L \supseteq F(\{a_i\}_{i \in I})$ is algebraic. Let $a \in L$ be arbitrary. As $\{a_i\}_{i \in I} \cup \{a\}$ is not algebraically independent there is some multivariate non-zero polynomial f with coefficients in F such that $f(a, a_{i_1}, \ldots, a_{i_n}) = 0$ for some $i_1, \ldots, i_n \in I$. This must have some non-zero a term as otherwise it gives an algebraic dependence among the a_i's. This gives a polynomial satisfied by a with coefficients in $F(\{a_i\}_{i \in I})$ by dividing through by the coefficient of the highest power of a, and thus $L \supseteq F(\{a_i\}_{i \in I})$ is algebraic.

To show that a transcendence basis exists, we use Zorn's lemma on the partially ordered set Σ of algebraically independent sets over F inside L. If Σ is empty then $L \supseteq F$ is algebraic and there is nothing to prove. Hence assume that Σ is non-empty. To apply Zorn's Lemma, we must show that any chain of algebraically independent sets has an upper bound in Σ. Suppose $(A_\alpha)_{\alpha \in \Omega}$ is such a chain, i.e. for all indexes $\alpha, \beta \in \Omega$, either $A_\alpha \subseteq A_\beta$ or $A_\alpha \supseteq A_\beta$ holds. Then $\bigcup_{\alpha \in \Omega} A_\alpha$ defines an algebraically independent set, since any polynomial relation in $\bigcup_{\alpha \in \Omega} A_\alpha$ is a polynomial relation in A_α for A_α sufficiently large. Therefore $\bigcup_{\alpha \in \Omega} A_\alpha$ is an uppe rbound for the chain $(A_\alpha)_{\alpha \in \Omega}$. By Zorn's Lemma there exists a maximal algebraically independent set of elements in L. By what has already been proven such a a maximal algebraically independent set consitutes a transcendence basis for L over F.

□

Exercise 10. Prove that if $F \subseteq K \subseteq L$ are field extensions such that $\mathrm{trdeg}_F L < \infty$, then $\mathrm{trdeg}_F L = \mathrm{trdeg}_F K + \mathrm{trdeg}_K L$

Proof. By previous exercises $\mathrm{trdeg}_F L$ is the cardinality of any maximal algebraically F-independent subset $\{\alpha_1, \dots, \alpha_{\mathrm{trdeg}_F L}\} \subseteq L$. Let $B = \{\beta_1, \dots, \beta_{\mathrm{trdeg}_F K}\} \subseteq K$ be a maximal algebraically F-independent subset of K and let $C = \{\gamma_1, \dots, \gamma_{\mathrm{trdeg}_K L}\} \subseteq L$ be a maximal algebraically K-independent subset of L. By construction,

$$B \cup C = \{\beta_1, \dots, \beta_{\mathrm{trdeg}_F K}, \gamma_1, \dots, \gamma_{\mathrm{trdeg}_K L}\} \subseteq L$$

is an algebraically F-independent subset of L. To conclude, we have to show that $F(B \cup C) \subseteq L$ is an algebraic extension. By elementary field theory, algebraicity is transitive, and so it it sufficient to show that both $F(B \cup C) \subseteq K(C)$ and $K(C) \subseteq L$ are algebraic. The latter is true by definition, so it remains to show that $F(B \cup C) \subseteq K(C)$ is algebraic. But now notice that $K(C) = (F(B \cup C))(K)$ (i.e. the field obtained by adjoining the elements of K to $F(B \cup C)$). So it is enough to show that every element of K is algebraic over $F(B \cup C)$, as then every rational function of the elements of C with coefficients in C is algebraic too. This is now automatic, since $F(B) \subseteq K$ is algebraic. Hence $F(B \cup C) \subseteq K(C)$ is algebraic, and thus also $F(B \cup C) \subseteq L$. So $B \cup C$ is a transcendence basis of L over F, which proves $\mathrm{trdeg}_F L = \mathrm{trdeg}_F K + \mathrm{trdeg}_K L$. □

Exercise 11. ♠ Consider the finitely generated $\mathbb{C}$-algebra

$$R := \mathbb{C}[x, y, z, t] \Big/ (xz - y^2, yt - z^2, xt - yz).$$

- Show that R is integral.
  Hint: One way to proceed is as follows: show that the morphism $\mathbb{C}[x, y, z, t] \to \mathbb{C}[u, v]$ given by sending $f(x, y, z, t)$ to $f(u^3, u^2v, uv^2, v^3)$ induces an injection $R \hookrightarrow \mathbb{C}[u, v]$.
- Calculate the transcendence degree over $\mathbb{C}$ of the fraction field of R.

Proof.

- We have seen in the proof of Exercise 5 in sheet 7 that the kernel of the morphism

$$\Phi : \mathbb{C}[x, y, z, w] \to \mathbb{C}[u, v]$$
$$x \mapsto u^3,\ y \mapsto u^2v,\ z \mapsto uv^2,\ w \mapsto v^3.$$

  is exactly $I = (y^2 - xz, z^2 - yw, xw - yz)$. Hence, we have an embedding of rings $R/I \hookrightarrow \mathbb{C}[u, v]$. Since the latter ring is integral, so is $R = \mathbb{C}[x, y, z, w]/I$.
- By the previous point, there is an inclusion of fields $\mathrm{Frac}(R) \subseteq \mathbb{C}(u, v)$. Moreover, both u and v are algebraic over $\mathrm{Frac}(R)$. Indeed, u^3 and v^3 are in R (hence also in $\mathrm{Frac}(R)$). Thus, the extension $\mathrm{Frac}(R) \subseteq \mathbb{C}(u, v)$ is algebraic, so by Exercise 10, we have

$$\mathrm{trdeg}_{\mathbb{C}}(\mathrm{Frac}(R)) = \mathrm{trdeg}_{\mathbb{C}}(\mathbb{C}(u, v)) = 2.$$

□

EPFL - Fall 2023 Prof. Zs. Patakfalvi
Rings and modules **Exercises**
Sheet 9 - Solutions

Exercise 1. Show the following:

(1) Prove that the only prime ideal of height zero in a domain is the ideal (0).
(2) Prove that a prime ideal of height 1 in a UFD is principal.
(3) Compute the prime ideals of height zero in $\mathbb{R}[x,y]/(xy)$.
[*Hint*: Recall that there is a one-to-one correspondence between the prime ideals R containing I and the prime ideals of R/I.]

Proof. (1) In any ring R, $(0) \subseteq \mathfrak{p}$ for every prime ideal $\mathfrak{p}$, hence (0) is prime (and thus R a domain) if and only if it is the only prime ideal of height zero.

(2) Let $\mathfrak{p}$ be a prime ideal of height one. We will prove that $\mathfrak{p}$ contains a prime element p. If $\mathfrak{p}$ contains a prime element p then $(p) = \mathfrak{p}$, since $(p) \subseteq \mathfrak{p}$ and the only prime ideal that is strictly contained in $\mathfrak{p}$ is (0) by the previous point. Let $f \in \mathfrak{p}$ be non-zero (this is possible since $\mathfrak{p} \neq 0$ because $\mathfrak{p}$ has height one), let $f = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the unique (up to multiplication by units) prime decomposition of f. Since $\mathfrak{p}$ is prime, we must have $p_i \in \mathfrak{p}$ for some $i \in \{1, \dots r\}$. We conclude that $\mathfrak{p} = (p_i)$.

(3) The prime ideals of height zero in $\mathbb{R}[x,y]/(xy)$ correspond to the primes $\mathfrak{p} \subseteq \mathbb{R}[x,y]$ that contain xy and that do not contain any other prime ideal $\mathfrak{p}'$ such that $xy \in \mathfrak{p}'$. Suppose $xy \in \mathfrak{p}$, then either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$, hence either $(x) \subseteq \mathfrak{p}$ or $(y) \subseteq \mathfrak{p}$. Now since (x) and (y) both are prime ideals that contain xy we conclude that $\mathfrak{p} = (x)$ or $\mathfrak{p} = (y)$. □

Exercise 2. Show the following:

(1) If R is a domain with $\dim R = 0$, then R is a field.
(2) We say that a ring R is reduced if there are no nilpotent elements in R. That is, if $r \in R$ is such that $r^n = 0$ for some n, then $r = 0$. Give an example of a reduced ring R of dimension zero which is not a field.

Proof. (1) A ring R is a domain if and only if the zero ideal is prime. A ring R is a field if and only if the zero ideal is maximal. Therefore, a domain is a field if and only if it is of dimension zero.

(2) Let F be a field and define a ring structure on $R = F \times F$ by coordinatewise multiplication. To compute the dimension of R we investigate its prime ideals. Let $\mathfrak{p}$ be a prime ideal. As $(1,0) \cdot (0,1) = (0,0) \in \mathfrak{p}$, we must have either $(1,0) \in \mathfrak{p}$ or $(0,1) \in \mathfrak{p}$. Hence either $F \times \{0\} \subseteq \mathfrak{p}$ or $\{0\} \times F \subseteq \mathfrak{p}$. Suppose we are in the first case; the other case is completely symmetric. If $F \times \{0\} \subsetneq \mathfrak{p}$ then there is an element $(a,b) \in \mathfrak{p}$ with $b \neq 0$, but then $(1,0), (a,b)$ is an F basis of $F \times F$ and thus $F \times F = \mathfrak{p}$, contradiction. Thus we conclude $\mathfrak{p} = F \times \{0\}$. This is indeed a prime ideal, because if $(a,b) \cdot (c,d) \in F \times \{0\}$ then $bd = 0$ and thus either $(a,b) \in F \times \{0\}$ or $(c,d) \in F \times \{0\}$. Together with the case with flipped coordinates, we conclude that the prime ideals of $F \times F$ are precisely $F \times \{0\}$ and $\{0\} \times F$. Hence, as neither contains the other, $F \times F$ has dimension 0. On the other hand, suppose that $(a,b)^n = (a^n, b^n) = (0,0)$ for some $(a,b) \in F \times F$ and $n \geq 1$. Then $a^n = 0$ and $b^n = 0$, since F is reduced this means that $a = 0$ and $b = 0$. So $F \times F$ is reduced.

□

Exercise 3. Solve the following exercises:

(1) Prove that every Artinian ring has dimension 0.
(2) Compute the dimension of the ring $\mathbb{Z}[x]/(4, x^2)$.
(3) Comupute the dimension of $\mathbb{Z}[x]$.

Proof. (1) By Exercise 1.2 of Sheet 1, every prime ideal in an Artinian ring is maximal. Hence every prime ideal has height 0, and thus an Artinian ring has dimension 0.

(2) The ring $\mathbb{Z}[x]/(4, x^2)$ is finite as a set (as a $\mathbb{Z}$-module it is isomorphic to $(\mathbb{Z}/4\mathbb{Z})^{\oplus 2}$), so in particular Artinian. Hence by the previous point, it has dimension 0.

(3) We will show that for any PID R, we have $\dim R[x] = 2$. This will require some serious work!

- Let $\pi \in R$ be a non-zero prime element (R is not a field). We then have an chain of inclusions
$$0 \subseteq (\pi) \subseteq (\pi, x)$$
and each ideal is prime. Indeed, the quotients are respectively $R[x]$, $R/(\pi)[x]$ and $R/(\pi)$ which are all domains. Thus, the height of (π, x) is at least 2, and hence $\dim(R[x]) \geq 2$.
- Let us start by studying prime ideals of height 1. We will show that if $\mathfrak{p}$ is a non-zero prime ideal of $R[x]$, then $\mathfrak{p}$ has height 1 if and only if it is principal.
Since R is a PID, it is in particular a UFD, so by Gauss' lemma $R[x]$ is also a UFD. Therefore by Exercise 1.2 any prime ideal of height 1 is principal. To see the converse, let $\mathfrak{p} = (p)$ be a principal prime ideal of $R[x]$, and let $\mathfrak{q} \subseteq \mathfrak{p}$ be a prime sub-ideal. We want to show that if $\mathfrak{q} \neq 0$, then $\mathfrak{q} = \mathfrak{p}$.
By the same argument as in Exercise 1.2 there would exist a non-zero prime element $q \in \mathfrak{q}$. But then, p divides q, so they must be equal, i.e. $\mathfrak{q} = \mathfrak{p}$.
- For any prime ideal $\mathfrak{q}$ of $R[x]$, we denote by $\mathfrak{q}^e$ the ideal of $K[x]$ generated by the elements of $\mathfrak{q}$.
Let $\mathfrak{p}$ be a prime ideal of height 2. The goal now is to show that $\mathfrak{p}^e = K[x]$.
Let $\mathfrak{q} \subseteq \mathfrak{p}$ be a prime sub-ideal of height 1, and write $\mathfrak{q} = (q)$ for q a prime element.
If $q \in R$, then $\mathfrak{p}^e$ contains q, which is invertible in $K[x]$! Therefore $\mathfrak{p}^e = K[x]$.

  Now let us deal with the case $q \notin R$. Then q is a primitive polynomial, and hence by Gauss' lemma it gives an irreducible polynomial in $K[x]$. Therefore $(q) = \mathfrak{q}^e$ is a maximal ideal in $K[x]$. Since $\mathfrak{q}^e \subseteq \mathfrak{p}^e$, we are left to show that $\mathfrak{q}^e \neq \mathfrak{p}^e$. If it was the case, then for any $a \in \mathfrak{p}$, $a \in \mathfrak{q}^e = (q)$, so we can write
$$a = \frac{q}{r}$$
with $r \in R$. Thus gives $ra = q$, and since q is primitive, r must be a unit. Therefore this would imply $\mathfrak{p} = \mathfrak{q}$, but this is impossible since $\mathfrak{p}$ has height 2.

  Thus, we have proven that $\mathfrak{p}^e = K[x]$.
- In particular, $1 \in \mathfrak{p}^e$. Write
$$1 = \sum_i \frac{a_i}{b_i} p_i$$

with $a_i, b_i \in R$ and $p_i \in \mathfrak{p}$. Multiplying by the product of the b_i's gives that $\mathfrak{p} \cap R \neq 0$. Writing this elements as a product of prime elements (which must all be in R!), we conclude that $\mathfrak{p}$ must contain a prime element $\pi \in R$. Let us show how to conclude the proof from here.
Let $\overline{\mathfrak{p}}$ denote the image of $\mathfrak{p}$ through the quotient $R[x] \to R[x]/(\pi) \cong R/(\pi)[x]$. Since $\mathfrak{p}$ is not principal (its height is not 1), $\overline{\mathfrak{p}}$ is a non-zero prime ideal of $R/(\pi)[x]$. However R is a PID, so $R/(\pi)$ is a field, whence $R/(\pi)[x]$ is a PID. This means that $\overline{\mathfrak{p}}$ is necessarily a maximal ideal, so by the correspondence theorem $\mathfrak{p}$ is maximal too.

To recapitulate, we have shown that any prime of height 2 is maximal, so there cannot be any prime of height > 2, which gives us $\dim(R[x]) \leq 2$. Thus we win thanks to the first point.

□

[*Remark:* It is a general fact that given a Noetherian commutative ring R of finite Krull dimension, $\dim(R[x]) = \dim(R)+1$. This is not so complicated once we have proven Krull's Hauptidealsatz, but we unfortunately do not have the time to cover this in the course. See the course "Modern algebraic geometry" (or any book in commutative algebra) if you want to know more about this.]

Exercise 4 (Nakayama's Lemma)**.** Let R be a ring and let M be a finitely generated R-module. Show the following:

(1) Let I be an ideal of R such that $IM = M$. Then there exists $x \in 1 + I$ such that $xM = 0$.
[*Hint:* The proof is similar to the direction (3) $\Rightarrow$ (1) in Proposition 6.2.3 of the lecture notes.]
(2) Suppose now that the ring R is local, i.e., that there is a unique maximal ideal $\mathfrak{m}$ of R. Show that if $\mathfrak{m}M = M$, then $M = 0$.
(3) For a ring R denote by $\mathrm{Jac}(R)$ the intersection of all maximal ideals of R; this is called the *Jacobson radical* of R (note also that $\mathrm{nil}(R) \subseteq \mathrm{Jac}(R)$). Show that if there is an ideal $I \subset \mathrm{Jac}(R)$ such that $IM = M$, then this implies that $M = 0$. This generalizes the previous point to any ring.

[*Hint:* Prove that in (2), (3) the element x, whose existence is assured by (1), is in fact invertible.]

Remark 0.1. Nakayama's lemma is a very powerful tool in commutative algebra and algebraic geometry, so keep it mind this exists.

To illustrate its power, recall you had an exercise about showing that if R is a commutative ring, M a finitely generated module and $f : M \to M$ a surjective endomorphism, then f is an isomorphism. Although the proof was quite tricky (you had show it in the Noetherian case, and then somehow reduce to this case), it follows immediately by considering M as an $R[x]$-module via $x \cdot m = f(m)$, and taking $I = (x)$ in (1).

Proof. (1) Let $m_1, ..., m_n$ be generators of M. As $IM = M$, we can express every $m \in M$ as an I-linear combination of $m_1, ..., m_n$. In particular, there is a matrix A with entries in I such that $A\underline{m} = \underline{m}$, where $\underline{m} \in M^{\oplus n}$ is the column vector with i^{th} entry m_i. Therefore $(\mathrm{Id}_n - A)\underline{m} = 0$. Multiplying by the adjugate of the matrix $A - \mathrm{Id}_n$ implies

that if $x := \det(\mathrm{Id}_n - A)$ then $xm_i = 0$ for all i. Hence $xM = 0$, since the m_i's generate M. If we can prove that $x \in 1 + I$ then we are done. By expanding the determinant, we have

$$x = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} (\delta_{i,\sigma(i)} - a_{i,\sigma(i)}).$$

The only term in this sum which isn't in I is the one corresponding to $\sigma = \mathrm{id}$, which is $\prod_{i=1}^{n}(1 - a_{i,i})$. This is in $1 + I$, so $x \in 1 + I$ and we are done.

(2) By the previous point, there is $x \in 1 + \mathfrak{m}$ such that $xM = 0$. But then $x \notin \mathfrak{m}$ since $1 \notin \mathfrak{m}$. Suppose that x is not a unit. Then x is contained in some proper maximal ideal by Zorn's lemma, but this is a contradiction since $x \notin \mathfrak{m}$ and $\mathfrak{m}$ is the only maximal ideal of R.

(3) Again by (1), there is $x \in 1 + I$ such that $xM = 0$. Suppose that x is not a unit, then there is a maximal ideal $\mathfrak{m}$ containing x. But then also $x \in 1 + \mathfrak{m}$ as $I \subseteq \mathrm{Jac}(R)$, and thus $1 \in \mathfrak{m}$, which is absurd.

□

Exercise 5. Let R be a commutative ring which is an integral domain but not a field, and let F be the fraction field of R. Show that F is not finitely generated as an R-module.

Proof. Suppose on the contrary that F is a finitely generated R-module, and let $y \in R$ be a non-invertible element. Since $yF = F$, we know by Nakayama's lemma (the version as in Exercise 4.1) that there exists $x \in 1 + yR$ such that $xM = 0$. Writing $x = 1 + yr$, we obtain that

$$0 = (1 + yr) \cdot 1 = 1 + yr,$$

so $yr = -1$. Hence, y is invertible, contradicting our assumption. □

Exercise 6. Let $R = \mathbb{F}_q[[t]]$ be the ring of power-series in the variable t over the finite field with q elements $\mathbb{F}_q$.

Recall that as a set, R is the set of formal power-series $f = \sum_{n \geq 0} a_n t^n$ with coefficients $a_n \in \mathbb{F}_q$. For two such power series, $\sum_{n \geq 0} a_n t^n$ and $\sum_{n \geq 0} b_n t^n$, one defines the addition to be the power-series $\sum_{n \geq 0}(a_n + b_n)t^n$ and multiplication to be the power-series $\sum_{n \geq 0}(\sum_{k=0}^{n} a_k b_{n-k})t^n$. Recall (or do) the two following exercises from "Anneaux et corps":

(1) If $f \in R \setminus (t)$, then f is invertible (and hence R is a local ring with maximal ideal (t)).

(2) A formal Laurent series over the field $\mathbb{F}_q$ is defined in a similar way to a formal power series, except that we also allow finitely many terms of negative degree. That is, series of the form $f = \sum_{n \geq N} a_n t^n$ where for some $N \in \mathbb{Z}$. Define a natural ring structure on this set and show that with this ring structure the ring of formal Laurent series over $\mathbb{F}_q$, usually denoted $\mathbb{F}_q((t))$, is equal to the fraction field of R.

Now let us go to the actual exercise:

(3) Show that $\mathrm{trdeg}_{\mathbb{F}_q}(\mathrm{Frac}(R))$ is infinite.
[*Hint*: show that $\mathbb{F}_q(t_1, \ldots, t_r)$ is countable, and R is not.]

(4) Show that $\dim R = 1$ and hence show that Theorem 6.1.12 in the course notes does not work with non-finitely-generated algebras.

Proof. (1) Let $f = a_0 + \sum_{n>0} a_n t^n$ where $a_0 \neq 0$ define $f^{-1} = \sum_n b_n t^n$ where (b_n) is defined recursively by $b_0 = \frac{1}{a_0}$ and $b_n = -\frac{1}{a_0} \sum_{i=1}^{n} a_i b_{n-i}$ for $n \geq 1$.

(2) Multiplication of such series can be defined similarly to the definition for formal power series, the coefficient of t^n of two series with respective sequences of coefficients $\{a_n\}$ and $\{b_n\}$ is defined to be: $\sum_{i\in\mathbb{Z}} a_i b_{n-i}$, this sum has only finitely many non-zero terms, since both b_{n-i} and a_i are zero in negative enough degrees. Again $\sum_{n\in\mathbb{Z}}(\sum_{i\in\mathbb{Z}} a_i b_{n-i})t^n$ is a Laurent series since if n is negative enough, then either a_i or b_{n-i} is zero for all i. Note that every non-zero element of $\mathbb{F}_q((t))$ can be written as the product of some power of t and an element of $f \in R \setminus (t)$; simply factor out the lowest power of t with non-zero coefficient. The former is clearly invertible, and the latter is invertible by the previous point. Hence $\mathbb{F}_q((t))$ is a field containing R. On the other hand, the above argument shows that every element of $\mathbb{F}_q((t))$ can be written as a fraction of elements in R, and thus $\mathbb{F}_q((t)) = \mathrm{Frac}(R)$.

(3) We first note that it is sufficient to prove the hint. We have that $R \subset \mathrm{Frac}(R)$ hence if R is not countable neither is $\mathrm{Frac}(R)$. Suppose that $\mathrm{Frac}(R)$ has finite transcendence degree over $\mathbb{F}_q$, then there exists $t_1, \dots t_r$ such that $\mathrm{Frac}(R)$ is algebraic over $\mathbb{F}_q(t_1, \dots, t_r)$. If $\mathbb{F}_q(t_1, \dots, t_r)$ is countable then so is the set of polynomials with coefficients in $\mathbb{F}_q(t_1, \dots, t_r)$, and so in particular every algebraic extension of $\mathbb{F}_q(t_1, \dots, t_r)$ is countable. Hence also $\mathrm{Frac}(R)$ is countable, which contradicts the hint.
So it is sufficient to show the hint. We first show that $\mathbb{F}_q(t_1, \dots, t_r)$ is countable. It is clear that $\mathbb{F}_q[t_1, \dots, t_r]$ is countable, because it is a countable union of polynomials of bounded degree. Thus $\mathbb{F}_q(t_1, ..., t_r)$ is countable as it is the fraction field of $bF_q[t_1, \dots, t_r]$. Lastly, we show that R is not countable. To see this, it suffices to note that the set of sequences $\{0,1\}^{\mathbb{N}}$ naturally injects into R, and the set of such sequences is uncountable by Cantor's diagonal argument.

(4) For $f = \sum_{n\geq 0} a_n t^n \in R \setminus \{0\}$ define $\deg f := \inf\{n \geq 0 \mid a_n \neq 0\}$. If I is an ideal of R, then by point (1) we have $f \in I \setminus \{0\}$ if and only if $t^{\deg f} \in I$. Hence a non-zero ideal $I \neq 0$ of R is generated by t^d where $d = \inf\{\deg f \mid f \in I \setminus \{0\}\}$. Therefore, the only prime ideals of R are $(0) \subset (t)$, and thus R has dimension 1. By the previous point, Theorem 6.1.12 hence fails for R.

□

Exercise 7. The goal of this exercise is to show that an Artinian ring is Noetherian.

Let R be a commutative Artinian ring. Recall from Exercise 1 on Sheet 1 that every prime ideal of R is maximal.

(1) Show that R has finitely many maximal ideals.
[*Hint:* For this you need the statement that if $I_1 \cap \cdots \cap I_r \subseteq \mathfrak{p}$ for a prime ideal $\mathfrak{p} \subseteq R$, then $I_i \subseteq \mathfrak{p}$ for some i, which you should also show. Now consider the set of finite intersections of maximal ideals.]

(2) Show that is an integer $j > 0$ such that $\mathrm{nil}(R)^j = 0$.
[*Hint:* Show that $\mathrm{nil}(R)^j$ stabilizes for $j \gg 0$, which we denote by I. In order to arrive at a contradiction assume that $I = I^2 \neq 0$. Consider a minimal element J in the set of ideals $\{J : JI \neq 0\}$, show that $IJ = J$, then show that J is principal. Conclude by Nakayama's Lemma, point (3).]

(3) Show that if $\mathfrak{m}_1, \dots, \mathfrak{m}_s$ are the maximal ideals of R, then $\mathfrak{m}_1^j \cdots \mathfrak{m}_s^j = 0$.
[*Hint:* Use the statement learned in 'Anneaux et corps' that the nilardical is the intersection of all prime ideals.]

(4) Show that $\text{length}_R R < \infty$, and conclude that R is Noetherian.
[*Hint:* Construct an increasing sequence of ideals using the products of maximal ideals. Thereafter, you have to use multiple times the earlier exercise that Artinianity is closed under passage to sub- and quotient-modules.]

[*Remark:* In point (7) of Example 3.1.2 in the notes you saw an example of an Artinian module which is not Noetherian. However, the exercise above shows that an Artinian ring is always a Noetherian ring.]

