RINGS AND MODULES 2020
SHEET 1 SOLUTIONS

Joe Waldron, Emelie Arvidsson, Maciek Zdanowicz
emelie.arvidsson@epfl.ch

Exercise 1. Let $R = k[x, y]$. We make $N = R \oplus R$ into a two-sided R-module via $f \cdot (p, q) = (fp, fq)$ (direct sum of R with itself).

(1) Let M be the submodule generated by the element $(x, y) \in R \oplus R$. Is $N/M \cong R$ as R-modules? Hint: R is a free R-module.
(2) Now let M be the submodule generated by the two elements $(x, 0)$ and $(0, y)$ of $R \oplus R$. Is $N/M \cong R$? Hint: Torsion

Proof. (1) R is a free R-module with one generator, so we are done if we show that N/M cannot be generated by one element. Suppose on the contrary that there is an element $(r_1, r_2) + M$ which generates N/M. We will show that (r_1, r_2) has to be equal to (xs_1, ys_2) for some $s_1, s_2 \in R$. This will give a contradiction since otherwise we could write $(1, 1) = j \cdot (xs_1, ys_2) + (xp, yp)$ in $R \oplus R$, which is clearly impossible since neither x nor y is a unit of R. In order to prove that (r_1, r_2) is equal to $(xs_1, ys_2) + M$ for some $s_1, s_2 \in R$ we will use the fact that R is a unique factorization domain. Assume that $(r_1, r_2) + M$ generates N/M, then in particular there are polynomials g, h, p and q in $k[x, y]$ such that

$$(y, 0) = g \cdot (r_1, r_2) + (xp, yp)$$
$$(0, x) = h \cdot (r_1, r_2) + (xq, yq)$$

Then we have

(Eq. 1) $$gr_1 + px = y \quad hr_2 + qy = x$$
(Eq. 2) $$gr_2 + py = 0 \quad hr_1 + qx = 0$$

From (Eq. 2) we see that y divides gr_2. In order to derive a contradiction assume that y does not divide r_2, then y necessarily divides g. Inspection of the first equation (Eq. 1) then tells us that y in fact most divide p. However, this implies (by (Eq. 2)) that y^2 divides g. This in particular means that y^2 divides $y - px$, but this is impossible. We therefore conclude that y divides r_2. The same argument applied to the equations involving h shows that x divides r_1.

(2) The element $(y, 0)$ represents a non-zero class in N/M. However, $x \cdot (y, 0) = (xy, 0)$ is in M. But R is an integral domain, so in particular there is no $f \in R$ such that $f \cdot x = 0$.

□

Exercise 2. Recall that a R-module M is *simple* if the only submodules $N \subset M$ are $N = 0$ and $N = M$.

(1) Show that any simple left R-module M is *cyclic*, i.e., isomorphic to the R-module Rm defined in the lecture, for some $m \in M$.
(2) Let M be a left R-module and let $m \in M$ be an element of M. Define $\mathcal{A}nn(m) \subset R$ to be the set of elements $r \in R$ such that $rm = 0$. Show that $\mathcal{A}nn(m)$ is a left ideal of R and that the cyclic left R-module Rm is isomorphic to the left R-module $R/\mathcal{A}nn(m)$.
Hint: Prove both statements by defining a morphism of R-modules $R \to Rm$ and investigate its kernel.
(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 $M = R0$ and the assertion is true. Hence assume that $M \neq 0$. Let $m \neq 0 \in M$, 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 $\Phi_m : R \to Rm$ by $\Phi_m(r) = rm$. The kernel of Φ_m is by definition the elements $r \in R$ such that $rm = 0$, i.e., $ker(\Phi_m) = \mathcal{A}nn(m)$. This proves that $\mathcal{A}nn(m)$ is a left ideal of R and that $Rm \cong R/\mathcal{A}nn(m)$.
(3) By 2 M is isomorphisc to $k[x]/\mathcal{A}nn(m)$ for some $m \in M$. Let $\mathcal{A}nn(m) = (f)$, we need to prove that f is irreducible. To this end let g divide f, $k[x]g+(f)$ is a left $k[x]$-submodule of $k[x]/(f)$, since by assumption $M = k[x]/(f)$ is simple we must have that $g \in (f)$ or $g = 1$, in particular f is irreducible.
(4) Notice that if R is a ring, then R has no proper nontrivial left ideals if and only if R is simple as a left R-modulue (by definition). In all of these examples $R = \mathbb{Z}$ is a commutative ring so the question reduces to finding proper non-trivial 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 $\mathcal{A}nn(m)$ is a left ideal of R. Give an example to show that $\mathcal{A}nn(m)$ might *not* be a two sided ideal of R.
(2) Define $\mathcal{A}nn(M)$ to the set of elements $r \in R$ such that $rm = 0$ for *all* $m \in M$. Prove that $\mathcal{A}nn(M)$ is a two sided ideal of R.

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 $a \neq 0 \in k$, we will calculate the annihilator of $m_a = \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}$

I.e., we are interested in solving the matrix equation

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

The solution is hence $b_{11} = b_{21} = 0$. Therefore $\mathcal{A}nn(\begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}) = \begin{bmatrix} 0 & b \\ 0 & c \end{bmatrix}$ where $b, c \in k$. 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 $b_{11} = b$, which is non-zero whenever b is.

(2) Let $r, s \in \mathcal{A}nn(M)$ and $l \in R$. Then $l(r+s)m = lrm + lsm = 0$ and $(r+s)lm = rlm + slm = 0$.

□

Exercise 4. Let k be an algebraically closed field. In this exercise we define a non-commutative ring $\mathcal{D}(k[x]/k)$ of *differential operators* on $k[x]$ over k. The non-commutative ring $\mathcal{D}(k[x]/k)$ is a sub k-algebra (which we will abbreviate as $\mathcal{D}$) of $\mathrm{Hom}_k(k[x], k[x])$ generated by the element ∂ and x where ∂ sends a polynomial $p(x)$ to its algebraic derivative with respect to x and the element $x \in \mathrm{Hom}_k(k[x], k[x])$ is multiplication by x.

(a) Show that the following relation hold in $\mathcal{D}$: for any polynomial $P(x) \in k[x]$,

$$\partial P(x) = \frac{\partial}{\partial x} P(x) + P(x)\partial.$$

where $\frac{\partial}{\partial x} P(x)$ denotes the formal derivative of $P(x)$ with respect to the variable x. [*Hint*: Prove it by induction on the degree of P(x) and use linearity.]

(b) Show that a basis of $\mathcal{D}$ as a k-vector space is given by the elements $x^i \partial^j$, where $(i, j) \in (\mathbb{Z}_{\geq 0})^2$ if the characteristic of k is zero and $i \in \mathbb{Z}$ and $j \in \{0, 1, \ldots, p-1\}$ if the characteristic of k is $p > 0$.
[*Hint*: Use part (a) to show that an element of the form $\partial^k x^s$ can be written in terms of the proposed basis.]

(c) Now we consider a quotient of the free k-algebra on two generators. $\mathcal{D}^{form} = k\langle u, v\rangle/(uv - vu - 1)$. Show that there is a well defined ring homomorphism $\phi\colon \mathcal{D}^{form} \to End_k(k[x])$ sending $u \to \partial$ and $v \to x$. Show that ϕ is surjective onto $\mathcal{D}$ and prove that ϕ defines an isomorphism between $\mathcal{D}$ and $\mathcal{D}^{form}$ if and only if the characteristic of k is zero.

(d) 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 k has characteristic zero

(e) Show that $\mathcal{D}$ has no two sided non-trivial ideals if k has characteristic zero. I.e., show that $\mathcal{D}$ is simple.

(f) Now suppose the characteristic of k is 2. Determine the left submodules of $k[x]$ as a $\mathcal{D}$-module in this case.

Proof. (a) It is sufficient to show that the formula holds for monomials x^n since all quantities involved are k-linear. For $n = 1$ this amounts to the given relation

$[X, \partial] = -1$. We want to show that

$$\partial x^n = nx^{n-1} + x^n\partial.$$

for $n \geq 2$. We proceed by induction: $\partial x^n = ((n-1)x^{n-2} + x^{n-1}\partial)x = nx^{n-1} + x^n\partial$.

(b) By construction, $\mathcal{D}$ is the k-span of all elements of the form $x^i\partial^j$ and $\partial^j x^i$ for $i, j \geq 0$. By successive application of part (a) all elements $\partial^k x^s$ lies in the k- span of $x^i\partial^j$ for $i, j \geq 0$. Since the elements $x^i\partial^j$ obviously are linearly independent over k the result follows.

(c) We need to check that the assignment $\phi\colon \mathcal{D}^{form} \to End_k(k[x])$ sending $u \to \partial$ and $v \to x$ is well-defined. This amount to $\partial x - x\partial - id$ being the zero endomorphism of $k[x]$. I.e., for all $f \in k[x]$ we have $\frac{\partial}{\partial_x}(xf) = f + x\frac{\partial}{\partial_x}(f)$, but this was proven in (a). By the previous exercise, ϕ is surjective since it is surjective onto a k-basis. We now assume that the characteristic of k is zero. Suppose that $a = \sum_{j=0}^n f_j\partial^j \in ker(\phi)$. Let m be minimal such that $f_j \in k[x]$ is non-zero. Then $\phi(a)(x^m) = \sum_{j=0}^n f_j \frac{\partial}{\partial_x}^j(x^m) = m!f_j(x) \neq 0$. A contradiction unless $a = 0$.
Now subbose that the characteristic of k is $p > 0$. We have $(\frac{\partial}{\partial x})^p = 0$. Therefore, the kernel of ϕ is non-trivial, containing u^p.

(d) 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 $f \in k[x]$, $(f(x)1_{\mathcal{D}})(1) = f(x)$. Now suppose N is a non-zero submodule of $k[x]$. We will show that $1 \in N$. As N is non-zero, it contains some non-zero element $f(x) = \sum_i^n a_i x^i$. We need to find a differential operator D such that $D(f) = 1$. $D = \frac{1}{a_n n!}(\frac{\partial}{\partial x})^n$ will do it.

(e) We will show that $\mathcal{D}$ has no two sided ideal. Assume on the contrary that I is a two sided ideal of $\mathcal{D}$. For any $a \in I$, write $a = \sum_{i=0}^n p_i(\frac{\partial}{\partial x})^i$ for $p_i \in k[x]$ such that $p_n \neq 0$, define the degree of a to be n. Suppose that I contains an element a of degree 0, i.e $a = p(x)1_{\mathcal{D}}$. If the degree of the polynomial $p(x)$ is d and the leading coefficient is a_d then $\frac{1}{a_d d!}(\frac{\partial}{\partial x})^d p(x) = 1$. Hence we are done if we can prove that I contains an element a of degree 0. Assume that I contains no element of degree 0 and let $b \in I$ be of minimal degree $m > 0$. That is, $b = \sum_{i=0}^m p_i(\frac{\partial}{\partial x})^i$ for $p_i \in k[x]$ and $p_m \neq 0$.

Write $\frac{\partial}{\partial x}x = (\frac{\partial}{\partial x}) \circ (x1_{\mathcal{D}})$. Then $\frac{\partial}{\partial x}x(f) = \frac{\partial}{\partial x}(xf) = f + x\frac{\partial}{\partial x}(f)$. Similarly calculate

$$(\frac{\partial}{\partial x})^i x = (\frac{\partial}{\partial x})^{i-1} + (\frac{\partial}{\partial x})^{i-1}x\frac{\partial}{\partial x} = ... = i(\frac{\partial}{\partial x})^{i-1} + x(\frac{\partial}{\partial x})^i$$

i.e.

$$((\frac{\partial}{\partial x})^i x - x(\frac{\partial}{\partial x})^i) = i(\frac{\partial}{\partial x})^{i-1}$$

But then $(bx - xb)$ has strictly less degree then b, which contradicts the minimality of m. Hence I contains an element of degree 0.

(f) The first thing to note is that

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

Similarly $\frac{\partial}{\partial x}(x^{2n}) = 0$ any $n \in \mathbb{N}$. Suppose that N is a non-zero submodule of $k[x]$, which contains $0 \neq f(x) = \sum_1^n a_i x^i$. For convenience, record polynomials as row vectors of coefficients, for instance

$$f = (a_0, a_1, a_2, a_3, ..., a_n)$$

Now we show that N is generated by its set of elements of the form $(b_0, 0, b_2, 0, ...)$. Suppose $f = (a_0, a_1, ..., a_n) \in N$. Then:

$$g := \frac{\partial}{\partial x}(f) = (a_1, 0, a_3, 0, a_5, ...)$$
$$xg = (0, a_1, 0, a_3, 0, a_5, ...)$$
$$h := f - xg = (a_0, 0, a_2, 0, a_4, ...)$$
$$f = xg + h$$

Next we claim that N is generated by a single element of this form. The ring $\mathcal{D}$ contains a copy of $k[x]$ as a subring, and the induced $k[x]$-module structure on $k[x]$ is the natural one. 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. Therefore f also generates $k[x]$ as a $\mathcal{D}$-module.

Finally, each monic polynomial of this form generates a different submodule, for it is the unique monic polynomial of least degree in $\mathcal{D}(f)$.

□

Exercise 5. Let

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

be a short exact sequence of modules over a ring R. 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, assume that N is finitely generated. Then N/M is finitely generated.
(3) Assume that N is finitely generated. Then M is finitely generated.

Proof. (1) As M is finitely generated, we can find a subset $\{m_i\}_{i=1}^k \subset M$ such that any $m \in M$ can be written as $m = \sum_{i=1}^k r_i m_i$ for some (possibly non-unique) $r_i \in R$. Similarly we can find a subset $\{\overline{n}_i\}_{i=1}^l \subset N/M$ such that any $\overline{n} \in N/M$ can be written as $\sum_{i=1}^l \overline{r}_i \overline{n}_i$ for some $\overline{r}_i \in R$. For $i = 1, ..., l$, choose $n_i \in N$ such that $\overline{n}_i = n_i + M$.

We claim that N is generated by $\{m_1, ..., m_k, n_1, ..., n_l\}$. Given $n \in N$, we can write $n + M = \sum_{i=1}^l \overline{r}_i (n_i + M)$ for some $\overline{r}_i \in R$, and so $n - \sum_{i+1}^l \overline{r}_i n_i \in M$. But then there exist $r_i \in R$ such that $n - \sum_{i+1}^l \overline{r}_i n_i = \sum_{i=1}^k r_i m_i$. This exhibits n as a linear combination of the m_i and n_i and so N is generated by these elements.

(2) The statement is true. Suppose $\{n_i\}_{i=1}^k$ generate N. Then $\{\overline{n}_i = n_i + M\}$ generates N/M, because any $\overline{n} \in N/M$ can be written as $n + M$ for some $n \in N$ which can then be written as

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

(3) This statement is not true. Take $R = \mathbb{C}[x_1, x_2, ...]$, the polynomial ring in infinitely many variables. (An element of R is by definition a polynomial in finitely many of the variables $x_1, x_2, ...$)

Let N be R viewed as a module over itself, and take the submodule M to be generated by $\{x_1, x_2, ...\}$. This is a proper submodule, as it does not contain the constants $\mathbb{C} \subset N$. Any element of M is a polynomial $f(x_1, ..., x_i)$ 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, Z, and $k[x_1, ..., x_n]$. So $\mathbb{C}[x_1, x_2, ...]$ 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 modules over a ring R.
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 of the form $\bigoplus_I R$ for some (possibly infinite) indexing set I.

Digression:

Definition 6.1. *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 6.2. *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 $M = 2 \cdot \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2Z$. This has too few elements to be a free $\mathbb{Z}/4\mathbb{Z}$-module.
- This is true. Suppose M has basis $\{m_i\}$ and N/M has basis $\{n_j + M\}$. We claim that $\{m_i, n_j\}$ are a basis for N. They span: given $n \in N$ we can write $n+M = \sum r_j(n_j+M)$ for some $r_j \in R$. Then $n-\sum r_j n_j \in M$, which means we can write $n - \sum r_j n_j = \sum r_i' m_i$ for some $r_i' \in R$. This shows spanning. For linear independence: suppose $\sum r_j n_j + \sum r_i' m_i = 0$. This implies $\sum r_j(n_j + M) = 0$ in N/M and so the r_j are all zero by the linear independence of the $n_j + M$. But then $\sum r_i' m_i = 0$ is a linear dependence among a basis of M, forcing the r_i' to be zero as well.

