Commutative Algebra

Written by Ádám Gyenge
based on the notes of Damian Rössler

September 1, 2024

Contents

1 Preliminaries

Let R be a commutative ring. If $I \subseteq R$ is an ideal in R, we shall say that I is non trivial if $I \neq R$ (this is not entirely standard terminology). The ideal I is *principal* if it can be generated by one element as an R-module.

We denote $R^* := R \backslash \{0\}$.

An element $r \in R$ is said to be *nilpotent* if there exists an integer $n \geq 1$ such that $r^n = \underbrace{r \cdots r}_{n\text{-times}} = 0$.

The ring R is *local* if it has a single maximal ideal $\mathfrak{m}$. Note that in this case, every element of $R \backslash \mathfrak{m}$ is a unit (because otherwise, any such element would be contained in a non trivial maximal ideal of R, which would not coincide with $\mathfrak{m}$ - see Lemma 2.4 below).

The prime ring of a ring R is the image of the unique ring homomorphism $\mathbb{Z} \to R$ (which sends $n \in \mathbb{Z}$ to the corresponding multiple of $1 \in R$).

If R is a ring, a *zero-divisor* of R is an element $r \in R$ such that there exists an element $r' \in R \backslash \{0\}$ such that $r \cdot r' = 0$. Note that 0 is always a zero-divisor of R.

A *domain* or (*integral domain*) is a ring R with the property that the set of zero-divisors of R consists only of 0 .

A *Unique Factorisation Domain (UFD)* is a domain R, which has the following property. For any $r \in R \backslash \{0\}$, there is a sequence $r_1, \ldots, r_k \in R$ (for some $k \geq 1$), such that

1. all the r_i are irreducible;
2. $(r) = (r_1 \cdots r_k)$;
3. if $r'_1, \ldots, r'_{k'}$ is another sequence with properties (1) and (2), then $k = k'$ and there is a permutation $\sigma \in S_k$ st $(r_i) = \left(r'_{\sigma(i)}\right)$ for all $i \in \{1, \ldots, k\}$.

If R, T are rings, then T is said to be a *R-algebra* if there is a homomorphism of rings $R \to T$. Note that this homomorphism is part of the datum of a R-algebra, so that strictly speaking, it is not T which should be called a R-algebra, but the homomorphism $R \to T$. Note also that a R-algebra T naturally carries a structure of R-module. If $\phi_1 : R \to T_1$ and $\phi_2 : R \to T_2$ are two R-algebras, a homomorphism of R-algebras is a homomorphism of rings $\lambda : T_1 \to T_2$ such that $\lambda \circ \phi_1 = \phi_2$.

A R-algebra $\phi : R \to T$ is said to be *finitely generated* if there exists an integer $k \geq 0$ and a surjective homomorphism of R-algebras $R[x_1, \ldots, x_k] \to T$ (where $R[x_1, \ldots, x_k] = R$ if $k = 0$). Note the following elementary fact: if $R \to T$ (resp. $T \to W$) is a finitely generated R-algebra (resp. a finitely generated T-algebra), then the composed map $R \to W$ makes W into a finitely generated R-algebra (why?).

If M is an R-module and $S \subseteq M$ is a subset of M, we write

$$\mathrm{Ann}(S) := \{r \in R \mid rm = 0 \text{ for all } m \in S\}$$

The set $\mathrm{Ann}_M(S)$ is an ideal of R (check), called the *annihilator* of S.

If $I, J \subseteq R$ are ideals in R, we shall write

$$(I : J) := \{r \in R \mid rJ \subseteq I\}$$

From the definitions, we see that $(I : J)$ is also an ideal and that $((0) : J) = \mathrm{Ann}(J)$. If $x, y \in R$, we shall often write $(I : x)$ for $(I : (x)), (x : I)$ for $((x), I)$ and $(x : y)$ for $((x) : (y))$. Note that if M is another ideal of R, we have $(I : M) \cap (J : M) = (I \cap J : M)$ (why?).

Let

$$\cdots \to M_i \xrightarrow{d_i} M_{i+1} \xrightarrow{d_{i+1}} \cdots$$

be a sequence of R-modules such that $d_{i+1} \circ d_i = 0$ for all $i \in \mathbb{Z}$. Such a sequence is called a complex of R-modules. We shall say that the complex is exact if $\ker(d_{i+1}) = \mathrm{Im}(d_i)$ for all $i \in \mathbb{Z}$.

For the record, we recall the following two basic results:

Theorem 1.1 (Chinese remainder theorem)**.** *Let R be a ring and let $I_1, \ldots, I_k$ be ideals of R. Let*

$$\phi : R \to \prod_{i=1}^{k} R/I_i$$

be the ring homomorphism such that $\phi(r) = \prod_{i=1}^{k} (r \,(\mathrm{mod} I_i))$ for all $r \in R$. Then $\ker(\phi) = \cap_{i=1}^{k} I_i$. Furthermore the map ϕ is surjective iff $I_i + I_j = R$ for any $i, j \in \{1, \ldots, k\}$ such that $i \neq j$, and in that case, we have $\cap_{i=1}^{k} I_i = \prod_{i=1}^{k} I_i$.

Proof. See Prop. 10 in AM. □

Proposition 1.2 (Euclidean division)**.** *Let R be a ring. Let $P(x), T(x) \in R[x]$ and suppose that the leading coefficient of $T(x)$ is a unit of R. Then there exist unique polynomials $Q(x), J(x) \in R[x]$ such that*

$$P(x) = Q(x)T(x) + J(x)$$

and $\deg(J(x)) < \deg(T(x))$ (here we set the degree of the zero polynomial to be $-\infty$).

We shall also need the following result from set theory.

A *partial order* on a set S is a relation $\leq$ on S, such that

- (reflexivity) $s \leq s$ for all $s \in S$;
- (transitivity) if $s \leq t$ and $t \leq r$ for $s, t, r \in S$ then $s \leq r$;

- (antisymmetry) if $s \leq t$ and $t \leq s$ for $t, s \in S$ then $s = t$.

If we also have

- (connexity) for all $s, t \in S$, either $s \leq t$ or $t \leq s$

then the relation $\leq$ is said to be a *total order* on S.

Let $T \subseteq S$ be a subset and let $b \in S$. We say that b is an *upper bound* for T if $t \leq b$ for all $t \in T$.

An element $s \in S$ is said to be a *maximal element* of S if for all $t \in S$, we have $s \leq t$ iff $s = t$. An element $s \in S$ is said to be a *minimal element* of S if for all $t \in S$, we have $t \leq s$ iff $s = t$.

Note that if S is partially ordered by the relation $\leq$ and $T \subseteq S$ is a subset, then the relation $\leq$ restricts to a partial order on T.

Proposition 1.3 (Zorn's lemma)**.** *Let $\leq$ be a partial order on a non-empty set S. Suppose that for every subset $T \subseteq S$, which is totally ordered (with the restriction of the relation $\leq$ to T), there is an upper bound for T in S. Then there exists a maximal element in S.*

Proof. Omitted. See any first course on set theory. Zorn's lemma is a consequence of the axiom of choice. □

A classical application of Zorn's lemma is the following.

Lemma 1.4. *Let R be a ring. If $I \subseteq R$ be a non trivial ideal. Then there is a maximal ideal $M \subseteq R$ such that $I \subseteq M$.*

Proof. Let $\mathcal{S}$ be the set of all non trivial ideals containing I. Endow $\mathcal{S}$ with the relation given by inclusion. If $\mathcal{T} \subseteq \mathcal{S}$ is a totally ordered subset, then $\mathcal{T}$ has the upper bound $\cup_{J \in \mathcal{T}} J$ (verify that this is an ideal containing I; it is non trivial because otherwise we would have $1 \in J$ for some $J \in \mathcal{T}$). Hence, by Zorn's lemma, there is a maximal element M in $\mathcal{S}$. By definition, the ideal M has the property that whenever J is a non trivial ideal containing I and $M \subseteq J$, then $M = J$. If J is an ideal of R, which does not contain I, then we cannot have $M \subseteq J$ (since M contains I). We conclude that for any non trivial ideal J of R, we have $M = J$ if $M \subseteq J$. In other words, M is a maximal ideal of R, which contains I. □

2 The nilradical and the Jacobson radical

Definition 2.1. Let R be a ring. The *nilradical* of R is the set of nilpotent elements of R.

