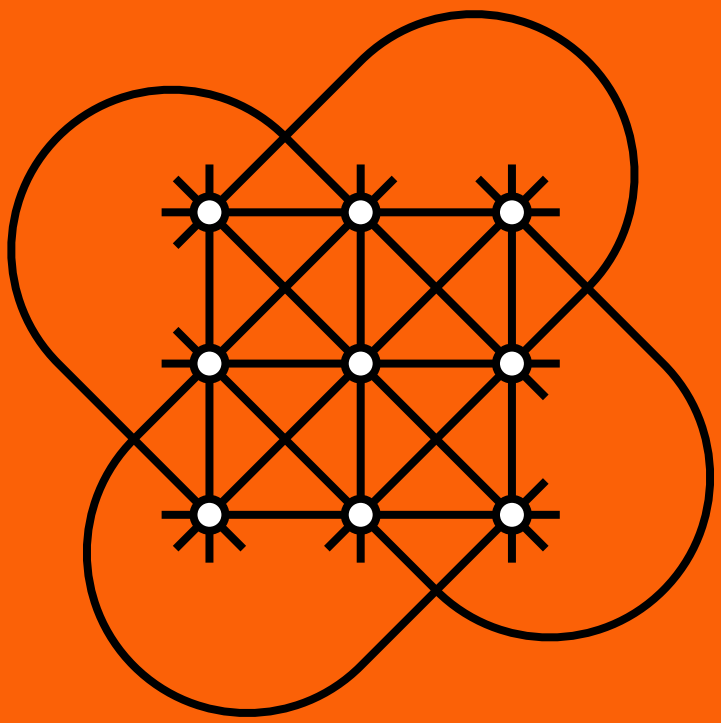
Algebraic Geometry



Mariano Suárez-Álvarez

Version: August 18, 2026

Contents

Chapter 1

Varieties

1.1. Polynomial functions on affine space

Let us fix a field $\Bbbk$. All the vector spaces and algebras that we consider here will be defined over $\Bbbk$, unless we say otherwise.

Definition 1.1.1. Let n be a non-negative integer. The ***affine space of dimension*** n is the set

$$\mathbb{A}^n := \Bbbk^n = \underbrace{\Bbbk \times \cdots \times \Bbbk}_{n \text{ factors}}.$$

If we need to make the ground field explicit in our notation, we write $\mathbb{A}^n_\Bbbk$ instead of simply $\mathbb{A}^n$. Let us notice that the set $\mathbb{A}^0$ has exactly one element, the 0-uple $()$.

We also fix a non-negative integer n and, as usual, write $\Bbbk[x_1, \ldots, x_n]$ for the algebra of polynomials in the variables $x_1, \ldots, x_n$ with coefficients in $\Bbbk$. When n is small we will usually use other names for the variables, and thus consider the algebras $\Bbbk[x]$, $\Bbbk[x, y]$, and on on.

If $p = (p_1, \ldots, p_n)$ is an element of $\mathbb{A}^n$, then the components of p are of course elements of $\Bbbk$, which is an algebra, and according to Proposition A.1.1 there is exactly one morphism of algebras $\varepsilon_p : \Bbbk[x_1, \ldots, x_n] \to \Bbbk$ such that $\varepsilon_p(x_i) = p_i$ for each i in $[\![n]\!]$. We call this map the ***evaluation map*** at p, and for each element f of $\Bbbk[x_1, \ldots, x_n]$ we write $f(p)$ to denote $\varepsilon_p(f)$. In terms of this notation, the fact that ε_p is a morphism of algebras implies that whenever f and g are elements of $\Bbbk[x_1, \ldots, x_n]$ and a and b are elements of $\Bbbk$ we have that

$$1(p) = 1, \qquad (a \cdot f + b \cdot g)(p) = a \cdot f(p) + b \cdot g(p), \qquad (f \cdot g)(p) = f(p) \cdot g(p).$$

We will use this all the time implicitly.