(2)
- $\mathbb{Z}[x]/(x^2+1)\mathbb{Z}[x]$ is a free $\mathbb{Z}$-module, with basis $\{1, x\}$.
- $\mathbb{Z}[x]/(2x^2)\mathbb{Z}[x]$ is not free since x^n is a torsion element for all $n \geq 2$.
- $\mathbb{Q}$ is not a free $\mathbb{Z}$ module. For suppose it were free, and had basis $\{\frac{p_i}{q_i}\}$. Then by spanning, we can write $\frac{p_1}{2q_1} = \sum_{i=1}^{n} \frac{p_i}{q_i}$. There must be some non-zero term on the right hand side, so by multiplying the equation by 2, we get a non-trivial linear dependence. (Non-trivial because the multiple of $\frac{p_1}{q_1}$ on the right hand side is even). It is not finitely generated since if $\{\frac{p_i}{q_i}\}_{1 \leq i \leq n}$ is a generating set, let $q = q_1 \times \cdots \times q_n$ then $\frac{1}{q+1}$ does not lie in the $\mathbb{Z}$-span of $\{\frac{p_i}{q_i}\}_{1 \leq i \leq n}$.

□

RINGS AND MODULES 2020- PROBLEM SHEET 2

There was one exercise in this problem sheet that was part of the second homework. The exercise was denoted by the symbol ** next to the exercise number.

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 an Artinian ring. Is every prime ideal of R maximal?

Proof. (a) 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).

(b) 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 ideal (x^n) is decreasing and hence 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 $x^n(1 - ux) = 0$, we have $ux = 1$ which proves that x is invertible, and hence $R/\mathfrak{p}$ is a field and therefore $\mathfrak{p}$ is maximal.

□

Exercise 2. Let R be the ring of 2×2 matrices $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ such that $a \in \mathbb{Z}$ and $b, c \in \mathbb{Q}$.

(1) For each $n \in \mathbb{N}$ define $I_n = \left\{ \begin{pmatrix} 0 & \frac{m}{2^n} \\ 0 & 0 \end{pmatrix} | m \in \mathbb{Z} \right\}$. Verify that each I_n is a left ideal of R, and using the chain $I_1 \subset I_2 \subset \ldots$ verify that R is not left Noetherian.
(2) Show that every right ideal of R is finitely generated, and deduce that R is right-Noetherian.

Proof. (a) To show that I_n is a left ideal, first note that it is an additive subgroup, for it is closed under addition, inverses and contains 0. It is also closed under left multiplication by elements of R because

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} 0 & \frac{m}{2^n} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & \frac{am}{2^n} \\ 0 & 0 \end{pmatrix}$$

because $a \in \mathbb{Z}$.

So each I_n is a left ideal of R, and $I_n \subset I_{n+1}$ holds because $\frac{m}{2^n} = \frac{2m}{2^{n+1}}$. Therefore R is not left Noetherian.

(b) To determine the right ideals of R, first write down the result of multiplying two general elements.

$$\begin{pmatrix} l & m \\ 0 & n \end{pmatrix}\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} al & bl + cm \\ 0 & cn \end{pmatrix}$$

Here the first matrix is in the module, the second in the ring. Remember that $a, l \in \mathbb{Z}$, $m, n, b, c \in \mathbb{Q}$. Let I be a right ideal. Notice that $\left\{ l : \begin{pmatrix} l & m \\ 0 & n \end{pmatrix} \in I \right\}$ forms an ideal of $\mathbb{Z}$, which is principally generated by some fixed L.

Suppose $L \neq 0$ and choose

$$\begin{pmatrix} L & m \\ 0 & n \end{pmatrix} \in I$$

first assuming we can take m and n to be non-zero. Then there is a choice of b and c which make $bL + cm$ and cn equal to any pair of rational numbers, while choosing $a = 1$ to preserve L. Notice also that any integer multiple of a matrix in I is in I. Therefore any matrix of the form

$$\begin{pmatrix} kL & m \\ 0 & n \end{pmatrix}$$

is in I, and this must be all of I (as there is nothing else we can add by choice of L).

Continuing to assume that $L \neq 0$, we are left with the cases where either $n = 0$ for all elements of I or $m = 0$ for all elements of I. In either case, we can show that all potential elements of I can be generated by a single element, and so these ideals are principal.

Finally we now assume that $L = 0$, so I consists of only matrices with zero top left entry. In this case, given

$$\begin{pmatrix} 0 & m \\ 0 & n \end{pmatrix} \in I$$

we see that

$$\begin{pmatrix} 0 & cm \\ 0 & cn \end{pmatrix} \in I$$

for each $c \in \mathbb{Q}$. This means the ideal is generated by at most two elements. In fact it is principal unless it contains both

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

in which case it is generated by these.

Therefore R is right-Noetherian.

□

Exercise 3. 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 each $n \in \mathbb{N}$, let $I_n := \{a_n : \sum_{i=n}^{\infty} a_i x^i \in I\}$. Then adapt the proof of the Hilbert basis theorem.
(4) $C^1(\mathbb{R})$, the ring of continuous functions $\mathbb{R} \to \mathbb{R}$ with pointwise operations.
(5) $\mathbb{R}[x]/(x-1)^2 x\mathbb{R}[x]$.

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 using Question 2 and the Hilbert basis theorem.

The isomorphism in question comes from the ring homomorphism:

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

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 $R[x, \frac{1}{x}] \cong R[u, v]/I$.

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 $g_2 = \sum a_i u^i + \sum b_j v^j$ 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 Notherianian ring. There is an infinite descending chain of ideals in $R[x, x^{-1}]$ given by $(x+1) \supsetneq ((x+1)^2) \supseteq ((x+1)^3) \supseteq ....$ We need to prove that the containment is strict. To this end suppose that there exists an $k > 0$ 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 $f(x, x^{-1}) = \sum_{i=-1}^{-m} a_i x^i + \sum_{i=0}^{n} a_i x^i$. Let $i \geq 0$ be maximal such that $a_i \neq 0$, then there is a non-zero term of degree $k+i+1$ on the righthandside corresponding to $a_i x^{k+i+1}$. This is not possible, since the lefthand side only has terms of degree less than or equal to k. Therefore, $a_i = 0$ for all $i \geq 0$. Let $i < 0$ be minimal such that $a_i \neq 0$, then there is a non-zero term of degree i on the righthand side corresponding to $a_i x^i$. This is not possible, since the lefthand 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 in the degrees k and 0 corresponding to the terms x^k and 1.

(2) $R[x_1, x_2, ...]$ is not Noetherian, as the ideal $(x_1, x_2, ...)$ cannot be finitely generated. See solution to Sheet 2 Q1(c). It is not Artinian (for any choice of $R \neq 0$), since it contains $R[x]$ as a subring and hence the descending chain $(x) \supsetneq (x^2) \supsetneq (x^3) \supsetneq \dots$

(3) $R[[x]]$ is not Artinian (for any choice of $R \neq 0$), since it contains $R[x]$ as a subring and hence the descending chain $(x) \supsetneq (x^2) \supsetneq (x^3) \supsetneq \dots$.

$R[[x]]$ 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, let

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

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 N such that $I_n = I_{n+1}$ for all $n \geq N$.

Also, for each $i \leq N$, I_i is finitely generated, so we may fix a finite set $\{a_{i,j_i}\}_{j_i}$ of generators for I_i. For each (i, j_i), fix $f_{i,j_i} \in R[[x]]$ such that

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

We claim that $\{f_{i,j_i}\}$ generate I. Let $g = \sum_{k=n_0}^{\infty} b_k x^k \in I$. If $k < N$, we can find $r_{j_{n_0}} \in R$ such that $g - r_{j_{n_0}} f_{n_0,j_{n_0}}$ has lowest order term of degree $n_0 + 1$. Repeating this finitely many times we may assume g has lowest degree at least N. Finally, suppose g has lowest degree $n_0 > n$. Then we can write it as $g = \sum_{j_N} x^{n_0-N} f_{N,j_N} + g'$ where g' had lowest degree greater than n_0. By induction this allows us to write $g = \sum h_{N,i_N} g_{N,i_N}$ where the h_{N,i_N} are some power series. Thus we see that the $\{f_{i,j_i}\}$ indeed generate I.

(4) $C^1(\mathbb{R})$ is neighter Artinian nor Noetherian. It is not Artinian since it contains $\mathbb{R}[x]$ as a subring and hence the descending chain $(x) \supsetneq (x^2) \supsetneq (x^3) \supsetneq \dots$. We will show that it is not Noetherian.

To this end define $I_n = \{f \in C(\mathbb{R}) : f(x) = 0 \text{ for all } x \geq n\}$ 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 continous 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 continous function $f \in I_{n+1} - I_n$.

(5) The ring is clearly noetherian and artinian because all its ideals are $\mathbb{R}$ vector spaces of dimension smaller than the dimension of the rings itself equal to two.

□

Exercise 4. **Show that the following holds for a R-modulue M of finite length $l(M)$ (i.e., an R-modulue M that admits a composition series of finite length)

(1) If there is a short exact sequence:

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

then $l(M) = l(M') + l(M'')$.

(2) If $N \subset M$ 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 necessary a composition series) has length $\leq l(M)$. Conclude that a module M is of finite length if and only if M is both Notherian and Artinian

Proof. (1) 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 $l(M') + l(M'')$, since

by the Jordan Holder Theorem $l(M)$ is the length of *any* composition series $l(M') + l(M'') = l(M)$. It is therefore sufficient to show that M' and M'' are both of finite length when M is. In order to do so we note that we do not use this exercise in the solution of subsequent exercises. Therefore we may use the conclusion of the subsequent exercises, i.e., that M is Noetherian and Artinian, therefore so is M' and M''.

(2) Suppose that $N \subset M$ is a proper submodule. Let (M_i) be a composition series of M and consider the submodules $N_i = M_i \cap N$ of N. Since N_i/N_{i-1} is a submodule of M_i/M_{i-1} and the latter is a simple module, we have either $N_i/N_{i-1} = M_i/M_{i-1}$ or $N_i = N_{i-1}$. Therefore, removing repeated terms, we have a composition series of N, so that $l(N) \leq l(M)$. If $l(N) = l(M) = n$, then this means that $N_i/N_{i-1} = M_i/M_{i-1}$ for all $i \in \{1, 2, \ldots, n\}$. In particular $N_1 = M_1$, and so $N_2 = M_2$, and so on until $M = N$. This is a contradiction to N being a proper submodule of M.

then $l(N) < l(M)$.

(3) Let $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ 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.

□

Exercise 5. Let R be a ring. Let M be a finitely generated module over R and let $f : M \to M$ be an R-module homomorphism.

(1) Suppose that R is a Noetherian ring.
   (a) Does injectivity of f implies surjectivity?
   (b) Does surjectivity of f implies injectivity?
   (c) What happens if R is not necessarily Noetherian?

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

Proof. (1) (a) 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 $m_a : R \to R$.

(b) Suppose that M is a finitely generated module over a Noetherian ring, then M is Noetherian. Let $f : M \to M$ be 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, $f : Im(f^m) \to M$ is injective, but by surjectivity $Im(f^m) = M$, therefore f is injective.

(c) 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 morphism. 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 $e_i = f(\sum_k b_{ik} e_k)$. By construction the element $m \in Ker(f')$ which by the discussion in the previous exercise is zero. This implies that $m = 0$.

(2) Consider the short exact sequence

$$0 \longrightarrow \mathrm{Ker}(f) \longrightarrow M \longrightarrow \mathrm{Im}(f) \longrightarrow 0 \ .$$

By Exercise 4, we have $l(M) = l(\mathrm{Ker}(f)) + l(\mathrm{Im}(f))$. Since the zero module is the only module of length zero, f is surjective implies that $\mathrm{Ker}(f) = 0$. Conversely, if f is injective $l(M) = l(\mathrm{Im}(f))$, hence $l(\mathrm{Im}(f))$ can not be a proper submodule of M by the same exercise, i.e., $M = \mathrm{Im}(f)$.

□

Exercise 6. This exercise is about *semi-simple* modules.

Definition 6.1. *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 some $M_i \leq_R M$ simple. I.e., prove that if $M = \sum_{i=1}^{d} M_i$ where $d \in \mathbb{N}$ is minimal with this property, then $M_i \cap M_j = 0$ for all $i \neq j$.

(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.

(a) For any ring R and 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 $\phi \in Hom_R(M, N)$ such that $\phi(n) = n$ for all $n \in N$. *Hint: Use the universal property of direct sums*

(b) Let M be any $k[G]$-module which has finite dimension over k. Show that for any submodule N there exists an element

$\phi \in Hom_{k[G]}(M,N)$ such that $\phi(n) = n$. *Hint: Take* $\xi \in Hom_k(M,N)$ *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.*

(c) Conclude the proof.

Proof. (1) The $\Leftarrow$ direction is immediate from Definition 6.1. So, we prove direction $\Rightarrow$.

Let us start with an arbitrary finite collection of simple submodules M_i of M (given by 6.1), 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 some $1 \leq j \leq i$, $M_j \cap \sum_{i\neq j} M_j = 0$. If this is the case, we are ready, so we may assume the contrary. By reindexing, we may assume then that $M_1 \cap \sum_{i=2}^d M_i \neq 0$. 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:

(a) We will show that $M = \mathrm{Ker}(\phi) \oplus N$. To this end let $i_N : N \hookrightarrow M$ and $i_{\mathrm{Ker}(\phi)} : \mathrm{Ker}(\phi) \hookrightarrow M$ denote the inclusion of the two submodules. By the universal property of direct sums there exists a unique morphism $i_{\mathrm{Ker}(\phi)} + i_N = \psi : \mathrm{Ker}(\phi) \oplus N \to M$, it is injective since $N \cap \mathrm{Ker}(\phi) = 0$. We show that ψ is surjective. Let $m \in M$, let $\phi(m) = n$, we have $m - n \in \mathrm{Ker}(\phi)$, say $m - n = l$. Hence $m = \psi(l, n)$ where $l \in \mathrm{Ker}(\phi)$ and $n \in N$.

(b) 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 M,

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

We claim that ϕ is as desired. Indeed, if $x \in N$, then $g^{-1}x \in N$, and hence $\xi(g^{-1}x) = g^{-1}x$. 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, since it is k-linear, so only the compatibility with $g \in G$ has to be shown, which is done by the next computation (here $h \in G$ arbitrary):

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

(c) 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.

□

RINGS AND MODULES 2020 - SOLUTIONS PROBLEM SHEET 3

Exercise 1. Make 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 the presentation $\mathbb{Z}^3 \to M$ by $e_1 \mapsto (2,9)$, $e_2 \mapsto (4,3)$, $e_3 \mapsto (6,8)$. We calculate a presentation 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
$$\mathbb{Z} \to \mathbb{Z}^3 \to M$$
where the first map is $t \mapsto (-7t, -19t, 15t)$

(2) We define a presentation $R^2 \to M$ 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 a presentation 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 $(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix})$ such that $a = -\beta$, $c = -\delta$, $\alpha = \gamma = 0$. I.e., the elements of the form
$$(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} 0 & -a \\ 0 & -c \end{pmatrix}).$$

A presentation of the kernel is hence given by $R \to R^2$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix})$$

□

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) Write down the invariant factor decomposition of the $\mathbb{Z}$-module with generators e_1, e_2, e_3, e_4 and relations

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

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) In terms of the generators $e_1, \dots, e_4$ 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

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

To give the invariant factor decomposition, we want to change the presentation of M, that is change the given set of generators and relations to new ones of the required simpler form. This is done by changing the bases of $\mathbb{Z}^3$ and $\mathbb{Z}^4$ so that the matrix of K is in Smith normal form with respect to the new basis. As we saw, the Smith normal form is

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

This produces a new set of generators f_1, f_2, f_3 and f_4 for M which satisfy relations $f_1 = 0$, $2f_2 = 0$ and $26f_3 = 0$. Thus

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

□

Exercise 3. ** Let $R = \mathbb{Q}[x]$. Determine the invariant factor decomposition of the R-module M with generators e_1, e_2 and relations

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

. In particular prove that M is isomorphic to a quotient of R.

Proof. As before, we get a homomorphism $R^2 \to M$ with kernel K, where the inclusion $K \to M$ is given 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:

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

□

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 the example is given by $\mathbb{Q}$ as a $\mathbb{Z}$-module. Indeed, assume for sake the of contradiction that $\mathbb{Q} \cong \bigoplus \mathbb{Z} \oplus \bigoplus \mathbb{Z}/n_i$ for $n_i \geq 2$. 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.

□

Exercise 5.
(1) Find a 2×2 matrix with coefficients in $\mathbb{Z}[X]$ that 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) Find also a finitely generated module over $\mathbb{Z}[X]$ that is not isomorphic to a direct sum of cyclic modules.