A ring R is called *reduced* if its nilradical is $\{0\}$.

The nilradical captures the "infinitesimal part" of a ring. In the classical algebraic geometry of varieties, the coordinate rings were always assumed to be reduced, and nilradicals did not play a role. Part of the strength of scheme theory is that it allows the presence of infinitesimal phenomena.

Proposition 2.2. *Let R be a ring. The nilradical of R is the intersection of all the prime ideals of R.*

Proof. Suppose that $f \in R$ is a nilpotent element. Let $\mathfrak{p} \subseteq R$ be a prime ideal. Some power of f is 0 , which is an element of $\mathfrak{p}$. In particular, $f (\mathrm{mod} \mathfrak{p}) \in A/\mathfrak{p}$ is a zero-divisor. Since $\mathfrak{p}$ is a prime ideal, the ring $A/\mathfrak{p}$ is a domain and so $f (\mathrm{mod} \mathfrak{p}) = 0 (\mathrm{mod} \mathfrak{p})$. In other words, $f \in \mathfrak{p}$. We conclude that f is in the intersection of all the prime ideals of R.

Conversely, suppose that $f \in R$ is not nilpotent. Let Σ be the set of non trivial ideals I of R, such that for all $n \geq 1$ we have $f^n \notin I$. The set Σ is non-empty, since $(0) \in \Sigma$. If we endow this set with the relation of inclusion, we may conclude from Zorn's lemma that Σ contains a maximal element M (verify that the assumptions of Zorn's lemma are verified). We claim that M is a prime ideal.

To prove this, suppose that $x, y \in R$ and that $x, y \notin M$. Note that the ideal $(x) + M$ strictly contains M and hence cannot belong to Σ (by the maximality property of M). Similarly, the ideal

$(y) + M$ strictly contains M and hence cannot belong to Σ. Hence there are integers $n_x, n_y \geq 1$ such that $f^{n_x} \in (x) + M$ and $f^{n_y} \in (y) + M$. In other words, $f^{n_x} = a_1 x + m_1$, where $a_1 \in R$ and $m_1 \in M$ and $f^{n_y} = a_2 y + m_2$, where $a_2 \in R$ and $m_2 \in M$. Thus

$$f^{n_x+n_y} = a_1 a_2 xy + m_3$$

where $m_3 \in M$. We thus see that $xy \notin M$, for otherwise we would have $f^{n_x+n_y} \in M$, which is not possible since $M \in \Sigma$. Since $x, y \in R$ were arbitrary, we conclude that M is a prime ideal.

Since $M \in \Sigma$, for all $n \geq 1$ we have $f^n \notin M$. In particular we have $f \notin M$. In other words, we have exhibited a prime ideal in R, which does not contain f. In particular, f does not lies in the intersection of all the prime ideals of R. □

Corollary 2.3. *Let R be a ring. The nilradical of R is an ideal.*

Note that this corollary can also easily be proven directly (without using Proposition 2.2) (exercise).

Example 2.4. The nilradical of a domain is the zero ideal. The nilradical of $\mathbb{C}[x]/(x^n)$ is (x).

Let $I \subseteq R$ be an ideal. Let $q : R \to R/I$ be the quotient map and let $\mathcal{N}$ be the nilradical of R/I. The radical $\mathfrak{r}(I)$ of I is defined to be $q^{-1}(\mathcal{N})$. From the definitions, we see that the nilradical of R coincides with the radical $\mathfrak{r}((0))$ of the 0 ideal. Abusing language, we will sometimes write $\mathfrak{r}(R)$ for the nilradical of R. Again from the definitions and from Proposition 2.2, we see that the radical of I has the two equivalent descriptions:

- it is the set of elements $f \in R$ such that there exists an integer $n \geq 1$ such that $f^n \in I$;
- it is the intersection of the prime ideals of R, which contain I.

Notice the following elementary properties of the operator $\mathfrak{r}(\bullet)$. Let I, J be a ideals of R. Then we have $\mathfrak{r}(\mathfrak{r}(I)) = \mathfrak{r}(I)$ and we have $\mathfrak{r}(I \cap J) = \mathfrak{r}(I) \cap \mathfrak{r}(J)$ (why?).

An ideal, which coincides with its own radical is called a *radical ideal*.

Definition 2.5. Let R be a ring. The *Jacobson radical* of R is the intersection of all the maximal ideals of R.

By definition, the Jacobson radical of R contains the nilradical of R.

Let $I \subseteq R$ be a non trivial ideal. Let $q : R \to R/I$ be the quotient map and let $\mathcal{J}$ be the Jacobson radical of R/I. The Jacobson radical of I is defined to be $q^{-1}(\mathcal{J})$. By definition, this coincides with the intersection of all the maximal ideals containing I. Again by definition, the Jacobson radical of I contains the radical of I.

Proposition 2.6 (Nakayama's lemma)**.** *Let R be a ring. Let M be a finitely generated R-module. Let I be an ideal of R, which is contained in the Jacobson radical of R. Suppose that $IM = M$ (ie every $m \in M$ is a finite sum of elements of the form $a \cdot n$, where $a \in I$ and $n \in M$). Then $M \simeq (0)$.*

Proof. Suppose for contradiction that $M \neq (0)$. Let $x_1, \ldots, x_s$ be a set of generators of M and suppose that s is minimal (ie every set of generators for M has at least s elements). By assumption, there are elements $a_1, \ldots, a_s \in I$ such that

$$x_s = a_1 x_1 + \cdots + a_s x_s$$

so that $(1 - a_s) x_s$ lies in the submodule M' generated by $x_1, \ldots, x_{s-1}$. Here we set $x_0 := 0$ if $s = 1$. Now the element $1 - a_s$ is a unit. Indeed, if $1 - a_s$ were not a unit then it would be contained in a maximal ideal $\mathfrak{m}$ of R (apply Lemma 2.4) and by assumption $a_s \in \mathfrak{m}$ so that we would have $1 \in \mathfrak{m}$, which is contradiction. Hence

$$x_s = \left((1 - a_s)^{-1} a_1\right) x_1 + \cdots + \left((1 - a_s)^{-1} a_{s-1}\right) x_{s-1} \tag{1}$$

If $s = 1$ then we see from (1) that $x_s = 0$. This is a contradiction, since $M \neq (0)$. Thus either $M \simeq (0)$ or $s > 1$. If $s > 1$ we again see from (1) that M has $s - 1$ generators, which is also a contradiction. Hence $M \simeq (0)$. □

3 Localisation

Let R be a ring. A subset $S \subseteq R$ is said to be a *multiplicatively closed set* if $1 \in S$ and if $xy \in S$ whenever $x, y \in S$. A basic example of a multiplicatively closed set is the set $\{1, f, f^2, f^3, \ldots\}$, where $f \in R$.

Let $S \subseteq R$ be a multiplicatively closed subset. Consider the set $R \times S$ (cartesian product). We define a relation $\sim$ on $R \times S$ as follows. If $(a, s), (b, t) \in R \times S$ then $(a, s) \sim (b, t)$ iff there exists $u \in S$ such that $u(ta - sb) = 0$. The relation $\sim$ is an equivalence relation (verify) and we define $S^{-1}R$ to be $(R \times S)/\sim$, ie $S^{-1}R$ is the set of equivalence classes of $R \times S$ under $\sim$. If $a \in R$ and $s \in S$, we write a/s for the image of (a, s) in $S^{-1}R$. We define a map $+ : S^{-1}R \times S^{-1}R \to S^{-1}R$ by the rule

$$(a/s, b/t) \mapsto (at + bs)/(st)$$

This is well-defined (verify). We also define a map $\cdot : S^{-1}R \times S^{-1}R \to S^{-1}R$ by the rule

$$(a/s, b/t) \mapsto (ab)/(ts)$$

Again this is well-defined. One checks that these two maps provide $S^{-1}R$ with the structure of a commutative unitary ring, whose identity element is $1/1$. Here $+$ give the addition in the ring and $\cdot$ gives the multiplication. The 0 element in $S^{-1}R$ is then the element $0/1$. There is natural ring homomorphism from R to R_S, given by the formula $r \mapsto r/1$. By construction, if $r \in S$, the element $r/1$ is invertible in R, with inverse $1/r$.

We shall see in Lemma-Definition 5.1 below that $S^{-1}R$ is the "minimal extension" of R making every element of S invertible.