Proof. (1) We first show the hint: Suppose by contradiction that $I_i \not\subseteq \mathfrak{p}$ for all i. Then for all i there exist $x_i \in I_i$, such that $x_i \notin \mathfrak{p}$ and thus for $x = x_1 \cdots x_r$ we have $x \in I_1 \cdots I_r \subseteq I_1 \cap \cdots \cap I_r \subset \mathfrak{p}$, but this contradicts that $\mathfrak{p}$ is prime.
Now consider the set of all finite intersections of maximal ideals in R. As R is Artinian, this set has a minimal element, say $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k$. By minimality we have for any maximal ideal $\mathfrak{m}$ that $\mathfrak{m} \cap (\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k$ and therefore $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k \subseteq \mathfrak{m}$. By the hint we obtain $\mathfrak{m}_i \subset \mathfrak{m}$ for some i, which by maximality implies $\mathfrak{m} = \mathfrak{m}_i$. Hence the maximal ideals of R are exactly $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$.

(2) We have a descending chain $\text{nil}(R) \supseteq \text{nil}(R)^2 \supseteq \text{nil}(R)^3 \supseteq \ldots$. By the Artinian property there exists j such that we have $\text{nil}(R)^j = \text{nil}(R)^{j+n}$ for all $n \geq 0$. Let $I = \text{nil}(R)^j$. If $I = I^2 = 0$ we are done, hence we assume that $I = I^2 \neq 0$. Since R is Artinian there exists a minimal element J in the set of ideals $\{J : JI \neq 0\}$. By assumption $J \neq 0$. We have $JI \subset J$ and $JII = JI \neq 0$, hence minimality of J implies that $JI = J$. In order to apply Nakayama's Lemma point (3) to this equality, we show that J is finitely generated. Since $JI \neq 0$ there exists a $x \in J$ such that $xI \neq 0$, by minimality of J, we have $J = (x)$. We can therefore apply Nakayama's Lemma point (3) to the finitely generated module J to conclude $J = 0$, which is a contradiction. Therefore, $\text{nil}(R)^j = 0$.

(3) By Exercise 1 on Sheet 1, every prime ideal in R is maximal. Hence $\text{nil}(R) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_s$, where the $\mathfrak{m}_i$ are the distinct maximal ideals of R. Note also that $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_s = \mathfrak{m}_1 \cdots \mathfrak{m}_s$, which can be proven using the fact that $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_i$ and $\mathfrak{m}_{i+1}$ are coprime for all i. It therefore follows from the previous point that $\mathfrak{m}_1^j \cdots \mathfrak{m}_s^j = 0$.

(4) Let $0 = \mathfrak{n}_1 \cdots \mathfrak{n}_t \subseteq \mathfrak{n}_2 \cdots \mathfrak{n}_t \subseteq \cdots \subseteq \mathfrak{n}_t \subseteq R$, for some not necessary distinct maximal ideals $\mathfrak{n}_1, \ldots, \mathfrak{n}_t$ of R; by the previous point such a sequence exists. Let $I_j = \prod_{j<i\leq t} \mathfrak{n}_i$ for $0 \leq j \leq t$ (the empty prodcut is equal to R by convention). We now prove by induction that every I_j has finite length; this holds trivially for $j = 0$. Suppose this is true for some $j \geq 0$. Then we have the short exact sequence $0 \to I_j \to I_{j+1} \to I_{j+1}/I_j \to 0$. Notice that $\mathfrak{n}_{j+1}$ is contained in the annihilator of I_{j+1}/I_j, and thus the latter is naturally a $R/\mathfrak{n}_{j+1}$-module. Furthermore, we have discussed already several times that the R submodules of I_{j+1}/I_j coincide with the $R/\mathfrak{n}_{j+1}$, and hence the length of I_{j+1}/I_j as an R-module is the same as the length as an $R/\mathfrak{n}_{j+1}$. But now I_{j+1}/I_j is an Artinian R-module because Artinianity is preserved under taking submodules and quotients, and thus it is an Artinian $R/\mathfrak{n}_{j+1}$-moudle. As $R/\mathfrak{n}_{j+1}$ is a field, this means that I_{j+1}/I_j is a finite dimensional $R/\mathfrak{n}_{j+1}$-vector space, and so it has finite length. So the outer modules in the short exact sequence $0 \to I_j \to I_{j+1} \to I_{j+1}/I_j \to 0$ both have finite length by induction hypothesis, and thus by (the proof of) Exercise 1.1 on Sheet 2 we

have that I_{j+1} has finite length too. We then conclude by induction that $I_t = R$ has finite length as an R-module.

□

Exercise 8. ♠ Let R be a PID which is not a field. The goal of this exercise is to show that $\dim R[x] = 2$ (in particular $\dim k[x,y] = 2$).

- Show that $\dim R[x] \geq 2$.
- Let $\mathfrak{p}$ be a non-zero prime ideal of $R[x]$. Show that $\mathfrak{p}$ has height 1 if and only if it is principal.
- Let $K = \mathrm{Frac}(R)$. For any prime ideal $\mathfrak{p}$ in $R[x]$, define $\mathfrak{p}^e$ to be the ideal of $K[x]$ generated by the elements of $\mathfrak{p}$. Show that if $\mathfrak{p}$ is a prime ideal of height 2, then $\mathfrak{p}^e = K[x]$. Conclude that there exists $\pi \in R$ irreducible such that $\pi \in \mathfrak{p}$.
  [*Hint: Recall the notion of primitive polynomial, and the statements around Gauss' lemma (see for example proposition 3.8.13 in the "Anneaux et corps" notes).*]
- Conclude that any prime ideal of height 2 is maximal, and deduce that $\dim(R[x]) = 2$.

[*Remark:* It is a general fact that given a Noetherian commutative ring R of finite Krull dimension, $\dim(R[x]) = \dim(R)+1$. This is not so complicated once we have proven Krull's Hauptidealsatz, but we unfortunately do not have the time to cover this in the course. See any book in commutative algebra if you want to know more about this.]

Proof.

- Let $\pi \in R$ be a non-zero prime element (R is not a field). We then have an chain of inclusions
$$0 \subseteq (\pi) \subseteq (\pi, x)$$
and each ideal is prime. Indeed, the quotients are respectively $R[x]$, $R/(\pi)[x]$ and $R/(\pi)$ which are all domains. Thus, the height of (π, x) is at least 2, and hence $\dim(R[x]) \geq 2$.
- Since R is a PID, it is in particular a UFD, so by Gauss' lemma $R[x]$ is also a UFD. Therefore by Exercise 2.2 any prime ideal of height 1 is principal. To see the converse, let $\mathfrak{p} = (p)$ be a principal prime ideal of $R[x]$, and let $\mathfrak{q} \subseteq \mathfrak{p}$ be a prime sub-ideal. We want to show that if $\mathfrak{q} \neq 0$, $\mathfrak{q} = \mathfrak{p}$.

  If it was not the case, by the same argument as in Exercise 2.2 there would exist a non-zero prime element $q \in \mathfrak{q}$. But then, p divides q, so they must be equal, i.e. $\mathfrak{q} = \mathfrak{p}$.
- Let $\mathfrak{q} \subseteq \mathfrak{p}$ be a prime sub-ideal of height 1, and write $\mathfrak{q} = (q)$ for q a prime element. If $q \in R$, then $\mathfrak{p}^e$ contains q, which is invertible in $K[x]$! Therefore $\mathfrak{p}^e = K[x]$.

  Now let us deal with the case $q \in R$. Then q is a primitive polynomial, and hence by Gauss' lemma it gives an irreducible polynomial in $K[x]$. Therefore $(q) = \mathfrak{q}^e$ is a maximal ideal in $K[x]$. Since $\mathfrak{q}^e \subseteq \mathfrak{p}^e$, we are left to show that $\mathfrak{q}^e \neq \mathfrak{p}^e$. If it was the case, then for any $a \in \mathfrak{p}$, $a \in \mathfrak{q}^e = (q)$, so we can write
$$a = \frac{q}{r}$$
with $r \in R$. Thus gives $ra = q$, and since q is primitive, r must be a unit. Therefore this would imply $\mathfrak{p} = \mathfrak{q}$, but this is impossible since $\mathfrak{p}$ has height 2.

  In both cases, we have proven that $\mathfrak{p}^e = K[x]$, so $1 \in \mathfrak{p}^e$. Write
$$1 = \sum_i \frac{a_i}{b_i} p_i$$

with $a_i, b_i \in R$ and $p_i \in \mathfrak{p}$. Multiplying by the product of the b_i's gives that $\mathfrak{p} \cap R \neq 0$. Writing this elements as a product of prime elements (which must all be in R!), we conclude that $\mathfrak{p}$ must contain a prime element in R.

- Let $\pi \in R \cap \mathfrak{p}$ be a prime element, and let $\overline{\mathfrak{p}}$ denote the image of $\mathfrak{p}$ through the quotient $R[x] \to R[x]/(\pi) \cong R/(\pi)[x]$. Since $\mathfrak{p}$ is not principal (its height is not 1), $\overline{\mathfrak{p}}$ is a non-zero prime ideal of $R/(\pi)[x]$. However R is a PID, so $R/(\pi)$ is a field, whence $R/(\pi)[x]$ is a PID. This means that $\overline{\mathfrak{p}}$ is necessarily a maximal ideal, so by the correspondence theorem $\mathfrak{p}$ is maximal too.

To recapitulate, we have shown that any prime of height 2 is maximal, so there cannot be any prime of height > 2, which gives us $\dim(R[x]) \leq 2$. Thus we win thanks to the first point.

□

EPFL - Fall 2023 Prof. Zs. Patakfalvi
Rings and modules **Exercises**
Sheet 10 - Solutions

There was one bonus exercise on this problem sheet. The exercise was denoted by the symbol ♠ next to the exercise number.

Exercise 1. Let G be a finite group, R an integrally closed domain, K the fraction field of R and let G act on K by (ring) automorphisms such that R is stable under this action, i.e. $g \cdot r \in R$ for all $g \in G$ and $r \in R$. Let $L := K^G$ be the fixed field of the action and set $S := L \cap R$. In this exercise we show that S is also integrally closed.

(1) Show that each element of K can be written in the form $\frac{a}{b}$, where $a \in R$ and $b \in S$.
(2) Show that L is the fraction field of S.
(3) Show that S is integrally closed.
(4) Show that $\mathbb{C}[x^n, x^{n-1}y, \dots, xy^{n-1}, y^n] \subseteq \mathbb{C}[x, y]$ is integrally closed.
[*Hint:* Show that there is automorphism of $\mathbb{C}(x, y)$ that sends x to $e^{2\pi i/n}x$ and y to $e^{2\pi i/n}y$.]

Proof. We denote by $\cdot$ the action of G; the ring multiplication is denoted by the empty symbol.

(1) Let $\frac{c}{d} \in K$ be an arbitrary element, where $c, d \in R$. Set $x = \prod_{g \neq e_G} g \cdot d$ and $a = cx$, $b = dx$. Note that $b \neq 0$ as all the factors are non-zero (as G acts by automorphisms). Then $b = \prod_{g \in G} g \cdot d$ and thus $h \cdot b = \prod_{g \in G} (hg) \cdot d = b$ for all $h \in G$. Therefore $b \in S$ and $\frac{c}{d} = \frac{a}{b}$.
(2) As L is a field containing S, we have to show that every element of L is a fraction of elements in S. Let $x \in L$ be arbitrary; by the previous point we can write $x = \frac{a}{b}$ with $b \in S$. Now as x is fixed by the action of G, we obtain
$$\frac{a}{b} = g \cdot \frac{a}{b} = \frac{g \cdot a}{g \cdot b} = \frac{g \cdot a}{b}$$
for all $g \in G$, where in the last step we used $b \in S$. But then we obtain $a = g \cdot a$ for all $g \in G$, and thus $a \in S$. Hence x is a fraction of elements in S, which proves $\mathrm{Frac}(S) = L$.
(3) Let $x \in L$ be integral over S. Then in particular, $x \in K$ it is integral over R, and thus as R is integrally closed we have $x \in R$. Hence $x \in L \cap R = S$, and thus S is integrally closed.
(4) Denote $R = \mathbb{C}[x, y]$, $K = \mathbb{C}(x, y)$ and $\zeta := e^{2\pi i/n}$. By the universal property of $\mathbb{C}[x, y]$ there exists a $\mathbb{C}$-algebra endomorphism ϕ of R mapping x to ζx and y to ζy. This is easily seen to be bijective, and thus it induces an automorphism Φ of K such that $\Phi|_R = \phi$. But then $\Phi^{\circ n}|_R = \phi^{\circ n} = \mathrm{Id}_R$, and thus $\Phi^{\circ n} = \mathrm{Id}_K$. So let $G = \langle \Phi \rangle$ be the finite subgroup of automorphisms of K generated by Φ. If we are able to show that $S := K^G \cap R$ is equal to $\mathbb{C}[x^n, x^{n-1}y, \dots, xy^{n-1}, y^n] \subseteq \mathbb{C}[x, y]$ then we are done by the previous point. As every element of $\mathbb{C}$ and every monomial among $x^n, x^{n-1}y, \dots, xy^{n-1}, y^n$ is fixed by ϕ, we may conclude already that $\mathbb{C}[x^n, x^{n-1}y, \dots, xy^{n-1}, y^n] \subseteq S$. Now let $f \in R$ be an element fixed by ϕ, and write $f = \sum_{i,j} f_{ij} x^i y^j$. Then $f_{ij} = \zeta^{i+j} f_{ij}$ for all i, j and hence $f_{ij} = 0$ unless $i + j$ is divisible by n. If $i + j$ is divisible by n then (i, j)

can be expressed as an $\mathbb{Z}_{\geq 0}$-linear combination of $(n,0),(n-1,1)\ldots,(1,n-1),(0,n)$; simply write $i = an+b$ and $j = cn+d$ with $0 \leq b,d < n$, then $b+d \in \{0,n\}$ and thus either $b = d = 0$ in which case $(i,j) = a(n,0)+c(0,n)$, or $b+d = n$ in which case $(i,j) = a(n,0)+c(0,n)+(b,d)$. Hence every monomial appearing in f with non-zero coefficient is inside $\mathbb{C}[x^n, x^{n-1}y,\ldots,xy^{n-1},y^n]$, and thus also f itself. Therefore $S = \mathbb{C}[x^n, x^{n-1}y,\ldots,xy^{n-1},y^n]$, so we are done.

□

Exercise 2. Let k be a field. For the following finitely generated k-algebras R, find a sub-algebra $S \subseteq R$ such that $S \subseteq R$ is integral and S is isomorphic to a polynomial ring:

(1) $R = k[x,y]\big/(xy-1)$;
(2) $R = k[x_1,x_2,x_3,y_1,y_2,y_3]\big/(x_1x_2x_3+y_1y_2y_3)$;
(3) $R = k[x,y,z]\big/(xy,xz-yz)$

Proof. The idea is to make a change a variable (hence an automorphism of the polynomial ring) to get an ideal which is much easier to work with (notice this is exactly what we do in the proof of Noether's normalization!).

(1) Let $z = x-y$. Then $xy-1 = (z+y)y-1 = y^2+yz-1$. Thus, $\overline{y}$ satisfies a monic equation with coefficients in $k[\overline{z}]$ which is isomorphic to a polynomial ring, so $S = k[\overline{z}] = k[\overline{x}-\overline{y}] \subseteq R$ does the job.
Before doing the other points, let us rephrase what we have just done in a more precise way. Let x, y, z denote variables, and let $\theta : k[x,y] \to k[z,y]$ be the automorphism sending x to $z+y$. This automorphism induces

$$k[x,y]\big/(xy-1) \cong k[z,y]\big/(z+y)y-1) = k[z,y]\big/(y^2+zy-1)$$

Since $\overline{y}$ satisfies a monic equation over $k[\overline{z}]$, we know by Proposition 8.1.4 in the notes that $k[\overline{z}] \subseteq k[z,y]\big/(y^2+zy-1)$ is an integral extension. Therefore $k[\overline{x}-\overline{y}] \subseteq k[x,y]\big/(xy-1)$ is also an integral extension. Finally, $k[\overline{x}-\overline{y}] \cong k[\overline{z}]$ is isomorphic to a polynomial ring, because of the following lemma (apply it to $R = k[z]$, $f = y^2+zy+1$):

Lemma 0.1. *Let R be a commutative ring, $f \in R[y]$ be a monic polynomial of degree at least 1. Then $R \to R[y]/(f)$ is injective.*

Proof. If not, there exists $r \neq 0$ such that f divides r. Since f is monic and of degree at least 1, this is impossible. □

(2) Apply $x_1' = x_1 - x_3$, $x_2' = x_2 - x_3$ so that the equation becomes

$$(x_1'+x_3)(x_2'+x_3)x_3 + y_1y_2y_3 = x_3^3 + x_3^2(x_1'+x_2') + x_3)x_1'x_2' + y_1y_2y_3$$

which is monic as a polynomial in $k[x_1',x_2',y_1,y_2,y_3][x_3]$. Thus, as before,

$$S = k[\overline{x_1}-\overline{x_3},\overline{x_2}-\overline{x_3},\overline{y_1},\overline{y_2},\overline{y_3}] \subseteq k[x_1,x_2,x_3,y_1,y_2,y_3]\big/(x_1x_2x_3+y_1y_2y_3)$$

works.

(3) Since we have to cut down by two equations, the computations is a bit more subtle, so we will use the language of the end of the first part, instead of the one of the second part. However, in order not to use too many different letters, we will stick with just x,

y, z.

Consider the automorphism $k[x,y,z] \to k[x,y,z]$ sending x to $x+y$. Then we deduce an isomorphism

$$k[x,y,z]\Big/(xy, xz-yz) \cong k[x,y,z]\Big/(y^2+yx, xz)$$

and as before we see that $k[\overline{x},\overline{z}] \subseteq k[x,y,z]\Big/(y^2+yx,xz)$ is an integral extension. However $k[\overline{x},\overline{z}]$ is not a polynomial ring, so we have to do one more step.

Let $\phi : k[x,z] \to k[x,y,z]\Big/(y^2+yx,xz)$ be the map sending x to $\overline{x}$ and z to $\overline{z}$. Let us compute $\ker(\phi)$.

Clearly, $xz \in \ker(\phi)$. Let us show we actually have $(xz) = \ker(\phi)$, so let $p(x,z) \in \ker(\phi)$. Then we can write

$$p(x,z) = \alpha(x,y,z)xz + \beta(x,y,z)(y^2+yx)$$

In particular, setting $y=0$ gives

$$p(x,z) = \alpha(x,0,z)xz$$

so $p(x,z) \in (xz)$

Thus, ϕ induces an inclusion (and actually an integral extension) $k[x,z]/(xz) \subseteq k[x,y,z]/(y^2+yx,xz)$. Now, the change of variables $x \mapsto x-z$ shows that $k[\overline{x}+\overline{z}] \subseteq k[x,z]/(xz)$ is an integral extension, but this time $k[\overline{x}+\overline{z}]$ is a polynomial ring!

By Corollary 8.1.6 in the notes, we conclude that

$$k[\overline{x}+\overline{z}] \subseteq k[x,y,z]\Big/(y^2+xy,xz)$$

is an integral extension, so

$$k[\overline{x}-\overline{y}+\overline{z}] \subseteq k[x,y,z]\Big/(xy,xz-yz)$$

works.

□

Exercise 3. Compute the integral closure of the following domains (you do not need to show they are domains):

(1) $k[x,y]\Big/(y^2+x^3)$

(2) $k[x,y,z]\Big/(y^3+y^2x^2+yx^2+x^3z)$

Proof. For this solution, let R denote the ring we are working with, S its integral closure (which we want to find) and K its field of fractions.

(1) Since $\overline{y}^2 = -\overline{x}^3$, we have

$$\left(\frac{\overline{y}}{\overline{x}}\right)^2 - \overline{x} = 0 \tag{0.1.a}$$

in K, so $\frac{\overline{y}}{\overline{x}}$ is integral over R. Hence, S contains $R[\frac{\overline{y}}{\overline{x}}]$. Let $\phi : k[t] \to R[\frac{\overline{y}}{\overline{x}}]$ be the map sending t to $\frac{\overline{y}}{\overline{x}}$. We want to show that it is an isomorphism.

To show that its surjectivity, it is enough to show that $\overline{x}$, $\overline{y}$ and $\frac{\overline{y}}{\overline{x}}$ are in the image. For the third element this is clear. However by equation 0.1.a, also $\overline{x}$ is in the image.

Now, since we have both $\overline{x}$ and $\frac{\overline{y}}{\overline{x}}$, we have $\overline{y}$, so we deduce ϕ is surjective.

Now let us show the injectivity. This can be done in a direct way with actual equations, but let us give an easier solution: if it was not injective, we would obtain an isomorphism

$$k[t]/p(t) \cong R[\frac{\overline{y}}{\overline{x}}]$$

with p irreducible. But then $k[t]/p(t)$ is simply a finite field extension of k, so its transcendence degree must be 0. On the other hand,

$$K = \mathrm{Frac}(S) = k(x)[y]/(y^2 + x^3)$$

(explained at the end) which is algebraic over $k(x)$, hence it transcendence degree is 1, so we have a contradiction. Thus, ϕ is injective, so it is an isomorphism, and hence $R[\frac{\overline{y}}{\overline{x}}]$ is isomorphic to a polynomial ring. In particular it is integrally closed by Example 8.2.3 from the notes, so $S = R[\frac{\overline{y}}{\overline{x}}]$.

Now let us explain why $K = \mathrm{Frac}(S) = k(x)[y]/y^2 + x^3$. The first equality is immediate since $R \subseteq S \subseteq K$ and $K = \mathrm{Frac}(R)$. The second one follows from the following general statement:

Lemma 0.2. *Let R be a UFD, and let p an irreducible primitive polynomial in $R[t]$. Then*

$$\mathrm{Frac}(R[t]/(p)) \cong \mathrm{Frac}(R)[t]/(p)$$

Proof. We know by Gauss lemma that $p(t)$ is irreducible in $\mathrm{Frac}(R)[t]$, so since this ring is a PID, the quotient $\mathrm{Frac}(R)[t]/(p)$ is a field. But for any element in $\mathrm{Frac}(R)[t]/(p)$, so multiple by an element in R lands in $R[t]/p(t)$, so we win. □

(2) By definition, we have

$$\left(\frac{\overline{y}}{\overline{x}}\right)^3 + \overline{y}\left(\frac{\overline{y}}{\overline{x}}\right)^2 + \frac{\overline{y}}{\overline{x}} + \overline{z} = 0 \tag{0.2.b}$$

so $\frac{\overline{y}}{\overline{x}}$ is integral over R. Let $\phi : k[u, v] \to R[\frac{\overline{y}}{\overline{x}}]$ be the map sending u to $\overline{x}$ and v to $\frac{\overline{y}}{\overline{x}}$.

This map is surjective, because in the image we have $\overline{x}$, $\frac{\overline{y}}{\overline{x}}$, and hence also $\overline{y}$. Finally, we have $\overline{z}$ because of equation 0.2.b.

This map is also injective, because otherwise we would obtain an isomorphism

$$T := k[u, v]/\mathfrak{p} \cong R[\frac{\overline{y}}{\overline{x}}]$$

for some non-zero prime ideal $\mathfrak{p}$. But then any element in $\mathfrak{p}$ gives an algebraic relation between $\overline{u}$ and $\overline{v}$, so

$$\mathrm{trdeg}_k(\mathrm{Frac}(T)) < 2$$

On the other hand, we have as in the previous point that

$$\mathrm{Frac}(S) = \mathrm{Frac}(R) = k(x, z)[y]/(y^3 + y^2x^2 + yx^2 + x^3z)$$

which is algebraic over $k(x, z)$. Hence it transcendence degree is 2, contradiction.

Thus, $R[\frac{\overline{y}}{\overline{x}}] \cong k[u, v]$, so it is integrall closed, and hence $S = R[\frac{\overline{y}}{\overline{x}}]$.

□

Exercise 4. Let R be a ring. Let M, N be R-modules and I an ideal of R. Prove that there are isomorphisms of R-modules $M \otimes_R N \cong N \otimes_R M$ and $M \otimes_R \left({}^{R}\!/_{I}\right) \cong {}^{M}\!/_{IM}$.

Proof. The solution consists of the following steps.

(1) We first prove that $M \otimes_R N \cong N \otimes_R M$. For this purpose, we construct mutually inverse maps from one side to the other. To construct, $M \otimes_R N \to N \otimes_R N$ we just observe that the map $M \times N \to N \otimes_R M$ given by $(m, n) \mapsto n \otimes m$ is bilinear. Hence we obtain a map $M \otimes_R N \to N \otimes_R N$ given on simple tensors by $m \otimes n \mapsto n \otimes m$. By swapping the roles of M and N we obtain also a map in the reverse direction, and the two maps are mutually inverse as their composition is the the identity on simple tensors (and simple tensors generate the tensor product).

(2) Let us give two proofs:

Proof 1: The bilinear map $M \times {}^{R}\!/_{I} \to {}^{M}\!/_{IM}$ sending $(m, \overline{r})$ to rm (it is straightforward to see it is well-defined) induces

$$M \otimes_R {}^{R}\!/_{I} \to {}^{M}\!/_{IM}$$

On the other hand, we have a map $M \to M \otimes_R {}^{R}\!/_{I}$ sending m to $m \otimes 1$. Furthermore, any element of the form rm with $r \in I$, $m \in M$ in sent to $rm \otimes 1 = m \otimes \overline{r} = 0$, so since these elements generate IM, we deduce a map

$$ {}^{M}\!/_{IM} \to M \otimes_R {}^{R}\!/_{I}$$

These two maps are inverses of each other, so we win.

Proof 2: We consider the exact sequence $0 \to I \to R \to {}^{R}\!/_{I} \to 0$. Taking its tensor product with a module M and using right exactness we obtain an exact sequence

$$I \otimes_R M \to R \otimes_R M \to \left({}^{R}\!/_{I}\right) \otimes_R M \to 0.$$

The middle group $R \otimes_R M$ can be identified with M using the map $r \otimes m \mapsto rm$. Under this identification the image of the homomorphism $I \otimes_R M \to R \otimes_R M$ is equal to IM. This implies that $\left({}^{R}\!/_{I}\right) \otimes_R M$ is isomorphic to ${}^{M}\!/_{IM}$.