Proof. (1) Let $A = \begin{pmatrix} 2 & x \\ 0 & 0 \end{pmatrix}$, 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 $det(A') = 0$ and therefore $\lambda_i = 0$ for $i = 1$ or $i = 2$. Assume that $\lambda_2 = 0$ (the case $\lambda_1 = 0$ can be treated in the same way). Then there exists invertable 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 $det(T) = t_{11}t_{22} - t_{12}t_{21} = 2t't_{22} - xt't_{21} = \pm 1$ this implies that the ideal $(2, x)$ contains 1, a contradiction.

(2) Let M be the cokernel of $A : \mathbb{Z}[x]^2 \to \mathbb{Z}[x]^2$. Suppose that there exists $f_i \in \mathbb{Z}[x]$ such that $M \cong \mathbb{Z}[x]/f_1 \bigoplus \mathbb{Z}[x]/f_2$. Let $e_i \in M$ be the image of a basis for $\mathbb{Z}[x]^2$ under the induced surjection:

$$\mathbb{Z}[x]^2 \to \mathbb{Z}[x]/f_1 \bigoplus \mathbb{Z}[x]/f_2 \cong M.$$

Then e_1, e_2 generates M and in terms of these generators

$$A = \begin{pmatrix} f_1 & 0 \\ 0 & f_2 \end{pmatrix},$$

a contradiction to the first part of this exercise.

□

Exercise 6. Set $M = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and let $\alpha : \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to M$ 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 necessarily equal to $\mathbb{Z} \times 0$

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 $(1, 0) \to (1, 1)$

□

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 homeomorphism ϕ takes torsion to torsion, hence the sequence is well define. 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 submodule. 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; $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, it is not a surjection on torsion submodules. □

SOLUTIONS SHEET 4 RINGS AND MODULES 2020

Exercise 1. Let $M \in \mathrm{Mat}(n,k)$ for a field k. Show that there is a basis with respect to which M is block diagonal with blocks of the form

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

Hint: M acts naturally on some n-dimensional k-vector space V. Consider V as a $k[x]$-module via $f \cdot v = f(M)(v)$.

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 $V \cong k[x]^{\oplus l} \oplus \sum_{i=0}^{m} k[x]/(f_i)$ 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 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 $f_i(x) = \sum_{j=0}^{d_i} a_i x^i$ then matrix of multiplication by x on $k[x]/(f_i)$ has the required form. $\square$

Exercise 2. Let R be a commutative ring, and let M be a R-module.

(1) Show that $\mathrm{Hom}_R(M, -)$ is *left exact.* That is for any 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 a R module M such that $\mathrm{Hom}_R(M, -)$ is not *right exact*. That is give an example of a surjection of R-modules $N \to N''$ 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 that $i\circ\phi : M \to N'$ is the zero morphism, since i is injective this implies that $\phi = 0$. It is therefore sufficient to check exactness in the middle, 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 $\phi(M) \subset i(N')$, 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

$$Hom_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \to Hom_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$$

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

□

Exercise 3. ** Extend the complex below to a free resolution $F_\bullet$ of the module $k := {}^{R}\!/_{(x,y)}$, where $R = k[x, y]$. 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 4.4.4. in the printed course notes.

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

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

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

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

Proof. The kernel of the first map has those (a, b, c) 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:

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

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

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

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

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

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

Upon applying $\mathrm{Hom}_R(\_, R)$ to the projective resolution determined by the complex above we get:

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

where the first non-zero map is given by $r \to (rx, ry, r(x + y))$ and the second map is given by

$$(r_1, r_2, r_3) \to (r_1, r_2, r_3) \begin{pmatrix} 1 & y \\ 1 & -x \\ -1 & 0 \end{pmatrix}.$$

We calculate the cohomology of this complex, The first map is injective, hence $H^0 = 0$, i.e., $Ext^0_{F_\bullet}(k, R) = 0$. The solution to the system:

$$r_1 + r_2 - r_3 = 0$$

$$r_1 y - r_2 x = 0$$

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 $Ext^1_{F_\bullet}(k, R) = 0$. Finally; the co-kernel of the map

$$(r_1, r_2, r_3) \to (r_1, r_2, r_3) \begin{pmatrix} 1 & y \\ 1 & -x \\ -1 & 0 \end{pmatrix},$$

is $R \oplus R/R \oplus R(x, y) \cong R/(x, y) \cong k$. Therefore, $Ext^2_{F_\bullet}(k, R) = k$. This agrees with the values for these groups given by the resolutions in Example 4.4.4. in the printed course notes.

□

Exercise 4. Let $0 \to M \xrightarrow{i} Z \xrightarrow{p} N \to 0$ be an exact sequence of R-modules.

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

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

(b) A *section* of i is a morphism $q\colon Z \to M$ such that $q \circ i = id_M$. Show that i admits a section if and only if there exists an isomorphism $\Phi : Z \cong M \oplus N$ and a commuting diagram with exact rows:

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

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

Proof. Suppose that we have a commuting diagram as the one described in the exercise. Define $s : N \to Z$ by $N \xrightarrow{e_N} M \oplus N \overset{\Phi^{-1}}{\cong} Z$ 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 $p = \pi \circ \Phi$ and hence $p \circ s = \pi \circ \Phi \circ \Phi^{-1} \circ e_N = \pi \circ e_N = id_N$.

Converserly, suppose that $s : N \to Z$ is a section of p. Define $\Phi : Z \to M \oplus N$ by $\Phi(z) = (i^{-1}(z - sp(z)), p(z))$. This is welldefined, because $p(z - sp(z)) = p(z) - p(z) = 0$ and hence $(z - sp(z)) \in ker(p) =$

$im(i)$. We prove that Φ is an isomorphism. Let $(m,n) \in M \oplus N$, then $\Phi(i(m)+s(n)) = (i^{-1}(i(m)+s(n)-sp(i(m)+s(n))), p(i(m)+s(n))) = (m,n)$ since $p \circ i = 0$ and $p \circ s = id_N$. This proves that Φ is surjective. Suppose $\Phi(z) = 0$, then $p(z) = 0$ and $z - sp(z) = 0$, hence $0 = z - sp(z) = z$. Moreover, $\pi \circ \phi = p$ by definition and $\phi \circ i = e$ as $p \circ i = 0$. □

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

(a) Is the ideal $(2, 1+\sqrt{-5})$ a free $\mathbb{Z}[\sqrt{-5}]$-module?
Hint: Consider the element $6 \in \mathbb{Z}[\sqrt{-5}]$.
(b) 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* $q : \mathbb{Z}[\sqrt{-5}]^2 \to (2, 1+\sqrt{-5})$ *and examine the assignment* $g : (2, 1+\sqrt{-5}) \to \mathbb{Z}[\sqrt{-5}]^2$ *defined by* $g(x) = 2xe_1 - \frac{1-\sqrt{-5}}{2}xe_2$.

Proof. (a) The $\mathbb{Z}[\sqrt{-5}]$-module $I = (2, 1+\sqrt{-5})$ is not free. It is not free on one generator since it can not be generated by a single element (a proof of this is given below). By definition the elements 2 and $1+\sqrt{-5}$ generate I, however they satisfy the non-trivial relation $3 \times 2 - (1-\sqrt{-5})(1+\sqrt{-5}) = 0$. Therefore I can not be free on any number of generators.

Here we show that $I = (2, 1+\sqrt{-5})$ is not generated by one element.

We first show that $1 \notin I$ by proving that for all elements $a + b\sqrt{-5} \in I$ we have that $a = b \bmod 2$. We calculate $(r_1+r_2\sqrt{-5})(1+\sqrt{-5}) = r_1 - 5r_2 + (r_1+r_2)\sqrt{-5}$. We have that $r_1 - 5r_2 = r_1 + r_2 \bmod 2$. Obviously $a = b \bmod 2$ 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 $r_1 = r_2 \bmod 2$ and $s_1 = s_2 \bmod 2$ then $(r_1 + r_2\sqrt{-5}) + (s_1+s_2\sqrt{-5}) = r_1+s_1+(r_2+s_2)\sqrt{-5}$ satisfies $s_1+r_1 = s_2+r_2 \bmod 2$.

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 $N(a + b\sqrt{-5}) = a^2 + 5b^2$ 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.

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

□

PROBLEM SHEET 5 RINGS AND MODULES 2020

There is one exercise in this problem sheet that will be part of the fifth homework. The solution has to be written in Latex and handed in as a pdf file on Moodle. The third homework is due on Sunday November 1 at 18:00. The exercise will be denoted by the symbol ** next to the exercise number.

Exercise 1. In this exercise we prove the the two *4-lemmas*. To this end, suppose that we have a commuting diagram with exact rows:

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

(a) Show that if a and c are epimorphisms and d is a monomorphism then b is an epimorphism.
(b) Show that if b and d are monomorphisms and a is an epimorphism then c is a monomorphism.

Proof. (a) Let $y \in B'$, we want to show that there exists $x \in B$ such that $b(x) = y$. To this end, since c is surjective there exists $x_C \in C$ such that $c(x_C) = f_2'(y)$. By commutativity of the diagram $df_3(x_C) = f_3'c(x_C) = f_3'f_2'(y)$. By exactness of the rows $f_3'f_2'(y) = 0$ and hence $f_3(x_C) \in \ker(d)$. By assumption $\ker(d) = 0$ and hence (using exactness of the rows) $x_C \in \mathrm{im}(f_2)$. Let $x_B \in B$ be such that $f_2(x_B) = x_C$. We have $f_2'(b(x_B) - y) = 0$, by commutativity and definition of x_B. By exactness of the lower row there therefore exists $y_A \in A'$ such that $f_1'(y_A) = b(x_B) - y$. By assumption a is surjective. Let $x_A \in A$ such that $a(x_A) = y_A$. We have $bf_1(x_A) = b(x_B) - y$ by commutativity. Let $x = x_B - f_1(x_A)$, then $b(x) = b(x_B) - b(x_B) + y = y$. We conclude that b is an epimorphism.
(b) This is very similar.

□

Exercise 2. Prove the following.

(a) If

$$0 \longrightarrow M_n \xrightarrow{f_n} \dots \xrightarrow{f_1} M_0 \longrightarrow 0$$

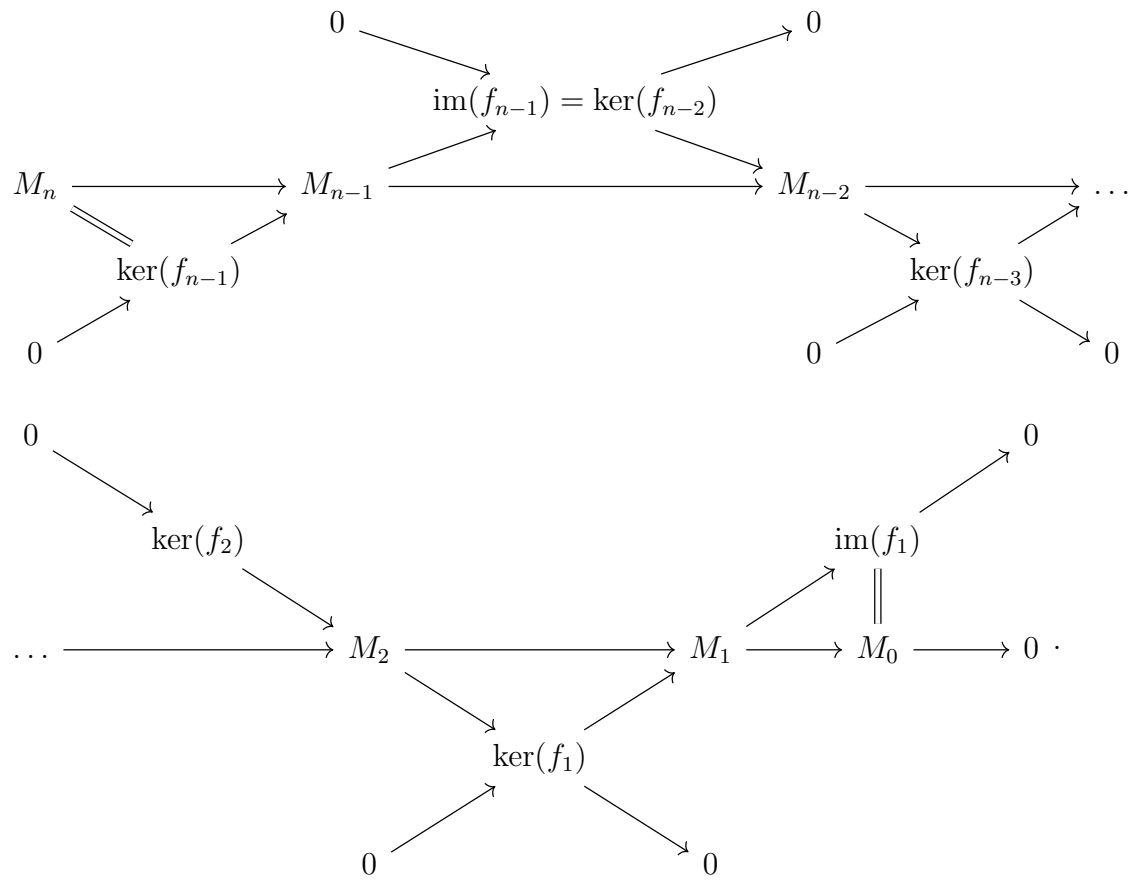
is an exact sequence of finitely generated modules over an Artinian and Notherian ring R, then $0 = (-1)^i \operatorname{length} M_i$

(b) Let $R = k[\varepsilon]$ denote (as usual) the quotient $k[x]/(x^2)$ where k is a field. Let M be the R-module $R/(x)$. Show that M has no finite resolution by finitely generated free modules.

(c) 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.

(d) Prove that over a PID every finitely generated module has a finite free resolution.

Proof. (a) 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 $\operatorname{length}(M_0) = \operatorname{length}(M_1) - \operatorname{length}(\ker(f_1))$ and $\operatorname{length}(\ker(f_i) =$

length(M_{i+1}) − length(ker(f_{i+1})) for $1 \leq i \leq n-2$. Finally length(ker(f_{n-1}) = length(ker(M_n).

(b) Suppose that

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

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

(c) Suppose that

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

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

(d) This follows from the structure theorem for finitely generated modules over principal ideal domains. Upto iso morphism $M = R^n \oplus_{i=1}^{k} R/f_i$ for some $f_i \in R$. Therefore we have a presentation:

$$R^k \to R^{k+n} \to M$$

where the first morphism is defined on a basis by $e_i \to f_i e_i$. Since R is a domain this map is injective, hence this is a resolution of finite length.

□

Exercise 3. Prove the following.

(a) Show that any finitely generated module over a semi-simple ring is semi-simple

(b) Show that any finitely generated module over a semi-simple ring is projective

(c) Deduce that any finitely generated module over $k[G]$ is projective, if char $k \nmid |G|$

(d) What are the Ext-groups then for finitely generated $k[G]$-modules?

Proof. (a) Let $\phi : R^k \to M$ be a surjection. Since R is semi-simple so is R^k. Write $R^k = \oplus_{i=1}^{s} I_i$, where each of the I_i are simple. Let $\phi(I_i) = M_i$, by surjectivity, $M = \sum_i M_i$. We will prove that M_i is simple. To this end let $0 \neq N_i \nsubseteq M_i$. We have $\phi^{-1}N_i \subset I_i$. Therefore $\phi^{-1}N_i = I_i$ and so $\phi(I_i) = \phi(\phi^{-1}N_i) \subset N_i$.

(b) Let R be a semi-simple ring and P a finitely generated R-module. Let $g : N \to M$ be a surjection of R modules and let $f : P \to M$ be a R-module homomorphism. By the previous part, $P = \oplus_i^n P_i$ where P_i is simple, and therefore cyclic.

Let $P_i = Ra_i$. Since g is surjective there exists $y_i \in N$ such that $g(y_i) = f(a_i)$. We define $s : \oplus_i^n R \to N$ by $e_i \to y_i$ and $q : \oplus_i^n R \to P$ by $e_i \to a_i$ we have $g \circ s = f \circ q$. Now, we use that R is semi-simple, in particular there is a splitting $R = Ann(a_i) \oplus I$ and therefore there exists an isomorphism $\phi_i : Ra_i \cong I$ where I is a submodule of R, we define $P \to N$ to be the composition $s \circ \oplus_i \phi_i$.

(c) We saw in Exercise 6.2 that $k[G]$ is semi-simple if $\operatorname{char} k \nmid |G|$, hence this follows from the previous point.