Note that if R is a domain, the fraction field of R is the ring $R_{R\setminus 0}$. Note also that if R is a domain and $0 \notin S$, then $S^{-1}R$ is a domain. Indeed suppose that R is domain and that $(a/s)(b/t) = 0$, where $a, b \in R$ and $s, t \in S$. Then by definition we have $u(ab) = 0$ for some $u \in S$, which implies that $ab = 0$ so that either $a = 0$ or $b = 0$, in particular either $a/s = 0/1$ or $b/t = 0/1$.

Note also that if $0 \in S$, then $S^{-1}R$ is the zero ring (ie $1 = 0$ in $S^{-1}R$. This simply follows from the fact that in this case $0/1$ is a unit in $S^{-1}R$. More generally, the definition shows that $S^{-1}R$ is the zero ring iff for all $r \in R$, there is an $s \in S$ st $sr = 0$.

If M is an R-module, we may carry out a similar construction. We define a relation $\sim$ on $M \times S$ as follows. If $(a, s), (b, t) \in M \times S$ then $(a, s) \sim (b, t)$ iff there exists $u \in S$ such that $u(ta - sb) = 0$. The relation $\sim$ is again an equivalence relation and we define $S^{-1}M$ to be $(M \times S)/\sim$, ie $S^{-1}M$ is the set of equivalence classes of $M \times S$ under $\sim$. If $a \in M$ and $s \in S$, we again write a/s for the image of (a, s) in $S^{-1}M$. We define a map $+ : S^{-1}M \times S^{-1}M \to S^{-1}M$ by the rule

$$(a/s, b/t) \mapsto (at + bs/(st)$$

This is also well-defined. Similarly, we define the map $\cdot : S^{-1}R \times S^{-1}M \to S^{-1}M$ by the rule

$$(a/s, b/t) \mapsto (ab)/(ts)$$

Again, this is well-defined. One checks that these two maps provide $S^{-1}M$ with the structure of a $S^{-1}R$ module. Here $+$ give the addition in the ring and $\cdot$ gives the scalar multiplication. The 0 element in $S^{-1}M$ is then the element $0/1$. The $S^{-1}R$-module $S^{-1}M$ carries a natural structure of R-module via the natural map $R \to S^{-1}R$ and there a natural map of R-modules $M \to S^{-1}M$, given by the formula $m \mapsto m/1$.

We shall also use the less cumbersome notation R_S for $S^{-1}R$ and M_S for $S^{-1}M$. The ring R_S (resp. the R-module M_S) is called the localisation of the ring R at S (resp. localisation of the R-module M at S).

Lemma-Definition 3.1. *Let $\phi : R \to R'$ be a ring homomorphism. Let $S \subseteq R$ be a multiplicatively closed subset. Suppose that $\phi(S)$ consists of units of R'. Then there is a unique ring homomorphism $\phi_S = S^{-1}\phi : R_S \to R'$ such that $\phi_S(r/1) = \phi(r)$ for all $r \in R$.*

Proof. Define the map $\lambda : R_S \to R'$ by the formula $\lambda(a/s) = \phi(a)(\phi(s))^{-1}$ for all $a \in R$ and $s \in S$. We show that λ is well-defined. Suppose that $(a, s) \sim (b, t)$. Then

$$\lambda(b/t) = \phi(b)(\phi(t))^{-1}$$

and we have $u(ta - sb) = 0$ for some $u \in S$. Thus $\phi(u)(\phi(t)\phi(a) - \phi(s)\phi(b)) = 0$ and since $\phi(u)$ is a unit in R', we have $\phi(t)\phi(a) - \phi(s)\phi(b) = 0$. Thus $\phi(t)\phi(a) = \phi(s)\phi(b)$ and

$$\lambda(a/s) = \phi(a)(\phi(s))^{-1} = \phi(b)(\phi(t))^{-1} = \lambda(b/t)$$

Thus λ is well-defined. We skip the straightforward verification that λ is a ring homomorphism. We have thus proven that there is a ring homomorphism $\phi_S : R_S \to R'$ such that $\phi_S(r/1) = \phi(r)$ for all $r \in R$ (namely λ). We now prove unicity. Suppose that $\phi'_S : R_S \to R'$ is another ring homomorphism such that $\phi'_S(r/1) = \phi(r)$ for all $r \in R$. Then for any $r \in R$ and $t \in S$, we have

$$\phi'_S(r/t) = \phi'_S\left((r/1)(t/1)^{-1}\right) = \phi'_S(r/1)\phi'_S(t/1)^{-1} = \phi_S(r)\phi_S(t)^{-1} = \phi_S(r/t)$$

and thus ϕ'_S coincides with ϕ_S (and in particular with λ). □

There is a similar result for modules:

Lemma 3.2. *Let R be a ring and let $S \subseteq R$ be a multiplicatively closed subset. Let M be a R-module and suppose for each $s \in S$, the "scalar multiplication by s" map $[s]_M : M \to M$ is an isomorphism. Then there is a unique structure of R_S-module on M such that $(r/1)m = rm$ for all $m \in M$ and $r \in R$.*

Keeping the notation of the lemma, note that if $r/s \in R_S$, we necessarily have $(r/s)(m) = [s]_M^{-1}(rm)$, where $[s]_M^{-1}$ is the inverse of the map $[s]_M$.

Proof. Left to the reader. □

We also record the following important fact.

Lemma 3.3. *Let R be a ring and let $f \in R$. Let $S = \{1, f, f^2, \ldots\}$. Then the ring R_S is finitely generated as a R-algebra.*

Proof. Consider the R-algebra $T := R[x]/(fx - 1)$. Note that T is a finitely generated R-algebra by definition. Let $\phi : R[x] \to R_S$ by the homomorphism of R-algebras such that $\phi(x) = 1/f$. Note that $\phi(fx - 1) = 0$ and hence ϕ induces a homomorphism of R-algebras $\psi : T \to R_S$. Now since the image of f in T is invertible by construction, there is by Lemma 3.1 a unique homomorphism of R-algebras $\lambda : R_S \to T$. We have $\psi \circ \lambda = \mathrm{Id}_T$ by unicity and hence λ is injective. On the other hand λ is surjective, since the image of λ contains $1/(f(\mathrm{mod}(fx - 1))) = x(\mathrm{mod}(fx - 1))$, which generates R as an R-algebra. Thus λ is bijective, and hence an isomorphism of R-algebras. □

In view of Lemma 3.2, if R is a ring and $\phi : N \to M$ is a homomorphism of R-modules, there is a unique homomorphism of R_S-modules $\phi_S : N_S \to M_S$ such that $\phi(n/1) = \phi(n)/1$ for all $n \in N$. We verify on the definitions that if $\psi : M \to T$ is another homomorphism of R-modules then we have $(\psi \circ \phi)_S = \psi_S \circ \phi_S$.

Lemma 3.4. *Let R be a ring and let $S \subseteq R$ be a multiplicatively closed subset. Let*

$$\cdots \to M_i \xrightarrow{d_i} M_{i+1} \xrightarrow{d_{i+1}} \cdots$$

be an exact complex of R-modules. Then the sequence

$$\cdots \to M_{i,S} \xrightarrow{d_{i,S}} M_{i+1,S} \xrightarrow{d_{i+1,S}} \cdots$$

is also exact.