□

Exercise 5. Let R be a ring, and M, N and P be R-modules. Show that there exists a natural bijection

$$\mathrm{Hom}_R(M \otimes_R N, P) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)).$$

Use this to prove that

$$- \otimes_R N : \{R\text{-modules}\} \to \{R\text{-modules}\}, \quad A \mapsto A \otimes_R N$$

is a right exact covariant functor.

Proof. We start by proving that $- \otimes_R N$ is a covariant functor. For this we need to assign to an R-module homomorphism $f : M \to M'$ an R-module homomorphism $M \otimes_R N \to M' \otimes_R N$, which for conceptual reasons we will denote by $f \otimes_R \mathrm{id}_N$ (but you may also denote it $f \otimes_R N$ if you like). To construct $f \otimes_R \mathrm{id}_N$, let $\iota : M \oplus N \to M \otimes_R N$ and $\iota' : M' \oplus N \to M' \otimes_R N$ be the unique R-bilinear maps in the definition of the tensor product. Let $f \oplus \mathrm{id}_N : M \oplus N \to M' \oplus N$ be defined by $(f \oplus \mathrm{id}_N)(n, m) = (f(n), m)$, then $f \oplus \mathrm{id}_N$ is obviously R-linear. The composition $\iota' \circ F$ defines an R-bilinear map $M \oplus N \to M' \otimes_R N$. By the universal property of $M \otimes_R N$ there exists a unique morphism $f \otimes_R \mathrm{id}_N : M \otimes_R N \to M' \otimes_R N$ such that $\iota' \circ (f \oplus \mathrm{id}_N) = (f \otimes_R \mathrm{id}_N) \circ \iota$. Notice that on

simple tensors, $f \otimes_R \mathrm{id}_N$ is given by $m \otimes n \mapsto f(m) \otimes n$. We now have to verify points (1) and (2) in the definition of a covariant functor given on the Sheet. It is a very useful thing to note that as simple tensors generate the tensor product, two maps with domain a tensor product agree if and only if they agree on simple tensors.

(1) By the above description, $\mathrm{id}_M \otimes_R \mathrm{id}_N$ maps any simple tensor $m \otimes n$ to $m \otimes n$, and thus $\mathrm{id}_M \otimes_R \mathrm{id}_N = \mathrm{id}_{M \otimes_R N}$

(2) Let $f : M \to M'$ and $f' : M' \to M''$ be R-module homomorphisms. Both the map $(f' \otimes_R \mathrm{id}_N) \circ (f \otimes_R \mathrm{id}_N)$ and the map $(f' \circ f) \otimes_R \mathrm{id}_N$ send any simple tensor $m \otimes n$ to $f'(f(m)) \otimes n$. As simple tensors generate $M \otimes_R N$ we hence have $(f' \otimes_R \mathrm{id}_N) \circ (f \otimes_R \mathrm{id}_N) = (f' \circ f) \otimes_R \mathrm{id}_N$.

We now construct the bijection in question. Let $\iota : M \oplus N \to M \otimes_R N$ be the R-bilinear map from the definition of the tensor product. Let $f : M \otimes_R N \to P$ be an R-module homomorphism. Then $f \circ \iota : M \oplus N \to P$ is R-bilinear. Define the map $\eta(f) = \eta_{M,N,P}(f) : M \to \mathrm{Hom}_R(N, P)$ by

$$\begin{aligned} \eta(f) : M &\to \mathrm{Hom}_R(N, P) \\ m &\mapsto (n \in N \mapsto (f \circ \iota)(m, n) \in P)\,. \end{aligned}$$

Using R-bilinearity of $f \circ \iota$ it is straightforward to verify that this is well-defined, i.e. that $\eta(f)(m) \in \mathrm{Hom}_R(N, P)$ an that η is an R-linear map.

To show that η is bijective, we also perform a construction in the reverse direction. Let $F : M \to \mathrm{Hom}_R(N, P)$ be R-linear, then it is straightforward to verify that the map $\widetilde{F} : M \oplus N \to P$ defined by $\widetilde{F}(m, n) = F(m)(n)$ is R-bilinear. Hence the universal property of the tensor product gives an R-module homomorphism $\theta(F) = \theta_{M,N,P}(F) : M \otimes_R N \to P$ such that $\theta(F) \circ \iota = \widetilde{F}$. We hence obtain a map $\theta : \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)) \to \mathrm{Hom}_R(M \otimes_R N, P)$.

We now verify that the above two constructions are mutually inverse. Let $f : M \otimes_R N \to P$ be R-linear, then

$$(\theta(\eta(f)))(m \otimes n) = \widetilde{\eta(f)}(m, n) = \eta(f)(m)(n) = (f \circ \iota)(m, n) = f(m \otimes n)$$

for all simple tensors $m \otimes n$. As simple tensors generate $M \otimes_R N$ we conclude $\theta(\eta(f)) = f$. On the other hand, let $F : M \to \mathrm{Hom}_R(N, P)$ be R-linear. Then we have for all $m \in M$ and $n \in N$ that

$$[(\eta(\theta(F)))(m)](n) = (\theta(F) \circ \iota)(m, n) = \widetilde{F}(m, n) = F(m)(n).$$

Hence we obtain $\eta(\theta(F)) = F$.

We conclude that η and θ are mutually inverse (and in particular also θ is R-linear, as η is). In fact, $\eta_{M,N,P}$ is a natural bijection, which means that it is functorial in M, N, P (i.e. it makes the appropriate commutative diagram commute). We will need only functoriality in M, so we only show this part: let $g : M \to M'$ be an R-module homomorphism. To show that for fixed N, P, the map $\eta_M := \eta_{M,N,P}$ is natural in M, means by definition that we need to verify that the diagram

$$\begin{array}{ccc} \mathrm{Hom}_R(M \otimes_R N, P) & \xrightarrow{\eta_M} & \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)) \\ {\scriptstyle \mathrm{Hom}_R(g \otimes_R \mathrm{id}_N, P)} \uparrow & & \uparrow {\scriptstyle \mathrm{Hom}_R(g, \mathrm{Hom}_R(N, P))} \\ \mathrm{Hom}_R(M' \otimes_R N, P) & \xrightarrow{\eta_{M'}} & \mathrm{Hom}_R(M', \mathrm{Hom}_R(N, P)) \end{array}$$

commutes. To do so, let $f' : M' \otimes_R N \to P$ be arbitrary. Then for any $m \in M$ and $n \in N$ we have

$$[\eta_M \circ \mathrm{Hom}_R(g \otimes_R \mathrm{id}_N, P)(f')](m)(n) = [\eta_M(f' \circ (g \otimes_R \mathrm{id}_N))](m)(n) = \\ = f' \circ (g \otimes_R \mathrm{id}_N) \circ \iota(m,n) = f'(g(m) \otimes n).$$

On the other hand, we have

$$[\mathrm{Hom}_R(g, \mathrm{Hom}_R(N,P)) \circ \eta_{M'}(f')](m)(n) = [\eta_{M'}(f') \circ g](m)(n) = \eta_{M'}(f')(g(m))(n) = \\ = f' \circ \iota'(g(m), n) = f'(g(m) \otimes n).$$

As both results agree, the above diagram indeed commutes, and thus the bijection is natural in M. If you want to verify that it is natural in all components the you need to take simultaneously R-module homomorphisms $M \to M'$, $N \to N'$ and $P \to P'$ and show that the appropriate diagram commutes, but this is more of a language verification and messy so we omit it here.
We now proceed to show right exactness. Let

$$0 \to K \to L \to M \to 0$$

be an exact sequence of R-modules. We want to show that the sequence

$$K \otimes_R N \to L \otimes_R N \to M \otimes_R N \to 0$$

is exact. As we want to use the natural bijection constructed above, we want to apply $\mathrm{Hom}_R(-, P)$ to this sequence and see what happens. To keep track of exactness, this suggests proving the following lemma.

Lemma 1. *Consider R-module homomorphisms $\alpha : A \to B$ and $\beta : B \to C$. If $0 \to \mathrm{Hom}_R(C,P) \to \mathrm{Hom}_R(B,P) \to \mathrm{Hom}_R(A,P)$ is exact for all R-modules P, then $A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ is exact. (This is in fact an 'if and only if' but we don't need it for this exercise.)*

Proof. We start by verifying exactness at C, i.e. that β is surjective. To do so, take $P = \mathrm{coker}(\beta)$, and let $q : C \to P$ be the natural surjection. Note that $\mathrm{Hom}_R(\beta, P)(q) = q \circ \beta = 0$, and thus by injectivity of $\mathrm{Hom}_R(\beta, P)$ we conclude $q = 0$. Hence $\mathrm{coker}(\beta) = 0$ which implies that β is surjective.
Now we verify exactness at B. Take $P = C$ and $\mathrm{id}_C \in \mathrm{Hom}_R(C,C)$. Then

$$0 = \mathrm{Hom}_R(\alpha, C) \circ \mathrm{Hom}_R(\beta, C)(\mathrm{id}_C) = \beta \circ \alpha.$$

Thus $\mathrm{im}(\alpha) \subseteq \ker(\beta)$. To verify the reverse inclusion, take $P = \mathrm{coker}(\alpha)$ and let $p : B \to P$ be the natural surjection. Then $\mathrm{Hom}_R(\alpha, P)(p) = p \circ \alpha = 0$, and thus by the exactness assumption we obtain that there exists $\phi \in \mathrm{Hom}_R(C,P)$ such that $\mathrm{Hom}_R(\beta, P)(\phi) = p$. That is, $\phi \circ \beta = p$ and in particular $\ker(\beta) \subseteq \ker(p) = \mathrm{im}(\alpha)$. Hence we have exactness at B. □

We are now ready to prove right exactness. As $\mathrm{Hom}_R(-, \mathrm{Hom}_R(N,P))$ is left exact, the sequence

$$0 \to \mathrm{Hom}_R(M, \mathrm{Hom}_R(N,P)) \to \mathrm{Hom}_R(L, \mathrm{Hom}_R(N,P)) \to \mathrm{Hom}_R(K, \mathrm{Hom}_R(N,P))$$

is exact. By naturality of η we have a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_R(M, \mathrm{Hom}_R(N,P)) & \longrightarrow & \mathrm{Hom}_R(L, \mathrm{Hom}_R(N,P)) & \longrightarrow & \mathrm{Hom}_R(K, \mathrm{Hom}_R(N,P)) \\ & & \uparrow{\scriptstyle \eta_M} & & \uparrow{\scriptstyle \eta_L} & & \uparrow{\scriptstyle \eta_K} \\ 0 & \longrightarrow & \mathrm{Hom}_R(M \otimes_R N, P) & \longrightarrow & \mathrm{Hom}_R(L \otimes_R N, P) & \longrightarrow & \mathrm{Hom}_R(K \otimes_R N, P). \end{array}$$

As the vertical arrows are bijective R-module homomorphisms, it is straightforward to verify that exactness of the top row implies exactness of the bottom row. As hence the bottom row is exact for any R-module P, the Lemma 1 allows us to conclude that $K \otimes_R N \to L \otimes_R N \to M \otimes_R N \to 0$ is exact. Hence $- \otimes_R N$ is a right exact covariant functor. □

Exercise 6. Let A be a ring, with A-algebras B and C and an A-module M. Show that:

(1) $B \otimes_A M$ naturally has the structure of a B-module,
(2) $B \otimes_A C$ naturally has the structure of an A-algebra,
(3) $B \otimes_A B$ naturally has a ring morphism to B.

Proof. (1) Giving a B-module structure on $B \otimes_A M$ is equivalent to giving a ring map $\lambda : B \to \mathrm{End}_{\mathbb{Z}}(B \otimes_A M)$. To define $\lambda(b)$, note that the map $B \oplus M \to B \otimes_A M$ given by $(b', m) \mapsto (bb') \otimes m$ is A-bilinear. Hence we obtain a map of A-modules $\lambda(b) : B \otimes_A M \to B \otimes_A M$ given on simple tensors by $\lambda(b)(b' \otimes m) = (bb') \otimes m$. In particular, $\lambda(b)$ is a $\mathbb{Z}$-endomorphism of $B \otimes_A M$. It is then straightforward to verify that $\lambda(1) = \mathrm{id}_{B \otimes M}$, $\lambda(b + b') = \lambda(b) + \lambda(b')$ and $\lambda(bb') = \lambda(b) \circ \lambda(b')$ for all $b, b' \in B$; simply check these identities on simple tensors where they easily follow.

(2) First we need to construct a ring structure on $B \otimes_A C$. On simple tensors, it would be natural to suspect $(b \otimes c) \cdot (b' \otimes c') = (bb') \otimes (cc')$ to work, but of course one needs to verify that this is well defined. A clean way is to do the following: For $b \in B$ and $c \in C$, the map

$$\begin{aligned} B \oplus C &\to B \otimes_A C \\ (b', c') &\mapsto (bb') \otimes (cc') \end{aligned}$$

is easily verified to be A-bilinear, and hence induces an A-linear map $\lambda_{(b,c)}$ given on simple tensors by $\lambda_{(b,c)}(b' \otimes c') = (bb') \otimes (cc')$. Next, one may verify that the map $\lambda_\bullet : B \oplus C \to \mathrm{End}_A(B \otimes_A C)$ given by $(b, c) \mapsto \lambda_{(b,c)}$ is A-bilinear, and hence induces an A-linear map $\Lambda : B \otimes_A C \to \mathrm{End}_A(B \otimes_A C)$, given on simple tensors by $\Lambda(b \otimes c) = \lambda_{b,c}$. Now for $\tau, \tau' \in B \otimes_A C$ we define their product by $\tau \cdot \tau' := \Lambda(\tau)(\tau')$. On simple tensors this indeed gives $(b \otimes c) \cdot (b' \otimes c') = (bb') \otimes (cc')$, and it is straightforward to verify the axioms of (commutative) ring multiplication. As Λ is a morphism of A-modules, it is also straightforward that the map $A \to B \otimes_A C$ given by $a \mapsto a \otimes 1 = 1 \otimes a$ gives $B \otimes_A C$ the structure of an A-algebra.

(3) The map $B \oplus B \to B$ given by $(b, b') \mapsto bb'$ is A-bilinear and hence induces an A-linear map $\Delta : B \otimes_A B \to B$, given on simple tensors by $\Delta(b \otimes b') = bb'$. As simple tensors generate $B \otimes_A B$ as an A-module, and hence also as an A-algebra, it suffices to verify multiplicativity on simple tensors. This is easily checked.

□

Exercise 7. Prove the following assertions:

(1) Let R be a commutative ring, and let M_1 and M_2 be free R-modules with bases $\{e_1, ..., e_m\}$ and $\{f_1, ..., f_n\}$ respectively. Show that a basis of $M_1 \otimes_R M_2$ is given by $\{e_i \otimes f_j\}_{\substack{1\le i\le m\\ 1\le j\le n}}$.

(2) Hence show that the element $e_1 \otimes f_2 + e_2 \otimes f_1$ cannot be written as $u \otimes v$ for any $u \in M_1$ and $v \in M_2$.

Proof. (1) As we have already seen, tensor products are distributive with respect to direct sums and for any R-module N, we have $N \otimes_R R \cong N$. Thus, we have

$$M_1 \otimes_R M_2 \xrightarrow{\cong}_{(1)} R^{\oplus m} \otimes_R R^{\oplus n} \xrightarrow{\cong}_{(2)} \left(R^{\oplus m} \otimes_R R\right)^{\oplus n} \xrightarrow{\cong}_{(3)} R^{\oplus mn}.$$

Hence, $M \otimes_R N$ is free of the right rank. Let us find an explicit basis by precisely remembering what our isomorphisms do. Let w_i denote the standard i'th coordinate vector (which we see both in $R^{\oplus m}$ and $R^{\oplus n}$). Then by definition, our choice of isomorphism (1) sends $e_i \otimes f_j$ to $w_i \otimes w_j$.

Recall that the isomorphism $M \otimes_R (S \oplus T) \to (M \otimes_R S) \oplus (M \otimes_R T)$ is given by

$$m \otimes (s, t) \mapsto (m \otimes s, m \otimes t).$$

Hence, isomorphism (2) sends $w_i \otimes w_j$ to

$$(w_i \otimes 0, \ldots, w_i \otimes 1, \ldots, w_i \otimes 0)$$

where the only $w_i \otimes 1$ term is the j'th one. Finally, in general, the isomorphism $M \otimes_R R \to M$ is given by $m \otimes r \mapsto rm$, so we conclude that the image of the elements $e_i \otimes f_j$ through this whole string os isomorphism is

$$w_{ij} := (0, \ldots, w_i, \ldots, 0).$$

Since these elements form a basis of $R^{\oplus mn}$, we win.

(2) Suppose we can write $e_1 \otimes f_2 + e_2 \otimes f_1 = u \otimes v$ for $u \in M_1$ and $v \in M_2$. Then writing $u = \sum_i a_i e_i$ and $v = \sum_j b_j f_j$ we get $e_1 \otimes f_2 + e_2 \otimes f_1 = \sum_{i,j} a_i b_j e_i \otimes f_j$. But this is a linear combination among basis vectors, so we have $a_1 b_2 = a_2 b_1 = 1$ and all other $a_i b_j = 0$. The first implies that all of a_1, b_2, a_2, b_1 are non-zero, which implies that $a_1 b_1$ is also non-zero. But this is a contradiction.

□

Exercise 8. ♠ We will define the exterior product of a module. This construction is especially important, for example in differential/algebraic geometry when one considers differential forms.

Let R be a commutative ring, and let M be an R-module. For any $n > 0$, define $T^n(M) := M \otimes_R \cdots \otimes_R M$ (n times). We also set $T^0(M) := R$. For any $n \ge 0$, we define $\bigwedge^n M$ as the quotient of $T^n M$ by the submodule I generated by elements of the form

$$m_1 \otimes \cdots \otimes m_n,$$

with $m_i = m_j$ for some $i \ne j$. The image of $m_1 \otimes \cdots \otimes m_n$ in $\bigwedge^n M$ is denoted $m_1 \wedge \cdots \wedge m_n$.

Note that if $f: M \to N$ is a morphism of R-modules, then it naturally induced a morphism $T^n(f): T^n(M) \to T^n(N)$ of R-modules (apply f to each tensor), and passes to the quotient $\bigwedge^n f: \bigwedge^n M \to \bigwedge^n N$.

From now on, assume that M is free of finite rank $r \ge 1$, with basis $\mathcal{B} = \{e_1, \ldots, e_r\}$.

- Show that $\bigwedge^r M$ is free with basis $e_1 \wedge \cdots \wedge e_r$, and that $\bigwedge^l M = 0$ for any $l > r$.

- Show that for $0 \leq i \leq r$, $\bigwedge^i M$ is free of rank $\binom{r}{i}$.
  Hint: First find a the appropriate number of generators. To show that it is a basis (i.e. the linear independance), wedge it by an appropriate element to get something in $\bigwedge^r M$, where you know an explicit basis.
- Fix the isomorphism $\theta\colon \bigwedge^r M \to R$ corresponding to the basis found in the first point. Let $f\colon M \to M$ be an endomorphism, corresponding to a matrix $A \in M_{r\times r}(R)$ (with respect to $\mathcal{B}$). Show that the diagram

$$\begin{array}{ccc} \bigwedge^r M & \xrightarrow{\bigwedge^r f} & \bigwedge^r M \\ {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle\theta} \\ R & \xrightarrow{\cdot \det(A)} & R \end{array}$$

  commutes.
- Use the above to give a new proof that if A and B are two $r \times r$-matrices, then $\det(AB) = \det(A)\det(B)$.
  Hint: $\bigwedge$ is functorial.

Proof. Before anything, let us show the following lemma:

Lemma 0.3. *For any $n > 0$, $m_1, \dots, m_n \in M$ and $\sigma \in S_n := \mathrm{Bij}\{1, \dots, n\}$, we have*

$$m_{\sigma(1)} \wedge \cdots \wedge m_{\sigma(n)} = \mathrm{sgn}(\sigma) m_1 \wedge \cdots \wedge m_n.$$

Proof of the lemma. Since the group S_n is generated by transpositions of the form $\sigma_i = (i, i+1)$, it is enough to show the result for these elements. Hence, it is enough to show that

$$m_1 \wedge \cdots \wedge m_{i-1} \wedge m_{i+1} \wedge m_i \wedge \cdots \wedge m_n = -m_1 \wedge \cdots \wedge m_n.$$

Up to wedging on the left by $m_1 \wedge \cdots \wedge m_{i-1}$ and on the right by $m_{i+2} \wedge \cdots \wedge m_n$, we are left to show that

$$m_{i+1} \wedge m_i = -m_i \wedge m_{i+1}.$$

Since by assumption $(m_i + m_{i+1}) \wedge (m_i + m_{i+1}) = 0$, we obtain that by multilinearity that

$$0 = m_i \wedge m_i + m_i \wedge m_{i+1} + m_{i+1} \wedge m_i + m_{i+1} \wedge m_{i+1}.$$

Since the extremal terms of the right-hand-side are zero by definition, we conclude. □

Now, let us start the proof if the exercise.

- By Exercise 7, we know that for any $n > 0$, a basis of $T^n(M)$ is given by the elements

$$e_{i_1} \otimes \cdots \otimes e_{i_n},$$

  with $i_1, \dots, i_n \in \{1, \dots, r\}$. By the lemma we just proved, we obtain that each $\bigwedge^i M$ is generated by the elements

$$e_{i_1} \wedge \cdots \wedge e_{i_r},$$

  with $1 \leq i_1 < \cdots < i_r \leq r$. This shows immediately that $\bigwedge^l M = 0$ for $l > r$, and that $\bigwedge^r M$ is generated by $e_1 \wedge \cdots \wedge e_r$.
  Our goal is to show that this element is a basis of $\wedge^r M$. Hence, assuming that there exists $s \in R$ such that $s(e_1 \wedge \cdots \wedge e_n) = 0$, we want to show that $s = 0$.

Consider the map $M^{\oplus r} \cong R^{\oplus r \times r} \to R$ given by taking the determinant, where the isomorphism above is induced by the basis $\mathcal{B}$. Since this map is multilinear, it induces an R-linear morphism

$$\det\colon T^r(M) \to R.$$

Furthermore, recall that if a matrix A has two identical colons, then $\det(A) = 0$. Thus, $\det$ induces an R-linear morphism at the level of quotients

$$\det\colon \bigwedge^r M \to R.$$

By definition, it sends $e_1 \wedge \cdots \wedge e_n$ to 1, so

$$0 = \det(s(e_1 \wedge \cdots \wedge e_n)) = s \det(e_1 \wedge \cdots \wedge e_n) = s.$$

In particular, $s = 0$ so this point is proven.

- For any $J = \{j_1, \ldots, j_i\} \subseteq \mathcal{B}$, set $e_I := e_{j_1} \wedge \cdots \wedge e_{j_i}$. By our proof of the previous point, we know that $\bigwedge^i M$ is generated by the elements e_J with $|J| = i$. Note that there are exactly $\binom{r}{i}$ of these elements, so our goal is to show that they form a basis.

  Assume that there exist elements $\lambda_J \in R$ such that

$$\sum_{|J|=i} \lambda_J e_J = 0,$$

  and let $J' \subseteq \mathcal{B}$ with $|J'| = i$. Denote $J'_c := \mathcal{B} \setminus J'$. Then for any $J \neq J'$, $e_J \wedge e_{J'_c} = 0$, so we obtain that

$$0 = e_{J'_c} \wedge \sum_J \lambda_J e_J = \pm \lambda_{J'} e_1 \wedge \cdots \wedge e_n.$$

  By the previous point, we deduce that $\lambda_{J'} = 0$. Doing this for all J', we conclude.
- Write $f(e_i) = \sum_j a_{ji} e_j$, so that $A = \{a_{ij}\}_{i,j}$. Then we obtain that

$$\begin{aligned}
\left(\bigwedge^r f\right)(e_1 \wedge \cdots \wedge e_r) &= \left(\sum_j a_{j1} e_j\right) \wedge \cdots \wedge \left(\sum_j a_{jr} e_j\right) \\
&= \sum_{j_1, \ldots, j_r} \left(\prod_i a_{j_i i}\right) e_{j_1} \wedge \cdots \wedge e_{j_r} \\
&= \sum_{\sigma \in S_r} \left(\prod_i a_{\sigma(i) i}\right) e_{\sigma(1)} \wedge \cdots \wedge e_{\sigma(r)} \\
&\quad \uparrow \text{we must have } \{j_1, \ldots, j_r\} = \{1, \ldots, r\} \text{ (i.e. } i \mapsto j_i \text{ is a permutation) to have a non-zero term} \\
&= \left(\sum_{\sigma \in S_r} \operatorname{sgn}(\sigma) \prod_i a_{\sigma(i) i}\right) e_1 \wedge \cdots \wedge e_r \\
&\quad \uparrow \text{see the lemma} \\
&= \det(A)(e_1 \wedge \cdots \wedge e_r).
\end{aligned}$$

- Let $f_A\colon R^{\oplus r} \to R^{\oplus r}$ denote the morphism corresponding to A (and similarly define f_B). Note that by definition, we have $\bigwedge^r (f_A \circ f_B) = \bigwedge^r f_A \circ \bigwedge^r f_B$. By the previous point,

we have

$$\begin{aligned}\det(AB)e_1 \wedge \cdots \wedge e_n &= \left(\bigwedge^r (f_A \circ f_B)\right)(e_1 \wedge \cdots \wedge e_n) \\ &= \left(\bigwedge^r f_A\right)\left(\bigwedge^r f_B\right)(e_1 \wedge \cdots \wedge e_n) = \left(\bigwedge^r f_A\right)(\det(B)e_1 \wedge \cdots \wedge e_n) \\ &= \det(A)\det(B)e_1 \wedge \cdots \wedge e_n.\end{aligned}$$

In particular,

$$\det(AB) = \det(A)\det(B).$$

□

Exercise 9. Prove the following:

(1) Let R be a ring, and let I and J be two ideals such that $I + J = R$. Prove that ${}^{R}\!/_{I} \otimes_R {}^{R}\!/_{J} = 0$.
(2) Show that if $F \subseteq L$ is a field extension, $L \otimes_F L$ is a field if and only if $F = L$.