(d) In class (Corollary 4.4.24) we proved that $\operatorname{Ext}^1_R(P, N) = 0$ whenever P is a projective R-module.

□

Exercise 4. **[1]

(a) Set $k = \mathbb{F}_p$ and $G = \mathbb{Z}/p\mathbb{Z}$. Find all the submodules (i.e. ideals) of $R = k[G]$. *Hint: Over a field of positive characteristic p we have $a^p + b^p = (a + b)^p$.*

(b) For $p = 2$, let x denote a generator of G, set $M = (x + 1)$. Compute all $\operatorname{Ext}^i_R(M, M)$.

Proof. (a) We define a ring homomorphism Φ from $k[G]$ to $\mathbb{F}_p[x]/(x^p - 1)$ by defining $\Phi(\psi) = x$ where ψ is a generator of the cyclic group G. I.e., we have $\Phi(\psi + \psi) = x^2$ and then we extend Φ by k-linearity, i.e., in general $\Phi(\lambda(m\psi)) = \lambda x^m$. This obviously defines a ring homomorphism. In particular, since $p\psi = 0$, Φ defines a surjection $\Phi : k[G] \to \mathbb{F}_p[x]/(x^p - 1)$. These have the same dimension as vector spaces over k and hence there is an isomorphism of rings $k[G] \cong \mathbb{F}_p[x]/(x^p - 1)$. The ideals of $\mathbb{F}_p[x]/(x^p - 1)$ is in one to one correspondence with the ideals of $\mathbb{F}_p[x]$ containing $(x^p - 1)$, but using the hint we easily see that $(x^p - 1) = (x - 1)^p$. Since $(x - 1)$ obviously is an irreducible polynomial the ideals strictly containing $(x - 1)^p$ are the ideals $(x - 1)^i$ where $1 \leq i \leq p - 1$.

(b) We have an infinite projective resolution $\cdots \to R \to R \to R \to R \to R \to R$ where every morphism is multiplication by $(x+1)$. When applying $Hom_R(,M)$ this gives $\cdots \leftarrow M \leftarrow M \leftarrow M \leftarrow M$, and all maps are zero, so all Ext-groups are isomorphic to M.

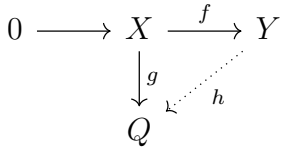
□

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

PROBLEM SHEET 6 RINGS AND MODULES 2020

There is one exercise in this problem sheet that will be part of the sixth homework. The solution has to be written in Latex and handed in as a pdf file on Moodle. The sixth homework is due on Sunday November 8 at 18:00. The exercise will be denoted by the symbol ** next to the exercise number.

Exercise 1. In this exercise we define injective modules and prove *Baer's criterion*. We say that a left R-module Q is injective if it satisfies the following universal property:
Whenever we have a monomorphism $X \to Y$ and a homomorphism $g : X \to Q$ of left R-modules, then there exists a left R-module homomorphism $h : Y \to Q$ making the following diagram commute:



We will prove the following:

Theorem 1.1. *(Baer's Criterion) Suppose that the left R-module Q has the property that if I is any ideal of R and $f : I \to Q$ is a R-module homomorphism, there exists an R-module homomorphism $F : R \to Q$ 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.

(a) Show that if $X = Ra$ and $Y = Rb$ are both *cyclic modules* and $X \to Y$ is a monomorphism and we are given a homomorphism $g : X \to Q$, then there exists a left R-module homomorphism $h : Y \to Q$ making the appropriate diagram commute. *Hint: Consider the subset of R defined by $I = \{r \in R : rb \in X\}$*

(b) Prove that if X, Y are finitely generated and we have a monomorphism $X \to Y$ and a homomorphism $g : X \to Q$ of left R-modules, then there exists a left R-module homomorphism $h : Y \to Q$ making the appropriate diagram commute. *Hint: Prove the case when $Y = X + Rb$ for some $b \notin X$ by defining the ideal I of R by $I = \{r \in R : rb \in X\}$*

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

Axiom 1.2. (Zorn's Lemma)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 $M \not\leq N$)

Exercise 2. Use Baer's Criterion to show that $\mathbb{Q}$ is an injective $\mathbb{Z}$-module.

Exercise 3. ** Let $R = k[x, y]$ be the polynomial ring in two variables over an algebraically closed field k. Recall that an ideal 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 3.1 (The weak Nullstellensatz in two variables)**.** *Let k be an algebraically closed field. Every maximal ideal m in the ring $k[x, y]$ is of the form $m = (x - a, y - b)$ for some $a, b \in k$.*

(a) if M is a finite length module over R, then the quotients of its composition series are of the form $R/(x - a, y - b)$.
(b) 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 maps $M \ni m \mapsto (x - a)m \in M$ and $M \ni m \mapsto (y - b)m \in M$. Apply then $\mathrm{Ext}^i_R(\_, N)$.
(c) Show that $\mathrm{Ext}^i(R/(x - a, y - b), N)$ is of finite length where N is any finitely generated module over R.
Hint: use the previous point
(d) Show that for each finite length module M and for each 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

Exercise 4. $R = k[x, y]$ as in the previous exercise (k is algebaically closed). We say that a finite length module is supported at $(x-a, y-b)$ if only $R/(x - a, y - b)$ appears as factors in the composition series. Show that if M is a finite length module supported at $(x - a, y - b)$, then $\mathrm{Ext}^i_R(M, R/(x - a', y - b')) = 0$, where $(a, b) \neq (a', b')$.

Exercise 5. For to 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.

Exercise 6. 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.

RINGS AND MODULES EXERCISE SHEET 7, 2020

There is one exercise in this problem sheet that will be part of the seventh homework. The solution has to be written in Latex and handed in as a pdf file on Moodle. The seventh homework is due on Sunday November 15 at 18:00. The exercise will be denoted by the symbol ** next to the exercise number.

Exercise 1. ** Let $R = k[x, y]$ and consider the R-module $M = k[x, y]/(x, y)$. Consider the free resolution:

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

Set $M = N$. Consider

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

Determine the isomorphism classes of the middle module of the Yoneda extension associated to $[\phi_i] \in \mathrm{Ext}^1_R(M, N)$ in Theorem 4.6.5 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 the above mentioned theorem, 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 $(\bar{a}, ax + by)$. Let's investigate the elements in the image of this map, we have $(\bar{a}, ax + by) = a(1, x) + b(0, y)$. Therefore, the image is the submodule $((1, x), (0, 1))$. Below we present three different solutions showing that this cokernel is isomorphic as a $k[x, y]$-module to $k[x, y]/(x^2, y)$.

(a) *Fast and slick.* Consider the element $\overline{(1, 1)} \in k\oplus k[x, y]/((1, x), (0, y))$, we have $y(1, 1) = (y, y) = y(1, x) + (1 - x)(0, y)$ and hence $y \in Ann(\overline{(1, 1)})$ similarly $x(1, 1) = \overline{(0, x)} \neq 0$ and $x^2(1, 1) = (0, x^2) = x(1, x)$, hence $(x^2, y) = Ann(\overline{(1, 1)})$. We therefore have an isomorphism $k[x, y]/(x^2, y) \to k[x, y]\overline{(1, 1)}$ defined by $1 \to \overline{(1, 1)}$. We

claim that in fact $k[x,y]\overline{(1,1)} = k \oplus k[x,y]/((1,x),(0,y))$. Let f_0 denote the constant term of f, an easy manipulation shows that $(\eta, f) = (f_0, f) + (\eta - f_0, 0)$, however $\overline{(\eta - f_0, 0)} = \overline{(0,(f_0-\eta)x)}$ and hence we see that $\overline{(\eta, f-(f_0-\eta)x)} = \overline{(f_0, f)}$. From this it follows that for $a, a' \in k$ $b, c \in k[x,y]$ we have $(a, a' + bx + cy) = (a, a' + (b+a'-a)x + cy - (a'-a)x) = \overline{(a', a' + (b+a'-a)x + cy)} = (a' + (b+a'-a)x + cy)\overline{(1,1)}$.

(b) *Explicit construction of the inverse of the isomorphism above.* We define a morphism $k \oplus k[x,y]/((1,x),(0,y)) \to k[x,y]/(x^2,y)$ by showing that there is a well-defined morphism of R-modules $k \oplus k[x,y] \to k[x,y]/(x^2,y)$ such that $(1,x)$ and $(0,y)$ is in the kernel. To this end we show that the map which send $(a,f) \to f - (a - f_0)x$ has this property, where f_0 is the constant term of f.
Remark: also $(a,f) \to f - ax$ has this property, but this does not give the same isomorphism as above, it corresponds instead to the isomorphism defined by $1 \to (0,1)$ above.
This is well-defined since if $a \in (x,y)$ then $ax \in (x^2,y)$. Similarly it is R-linear since $r(f-(a-f_0)x) - rf - (ra - (rf)_0)x = (rf_0 - (rf)_0)x \in (x^2,y)$. Moreover, $f(1,x) = x - x = 0$ and $f(0,y) = -y \in (x^2,y)$. We have $(1,1) \to 1$ and $(0,x) \to x$, hence it is a surjective. By a dimension count over k this is an isomorphism of R-modules.

(c) *Hands on approach.* There is a natural isomorphism of R-modules from $k \oplus k[x,y]/((1,x),(0,y))$ to $k \oplus k[x]/ < (1,x) >$ defined by mapping the variable y to zero. Over k, the module $k \oplus k[x]/ < (1,x) >$ 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 $x(1,1) = (0,x) = (-1,0)$ and $x^2(1,1) = (0,x^2) = x(1,x)$ and hence zero. Therefore, $k \oplus k[x]/ < (1,x) >$ has a natural structure of $k[x]/x^2 = k[\epsilon]$-module. Define a $k[\epsilon]$- modules morphism $k[\epsilon] \to k[x]/ < (1,x) >$ by mapping $1 \to (1,1)$, we check that $\epsilon \to x(1,1) = (0,x)$. This is a surjective morphism of $k[\epsilon]$-modules by the previous remarks. Since the dimension over k is two for both modules it is an isomorphism. Spelling this out, the composition $k[x,y]/(x^2,y) \to k \oplus k[x,y]/ < (1,x),(0,y) >$ is defined by $1 \to (1,1)$ i.e., for $f(x,y) = a + bx + cy$ for $a \in k$ and $b, c \in k[x,y]$ we have $f \to (\bar{f}, f) = (a, a + bx + cy)$, the argument given says that this is a well-defined isomorphism of $k[x,y]$-modules.

(d) 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: I.e., 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 $1 \to -x$ and the second $x \to 0$. 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 $1 \to -y$ and the second $y \to 0$. 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 $k[x,y]/(x^2,y)$, i.e., for any such f, $f(y) = yf(1) = 0$ (they are however the same as extensions of k-algebras, by mapping $x \to y$).

Exercise 2. Let $R = k[x,y]$.

(a) Show that $\mathrm{Ext}^1\left((x,y), {}^{R}\!/_{(x,y)}\right) \neq 0$.

(b) Construct a finitely generated module M such that $\mathrm{Tors}(M) \subseteq M$ is not a direct summand.

Note: $\mathrm{Tors}(M) \subseteq M$ *is always a direct summand if* R *is a PID by the fundamental theorem for finitely generatid modulues over PIDs.*

Proof. (a) As seen on several occasions in this course, we have a projective resolution:

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

where the morphisms are given by $r \to (-ry, rx)$ and $(r_1, r_2) \to (r_1x, r_2y)$ respectively. To calculate $\mathrm{Ext}^1\left((x,y), {}^{R}\!/_{(x,y)}\right)$ we apply $Hom(\_, k)$ and calculate the cohomology in degree one of the corresponding complex. I.e., the cokernel of $k \oplus k \to k$ given by $(r_1, r_2) \to (r_1, r_2)\begin{pmatrix} x \\ y \end{pmatrix} = r_1x + r_2y = 0$. Here we used that multiplication by x and y are zero. In particular:

$$\mathrm{Ext}^1\left((x,y), {}^{R}\!/_{(x,y)}\right) = k.$$

(b) Let $\lambda \in k$ be non-zero and let $[\lambda] \in \mathrm{Ext}^1\left((x,y), {}^{R}\!/_{(x,y)}\right)$ be the corresponding extension. Then $[\lambda]$ correspond to a non-split short

exact sequence of R-modules:

$$0 \to R/(x,y) \to N \xrightarrow{\phi} (x,y) \to 0,$$

For any $n \in N$ coming from $R/(x,y)$ we have $xn = 0$, in particular $\ker(\phi) \subset \mathrm{Tors}(N)$. Similarly, suppose $n \in \mathrm{Tors}(N)$ and let $rn = 0$, since (x,y) is a torsion free module we have $r\phi(n) = 0$ if and only if $n \in \ker(\phi)$. This shows that $\ker(\phi) = \mathrm{Tors}(N)$. Since the sequence does not split by assumption, we have that $\mathrm{Tors}(N)$ is not a direct summand of N.

□

Exercise 3. Let R be a ring and let M, K, L and N be R-modules. Assume that $\mathrm{Ext}^i_R(M,N)$, $\mathrm{Ext}^i_R(K,N)$ and $\mathrm{Ext}^i_R(L,N)$ have finite length and that there exists integers r, s such that they are all zero for all $i < r$ and all $i > s$. Show that if

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

is a short exact sequence, then

$$\sum_{i=r}^{s} \mathrm{length}(-1)^i \,\mathrm{Ext}^i_R(M,N) =$$

$$\sum_{i=r}^{s} \mathrm{length}(-1)^i \,\mathrm{Ext}^i_R(K,N) + \sum_{i=r}^{s} \mathrm{length}(-1)^i \,\mathrm{Ext}^i_R(L,N).$$

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 5.2. *Note:* Exercise 5.2 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 4. Set $R = \mathbb{Z}\left[\mathbb{Z}/2\mathbb{Z}\right] \cong \mathbb{Z}[x]\Big/(x^2-1)$. We show properties exhibiting that R is different than both $\mathbb{F}_2\left[\mathbb{Z}/2\mathbb{Z}\right]$ and $\mathbb{C}\left[\mathbb{Z}/2\mathbb{Z}\right]$:

(a) Show that R contains no simple submodules and hence show that it it is not semi-simple.
(b) Show that $R(1+x) \subseteq R$ is not projective by showing that

$$\mathrm{Ext}^1_R(R(1+x), R(1-x)) \cong R/2R + R(1+x) \neq 0.$$

Proof. (a) We have seen that every simple R-submodule of R is of the form Rm for some $m \in R$ such that $\mathrm{Ann}(m)$ is a maximal ideal of R. Let $\overline{m} \in R$, if $m \in \mathbb{Z}$ then $\mathrm{Ann}(m) = 0$ which is not maximal. If $m = p(x)$ is a polynomial in $\mathbb{Z}[x]$ then either $\mathrm{Ann}(p(x)) = (x+1)$,

if $p(x)$ is divisible by $(x-1)$ or $\mathrm{Ann}(p(x)) = (x-1)$, if $p(x)$ is divisible by $(x+1)$, or else $\mathrm{Ann}(p(x)) = 0$. Therefore $\mathrm{Ann}(m)$ is never maximal.

(b) A projecive resolution is given by:

$$\ldots \xrightarrow{m_{(1-x)}} R \xrightarrow{m_{(1+x)}} R \xrightarrow{m_{(1-x)}} R.$$

This gives, after applying $Hom(\_, (1-x))$ that the cohomology in degree one is

$$R(1-x)/R(1-x)^2.$$

Under the isomorphism $R(1-x) \cong R/(1+x)R$, this gives $R/2R + R(1+x)$. □

Exercise 5. Let R be an integral domain, and let K be its fraction field.

(a) Prove that if $f \in R$ is a non-zero element, then $\mathrm{Ext}^1_R(R/(f), K) = 0$.

(b) More generally, prove that if $f_1, \ldots, f_n$ is a sequence of elements such that for every $1 \leq i \leq n$ the multiplication by f_i is injective on $R/(f_1, \ldots, f_{i-1})$ then

$$\mathrm{Ext}^1_R(R/(f_1, \ldots, f_n), K) = 0.$$

Proof. (a) Since f is a non-zero and R is an integral domain the sequence (not exact at the right spot):

$$P^\bullet \colon 0 \to R \xrightarrow{f\cdot} R \to 0$$

is the projective resolution of $R/(f)$. Consequently, we compute $\mathrm{Ext}^1(R/(f), K)$ by taking $\mathrm{Hom}(-, K)$ functor of the $P^\bullet$ and computing cohomology at the first spot – note that the arrows get reversed. Identifying $\mathrm{Hom}(R, K)$ with K (by an isomorphism given by evaluation at $1 \in R$) we see that $\mathrm{Ext}^1(R/(f), K)$ is isomorphic to the cokernel of multiplication by f on K. This is clearly zero, because f is invertible in K, that is, $x = f \cdot f^{-1}x \in K$. In terms of homomorphisms every $\phi \in \mathrm{Hom}(R, K)$ is f-divisible – consider post multiplication by $f^{-1} \in K$.

