EPFL - Fall 2024 | Domenico Valloni
Rings and modules | **Exercises**
Sheet 9 - Solutions

Exercise 1. Show the following:

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

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

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

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

Exercise 2. Show the following:

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

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

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

□

Exercise 3. Solve the following exercises:

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

Proof. (1) By Exercise 1.2 of Sheet 1, every prime ideal in an Artinian ring is maximal. Hence every prime ideal has height 0, and thus an Artinian ring has dimension 0.
(2) The ring $\mathbb{Z}[x]/(4, x^2)$ is finite as a set (as a $\mathbb{Z}$-module it is isomorphic to $(\mathbb{Z}/4\mathbb{Z})^{\oplus 2}$), so in particular Artinian. Hence by the previous point, it has dimension 0.
(3) We will show that for any PID R, we have $\dim R[x] = 2$. This will require some serious work!
- Let $\pi \in R$ be a non-zero prime element (R is not a field). We then have an chain of inclusions
$$0 \subseteq (\pi) \subseteq (\pi, x)$$
and each ideal is prime. Indeed, the quotients are respectively $R[x]$, $R/(\pi)[x]$ and $R/(\pi)$ which are all domains. Thus, the height of (π, x) is at least 2, and hence $\dim(R[x]) \geq 2$.
- Let us start by studying prime ideals of height 1. We will show that if $\mathfrak{p}$ is a non-zero prime ideal of $R[x]$, then $\mathfrak{p}$ has height 1 if and only if it is principal.
Since R is a PID, it is in particular a UFD, so by Gauss' lemma $R[x]$ is also a UFD. Therefore by Exercise 1.2 any prime ideal of height 1 is principal. To see the converse, let $\mathfrak{p} = (p)$ be a principal prime ideal of $R[x]$, and let $\mathfrak{q} \subseteq \mathfrak{p}$ be a prime sub-ideal. We want to show that if $\mathfrak{q} \neq 0$, then $\mathfrak{q} = \mathfrak{p}$.
By the same argument as in Exercise 1.2 there would exist a non-zero prime element $q \in \mathfrak{q}$. But then, p divides q, so they must be equal, i.e. $\mathfrak{q} = \mathfrak{p}$.

□

Exercise 4. Let R be a PID which is not a field. The goal of this exercise is to show that $\dim R[x] = 2$ (in particular $\dim k[x, y] = 2$).

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

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

Proof. - Let $\pi \in R$ be a non-zero prime element (R is not a field). We then have an chain of inclusions
$$0 \subseteq (\pi) \subseteq (\pi, x)$$

and each ideal is prime. Indeed, the quotients are respectively $R[x]$, $R/(\pi)[x]$ and $R/(\pi)$ which are all domains. Thus, the height of (π, x) is at least 2, and hence $\dim(R[x]) \geq 2$.

- Since R is a PID, it is in particular a UFD, so by Gauss' lemma $R[x]$ is also a UFD. Therefore by Exercise 2.2 any prime ideal of height 1 is principal. To see the converse, let $\mathfrak{p} = (p)$ be a principal prime ideal of $R[x]$, and let $\mathfrak{q} \subseteq \mathfrak{p}$ be a prime sub-ideal. We want to show that if $\mathfrak{q} \neq 0$, $\mathfrak{q} = \mathfrak{p}$.

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

  Now let us deal with the case $q \in R$. Then q is a primitive polynomial, and hence by Gauss' lemma it gives an irreducible polynomial in $K[x]$. Therefore $(q) = \mathfrak{q}^e$ is a maximal ideal in $K[x]$. Since $\mathfrak{q}^e \subseteq \mathfrak{p}^e$, we are left to show that $\mathfrak{q}^e \neq \mathfrak{p}^e$. If it was the case, then for any $a \in \mathfrak{p}$, $a \in \mathfrak{q}^e = (q)$, so we can write

$$a = \frac{q}{r}$$

  with $r \in R$. Thus gives $ra = q$, and since q is primitive, r must be a unit. Therefore this would imply $\mathfrak{p} = \mathfrak{q}$, but this is impossible since $\mathfrak{p}$ has height 2.