Proof. (1) We give two proofs:

Proof 1:Since $I + J = (1)$, there are two element $i \in I$ and $j \in J$ such that $i + j = 1$. Consider a simple tensor $(r + I) \otimes (s + J)$. Then we have

$$\begin{aligned}(r + I) \otimes (s + J) &= (i + j) \cdot ((r + I) \otimes (s + J)) = \\ &= (i \cdot (r + I)) \otimes (s + J) + (r + I) \otimes (j \cdot (s + J)) = 0.\end{aligned}$$

As ${}^{R}\!/_{I} \otimes_R {}^{R}\!/_{J}$ is generated by simple tensors, this implies ${}^{R}\!/_{I} \otimes_R {}^{R}\!/_{J} = 0$

Proof 2: By exercise 4, we have

$${}^{R}\!/_{I} \otimes_R {}^{R}\!/_{J} \cong \left({}^{R}\!/_{I}\right)\Big/\left(J \cdot {}^{R}\!/_{I}\right) = \left({}^{R}\!/_{I}\right)\Big/\left({}^{I+J}\!/_{I}\right) \cong {}^{R}\!/_{I+J} = 0$$

where the last equality comes from $I + J = R$.

(2) If $F = L$, then the ring in question is $F \otimes_F F$, and it holds for any ring R that $R \otimes_R R \cong R$. This is easily checked to be a ring isomorphism for the ring structure given by point (2) of Exercise 3.

Conversely, assume that $F \subsetneq L$, and we show that $L \otimes_F L$ is not a field. To do this it is enough to show that it has a non-zero proper ideal, for a field has no non-zero proper ideals. By the previous point (3) of Exercise 3, there is a ring homomorphism $\phi : L \otimes_F L \to L$ given by $b \otimes b' \mapsto bb'$. This is surjective, but it is not injective. This is because we will find $l \in L \backslash F$ such that $r = l \otimes 1 - 1 \otimes l \neq 0$ but $\phi(r) = 0$. Any such r satisfies that $\phi(r) = 0$, hence it is sufficient to find $l \in L \backslash F$ such that $r = l \otimes 1 - 1 \otimes l \neq 0$. To construct such an l, we apply the universal property of tensor products. It is enough to exhibit an F-bilinear map $\theta : L \oplus L \to Z$ of F-modules for some F-module Z which has different values at $(l, 1)$ and $(1, l)$, for the bilinear map factors through $L \oplus L \to L \otimes_F L$. As $L \neq F$, there is a non-trivial (not equal to the identity) F-module homomorphism $\phi : L \to L$ such that $\phi(1) = 1$ (simply pick an F-basis starting with 1, send 1 to itself and for example send all the other elements to 0). Define $\theta(a, b) = a \cdot \phi(b)$. Then θ is F-bilinear and since $\phi \neq id$ there exists an l such that $\phi(l) \neq l$. Therefore, $\theta(1, l) = 1\phi(l) \neq l = \phi(1)l = \theta(l, 1)$. Thus we are done.

□

EPFL - Fall 2023 Prof. Zs. Patakfalvi
Rings and modules **Exercises**
Sheet 11 - Solutions

There was one bonus exercise on this problem sheet. The exercise was denoted by the symbol ♠ next to the exercise number.

Exercise 1. Let R be a ring and let M, N be R-modules. Prove that $\mathrm{Tor}_0^R(M,N) \cong M \otimes_R N$. [*Hint:* Try to adapt the proof of Proposition 5.3.8 in the printed course notes.]

Proof. Let $P_\bullet \to M$ be a projective resolution. Notice that we have a short exact sequence $0 \to \mathrm{im}(p_1) \xrightarrow{i} P_0 \xrightarrow{p_0} M \to 0$. By right exactness of the tensor product, it follows that $\mathrm{im}(p_1) \otimes_R N \to P_0 \otimes_R N \to M \otimes_R N \to 0$ is exact. To conclude, it suffices to verify that the image of $i \otimes_R \mathrm{id}_N$ coincides with the image of $p_1 \otimes_R \mathrm{id}_N$. For this, notice that $p_1 = i \circ p_1|^{\mathrm{im}(p_1)}$, where $p_1|^{\mathrm{im}(p_1)}$ is the corestriction of p_1 to $\mathrm{im}(p_1)$. Hence

$$p_1 \otimes_R \mathrm{id}_N = (i \otimes_R \mathrm{id}_N) \circ (p_1|^{\mathrm{im}(p_1)} \otimes_R \mathrm{id}_N),$$

but $p_1|^{\mathrm{im}(p_1)}$ is surjective and thus by right exactness also $p_1|^{\mathrm{im}(p_1)} \otimes_R \mathrm{id}_N$, and thus $\mathrm{im}(p_1 \otimes_R \mathrm{id}_N) = \mathrm{im}(i \otimes_R \mathrm{id}_N)$. Hence we have

$$M \otimes_R N \cong P_0 \otimes_R N \big/ \mathrm{im}(i \otimes_R \mathrm{id}_N) = P_0 \otimes_R N \big/ \mathrm{im}(p_1 \otimes_R \mathrm{id}_N) = H_0(P_\bullet \otimes_R N) = \mathrm{Tor}_0^R(M,N).$$

□

Exercise 2. Let R be a ring and N an R-module. We say that N is *flat* if for every short exact sequence of R-modules

$$0 \to M \to M' \to M'' \to 0$$

the sequence

$$0 \to M \otimes_R N \to M' \otimes_R N \to M'' \otimes_R N \to 0$$

is exact. Prove that the following are equivalent:

(1) N is flat,
(2) $\mathrm{Tor}_i^R(M,N) = 0$ for every R-module M and every $i > 0$,
(3) $\mathrm{Tor}_1^R(M,N) = 0$ for every R-module M.

[*Hint:* For (1)⇒(2) take a free resolution of M and tensor it with N to compute the Tor-functors. For (3)⇒(1) use the long exact sequence for left derived functors.]

Proof. We prove a cycle of implications:

(1) ⇒ (2) : Let $P_\bullet \to M$ be a projective resolution of some R-module M. As N is flat, the chain complex $(P_\bullet \to M) \otimes_R N$ (with the M at position -1) is still exact, and thus its homology groups vanish. Thus for $i > 0$ we obtain

$$\mathrm{Tor}_i^R(M,N) = H_i(P_\bullet) = H_i(P_\bullet \to M) = 0.$$

(2) ⇒ (3) : Trivial.

(3) ⇒ (1) : Let $0 \to M \to M' \to M'' \to 0$ be an exact sequence of R-modules. From the long exact sequence for left derived functors, we obtain an exact sequence

$$\cdots \to \mathrm{Tor}_1^R(M',N) \to \underbrace{\mathrm{Tor}_1^R(M'',N)}_{=0} \to M \otimes_R N \to M' \otimes_R N \to M'' \otimes_R N \to 0.$$

In particular, $0 \to M \otimes_R N \to M' \otimes_R N \to M'' \otimes_R N \to 0$ is exact, and thus N is flat. □

Exercise 3. Let $R = k[x, y]$ where k is a field. Consider the R-modules $M := (x, y)$ (i.e. the ideal generated by x and y) and $N := R/M$.

(1) Compute $\mathrm{Tor}_i^R(M, N)$ for all integers $i \geq 0$.
[*Hint:* Use the definition.]
(2) Is N flat?
(3) Compute $\mathrm{Tor}_i^R(N, N)$ for all integers $i \geq 0$.
[*Hint:* Use the long exact sequence.]

Proof. (1) We saw already a couple of times that M admits the free resolution $P_\bullet \to M$ given by

$$\begin{aligned} 0 \longrightarrow P_1 = R &\longrightarrow R \oplus R = P_0 \longrightarrow M \longrightarrow 0 \\ 1 &\longmapsto (y, -x) \\ (1,0) &\longmapsto x \\ (0,1) &\longmapsto y. \end{aligned}$$

This already shows that $\mathrm{Tor}_i^R(M, N) = 0$ for all $i \geq 2$. Furthermore, we have $\mathrm{Tor}_1^R(M, N) = \ker(p_1 \otimes_R \mathrm{id}_N)$. Notice that $p_1 \otimes_R \mathrm{id}_N$ maps a simple tensor $r \otimes n$ to $(ry, -rx) \otimes n$, and

$$(ry, -rx) \otimes n = (ry, 0) \otimes n - (0, rx) \otimes n = (r, 0) \otimes \underbrace{(yn)}_{=0} - (0, r) \otimes \underbrace{(xn)}_{=0} = 0.$$

Hence $p_1 \otimes_R \mathrm{id}_N$ is equal to 0 on simple tensors, and thus equal to 0. We therefore obtain $\mathrm{Tor}_1^R(M, N) \cong R \otimes_R N \cong N$. Also, as then $\mathrm{im}(p_1 \otimes_R \mathrm{id}_N) = 0$ we have $\mathrm{Tor}_0^R(M, N) \cong (R \oplus R) \otimes_R N \cong N \oplus N$. In conclusion

$$\mathrm{Tor}_i^R(M, N) \cong \begin{cases} N \oplus N & \text{if } i = 0, \\ N & \text{if } i = 1, \\ 0 & \text{otherwise.} \end{cases}$$

(2) We have $\mathrm{Tor}_1^R(M, N) = N \neq 0$ and thus N isn't flat by Exercise 2.
(3) Notice that we have a short exact sequence $0 \to M \to R \to N \to 0$. We would like to tensor this with N and take the induced long exact sequence. To prepare this, notice that $\mathrm{Tor}_i^R(R, N) = 0$ for all integers $i > 0$. Indeed, a projective resolution of R is provided by $\cdots \to 0 \to R \xrightarrow{\mathrm{id}} R \to 0$. As we have the 0 module on positions with index $i > 0$, and this remains the case after tensoring with N, we conclude that indeed $\mathrm{Tor}_i^R(R, N) = 0$ for all integers $i > 0$. For $i > 1$, consider now the following excerpt from the long exact sequence

$$\cdots \to \underbrace{\mathrm{Tor}_i^R(R, N)}_{=0} \to \mathrm{Tor}_i^R(N, N) \to \mathrm{Tor}_{i-1}^R(M, N) \to \underbrace{\mathrm{Tor}_{i-1}^R(R, N)}_{=0} \to \cdots.$$

Hence we obtain that $\mathrm{Tor}_i^R(N, N) \cong \mathrm{Tor}_{i-1}^R(M, N)$ for all integers $i > 1$, and thus by point (1) we have $\mathrm{Tor}_i^R(N, N) = 0$ for all integers $i > 2$ and $\mathrm{Tor}_2^R(N, N) \cong N$. Now we

focus on the start of the long exact sequence:

$$(*) \qquad \cdots \to \underbrace{\mathrm{Tor}_1^R(R,N)}_{=0} \to \mathrm{Tor}_1^R(N,N) \to M \otimes_R N \to R \otimes_R N \to N \otimes_R N \to 0.$$

The key observation here is that the map $M \otimes_R N \to R \otimes_R N$ is the zero map. Indeed, if $r \otimes (s+M) \in M \otimes_R N$ is a simple tensor then this is mapped to

$$r \otimes (s+M) = 1 \otimes (\underbrace{r(s+M)}_{=0}) = 0$$

insinde $R \otimes_R N$. So as simple tensors generate the tensor product, we indeed have that the map $M \otimes_R N \to R \otimes_R N$ is trivial. Plugging this back into $(*)$ we directly obtain $\mathrm{Tor}_1^R(N,N) \cong M \otimes_R N \cong N \oplus N$, where we used the previous point and Exercise 6. Finally, as the image of $M \otimes_R N$ inside $R \otimes_R N$ is 0, we obtain also from $(*)$ that $R \otimes_R N \to N \otimes_R N$ is an isomorphism. Hence $\mathrm{Tor}_0^R(N,N) \cong N \otimes_R N \cong N$. In conclusion,

$$\mathrm{Tor}_i^R(N,N) \cong \begin{cases} N & \text{if } i \in \{0,2\}, \\ N \oplus N & \text{if } i = 1, \\ 0 & \text{otherwise.} \end{cases}$$

□

Exercise 4. Let R be a ring.

(1) Prove that free R-modules are flat.
(2) Prove that projective R-modules are flat.
[*Hint:* Use the characterization of projective modules as direct summands of free modules.]
(3) Assume that R is an integral domain. Determine for which ideals I of R the R-module R/I is flat.

Remark 0.1. There exists a partial converse of (2): a flat finitely generated module over a Noetherian ring is projective.

The finite generation hypothesis is very important, as the $\mathbb{Z}$-module $\mathbb{Q}$ is flat (see exercise 6.3), but not projective. There are also counter-examples in the Non-noetherian case.

Proof. (1) It suffices to prove that $R^{\oplus I}$ is flat, where I is an arbitrary set. Notice that for an R-module M, we have a natural isomorphism $\eta_M : M \otimes_R R^{\oplus I} \to M^{\oplus I}$, given on simple tensors by $m \otimes (r_i)_i \mapsto (r_i m)_i$. Indeed, η_M exists as it is the map induced by the R-bliniear map $(m,(r_i)_i) \in M \oplus R^{\oplus I} \mapsto (r_i m)_i \in M^{\oplus I}$. We now construct an inverse: let $\theta_M : M^{\oplus I} \to M \otimes_R R^{\oplus I}$ be the map defined by sending $(m_i)_i$ to $\sum_{j : m_j \neq 0} m_j \otimes (\delta_{ij})_i$. It is straightforward to verify that this is the inverse of η_M. Lastly, note that η_M is natural. To see this, let $f : M \to N$ is an R-module homomorphism. We must verify that $f^{\oplus I} \circ \eta_M = \eta_N \circ (f \otimes_R \mathrm{id}_{R^{\oplus I}})$. It suffices to verify this on simple tensors: the LHS maps $m \otimes (r_i)_i$ via $(r_i m)_i$ to $(f(r_i m))_i$, and the RHS maps $m \otimes (r_i)_i$ via $f(m) \otimes (r_i)_i$ to $(r_i f(m))_i$. These two agree as as f is R-linear.
Now to show that $R^{\oplus I}$ is flat, it suffices to show that $- \otimes_R R^{\oplus I}$ preserves injections (as we already know that it is right exact by Exercise 5 of sheet 10). So let $f : M \to N$ be injective, then by what we showed above, under the identifications $M \otimes_R R^{\oplus I} \cong M^{\oplus I}$

and $N \otimes_R R^{\oplus I} \cong N^{\oplus I}$, the map $f \otimes_R \mathrm{id}_{R^{\oplus I}}$ is just $f^{\oplus I}$. So as $f^{\oplus I}$ is injective, $f \otimes_R \mathrm{id}_{R^{\oplus I}}$ is too, and hence $R^{\oplus I}$ is flat.

(2) Suppose M is projective and let M' be an R-module such that $M \oplus M' \cong R^I$. In a similar way as for the previous point, if A is an R-module, then there is a natural isomorphism $\eta_A : A \otimes_R (M \oplus M') \to (A \otimes_R M) \oplus (A \otimes_R M')$ which maps $a \otimes (m, m')$ to $(a \otimes m, a \otimes m')$. Under this identification, if $f : A \to B$ is an R-linear map, then $f \otimes_R \mathrm{id}_{M \oplus M'}$ corresponds to $(f \otimes_R \mathrm{id}_M) \oplus (f \otimes_R \mathrm{id}_{M'})$; it suffices to check this on simple tensors.
Now if f is injective, then by the previous point $f \otimes_R \mathrm{id}_{M \oplus M'}$, and thus under the identifications provided by $\eta_\bullet$ the map $(f \otimes_R \mathrm{id}_M) \oplus (f \otimes_R \mathrm{id}_{M'})$ is injective. In particular, $f \otimes_R \mathrm{id}_M$ is injective. Hence $- \otimes_R M$ preserves injections, which proves that M is flat.

(3) If $I = 0$ then $R/I = R$ is flat. If $I = R$ then $R/I = 0$ is also flat. We will show that $R/I = 0$ is flat only in these two cases. Let $I \subset R$ be a non-zero proper ideal and let $a \in I$ be non-zero. Since R is a domain the R-module morphism $m_a : R \to R$ defined by $m_a(r) = ar$ is injective. However, if we apply $- \otimes_R R/I$ and identify $R \otimes_R R/I \cong R/I$, we obtain $m_a \otimes_R \mathrm{id}_{R/I} : R/I \to R/I$ which maps $r + I$ to $ar + I = 0$. Therefore $m_a \otimes \mathrm{id}_{R/I}$ is the zero map, which is not injective since $I \neq R$, hence R/I is not flat.

□

Exercise 5. Let R be a ring containing a multiplicatively closed subset T, and let M be an R-module. Show that there is an isomorphism of R-modules

$$T^{-1}M \cong T^{-1}R \otimes_R M.$$

Further show that this is an isomorphism of $T^{-1}R$-modules.
[*Remark:* The right hand side naturally has the structure of a $T^{-1}R$-module by point (1) of Exercise 6 on Sheet 10.]

Proof. Let $\psi : T^{-1}R \otimes_R M \to T^{-1}M$ be defined as being induced from the bilinear map $T^{-1}R \oplus M \to T^{-1}M$ given by $(\frac{r}{t}, m) \mapsto \frac{rm}{t}$; that the latter is well-defined and bilinear is direct. In formulas, ψ is given on simple tensors by $\frac{r}{t} \otimes m \mapsto \frac{rm}{t}$
Defining an inverse to ψ can be done by hand (by mapping m/t to $(1/t) \otimes m$ and showing that it is well-defined and a morphism), and this approach will be given first. A more conceptual approach is to prove a universal property for $T^{-1}M$, similar to the one in Theorem 9.2.3 of the notes, that allows to construct a map out of $T^{-1}M$ from a map out of M. This is stated in Remark 9.2.8, and proven below the approach by hand.

First the approach by hand. We show that $g : T^{-1}M \to T^{-1}R \otimes_R M$ defined by $g(\frac{m}{t}) = \frac{1}{t} \otimes m$ for $m \in M$ and $t \in T$ is well-defined and inverse to ψ. Suppose that $\frac{m_1}{t_1} = \frac{m_2}{t_2}$. Then there is $t' \in T$ such that $t'(t_2 m_1 - t_1 m_2) = 0$. Thus $\frac{1}{t_1} \otimes m_1 = \frac{t't_2}{t't_2t_1} \otimes m_1 = \frac{1}{t't_2t_1} \otimes t't_2 m_1 = \frac{1}{t't_2t_1} \otimes t't_1 m_2$, which is equal to $\frac{1}{t_2} \otimes m_2$ by a symmetrical argument. This shows that g is well defined. To show that it is a $T^{-1}R$-module homomorphism, we must show that it respects addition and scalar multiplication: for addition, $g(\frac{m_1}{t_1} + \frac{m_2}{t_2}) = g(\frac{t_2 m_1 + t_1 m_2}{t_1 t_2}) = \frac{1}{t_1 t_2} \otimes (t_2 m_1 + t_1 m_2) = \frac{1}{t_1 t_2} \otimes t_2 m_1 + \frac{1}{t_1 t_2} \otimes t_1 m_2 = \frac{1}{t_1} \otimes m_1 + \frac{1}{t_2} \otimes m_2$ as required. For scalar multiplication, $g(\frac{r}{s}\frac{m}{t}) = \frac{1}{st} \otimes rm = \frac{r}{st} \otimes m = \frac{r}{s}(\frac{1}{t} \otimes m) = \frac{r}{s}\phi(\frac{m}{t})$. Now it remains to show

that ψ and g are mutually inverse: we have

$$\psi(g(\frac{m}{t})) = \psi(\frac{1}{t} \otimes m) = \frac{m}{t}$$

and on simple tensors (it suffices to check these as they generate the tensor product)

$$g(\psi(\frac{r}{t} \otimes m)) = g(\frac{rm}{t}) = \frac{1}{t} \otimes rm = \frac{r}{t} \otimes m.$$

So g and ψ are isomorphisms, and as g is $T^{-1}R$-linear, ψ is too. As a side note, notice that it follows from this isomorphism that every element of $T^{-1}R \otimes_R M$ is expressible as a simple tensor.

Conceptual approach:

Theorem. *Let R be a ring with multiplicatively closed subset T and let M be an R-module. Let $i : M \to T^{-1}M$ be the R-module homomorphism defined by $m \mapsto \frac{m}{1}$. Lastly, an R-module N will be called T-invertible if for every $t \in T$ the multiplication map $\mu_t : n \in N \mapsto tn \in N$ is an isomorphism.*

(1) A T-invertible R-module N admits a natural $T^{-1}R$-module structure, defined by $\frac{r}{t} \cdot n := \mu_t^{-1}(rn)$.

(2) For every R-module homomorphism $\phi : M \to N$ with N being T-invertible, there exists a unique R-module homomorphism $\overline{\phi} : T^{-1}M \to N$ such that $\phi = \overline{\phi} \circ i$. Furthermore, $\overline{\phi}$ is a $T^{-1}R$-module homomorphism for the $T^{-1}R$-module structure on N from the previous point.

Proof. (1) The R-module structure is equivalent to a ring homomorphism $\lambda : R \to \mathrm{End}_{\mathbb{Z}}(N)$, mapping r to μ_r. The ring $\mathrm{End}_{\mathbb{Z}}(N)$ isn't necessarily commutative, so to get around this let $S \subseteq \mathrm{End}_{\mathbb{Z}}(N)$ be the subring generated by $\lambda(R)$ and $\{\mu_t^{-1} \mid t \in T\}$. Then it is straightforward to check that S is commutative, and that the corestriction $\lambda|^S : R \to S$ maps every element of T to a unit. Hence, by the universal property of $T^{-1}R$, there exists a map $\Lambda : T^{-1}R \to S \hookrightarrow \mathrm{End}_{\mathbb{Z}}(N)$ extending $\lambda|^S$. This gives N the structure of a $T^{-1}R$-module, and it is straightforward to check that $\frac{r}{t} \cdot n := \mu_t^{-1}(rn)$.

(2) We define $\overline{\phi} : T^{-1}M \to N$ by the formula $\overline{\phi}\left(\frac{m}{t}\right) = \frac{1}{t}\phi(m)$ (where we make use of the $T^{-1}R$-module structure on N). We have to check that this is well defined: suppose $\frac{m_1}{t_1} = \frac{m_2}{t_2}$, i.e. there is a $t' \in T$ such that $t'(t_2m_1 - t_1m_2) = 0$. Then by applying ϕ we obtain $t'(t_2\phi(m_1) - t_1\phi(m_2)) = 0$ inside N, and as N is T-invertible this implies $\frac{1}{t_1}\phi(m_1) = \frac{1}{t_2}\phi(m_2)$. Hence $\overline{\phi}$ is well-defined. Note that $\phi = \overline{\phi} \circ i$ follows immediately from the construction. So what is left to check is that $\overline{\phi}$ is a $T^{-1}R$-module homomorphism:

(additive): $\overline{\phi}\left(\frac{m_1}{t_1} + \frac{m_2}{t_2}\right) = \frac{1}{t_1t_2}\phi(t_2m_1 + t_1m_2) = \frac{1}{t_1}\phi(m_1) + \frac{1}{t_2}\phi(m_2) = \overline{\phi}\left(\frac{m_1}{t_1}\right) + \overline{\phi}\left(\frac{m_2}{t_2}\right)$ for all $t_1, t_2 \in T$ and $m_1, m_2 \in M$.

($T^{-1}R$-linear): $\overline{\phi}\left(\frac{r}{s}\frac{m}{t}\right) = \frac{1}{st}\phi(rm) = \frac{r}{st}\phi(m) = \frac{r}{s}\overline{\phi}\left(\frac{m}{t}\right)$ for all $r \in R$, $s, t \in T$ and $m \in M$.

Hence $\overline{\phi}$ is a $T^{-1}R$-module homomorphism (and in particular an R-module homomorphism).

□

With this at hand, notice that $T^{-1}R \otimes_R M$ is T-invertible: indeed, by Exercise 6.1 on Sheet 10, $T^{-1}R \otimes_R M$ has the structure of a $T^{-1}R$-module (such that multiplication by $r/1$ is multiplication by r). In particular, multiplication by $t \in T$ is invertible (the inverse being multiplication by $\frac{1}{t}$). Therefore, by the universal property of $T^{-1}M$, the map $\phi : M \to T^{-1}R \otimes_R M$ which sends $m \mapsto 1 \otimes m$ induces $\overline{\phi} : T^{-1}M \to T^{-1}R \otimes_R M$ defined by $\frac{m}{t} \mapsto \frac{1}{t}(1 \otimes m) = \frac{1}{t} \otimes m$. It is then easy to see that $\overline{\phi}$ is inverse to ψ, and as $\overline{\phi}$ is a $T^{-1}R$-module homomorphism, ψ is too. □

Exercise 6. Let R be a ring with multiplicative subset T, and suppose that L, M and N are R-modules.

(1) Show that if there is an R-module homomorphism $f : M \to N$ then there is a natural $T^{-1}R$-module homomorphism $f_T : T^{-1}M \to T^{-1}N$.
(2) Show that there is an isomorphism of $T^{-1}R$-modules $T^{-1}(M \oplus N) \cong (T^{-1}M) \oplus (T^{-1}N)$.
(3) Suppose there is an exact sequence
$$0 \to L \to M \to N \to 0.$$
Prove that the sequence
$$0 \to T^{-1}L \to T^{-1}M \to T^{-1}N \to 0$$
is also exact. Deduce that if $L \subset M$ is a sub R-module, then $T^{-1}\left(M/L\right) \cong T^{-1}M \Big/ T^{-1}L$ and that localization by T is an exact functor of R-modules and that $T^{-1}R$ is a flat R-module.
(4) Let $\mathfrak{p}$ be a prime ideal of R. Show that there is an isomorphism of rings $\mathrm{Frac}\left(R/\mathfrak{p}\right) \cong R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$.
[*Remark:* For a local ring A with maximal ideal $\mathfrak{m}$ we call $A/\mathfrak{m}$ the residue field of A.]

Proof. There are two possible approaches to the first three points: either one uses the universal property of localisation of a module proven in the conceptual solution to Exercise 5, or one uses the description of localisation of a module by a tensor product provided by Exercise 5. Both have their advantages and disadvantages, so will discuss both.