Proposition 1.1.2. *Let* $\mathrm{Fun}(\mathbb{A}^n)$ *be the algebra of all functions* $\mathbb{A}^n \to \Bbbk$*, and for each element* f *of* $\Bbbk[x_1, \ldots, x_n]$ *let us consider the function*

$$\phi_f \colon p \in \mathbb{A}^n \mapsto f(p) \in \Bbbk.$$

The function $\Phi_n \colon f \in \Bbbk[x_1, \ldots, x_n] \mapsto \phi_f \in \mathrm{Fun}(\mathbb{A}^n)$ *is a morphism of algebras.*

Proof. If f and g are elements of $\Bbbk[x_1, \ldots, x_n]$ and a and b are elements of $\Bbbk$, then for all points p in $\mathbb{A}^n$ we have that

$$\begin{aligned}\Phi_n(af + bg)(p) &= \phi_{af+bg}(p) = (af + bg)(p) = af(p) + bg(p) = a\phi_f(p) + b\phi_g(p) \\ &= a\Phi_n(f)(p) + b\Phi_n(g)(p) = (a\Phi_n(f) + b\Phi_n(g))(p),\end{aligned}$$

so that, in fact, $\Phi_n(af + bg) = a\Phi_n(f) + b\Phi_n(g)$. This tells us that the function Φ_n is linear.

Since for each p in $\mathbb{A}^n$ we have that $\Phi_n(1)(p) = \phi_1(p) = 1(p) = 1$, the function $\Phi_n(1)$ is the unit element of $\mathrm{Fun}(\mathbb{A}^n)$. On the other hand, if f and g are elements of $\Bbbk[x_1, \ldots, x_n]$, then we have that $\Phi_n(fg) = \Phi_n(f)\Phi_n(g)$ because for each element p of $\mathbb{A}^n$ we have that

$$\begin{aligned}\Phi_n(f \cdot g)(p) &= \phi_{f\cdot g}(p) = (f \cdot g)(p) = f(p) \cdot g(p) = \phi_f(p) \cdot \phi_g(p) \\ &= \Phi_n(f)(p) \cdot \Phi_n(g)(p) = (\Phi_n(f) \cdot \Phi_n(g))(p).\end{aligned}$$

All this allows us to conclude that the function Φ_n is a morphism of algebras. □

The map Φ_n of Proposition 1.1.2 is not injective, in general.

Example 1.1.3. Let us suppose that the field $\Bbbk$ is finite and that the integer n is positive. The algebra $\mathrm{Fun}(\mathbb{A}^n)$ is then a finite set — because its elements are functions $\mathbb{A}^n \to \Bbbk$, of which there are finitely many — and the algebra $\Bbbk[x_1, \ldots, x_n]$ is an infinite set. It follows immediately from this that the map Φ_n is not injective in that case.

However, our next proposition tells us that this example describes, in fact, the *only* case in which the map Φ_n is not injective.

Proposition 1.1.4. *The map* $\Phi_n \colon \Bbbk[x_1, \ldots, x_n] \to \mathrm{Fun}(\mathbb{A}^n)$ *is injective if and only if the field* $\Bbbk$ *is infinite or* n *is* 0.

Proof. Example 1.1.3 shows that the condition given by the proposition is necessary. Let us show that it is also sufficient. It is clear that the map Φ_n is an isomorphism if n is 0, so we may suppose that the field $\Bbbk$ is infinite and that the integer n is positive. Let us consider a non-zero element f of $\Bbbk[x_1, \ldots, x_n]$. We will show that $\Phi_n(f) \neq 0$ proceeding by induction with respect to n.

Let us suppose first that n is 1. The polynomial f, which is a non-zero element of $\Bbbk[x_1]$, has finitely many roots in $\Bbbk$ and, since the field $\Bbbk$ is infinite, there is then an element p of $\Bbbk$ such that $f(p) \neq 0$. As then $\Phi_n(f)(p) = f(p) \neq 0$, we have that $\Phi_n(f) \neq 0$, as we want.