(b) We reason by induction. The case $n = 1$ is (1). Since $f_n \in R/(f_1, \ldots, f_{n-1})$ is a non-zero divisor we obtain a short exact sequence:

$$0 \to R/(f_1, \ldots, f_{n-1}) \xrightarrow{f_n\cdot} R/(f_1, \ldots, f_{n-1}) \to R/(f_1, \ldots, f_{n-1}, f_n) \to 0.$$

By considering corresponding long exact sequence of Ext groups (note that the arrows get reversed) we obtain:

$$\ldots \to \mathrm{Hom}(R/(f_1,\ldots,f_{n-1}),K) \to \mathrm{Ext}^1(R/(f_1,\ldots,f_n),K) \to \mathrm{Ext}^1(R/(f_1,\ldots,f_{n-1}),K) \to \ldots$$

The right term in the sequence is zero by induction. The left one is zero because $R/(f_1,\ldots,f_{n-1})$ is f_1-torsion and K is f_1-divisible (every element is divisible by f_1). Consequently, we see that

$$\mathrm{Ext}^1(R/(f_1,\ldots,f_n),K) = 0,$$

because it fits between to zeroes in a long exact sequence.

□

RINGS AND MODULES 2020 - SOLUTIONS SHEET 8

There is one exercise in this problem sheet that will be part of the eight homework. The solution has to be written in Latex and handed in as a pdf file on Moodle. The eight homework is due on Sunday November 22 at 18:00. The exercise will be denoted by the symbol ** next to the exercise number.

Exercise 1. ** 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 $\mathrm{Frac}(R)[t]$ *iff 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: $\frac{f^3(y)}{g^3(y)} + y^7 = 0$, and hence $f^3(y) = -g^3(y)y^7$, this is impossible since three does not divide seven.

□

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

□

Exercise 3. Solve the following exercises:

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

Proof. (a) $p = x - 1$ is prime in $\mathbb{C}[x]$ and satisfies the conditions of Eisenstein's criterion.
(b) 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 $X^2 + Y^2 - 1 = X^2 + (Y + 1)^2 = (X + Y + 1)^2$ and hence this polynomial is not irreducible.

□

Exercise 4. Solve the following exercises:

(a) Prove that $R := \mathbb{C}[x, y, z]/(xy - z^2)$ is a domain. Calculate the transcendent degree over $\mathbb{C}$ of the fraction field of R.
(b) Calculate the dimension of the ring $\mathbb{Z}[x]$.

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

Proof. (a) To show that R is a domain it is sufficient to show that $xy - z^2$ is irreducible. This follow from Eisenstein's criterion applied to $xy - z^2 \in k[x, y][z]$, with $p = x$. Let $\bar{x}$, $\bar{y}$,$\bar{z}$ denote the image of x, y and z in $R = \mathbb{C}[x, y, z]/(xy-z^2)$ under the quotient map $\mathbb{C}[x, y, z] \to R$. We see that $\mathbb{C}[x, y] \cong \mathbb{C}[\bar{x}, \bar{y}] \subset R$ since the kernel of the quotient map consits of those polynomials that belongs to the ideal $(xy-z^2)$ and there are no such polynomials in the variables x, y. Moreover, $\bar{z}$ is integral over $S = \mathbb{C}[\bar{x}, \bar{y}]$ since $\bar{x}\bar{y} - \bar{z}^2 = 0$. This implies that R is integral over the subring S where $S \cong \mathbb{C}[x, y]$. We conclude by Noether Normalization that $Frac(R)$ has transcendence degree two over $\mathbb{C}$.

(b) Let $P \in \mathbb{Z}[x]$ be a prime ideal. Then $P \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, we will treat the two cases $P \cap \mathbb{Z} = 0$ and $P \cap \mathbb{Z} = p$ for a prime p separatly. We start with the case $P \cap \mathbb{Z} = 0$. In this case P contains no integer and therefore $P^e \subset \mathbb{Q}[x]$ contains no element of $\mathbb{Q}$, i.e., $P^e \subset \mathbb{Q}[x]$ is a proper ideal. Since $\mathbb{Q}[x]$ is a PID there exists a polynomial $f \in \mathbb{Q}[x]$ such that $P^e = (f)$. Let $c(f)$ be the content of f as in the proof of Gauss' Lemma, then $P \subset P^{ec} = (c(f)f)$. This means that every element of P is divisible by $c(f)f$, since P is prime this means that $P = (c(f)f)$ and that $c(f)f$ is an irreducible polynomial in $\mathbb{Z}[x]$. Hence the primes P which intersects $\mathbb{Z}$ trivially are principal, generated by an irreducible polynomial in $\mathbb{Z}[x]$.

We now suppose that $P \cap \mathbb{Z} = p$, where p is a prime. Since $(p) \in P$, this implies that P corresponds to a unique prime ideal in the quotient $\mathbb{Z}[x]/(p) = \mathbb{Z}/p\mathbb{Z}[x]$. This is a principal ideal domain and hence P corresponds to either 0 or to $(\bar{f})$ for an irreducible polynomial $\bar{f} \in \mathbb{Z}_p[x]$, i.e., $P = p$ or $P = (p, f)$ for f a preimage of $\bar{f}$.

Since principal prime ideals in an UFD necessarily is of height one, it is sufficient to examine the height of the maximal ideals $m = (p, f)$ where p is a prime number and $f \in \mathbb{Z}[x]$ is irreducible mod p. We claim that the height of such a prime is two. Since $0 \subset (p) \subset m$ is a chain of length two it is sufficient to prove that there is no chain of strictly bigger length. Let $P \subset (p, f)$ be a non-zero prime ideal. If $(p) \subset P$ we must have that $P = (p)$ or $P = (p, f)$ since $\mathbb{Z}_p[x]$ has dimension one. We conclude that the only chain of prime ideals inside m that contains p is the chain $0 \subset (p) \subset m$. Hence we suppose that $P \subset m$ is a prime ideal that does not contain p. Then $P = (g)$ for some irreducible polynomial $g \in \mathbb{Z}[x]$ by our previous disscussion. Any such prime is of height one and hence every such chain has maximal length two, i.e., if $0 \subset P_1 \subset P_2 \subset m$ is a chain of prime ideals such that $p \notin P_2$ then $P_1 = (g)$, $P_2 = (g')$ for some irreducible polynomial $g, g' \in \mathbb{Z}[x]$. The containment $(g) \subset (g')$ implies that $P_1 = P_2$ since both g' and g are irreducible polynomials in $\mathbb{Z}[x]$.

We conclude that the maximal height of a prime ideal in $\mathbb{Z}[x]$ is two, i.e., the dimension of the ring $\mathbb{Z}[x]$ is two.

(c) We have seen in a previous exercise that every prime ideal in an Artinian ring is maximal. Hence every prime ideal has height 0, i.e., an Artinian ring has dimension 0.

(d) The prime ideals of $\mathbb{Z}[x]/(4, x^2)$ correspond to the prime ideals of $\mathbb{Z}[x]$ that contain $(4, x^2)$. If P is prime such that $4 \in P$ then $2 \in P$, similarly if $x^2 \in P$ then $x \in P$. Hence $(4, x^2) \subset P$ implies that $(2, x) \subset P$. Since $(2, x)$ is maximal

we must have $P = (2, x)$. Converserly, $(4, x^2) \subset (2, x)$. Hence the unique prime ideal of $\mathbb{Z}[x]/(4, x^2)$ is $(2, x)/(4, x^2)$. In particular $\mathbb{Z}[x]/(4, x^2)$ has dimension 0.

□

Exercise 5. Show the following:

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

Proof. (a) In any ring R, $0 \subset P$ for every prime ideal P, hence 0 is prime if and only if it is the only prime ideal of height zero.
(b) Let P be a prime ideal of height one. We will prove that P contains a prime element p. If P contains a prime element p then $(p) = P$, since $(p) \subset P$ and the only prime ideal that is strictly contained in P is 0 by part a). Let $f \in P$ be non zero (this is possible since $P \neq 0$ because P has height one), let $f = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ be a unique (upto multiplication by units) prime decomposition of f. Since P is prime, we must have $p_i \in P$ for some $i \in \{1, \dots r\}$. We conclude that $P = (p_i)$.
(c) The prime ideals of height zero in $\mathbb{R}[x, y]/(xy)$ correspond to the primes $P \subset \mathbb{R}[x, y]$ that contains xy and that do not contain any other prime ideal P' such that $xy \in P'$. Suppose $xy \in P$ then either $x \in P$ or $y \in P$, hence either $(x) \subset P$ or $(y) \subset P$, since (x) and (y) both are prime ideals that contain xy we conclude that $P = (x)$ or $P = (y)$.

□

Exercise 6. Show the following:

(a) Let $F \subset L$ be a field extension, and suppose $a_1, ..., a_n$ are elements of L which are algebraically independent over F. Prove that $F(a_1, ..., a_n)$ is isomorphic to the fraction field of the polynomial ring $F[x_1, ..., x_n]$.
(b) Let $F \subset L$ be a field extension. Show that a subset of L is a transcendence basis for L/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 L/F.

Proof. (a) Let $F \subset L$ be a field extension, and suppose $a_1, ..., a_n$ are elements of L which are algebraically independent over F. We will prove that $F(a_1, ..., a_n)$ is isomorphic to the fraction field of the polynomial ring $F[x_1, ..., x_n]$. To this end, define a ring homomorphism $\phi : F[x_1, ..., x_n] \to L$ by $x_i \mapsto a_i$. 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 $F(x_1, ..., x_n) \to L$. This is surjective because F and each of the a_i is in the image, and these generate L over F.
(b) Suppose the set $\{a_i\}_I$ is a transcendence basis for L/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 is not algebraically dependent on $\{a_i\}_I$. But by definition of transcendent basis, $L/F(\{a_i\})$ is finite, so there is a polynomial $p \in F(\{a_i\})[X]$ such that $p(a) = 0$. Multiply through to clear denominators, we can view p as a non-zero multivariate polynomial with coefficients in F satisfied by some subset of $\{a_i\}$ and a. This contradicts the choice of a.

Conversely, suppose $\{a_i\}_I$ is a maximal algebraically independent set. We need to show that $L/F(\{a_i\}_I)$ is algebraic. Suppose $a \in L$. As $\{a_i\}_I \cup \{a\}$ is not algebraically independent there is some multivariate polynomial with coefficients in F such that $f(a, a_{i_1}, ..., a_{i_n}) = 0$. This must have some non-zero a term as otherwise it gives an algebraic dependence among the a_i. This gives the required polynomial satisfied by a with coefficients in $F(\{a_i\})$ by dividing through by the coefficient of the highest power of a.

To show that a transcendence basis exists, we use Zorn's lemma on the partially ordered set Σ of algebraically independent sets inside L. If Σ is empty then L/F is algebraic and there is nothing to prove. Hence assume that Σ is non-empty. To use Zorn's Lemma we must show that any chain of algebraically independent sets has an upper bound in Σ. Suppose (A_α) is such a chain, i.e., for all indexes α, β either $A_\alpha \subset A_\beta$ or $A_\alpha \supset A_\beta$ holds. Then $\cup_\alpha A_\alpha$ defines an algebraically independent set, since any polynomial relation in $\cup_\alpha A_\alpha$ is a polynomial relation in A_α for α sufficiently large. Therefore $\cup_\alpha A_\alpha$ is an upperbound for the chain (A_α). 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 7. 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 $\alpha_1, \ldots, \alpha_{\mathrm{trdeg}_F L} \in L$. Let $\beta_1, \ldots, \beta_{\mathrm{trdeg}_F K} \in K$ be a maximal algebraically F-independent subset of K and let $\gamma_1, \ldots, \gamma_{\mathrm{trdeg}_K L} \in L$ be a maximal algebraically K-independent subset of L. By construction:

$$\beta_1, \ldots, \beta_{\mathrm{trdeg}_F K}, \gamma_1, \ldots, \gamma_{\mathrm{trdeg}_K L} \in L$$

is an algebraically F-independent subset of L. Suppose $\alpha \in L$ such that

$$\beta_1, \ldots, \beta_{\mathrm{trdeg}_F K}, \gamma_1, \ldots, \gamma_{\mathrm{trdeg}_K L}, \alpha \in L$$

is algebraically F-independent. Then $\gamma_1, \ldots, \gamma_{\mathrm{trdeg}_K L}, \alpha \in L$ is algebraically K-independent, but this is impossible since $\gamma_1, \ldots, \gamma_{\mathrm{trdeg}_K L} \in L$ is a maximal algebraically K-independent subset of L. □

RINGS AND MODULES 2020
SHEET 9 SOLUTIONS

emelie.arvidsson@epfl.ch

Exercise 1 (Nakayama's Lemma)**.** Let R be a ring and let M be a finitely generated R-module. Show the following:

(a) Let I be an ideal of R such that $IM = M$. Then there exists $x \in 1 + I$ such that $xM = 0$.
(b) Suppose now that the ring R is local, i.e., that there is a unique maximal ideal m of R. Suppose that $mM = M$, show that this implies that $M = 0$
(c) Show that (removing the previous assumption on R being local) that if there is an ideal $I \subset \mathrm{nil}(R)$, where $\mathrm{nil}(R)$ is the nilradical of R, such that $IM = M$, then this implies that $M = 0$.

Hint: Prove that in b, c the element x, whose existence is assured by a, in fact is invertible.

Proof. (a) Let $m_1, ..., m_n$ be generators of M. As $IM = M$, there is a matrix A with entries in I such that $A\underline{m} = \underline{m}$, where $\underline{m}$ is the column vector with i^{th} entry m_i. Therefore $(A - Id)\underline{m} = 0$. Multiplying by the adjugate of the matrix $A - Id$ implies that if $D = \det(A - Id)$ then $Dm_i = 0$ for all i. Hence $DM = 0$, since the m_i generate M. If we can prove that $D \in 1 + I$ then we are done. By expanding the determinant, we can see that $D = \det(A - Id)$ cannot be in I, for all the components of A are in I, and so there is only one term of the expansion of $\det(A - Id)$ which is not, and this is the 1 which comes from the $\Pi(a_{ii} - 1)$ terms. In particular, $D - 1 \in I$.
(b) We have $D \notin m$ since $1 \notin m$. Suppose that D is not a unit. Then D is contained in some proper maximal ideal by Zorn's lemma, but this is a contradiction since $D \notin m$.
(c) You have seen that the nil-radical of R is the intersection of all prime ideals of R. Let $1 - D = x$ for $x \in \mathrm{nil}(R)$. Suppose $1 - x$ is not a unit. It belongs to some maximal ideal m, but $x \in m$ and therefore $1 \in m$, which is absurd.

□

Let M be a finitely generated A-module and let a be an ideal ofA such that aM = M. Then there exists X == l(mod a) such that xM = O.

Exercise 2. Let R be a local 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. (After a few more lectures, you will be able to remove the assumption that R is local.)

Proof. Suppose on the contrary that F is a finitely generated R-module. Notice that $\mathfrak{m}F = F$, because every element of $\mathfrak{m}$ is invertible in F. Therefore by Nakayama's lemma $F = 0$. This gives a contradiction, so F cannot be finitely generated. □

Exercise 3. Let $\mathbb{F}_q$ be the finite field with q elements. Suppose that R is a quotient of $\mathbb{F}_q[x_1, ..., x_n]$. Prove that there is a subring $S \subset R$ such that $S \cong \mathbb{F}_q[t_1, ..., t_r]$ and R is integral over S.

Proof. We follow the proof from the course notes, amending as suggested by the hint.

We use induction on n. If $n = 1$ we are done exactly as in the notes. So assume we know the statement for smaller values of n. Let $\overline{x}_i$ be the residue class of x_i in R. After reordering we may assume that $\overline{x}_n$ is algebraic over $F(\overline{x}_1, ..., \overline{x}_{n-1})$, otherwise the $\overline{x}_i$ are algebraically independent and we are done. Therefore there is a polynomial $g \in k[y_1, ..., y_n]$ such that $g(\overline{x}_1, ..., \overline{x}_n) = 0$, and $g(\overline{x}_1, ..., \overline{x}_{n-1}, y_n)$ is non-zero as a polynomial in $(k[\overline{x}_1, ..., \overline{x}_{n-1}])[y_n]$.