Proof. Let $m/s \in M_{i,S}$ (with $m \in M_i$ and $s \in S$) and suppose that $d_{i,S}(m/s) = (1/s)d_{i,S}(m/1) = 0$. Then $d_{i,S}(m/1) = d_i(m)/1 = 0$ so that there is a $u \in S$, such that $u \cdot d_i(m) = d_i(um) = 0$. Now by assumption there is an element $p \in M_{i-1}$ such that $d_{i-1}(p) = um$. Then we have $d_{i-1,S}(p/(us)) = m/s$. This concludes the proof. □

Lemma 3.5. *Let $\phi : R \to T$ be a ring homomorphism. Let $S \subseteq R$ be a multiplicatively closed subset. By Lemma-Definition 3.1 there is a unique homomorphism of rings $\phi' : R_S \to T_{\phi(S)}$ such that $\phi'(r/1) = \phi(r)/1$. We may thus view $T_{\phi(S)}$ (resp. T) as a R_S-modules (resp. as a R-module). There is then a unique isomorphism of R_S-modules $\mu : T_S \simeq T_{\phi(S)}$ such that $\mu(a/1) = a/1$ for all $a \in T$ and we have $\mu \circ \phi_S = \phi'$.*

Proof. Define $\mu(a/s) := a/\phi(s)$ for any $a \in T$ and $s \in S$. This is well-defined. Indeed, suppose that $a/s = b/t$. Then there is $u \in S$ such that $\phi(u)(\phi(t)a - \phi(s)b) = 0$, ie $\phi(u)\phi(t)a = \phi(u)\phi(s)b$. We thus see that $a/\phi(s) = b/\phi(t)$, which shows that μ is well-defined. From the definitions, we see that μ is a map of R_S-modules. We also see from the definition that μ is surjective. To see that μ is injective, suppose that $\mu(a/s) = 0/1$ for some $a \in T$ and $s \in S$. Then there is a $u \in \phi(S)$ such that $ua = 0$. Hence $a/1 = 0$ in T_S and thus $a/s = 0$. Thus μ is bijective. The identity $\mu \circ \phi_S = \phi'$ follows from the fact that μ, ϕ_S and ϕ' are homomorphisms of R_S-modules and from the fact that $\mu \circ \phi_S(1) = \phi'(1/1)$. □

Let R be a ring and let $\mathfrak{p}$ be a prime ideal in R. Then the set $R\backslash\mathfrak{p}$ is a multiplicatively closed subset. Indeed, $1 \notin \mathfrak{p}$ for otherwise $\mathfrak{p}$ would be equal to R and if $x, y \notin \mathfrak{p}$ then $xy \notin \mathfrak{p}$, for otherwise either x or y would lie in $\mathfrak{p}$. We shall use the shorthand $R_\mathfrak{p}$ for $R_{R\backslash\mathfrak{p}}$ and if M is a R-module, we shall use the shorthand $M_\mathfrak{p}$ for $M_{R\backslash\mathfrak{p}}$. If $\phi : M \to N$ is a homomorphism of R-modules, we shall write $\phi_\mathfrak{p}$ for $\phi_{R\backslash\mathfrak{p}} : M_\mathfrak{p} \to N_\mathfrak{p}$.

If $\phi : U \to R$ is a homomorphism of rings and $\mathfrak{p}$ is a prime ideal of R, then ϕ naturally induces a homomorphism of rings $U_{\phi^{-1}(\mathfrak{p})} \to R_\mathfrak{p}$, since $\phi\left(U\backslash\phi^{-1}(\mathfrak{p})\right) \subseteq R\backslash\mathfrak{p}$. This homomorphism is sometimes also denoted ϕ_p.

Lemma 3.6. *Let R be a ring and let $S \subseteq R$ be a multiplicatively closed subset. Let $\lambda : R \to R_S$ be the natural ring homomorphism. Then the prime ideals of R_S are in one-to-one correspondence with the prime ideals $\mathfrak{p}$ of R such that $\mathfrak{p} \cap S = \emptyset$. If $\mathfrak{q}$ is a prime ideal of R_S then the corresponding ideal of R is $\lambda^{-1}(\mathfrak{q})$. If $\mathfrak{p}$ is a prime ideal of R such that $\mathfrak{p} \cap S = \emptyset$ then the corresponding prime ideal of R_S is $\iota_{\mathfrak{p},S}(\mathfrak{p}_S) \subseteq R_S$, where $\iota_\mathfrak{p} : \mathfrak{p} \to R$ is the inclusion map (which is a homomorphism of R-modules). Furthermore, $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is then the ideal generated by $\lambda(\mathfrak{p})$ in R_S.*

Note that in view of Lemma 3.5, if we localise R at S when R is viewed as a R-module or as a ring, we get the same R_S-module.

Proof. We first prove that if $\mathfrak{p}$ is any ideal of R, then $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is the ideal generated by $\lambda(\mathfrak{p})$ in R_S. For this, notice that by definition $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ consists of all the element $a/s \in R_S$, where $a \in \mathfrak{p}$ and $s \in S$. Hence $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is an ideal of R_S, which contains $\lambda(\mathfrak{p})$. Furthermore, since $a/s = (a/1)(1/s)$, any element a/s as above is contained in the ideal generated by $\lambda(\mathfrak{p})$ in R_S. Hence $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is the ideal generated by $\lambda(\mathfrak{p})$ in R_S.

To prove the lemma, we thus only have to show the following

(i) If $\mathfrak{q}$ is a non trivial ideal of R_S then $\lambda^{-1}(\mathfrak{q}) \cap S = \emptyset$.

(ii) If $\mathfrak{q}$ is an ideal of R_S, the ideal generated by $\lambda\left(\lambda^{-1}(\mathfrak{q})\right)$ in R_S is $\mathfrak{q}$.

(iii) If $\mathfrak{p}$ is a prime ideal of R such that $\mathfrak{p} \cap S = \emptyset$, then $\lambda^{-1}\left(\iota_{\mathfrak{p},S}(\mathfrak{p}_S)\right) = \mathfrak{p}$.

(iv) If $\mathfrak{p}$ is a prime ideal of R such that $\mathfrak{p} \cap S = \emptyset$ then $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is a prime ideal of R_S.

(v) If $\mathfrak{q}$ is a prime ideal of R_S then $\lambda^{-1}(\mathfrak{q})$ is a prime ideal.

We skip the proof of (v).

We prove (i). If $\lambda^{-1}(\mathfrak{q}) \cap S \neq \emptyset$ then (by definition) there exists $s \in \lambda^{-1}(\mathfrak{q})$ such that $s \in S$. But then $\lambda(s) = s/1 \in \mathfrak{q}$ and $s/1$ is a unit, so that $\mathfrak{q}$ is trivial. This proves (i).

To prove (ii), notice first that $\lambda\left(\lambda^{-1}(\mathfrak{q})\right) \subseteq \mathfrak{q}$. Furthermore, if $a/s \in \mathfrak{q}$ then as before $a/1 = (a/s)(s/1)$ also lies in $\mathfrak{q}$ and hence $a \in \lambda\left(\lambda^{-1}(\mathfrak{q})\right)$. Since $a/s = (a/1)(1/s)$ we thus see that a/s lies in the ideal generated by $\lambda\left(\lambda^{-1}(\mathfrak{q})\right)$. Since a/s was arbitrary, $\mathfrak{q}$ is thus the ideal generated by $\lambda\left(\lambda^{-1}(\mathfrak{q})\right)$.

To prove (iii) note that since $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is the ideal generated by $\lambda(\mathfrak{p})$ in R_S, we clearly have $\lambda^{-1}\left(\iota_{\mathfrak{p},S}(\mathfrak{p}_S)\right) \supseteq \mathfrak{p}$. Now suppose that $a \in \lambda^{-1}\left(\iota_{\mathfrak{p},S}(\mathfrak{p}_S)\right)$. Then by definition $a/1 = b/s$ for some $b \in \mathfrak{p}$ and some $s \in S$. Again by definition, this means that for some $t \in S$, we have $t(sa - b) = 0$, ie $tsa = tb$. Since $tb \in \mathfrak{p}$ and $ts \notin \mathfrak{p}$ (by assumption), we deduce from the fact that $\mathfrak{p}$ is prime that $a \in \mathfrak{p}$, as required.