Let us now suppose that n is greater than 1. Viewing the algebra $\Bbbk[x_1, \dots, x_n]$ as the polynomial algebra $\Bbbk[x_1, \dots, x_{n-1}][x_n]$, we see that there are a non-negative integer d and elements $f_0, \dots, f_d$ of $\Bbbk[x_1, \dots, x_{n-1}]$ such that $f = f_0 + f_1 x_n + \cdots + f_d x_n^d$. As f is not zero, there is an element j of $[\![0, d]\!]$ such that $f_j \neq 0$, and the inductive hypothesis implies that $\Phi_{n-1}(f_j) \neq 0$, so that there is an element $q = (q_1, \dots, q_{n-1})$ of $\mathbb{A}^{n-1}$ such that $f_j(q) = \Phi_{n-1}(f_j)(q) \neq 0$.

For each i in $[\![0, d]\!]$ let $a_i \coloneqq f_i(q)$, and let us consider the element $g \coloneqq a_0 + a_1 x + \cdots + a_d x^d$ of $\Bbbk[x]$. Since $a_j = f_j(q) \neq 0$, this polynomial g is not zero, so, just as before, there is an element t of $\Bbbk$ such that $g(t) \neq 0$. The point $p \coloneqq (q_1, \dots, q_{n-1}, t)$ of $\mathbb{A}^n$ is then such that

$$f(p) = f_0(q) + f_1(q)t + \cdots + f_d(q)t^d = g(t) \neq 0,$$

and therefore $\Phi_n(f) \neq 0$. This completes the induction. □

The special case of this proposition in which the ground field $\Bbbk$ is not only infinite but algebraically closed can be dealt with in a more expedient way using the *Nullstellensatz*.

Proof of Proposition 1.1.4 when $\Bbbk$ is algebraically closed. Let us suppose that the ground field $\Bbbk$ is algebraically closed, and let f be an element of $\Bbbk[x_1, \dots, x_n]$ such that $f(p) = 0$ for all p in $\mathbb{A}^n$ or, equivalently, using the notation of Corollary A.11.3, such that $f \in \mathfrak{m}_p$ for all p in $\mathbb{A}^n$. According to that corollary, the set $\{\mathfrak{m}_p : p \in \mathbb{A}^n\}$ is the set of all maximal ideals of $\Bbbk[x_1, \dots, x_n]$, so we have that

$$f \in \bigcap_{p \in \mathbb{A}^n} \mathfrak{m}_p = \bigcap_{\mathfrak{m} \in \operatorname{Spm} \Bbbk[x_1, \dots, x_n]} \mathfrak{m} = \operatorname{Nil}(\Bbbk[x_1, \dots, x_n]) = 0,$$

since $\Bbbk[x_1, \dots, x_n]$ is an integral domain. □

The morphism Φ_n of Proposition 1.1.2 is also not surjective, in general.

Example 1.1.5. If f is a non-zero element of $\Bbbk[x_1]$, then the function $\phi_f \colon p \in \mathbb{A}^1 \mapsto f(p) \in \Bbbk$ vanishes precisely at the roots of f, and there are finitely many of these. Let us now suppose that the field $\Bbbk$ is infinite, and consider the function $\phi \colon \mathbb{A}^1 \to \Bbbk$ that on each element p of $\mathbb{A}^1$ takes the value

$$\phi(p) = \begin{cases} 1 & \text{if } p = 0; \\ 0 & \text{otherwise.} \end{cases}$$

As this function is not identically zero yet vanishes on an infinite subset of $\Bbbk$, our observation implies that there is no polynomial f in $\Bbbk[x_1]$ such that $\phi = \phi_f$.

In this example we supposed that the field $\Bbbk$ is infinite. The following proposition shows that we were forced to do that.