Let d be the degree of g. Let $\overline{y}_i = y_i - y_n^{N^i}$ for $i < n$ for some $N > d$ and $\overline{y_n} = y_n$. Then let $h(\overline{y}_1, ..., \overline{y}_n) = g(\overline{y}_1 + \overline{y}_n^N, \overline{y}_2 + \overline{y}_n^{N^2}, ..., \overline{y}_n)$. The highest power of $\overline{y}_n$ in the expansion of any monomial in the y_i occurs from taking each $\overline{y}_n$ term. The exponent N is arranged so that this highest power is different for every monomial of degree at most d. Thus the highest $\overline{y}_n$ degree terms from each monomial do not cancel in the expansion of g in terms of the $\overline{y}_i$, and so (after dividing by an element of $\mathbb{F}_q$), $h(\overline{y}_n)$ is a monic polynomial in $k[\overline{y}_1, ..., \overline{y}_{n-1}]$. This implies that $\overline{x}_n$ is integral over $k[\overline{x}_1 - \overline{x}_n^N, ..., \overline{x}_{n-1} - \overline{x}_n^{N^{n-1}}]$ which is isomorphic to a quotient of $k[y_1 - y_n^N, ..., y_{n-1} - y_n^{N^{n-1}}]$, which is isomorphic to a polynomial ring in $n - 1$ variables. Applying induction on n, we can conclude the result.

□

Exercise 4. Let $R = \mathbb{F}_q[[t]]$ be the ring of power-series in the variable t over the field $\mathbb{F}_q$. As a set, R is the set of power-series $f = \sum_{n\in\mathbb{N}} a_n t^n$ with coefficients $a_n \in \mathbb{F}_q$. For two such power series, $\sum_{n\in\mathbb{N}} a_n t^n$ and $\sum_{n\in\mathbb{N}} b_n t^n$, one defines the addition to be the power-series $\sum_{n\in\mathbb{N}}(a_n + b_n)t^n$ and multiplication to be the power-series$\sum_{n\in\mathbb{N}}(\sum_{k=0}^n a_k b_{n-k})t^n$ Show the following:

(a) If $f \in R - (t)$, then f is invertible (and hence R is a local ring with maximal ideal (t)).
(b) 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 $f = \sum_{n\in\mathbb{Z}} a_n t^n$ where $a_n = 0$ for all but finitely many negative indices n. 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.
(c) 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
(d) Show that $\dim R = 1$ and hence show that Thm 5.1.11 does not work with not finitely generated algebras

Proof. (a) 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 $b_0 = \frac{1}{a_0}$ and $b_n = -\frac{1}{a_0}\sum_{i=1}^n a_i b_{n-i}$ for $n \geq 1$.
(b) 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. By the previous point $\mathrm{Frac}(R) = R_t$, but it is clear from the above definition that the ring of Laurent series is also equal to the ring R_t.

(c) 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 $\mathrm{Frac}(R)$ have 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 any algebraic extension. We now show that $\mathbb{F}_q(t_1, \dots, t_r)$ is countable. This can be seen by evaluating $f \in \mathbb{F}_q(t_1, \dots, t_r)$ at large enough primes $p_1, p_2, \dots p_r$, and in this way identifying a bijection between $\mathbb{F}_q(t_1, \dots, t_r)$ and a subset of the rational numbers. However R is not countable, for example the set of infinite sequences $(a_n)_{n\in\mathbb{N}}$ where $a_n \in \{0, 1\}$ is not countable. The latter is usually proven in order to show that the real numbers are uncountable and we will not repeat that argument here.

(d) We have that R is a domain and that $0 \in t$ for t maximal and it is clear that $0 \subset t$ is a maximal chain. Since t is the unique maximal ideal this shows $\dim R = 1$.

□

Exercise 5. Show the following:

(a) If R is a domain with $\dim R = 0$, then R is a field.

(b) We say that a ring R is reduced if there are no nilpotent elements in R. I.e., if $r \in R$ is such that $r^n = 0$ then $r = 0$. Give an example of a reduced ring R of dimension zero which is not a field.

Proof. (a) 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 it is of dimension zero.

(b) Let F be a field and define a ring structure on $F \oplus F$ by cordinatevise multiplication. There are two non-trivial ideals $0 \oplus F$ and $F \oplus 0$ and $0 = 0 \oplus 0 = 0 \oplus F \cap F \oplus 0$ and hence 0 is not an irreducible ideal and hence not prime. It is direct to see that 0 is the only ideal strictly contained in $0 \oplus F$, which itself is maximal $(F \oplus F/0 \oplus F = F)$. Any prime ideal p has to contain 0 and so $0 \oplus F \cap F \oplus 0 \subset p$ but then either $F \oplus 0 \subset p$ or $0 \oplus F \subset p$ which implies $p = 0 \oplus F$ or $F \oplus 0 = p$. Therefore $F \oplus F$ has exactly two prime ideals, which are both maximal. Suppose that $(a, b)^n = (a^n, b^n) = (0, 0)$ then $a^n = 0$ and $b^n = 0$, since F is reduced this means that $a = 0$, $b = 0$.

□

Exercise 6. ** *You should only hand in solutions to c, d and e. In proving points points c, d and e below you may freely use the results in a, b.*
Let R be an Artinian ring. Recall from Exercise 2.1 that every prime ideal of R is maximal

(a) Show that $\dim R = 0$.

(b) Show that R has finitely many maximal ideals.
Hint : for this you need the statement that if $I_1 \cap \dots \cap I_r \subseteq p$ for a prime ideal $p \subseteq R$, then $I_i \subseteq p$ for some i, which you should also show

(c) ** There is an integer $j > 0$ such that $\mathrm{nil}(R)^j = 0$.
Hint: Show that $nil(R)^j$ 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 point c.)

(d) **Show that if $m_1, \ldots, m_s$ are the maximal ideals of R, then $m_1^j \cdot \cdots \cdot m_s^j = 0$.
Hint: Use the statement learned in 'Anneaux et corps' that the nilardical is the intersection of all prime ideals.

(e) **Show that $\text{length}_R R < \infty$, and deduce that R is Noetherian.
Hint: construct an increasing sequence of ideals using the product 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 (5) of Example 2.1.2 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. (a) Let $P \subset Q$ be an inclusion of prime ideals, since P is maximal we have $P = Q$.

(b) We first show the hint: Suppose $I_i \not\subset p$ for all i. Then there exist $x_i \in I_i$, such that $x_i \notin p$ and therefore for $x = x_1 \cdots \cdots x_r$ we have $x \in I_1 \ldots I_r \subset I_1 \cap \cdots \cap I_r \subset P$, but this contradicts that P is prime. Now, for the exercise, we first remember that every maximal ideal is prime by the previous point. Consider the set of all finite intersections $m_1 \cap \cdots \cap m_n$ where the m_i are maximal ideals. This set has a minimal element, say $m_1 \cap \cdots \cap m_k$. By minimality we have for any maximal ideal m that $m \cap (m_1 \cap \cdots \cap m_k) = m_1 \cap \cdots \cap m_k$ and therefore $m_1 \cap \cdots \cap m_k \subset m$. By what we just showed $m_i \subset m$ for some i. By maximality this means that $m = m_i$.

(c) ** We have an ascending chain $\text{nil}(R) \supseteq \text{nil}(R)^2 \supseteq \text{nil}(R)^3 \supseteq \ldots$. By the Artinian property we have $\text{nil}(R)^j = \text{nil}(R)^{j+1}$ for some j. Let $I = \text{nil}(R)^j$, if $I^2 = 0$ 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 $IJ = J$. In order to apply Nakayama's Lemma point c) 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 c) to the finitely generated module J to conclude $J = 0$, this is a contradiction. Therefore, $\text{nil}(R)^j = 0$.

(d) **Every prime ideal in R is maximal. Hence $\text{nil}(R) = m_1 \cap \cdots \cap m_s$, where the m_i are distinct maximal ideals, i.e., $m_1 \cap \cdots \cap m_s = m_1 \cdot \cdots \cdot m_s$. It therefore follows from the previous point that $m_1^j \cdot \cdots \cdot m_s^j = 0$.

(e) ** Let $0 = m_1 \cdot \cdots \cdot m_n \subset m_2 \cdot \cdots \cdot m_n \subset \cdots \subset m_n \subset R$, for some not necessary distinct maximal ideals of R. We have a short exact sequence $0 \to m_n \to R \to R/m_n \to 0$, since R is Artinian so is m_n. Therefore, we conclude that $m_n \cdot m_{n-1} \cdot \cdots \cdot m_j$ is Artinian for all j as well as $m_n \cdot m_{n-1} \cdot \cdots \cdot m_j / m_n \cdot m_{n-1} \cdot \ldots m_j \cdot m_{j-1}$. The latter is a R/m_{j-1}-vector-space, hence being Artinian is equivalent to being Noetherian. Now we proceed to show that R is Noetherian. By the short exact sequence above it is sufficient to show that m_n is Noetherian. We prove this by descending induction on the number of terms in the intersection, we have that $0 = m_1 \cdot \cdots \cdot m_n$ is Noetherian. Suppose that $m_{n-k} \cdot \cdots \cdot m_n$ is Noetherian, since $m_{n-k+1} \cdot \cdots \cdot m_n / m_{n-k} \cdot \cdots \cdot m_n$ is Noetherian so is $m_{n-k-1} \cdot \cdots \cdot m_n$.

□

RINGS AND MODULES 2020
SHEET 10 SOLUTIONS

Joe Waldron, Emelie Arvidsson, Maciek Zdanowicz

emelie.arvidsson@epfl.ch

Exercise 1. 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

$$\cdot \otimes_R M : \{R\text{-modules}\} \to \{R\text{-modules}\}, \quad A \mapsto A \otimes_R M$$

is a right exact covariant functor.

Proof. We start by remarking on the functoriality, let $f : N \to N'$ be a morphism of R-modules. Let $\iota : N \oplus M \to N \otimes_R M$ and $\iota' : N' \oplus M \to N' \otimes_R M$ be the unique R-bilinear map in the definition of the tensor product. Let $\tilde{f} : N \oplus M \to N' \oplus M$ be defined by $\tilde{f}(n, m) = (f(n), m)$, then $\tilde{f}$ is obviously R-bilinear. The composition $\iota' \circ \tilde{f}$ defines a R-bilinear map $N \oplus M \to N' \otimes_R M$. By the universal property of $N \otimes_R M$ there exists a unique morphism $f \otimes 1 : N \otimes_R M \to N' \otimes_R M$ such that $\iota' \circ \tilde{f} = f \otimes 1 \circ \iota$. Defining $f \otimes 1$ to be the image of f is easily seen to be functorial and hence $\cdot \otimes_R M$ defines a covariant functor as claimed.

To show that it is right exact we will make use of the corresponding statement for the Hom-functors. Let us prove the existence of a natural bijection as described in the exercise. Let $f\colon M \oplus N \to P$ be an R-bilinear mapping. For each $x \in M$ the mapping $y \to f(x, y)$ of N into P is R-linear, hence f gives rise to a mapping $\Phi : M \to Hom_R(N, P)$ which is R -linear because f is linear in the variable x. Conversely any R-homomorphism $\Phi : M \to \mathrm{Hom}_R(N, P)$ defines a bilinear map, namely $(x, y) \to \Phi(x)(y)$. Hence the set S of R-bilinear mappings $M \oplus N \to P$ is in natural one-to-one correspondence with $\mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$. On the other hand the set S is in one-to-one correspondence with $\mathrm{Hom}_R(M \otimes_R N, P)$, by the defining property of the tensor product. Hence we have an isomorphism (which easily can be seen to be an isomorphism of R-modules) $\mathrm{Hom}_R(M \otimes_R N, P) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P))$. In fact it is *natural* i.e., functorial in M, N and P. For this exercise we only need functoriality in M.

We now proceed to show right exactness. Let

$$0 \to A \to B \to C \to 0$$

be an exact sequence of R-modules. We want to show that the sequence

$$A \otimes_R M \to B \otimes_R M \to C \otimes_R M \to 0$$

is exact. We let E denote the exact sequence, and let $E \otimes M$ denote the second sequence for which we want to prove exactness. We first claim that it is sufficient to prove that the sequence $Hom(E \otimes M, P)$ defined as

$$0 \to \mathrm{Hom}_R(C \otimes_R M, P) \to \mathrm{Hom}_R(B \otimes_R M, P) \to \mathrm{Hom}_R(A \otimes_R M, P)$$

is exact for every R-module P.

In fact, more generally:
The sequence

$$A \xrightarrow{\gamma} B \xrightarrow{\beta} C \to 0$$

of R-modules is exact if and only if for all R-modules P the sequence

$$0 \to \mathrm{Hom}_R(C,P) \xrightarrow{\circ\beta} \mathrm{Hom}_R(B,P) \xrightarrow{\circ\gamma} \mathrm{Hom}_R(A,P)$$

is exact. Only the first implication needs a motivation. Taking $P = C$ and $id \in \mathrm{Hom}_R(C,P)$ we find $\beta \circ \gamma = 0$. Take $P = Coker(\beta)$ and $q : C \to Coker(\beta) \in \mathrm{Hom}_R(C,P)$, injectivity of $\circ\beta$ implies that $q = 0$, i.e., β is surjective. Lastly, take $P = Coker(\gamma)$ and let $q : B \to P$ be the projection. Then $q \circ \gamma = 0$ and hence there exists $\phi : C \to P$ such that $ker(\phi\circ\beta) = im(\gamma)$. Consequently, $ker(\beta) \subset im(\gamma)$.

To conclude, we consider the following commutative diagram:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}_R(C \otimes_R M, P) & \longrightarrow & \mathrm{Hom}_R(B \otimes_R M, P) & \longrightarrow & \mathrm{Hom}_R(A \otimes_R M, P) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}_R(C, \mathrm{Hom}_R(M,P)) & \longrightarrow & \mathrm{Hom}_R(B, Hom_R(M,P)) & \longrightarrow & \mathrm{Hom}_R(A, Hom_R(M,P))
\end{array}$$

Where the vertical maps are the isomorphism discussed above and the horisontal maps are the ones induced by the short exact sequence E. We leave to the reader to check the commutativity of this diagram (i.e., the isomorphism $\mathrm{Hom}_R(N \otimes_R M, P) \cong \mathrm{Hom}_R(N, \mathrm{Hom}_R(M,P))$ is *natural* in N). Since E is exact, the bottom row in the above diagram is exact by left exactness of the Hom-functors. Commutativity of the diagram together with the vertical arrows being isomorphisms now imply exactness of the sequence $E \otimes M$.

□

Exercise 2. ** Let R be a ring. Let M, N be R-modules and I and ideal of R. Prove that there are isomorphisms of R-modules $M \otimes_R N \cong N \otimes_R M$ and $M \otimes_R (R/I) \cong M/(IM)$.

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 and hence induces a desired map. We construct the inverse by the analogous procedure.
(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

$$I \otimes_R M \to R \otimes_R M \to (R/I) \otimes_R M \to 0.$$

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 $(R/I) \otimes_R M$ is isomorphic to M/IM.

□

Exercise 3. Let A be a ring, with A-algebras B and C and an A-module M. Show that:

(a) $B \otimes_A M$ naturally has the structure of a B-module,
(b) $B \otimes_A C$ naturally has the structure of an A-algebra,
(c) $B \otimes_A B$ naturally has a ring morphism to B.

Proof. The solution consists of the following steps.

(a) $B \otimes_A M$ is a B module via extending linearly from the definition $b'(b \otimes m) = (b'b) \otimes m$. First we must check that this is well defined. This follows from:
- $b'((b_1 + b_2) \otimes m) = (b'b_1 + b'b_2) \otimes m = b'(b_1 \otimes m + b_2 \otimes m)$
- $b'(b \otimes (m_1 + m_2)) = b'b \otimes (m_1 + m_2) = b'b \otimes b_1 + b'b \otimes m_2$
- $b'ab \otimes m = b'(ab \otimes m) = b'(b \otimes am) = b'b \otimes am$.

Now it is enough to check that it satisfies the distributivity properties of modules, which is another easy check.

(b) $B \otimes_A C$ is an A-algebra via the multiplication $(b \otimes c)(b' \otimes c') = bb' \otimes cc'$. First check well defined. Then we need to check the associativity and distributivity properties, and also note that the unit in $B \otimes_A C$ is $1_B \otimes 1_C$. These are similar to the previous part.