To prove (iv), consider the exact sequence of R-modules

$$0 \to \mathfrak{p} \to R \xrightarrow{q} R/\mathfrak{p} \to 0$$

where q is the quotient map. Applying Lemma 3.4 we see that the sequence of R_S-modules

$$0 \to \mathfrak{p}_S \to R_S \xrightarrow{q_S} (R/\mathfrak{p})_S \to 0$$

is also exact. Furthermore, by Lemma 3.5, we see that $(R/\mathfrak{p})_S$ is isomorphic as a R_S-module with the ring $(R/\mathfrak{p})_{q(S)}$ and that we have an isomorphism of rings $R_S/\mathfrak{p}_S \simeq (R/\mathfrak{p})_{q(S)}$. Now since $S \cap \mathfrak{p} = \emptyset$, we see that $0 \notin q(S)$. Since $R/\mathfrak{p}$ is a domain by assumption, we deduce that $(R/\mathfrak{p})_{q(S)}$ is also a domain (see beginning of this section). We conclude that $\mathfrak{p}_S$ is a prime ideal. □

Lemma 3.7. *Let R be a ring and let $\mathfrak{p} \subseteq R$ be a prime ideal. Then the ring $R_\mathfrak{p}$ is a local ring. If $\mathfrak{m}$ is the maximal ideal of $R_\mathfrak{p}$ and $\lambda : R \to R_\mathfrak{p}$ is the natural homomorphism of rings, then $\lambda^{-1}(\mathfrak{m}) = \mathfrak{p}$.*

Proof. By Lemma 3.6 the prime ideals of $R_\mathfrak{p}$ correspond to the prime ideals of R which do not meet $R\backslash\mathfrak{p}$, ie to the prime ideals of R which are contained in $\mathfrak{p}$. This correspondence preserves the inclusion relation,
so every prime ideal of $R_\mathfrak{p}$ is contained in the prime ideal corresponding to $\mathfrak{p}$. Now let I be a maximal ideal of $R_\mathfrak{p}$. Since I is contained in the prime ideal corresponding to $\mathfrak{p}$, it must coincide with this ideal by maximality. So the prime ideal $\mathfrak{m}$ corresponding to $\mathfrak{p}$ is maximal and it is the only maximal ideal of $R_\mathfrak{p}$. By Lemma 3.6, we have $\lambda^{-1}(\mathfrak{m}) = \mathfrak{p}$. □

Lemma 3.8. *Let R be a ring. Let*

$$\cdots \to M_i \xrightarrow{d_i} M_{i+1} \xrightarrow{d_{i+1}} \cdots \tag{4}$$

be a complex of R-modules. Then the complex (4) is exact iff the complex

$$\cdots \to M_{i,\mathfrak{p}} \xrightarrow{d_{i,p}} M_{i+1,\mathfrak{p}} \xrightarrow{d_{i+1,p}} \cdots \tag{5}$$

is exact for all the maximal ideals $\mathfrak{p}$ of R.

Proof. " $\Rightarrow$ " By Lemma 3.4.

" $\Leftarrow$ ": Suppose that the complex (4) is not exact. Then $\ker(d_{i+1}) / \operatorname{Im}(d_i) \neq 0$ for some $i \in \mathbb{Z}$. By Lemma 3.4, there is a natural isomorphism

$$\left(\ker(d_{i+1}) / \operatorname{Im}(d_i)\right)_\mathfrak{p} \simeq \ker(d_{i+1})_\mathfrak{p} / \operatorname{Im}(d_i)_\mathfrak{p}$$

for all the prime ideals $\mathfrak{p}$ in R. In particular, if $\left(\ker(d_{i+1}) / \operatorname{Im}(d_i)\right)_\mathfrak{p} \neq 0$ for some prime ideal $\mathfrak{p}$, then the complex (5) is not exact for that choice of prime ideal.

Now since $\ker(d_{i+1}) / \operatorname{Im}(d_i) \neq 0$, we see that there is an element $a \in \ker(d_{i+1}) / \operatorname{Im}(d_i)$ such that $\operatorname{Ann}(a) \neq R$ (any non zero element of $\ker(d_{i+1}) / \operatorname{Im}(d_i)$ will do). Let $\mathfrak{p}$ be a maximal ideal of R, which contains $\operatorname{Ann}(a)$ (this exists by Lemma 1.4). Then $\left(\ker(d_{i+1}) / \operatorname{Im}(d_i)\right)_\mathfrak{p} \neq 0$ for otherwise there would be an element $u \in R\backslash\mathfrak{p} \subseteq R\backslash \operatorname{Ann}(a)$ such that $ua = 0$, which is a contradiction. Thus the complex (5) is not exact. □

4 Primary decomposition

In this section, we study a generalisation of the decomposition of integers into products of prime numbers. In a geometric context (ie for affine varieties over algebraically closed fields) this generalisation also provides the classical decomposition of a subvariety into a disjoint union of irreducible subvarieties. Applied to the ring of polynomials in one variable over a field, it yields the decomposition of a monic polynomial into a product of irreducible monic polynomials.

The main result is Theorem 4.9 below.

Proposition 4.1. *Let R be a ring.*

(i) Let $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ be prime ideals of R. Let I be an ideal of R. Suppose that $I \subseteq \cup_{i=1}^k \mathfrak{p}_i$. Then there is $i_0 \in \{1, \dots, k\}$ such that $I \subseteq \mathfrak{p}_{i_0}$.

(ii) Let $I_1, \dots, I_k$ be ideals of R and let $\mathfrak{p}$ be a prime ideal of R. Suppose that $\mathfrak{p} \supseteq \cap_{i=1}^k I_i$. Then there is $i_0 \in \{1, \dots, k\}$ such that $\mathfrak{p} \supseteq I_{i_0}$. If $\mathfrak{p} = \cap_{i=1}^k I_i$, then there is a $i_0 \in \{1, \dots, k\}$ such that $\mathfrak{p} = I_{i_0}$.

Proof. (i) By induction on k. The case $k = 1$ holds tautologically. Suppose for contradiction that the conclusion does not hold. By the inductive hypothesis, we see that for each $i \in \{1, \dots, k\}$, we have $I \nsubseteq \cup_{j \neq i} \mathfrak{p}_i$. In other words, there are elements $x_1, \dots, x_k \in I$ such that for each $i \in \{1, \dots, k\}$ we have $x_i \in \mathfrak{p}_i$ and $x_i \notin \mathfrak{p}_j$ if $j \neq i$. Now consider the element

$$y := \sum_{i=1}^{k} x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_k$$

where we set $x_0 = x_{k+1} = 1$. Note that for each $i \in \{1, \dots, k\}$ we have $x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_k \in \mathfrak{p}_j$ for all $j \neq i$. Now let $i \in \{1, \dots, k\}$ be such that $y \in \mathfrak{p}_i$. Then $y - x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_k \in \mathfrak{p}_i$ and thus

$$x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_k \in \mathfrak{p}_i$$

Now, since $\mathfrak{p}_i$ is prime, one of $x_1, x_2, \dots, x_{i-1}, x_{i+1}, \dots, x_k$ must lie in $\mathfrak{p}_i$, which is a contradiction.

(ii) We first prove the first statement. Suppose that the conclusion does not hold. Then for each $i \in \{1, \dots, k\}$, there is an element $x_i \in I_i$ such that $x_i \notin \mathfrak{p}$. But $x_1 x_2 \cdots x_k \in \cap_{i=1}^k I_i \subseteq \mathfrak{p}$ and since $\mathfrak{p}$ is prime, one of the x_i must lie in $\mathfrak{p}$, which is a contradiction.

The second statement follows from the first, since $\cap_{i=1}^k I_i \subseteq I_{i_0}$. □

Remark 4.2. The proof of Proposition 4.1 shows that in (i), the condition that the ideals $\mathfrak{p}_i$ are prime is superfluous if $k \leq 2$.

Definition 4.3. An ideal I of R is *primary* if it is non trivial and all the zero-divisors of R/I are nilpotent.

In other words, I is primary if the following holds: if $xy \in I$ and $x, y \notin I$ then $x^l \in I$ and $y^n \in I$ for some $l, n > 1$ (in other words, $x, y \in \mathfrak{r}(I)$). From the definition, we see that every prime ideal is primary.

Example 4.4. The ideals (p^n) of $\mathbb{Z}$ are primary if p is prime and $n > 0$.

Lemma 4.5. *Suppose that I is a primary ideal of R. Then $\mathfrak{r}(I)$ is a prime ideal.*

Proof. Let $x, y \in R$ and suppose that $xy \in \mathfrak{r}(I)$. Then there is $n > 0$ such that $x^n y^n \in I$ and thus either $x^n \in I$, or $y^n \in I$, or $x^{ln} \in I$ and $y^{nk} \in I$ for some $l, k > 1$. Hence either x or y lies in $\mathfrak{r}(I)$. □

The previous Lemma justifies the following terminology.

If $\mathfrak{p}$ is a prime ideal and I is a primary ideal, we say that I is $\mathfrak{p}$-*primary* if $\mathfrak{r}(I) = \mathfrak{p}$.