Proposition 1.1.6. *Let us suppose that the ground field $\Bbbk$ is finite. The morphism of algebras $\Phi_n\colon \Bbbk[x_1,\dots,x_n] \to \mathrm{Fun}(\mathbb{A}^n)$ is surjective.*

Proof. Let N be the cardinal of $\Bbbk$. As the multiplicative group $\Bbbk^\times$ has order $N-1$, it follows immediately from Lagrange's theorem that for all t in $\Bbbk$ we have

$$t^{N-1} = \begin{cases} 0 & \text{if } t = 0; \\ 1 & \text{otherwise.} \end{cases}$$

For each element $p = (p_1,\dots,p_n)$ of $\mathbb{A}^n$ the polynomial

$$f_p \coloneqq \prod_{i=1}^{n} (1 - (x_i - p_i)^{N-1})$$

of $\Bbbk[x_1,\dots,x_n]$ is then such that $f_p(p) = 1$ and $f_p(q) = 0$ for all q in $\mathbb{A}^n \setminus \{p\}$. If now $\phi\colon \mathbb{A}^n \to \Bbbk$ is any function on $\mathbb{A}^n$, then clearly we have that

$$\phi(q) = \sum_{p \in \mathbb{A}^n} \phi(p) f_p(q)$$

for all q in $\mathbb{A}^n$, so that, in fact,

$$\phi = \Phi_n\left(\sum_{p \in \mathbb{A}^n} \phi(p) f_p\right).$$

This shows that the map Φ_n is surjective. □

The functions that are in the image of the morphism Φ_n are particularly important for us, so we give them a name.

Definition 1.1.7.

- A function $\phi\colon \mathbb{A}^n \to \Bbbk$ is a ***polynomial function*** if it belongs to the image of the morphism Φ_n of Proposition 1.1.2, that is, if there is a polynomial f in $\Bbbk[x_1,\dots,x_n]$ such that for all points p of $\mathbb{A}^n$ we have $\phi(p) = f(p)$.
- We write $\Bbbk[\mathbb{A}^n]$ for the subset of $\mathrm{Fun}(\mathbb{A}^n)$ of all polynomial functions on $\mathbb{A}^n$.

Of course, since the set $\Bbbk[\mathbb{A}^n]$ is the image of the function Φ_n, which is a morphism of algebras, it is a subalgebra of $\mathrm{Fun}(\mathbb{A}^n)$ and we may consider the corestriction of that morphism to $\Bbbk[\mathbb{A}^n]$.

Proposition 1.1.8. *The function*

$$f \in \Bbbk[x_1, \ldots, x_n] \mapsto \phi_f \in \Bbbk[\mathbb{A}^n]$$

is an isomorphism of algebras if and only if the field $\Bbbk$ *is infinite or* n *is* 0.

Proof. The map is the corestriction of Φ_n to its image, so it is a surjective morphism of algebras and, according to Proposition 1.1.4, it is injective if and only if the field $\Bbbk$ is infinite or n is 0. □

In what follows we will work, for the most part, with algebraically closed ground fields, which are infinite, and in that situation the map of this proposition is an isomorphism. We will view it as an identification, and make no distinction between a polynomial in $\Bbbk[x_1, \ldots, x_n]$ and the polynomial function on $\mathbb{A}^n$ that it determines.

Exercise 1.1.9. Since $\mathbb{A}^n = \Bbbk^n$, we may regard the affine space $\mathbb{A}^n$ as a vector space as usual.

(a) Show that any linear function $\mathbb{A}^n \to \Bbbk$ is a polynomial function.

(b) Let $(\lambda_1, \ldots, \lambda_n)$ be an ordered basis for the dual space $(\mathbb{A}^n)^*$ of $\mathbb{A}^n$. Show that the unique morphism of algebras $\omega\colon \Bbbk[x_1, \ldots, x_n] \to \Bbbk[\mathbb{A}^n]$ such that $\omega(x_i) = \lambda_i$ for each i in $[\![n]\!]$ is an isomorphism, and therefore that the set $\{\lambda_1, \ldots, \lambda_n\}$ generates $\Bbbk[\mathbb{A}^n]$ as an algebra.

1.2. Algebraic subsets

Using polynomial functions we now define the class of subsets of $\mathbb{A}^n$ that interest us most.