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

$$1 = \sum_i \frac{a_i}{b_i} p_i$$

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

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

□

Exercise 5 (Nakayama's Lemma)**.** Let R be a ring and let M be a finitely generated R-module. Show the following:

(1) Let I be an ideal of R such that $IM = M$. Then there exists $x \in 1 + I$ such that $xM = 0$.
[*Hint:* The proof is similar to the direction (3) $\Rightarrow$ (1) in Proposition 6.2.3 of the lecture notes.]

(2) Suppose now that the ring R is local, i.e., that there is a unique maximal ideal $\mathfrak{m}$ of R. Show that if $\mathfrak{m}M = M$, then $M = 0$.

(3) For a ring R denote by $\mathrm{Jac}(R)$ the intersection of all maximal ideals of R; this is called the *Jacobson radical* of R (note also that $\mathrm{nil}(R) \subseteq \mathrm{Jac}(R)$). Show that if there is an ideal $I \subset \mathrm{Jac}(R)$ such that $IM = M$, then this implies that $M = 0$. This generalizes the previous point to any ring.

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

Remark 0.1. Nakayama's lemma is a **EXTREMELY** powerful tool in commutative algebra and algebraic geometry, so keep it mind this exists. You should really (really) remember it!

To give a hint of its tremendous power, recall you had an exercise about showing that if R is a commutative ring, M a finitely generated module and $f\colon M \to M$ a surjective endomorphism, then f is an isomorphism. Actually, the statement follows immediately by considering M as an $R[x]$-module via $x \cdot m = f(m)$, and taking $I = (x)$ in (1).

Recall that when you proved it in an early exercise sheet, you had a Noetherian assumption on R (and it was fundamental to the proof, have fun trying to prove it directly without this assumption!). With this argument, you don't need it!

Proof. (1) Let $m_1, ..., m_n$ be generators of M. As $IM = M$, we can express every $m \in M$ as an I-linear combination of $m_1, ..., m_n$. In particular, there is a matrix A with entries in I such that $A\underline{m} = \underline{m}$, where $\underline{m} \in M^{\oplus n}$ is the column vector with i^{th} entry m_i. Therefore $(\mathrm{Id}_n - A)\underline{m} = 0$. Multiplying by the adjugate of the matrix $A - \mathrm{Id}_n$ implies that if $x := \det(\mathrm{Id}_n - A)$ then $xm_i = 0$ for all i. Hence $xM = 0$, since the m_i's generate M. If we can prove that $x \in 1 + I$ then we are done. By expanding the determinant, we have

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

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

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

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

□

Exercise 6. Let R be a commutative ring which is an integral domain but not a field, and let F be the fraction field of R. Show that F is not finitely generated as an R-module.

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

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

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

Exercise 7. Let $R = \mathbb{F}_q[[t]]$ be the ring of power-series in the variable t over the finite field with q elements $\mathbb{F}_q$.

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

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

Now let us go to the actual exercise:

(3) Show that $\mathrm{trdeg}_{\mathbb{F}_q}(\mathrm{Frac}(R))$ is infinite.
[*Hint*: show that $\mathbb{F}_q(t_1, \ldots, t_r)$ is countable, and R is not.]
(4) Show that $\dim R = 1$ and hence show that Theorem 6.1.12 in the course notes does not work with non-finitely-generated algebras.