(1) *Tensor approach:* By applying the functor $T^{-1}R \otimes_R -$ we obtain a map $\mathrm{id}_{T^{-1}R} \otimes_R f : T^{-1}R \otimes_R M \to T^{-1}R \otimes_R N$ which on simple tensors is defined by $\frac{r}{t} \otimes m \mapsto \frac{r}{t} \otimes f(m)$. Under the identification provided by Exercise 5, this gives a map of R-modules $f_T : T^{-1}M \to T^{-1}N$ defined by $\frac{m}{t} \mapsto \frac{f(m)}{t}$. It is then straightforward to check to see that this is a $T^{-1}R$-module homomorphism.
Pure localisation approach: Denote by i_M resp. i_N the natural maps $i_M : M \to T^{-1}M$ and $i_N : N \to T^{-1}N$. Then as $T^{-1}N$ seen as an R-module is T-invertible, the map $i_N \circ f : M \to T^{-1}N$ induces a $T^{-1}R$-module homomorphism $f_T : T^{-1}M \to T^{-1}N$ such that $f_T \circ i_M = i_N \circ f$ (by the universal property of module localisation proven in the solution to Exercise 5). It is straightforward to check that f_T maps $\frac{m}{t} \in T^{-1}M$ to $\frac{f(m)}{t} \in T^{-1}N$.
(2) *Tensor approach:* The functor $L \otimes_R -$ is additive for any R-module L, meaning more precisely that the map $L \otimes_R (M \oplus N) \to (L \otimes_R M) \oplus (L \otimes_R N)$ sending a simple tensor $l \otimes (m, n)$ to $(l \otimes m, l \otimes n)$ is a well-defined isomorphism of R-modules. By applying this to $L = T^{-1}R$ and using the identification provided by Exercise 5, we

obtain that the map $T^{-1}(M \oplus N) \to (T^{-1}M) \oplus (T^{-1}N)$ defined by sending $\frac{(m,n)}{t}$ to $\left(\frac{m}{t}, \frac{n}{t}\right)$ is an R-module isomorphism. It is then straightforward to check that this is in fact a $T^{-1}R$-module homomorphism.

Pure localisation approach: Denote by i_M, i_N resp. $i_{M\oplus N}$ the natural localisation maps. The map $i_M \oplus i_N : M \oplus N \to T^{-1}M \oplus T^{-1}N$ goes to a T-invertible module, and hence by the universal property induces a map of $T^{-1}R$-modules $\phi : T^{-1}(M \oplus N) \to T^{-1}M \oplus T^{-1}N$ such that $\phi \circ i_{M\oplus N} = i_M \oplus i_N$ (which in particular implies that $\frac{(m,n)}{t}$ is mapped to $\left(\frac{m}{t}, \frac{n}{t}\right)$). Now either one checks by hand that this is bijective (which is straightforward), or one constructs an inverse (which is a bit heavy on notation but a good exercise). We will do the latter. If j_M resp. j_N are the natural inclusions $j_M : M \hookrightarrow M \oplus N$ resp. $j_N : N \hookrightarrow M \oplus N$, then the maps $i_{M\oplus N} \circ j_M$ and $i_{M\oplus N} \circ j_N$ induce $T^{-1}R$-maps $\psi_M : T^{-1}M \to T^{-1}(M \oplus N)$ and $\psi_N : T^{-1}N \to T^{-1}(M \oplus N)$ such that $\psi_M \circ i_M = i_{M\oplus N} \circ j_M$ and $\psi_N \circ i_N = i_{M\oplus N} \circ j_N$ (which in particular implies that $\frac{m}{t}$ is mapped to $\frac{(m,0)}{t}$ and $\frac{n}{t}$ is mapped to $\frac{(0,n)}{t}$). Then ψ_M and ψ_N together induce $\psi : T^{-1}M \oplus T^{-1}N \to T^{-1}(M \oplus N)$, given by mapping $\left(\frac{m}{t}, \frac{n}{t'}\right)$ to $\frac{(m,0)}{t} + \frac{(0,n)}{t'}$, which can also be written as $\frac{(t'm,tn)}{tt'}$. It is then straightforward to check that ϕ and ψ are mutually inverse.

(3) We first prove exactness of the sequence.

Tensor approach: As $T^{-1}R \otimes_R -$ is right exact by Exercise 5 on sheet 10, we already have that $T^{-1}L \to T^{-1}M \to T^{-1}N \to 0$ is exact. Let f be the map $f : L \to M$; to conclude, we must show that f_T is injective. So suppose that $\frac{l}{t}$ is mapped to 0 by f_T, i.e. $\frac{f(l)}{t}$ is 0 inside $T^{-1}M$. This means that there is $t' \in T$ such that $t'f(l) = 0$ in M, which by injectivity of f means that $t'l = 0$. But then $\frac{l}{t} = 0$ inside $T^{-1}L$, so f_T is injective. Hence $0 \to T^{-1}L \to T^{-1}M \to T^{-1}N \to 0$.

Pure localisation approach: Denote by $f : L \to M$ and $g : M \to N$ the maps of the sequence. Just as in the tensor approach, one proves that f_T is injective. To show that g_T is surjective, let $\frac{n}{t} \in T^{-1}N$ be arbitrary. Then as g is surjective, there is $m \in M$ such that $g(m) = n$, and thus g_T maps $\frac{m}{t}$ to $\frac{n}{t}$, so g_T is surjective. So it remains to show exactness at $T^{-1}M$. As $g_T \circ f_T$ is equal to $(g \circ f)_T$ which is 0, we obtain $\operatorname{im} f_T \subseteq \ker g_T$. To prove the reverse inclusion, let take $\frac{m}{t} \in \ker g_T$. That is, we have that $\frac{g(m)}{n}$ is 0 inside $T^{-1}N$, i.e. there exists $t' \in T$ such that $t'g(m) = 0$. By exactness of the original sequence, there exists $l \in L$ such that $f(l) = t'm$. Hence we obtain that f_T maps $\frac{l}{tt'}$ to $\frac{m}{t}$. Thus we proved that also $\ker g_T \subseteq \operatorname{im} f_T$, and thus $0 \to T^{-1}L \to T^{-1}M \to T^{-1}N \to 0$ is exact.

Note that for any R-submodule $L \subseteq M$ we can set $N := M/L$ to obtain an exact sequence $0 \to L \to M \to N \to 0$, and then as $0 \to T^{-1}L \to T^{-1}M \to T^{-1}N \to 0$ is also exact we obtain

$$T^{-1}\left(M/L\right) = T^{-1}N \cong T^{-1}M \Big/ T^{-1}L.$$

Note that under this isomorphism, $\frac{m+L}{t}$ is mapped to $\frac{m}{t} + T^{-1}L$.

To prove that localisation by T is a (covariant) functor, we must show that $(\mathrm{id}_M)_T =$

$\mathrm{id}_{T^{-1}M}$ and $(g \circ f)_T = g_T \circ f_T$ for any R-module homomorphisms $f : L \to M$ and $g : M \to N$, which are both straightforward. The above then implies that localisation by T is moreover exact.

Finally, the identification provided by Exercise 5 shows that $T^{-1}R \otimes_R -$ is an exact functor, which means that $T^{-1}R$ is a flat R-module.

(4) We construct mutually inverse morphisms. First, notice that the composition $R \to R_\mathfrak{p} \to {}^{R_\mathfrak{p}}\!/_{\mathfrak{p}R_\mathfrak{p}}$ has kernel equal to $\mathfrak{p}$. Indeed, every element of $\mathfrak{p}$ is mapped to 0, and if $r \in R$ is mapped to 0 then $\frac{r}{1}$ is inside $\mathfrak{p}R_\mathfrak{p}$, which means that there exists $r' \in \mathfrak{p}$ and $t \in R \setminus \mathfrak{p}$ such that $\frac{r}{1} = \frac{r'}{t}$. This in turn means that there is $t' \in R \setminus \mathfrak{p}$ such that $t'(rt - r') = 0$. In particular, $rtt' \in \mathfrak{p}$, and as $tt' \notin \mathfrak{p}$ we obtain $r \in \mathfrak{p}$. Therefore, we obtain an injective ring morphism ${}^{R}\!/_{\mathfrak{p}} \to {}^{R_\mathfrak{p}}\!/_{\mathfrak{p}R_\mathfrak{p}}$. Notice that if $t + \mathfrak{p} \neq 0$, then this is mapped to $\frac{t}{1} + \mathfrak{p}R_\mathfrak{p}$. This has inverse $\frac{1}{t} + \mathfrak{p}R_\mathfrak{p}$, so every non-zero element is mapped to an invertible element in ${}^{R_\mathfrak{p}}\!/_{\mathfrak{p}R_\mathfrak{p}}$. Thus the universal property of localisation induces a ring morphism $\mathrm{Frac}\left({}^{R}\!/_{\mathfrak{p}}\right) \to {}^{R_\mathfrak{p}}\!/_{\mathfrak{p}R_\mathfrak{p}}$, mapping $\frac{r+\mathfrak{p}}{t+\mathfrak{p}}$ to $\frac{r}{t} + \mathfrak{p}R_\mathfrak{p}$.

On the other hand, the composition $R \to {}^{R}\!/_{\mathfrak{p}} \to \mathrm{Frac}\left({}^{R}\!/_{\mathfrak{p}}\right)$ maps every element of $R \setminus \mathfrak{p}$ to an invertible element, and hence induces a ring map $R_\mathfrak{p} \to \mathrm{Frac}\left({}^{R}\!/_{\mathfrak{p}}\right)$ given by sending $\frac{r}{t}$ to $\frac{r+\mathfrak{p}}{t+\mathfrak{p}}$. Then, if $r \in \mathfrak{p}$, then $\frac{r}{1}$ is mapped to 0, and thus the ideal generated by elements of this form, i.e. $\mathfrak{p}R_\mathfrak{p}$, is in the kernel. Hence we obtain ${}^{R_\mathfrak{p}}\!/_{\mathfrak{p}R_\mathfrak{p}} \to \mathrm{Frac}\left({}^{R}\!/_{\mathfrak{p}}\right)$ given by sending ${}^{r}\!/_{t} + \mathfrak{p}R_\mathfrak{p}$ to $\frac{r+\mathfrak{p}}{t+\mathfrak{p}}$. This is clearly inverse to the morphism constructed in the previous paragraph, so it is an isomorphism of rings.

□

Exercise 7. Let R be a ring, let S be a multiplicatively closed subset, and let M and N be R-modules. Show that for all $i \geq 0$,

$$S^{-1}\operatorname{Tor}_i^R(M,N) \cong \operatorname{Tor}_i^{S^{-1}R}(S^{-1}M, S^{-1}N).$$

If furthermore R is Noetherian and M is finitely generated, then also

$$S^{-1}\operatorname{Ext}^i_R(M,N) \cong \operatorname{Ext}^i_{S^{-1}R}(S^{-1}M, S^{-1}N).$$

Proof. Let us first show the statement about Tor's. Let $P_\bullet \to M$ be a projective resolution. Note that each $S^{-1}P_i$ is also projective about $S^{-1}R$ (for example use Exercise 5, and the analogous fact for tensor products). Furthermore, by exactness of the functor S^{-1} (see Exercise 6), we deduce that $S^{-1}P_\bullet$ is a projective resolution (over $S^{-1}R$) of $S^{-1}M$.

Before, concluding, let us show that for any R-modules A, B, we have $S^{-1}A \otimes_{S^{-1}R} S^{-1}B \cong S^{-1}(A \otimes_R B)$.

This follows from the computation

$$S^{-1}A \otimes_{S^{-1}R} S^{-1}B \cong A \otimes_R S^{-1}R \otimes_{S^{-1}R} S^{-1}B \cong A \otimes_R S^{-1}B \cong A \otimes_R B \otimes_R S^{-1}R \cong S^{-1}(A \otimes_R B).$$

Combining all this, we deduce that $S^{-1}P_\bullet \otimes_{S^{-1}R} S^{-1}N \cong S^{-1}(P_\bullet \otimes_R N)$. Taking i'th homology (and again using exactness of S^{-1}) shows the statement.

Now, let us show the statement about Ext-functors. The exact same argument will work, once we know that $S^{-1}\operatorname{Hom}_R(M,N) \cong \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$. First of all, there is always

a natural map

$$\theta_{M,N}\colon S^{-1}\operatorname{Hom}_R(M,N) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$$

given by sending an element $\frac{f}{s}$ (with $f\colon M \to N$ and $s \in S$) to the map

$$\frac{m}{s'} \longmapsto \frac{f(m)}{ss'}.$$

If $M \cong R^{\oplus m}$ (let $e_1, \ldots, e_m$ denote a basis of M), then this map is an isomorphism. Indeed, we have

$$S^{-1}\operatorname{Hom}_R(M,N) \cong S^{-1}\operatorname{Hom}_R(R^{\oplus m}, N) \cong S^{-1}(N^{\oplus m}) \cong (S^{-1}N)^{\oplus m},$$

where the isomorphism sends

$$\frac{f}{s} \longmapsto \left(\frac{f(e_1)}{s}, \ldots, \frac{f(e_m)}{s}\right).$$

On the other hand, we also have an isomorphism

$$\operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \cong \operatorname{Hom}_{S^{-1}R}((S^{-1}R)^{\oplus m}, S^{-1}N) \cong (S^{-1}N)^{\oplus m}$$

sending

$$g \longmapsto \left(g\left(\frac{e_1}{1}\right), \ldots, g\left(\frac{e_m}{1}\right)\right).$$

We then immediately see that the triangle

$$\begin{array}{ccc} S^{-1}\operatorname{Hom}_R(M,N) & \xrightarrow{\quad\theta_{M,N}\quad} & \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \\ & {\scriptstyle\cong}\searrow \quad \swarrow{\scriptstyle\cong} & \\ & (S^{-1}N)^{\oplus m} & \end{array}$$

commutes, so $\theta_{M,N}$ is an isomorphism in this case.

For the general case, consider an exact sequence

$$R^{\oplus m_2} \to R^{\oplus m_1} \to M \to 0$$

(recall that M is finitely generated and R is Noetherian). We can then apply $\operatorname{Hom}_R(-, N)$ and then S^{-1} to obtain an exact sequence

$$0 \longrightarrow S^{-1}\operatorname{Hom}_R(M,N) \longrightarrow S^{-1}\operatorname{Hom}_R(R^{\oplus m_1}, N) \longrightarrow S^{-1}\operatorname{Hom}_R(R^{\oplus m_2}, N).$$

We could also have applied first S^{-1} and then $\operatorname{Hom}_{S^{-1}R}(-, S^{-1}N)$ to obtain

$$0 \longrightarrow \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \longrightarrow \operatorname{Hom}_{S^{-1}R}(S^{-1}R^{\oplus m_1}, S^{-1}N) \longrightarrow \operatorname{Hom}_{S^{-1}R}(S^{-1}R^{\oplus m_2}, S^{-1}N).$$

Our natural maps θ give the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & S^{-1}\operatorname{Hom}_R(M,N) & \longrightarrow & S^{-1}\operatorname{Hom}_R(R^{\oplus m_1}, N) & \longrightarrow & S^{-1}\operatorname{Hom}_R(R^{\oplus m_2}, N) \\ & & \downarrow{\scriptstyle\theta_{M,N}} & & \downarrow{\scriptstyle\theta_{R^{\oplus m_1},N}} & & \downarrow{\scriptstyle\theta_{R^{\oplus m_2},N}} \\ 0 & \longrightarrow & \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) & \longrightarrow & \operatorname{Hom}_{S^{-1}R}(S^{-1}R^{\oplus m_1}, S^{-1}N) & \longrightarrow & \operatorname{Hom}_{S^{-1}R}(S^{-1}R^{\oplus m_2}, S^{-1}N) \end{array}$$

Since both $\theta_{R^{\oplus m_1},N}$ and $\theta_{R^{\oplus m_2},N}$ are isomorphisms, we deduce by the 5-lemma (Lemma 5.6.2 in the notes) that $\theta_{M,N}$ is an isomorphism. $\square$

Exercise 8. ♠ Many algebraic geometers tend not to say "projective modules", but more "locally free modules" or even "vector bundles" (as in differential geometry!). It would take us too far to understand the name "vector bundle" (see the course Algebraic Geometry II), but we can already understand the name "locally free".

Let R be a commutative Noetherian ring, and let M be a finitely generated R-module. Our goal is to show that M is projective if and only if there exists a collection of elements $\{a_i\}_i$ of R such that each M_{a_i} is free as an R_{a_i}-module, and $\operatorname{Spec} R = \bigcup_i D(a_i)$ (we call such a module a *locally free module*).

Throughout, you may freely use the following statement, which will be an exercise in the next exercise sheet.

Proposition 0.2. *For any finitely generated R-module N, we have*

$$N = 0 \iff N_{\mathfrak{p}} = 0 \ \forall \mathfrak{p} \in \operatorname{Spec}(R).$$

We will prove our result in several steps:

- Show that M is locally free if and only if $M_{\mathfrak{p}}$ is free as an $R_{\mathfrak{p}}$-module for all $\mathfrak{p} \in \operatorname{Spec}(R)$.
  Hint: It can be useful to show that for any finitely generated module N and $\mathfrak{p} \in \operatorname{Spec}(R)$, if $N_{\mathfrak{p}} = 0$, then there exists $a \notin \mathfrak{p}$ such that $N_a = 0$.
- Show that if M is locally free, then it is projective.
  Hint: Remember that projectivity can be detected by exactness of a certain functor.
- Assume that R is a *local ring* (i.e. it has a unique maximal ideal). Show that M is projective if and only if it is free.
  Hint: Let $\mathfrak{m}$ be the maximal ideal of R. A good starting idea would be to show that if $m_1, \dots, m_n \in M$ is a basis of $M/\mathfrak{m}M$, then M is in fact generated by $m_1, \dots, m_n$. Nakayama's lemma can help.
- Conclude that if M is projective, then it is locally free.

Proof. ∘ Assume first that M is locally free, and let $\mathfrak{p} \in \operatorname{Spec} R$. By assumption, there exists $a \in R$ such that $\mathfrak{p} \in D(a)$ (i.e. $a \notin \mathfrak{p}$) and for some $n \geq 0$, we have $M_a \cong R_a^{\oplus n}$ as R_a-modules. Let $T := R_a \setminus \mathfrak{p}^e$ (since $a \notin \mathfrak{p}$, $\mathfrak{p}^e$ is still a prime ideal). Then

$$M_{\mathfrak{p}} = (R \setminus \mathfrak{p})^{-1} M \cong T^{-1} M_a.$$

Intuitively, this comes from the fact that $M_{\mathfrak{p}}$ is obtained form M by inverting the action of all elements outside of $\mathfrak{p}$. Instead of inverting everything at once, one may first invert a and then the other elements. This observation is exactly a rephrasement of the isomorphism above.

A precise way to prove this is to invoke Exercise 7.3 of sheet 12. We leave the reader to work out these exact details.

Once we have this isomorphism, we win since

$$M_{\mathfrak{p}} \cong T^{-1} M_a \cong T^{-1}(R_a^{\oplus n}) \cong (T^{-1} R_a)^{\oplus n} \cong R_{\mathfrak{p}}^{\oplus n}.$$

Now, assume that $M_{\mathfrak{p}}$ is free for all $\mathfrak{p}$. Our goal is to show that M is locally free. In fact, fix some prime $\mathfrak{p}$. We will show that if $M_{\mathfrak{p}}$ is free, then there exists some $a \notin \mathfrak{p}$ such that M_a is free (by definition, this will conclude). We will need the following:

Lemma 0.3. *Let N be a finitely generated module. If $N_{\mathfrak{p}} = 0$, then there exists $a \notin \mathfrak{p}$ such that $N_a = 0$.*

Proof. Let $n_1, \dots, n_l$ be generators of N. Since $N_\mathfrak{p} = 0$, we have that each elements $\frac{n_i}{1}$ are zero, so for all i there exists $a_i \notin \mathfrak{p}$ such that

$$a_i n_i = 0.$$

Let $a := n_1 \dots n_l \notin \mathfrak{p}$. Then $an_i = 0$ for all i, so $aN = 0$. In other words, we deduce that $N_a = 0$. □

Let $\frac{m_1}{r_1}, \dots, \frac{m_s}{r_s}$ denote free generators of $M_\mathfrak{p}$. Up to multiplying by a unit (the elements r_i), we may assume that $r_1 = \dots = r_s = 1$.

Consider the morphism $\theta : R^{\oplus s} \to M$ given by sending e_i to m_i. By construction, we have $\ker(\theta_\mathfrak{p}) = \operatorname{coker}(\theta_\mathfrak{p}) = 0$. By exactness of localization (see Exercise 6.3), we know that $\ker(\theta_\mathfrak{p}) = \ker(\theta)_\mathfrak{p}$ (and similarly for $\operatorname{coker}(\theta)$). Using the lemma, we then conclude that for some $a \notin \mathfrak{p}$,

$$\operatorname{coker}(\theta)_a = \ker(\theta)_a = 0$$

so as before,

$$\operatorname{coker}(\theta_a) = \ker(\theta_a) = 0.$$

In other words, $\theta_a : R_a^{\oplus s} \to M_a$ is an isomorphism, so M_a is free.

- We will show that the functor $\operatorname{Hom}(M, -)$ preserves surjections (by definition, this is equivalent to M being projective). Let $N \to L$ be a surjection, and let J denote the cokernel of the induced map $\operatorname{Hom}(M, N) \to \operatorname{Hom}(M, L)$. Fix some prime ideal $\mathfrak{p}$. By definition, we an exact sequence

$$\operatorname{Hom}(M, N) \to \operatorname{Hom}(M, L) \to J \to 0.$$

Since localization is exact, we then obtian an exact sequence

$$\operatorname{Hom}(M, N)_\mathfrak{p} \to \operatorname{Hom}(M, L)_\mathfrak{p} \to J_\mathfrak{p} \to 0.$$

By Exercise 7, we have natural isomorphisms $\operatorname{Hom}(M, N)_\mathfrak{p} \to \operatorname{Hom}(M_\mathfrak{p}, N_\mathfrak{p})$ and $\operatorname{Hom}(M, L)_\mathfrak{p} \to \operatorname{Hom}(M_\mathfrak{p}, L_\mathfrak{p})$. A quick compatibility check shows that we have an exact sequence

$$\operatorname{Hom}(M_\mathfrak{p}, N_\mathfrak{p}) \xrightarrow{\phi} \operatorname{Hom}(M_\mathfrak{p}, L_\mathfrak{p} \to J_\mathfrak{p} \to 0,$$

where the morphism ϕ is induced by applying $\operatorname{Hom}(M_\mathfrak{p}, -)$ to the surjection $N_\mathfrak{p} \to L_\mathfrak{p}$.

By projectivity of $M_\mathfrak{p}$ as an $R_\mathfrak{p}$-module, we deduce that $\operatorname{Hom}(M, L)_\mathfrak{p} \to \operatorname{Hom}(M_\mathfrak{p}, L_\mathfrak{p})$ is surjective. In other words, $J_\mathfrak{p} = 0$.

Since this holds for all $\mathfrak{p} \in \operatorname{Spec}(R)$ by the first point, we conclude by Proposition 0.2 (see the satum of the exercise).

- A free module is always projective, so we have to show the converse. Hence, assume that M is projective, and let us show that M is free.

Let $m_1, \dots, m_n \in M$ be elements such that their reduction module the maximal ideal $\mathfrak{m}$ of R forms a basis of $M/\mathfrak{m}M$ as an $R/\mathfrak{m}$-vector space.

In particular, they generate $M/\mathfrak{m}M$, so if N denotes the submodule generated by $m_1, \dots, m_n$, we obtain that

$$M = \mathfrak{m}M + N.$$

A way to rephrase this is that

$$M/N = \mathfrak{m}M/N.$$

By Nakayama's lemma (see Exercise 4.2 of sheet 9), we deduce that $M/N = 0$, so $M = N$.

Hence, the morphism $R^{\oplus n} \to M$ given by sending e_i to m_i is surjective, so we have a short exact sequence

$$0 \to K \to R^{\oplus n} \to M \to 0.$$

Since M is projective, this sequence actually splits, so $R^{\oplus n} \cong M \oplus K$. Reducing modulo $\mathfrak{m}$ shows that

$$R/\mathfrak{m}^{\oplus n} \cong M/\mathfrak{m} \oplus K/\mathfrak{m}K.$$

Since by construction, the map $R/\mathfrak{m}^{\oplus n} \to M/\mathfrak{m}$ is an isomorphism, we deduce that $K/\mathfrak{m}K = 0$. Hence, $K = \mathfrak{m}K$, so again by Nakayama's lemma, $K = 0$.

In other words, $R^{\oplus n} \to M$ is an isomorphism, so M is free.

- Let $\mathfrak{p}$ be a prime ideal. Since M is projective, so is $M_{\mathfrak{p}}$ (a direct way to see this is using that a module is projective if and only if it is a direct summand of a free module). By the previous point and the fact that $R_{\mathfrak{m}}$ is local, we deduce that $M_{\mathfrak{p}}$ is free. Since this holds for any prime ideal $\mathfrak{p}$, we conclude that M is locally free.

□

EPFL - Fall 2023 | Prof. Zs. Patakfalvi
Rings and modules | **Exercises**
Sheet 12 - Solutions

Exercise 1. The goal of this exercise is to see that the statement of Exercise 8 is wrong without the algebraically closed assumption.

(1) Let $R \to S$ be a morphism of commutative rings (thus making S an R-algebra), and let I be an ideal of $R[x_1, \dots, x_n]$. Then we have an isomorphism of S-algebras
$$R[x_1, \dots, x_n]\big/_I \otimes_R S \cong S[x_1, \dots, x_n]\big/_{(I)}$$
[*Hint: First show it for $I = 0$, and then deduce the general case using right exactness of the tensor product. The case $I = 0$ can be handled by a direct computation, or by showing that both sides satisfy the same universal property.*]

(2) Show that
$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$$
and hence it is not a domain (but it is nevertheless reduced!)

(3) Show that
$$\mathbb{F}_p(x) \otimes_{\mathbb{F}_p(x^p)} \mathbb{F}_p(x) \cong \mathbb{F}_p(x)[t]\big/_{(t-x)^p}$$
which is not even reduced.

Proof. (1) First let us deal with the case $I = 0$.