(c) the ring homomorphism is induced by the A-bilinear map $B \times B \to B$ given by $(b, b') \mapsto bb'$. It is clealy compatible with the ring structure on the tensor product $B \otimes_A B$.v

□

Exercise 4. Prove the following assertions:

(a) Let k be a field, and let V_1 and V_2 be vector spaces over k with bases $\{e_1, ..., e_m\}$ and $\{f_1, ..., f_n\}$ respectively. Show that there is an isomorphism $V_1 \otimes_k V_2 \cong V_1^n$. In particular, show that $V_1 \otimes_k V_2$ has basis $\{e_i \otimes f_j\}$.
(b) Hence show that the element $e_1 \otimes f_2 + e_2 \otimes f_1$ cannot be written as $u \otimes v$ for any $u \in V_1$ and $v \in V_2$.

Proof. The solution consists of the following steps.

(a) Define a bilinear map $F : V_1 \times V_2 \to V_1^n$ by $F(v, \sum b_i f_i) = (b_i v)_i$. This determines a linear map $\phi : V_1 \otimes V_2 \to V_1^n$ which sends $v \otimes f_j$ to $(\delta_{jk} v)_k$. Define a converse $\psi : V_1^n \to V_1 \otimes V_2$ by $\psi((v_i)_i) = \sum_i v_i \otimes f_i$. This respects addition and scalar multiplication, so is a module homomorphism. We can compute that $\phi \circ \psi = id_{V_1^n}$ and $\psi \circ \phi = id_{V_1 \otimes V_2}$.
(b) Suppose we can write $e_1 \otimes f_2 + e_2 \otimes f_1 = u \otimes v$. Then writing $u = \sum a_i e_i$ and $v = \sum b_j f_j$ we get $e_1 \otimes f_2 + e_2 \otimes f_1 = \sum a_i b_j e_i \otimes f_j$. 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 5. Prove the following:

(a) Let R be a ring, and let I and J be two ideals such that $I + J = (1)$. Prove that $R/I \otimes_R R/J = 0$.
(b) Show that if $F \subset L$ is a field extension, $L \otimes_F L$ is a field if and only if $F = L$.

Proof. The solution consists of the following steps.

(a) Since $I+J=(1)$, there are two element $i \in I$ and $j \in J$ such that $i+j=1$. Let $m=\sum r_k \otimes r'_k$ be an element $R/I \otimes R/J$. Multiplying by $1=i+j$ and moving element j to the other side of the tensor product (using one of the defining relations) we see that

$$m=\sum ((i+j)r_k)\otimes r'_k = \sum ir_k \otimes r'_k + \sum r_k \otimes jr'_k = 0.$$

This implies that $R/I \otimes R/J = 0$.

(b) If $F=L$, then the ring in question is $F \otimes_F F$, and it holds for any ring R that $R \otimes_R R \cong R$.

Conversely, assume that $F \neq L$, 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 exercise (3), there is a ring homomorphism $\phi\colon L \otimes_F L \to L$ 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 a bilinear map $\theta : L \times L \to Z$ of F-modules for some F-module Z which has different values at $(l,1)$ and $(1,l)$, for the bilinear map factors through $L \times L \to L \otimes_F L$. As $L \neq F$, there is a non-trivial (not equal to the identity) F-module homomorphism $\phi : L \to L$. 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.

□

Exercise 6. Let R be a ring and M an R-module. We say that M is *flat* if for every short exact sequence of R-modules

$$0 \to A \to B \to C \to 0$$

the sequence

$$0 \to A \otimes_R M \to B \otimes_R M \to C \otimes_R M \to 0$$

is exact.

Prove that the following are equivalent:

(a) M is flat;
(b) $\operatorname{Tor}_i^R(A,M) = 0$ for every R-module A and every $i>0$;
(c) $\operatorname{Tor}_1^R(A,M) = 0$ for every R-module A.

Hint: for (a)⇒(b) take a free resolution of A and tensor it with M to compute the Tor functors. For (c)⇒(a) use the long exact sequence for left derived functors.

Proof. We follow the hint and consider a free resolution of A:

$$\ldots \to R^K \to R^I \to R^J \to A \to 0.$$

Since M is flat, we obtain an exact sequence

$$\cdots \to R^K \otimes_R M \to R^I \otimes_R M \to R^J \otimes_R M \to A \otimes_R M \to 0.$$

Therefore, $\operatorname{Tor}_i^R(A,M) = H^i(\cdots \to R^K \otimes_R M \to R^I \otimes_R M \to R^J \otimes_R M \to 0)$ is zero if $i \neq 0$.

The implication (b)⇒(c) is trivial.

For (c)⇒(a) we follow the second hint. Let

$$0 \to A \to B \to C \to 0$$

be an exact sequence of R-modules. By the theory of left derived functors there is a long-exact sequence

$$\cdots \to Tor^1(C, M) \to A \otimes_R M \to B \otimes_R M \to C \otimes_R M \to 0$$

Therefore, $Tor^1(C, M) = 0$ implies that M is flat. □

Exercise 7. Let R be a ring.

(a) Prove that free R-modules are flat.
(b) Prove that projective R-modules are flat.
Hint: use the characterization of projective modules as direct summands of free modules
(c) Assume that R is an integral domain. Determine for which ideals I of R the R-module R/I is flat.

Proof. The proof consists of the following steps.

(a) Let $M = R^I$ be a free R-module. We will prove that $\otimes_R M$ is exact. Note that $\otimes_R R$ is exact since for all R-modules A we have $A \otimes_R R \cong A$ as was described in the lecture. Since $\otimes_R M$ is an additive functor (Exercise Sheet 7, Exercise 7) it is the direct sum of the exact functors $\otimes_R R$.
Let

$$0 \to A \to B \to C \to 0$$

be an exact sequence of R-modules. We want to show that the sequence

$$0 \to A \otimes_R M \to B \otimes_R M \to C \otimes_R M \to 0$$

is exact.
Since right-exactness has already been proven it is sufficient to prove that if $0 \to A \xrightarrow{f} B$ is exact then $0 \to A \otimes_R M \xrightarrow{f \otimes 1_M} B \otimes_R M$ is exact. But the latter sequence is isomorphic to the sequence $0 \to \oplus^I (A \otimes_R R) \xrightarrow{\oplus (f \otimes 1_R)} \oplus^I (B \otimes_R R)$ by additivity of the tensor product. Under the isomorphism $A \otimes_R R \cong A$ this is just the injection $0 \to \oplus^I A \xrightarrow{\oplus f} \oplus^I B$ which maps $(a_i)_i$ to $(f(a_i))_i$.
(b) Suppose M is projective and let M' be an R-module such that $M \oplus M' \cong R^I$. Let $f : A \to B$ be injective, then $f \otimes 1_{M \oplus M'} : A \otimes (M \oplus M') \to B \otimes (M \oplus M')$ is injective by part a) of this exercise. By additivity of the tensor product $(f \otimes 1_M) \oplus (f \otimes 1_{M'}) : (A \otimes M) \oplus (A \otimes M') \to (B \otimes M) \oplus (B \otimes M')$ is injective. Suppose $a \in ker(f \otimes 1_M)$ then $(a, 0) \in ker(f \otimes 1_M \oplus f \otimes 1_{M'})$, i.e., $a = 0$. This proves that M is flat.
(c) If $I = 0$ then $R/I = R$ is flat. If $I = R$ then $R/I = 0$, the zero module is flat over every ring since it sends every module and every morphism to zero. We will show that R/I is only flat 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 tensor with $\otimes_R R/I$ we obtain $m_a \otimes 1 : R/I \to R/I$ which maps $\overline{r}$ to $\overline{ar} = 0$, i.e., $m_a \otimes 1$ is the zero map, which is not injective since $I \neq R$, hence R/I is not flat.

□

RINGS AND MODULES 2020
SHEET 11 SOLUTIONS

Joe Waldron, Emelie Arvidsson, Maciek Zdanowicz

emelie.arvidsson@epfl.ch

Exercise 1. 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.

Proof. Let $f : T^{-1}R \otimes M \to T^{-1}M$ be defined as being induced from the bilinear map $\phi : T^{-1}R \oplus M \to T^{-1}M$ given by $\phi(\frac{r}{t}, m) = \frac{rm}{t}$, that the latter is well-defined and bilinear is direct. We define an inverse to f, and we show this is well defined. So let $g(\frac{m}{t}) = \frac{1}{t} \otimes m$ for $m \in M$ and $t \in T$. This will be the inverse if it gives a well defined R-homomorphism. Suppose that $\frac{m_1}{t_1} = \frac{m_2}{t_2}$. Then there is $t' \in T$ such that $t'(t_2m_1 - t_1m_2) = 0$. Thus $\frac{1}{t_1} \otimes m_1 = \frac{t't_2}{t't_2t_1} \otimes m_1 = \frac{1}{t't_2t_1} \otimes t't_2m_1 = \frac{1}{t't_2t_1} \otimes t't_1m_2$, 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 an R-homomorphism we must show that it respects addition and scalar multiplication. Multiplication is clear. For addition, $g(\frac{m_1}{t_1} + \frac{m_2}{t_2}) = g(\frac{t_2m_1 + t_1m_2}{t_1t_2}) = \frac{1}{t_1t_2} \otimes (t_2m_1 + t_1m_2) = \frac{1}{t_1t_2} \otimes t_2m_1 + \frac{1}{t_1t_2} \otimes t_1m_2 = \frac{1}{t_1} \otimes m_1 + \frac{1}{t_2} \otimes m_2$ as required. Therefore this is an isomorphism of R-modules.

To show that it is an isomorphism of $T^{-1}R$ modules, it is enough to show that f and g respect the $T^{-1}R$-module structures. This is clear from the definitions. (The $T^{-1}R$-module structure on $T^{-1}R \otimes_R M$ is given by $\frac{r}{t}(\frac{r'}{t'} \otimes m) = \frac{rr'}{tt'} \otimes m$, as a special case of Question 3 in Sheet 8.)

□

Exercise 2. Let R be a ring with multiplicative subset T, and suppose that L, M and N are R-modules.

(a) Show that if there is an R-module homomorphism $f : M \to N$ then there is a natural $T^{-1}R$-module homomorphism $f_T : T^{-1}M \to T^{-1}N$.
(b) Show that there is an isomorphism of R-modules $T^{-1}(M \oplus N) \cong (T^{-1}M) \oplus (T^{-1}N)$.
(c) 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 $T^{-1}(M/L) \cong (T^{-1}M)/(T^{-1}L)$ and that localization by T is an exact functor of R-modules and that $T^{-1}R$ is a flat R-module.
(d) Let p be a prime ideal of R. Show that there is an isomorphism of rings $\mathrm{Frac}(R/p) \cong R_p/(pR_p)$.

Remark: For a local ring A with maximal ideal m we call A/m the residue field of A

Proof. a) and b) follows from the isomorphism $T^{-1}M \cong M \otimes_R T^{-1}R$, since $\otimes_R T^{-1}R$ is a right-exact additive covariant functor. To prove c) it is sufficient to prove that if $g : L \to M$ is injective then $g_T : T^{-1}L \to T^{-1}M$ is injective. To this end, suppose that $g_T(\frac{l}{t}) = 0$. Then there is $t' \in T$ such that $t'g(l) = 0$. But this is equal to $g(t'l)$ and so $t'l = 0$ by injectivity of g. This implies that $\frac{l}{t} = 0$.
For d) we see that by part c) $R_p/(pR_p) \cong T^{-1}(R/p)$ for $T = R - p$. By definition $Frac(R/p) = T^{-1}(R/p)$. □

Exercise 3. Let $R = F[x]$, where F is a field.

(a) If F is algebraically closed, then show that for every prime ideal p of R, either $R_p \cong F(x)$ or $R_p \cong F[x]_{(x)}$, where these isomorphisms are isomorphisms of F-algebras. Show that the above two cases are not isomorphic.
(b) If $F = \mathbb{R}$, then show that up to ring isomorphism there are three possibilities for R_p, where 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
(c) Show that if F is algebraically closed, then $F[x, y]$ has infinitely many prime ideals p for which $F[x, y]_p$ are pairwise non-isomorphic F-algebras. For this, you can use the following theorem of algebraic geometry:

Theorem 3.1. *For each integer $d \in \mathbb{N}\backslash\{0, 2\}$, there exist irreducible polynomials $f_d \in F[x, y]$ (of degree d) such that* $\mathrm{Frac}(F[x, y]/(f_d))$ *are non-isomorphic as F-algebras for different $d's$.*

Proof. (a) 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 $F[x]_{(x)} \cong F[x]_{(x-a)}$ for all $a \in F$. We define a ring-homomorphism $f : F[x]_{(x)} \to F[x]_{(x-a)}$ by a linear variable change sending x to $x-a$. This is well-defined, i.e., if $g(x) \notin (x)$ then $g(x-a) \notin (x-a)$ moreover, if there exists $s, g, g' \notin (x)$ and polynomials f, f' such that $s(x)(g(x)f(x) - f'(x)g'(x)) = 0$, then $s(x-a)(g(x-a)f(x-a) - f'(x-a)g'(x-a)) = 0$, where $s(x-a) \notin (x-a)$, it is clearly a F-algebra homomorphism, i.e., it is the identity on constants and for two fraction of polynomials $\frac{f}{g}$ and $\frac{f'}{g'}$ we have $\frac{ff'}{gg'}(x-a) = \frac{f}{g}(x-a)\frac{f'}{g'}(x-a)$. The inverse is given by the linear variable change $x \to x + a$, which is well-defined by a similar reasoning. There is an inclusion $F[x]_{(x)} \to F(x)$, since the former is not a field but the latter is they can not be isomorphic.
(b) 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. There is a linear change of coordinates that take any linear polynomial $(x - a)$ into the polynomial x ($x \to x + a$) and any degree two polynomial with no real roots ($(x - (a + ib))(x - (a - ib))$ for $b \neq 0$) into the polynomial $b^2(x^2 + 1)$ where $b \in \mathbb{R}$ (i.e., $x \to bx + a$). As above, these linear coordinate changes defines isomorphisms of $\mathbb{R}$-algebras $\mathbb{R}[x]_{(x-a)} \cong \mathbb{R}[x]_{(x)}$, $\mathbb{R}[x]_{(x^2-2a+b^2+a^2)} \cong \mathbb{R}[x]_{b^2(x^2+1)} = \mathbb{R}[x]_{(x^2+1)}$. The residue fields are $\mathbb{R}(x)$, $\mathbb{R}$ and $\mathbb{C}$ respectively, since any isomorphism between two of these rings would induce an isomorphism on residue fields (here you need to check that any isomorphism would map the generators of the maximal ideals to each other, this sort of argument is given in c) below) they can not be isomorphic.

(c) Let f_d be as in the theorem, we will show that $F[x,y]_{f_d}$ are non-isomorphic for $d \in \mathbb{N} \setminus \{0,2\}$. Let $\phi : F[x,y]_{f_d} \to F[x,y]_{f_{d'}}$ be an isomorphism. It is sufficient to prove $\phi(f_d) = r f_{d'}$, for a unit r since if this is a case ϕ induces an isomorphism on residue fields, which is a contradiction to the theorem. First we note that $\phi(f_d)$ can not be a unit since othervise there exists $f \in F[x,y]_{f_d}$ such that $\phi(f_d)\phi(f) = 1$, i.e., $\phi(f_d f) = \phi(1)$, which by injectivity means that f_d is a unit. Therefore, $\phi(f_d) = r {f_{d'}}^n$ for a unit r and some non-negative integer n. Applying, ϕ^{-1} gives that $f_d = r'\phi^{-1}(f_{d'})^n$ for some unit r', by the discussion above applied to ϕ^{-1} there exists a non-negative integer m such that up-to multiplication of units $\phi^{-1}(f_{d'}) = f_d^m$, this implies that $n = m = 1$.

□

Exercise 4. Let F be an algebraically closed field.

(a) List the prime ideals of $R = F[x,y]/(xy)$
Hint: Consider the implications of a containment $xy \in P$, for a prime ideal P. Consider the projections $R \to R/x$ and $R \to R/y$ and use that you know the prime ideals of $F[y]$ and $F[x]$.
(b) Show that for all prime ideals p of R, R_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 of which is not a domain.