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

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

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

(4) For $f = \sum_{n\geq 0} a_n t^n \in R \setminus \{0\}$ define $\deg f := \inf\{n \geq 0 \mid a_n \neq 0\}$. If I is an ideal of R, then by point (1) we have $f \in I \setminus \{0\}$ if and only if $t^{\deg f} \in I$. Hence a non-zero ideal

$I \neq 0$ of R is generated by t^d where $d = \inf\{\deg f \mid f \in I \setminus \{0\}\}$. Therefore, the only prime ideals of R are $(0) \subset (t)$, and thus R has dimension 1. By the previous point, Theorem 6.1.12 hence fails for R.

□

Exercise 8. ♠ Let R be a Noetherian local ring (i.e. it has a unique maximal ideal) with maximal ideal $\mathfrak{m}$, and set $k = R/\mathfrak{m}$. Furthermore, fix a finitely generated module M over R.

(1) Show that if $f\colon M \to N$ is a morphism of finitely generated modules, such that the induced map $M/\mathfrak{m}M \to N/\mathfrak{m}N$ is surjective. Show that f is then surjective.
(2) A *minimal free resolution* of M is a resolution

$$\cdots \to F_n \xrightarrow{d_n} F_{n-1} \cdots \to F_0$$

of M such that for all n, F_n is free of finite rank and $\operatorname{im}(d_n) \subseteq \mathfrak{m}F_{n-1}$. Show that M admits a minimal free resolution.
(3) Fix a minimal free resolution $F_\bullet$ of M. Then show that for all $n \geq 0$, $\operatorname{Ext}^n(M,k) \neq 0$ if and only if $F_n \neq 0$.
(4) Deduce the surprising fact that if $\operatorname{Ext}^{n+1}(M,k) \neq 0$, then $\operatorname{Ext}^n(M,k) \neq 0$.
(5) Show that a finitely generated projective module over R is free.

Proof. (1) Since the induced map $M/\mathfrak{m}M \to N/\mathfrak{m}N$ is surjective, we automatically obtain that $N = f(M) + \mathfrak{m}$. In other words, $\mathfrak{m}\operatorname{coker}(f) = \operatorname{coker}(f)$, so by Nakayama's lemma, $\operatorname{coker}(f) = 0$ (i.e. f is surjective).

(2) We will construct this step by step. Let $m_1, \ldots, m_n \in M$ such that $\{\overline{m_1}, \ldots, \overline{m_n}\}$ is a basis of the $R/\mathfrak{m}$-vector space $M/\mathfrak{m}M$, and let $f\colon F_0 = R^n \to M$ be the map sending e_i to m_i. Then this map is by definition surjective modulo $\mathfrak{m}$, so it is surjective by the previous point. Furthermore, this map is in fact an isomorphism modulo $\mathfrak{m}$, so $\ker(f) \subseteq \mathfrak{m}F_0$. Finally, this kernel is finitely generated by Noetherianity of R.

Hence, we can keep this procedure going (replacing M by $\ker(f)$ and so on) and we find our sought minimal resolution.

(3) Let r denote the rank of F_n. Note that for all j, $\operatorname{Hom}(d_j, k) = 0$. Indeed, given $g\colon F_{j-1} \to k = R/\mathfrak{m}$, then $g \circ d_{j-1}\colon F_j \to k$ has its image included in $\mathfrak{m}k = 0$.

Thus, $\operatorname{Ext}^n(M,k) \cong \operatorname{Hom}(F_n, k) \cong \operatorname{Hom}(R^r, k) \cong k^r$, so we are done.

(4) If $F_n = 0$, then by exactness, $F^{n+2} \to F^{n+1}$ is surjective. In particular, this implies that $\mathfrak{m}F^{n+1} = F^{n+1}$, so $F^{n+1} = 0$ by Nakayama's lemma.

(5) Let M be a finitely generated projective module over R. Since M is projective, we know in particular that $\operatorname{Ext}^i(M,k) = 0$ for all $i > 0$. In particular, if $F_\bullet$ denotes a minimal free resolution of M, then by the previous point, $F_i = 0$ for all $i > 0$. In other words, $F_0 \to M$ is an isomorphism, and hence M is free.

□