Hands-on approach: There is a bilinear map
$$R[x_1, \dots, x_n] \times S \to S[x_1, \dots, x_n]$$
given $(p, s) \mapsto sp$, so by definition this induced a morphism
$$R[x_1, \dots, x_n] \otimes_R S \to S[x_1, \dots, S_n]$$
and it is staightforward to see that this is an S-alebra morphism. Thus we are left to show that it is bijective. The point is that $R[x_1, \dots, x_n]$ is free as an R-module, with basis $\{x_1^{i_1} \cdots x_n^{i_n}\}_{i_1, \dots, i_n \geq 0}$. Therefore, as an S-module,
$$R[x_1, \dots, x_n] \otimes_R S$$
is also free with basis $\mathcal{B}_1 = \{x_1^{i_1} \cdots x_n^{i_n} \otimes 1\}_{i_1, \dots, i_n \geq 0}$ (we are using that $R \otimes_R S \cong S$ and that tensor products commute with direct sums). On the other hand, $S[x_1, \dots, x_n]$ is free with basis $\mathcal{B}_2 = \{x_1^{i_1} \cdots x_n^{i_n}\}_{i_1, \dots, i_n \geq 0}$, so since the maps $R[x_1, \dots, x_n] \otimes_R S \to S[x_1, \dots, x_n]$ described before maps bijectively $\mathcal{B}_1$ to $\mathcal{B}_2$, we win.

Categorical approach: We will freely use the categorical language here (i.e. categories, functors, adjoints, universal properties). Given A a ring, we denote by Alg_A the category of A-algebras. We have the obvious forgetful functor $\mathrm{Alg}_S \to \mathrm{Alg}_R$. Let us show that $- \otimes_R S$ defines a left adjoint.

Given $A \in \mathrm{Alg}_R, B \in \mathrm{Alg}_S$, we have to show that there is a natural bijection
$$\mathrm{Hom}_{\mathrm{Alg}_S}(A \otimes_R S, B) \to \mathrm{Hom}_{\mathrm{Alg}_R}(A, B)$$

Given $f : A \to B$ a map of R-algebras, define

$$f' : A \otimes S \to R$$

by $f'(a \otimes s) = sf(a)$, and conversely given a map $f' : A \otimes_R S \to B$ of S-algebras, define $f : A \to B$ via $f(a) = f'(a \otimes 1)$. We leave the fact that this gives a well-defined bijection to the reader (note that we could replace the word "algebras" by "modules" and this would work exactly the same way).

Note that if A is any ring, and B is an A-algebra,

$$\mathrm{Hom}_{\mathrm{Alg}_A}(A[x_1, \ldots, x_n], B) \cong \prod_{i=1}^{n} B$$

by definition of a polynomial ring (we can send the x_i's wherever we want, and this defines a ring map form the polynomial algebra).

From the above discussion, we obtain that if T is any S algebra, we have a natural bijection

$$\mathrm{Hom}_{\mathrm{Alg}_S}(R[x_1, \ldots, x_n] \otimes_R S, T) \cong \mathrm{Hom}_{\mathrm{Alg}_R}(R[x_1, \ldots, x_n], T) \cong \prod_{i=1}^{n} T \cong \mathrm{Hom}_{\mathrm{Alg}_S}(S[x_1, \ldots, x_n], T)$$

so both $R[x_1, \ldots, x_n] \otimes_R S$ and $S[x_1, \ldots, x_n]$ share the same universal property in the category of S-algebras, so there is a natural isomorphism between these two objects. To find it explicitly, we simply have to see what

$$id \in \mathrm{Hom}_{\mathrm{Alg}_S}(S[x_1, \ldots, x_n], S[x_1, \ldots, x_n])$$

corresponds to in $\mathrm{Hom}_{\mathrm{Alg}_S}(R[x_1, \ldots, x_n] \otimes_R S, S[x_1, \ldots, x_n])$. Unraveling the definitions gives us that this morphism is exactly the one given with the previous strategy.

Now let us work out the general case (i.e. I is not necessarily 0). We have a short exact sequence

$$0 \to I \to R[x_1, \ldots, x_n] \to R[x_1, \ldots, x_n]/I \to 0$$

Tensoring by S gives the exact sequence

$$I \otimes_R S \to R[x_1, \ldots, x_n] \otimes_R S \to R[x_1, \ldots, x_n]/I \otimes_R S \to 0$$

Note that the composition

$$I \otimes_R S \to R[x_1, \ldots, x_n] \otimes_R S \cong S[x_1, \ldots, x_n]$$

simply sends $\sum_i p_i \otimes s_i$ to $\sum_i p_i s_i$, so by definition its image is (I), whence we deduce that

$$R[x_1, \ldots, x_n]/I \otimes_R S \cong S[x_1, \ldots, x_n]/(I)$$

It is striaghtforward to check that this map is not only an isomorphism of S-modules, but actually S-algebras.

(2) Since $\mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1)$, we see by the previous point that

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{R}[x]/(x^2 + 1) \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}[x]/(x^2 + 1)$$

by the Chinese remainder theorem,

$$\mathbb{C}[x]/(x^2 + 1) = \mathbb{C}[x]/(x + i) \times \mathbb{C}[x]/(x - i) \cong \mathbb{C} \times \mathbb{C}$$

(3) Let us show the following result: let k be a field of characteristic $p > 0$ and $a \in k \setminus k^p$, and let $a^{1/p}$ be a p'th root living in some higher extension L of k. Then

$$k(a^{1/p}) \cong k[t]/(t^p - a)$$

Proof. The only thing to show is that $t^p - a$ is irreducible, so let us write by contradiction that $t^p - a = \alpha(t)\beta(t)$. Since in L, $t^p - a = (t - a^{1/p})^p$, we can write $\alpha(t) = (t - a^{1/p})^n$ and $\beta(t) = (t - a^{1/p})^m$ for some $m + n = p$. Therefore we get

$$k[t] \ni \alpha(t) = t^n - nt^{n-1}a^{1/p} + \text{lower order terms}$$

so since $a^{1/p} \notin k$, we must have $n = 0 \in k$, so since k has characteristic p either $n = 0 \in \mathbb{Z}$ or $n = p \in \mathbb{Z}$. In other words, either $\alpha(t)$ or $\beta(t)$ is a unit, hence we win. □

From the above, we deduce that

$$\mathbb{F}_p(x) \otimes_{\mathbb{F}_p(x^p)} \mathbb{F}_p(x) \cong \mathbb{F}_p(x^p)[t]/(t^p - x^p) \otimes_{\mathbb{F}_p(x^p)} \mathbb{F}_p(x) \cong \mathbb{F}_p(x)[t]/(t^p - x^p) = \mathbb{F}_p(x)[t]/(t-x)^p$$

□

Exercise 2. Let M be an A-module, and let $\mathfrak{a}$ be an ideal in A. Show that the following are equivalent:

(1) $M = 0$,
(2) $M_\mathfrak{p} = 0$, for every prime ideal $\mathfrak{p} \subseteq A$,
(3) $M_\mathfrak{m} = 0$, for every maximal ideal $\mathfrak{m} \subseteq A$.

Moreover, suppose that M is a finitely generated A-module, under this assumption prove that $M = \mathfrak{a}M$ if and only if $M_\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m}$ satisfying $\mathfrak{a} \subseteq \mathfrak{m}$.
[*Hint/Remark:* Although the exercise can be solved without directly proving the implication (3) ⇒ (2), it is highly instructive for anyone who thinks about studying more commutative algebra/algebraic geometry, to think through the (3) ⇒ (2) implication using Exercise 7.]

Proof. The implications (1) ⟹ (2) ⟹ (3) are obvious. Note also that by Exercise 7, the implication (3) ⟹ (2) is also straightforward: if (3) holds and $\mathfrak{p}$ is any prime ideal, then let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{p}$. Set $T = R \setminus \mathfrak{m}$ and $S = R \setminus \mathfrak{p}$ so that $T \subseteq S$, and define $\widetilde{S} \subseteq T^{-1}R$ as in Exercise 7. Then we have

$$M_\mathfrak{p} = S^{-1}M \cong \widetilde{S}^{-1}(T^{-1}M) = \widetilde{S}^{-1}M_\mathfrak{m} = 0,$$

as any localization of the zero module is the zero module. Thus (2) holds as well.
Now to prove (3) ⇒ (1), assume by contradiction that $M \neq 0$ but that $M_\mathfrak{m} = 0$, for every maximal ideal $\mathfrak{m}$. Then there exists $x \in M \setminus \{0\}$, and in particular $\mathrm{Ann}(x) \neq A$. Consider the inclusion $Ax \hookrightarrow M$ and let $\mathfrak{m}$ be a maximal ideal of A containing $\mathrm{Ann}(x)$. As localisation is exact, localisation at $\mathfrak{m}$ preserves injectivity, so $(Ax)_\mathfrak{m} \hookrightarrow M_\mathfrak{m} = 0$ is still injective. Therefore $(Ax)_\mathfrak{m} = 0$, which implies in particular that $x/1$ is equal to 0 inside $(Ax)_\mathfrak{m}$. By definition, this means that there exists $t \in A \setminus m$ such that $tx = 0$, which contradicts $\mathrm{Ann}(x) \subseteq \mathfrak{m}$. Hence we must have $M = 0$, and thus we proved the equivalence of the three statements.

Now to the second part. We have $M = \mathfrak{a}M$ if and only if $M/\mathfrak{a}M = 0$, which by the above is equivalent to $(M/\mathfrak{a}M)_\mathfrak{m} = 0$ for every maximal ideal $\mathfrak{m}$ of A. By exactness of taking localization (see Exercise 6.3 of sheet 11), we have $(M/\mathfrak{a}M)_m \cong M_\mathfrak{m}/(\mathfrak{a}M)_\mathfrak{m}$, and

notice that $(\mathfrak{a}M)_\mathfrak{m}$ can be naturally identified with the submodule $(\mathfrak{a}A_\mathfrak{m})M_\mathfrak{m}$ of $M_\mathfrak{m}$ (as the localization of the inclusion $\mathfrak{a}M \hookrightarrow M$ at $\mathfrak{m}$ has image $(\mathfrak{a}A_\mathfrak{m})M_\mathfrak{m}$).

Thus $\left(M/\mathfrak{a}M\right)_m$ is zero iff $M_\mathfrak{m} = (\mathfrak{a}A_\mathfrak{m})M_\mathfrak{m}$. If $\mathfrak{a}$ is not contained in the maximal ideal $\mathfrak{m}$ then $\mathfrak{a}$ contains a unit of $A_\mathfrak{m}$ and thus $M_\mathfrak{m} = (\mathfrak{a}A_\mathfrak{m})M_\mathfrak{m}$. Therefore, $M = \mathfrak{a}M$ if and only if $M_\mathfrak{m} = (\mathfrak{a}A_\mathfrak{m})M_\mathfrak{m}$ for all maximal ideals $\mathfrak{m}$ satisfying $\mathfrak{a} \subseteq \mathfrak{m}$. Finally, observe that if $M_\mathfrak{m}$ then trivially $M_\mathfrak{m} = (\mathfrak{a}A_\mathfrak{m})M_\mathfrak{m}$. On the other hand, if $M_\mathfrak{m} = (\mathfrak{a}A_\mathfrak{m})M_\mathfrak{m}$, then as $\mathfrak{a} \subseteq \mathfrak{m}$ we also have $M_\mathfrak{m} = (\mathfrak{m}A_\mathfrak{m})M_\mathfrak{m}$. By applying Nakayama's Lemma (Exercise 4.2 on sheet 9) to the finitely generated $A_\mathfrak{m}$-module $M_\mathfrak{m}$ and the local ring $(A_\mathfrak{m}, \mathfrak{m}A_\mathfrak{m})$, this implies $M_\mathfrak{m} = 0$. So $M_\mathfrak{m} = (\mathfrak{a}A_\mathfrak{m})M_\mathfrak{m}$ for $\mathfrak{a} \subseteq \mathfrak{m}$ if and only if $M_\mathfrak{m} = 0$. By combining all of the above, we hence obtain that $M = \mathfrak{a}M$ if and only if $M_\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m}$ with $\mathfrak{a} \subseteq \mathfrak{m}$. □

Exercise 3. Let $R = F[x]$, where F is a field.

(1) If F is algebraically closed, then show that for every prime ideal $\mathfrak{p}$ of R, either $R_\mathfrak{p} \cong F(x)$ or $R_\mathfrak{p} \cong F[x]_{(x)}$, where these isomorphisms are isomorphisms of F-algebras. Show that the above two cases are not isomorphic.

(2) If $F = \mathbb{R}$, then show that up to ring isomorphism there are three possibilities for $R_\mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of $F[x]$.
[*Hint:* To tell the three cases apart, consider the residue field, to show that there are only three cases, apply linear transformations to x.]

(3) Show that if F is algebraically closed, then $F[x, y]$ has infinitely many prime ideals $\mathfrak{p}$ for which $F[x, y]_\mathfrak{p}$ are pairwise non-isomorphic F-algebras. For this, you can use the following theorem of algebraic geometry:

Theorem. *There exists a sequence of irreducible polynomials $(f_d)_{d\in\mathbb{N}\setminus\{0,2\}}$ in $F[x, y]$ such that f_d is of degree d and such that the fields* $\mathrm{Frac}\left(F[x, y]/(f_d)\right)$ *are pairwise non-isomorphic as F-algebras.*

Proof. Let us first prove a useful result which we will use throughout this solution.

Lemma 0.1. *Let R, S be two local rings with respective maximal ideals $\mathfrak{m}_R$ and $\mathfrak{m}_S$. If $R \cong S$, then we also have an isomorphism of residue fields $R/\mathfrak{m}_R \cong S/\mathfrak{m}_S$.*

Proof. Recall that given a local ring T, its maximal ideal is exactly the set of non-invertible elements of T, which is certainly a notion preserved by isomorphisms.

Thus, in our case, an isomorphism $\theta : R \to S$ must satisfy $\theta^{-1}(\mathfrak{m}_S) = \mathfrak{m}_R$, so it induces an isomorphism of residue fields. □

(1) Every non-zero prime ideal of $F[x]$ is principal of the form $(x - a)$ since F is algebraically closed. We have $F[x]_{(0)} = F(x)$, hence it is sufficient to prove that there is a F-algebra isomorphism $F[x]_{(x-a)} \cong F[x]_{(x-b)}$ for all $a, b \in F$. First, consider the F-algebra endomorphism $\phi_{a,b} : F[x] \to F[x]$ obtained by mapping x to $x+a-b$. Then the composition $F[x] \overset{\phi_{a,b}}{\to} F[x] \to F[x]_{(x-b)}$ maps every element not divisible by $x - a$ to a unit in $F[x]_{(x-b)}$, and thus induces an F-algebra map $\overline{\phi_{a,b}} : F[x]_{(x-a)} \to F[x]_{(x-b)}$, which sends $f(x)/g(x)$ to $f(x + a - b)/g(x + a - b)$. It is thus clear that $\overline{\phi_{a,b}}$ and $\overline{\phi_{b,a}}$ are mutually inverse, and hence $F[x]_{(x-a)} \cong F[x]_{(x-b)}$ for all $a, b \in F$. Finally, there is an inclusion $F[x]_{(x)} \to F(x)$, but the two rings aren't isomorphic as $x \in F[x]_{(x)}$ is a non-zero non-unit, but $F(x)$ is a field.

(2) There are three options for prime ideals in $\mathbb{R}[x]$ we have that $p = 0$ or p is principal generated by $(x - a)$ for $a \in \mathbb{R}$ or p is principal generated by a degree two polynomial with no real roots. With the same proof as in the previous point one has $\mathbb{R}[x]_{(x-a)} \cong \mathbb{R}[x]_{(x-b)}$ for all $a, b \in \mathbb{R}[x]$. Now let $x^2 + bx + c$ be a monic quadratic polynomial without real roots (we can assume monicity without loss of generality). That is, we have $d^2 := c - b^2/4 > 0$. Then the linear change of coordinates where x is replaced by $dx + e$ where $e : -b/2$ transforms $x^2 + bx + c$ into $d^2(x^2 + 1)$. Another way of putting this, is that under the $\mathbb{R}$-agebra map $\phi : \mathbb{R}[x] \to \mathbb{R}[x]$ which sends x to $dx + e$, the polynomial $x^2 + bx + c$ is mapped to $d^2(x^2 + 1)$. Therefore, the composition $\mathbb{R}[x] \xrightarrow{\phi} \mathbb{R}[x] \to \mathbb{R}[x]_{d^2(x^2+1)}$ maps elements outside of (x^2+bx+c) to units, and thus we obtain an induced map of $\mathbb{R}$-algebras $\overline{\phi} : \mathbb{R}[x]_{(x^2+bx+c)} \to \mathbb{R}[x]_{(d^2(x^2+1))} = \mathbb{R}[x]_{(x^2+1)}$. By performing the inverse linear substitution (i.e. mapping x to $(x - e)/d$) one can construct an inverse to $\overline{\phi}$ with the same argument, and thus we obtain that $\mathbb{R}[x]_{(x^2+bx+c)} \cong \mathbb{R}[x]_{(x^2+1)}$ for all quadratic irreducible polynomials $x^2 + bx + c \in \mathbb{R}[x]$. So to conclude, we need to show that $\mathbb{R}(x)$, $\mathbb{R}[x]_{(x)}$ and $\mathbb{R}[x]_{(x^2+1)}$ are pairwise non-isomorphic. Notice that $x \in \mathbb{R}[x]_{(x)}$ and $x^2 + 1 \in \mathbb{R}[x]_{(x^2+1)}$ are non-zero non-units, and thus $\mathbb{R}(x)$ is not isomorphic to $\mathbb{R}[x]_{(x)}$ nor to $\mathbb{R}[x]_{(x^2+1)}$. Now the residue field of $\mathbb{R}[x]_{(x)}$, i.e. $\mathbb{R}[x]_{(x)}\big/ x \cdot \mathbb{R}[x]_{(x)}$ is, by Exercise 6.4 on sheet 11, isomorphic to $\mathrm{Frac}\left(\mathbb{R}[x]\big/(x)\right) \cong \mathbb{R}$. By the same argument, the residue field of $\mathbb{R}[x]_{(x^2+1)}$ is isomorphic to $\mathrm{Frac}\left(\mathbb{R}[x]\big/(x^2+1)\right) \cong \mathrm{Frac}(\mathbb{C}) = \mathbb{C}$. As $\mathbb{R} \ncong \mathbb{C}$ we conclude that $\mathbb{R}[x]_{(x)}$ and $\mathbb{R}[x]_{(x^2+1)}$ are non-isomorphic.

(3) Let $(f_d)_d$ be as in the theorem; we will show that $(F[x,y]_{(f_d)})_d$ are pairwise non-isomorphic for $d \in \mathbb{N} \setminus \{0, 2\}$. Suppose that there is an isomorphism $\phi : F[x,y]_{(f_d)} \to F[x,y]_{(f_{d'})}$ for some d, d'. Then the residue fields must be isomorphic too. However recall that in general, given a ring R and a prime ideal $\mathfrak{p}$, the maximal ideal of $R_\mathfrak{p}$ is $\mathfrak{p}R_\mathfrak{p}$ and the residue field is isomorphic to $\mathrm{Frac}(R/\mathfrak{p})$.

Using this fact in our case contradicts the choices of f_d and $f_{d'}$.

□

Exercise 4. Let F be an algebraically closed field.

(1) List the prime ideals of $R = F[x,y]\big/(xy)$.
[*Hint:* Consider the implications of a containment $xy \in \mathfrak{p}$, for a prime ideal $\mathfrak{p}$. Consider the projections $R \to R\big/(x)$ and $R \to R\big/(y)$ and use that you know the prime ideals of $F[y]$ and $F[x]$.]

(2) Show that for all prime ideals $\mathfrak{p}$ of R, $R_\mathfrak{p}$ falls into three cases up to F-algebra isomorphism, one which is a field, one which is a domain but not a field and one which is not a domain.

Proof. (1) The prime ideals of $R = F[x,y]\big/(xy)$ corresponds to prime ideals inside $F[x,y]$ containing xy. If $xy \in \mathfrak{p}$ for $\mathfrak{p}$ prime, then either $(x) \subseteq \mathfrak{p}$ or $(y) \subseteq \mathfrak{p}$. Suppose $(x) \subseteq \mathfrak{p}$, then the image $\mathfrak{q}$ of $\mathfrak{p}$ under the projection $F[x,y] \twoheadrightarrow F[x,y]\big/(x) \cong F[y]$ is prime (where the last isomorphism is given by setting x to 0). As F is algebraically closed, $\mathfrak{q}$ must be either (0), or of the form $\mathfrak{q} = (y - b)$ for some $b \in F$. As $\mathfrak{p}$ is the preimage of $\mathfrak{q}$, we obtain that $\mathfrak{p}$ is either equal to (x), or equal to $(x, y - b)$, and it is straightforward

to see that any such ideal is prime. By doing the same argument where the roles of x and y are swapped, we hence conclude that prime ideals of $F[x,y]$ containing xy are precisely (x), (y), $(x-a,y)$ for $a \in F$ and $(x,y-b)$ for $b \in F$. Hence the prime ideals of R are precisely $(\overline{x})$, $(\overline{y})$, $(\overline{x-a},\overline{y})$ for $a \in F$ and $(\overline{x},\overline{y-b})$ for $b \in F$, where we use $\overline{\bullet}$ to denote the class of an element.

(2) For this exercise, it is useful to know (and prove) the following lemma.

Lemma 1. *Let R be a ring with multiplicative subset T and ideal I. Let $S = R/I$ and let $\overline{T}$ be the image of T under $R \twoheadrightarrow S$. Then there is a natural ring isomorphism $\overline{T}^{-1}S \cong T^{-1}R\Big/I \cdot T^{-1}R$.*

Proof. Consider the composition $R \to T^{-1}R \to T^{-1}R\Big/I \cdot T^{-1}R$. As every element of I is mapped to 0, this induces a map $S \to T^{-1}R\Big/I \cdot T^{-1}R$ which sends $r+I$ to $\frac{r}{1}+I \cdot T^{-1}R$. In particular, let $\overline{t} \in \overline{T}$ be arbitrary, and write $\overline{t} = t+I$ for a $t \in T$. Then $\overline{t}$ is mapped to $\frac{t}{1}+I \cdot T^{-1}R$, which has inverse $\frac{1}{t}+I \cdot T^{-1}R$. Hence every element of $\overline{T}$ is mapped to a unit, and thus we obtain a ring map $\overline{T}^{-1}S \to T^{-1}R\Big/I \cdot T^{-1}R$, given by sending $\frac{r+I}{t+I}$ (with $t \in T$) to $\frac{r}{t}+I \cdot T^{-1}R$.

On the other hand, consider the composition $R \to S \to \overline{T}^{-1}S$. Then an element $t \in T$ is mapped to $(t+I)/1$, which is a unit since $t+I \in \overline{T}$. Hence we obtain an induced map $T^{-1}R \to \overline{T}^{-1}S$ sending $\frac{r}{t}$ to $\frac{r+I}{t+I}$. Notice that every element of the form $r/1$ with $r \in I$ is mapped to 0 by this mapped, and thus the ideal generated by elements of this form, i.e. $I \cdot T^{-1}R$, is in the kernel. Hence we obtain a map $T^{-1}R\Big/I \cdot T^{-1}R \to \overline{T}^{-1}S$ which maps $\frac{r}{t}+I \cdot T^{-1}R$ to $\frac{r+I}{t+I}$. It is then easy to see that this is inverse to the morphism constructed in the previous paragraph. □

Now to the exercise. By the above Lemma, we have

$$\Big(F[x,y]\Big/(xy)\Big)_{(\overline{x})} \cong (F[x,y]\setminus(x))^{-1}F[x,y]\Big/(xy)\cdot(F[x,y]\setminus(x))^{-1}F[x,y] =$$
$$= F[x,y]_{(x)}\Big/x \cdot F[x,y]_{(x)} \cong \operatorname{Frac}\Big(F[x,y]\Big/(x)\Big) \cong F(y)$$

where in the second to last isomorphism we Exercise 6.4 on sheet 11. By swapping the roles of x and y, one obtains $R_{(\overline{y})} \cong F(x)$.
Now let $b \in F \setminus \{0\}$, then

$$\Big(F[x,y]\Big/(xy)\Big)_{(\overline{x},\overline{y-b})} \cong (F[x,y]\setminus(x,y-b))^{-1}F[x,y]\Big/(xy)\cdot(F[x,y]\setminus(x,y-b))^{-1}F[x,y] =$$
$$= F[x,y]_{(x,y-b)}\Big/x \cdot F[x,y]_{(x,y-b)} \cong F[y]_{(y-b)}$$

where the last isomorphism is induced by sending x to 0 (or identifying $F[y] = F[x,y]\Big/(x)$ and using the Lemma). Again by swapping the roles of x and y we obtain $\Big(F[x,y]\Big/(xy)\Big)_{(\overline{x-a},\overline{y})} \cong F[x]_{(x-a)}$ for all $a \in F \setminus \{0\}$. These are all isomorphic by the proof of point Exercise 3.1, and are a domain which isn't a field.

Finally, $(F[x,y]\Big/(xy))_{(\overline{x},\overline{y})}$ is not a domain, since neither $\overline{x}/1$ nor $\overline{y}/1$ are zero, but their product is 0.

To sum up, up to a linear coordinate change we have $R_{\mathfrak{p}} \cong F(y)$ a field, $R_{\mathfrak{p}} \cong F[y]_{(y)}$ which is a domain but not a field or $R_{\mathfrak{p}} = (F[x,y]/(xy))_{(\overline{x},\overline{y})}$ which is not a domain. □

Exercise 5. Let R be a ring.

(1) Let $T \subseteq R$ a multiplicatively closed subset of R. Let $\mathfrak{q}$ be a prime ideal of $T^{-1}R$. Let $\mathfrak{q}^c$ be the contraction of q under $R \to T^{-1}R$. Prove that $\mathrm{ht}(\mathfrak{q}) = \mathrm{ht}(\mathfrak{q}^c)$.
(2) Let $\mathfrak{p}$ be a prime ideal of R. Prove that $\mathrm{ht}(\mathfrak{p}) = \dim R_{\mathfrak{p}}$.