Lemma 4.6. *Let J be an ideal of R. Suppose that $\mathfrak{r}(J)$ is a maximal ideal. Then J is primary.*

Proof. From the assumptions, we see that the nilradical $\mathfrak{r}(R/J)$ of R/J is maximal. Hence R/J is a local ring, because any maximal ideal of R/J contains $\mathfrak{r}(R/J)$ by Proposition 3.2 and hence must coincide with it. Hence any element of R/J is either a unit or is nilpotent. In particular, all the zero divisors of R/J are nilpotent, in particular J is primary. □

From the previous Lemma, we see that powers of maximal ideals are primary ideals.

Lemma 4.7. *Let $\mathfrak{p}$ be a prime ideal and let I be a $\mathfrak{p}$-primary ideal. Let $x \in R$.*

(i) If $x \in I$ then $(I : x) = R$.

(ii) If $x \notin I$ then $\mathfrak{r}(I : x) = \mathfrak{p}$.

(iii) If $x \notin \mathfrak{p}$ then $(I : x) = I$.

Proof. (i) and (iii) follow directly from the definitions. We prove (ii). Suppose that $y \in \mathfrak{r}(I : x)$. By definition, this means that for some $n > 0$, we have $xy^n \in I$. As $x \notin I$, we see that $y^{ln} \in I$ for some $l > 0$ so that $y \in \mathfrak{r}(I) = \mathfrak{p}$. Hence $\mathfrak{r}(I : x) \subseteq \mathfrak{p}$. Now consider that we have $I \subseteq \mathfrak{r}(I : x) \subseteq \mathfrak{p}$. Applying the operator $\mathfrak{r}(\bullet)$, we see that we have $\mathfrak{r}(I) = \mathfrak{p} \subseteq \mathfrak{r}(\mathfrak{r}(I : x)) = \mathfrak{r}(I : x) \subseteq \mathfrak{r}(\mathfrak{p}) = \mathfrak{p}$ so that $\mathfrak{r}(I : x) = \mathfrak{p}$. □

Lemma 4.8. *Let $\mathfrak{p}$ be a prime ideal and let $\mathfrak{q}_1 \ldots, \mathfrak{q}_k$ be $\mathfrak{p}$-primary ideals. Then $\mathfrak{q} := \cap_{i=1}^k \mathfrak{q}_i$ is also $\mathfrak{p}$-primary.*

Proof. We compute

$$\mathfrak{r}(\mathfrak{q}) = \cap_{i=1}^k \mathfrak{r}\left(\mathfrak{q}_i\right) = \mathfrak{p}$$

In particular, $\mathfrak{q}$ is $\mathfrak{p}$-primary if it is primary. We verify that $\mathfrak{q}$ is primary. Suppose that $xy \in \mathfrak{q}$ and that $x, y \notin \mathfrak{q}$. Then then there are $i, j \in \{1 \ldots, k\}$ such that $x \notin \mathfrak{q}_i$ and $y \notin \mathfrak{q}_j$. Hence there are $l, t > 0$ such $y^l \in \mathfrak{q}_i$ and $x^t \in \mathfrak{q}_j$. In other words, $x, y \in \mathfrak{r}\left(\mathfrak{q}_i\right) = \mathfrak{r}\left(\mathfrak{q}_j\right) = \mathfrak{p} = \mathfrak{r}(\mathfrak{q})$. In other words, $\mathfrak{q}$ is primary. □

We shall say that an ideal I of R is *decomposable* if there exists a sequence $\mathfrak{q}_1 \ldots, \mathfrak{q}_k$ of primary ideals in R such that $I = \cap_{i=1}^k \mathfrak{q}_i$. Such a sequence is called a *primary decomposition* of I. A primary decomposition as above is called *minimal* if

(a) all the $\mathfrak{r}\left(\mathfrak{q}_i\right)$ are distinct;

(b) for all $i \in \{1, \ldots, k\}$ we have $\mathfrak{q}_i \not\supseteq \cap_{j \neq i} \mathfrak{q}_j$.

Note that any primary decomposition can be reduced to a minimal primary decomposition in the following way:

- first use Lemma 4.8 to replace the sets of primary ideals with the same radical by their intersection; then (a) is achieved;
- then successively throw away any primary ideal violating (b).

In general, not all ideals are decomposable. We shall see in section 7 below that all ideals are decomposable if R is noetherian.

The following theorem examines what part of primary decompositions are unique.

Theorem 4.9. *Let I be a decomposable ideal. Let $\mathfrak{q}_1 \ldots, \mathfrak{q}_k$ be primary ideals and let $I = \cap_{i=1}^k \mathfrak{q}_i$ be a minimal primary decomposition of I. Let $\mathfrak{p}_i := \mathfrak{r}\left(\mathfrak{q}_i\right)$ (so that $\mathfrak{p}_i$ is a prime ideal). Then the following two sets of prime ideals coincide*

- *the set $\{\mathfrak{p}_i\}_{i \in \{1, \ldots, k\}}$*

- *the ideals among the ideals of the type* $\mathfrak{r}(I:x)$ *(where* $x \in R$ *), which are prime.*

Proof. Let $x \in R$. Note that $(I:x) = \cap_{i=1}^{k}(\mathfrak{q}_i : x)$ and $\mathfrak{r}(I:x) = \cap_{i=1}^{k}\mathfrak{r}(\mathfrak{q}_i : x)$. Hence by Lemma 4.8, we have $\mathfrak{r}(I:x) = \cap_{i,x\notin\mathfrak{q}_i}\mathfrak{p}_i$.

Now suppose that $\mathfrak{r}(I:x)$ is a prime ideal. Then $\mathfrak{r}(I:x) = \mathfrak{p}_{i_0}$ for some $i_0 \in \{1,\dots,k\}$ by Proposition 4.1. Conversely, note that for any $i_0 \in \{1,\dots,k\}$, there exists an $x \in R$, such that $x \notin \mathfrak{q}_{i_0}$ and such that $x \in \mathfrak{q}_i$ for all $i \neq i_0$. This follows from the minimality of the decomposition. For such an x, we have $\mathfrak{r}(I:x) = \mathfrak{p}_{i_0}$ by the above.

As a consequence of Theorem 4.9 , we can associate with any decomposable ideal I in R a uniquely defined set of prime ideals. These prime ideals are said to be *associated with* I. Note that the intersection of these prime ideals is the ideal $\mathfrak{r}(I)$. Another consequence is that any radical decomposable ideal has a minimal primary decomposition by prime ideals (so that in this case, the associated primes are the elements of the minimal primary decomposition itself). Furthermore, any two minimal primary decompositions by prime ideals of a radical ideal coincide.

Remark 4.10. One can show that any minimal primary decomposition of a radical ideal consists only of prime ideals (without requiring a priori that the primary decomposition consist of prime ideals, as in the previous paragraph). This is called the '2nd uniqueness theorem'. In particular, a decomposable radical ideal has a unique primary decomposition. We do not prove this in these notes however.

Example 4.11.

1. If $n = \pm p_1^{n_1}\cdots p_k^{n_k} \in \mathbb{Z}$, where the p_i are distinct prime numbers, a primary decomposition of (n) is given by
$$(n) = \cap_{i=1}^{k}(p^{n_i})$$
(apply the Chinese Remainder Theorem). The set of prime ideals associated to this decomposition is of course $\{(p_1),\dots,(p_k)\}$.

2. A more complex example is the ideal $\left(x^2, xy\right) \subseteq \mathbb{C}[x,y]$. Here
$$\left(x^2, xy\right) = (x) \cap (x,y)^2$$
is a primary decomposition and the associated set of prime ideals is $\{(x),(x,y)\}$. To see that we indeed have $\left(x^2, xy\right) = (x) \cap (x,y)^2$ note that by construction, the ideal $(x,y)^2$ consists of the polynomials of the form $x^2P(x,y) + xyQ(x,y) + y^2T(x,y)$. Thus $(x)\cap(x,y)^2$ consists of the polynomials $x^2P(x,y) + xyQ(x,y) + y^2T(x,y)$ such that $T(x,y)$ is divisible by x. Hence $(x) \cap (x,y)^2 \subseteq \left(x^2, xy\right)$ and clearly we also have $\left(x^2, xy\right) \subseteq (x)\cap(x,y)^2$ so that $\left(x^2, xy\right) = (x)\cap(x,y)^2$. To see that the decomposition is primary, note that $\mathbb{C}[x,y]/(x) \simeq \mathbb{C}[y]$ and $\mathbb{C}[x,y]/(x,y) \simeq \mathbb{C}$. Thus (x) is prime and (hence primary) and (x,y) is maximal, so that $(x,y)^2$ is primary by Lemma 4.6.