Proof. (a) The prime ideals of $R = F[x,y]/(xy)$ corresponds to prime ideals inside $F[x,y]$ containing xy, these are (x) and (y) (note if $xy \in P$ for P prime then either $(x) \subset P$ or $(y) \subset P$) and all prime ideals containing (x) and (y) respectively. The latter are, for all $a \in F$, the ideals $(x, y-a)$ and $(x-a, y)$. To see that the latter are really all, we consider $R \to R/x$ and $R \to R/y$ respectively and we use the correspondence between prime ideals P of R above (x) and the prime ideals of $R/x \cong F[y]$. In the principal ideal domain $F[y]$ every prime ideal is generated by an irreducible polynomial f, since every polynomial f has a root in F (since F is algebraically closed) we have $f = (x-a)$.
(b) We have $(F[x,y]/(xy))_{(\overline{x})} \cong F[x,y]_{(x)}/(xy)F[x,y]_{(x)} \cong F[x,y]_{(x)}/(x)F[x,y]_{(x)} = F[y]_0 = F(y)$. Suppose that $a \neq 0$ then we have $(F[x,y]/(xy))_{(}\overline{x}, \overline{y-a}) \cong F[x,y]_{(x,y-a)}/(xy)F[x,y]_{(x,y-a)} \cong F[x,y]_{(x,y-a)}/(x)F[x,y]_{(x,y-a)}$ since y is a unit. But $F[x,y]_{(x,y-a)}/(x)F[x,y]_{(x,y-a)} \cong F[y]_{(y-a)}$. Finally, $(F[x,y]/(xy))_{(\overline{x},\overline{y})}$ is not a domain since neither y nor x is a unit and $xy = 0$. I.e., up-to a linear coordinate change we have $R_p = F(y)$ a field, $R_p = F[y]_{(y-a)}$ which is a domain but not a field and $R_p = (F[x,y]/(xy))_{(\overline{x},\overline{y})}$ which is not a domain.

□

Exercise 5. Let M be an A-module, and let $\mathfrak{a}$ be an ideal in A. Show that the following are equivalent:

(a) $M = 0$,
(b) $M_{\mathfrak{m}} = 0$, for every maximal ideal $\mathfrak{m}$,
(c) $M_{\mathfrak{p}} = 0$, for every prime ideal $\mathfrak{p}$.

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 maximal ideals satisfying $\mathfrak{a} \subset \mathfrak{m}$.

Proof. . The implications $a \implies b \implies c$ is obvious. Assume that $M \neq 0$ but that $M_{\mathfrak{p}} = 0$, for every prime ideal $\mathfrak{p}$. Then there exists $x \neq 0 \in M$, in particular $Ann(x) \neq A$. Consider the inclusion $Ax \hookrightarrow M$. Let m be a maximal ideal

containing $Ann(x)$. By assumption $M_m = 0$ and hence $A_m x \hookrightarrow M_m$ is the zero map, by exactness of localization we therefore must have $A_m x = 0$, i.e., there exists $s \in A - m$ such that $sx = 0$. This is a contradiction since $Ann(x) \subset m$.

We have $M = aM$ if and only if $M/aM = 0$ which by the exercise is equivalent to $(M/aM)_m = 0$ for every maximal ideal m of A. By the previous exercise $(M/aM)_m \cong M_m/aM_m$ and the latter is zero iff $M_m = aM_m$. If a is not contained in the maximal ideal m then a contains a unit of A_m and $M_m = aM_m$. Therefore, $M = \mathfrak{a}M$ if and only if $M_{\mathfrak{m}} = aM_m$ for maximal ideals satisfying $\mathfrak{a} \subset \mathfrak{m}$, if $M_m = 0$ for such ideals then the equality holds. Conversely, suppose $a \subset m$ and that $M_m = aM_m$ then obviously $M_m = mM_m$ and therefore Nakayamas Lemma applied to the finitely generated A_m-module M_m implies that $M_m = 0$.

□

Exercise 6. Let R be a ring.

(a) Let $T \subseteq R$ a multiplicatively closed subset of R. Let q be a prime ideal of $T^{-1}R$. Let q^c be the contraction of q under $R \to T^{-1}R$. Prove that $\mathrm{ht}(q) = \mathrm{ht}(q^c)$.
(b) Let p be a prime ideal of R. Prove that $\mathrm{ht}(p) = \dim R_p$.

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.

(a) Prime ideals of $T^{-1}R$ are in 1-1 correspondence with prime ideals of R that do not intersect T.
(b) Prime ideals of R_p are in 1-1 correspondence with prime ideals of R contained in p.

□

RINGS AND MODULES 2020
SHEET 12 SOLUTIONS

Exercise 1. Let $S \to R$ be a morphism of rings. Show that a prime ideal p of S is the contraction of a prime ideal of R if and only if $p^{ec} = p$.

Hint: for one direction use ideas from the proof of "going-up" theorem

Exercise 2. Let R be a ring and $I \subset R$ be an ideal. Prove that the radical $\sqrt{I}$ of I is an ideal. Prove that if there is a containment $I \subset P \subset \sqrt{I}$ for a prime ideal P then $P = \sqrt{I}$.

Exercise 3. Let F be an algebraically closed field.

Let I, J be ideals of $R = F[x_1, ..., x_n]$. Prove that $\sqrt{I} \subset \sqrt{J}$ if and only if $Z(J) \subset Z(I)$.

Exercise 4. Let F be an algebraically closed field. Let $R = F[x_1, ..., x_n]$ and let I and J be ideals of R. Show that

(a) $Z(I) \cup Z(J) = Z(I \cap J) = Z(IJ)$
(b) $Z(I) \cap Z(J) = Z(I + J)$

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. Find $I(Z)$.

Hint: make sure you have everything!

Exercise 6. (a) Let F be an algebraically closed field, and $X \subseteq F^n$ an algebraic set with ideal $I = I(X)$. Define the coordinate ring $A(X)$ of X to be $F[x_1, \ldots, x_n]/I$. If $X = Z(I) \subseteq F^n$, and $Y = Z(J) \subseteq F^m$ are algebraic sets with $I = I(X)$ and $J = I(Y)$, then a morphism $f : X \to Y$ is defined to be a vector $(h_1, \ldots, h_m)$ of polynomials $h_i \in F[x_1, \ldots, x_n]$, such that for every $\underline{a} \in X$, $(h_1(\underline{a}), h_2(\underline{a}), \ldots, h_m(\underline{a})) \in Y$.

Show that whenever there is a morphism $f : X \to Y$ of algebraic sets as defined above there is a unique homomorphism of rings $\lambda_f : A(Y) \to A(X)$, such that the following diagram commutes.

$$\begin{array}{ccc} F[y_1, \ldots, y_m] & \xrightarrow{y_i \mapsto h_i} & F[x_1, \ldots, x_n] \\ \downarrow & & \downarrow \\ A(Y) & \xrightarrow{\lambda} & A(X) \end{array}$$

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 $h_i(x_1, ..., x_n)$.

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

(c) Compute the integral closure R_1 of $S_1 := F[x, y]/(y^2 - x^3 - x^2)$ in the fraction field of S_1.

(d) Let R_1 and S_1 be as above. Let $S_2 := F[x, y, z]/(x^2 - y^2 z)$ and denote by R_2 the integral closure of S_2 inside its field of fractions (R_2 was computed in lectures).
For $i = 1, 2$, define the conductor ideal $\mathcal{I}_i$ to be the ideal in S_i which is the annihilator of the S_i-module R_i/S_i. Calculate $\mathcal{I}_i$ for $i = 1, 2$.

(e) With the notation as above, let $Y_i \to X_i$ be the morphisms of algebraic sets induced by the inclusion $S_i \to R_i$ for $i = 1, 2$. Assuming that $k = \mathbb{C}$, draw the real points of the X_i. Draw also in $Z(\mathcal{I}_i + I(X_i))$[1]. What do you notice about $Z(\mathcal{I}_i + I(X_i)) \subset X_i$?

Exercise 7. 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 co-ordinate ring is R. Noether normalisation says there is a subring $S \subset R$ 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 ϕ of algebraic sets. Prove that the fibres of ϕ are finite, i.e., the preimage of any point in F^r under ϕ consis of a finite set of points in X.

Exercise 8. Let F be an algebraically closed field.

Let X be an algebraic set in $F[x_1, ..., x_n]$ with $I(X) = I$. Prove that points of F^n contained in X are naturally in bijection with maximal ideals of $F[x_1, ..., x_n]/I$.

Exercise 9. Let F be an algebraically closed field.

Calculate the Krull dimension of the ring

$$F[w, x, y, z]/(x^2 - wy, y^2 - xz, wz - xy).$$

[1]This is equal to the subset of X_i in k^n which is the vanishing locus of the functions in $\mathcal{I}_i$

RINGS AND MODULES 2020
SHEET 13 SOLUTIONS

Exercise 1. *Let $R = \mathbb{C}[x, y, z]$ and $I = (xy - z^2, x^2 - y^2)$. Identify $\mathrm{V}(I) \subset \mathbb{C}^3$. You should see that this naturally breaks into smaller algebraic sets. What are the ideals of each piece? How do they relate to I?*

Proof. A point $(p, q, r) \in \mathbb{C}^3$ is in $\mathrm{V}(I)$ 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

$$\mathrm{V}(I) = \{(p, p, p) : p \in \mathbb{C}\} \cup \{(p, p, -p) : p \in \mathbb{C}\} \cup \{(p, -p, ip) : p \in \mathbb{C}\}$$
$$\cup \{(p, -p, -ip) : p \in \mathbb{C}\}$$

The ideals of these four pieces are $(x - y, x - z)$, $(x - y, x + z)$, $(x + y, x - iz)$ and $(x + y, x + iz)$ respectively. Each is a prime ideal which strictly contains the ideal I.

□

Exercise 2. *Let F be an algebraically closed field. Let U and V be algebraic sets in F^n.*

(a) Prove that $I(U \cup V) = I(U) \cap I(V)$

(b) By considering $U = \mathrm{V}(x^2 - y)$ and $V = \mathrm{V}(y)$ for the ideals $(x^2 - y)$ and (y) in $F[x, y]$, show that it need not be true that $I(U \cap V) = I(U) + I(V)$.

(c) Prove that in general, $\sqrt{I(U) + I(V)} = I(U \cap V)$.

Proof. (a) Suppose $f \in I(U \cup V)$. Then $f(P) = 0$ for all $P \in U$ and all $p \in V$. So $f \in I(U)$ and $f \in I(V)$. Conversely, suppose $f \in I(U)$ and $f \in I(V)$. Then $f(P) = 0$ for all $P \in U$ and all $P \in V$. Therefore $f \in I(U \cup V)$.

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

(c) This follows from a question on the previous exercise sheet and the Nulstellensatz. In particular, let $I = I(U)$ and $J = I(V)$, so $\mathrm{V}(I) = U$ and $\mathrm{V}(J) = V$. By the last exercise sheet $I(U \cap V) = I(\mathrm{V}(I + J))$. But by the Nulstellensatz, $I(\mathrm{V}(I + J)) = \sqrt{I + J}$.

□

Exercise 3. *Let F be an algebraically closed field. Calculate a primary decomposition for the ideals:*
(a) $(x^4 - 2x^3 - 4x^2 + 2x + 3) \subset F[x]$
(b) $(x^2, xy^2) \subset F[x.y]$
(c) $(x^2, xy, xz, yz) \subset F[x, y, z]$

Proof. (a) Factorising 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.

(b) 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.

(c) It may help to first calculate the irreducible components of $\mathrm{V}(I)$ 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. So two elements of the primary decomposition will have associated primes (x, y) and (x, z). Geometrically these components consist of the z-axis intersected with the y-axis. When intersecting these two ideals we get:

$$(x, y) \cap (x, z) = (x, yz)$$

Now take a look to see if we can make I by intersecting something with this and spot that $(x, y, z)^2$ does the job. Since the radical of $(x, y, z)^2$ is (x, y, z) which is maximal, we conclude that $I = (x, y) \cap (x, z) \cap (x, y, z)^2$ is a primary decomposition for I.

□

Exercise 4. *Let $S \subseteq R$ be a multiplicative subset and let I_i be finitely many ideals in R. By extension and contraction of ideals we shall mean extension and contraction via the natural morphism $R \to S^{-1}R$. Prove the following:*
(a) $(\bigcap_i I_i)^{ec} = \bigcap I_i^{ec}$

(b) $(\bigcap_i I_i)^e = \bigcap I_i^e$
(c) $S^{-1}(R/I) \cong S^{-1}R/I^e$, *where the localization on the left is localization of an R-module*
(d) *If I is primary, and $u \notin \sqrt{I}$, then $(I : u) = I$*
(e) *For an ideal I of a ring R admitting a finite primary decomposition let $I = \cap I_i$ be such a primary decomposition, show the following:*
  (a) $I^e = \bigcap_{p \supseteq I_i} I_i^e$
  (b) $I^{ec} = \bigcap_{p \supseteq I_i} I_i$
(f) *From now, let $R = F[x, y]$ for a field F, $I_1 = (x)$, $I_2 = m^s$ where $m = (x, y)$ and $s > 1$ is some integer, $I_3 = (x, y - 1)^2$ and $p \subseteq R$ is a prime ideal for which we set $S = R \setminus p$.*
  (a) *if $p = (x)$, then $S^{-1}(R/(I_1 \cap I_2 \cap I_3)) \cong F(y)$ as an R-module*
  (b) *if $p = (x, y)$, then $S^{-1}(R/(I_1 \cap I_2 \cap I_3)) \cong S^{-1}R/(I_1^e \cap I_2^e)$*
  (c) *if $p = (x, y)$, compute the smallest integer n such that $\left(\frac{x}{1}\right)^n \in S^{-1}(R/(I_1 \cap I_2 \cap I_3))$ is zero.*

Proof. (a) $(\bigcap_i I_i : u) = \bigcap_i (I_i : u)$ by Prop 7.5.19.(1) , and then we use Prop 6.3.9.(2), but there's still to prove $\bigcup_{u \in S} \bigcap_i (I_i : u) = \bigcap_i \bigcup_{u \in S} (I_i : u)$, for which we have to show that if $a \in (I_i, u_i)$ for diffferent $u_i \in S$, then there is a common u, but for that we can take $u = \prod_i u_i$

(b) By Prop 6.3.9.(1) two ideals of $S^{-1}R$ are equal if their contractions are equal. This follows from the previous point using that contraction commutes with intersection.

(c) It is not difficult to see that I^e is naturally isomorphic via a unique isomorphism with $S^{-1}I$, now the result follows from applying the exact functor $S^{-1}(\_)$ to the exact sequence:

$$0 \to I \to R \to R/I \to 0$$

(d) $t \in (I : u) \Rightarrow tu \in I \Rightarrow t \in I$, where in the last implication we used that no power of u is in I

(e) Let $I = \cap I_i$ be such a primary decomposition.
  (a) From a previous exercise $I^e = \bigcap I_i^e$, but for I_i not contained in p we have $I_i^e = S^{-1}R$.
  (b) Since $S^{-1}R^c = R$ it follows from above that $I^{ec} = \bigcap_{p \supseteq I_i} I_i$

(f) We begin by calculating a set of generators of $I_1 \cap I_2 \cap I_3$. We have $I_1 \cap I_2 = (x^k y^{s-k})_{k \geq 1}$. $I_3 = (x^2, x(y-1), (y-1)^2)$. Therefore,

$$I_1 \cap I_2 \cap I_3 = ((x^k y^{s-k})_{k \geq 2}, x(y-1)y^{s-1}).$$

With this at hand it is easy to solve the exercise:
  (a) We have

$$S^{-1}(R/(I_1 \cap I_2 \cap I_3) = (S^{-1}R)/(I_1 \cap I_2 \cap I_3)^e = (S^{-1}R)/(I_1)^e,$$

where the last equality comes from that y and $y-1$ are both units in $S^{-1}R$ and hence

$$(I_1 \cap I_2 \cap I_3)^e = ((x^k y^{s-k})_{k\geq 2}, x(y-1)y^{s-1})^e = (x)^e.$$

Finally the last quotient is just the residue field of $S^{-1}R$, so it is $F(y)$.

(b) We have that $y-1$ is a unit in $S^{-1}R$, hence $(I_1 \cap I_2 \cap I_3)^e = ((x^k y^{s-k})_{k\geq 2}, x(y-1)y^{s-1})^e = ((x^k y^{s-k})_{k\geq 1})^e = (I_1 \cap I_2)^e$, which is what we wanted to prove (here we use the previous exercise b)).

(c) $S^{-1}(R/(I_1 \cap I_2 \cap I_3) = (S^{-1}R)/(I_1^e \cap I_2^e)$, so $\frac{x^s}{1}$ is zero as $x^s \in I_1 \cap I_2$. For $j < s$ we have $x^j \notin I_1 \cap I_2$, and $I_1^{ec} \cap I_2^{ec} = I_1 \cap I_2$ so it follows that $\frac{x^j}{1} \notin I_1^e \cap I_2^e$. Therefore s is the smallest integer n such that $(\frac{x}{1})^n = 0$.

□