Proof. The proof consists of the following steps based on the observation that both heights and dimensions are defined in terms of chains of ideals.

(1) Prime ideals of $T^{-1}R$ are in one-to-one correspondence with prime ideals of R that do not intersect T. A strictly increasing chain of prime ideals ending in $\mathfrak{q}$ induces a strictly increasing chain of prime ideals ending in $\mathfrak{q}^c$ by contraction. Conversely, if $\mathfrak{p} \subseteq \mathfrak{q}^c$ is prime, then in particular it must avoid T (as otherwise $\mathfrak{q}$ would contain a unit), and thus in a strictly increasing chain of prime ideals ending in $\mathfrak{q}^c$ induces a strictly increasing chain of prime ideals ending in $\mathfrak{p}$ by extension.
(2) Prime ideals of $R_{\mathfrak{p}}$ are in an inclusion preserving one-to-one correspondence with prime ideals of R avoiding $R \setminus \mathfrak{p}$, i.e. contained in $\mathfrak{p}$.

□

Exercise 6. Let $S \to R$ be a morphism of rings. Show that a prime ideal $\mathfrak{p}$ of S is the contraction of a prime ideal of R if and only if $\mathfrak{p}^{ec} = \mathfrak{p}$.
[*Hint:* For one direction use ideas from the proof of Going-Up Theorem (Proposition 9.4.2 of the lecture notes).]

Proof. Recall that if $\mathfrak{p}$ is an ideal of S and $\mathfrak{q}$ is an ideal of R then there are always containments $\mathfrak{q}^{ce} \subseteq \mathfrak{q}$ and $\mathfrak{p}^{ec} \supseteq \mathfrak{p}$. If there exists a prime ideal $\mathfrak{q}$ of R such that $\mathfrak{p} = \mathfrak{q}^c$, then $\mathfrak{p}^e = \mathfrak{q}^{ce} \subseteq \mathfrak{q}$ and therefore $\mathfrak{p}^{ec} \subseteq \mathfrak{q}^c = \mathfrak{p}$. Since the inclusion $\mathfrak{p} \subseteq \mathfrak{p}^{ec}$ holds always this shows that $\mathfrak{p}^{ec} = \mathfrak{p}$.
Conversely, denote $R_{\mathfrak{p}} := (\phi(S \setminus \mathfrak{p}))^{-1}R$ (this is a common notation so remember it) where $\phi : S \to R$ is the ring morphism from the statement. If $\mathfrak{p}^{ec} = \mathfrak{p}$ holds, then the ideal $\mathfrak{p}^e$ doesn't meet the image of $S \setminus \mathfrak{p}$ in R. Thus $\mathfrak{p}^e R_{\mathfrak{p}}$ is a proper ideal of $R_{\mathfrak{p}}$. Let $\mathfrak{m}$ be a maximal ideal of $R_{\mathfrak{p}}$ that contains $\mathfrak{p}^e R_{\mathfrak{p}}$. Let $\mathfrak{q} \subseteq R$ be the contraction of $\mathfrak{m}$ along $R \to R_{\mathfrak{p}}$. Then $\mathfrak{q}$ is a prime ideal of R that doesn't intersect the image of $S \setminus \mathfrak{p}$ in R, and $\mathfrak{p}^e \subseteq \mathfrak{q}$. Hence, $\mathfrak{p} = \mathfrak{p}^{ec} \subseteq \mathfrak{q}^c$, and $\mathfrak{q}^c \subseteq \mathfrak{p}$ as $\mathfrak{q}^c \cap (S \setminus \mathfrak{p}) = \emptyset$. □

Exercise 7. Let R be a ring, let M be an R-module and let $T, S \subseteq R$ be two multiplicatively closed subsets of R. Define $ST := \{st \mid s \in S, t \in T\}$ and $\widetilde{S} := \{s/1 \mid s \in S\} \subseteq T^{-1}R$.

(1) Show that ST and $\widetilde{S}$ are multiplicatively closed subsets of R resp. $T^{-1}R$.
(2) Show that there exists a ring morphism $\widetilde{S}^{-1}(T^{-1}R) \to (ST)^{-1}R$ sending $(r/t)/(s/1) \in \widetilde{S}^{-1}(T^{-1}R)$ to $r/(st) \in (ST)^{-1}R$. Show further that this is an isomorphism.
(3) Show that $\widetilde{S}^{-1}(T^{-1}M)$ and $(ST)^{-1}M$ are isomorphic as $(ST)^{-1}R$-modules, where the $(ST)^{-1}R$-module structure of $\widetilde{S}^{-1}(T^{-1}M)$ is provided via the isomorphism of the previous point.
(4) Show that if $T \subseteq S$ then $ST = S$, and formulate the results of points (2) and (3) in this case.

Proof. (1) Note that $1 \in S \cap T$ and thus $1 = 1 \cdot 1 \in ST$. Furthermore, if $s, s' \in S$ and $t, t' \in T$ then $(st)(s't') = (ss')(tt') \in ST$ as $ss' \in S$ and $tt' \in T$. Hence ST is multiplicatively closed. As for $\tilde{S}$, note that if $\phi : R \to R'$ is any ring morphism, then $\phi(S) \subseteq R'$ is multiplicatively closed as $\phi(1) = 1$ and ϕ preserves multiplication. So as $\tilde{S}$ is the image of S under the localisation morphism $R \to T^{-1}R$, we conclude that it is a multiplicatively closed subset of $T^{-1}R$.

(2) Denote by $\iota_T : R \to T^{-1}R$, $\iota_{ST} : R \to (ST)^{-1}R$ and $\iota_{\tilde{S}} : T^{-1}R \to \tilde{S}^{-1}(T^{-1}R)$ the localization morphisms. As $T \subseteq ST$, the morphism ι_{ST} sends every element of T to a unit. Hence by the universal property of localization, there exists a ring morphism $\iota_{T,ST} : T^{-1}R \to (ST)^{-1}R$ such that $\iota_{T,ST} \circ \iota_T = \iota_{ST}$. This implies that any $\frac{r}{t} \in T^{-1}R$ is mapped to $\frac{r}{t} \in (ST)^{-1}R$. Now let $s/1 \in \tilde{S}$ be arbitrary. Then $\iota_{T,ST}$ sends $s/1$ to $s/1 \in (ST)^{-1}R$, which is a unit (with inverse $1/s$). Hence by the universal property of localization, there exists a ring morphism $\phi : \tilde{S}^{-1}(T^{-1}R) \to (ST)^{-1}R$ such that $\phi \circ \iota_{\tilde{S}} = \iota_{T,ST}$. This implies that ϕ sends any $(r/t)/(s/1) \in \tilde{S}^{-1}(T^{-1}R)$ to $\iota_{S,ST}(r/t)(\iota_{S,ST}(s/1))^{-1} = r/(ts) \in (ST)^{-1}R$, so this is the morphism we sought to construct.

To prove that ϕ is an isomorphism, we construct an inverse. Note that $\iota_{\tilde{S}} \circ \iota_T : R \to \tilde{S}^{-1}(T^{-1}R)$ sends any $st \in ST$ to $(st/1)/(1/1)$, which has inverse $(1/t)/(s/1) \in \tilde{S}^{-1}(T^{-1}R)$. Indeed, we have

$$\left(\left(\frac{st}{1}\right)/\left(\frac{1}{1}\right)\right) \cdot \left(\left(\frac{1}{t}\right)/\left(\frac{s}{1}\right)\right) = \left(\left(\frac{s}{1}\right)/\left(\frac{s}{1}\right)\right) = 1_{\tilde{S}^{-1}(T^{-1}R)}.$$

Hence by the universal property of localization, there exists a ring morphism $\psi : (ST)^{-1}R \to \tilde{S}^{-1}(T^{-1}R)$ such that $\psi \circ \iota_{ST} = \iota_{\tilde{S}} \circ \iota_T$. This implies that any $r/(st) \in \tilde{S}^{-1}R$ is mapped to

$$\psi(r/(st)) = (\iota_{\tilde{S}} \circ \iota_T(r)) \cdot (\iota_{\tilde{S}} \circ \iota_T(st))^{-1} = \left(\left(\frac{r}{1}\right)/\left(\frac{1}{1}\right)\right) \cdot \left(\left(\frac{1}{t}\right)/\left(\frac{s}{1}\right)\right) = \left(\left(\frac{r}{t}\right)/\left(\frac{s}{1}\right)\right).$$

Hence ϕ and ψ are mutually inverse, and thus isomorphisms.

(3) The structure of $\tilde{S}^{-1}(T^{-1}M)$ as an $(ST)^{-1}R$-module is given by the formula

$$\frac{r}{st} \cdot \left(\left(\frac{m}{t'}\right)/\left(\frac{s'}{1}\right)\right) := \psi\left(\frac{r}{st}\right)\left(\left(\frac{m}{t'}\right)/\left(\frac{s'}{1}\right)\right) = \left(\left(\frac{rm}{tt'}\right)/\left(\frac{ss'}{1}\right)\right).$$

Tensor approach: Note that by Exercise 5 of Sheet 11, we have

$$(ST)^{-1}M \cong (ST)^{-1}R \otimes_R M$$

and

$$\tilde{S}^{-1}(T^{-1}M) \cong \tilde{S}^{-1}(T^{-1}R) \otimes_{T^{-1}R} (T^{-1}R \otimes_R M).$$

Note that we have

$$\tilde{S}^{-1}(T^{-1}R) \otimes_{T^{-1}R} (T^{-1}R \otimes_R M) \cong (\tilde{S}^{-1}(T^{-1}R) \otimes_{T^{-1}R} T^{-1}R) \otimes_R M \cong$$
$$\cong \tilde{S}^{-1}(T^{-1}R) \otimes_R M \cong (ST)^{-1}R \otimes_R M,$$

at the very least as R-modules. By following the chain of isomorphisms, the above isomorphism is given on simple tensors by mapping $(r/t)/(s/1) \otimes (r'/t' \otimes m)$ to

$((rr')/(tt's))\otimes m$. It is then straightforward to check that this map is in fact $(ST)^{-1}R$-linear, and thus an isomorphism of $(ST)^{-1}R$-modules.

Pure localization approach: Denote by $\iota_T^M : M \to T^{-1}M$, $\iota_{ST}^M : M \to (ST)^{-1}M$ and $\iota_{\tilde{S}}^M : T^{-1}M \to \tilde{S}^{-1}(T^{-1}M)$ the localization morphisms. Recall that $\tilde{S}^{-1}(T^{-1}M)$ is naturally an R-module, via the localization morphisms (i.e. multiplication by r is multiplication by $(r/1)/(1/1)$). Notice that multiplication by any $st \in ST$ on $\tilde{S}^{-1}(T^{-1}M)$ is invertible, with inverse being multiplication by $(1/t)/(s/1)$. Hence by the universal property of localization of a module (see the solution of Exercise 1 on Sheet 10), $\tilde{S}^{-1}(T^{-1}M)$ naturally has the structure of an $(ST)^{-1}R$-module via the formula

$$\frac{r}{st}\cdot\left(\left(\frac{m}{t'}\right)/\left(\frac{s'}{1}\right)\right) := ((r/1)/(1/1))\cdot(((st)/1)/(1/1))^{-1}\cdot\left(\left(\frac{m}{t'}\right)/\left(\frac{s'}{1}\right)\right) = \left(\left(\frac{rm}{tt'}\right)/\left(\frac{ss'}{1}\right)\right),$$

and there exists an $(ST)^{-1}M$-module morphism $\psi^M : (ST)^{-1}M \to \tilde{S}^{-1}(T^{-1}M)$ such that $\psi^M \circ \iota_{ST}^M = \iota_{\tilde{S}}^M \circ \iota_T^M$. Notice that the $(ST)^{-1}M$-module structure on $\tilde{S}^{-1}(T^{-1}M)$ is the same as the one defined via the isomorphism of the previous point, and that ψ^M maps an element $m/(st)$ to $(m/t)/(s/1)$.
Now either one constructs an inverse to ψ^M with a similar procedure, or one proves directly that ψ^M is an isomorphism. We will do the latter for once: if $y := (m/t)/(s/1) \in \tilde{S}^{-1}(T^{-1}M)$ is arbitrary, then ψ^M maps $x := m/(ts)$ to $(m/t)/(s/1)$, so ψ^M is surjective. Finally, suppose that ψ^M maps some $m/(st) \in (ST)^{-1}M$ to 0. Then there exists $s'/1 \in \tilde{S}$ such that $(s'/1)(m/t) = 0$ inside $T^{-1}M$. Therefore, there exists $t' \in T$ such that $t's'm = 0$ inside M. But then as $t's' \in S$, this means $m/(st) = 0$ inside $(ST)^{-1}M$. Thus ψ^M is also injective, and hence an isomorphism.

(4) As $1 \in T$ we have $S \subseteq ST$. On the other hand, we have $ST \subseteq SS \subseteq S$ as S is multiplicatively closed, so $ST = S$. Hence point (2) gives $\tilde{S}^{-1}(T^{-1}R) \cong S^{-1}R$ as rings, and point (3) gives $\tilde{S}^{-1}(T^{-1}M) \cong S^{-1}M$ as $S^{-1}R$-modules.

□

Exercise 8. In Exercise 6 of sheet 10, we saw how to construct the tensor product of two R-algebras. The goal is to show the following result:

Proposition 0.2. *Let k be an algebraically closed field, and let R, S two finitely generated k-algebras which are domains. Then $R \otimes_k S$ is again a domain.*

During this exercise, you can freely use the following results (which you will see shortly) :

- Nullstellensatz (Theorem 6.5.4 from the notes)
- For any finitely generated k-algebra T and any maximal ideal $\mathfrak{m}$, the composition $k \to T \to T/\mathfrak{m}$ is an isomorphism (see the proof of the weak Nullstelensatz, which is Theorem 6.2.2 in the notes).

Proceed as follows:

(1) Let T be a finitely generated k-algebra which is a domain, and let $a_1, \dots a_s \in T$ be non-zero. Show that there is a maximal ideal $\mathfrak{m}$ of T such that $a_i \notin \mathfrak{m}$ for all i.
[*Hint*: write T as a quotient of a polynomial ring, and use Nullstellensatz.]

(2) Show that any element in $R \otimes_k S$ can be written as

$$\sum_i a_i \otimes b_i$$

with the b_i's linearly independent over k.

(3) Assume that

$$\left(\sum_i a_i \otimes b_i\right) \cdot \left(\sum_j a'_j \otimes b'_j\right) = 0$$

where both families $(b_i)_i$ and $(b'_j)_j$ are linearly independent. Let $\mathfrak{m}$ be a maximal ideal not containing any of the a_i, a'_j.
Show by applying the ring map

$$R \otimes_k S \to R/\mathfrak{m} \otimes_k S \cong S$$

that one of the factors must be zero, and hence conclude that $R \otimes_k S$ is a domain.

Proof. (1) We give two proofs of this part: one uses the intended way (which is more "geometric"), while the other one works over arbitrary fields (and is more "algebraic").

Note that in both cases, we may assume $s = 1$ (we will write $a = a_1$). Indeed, since T is a domain, $\prod_i a_i \neq 0$, so we reduce to the case $s = 1$ since maximal ideals are prime.

Intended way: Let us write $T = k[x_1, \ldots, x_n]/I$ (this is possible by definitionof a finitely generated k-algebra). We need to find a maximal ideal in T which does not contain a. Let $b \in k[x_1, \ldots, x_n]$ be a lift of a. By the correspondence theorem, we need to find a maximal ideal in $k[x_1, \ldots, x_n]$ which contains I but not b.

By Nullstellensatz, this is equivalent to finding some $x \in k^n$ such that $x \in V(I)$ but $x \notin V(b)$. Indeed, if we had such an element, the maximal ideal $\mathfrak{m} := I(\{x\})$ would do the job by Nullstellensatz.

If such an x did not exist, then we would have $V(I) \subseteq V(b)$. Applying Nullstensatz would then give

$$b \in \sqrt{(b)} = I(V(b)) \subseteq I(V(I)) = \sqrt{I} = I$$

where the last equality holds since I is prime ($T = k[x_1, \ldots, x_n]/I$ is a domain). However, $b \in I$ implies that $a = 0$ (recall b is a lift of $a \in k[x_1, \ldots, x_n]/I$) which contradicts the hypothesis.

More general way: Let us show the following result:

Lemma 0.3. *Let k be an arbitrary field, and let $f : T \to S$ be a morphism of finitely generated k-algebras. Then for all maximal ideal $\mathfrak{m} \subseteq S$, $f^{-1}(\mathfrak{m})$ is maximal.*

Proof. The map f induces an injection

$$T/f^{-1}(\mathfrak{m}) \to S/\mathfrak{m}$$

Since $S/\mathfrak{m}$ is a field, we have

$$\operatorname{trdeg}_k(S/\mathfrak{m}) = \dim(S/\mathfrak{m}) = 0$$

Since $T/f^{-1}(\mathfrak{m}) \subseteq S/\mathfrak{m}$, we also have $\operatorname{trdeg}_k(T/f^{-1}(\mathfrak{m})) = 0$, and hence $\dim(T/f^{-1}(\mathfrak{m})) = 0$. This means by definition that any prime ideal of $\dim(T/f^{-1}(\mathfrak{m}))$ is maximal. Since

$T/f^{-1}(\mathfrak{m})$ is a domain (the preimage of a prime ideal is always a prime ideal!), we deduce that (0) is maximal, so $T/f^{-1}(\mathfrak{m})$ is a field (i.e. $f^{-1}(\mathfrak{m})$ is maximal). □

Remark 0.4. This lemma above is completely wrong for non-finitely generated k-algebras! For example $k[x] \subseteq k(x)$ gives a counterexample ((0) is maximal in $k(x)$, but not in $k[x]$).

Now, the point is that T_a is again a finitely generated k-algebra! (indeed, we have $T_a \cong T[x]/(xa-1)$). Thus, given any maximal ideal $\mathfrak{m} \subseteq T_a$, its preimage $\mathfrak{m}^c$ will be maximal in T by the lemma above. Since it cannot contain a, we win.

(2) Let $\sum_{i\in I} r_i \otimes s_i \in R \otimes_k S$. If the elements s_i are linearly independent, we are fine. If not, we can write $s_j = \sum_{i\neq j} \alpha_i s_i$, we

$$\sum_{i\in I} r_i \otimes s_i = \sum_{i\neq j}(r_i \otimes s_i) + r_j \otimes \sum_{i\neq j} \alpha_i s_i = \sum_{i\neq j}(r_i \otimes s_i) + \sum_{i\neq j}(\alpha_i r_j) \otimes s_i = \sum_{i\neq j}(r_i + \alpha_i r_j) \otimes s_i$$

Note that in the right-hand side, s_j never appears. Since the index set I is finite, this process has to finish at some point.

(3) Let us show that $R \otimes_k S$ is a domain. Assume that

$$\left(\sum_i a_i \otimes b_i\right) \cdot \left(\sum_j a'_j \otimes b'_j\right) = 0$$

and assume that both families $(b_i)_i$ and $(b'_j)_j$ are linearly independent (see the previous point). By contradiction, further assume that both elements above are non-zero. Therefore, $a_{i_1} \neq 0$ and $a'_{j_1} \neq 0$ for some i_1, j_1. By the first point, there exists a maximal ideal $\mathfrak{m}$ be a maximal ideal not containing a_{i_1} and a_{j_1}.

Since k is algebraically closed, $R/\mathfrak{m} \cong k$ by the weak Nullstellensatz. Let $\theta : R/\mathfrak{m} \to k$ denote an isomorphism. Thus there is a ring map $R \otimes_k S \to S$ is given by $\sum_i r_i \otimes s_i \mapsto \sum_i \theta(\overline{r_i}) s_i$. Applying our ring map above gives the element

$$\left(\sum_i \theta(\overline{a_i}) b_i\right) \cdot \left(\sum_j \theta(\overline{a'_j}) b_j\right) = 0$$

Since S is a domain, one of the two terms above is 0 (without loss of generality we may assume $\sum_i \theta(\overline{a_i}) b_i = 0$).

Since the b_i's are linearly independent, we have $\theta(\overline{a_i}) = 0$ for all i. However, θ is an isomorphism, so $\overline{a_{i_1}} = 0$. This is impossible since $a_{i_1} \notin \mathfrak{m}$ by assumption.

□

EPFL - Fall 2022 | Prof. Zs. Patakfalvi
Rings and modules | **Exercises**
Sheet 13 - Solutions

Exercise 1. Let F be a field and let R be a ring, let $I = (f) \subseteq F[x]$ be a principal ideal, and let $\phi : F[x] \to R$ be a ring morphism. If we speak of extensions and contractions of ideals in this exercise, they are always understood to be with respect to ϕ. Let g be a generator of the ideal $I^{ec} \subseteq F[x]$, and note that g is uniquely defined up to multiplication by a unit. Give a formula for g in terms of the prime factors of f when ϕ is

(1) the localization $F[x] \to F[x]_x$.
(2) the localization $F[x] \to F[x]_{(x)}$ (i.e. localization at the prime ideal $(x) \subseteq F[x]$).

Additionally, characterize in both casers when $I^{ec} = I$, in terms of the prime factors of f.

Proof. If $f = 0$ we have $g = 0$ in both cases, so suppose $f \neq 0$. Write $f = x^n f_0$ where $f_0 \in F[x] \setminus \{0\}$ is such that x doesn't divide f_0 and $n \in \mathbb{Z}_{\geq 0}$.

(1) Using point (2) of Proposition 9.3.8 of the printed course notes we have

$$\begin{aligned} I^{ec} = \bigcup_{m \geq 0} (I : x^m) &= \{r \in F[x] \text{ such that } \exists m \geq 0 : \ x^m r \in I\} \\ &= \{r \in F[x] \text{ such that } \exists m \geq 0 : \ x^n f_0 \mid x^m r\} \\ &= \{r \in F[x] \text{ such that } f_0 \mid r\} = (f_0). \end{aligned}$$

Hence $g = f_0$, and thus $I^{ec} = I$ if and only if $f = 0$ or x doesn't divide f, i.e. $f(0) \neq 0$.

(2) Using point (2) of Proposition 9.3.8 of the printed course notes we have

$$\begin{aligned} I^{ec} = \bigcup_{h \notin (x)} (I : h) &= \{r \in F[x] \text{ such that } \exists h \notin (x) : \ hr \in I\} \\ &= \{r \in F[x] \text{ such that } \exists h \notin (x) : \ x^n f_0 \mid hr\} \\ &= \{r \in F[x] \text{ such that } x^n \mid r\} \end{aligned}$$

where for the last equality we used that as $x^n | hr$ and $h \notin (x)$ we have $x^n | r$ and if $x^n | r$ then we can take $h = f_0$ to obtain $x^n f_0 | f_0 r$. Hence $I^{ec} = (x^n)$, i.e. $g = x^n$. In particular, we have $I^{ec} = I$ if and only if f is of the form $f = \lambda x^n$ for $\lambda \in F$ and $n \geq 0$.

□

Exercise 2. If $S \subseteq R$ is a ring extension and $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals of S resp. R, respectively, we say that $\mathfrak{q}$ lies above $\mathfrak{p}$ if and only if $\mathfrak{q}^c = \mathfrak{p}$. Show the following:

(1) Let R be a UFD. Then an ideal $\mathfrak{p} \subseteq R$ is a prime ideal of height 1 if and only there exists an irreducible element $f \in R$ such that $\mathfrak{p} = (f)$.
(2) If $S \subseteq R$ is an integral extension and $\mathfrak{p} \subseteq S$ is a prime ideal, then all prime ideals lying over $\mathfrak{p}$ have height at most that of $\mathfrak{p}$, with equality for at least one of them.
[*Hint:* Localize at $\mathfrak{p}$.]
(3) If $S \subseteq R$ is an integral extension of domains, then all primes of R lying over height 1 primes of S are of height 1.
(4) The ideal $\mathfrak{p} = (x^2 + y^2 + 1) \subseteq \mathbb{C}[x^2, y^2]$ is a height 1 prime, and there is a single prime in $\mathbb{C}[x, y]$ lying over it.

Proof. (1) Let f be an irreducible element of R. Then if $ab \in (f)$ for some $a, b \in R$ we have that f divides ab, and thus f must appear in the irreducible factor decomposition of either a or b. That is, either $a \in (f)$ or $b \in (f)$, and thus (f) is prime.
Now suppose that $\mathfrak{p} \subseteq R$ is a prime of height 1. In particular $\mathfrak{p} \neq (0)$, so let $r \in \mathfrak{p}$ be non-zero. As $\mathfrak{p}$ is prime, there must be an irreducible factor f of r such that $f \in \mathfrak{p}$. But then $(0) \subsetneq (f) \subseteq \mathfrak{p}$, so as $\mathfrak{p}$ is of height 1 and $(0), (f)$ are prime, we must have $\mathfrak{p} = (f)$.
Finally, if $f \in R$ is irreducible and by contradiction we have a chain $(0) \subsetneq \mathfrak{q} \subsetneq (f)$ with $\mathfrak{q}$ a prime ideal. Take some non-zero $s_0 \in \mathfrak{q}$. Then f divides s_0, so there is $s_1 \in R$ with $s_0 = fs_1$. As $f \notin \mathfrak{q}$, this implies $s_1 \in \mathfrak{q}$. Repeating this argument, we obtain a sequence of elements $(s_i)_i$ of $\mathfrak{q}$ such that $s_i = fs_{i+1}$, and thus f^i divides s_0 for every $i \geq 0$. This is a contradiction, so (f) must have height 1.

(2) Let $\mathfrak{q}$ be a prime of R lying over $\mathfrak{p}$. Let $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_n = \mathfrak{q}$ be a strictly increasing chain of prime ideals of R. Then by point (2) of the Going-Up Theorem (Proposition 9.4.2 of the printed course notes) $\mathfrak{q}_0 \cap S \subsetneq \cdots \subsetneq \mathfrak{q}_n \cap S = \mathfrak{p}$ is a strictly increasing chain of prime ideals of S, and thus $n \leq \operatorname{ht} \mathfrak{p}$. Thus we conclude $\operatorname{ht} \mathfrak{q} \leq \operatorname{ht} \mathfrak{p}$.