Lemma 4.12. *Let* I *be a decomposable ideal. Let* $\mathcal{S}$ *be the set of prime ideals associated with some (and hence any) minimal primary decomposition of* I*. Let* $\mathcal{I}$ *be the set of all the prime ideals of* R*, which contain* I*. View* $\mathcal{S}$ *(resp.* $\mathcal{I}$ *) as partially ordered by the inclusion relation. Then the minimal elements of* $\mathcal{S}$ *coincide with the minimal elements of* $\mathcal{I}$*.*

Proof. Clearly the minimal elements of $\mathcal{I}$ are also minimal elements of $\mathcal{S}$. We only have to show that the minimal elements of $\mathcal{S}$ are also minimal in $\mathcal{I}$. Let $\mathcal{S}_{\min} \subseteq \mathcal{S}$ (resp. $\mathcal{I}_{\min} \subseteq \mathcal{I}$) be the set of minimal elements of $\mathcal{S}$ (resp. $\mathcal{I}$). Note first that by Theorem 4.9, we have $\mathfrak{r}(I) = \cap_{\mathfrak{p}\in\mathcal{S}}\mathfrak{p}$ and thus we also have $\mathfrak{r}(I) = \cap_{\mathfrak{p}\in\mathcal{S}_{\min}}\mathfrak{p}$. Now let $\mathfrak{p}_0 \in \mathcal{S}_{\min}$. Suppose for contradiction that $\mathfrak{p}_0 \notin \mathcal{I}_{\min}$. Then there exists an element $\mathfrak{p}_0' \in \mathcal{I}$ such that $\mathfrak{p}_0' \subsetneq \mathfrak{p}_0$. On the other hand, we have $\mathfrak{p}_0' \supseteq I$, so that $\mathfrak{p}_0' \supseteq \mathfrak{p}$ for some $\mathfrak{p} \in \mathcal{S}_{\min}$ by Proposition 4.1. We conclude that $\mathfrak{p}_0 \supsetneq \mathfrak{p}$, which contradicts the minimality of $\mathfrak{p}_0$. Thus $\mathcal{S}_{\min} = \mathcal{I}_{\min}$. □

The elements of $\mathcal{S}_{\min}$ are called the *isolated* or *minimal* prime ideals associated with I whereas the elements of $\mathcal{S}\backslash\mathcal{S}_{\min}$ are called the *embedded* prime ideals associated with I. This terminology is

justified by algebraic geometry. According to the last lemma, the isolated prime ideals associate with I are precisely the prime ideals, which are minimal among all the prime ideals containing I.

In Example 4.11 (2), the set $\mathcal{S}_{\min}$ consists only of (x).

Note also the following important facts:

- if I is a decomposable radical ideal, then all the associated primes of I (which coincide with the elements of the unique minimal primary decomposition - see above) are isolated. This simply follows from the fact that I has a minimal primary decomposition by prime ideals.
- if I is a decomposable ideal, there are only finitely many prime ideals, which contain I and are minimal among all the prime ideals containing I. These prime ideals are also the isolated ideals associated with I.

We also record the following lemma, which makes no assumption of decomposability.

Lemma 4.13. *Let R be a ring. Let $I \subseteq R$ be an ideal. Then there are prime ideals, which are minimal among all the prime ideals containing I. Furthermore, if $\mathfrak{p} \supseteq I$ is a prime ideal, then $\mathfrak{p}$ contains such a prime ideal.*

Proof. Exercise. □

5 Noetherian rings

Let R be a ring. We say that R is *noetherian* if every ideal of R is finitely generated. In other words, if $I \subseteq R$ is an ideal of R, then there are elements $r_1, \ldots, r_k$ such that $I = (r_1, \ldots, r_k)$.

Example 5.1. Fields and PIDs are noetherian (why?). In particular, $\mathbb{Z}$ and $\mathbb{C}$ are noetherian, and so is $K[x]$, for any field K.

We shall see that "most" rings that one encounters are noetherian. In fact any finitely generated algebra over a noetherian ring is noetherian (see below).

We begin with some generalities.

Lemma 5.2. *The ring R is noetherian iff whenever $I_1 \subseteq I_2 \subseteq \ldots$ is an ascending sequence of ideals, there exists a $k \geq 1$ such that $I_k = I_{k+i} = \cup_{t=1}^{\infty} I_t$ for all $i \geq 0$.*

Proof. " $\Rightarrow$ ". Suppose first that R is noetherian. Let $I_1 \subseteq I_2 \subseteq \ldots$ be an ascending sequence of ideals. The set $\cup_{t=1}^{\infty} I_t$ is clearly an ideal (verify) and it is finitely generated by assumption. A given finite set of generators for $\cup_{t=1}^{\infty} I_t$ lies in I_k for some $k \geq 1$. The conclusion follows.

" $\Leftarrow$ ". Conversely, suppose that whenever $I_1 \subseteq I_2 \subseteq \ldots$ is an ascending sequence of ideals, there exists a $k \geq 1$ such that $I_k = I_{k+i} = \cup_{t=1}^{\infty} I_t$ for all $i \geq 0$. Let $J \subseteq R$ be an ideal. We need to show that J is finitely generated. For contradiction, suppose that J is not finitely generated. Define a sequence $r_1, r_2 \cdots \in J$ by the following inductive procedure. Let $r_1 \in J$ be arbitrary. Suppose that $r_1, \ldots, r_i \in J$ is given and let $r_{i+1} \in J \backslash (r_1, \ldots, r_i)$. Note that $J \backslash (r_1, \ldots, r_i) \neq \emptyset$ for otherwise J would be finitely generated. We then have an ascending sequence

$$(r_1) \subsetneq (r_1, r_2) \subsetneq (r_1, r_2, r_3) \subsetneq \ldots$$

which contradicts our assumptions. So J is finitely generated. □

Lemma 5.3. *Let R be a noetherian ring and $I \subseteq R$ an ideal. Then the quotient ring R/I is noetherian.*

Proof. Let $q : R \to R/I$ be the quotient map. Let J be an ideal of R/I. The ideal $q^{-1}(J)$ is finitely generated by assumption and the image by q of any set of generators of $q^{-1}(J)$ is a set of generators for J. □

Lemma 5.4. *Let R be a noetherian ring and let $S \subseteq R$ be a multiplicatively closed subset. Then the ring R_S is noetherian.*

Proof. Let $\lambda : R \to R_S$ be the natural ring homomorphism. In the proof of Lemma 3.6 we showed that for any ideal I of R_S, the ideal generated by $\lambda\left(\lambda^{-1}(I)\right)$ is I (see (ii) in the proof). The image of any finite set of generators of $\lambda^{-1}(I)$ under λ is thus a finite set of generators for I. □

Lemma 5.5. *Let R be a noetherian ring. Let M be a finitely generated R-module. Then any submodule of M is also finitely generated.*

Proof. By assumption there is a surjective map of R-modules $q : R^n \to M$ for some $n \geq 0$. To prove that a submodule $N \subseteq M$ is finitely generated, it is sufficient to prove that $q^{-1}(N)$ is finitely generated. Hence we may assume that $M = R^n$. We now prove the statement by induction on n. The case $n = 1$ is verified by assumption. Let $\phi : R^n \to R$ be the projection on the first factor. Let $N \subseteq R^n$ be a submodule. We then have an exact sequence

$$0 \to N \cap R^{n-1} \to N \to \phi(N) \to 0$$

where R^{n-1} is viewed as a submodule of R^n via the map $(r_1, \ldots, r_{n-1}) \mapsto (r_1, \ldots, r_{n-1}, 0)$. Now $\phi(N)$ is finitely generated since $\phi(N)$ is an ideal in R and $N \cap R^{n-1}$ is finitely generated by the inductive hypothesis. Let $a_1, \ldots, a_k \in N \cap R^{n-1}$ be generators of $N \cap R^{n-1}$ and let $b_1, \ldots, b_l \in \phi(N)$ be generators of $\phi(N)$. Let $b_1', \ldots, b_l' \in R^n$ be such that $\phi\left(b_i'\right) = b_i$ for all $i \in \{1, \ldots, l\}$. Then the set $\{a_1, \ldots, a_k, b_1', \ldots, b_l'\}$ generates N (verify). □

Lemma 5.6. *Let R be a noetherian ring. If $I \subseteq R$ is an ideal, then there is an integer $t \geq 1$ such that $\mathfrak{r}(I)^t \subseteq I$. In particular, some power of the nilradical of R is the 0 ideal.*

Proof. By assumption, we have $\mathfrak{r}(I) = (a_1, \ldots, a_k)$ for some $a_1, \ldots, a_k \in R$. By assumption again, there is an integer $n \geq 1$ such that $a_i^n \in I$ for all $i \in \{1, \ldots, k\}$. Let $t = k(n-1) + 1$. Then $\mathfrak{r}(I)^t \subseteq (a_1^n \ldots, a_k^n) \subseteq I$. □

The following theorem is one of the main justifications for the introduction of the noetherian condition.