Definition 1.2.1. The ***zero locus*** of a subset S of $\Bbbk[x_1, \ldots, x_n]$ is the subset

$$\mathrm{V}(S) \coloneqq \{x \in \mathbb{A}^n : f(x) = 0 \text{ for each } f \text{ in } S\}$$

of $\mathbb{A}^n$. If the set S is finite and $f_1, \ldots, f_m$ are its elements, then we write $\mathrm{V}(f_1, \ldots, f_m)$ instead of $\mathrm{V}(S)$.

The next proposition describes the basic properties of this construction.

Proposition 1.2.2.

(*i*) *If* S *and* T *are two subsets of* $\Bbbk[x_1, \ldots, x_n]$ *such that* $S \subseteq T$, *then* $\mathrm{V}(S) \supseteq \mathrm{V}(T)$.

(*ii*) *If* S *and* T *are two subsets of* $\Bbbk[x_1, \ldots, x_n]$, *then* $\mathrm{V}(S) \cup \mathrm{V}(T) = \mathrm{V}(ST)$.

(*iii*) *If* $\mathscr{S}$ *is a set of subsets of* $\Bbbk[x_1, \ldots, x_n]$, *then* $\bigcap_{S \in \mathscr{S}} \mathrm{V}(S) = \mathrm{V}(\bigcup_{S \in \mathscr{S}} S)$.

In (*ii*) we are writing ST for the subset $\{st : s \in S, t \in T\}$ of $\Bbbk[x_1, \ldots, x_n]$.

Proof. (*i*) Let S and T be two subsets of $\Bbbk[x_1, \dots, x_n]$, and let us suppose that $S \subseteq T$. If p is an element of $\mathrm{V}(T)$ then for each element f of S we have that $f \in T$, so that $f(p) = 0$, and this tells us that p is in $\mathrm{V}(S)$.

(*ii*) Let again S and T be two subsets of $\Bbbk[x_1, \dots, x_n]$. If p is an element of $\mathrm{V}(S)$ and h is an element of ST, so that there are elements f and g of S and of T such that $h = fg$, then we have that $h(p) = f(p)g(p) = 0$ because $f(p) = 0$: this tells us that p is in $\mathrm{V}(ST)$. It follows from this that $\mathrm{V}(S) \subseteq \mathrm{V}(ST)$, and similarly we can see that $\mathrm{V}(T) \subseteq \mathrm{V}(ST)$, so that $\mathrm{V}(S) \cup \mathrm{V}(T) \subseteq \mathrm{V}(ST)$.

Let now p be an element of $\mathbb{A}^n$ that is not in $\mathrm{V}(S) \cup \mathrm{V}(T)$, so that there are elements f and g of S and of T, respectively, such that $f(p) \neq 0$ and $g(p) \neq 0$. The polynomial $h \coloneqq fg$ then belongs to ST and is such that $h(p) = f(p)g(p) \neq 0$: this shows that p is not in $\mathrm{V}(ST)$. We can conclude from this that $\mathrm{V}(ST) \subseteq \mathrm{V}(S) \cup \mathrm{V}(T)$.

(*iii*) If T is an element of $\mathscr{S}$, then of course $T \subseteq \bigcup_{S \in \mathscr{S}} S$, so that according to (*i*) we have that $\mathrm{V}(T) \supseteq \mathrm{V}(\bigcup_{S \in \mathscr{S}} S)$, and this implies that $\bigcap_{S \in \mathscr{S}} \mathrm{V}(S) \supseteq \mathrm{V}(\bigcup_{S \in \mathscr{S}} S)$. On the other hand, if p is an element of $\bigcap_{S \in \mathscr{S}} \mathrm{V}(S)$, then for each element f of $\bigcup_{S \in \mathscr{S}} S$ there is an element T of $\mathscr{S}$ such that $f \in T$ and, since $p \in \mathrm{V}(T)$, we have $f(p) = 0$: we see with this that $\mathrm{V}(\bigcup_{S \in \mathscr{S}} S) \supseteq \bigcap_{S \in \mathscr{S}} \mathrm{V}(S)$. □

The following definition allows us to refer to the subsets of $\mathbb{A}^n$ that occur as the zero loci of sets of polynomials in a convenient way.