To construct a prime ideal where we have equality, as in the proof of Proposition 9.4.2 denote $R_{\mathfrak{p}} := (S \setminus \mathfrak{p})^{-1}R$, and observe that $S_{\mathfrak{p}} \to R_{\mathfrak{p}}$ is integral. Hence by Corollary 9.4.4 in the printed course notes we have $\dim R_{\mathfrak{p}} = \dim S_{\mathfrak{p}}$, and by point (2) of Exercise 5 on Sheet 12 we have $\dim S_{\mathfrak{p}} = \operatorname{ht} \mathfrak{p}$. Therefore, there exists a maximal ideal $\mathfrak{n}$ of $R_{\mathfrak{p}}$ such that $\operatorname{ht} \mathfrak{n} = \operatorname{ht} \mathfrak{p}$. Just as in the proof of Proposition 9.4.2, if $\mathfrak{q}$ denotes the contraction of $\mathfrak{n}$ under $R \to R_{\mathfrak{p}}$, then $\mathfrak{q}$ lies over $\mathfrak{p}$. But then by point (1) of Exercise 5 on Sheet 12 we have $\operatorname{ht} \mathfrak{n} = \operatorname{ht} \mathfrak{q}$ and thus $\mathfrak{q}$ is a prime lying over $\mathfrak{p}$ with same height as $\mathfrak{p}$.

(3) Let $\mathfrak{p} \subseteq S$ be a prime of height 1 and let $\mathfrak{q} \subseteq R$ be a prime lying over S. By the previous point, we have $\operatorname{ht} \mathfrak{q} \leq 1$. If by contradiction $\operatorname{ht} \mathfrak{q} = 0$, then as R is a domain we must have $\mathfrak{q} = 0$, and thus also $\mathfrak{p} = 0$, which contradicts $\operatorname{ht} \mathfrak{p} = 1$. Hence $\operatorname{ht} \mathfrak{q} = 1$.

(4) As $\mathbb{C}[x^2, y^2] \cong \mathbb{C}[u, v]$, it is a UFD. Notice also that $\mathbb{C}[x^2, y^2] \subseteq \mathbb{C}[x, y]$ is an integral extension, as x, y are integral over $\mathbb{C}[x^2, y^2]$.
First of all, notice that $x^2 + y^2 + 1$ is an irreducible element of $\mathbb{C}[x^2, y^2]$, and thus by point (1) it is a prime of height 1. Let $\mathfrak{q} \subseteq \mathbb{C}[x, y]$ be a prime lying over $\mathfrak{p}$, which exists by Going-Up. But now notice that $x^2 + y^2 + 1$ is also irreducible in $\mathbb{C}[x, y]$, by seeing it as an element of $\mathbb{C}[x][y]$ and applying Eisenstein's criterion with the prime element $x + i$. Thus $(x^2 + y^2 + 1) \cdot \mathbb{C}[x, y]$ is a prime contained inside $\mathfrak{q}$, and as the latter is of height 1, we must have $\mathfrak{q} = (x^2 + y^2 + 1) \cdot \mathbb{C}[x, y]$. This is clearly a prime of height 1, and it lays over $\mathfrak{p}$: indeed, if $f \in \mathbb{C}[x, y]$ is such that $(x^2 + y^2 + 1)f \in \mathbb{C}[x^2, y^2]$, then f can't contain a monomial of the form $x^i y^j$ with at least one of i, j being odd, because if we take such i, j with $i + j$ minimal then $x^i y^j$ also appears in $x^2 + y^2 + 1$, contradiction. So $\mathfrak{q} = (x^2 + y^2 + 1) \cdot \mathbb{C}[x, y]$ is the only prime of height 1 lying over $\mathfrak{p}$. □

Exercise 3. Let R be a ring which is the quotient of a polynomial ring over an algebraically closed field F by a radical ideal. This naturally determines an algebraic set X whose coordinate ring is R. Noether normalisation says there is a subring $S \subseteq R$ such that $S \cong F[t_1, ..., t_r]$ and R is an integral extension of S. Give a geometric interpretation of Noether normalisation. That is, the inclusion $S \to R$ corresponds to a morphism f of

algebraic sets. Prove that the fibres of f are finite, i.e. the preimage of any point in F^r under f consists of a finite set of points in X.

Proof. Recall that if for two algebraic sets $X \subseteq F^m$ and $Y \subseteq F^n$ we have an F-algebra morphism $\lambda : A(Y) \to A(X)$ then this determines a morphism of algebraic sets $f : X \to Y$ such that $\lambda = \lambda_f$. Following the hint and using the same notations as in the solution to Exercise 5, let $\overline{\mathfrak{m}}_P$ be a maximal ideal of $A(X)$ (where $P = (a_1, \dots, a_m) \in X$). Let $h_1, \dots, h_n \in F[x_1, \dots, x_m]$ be such that $\lambda(y_j + I(Y)) = h_j + I(X)$ for all j. Let $\phi : F[y_1, \dots, y_n] \to F[x_1, \dots, x_m]$ be the F-algebra morphism defined by mapping y_j to h_j, and let $\pi_X : F[x_1, \dots, x_m] \to A(X)$ and $\pi_Y : F[y_1, \dots, y_m] \to A(Y)$ be the projection maps. Then by Exercise 4 we have $\pi_X \circ \phi = \lambda \circ \pi_Y$. Therefore

$$\pi_Y^{-1}(\lambda^{-1}(\overline{\mathfrak{m}}_P)) = \phi^{-1}(\pi_X^{-1}(\overline{\mathfrak{m}}_P)) = \phi^{-1}(\mathfrak{m}_P).$$

Now by construction we have $\phi(y_j - f(P)_j) = h_j - h_j(P)$ and thus evaluating $\phi(y_j - f(P)_j)$ at P gives 0. Hence $y_j - f(P)_j \in \phi^{-1}(\mathfrak{m}_P)$ for all j, and thus $\mathfrak{n}_{f(P)} := (y_1 - f(P)_1, \dots, y_n - f(P)_n) \subseteq \phi^{-1}(\mathfrak{m}_P)$. As $\mathfrak{n}_{f(P)}$ is maximal and $1 \notin \phi^{-1}(\mathfrak{m}_P)$, we thus have

$$\mathfrak{n}_{f(P)} = \phi^{-1}(\mathfrak{m}_P) = \pi_Y^{-1}(\lambda^{-1}(\overline{\mathfrak{m}}_P)).$$

Applying π_Y on both sides this gives

$$\overline{\mathfrak{n}}_{f(P)} = \lambda^{-1}(\overline{\mathfrak{m}}_P).$$

This expresses how one can obtain $f : X \to Y$ from $\lambda : A(Y) \to A(X)$ in terms of maximal ideals.

Now we are ready to tackle the Exercise. Let $\lambda : S \hookrightarrow R$ be the inclusion. By Exercise 7 of sheet 7, the algebraic sets determined by S and R can be identified with $\mathrm{MaxSpec}(S)$ resp. $\mathrm{MaxSpec}(R)$, and by the paragraph above λ determines a morphism of algebraic sets $f : \mathrm{MaxSpec}(R) \to \mathrm{MaxSpec}(S) \cong F^r$ given by $\mathfrak{m} \mapsto \lambda^{-1}\mathfrak{m} = \mathfrak{m} \cap S$. So to show that f has finite fibers, we need to show that for every maximal ideal $\mathfrak{n} \subseteq S$, there exist at most finitely many maximal ideals $\mathfrak{m}$ of R such that $\mathfrak{m} \cap S = \mathfrak{n}$. Any such $\mathfrak{m}$ contains $\mathfrak{n}^e = R \cdot \mathfrak{n}$, so we may suppose that the latter is non-trivial, and then the maximal ideals $\mathfrak{m} \subseteq R$ with $\mathfrak{m} \cap S = \mathfrak{n}$ are in one-to-one correspondence with the maximal ideals of $R/\mathfrak{n}^e$. Note that λ gives rise to a map $\overline{\lambda} : S/\mathfrak{n} \to R/\mathfrak{n}^e$. Furthermore, we have $S/\mathfrak{n} \cong F$ (by sending a scalar α to its class $\alpha + \mathfrak{n}$), and as the target ring is non-trivial we must have $\ker \overline{\lambda} = 0$. Hence, under the identification $S/\mathfrak{n} \cong F$, we have that $\overline{\lambda}$ is just the natural inclusion of F into $R/\mathfrak{n}^e$ (as R is a quotient of a polynomial ring over F, $R/\mathfrak{n}^e$ is too, and thus there is a natural inclusion $F \to R/\mathfrak{n}^e$). On the other hand, as λ is an integral extension, $\overline{\lambda}$ is too. Indeed, if $r + \mathfrak{n}^e \in R/\mathfrak{n}^e$ then there is a monic polynomial $T^d + s_{d-1}T^{d-1} + \cdots + s_0 \in S[T]$ annihilating r, and thus $T^d + (s_{d-1} + \mathfrak{n})T^{d-1} + \cdots + (s_0 + \mathfrak{n}) \in (S/\mathfrak{n})[T]$ is a monic polynomial annihilating $r + \mathfrak{n}^e$. In conclusion, $R/\mathfrak{n}^e$ is a finitely generated F-algebra which is integral over F. Let $g_1, \dots, g_l$ be generators of $R/\mathfrak{n}^e$, i.e. $R/\mathfrak{n}^e = F[g_1, \dots, g_l]$. Now let $N \in \mathbb{Z}_{>0}$ be such that for every g_i there exists a monic polynomial in $F[T]$ annihilating it. Then every power of g_i can be written as an F-linear combination of $1, g_i, \dots, g_i^{N-1}$. Hence every element of $R/\mathfrak{n}^e = F[g_1, \dots, g_l]$ can be written as an F-linear combination of $\{g_1^{c_1} \cdots g_l^{c_l} \mid c_1, \dots, c_l \in \{0, \dots, N-1\}\}$. In partiular, $R/\mathfrak{n}^e$ is finite as an F-vector space, so in particular Artinian. So by Exercise 7 on Sheet 9, $R/\mathfrak{n}^e$ has only finitely many maximal

ideals, and hence the fiber $f^{-1}(\mathfrak{n})$ is finite.

Alternative approach, following the proof of Noether Normalization S is itself a polynomial ring, so it is the co-ordinate ring of the algebraic set F^r. Thus by the previous Question, the inclusion $S \to R$ corresponds to a morphism $f : X \to F^r$.
To show that the fibres (i.e. the set of pre-images of a point) are finite, use the notation of the proof of Noether normalisation for an infinite field as in the lecture notes. That is, we use induction on the number of variables n such that R is a quotient of a polynomial ring in n variables to prove that there exists a poynomial ring $S \subset R$ over which R is integral and such that the induced morphism of algebraic sets has finite fibers. Hence, we only need to modify the proof in the lecture notes slightly. For $n = 1$ the statement is clear since the algebraic set X in this case is the finite set of roots of the polynomial f. Let X' be the algebraic set determined by the ring R' as a quotient of $F[x_1 - c_1x_n, ..., x_{n-1} - c_{n-1}x_n]$ (notation as in the lecture notes). If we show that the fibres of $X \to X'$ are finite then we are done by induction. Suppose $P = (p_1, ..., p_{n-1}) \in X' \subset F^{n-1}$. Then we wish to show that the set $\Lambda = \{x \in F : (p_1 - c_1x, ..., p_{n-1} - c_{n-1}x, x) \in X\}$ is finite. In the proof of Noether normalisation, we found a polynomial $g'(y_1 - c_1y_n, ..., y_{n-1} - c_{n-1}y_n, y_n)$ which is satisfied everywhere on X but which is monic as a polynomial in y_n. But this then implies there can be only finitely many possible values of x in Λ, as these are the solutions of this polynomial for certain values of y_i for $i = 1, ..., n - 1$.

□

Exercise 4. Let F be an algebraically closed field. Calculate the Krull dimension of the ring

$$F[w, x, y, z]\Big/(x^2 - wy, y^2 - xz, wz - xy).$$

Proof. We saw already in Exercise 5 of sheet 7 (the same proof works over any algebraically closed field) that the $R = F[w, x, y, z]\Big/(x^2 - wy, y^2 - xz, wz - xy)$ is the coordinate ring of the algebraic set $Z = \{(u^3, u^2v, uv^2, v^3) \mid u, v \in F\}$. In fact, define $\Phi : F[w, x, y, z] \to F[u^3, u^2v, uv^2, v^3]$ by $w \mapsto u^3, x \mapsto u^2v, y \mapsto uv^2, z \mapsto v^3$ (as in the solution to Exercise 3). The kernel is precisely the set of all polynomials $f \in F[w, x, y, z]$ that vanish on the set Z, i.e., the kernel of Φ is the ideal $I(Z) = (x^2 - wy, y^2 - xz, wz - xy)$. Thus R is isomorphic to the image of Φ, which is $F[u^3, u^2v, uv^2, v^3]$. There is an obvious inclusion of rings $F[u^3, u^2v, uv^2, v^3] \subset F[u, v]$ and the latter is obviously integral over the former. Therefore the dimension of $R \cong F[u^3, u^2v, uv^2, v^3]$ is the same as the dimension of the polynomial ring $F[u, v]$. As we have seen repeatedly in this course the dimension of a polynomial ring in two variables is two. So $\dim R = 2$. □

Exercise 5. Let F be an algebraically closed field. Calculate a primary decomposition for the ideals

(1) $(x^4 - 2x^3 - 4x^2 + 2x + 3) \subseteq F[x]$,
(2) $(x^2, xy^2) \subseteq F[x, y]$,
(3) $(x^2, xy, xz, yz) \subseteq F[x, y, z]$.

Proof. (1) Factorizing the polynomial, we get:

$$x^4 - 2x^3 - 4x^2 + 2x + 3 = (x - 3)(x - 1)(x + 1)^2$$

Therefore the ideal is the intersection of the primary factors $(x-3)$, $(x-1)$ and $(x+1)^2$. These are primary because their radicals are maximal.

(2) A primary decomposition is

$$(x^2, xy^2) = (x^2, y^2) \cap (x)$$

The first factor is primary as it has a radical which is a maximal ideal, while the second is prime. The above equation holds because if $p \in (x^2, y^2) \cap (x)$, then $p = x^2a + y^2b$ and $x \mid p$, so $b = xc$ for some c and $p = x^2a + xy^2c$. Hence $p \in (x^2, xy^2)$.

(3) It may help to first calculate the irreducible components of $V(I)$ where $I = (x^2, xy, xz, yz)$. If (a, b, c) is a point of F^3 where a^2, ab, ac, bc all vanish, the first thing we can deduce from $a^2 = 0$ is that $a = 0$. Hence $ab = ac = 0$ gives us no new information, and $bc = 0$ implies that at least one of b and c is zero. Hence $V(I) = V((x, y)) \cup V((x, z))$ is the decomposition into irreducible components of $V(I)$, and hence as a first guess, we may try if (x, y) and (x, z) themselves appear in the minimal primary decomposition. As

$$(x, y) \cap (x, z) = (x, yz)$$

we need at least another ideal. The point is that, as you may see later in your studies, the primary decomposition is somewhat related to the order of vanishing of elements in the ideal. Here, all elements vanish at order 2 at the origin (and no other point has this property). This suggests that we should try $(x, y, z)^2$ as the corresponding primary ideal (this is (x, y, z)-primary as its radical is (x, y, z) and hence maximal).

So let us try to show that $I = (x, yz) \cap (x, y, z)^2$. Let $p \in (x, yz) \cap (x, y, z)^2$, then on the one hand we can write p as $p = x\alpha + yz\beta(y, z)$, where we can suppose that β only depends on y, z as we can put everything with an x into α. On the other hand, as p is a combination of $x^2, y^2, z^2, xy, yz, zx$, we can write it as $p = x^2a + xyb + xzc + yzd(y, z) + y^2e(y, z) + z^2f(y, z)$, where we can suppose that d, e, f only depend on y, z as we can put everything with xy resp. xz into b resp. c. Hence by evaluating at $x = 0$ we obtain $yz\beta(y, z) = yzd(y, z) + y^2e(y, z) + z^2f(y, z)$, so $p = x^2a + xyb + xzc + yz\beta(y, z)$. Hence $p \in I$.

Hence $I = (x, y) \cap (x, z) \cap (x, y, z)^2$ is a primary decomposition of I.

□

Exercise 6. Let $T \subseteq R$ be a multiplicative subset of a ring R and let $\{I_i\}_{1 \le i \le n}$ be finitely many ideals in R. By extension and contraction of ideals we shall mean extension and contraction via the natural morphism $R \to T^{-1}R$. Prove the following:

(1) $(\bigcap_i I_i)^{ec} = \bigcap_i I_i^{ec}$
(2) $(\bigcap_i I_i)^{e} = \bigcap_i I_i^{e}$
(3) Show that $T^{-1}(R/I) \cong T^{-1}R/I^e$ as R-modules. Use this to endow $T^{-1}(R/I)$ with a ring structure, so that it becomes in fact an isomorphism of rings.
(4) If I is primary, and $u \notin \sqrt{I}$, then $(I : u) = I$
(5) For an ideal I of a ring R admitting a finite primary decomposition, let $I = \bigcap_i I_i$ be such a primary decomposition, and show the following
   (i) $I^e = \bigcap_{T \cap I_i = \varnothing} I_i^e$,
   (ii) $I^{ec} = \bigcap_{T \cap I_i = \varnothing} I_i$

(6) From now on, let $R = F[x,y]$ for a field F, $I_1 = (x)$, $I_2 = \mathfrak{m}^s$ where $\mathfrak{m} = (x,y)$ and $s > 1$ is some integer, $I_3 = (x, y-1)^2$, and $\mathfrak{p} \subseteq R$ a prime ideal for which we set $T = R \setminus \mathfrak{p}$. Show that
   (i) if $\mathfrak{p} = (x)$, then $T^{-1}\left(R/I_1 \cap I_2 \cap I_3\right) \cong F(y)$.
   (ii) if $\mathfrak{p} = (x,y)$, then $T^{-1}\left(R/I_1 \cap I_2 \cap I_3\right) \cong T^{-1}R/I_1^e \cap I_2^e$
   (iii) if $\mathfrak{p} = (x,y)$, compute the smallest integer n such that $\left(\frac{x}{1}\right)^n \in T^{-1}\left(R/I_1 \cap I_2 \cap I_3\right)$ is zero.

Proof. (1) We have

$$\left(\bigcap_i I_i\right)^{ec} \overset{\text{Prop 9.3.8}}{=} \bigcup_{u\in T}\left(\left(\bigcap_i I_i\right) : u\right) \overset{\text{Prop 10.3.19}}{=} \bigcup_{u\in T}\left(\bigcap_i (I_i : u)\right).$$

Now we would like to swap the $\bigcup$ and the $\bigcap$. To this end, note that if $(u_i)_i$ is a sequence of elements of T, and $u := \prod_i u_i$, then

$$\bigcap_i (I_i : u_i) \subseteq \bigcap_i (I_i : u).$$

Hence

$$\bigcap_i \bigcup_{u\in T} (I_i : u) \subseteq \bigcup_{u\in T} \bigcap_i (I_i : u),$$

and as the reverse inclusion is elementary set theory we have

$$\left(\bigcap_i I_i\right)^{ec} = \bigcup_{u\in T}\left(\bigcap_i (I_i : u)\right) = \bigcap_i \bigcup_{u\in T} (I_i : u) \overset{\text{Prop 9.3.8}}{=} \bigcap_i I_i^{ec}.$$

(2) By Prop 9.3.8.(1), two ideals of $S^{-1}R$ are equal if and only if their contractions are equal. From the previous point we have

$$\left(\bigcap_i I_i\right)^{ec} \overset{(1)}{=} \bigcap_i I_i^{ec} = \left(\bigcap_i I_i^e\right)^c$$

where for the last equality we used that contraction (i.e. taking preimage) commutes with intersections. Hence it follows that $\left(\bigcap_i I_i\right)^e = \bigcap_i I_i^e$.

(3) The structure of $T^{-1}R/I^e$ as an R-module is given by $r \cdot (r'/t + I^e) = (rr')/t + I^e$. We have a natural morphism of R-modules $R \to T^{-1}R/I^e$ given by mapping $r \in R$ to $r/1 + I^e \in T^{-1}R/I^e$. This morphism has I in its kernel, so we obtain a morphism of R-modules $R/I \to T^{-1}R/I^e$. Notice that $T^{-1}R/I^e$ is T-invertible (see the solution of Exercise 5 on Exercise Sheet 11), and thus by the universal property of localization of a module we obtain an R-module homomorphism $\phi : T^{-1}(R/I) \to T^{-1}R/I^e$ given by mapping $(r+I)/t$ to $r/t + I^e$. This is clearly surjective, so to prove injectivity suppose that $(r+I)/t$ is mapped to 0. Then $r/t \in I^e$, and thus by the proof of point (2) of Proposition 9.3.8 there exist $r' \in I$ and $t' \in T$ such that $r/t = r'/t'$. Hence there exists $t'' \in T$ such that $t''(rt' - r't) = 0$. Hence we have $t''t'(r+I) = 0$ inside R/I, and

thus $(r+I)/t = 0$ inside $T^{-1}(R/I)$. Hence our map $\phi : T^{-1}(R/I) \to T^{-1}R/I^e$ is also injective. This endows $T^{-1}(R/I)$ with a natural ring structure by the formula

$$\frac{r+I}{t} \cdot \frac{r'+I}{t'} := \phi^{-1}\left(\phi\left(\frac{r+I}{t}\right)\phi\left(\frac{r'+I}{t'}\right)\right) = \phi^{-1}\left(\frac{rr'}{tt'} + I^e\right) = \frac{rr'+I}{tt'}.$$

With this ring structure, ϕ is tautologically a ring morphism.

(4) $t \in (I : u) \Rightarrow tu \in I \Rightarrow t \in I$, where in the last implication we used that no power of u is in I.

(5) Let $I = \cap I_i$ be such a primary decomposition.

(i) From point (2) we have $I^e = \bigcap I_i^e$, but for I_i intersecting T non-trivially we have $I_i^e = S^{-1}R$. Hence $I^e = \bigcap_{T\cap I_i=\varnothing} I_i^e$.

(ii) Since $(S^{-1}R)^c = R$ it follows from taking the contraction of the identity of point (2) that $I^{ec} = \bigcap_{T\cap I_i=\varnothing} I_i^{ec}$. Now for an ideal I_i with $T \cap I_i = \varnothing$, notice that as T is multiplicatively closed we also have $T \cap \sqrt{I_i} = \varnothing$. Hence it follows that

$$I_i^{ec} \overset{\text{Prop.9.3.8}}{=} \bigcup_{u\in T}(I_i : u) \overset{(4)}{=} \bigcup_{u\in T} I_i = I_i.$$

So $I^{ec} = \bigcap_{T\cap I_i=\varnothing} I_i$.

(6) Note that I_i is primary for all i, as I_1 is prime, and $\sqrt{I_2} = (x, y)$ and $\sqrt{I_3} = (x, y-1)$ are maximal. Let $I = I_1 \cap I_2 \cap I_3$. We start with the following lemma.

Lemma 1. *Let R be a ring, $T \subseteq R$ a multiplicative subset and $I \subseteq R$ an ideal. Let $\tilde{T} := \{t + I \mid t \in T\} \subseteq R/I$. Then $T^{-1}(R/I) \cong \tilde{T}^{-1}(R/I)$ as rings, where the ring structure on $T^{-1}(R/I)$ is given by point (3).*

Proof. It is straightforward to see that the localisation map of R-modules $R/I \to T^{-1}(R/I)$ is a ring morphism for the ring structure on $T^{-1}(R/I)$ given by point (3). Furthermore, $t + I \in \tilde{T}$ is mapped to $(t+I)/1$, which is a unit with inverse $(1+I)/t$. Hence by the universal property of localisation there exists a ring morphism $\tilde{T}^{-1}(R/I) \to T^{-1}(R/I)$ mapping $(r+I)/(t+I)$ to $(r+I)/t$. This is clearly surjective. To prove that it is injective, let $(r+I)/(t+I)$ be in the kernel, i.e. there exists $t' \in T$ such that $t'(r+I) = 0$. But then $(t'+I)(r+I) = 0$, so $(r+I)/(t+I) = 0$ as well. Hence $\tilde{T}^{-1}(R/I) \to T^{-1}(R/I)$ is an isomorphism. □

(i) By the previous point we have $I^e = \bigcap_{I_i\subseteq\mathfrak{p}} I_i^e$. As I_1 is the only ideal contained in $\mathfrak{p}$ we hence have $I^e = I_1^e = (x)^e$. Therefore, by point (3) we have

$$T^{-1}(R/I) \overset{(3)}{\cong} T^{-1}R/I^e = T^{-1}R/I_1^e \overset{(3)}{\cong} T^{-1}(R/(x)) \overset{\text{Lemma 1}}{\cong} \tilde{T}^{-1}(R/(x))$$

Now notice that $\tilde{T} = \{p + (x) \mid p \notin (x)\} = \{p(y) + (x) \mid p(y) \in F[y] \setminus \{0\}\}$. So under the identification $F[x,y]/(x) = F[y]$ we have $\tilde{T} = F[y] \setminus \{0\}$ and thus $\tilde{T}^{-1}(R/I_1) \cong F(y)$.

(ii) Note that I_3 is not contained in $\mathfrak{p}$, while I_1 and I_2 are. Hence by points (5) and (3) we have

$$T^{-1}(R/I) \overset{(3)}{\cong} T^{-1}R/I^e \overset{(5)}{=} T^{-1}R/I_1^e \cap I_2^e.$$

(iii) Under the isomorphism of the previous point, $(x+I)/1$ is mapped to $x/1+I_1^e \cap I_2^e$. So we need to compute the smalles integer $n > 0$ such that $x^n/1 \in I_1^e$ and $x^n/1 \in I_2^e$. Or equivalently, the smallest integer $n > 0$ such that $x^n \in I_1^{ec}$ and $x^n \in I_2^{ec}$. But by the argument in point (5).(ii) we have $I_1^{ec} = I_1$ and $I_2^{ec} = I_2$, so we need to find the smallest integer n with $x^n \in I_1$ and $x^n \in I_2$. Clearly $n = s$ works, and if $x^n \in I_2$ we must have $n \geq s$ as every non-zero element of I_2 has degree at least s. Hence $n = s$ is the minimal integer with the searched property.

□