Theorem 5.7 (Hilbert basis theorem)**.** *Suppose that R is noetherian. Then the polynomial ring $R[x]$ is also noetherian.*

Proof. Let $I \subseteq R[x]$ be an ideal. The leading coefficients of the polynomials in I form an ideal J of R (check). Since R is noetherian, J has a finite set of generators, say $a_1, \ldots, a_k$. For each $i \in \{1, \ldots, k\}$, choose $f_i \in I$ such that $f_i(x) = a_i x^{n_i} +$ (terms of lower degree). Let n be the maximum of the n_i. Let $I' = (f_1(x), \ldots, f_k(x)) \subseteq I$ be the ideal generated by the $f_i(x)$.

Now let $f(x) = ax^m +$ (terms of lower degree) be any polynomial in I. By construction, we have $a = r_1 a_1 + \cdots + r_k a_k$ for some $r_1, \ldots, r_k \in R$.

Suppose first that $m \geq n$. The polynomial

$$f(x) - r_1 f_1(x) x^{m-n_1} + \cdots + r_k f_k(x) x^{m-n_k}$$

is then of degree $< m$ (the leading terms cancel) and it also lies in I. Applying the same procedure to this polynomial we obtain a new polynomial of degree $< m-1$ and we keep going in the same way until we obtain a polynomial of degree $< n$. We have then expressed the polynomial $f(x)$ as a sum of a polynomial of degree $< n$ and an element of I'. In other words, we have shown that $f(x)$ lies in the R-submodule $M \cap I + I'$ of $R[x]$, where M is the R-submodule of $R[x]$, generated by $1, x, x^2, \ldots, x^{n-1}$.

If $m < n$ then we have $f(x) \in M \cap I$ so that we also have $f(x) \in M \cap I + I'$.

Since $f(x)$ was arbitrary, we see that we have shown that

$$I = M \cap I + I'$$

Now $M \cap I$ is an R-submodule of $M \simeq R^n$ and is thus finitely generated (as an R-module) by Lemma 7.4. If we let $g_1(x), \ldots, g_t(x) \in M \cap I$ be a set of generators, then the set $g_1(x), \ldots, g_t(x), f_1(x), \ldots, f_k(x)$ is clearly a set of generators of I (as an ideal). $\square$

Some history. The German mathematician Paul Gordan, who was active at the beginning of the 20th century, was the first to ask explicitly (to my knowledge) whether Theorem 7.6 is true and considered this to be a central question of a then very popular subject, called Invariant Theory (which we don't have the time to describe here). As the name of the theorem suggests, David Hilbert found the above simple proof. Paul Gordan had presumably tried to tackle the problem directly, by devising an algorithm that would provide a finite set of generators for an ideal given by an infinite set of generators and did not think of applying the abstract methods, which are used in Hilbert's proof (which is the above proof). The proof of Hilbert's basis theorem is one of the starting points of modern commutative algebra. Paul Gordan is said to have quipped on seeing Hilbert's proof that "Das is nicht Mathematik, das ist Theologie!" (This is not mathematics, this is theology!). There are nowadays more "effective" proofs of Hilbert's basis theorem, using so-called Groebner bases.

From Theorem 5.7, we deduce that $R[x_1, \ldots, x_k]$ is noetherian for any $k \geq 0$. From this and Lemma 5.3, we deduce that every finitely generated algebra over a noetherian ring is noetherian.

Finally, we consider primary decompositions in noetherian rings.

Theorem 5.8 (Lasker-Noether)**.** *Let R be a noetherian ring. Then every ideal of R is decomposable.*

Proof. If I is an ideal of R, we shall say that I is irreducible if whenever I_1, I_2 are ideals of R and $I = I_1 \cap I_2$, we have either $I = I_1$ or $I = I_2$.

Claim. Let $J \subseteq R$ be an ideal. Then there are irreducible ideals $J_1, \ldots, J_k$ such that $J = \cap_{i=1}^k J_k$.

We prove the claim. Let us say that an ideal is decomposable by irreducible ideals (short: dic) if it is a finite intersection of irreducible ideals. Suppose that J is not dic (otherwise we are done). In particular, J is not irreducible and thus there are ideals M and N such that $M \cap N = J$ and such that $J \subsetneq M$ and $J \subsetneq N$. Since J is not dic, we see that either N or M are not dic. Suppose without restriction of generality that M is not dic. Repeating the same reasoning for M and continuing we obtain a sequence of dic ideals $J \subsetneq M \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots$ This contradicts Lemma 5.2. Thus J is dic.

Claim. An irreducible ideal is primary.

We prove the claim. Let J be an irreducible ideal and suppose that J is not primary. Then there is an element $x \in R/J$, which is a zero divisor and is not nilpotent. Let $q : R \to R/J$ be the quotient map.

Consider the ascending sequence

$$\mathrm{Ann}(x) \subseteq \mathrm{Ann}\left(x^2\right) \subseteq \mathrm{Ann}\left(x^3\right) \subseteq \ldots$$

This sequence must stop by Lemma 5.2 and Lemma 5.3. So let us suppose that

$$\mathrm{Ann}\left(x^k\right) = \mathrm{Ann}\left(x^{k+1}\right) = \mathrm{Ann}\left(x^{k+2}\right) = \ldots$$

for some $k \geq 1$. Now consider the ideal $\left(x^k\right) \cap \mathrm{Ann}\left(x^k\right)$. If $\lambda x^k \in \left(x^k\right) \cap \mathrm{Ann}\left(x^k\right)$ for some $\lambda \in R/J$ then we have by definition $\lambda x^{2k} = 0$ and hence $\lambda \in \mathrm{Ann}\left(x^{2k}\right)$. Since $\mathrm{Ann}\left(x^{2k}\right) = \mathrm{Ann}\left(x^k\right)$ we then have $\lambda x^k = 0$. Thus $\left(x^k\right) \cap \mathrm{Ann}\left(x^k\right) = (0)$. On the other hand, note that $\left(x^k\right) \neq (0)$ and $\mathrm{Ann}\left(x^k\right) \neq 0$ by construction. Thus we have $J = q^{-1}\left(\left(x^k\right)\right) \cap q^{-1}\left(\mathrm{Ann}\left(x^k\right)\right)$ and $q^{-1}\left(\left(x^k\right)\right) \neq J, q^{-1}\left(\mathrm{Ann}\left(x^k\right)\right)\right) \neq J$, a contradiction. Thus J is primary.

The conjunction of both claims obviously proves the Theorem, so we are done. $\square$

Let R be a noetherian ring and let $I \subseteq R$ be a radical ideal. As explained after Theorem 4.9, a consequence of Theorem 5.8 is that there is a unique set $\{\mathfrak{q}_1 \ldots, \mathfrak{q}_k\}$ of distinct prime ideals in R such that

- $I = \cap_{i=1}^k \mathfrak{q}_i$

- for all $i \in \{1, \ldots, k\}$ we have $\mathfrak{q}_i \not\supseteq \cap_{j \neq i} \mathfrak{q}_j$.

Furthermore, the set $\{\mathfrak{q}_1 \ldots, \mathfrak{q}_k\}$ is precisely the set of prime ideals, which are minimal among the prime ideals containing I. For affine varieties, $V(I)$ is the union of the $V(\mathfrak{q}_i)$.

In particular, if $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ is the set of minimal prime ideal of R, there there is a natural injective homomorphism of rings

$$R/\mathfrak{r}((0)) \hookrightarrow \prod_{i=1}^{l} R/\mathfrak{p}_i$$