Definition 1.2.3. A subset X of $\mathbb{A}^n$ is ***algebraic*** if there is a subset S of $\Bbbk[x_1, \dots, x_n]$ such that $X = \mathrm{V}(S)$.

Proposition 1.2.2 implies immediately that the set of algebraic subsets of $\mathbb{A}^n$ is closed under finite unions and arbitrary intersections, and we clearly have that $\varnothing = \mathrm{V}(1)$ and $\mathbb{A}^n = \mathrm{V}(0)$. This gives us the following result.

Proposition 1.2.4. *The set* $\{\mathbb{A}^n \setminus \mathrm{V}(S) : S \subseteq \Bbbk[x_1, \dots, x_n]\}$ *is a topology on the set* $\mathbb{A}^n$.

Proof. As the set of algebraic sets is closed under finite unions and arbitrary intersections, and contains $\varnothing$ and $\mathbb{A}^n$, the set of their complements is closed under finite intersections and arbitrary unions, and contains $\varnothing$ and $\mathbb{A}^n$, so it is a topology on $\mathbb{A}^n$. □

This topology plays a key role in all that follows. Since it was originally considered by Oscar Zariski, we make the following definition.

Definition 1.2.5. The topology described in Proposition 1.2.4 is the ***Zariski topology*** on $\mathbb{A}^n$.

From now on, we will always consider affine spaces as topological spaces with their Zariski topologies. According to this definition, a subset of $\mathbb{A}^n$ is closed for the Zariski topology exactly when it is algebraic. In fact, the Zariski topology has the following characterization.

Exercise 1.2.6. Show that the Zariski topology on $\mathbb{A}^n$ is the coarsest topology on that set with respect to which all algebraic subsets are closed.

We will see later many, many examples of algebraic subsets. For now, let us just present one very simple class.

Example 1.2.7. As $\mathbb{A}^n$ is, as a set, simply $\Bbbk^n$ and this set has a standard structure of a $\Bbbk$-vector space, we can talk about ***linear subspaces*** of $\mathbb{A}^n$. Let us show that

the linear subspaces of $\mathbb{A}^n$ are algebraic subsets.

Let L be a linear subspace of $\mathbb{A}^n$, and let L° be the annihilator of L in the dual space $(\mathbb{A}^n)^*$, that is, the set of all linear maps $\mathbb{A}^n \to \Bbbk$ that vanish on L. We know from *Linear Algebra* that

$$L = \bigcap_{\lambda \in L^\circ} \ker \lambda. \tag{1.1}$$

According to the result of Exercise 1.1.9, the elements of L° are polynomial functions on $\mathbb{A}^n$, so that L° is a subset of $\Bbbk[x_1, \dots, x_n]$. Finally, the equality (1.1) implies immediately that $L = \mathrm{V}(L^\circ)$, so L is an algebraic subset of $\mathbb{A}^n$.

Exercise 1.2.8. Show that, more generally, all affine subspaces of $\mathbb{A}^n$ are algebraic subsets.

As we will see, the Zariski topology is quite different from the usual topologies that we see in calculus and geometry. The following lemma states one thing that it has in common with these other topologies, though.

Proposition 1.2.9. *For every element x of $\mathbb{A}^n$ the set $\{x\}$ is closed, so that the Zariski topology is T_1.*

Proof. If $p = (p_1, \dots, p_n)$ is an element of $\mathbb{A}^n$, then clearly $\{p\} = \mathrm{V}(x_1 - p_1, \dots, x_n - p_n)$, so the set $\{p\}$ is an algebraic subset of $\mathbb{A}^n$ and, therefore, closed. □

On the other hand, the Zariski topology is usually not T_2 or, equivalently, Hausdorff. This will be made clear by Example 1.2.12 below. In any case, it follows from Proposition 1.2.9, of course, that every finite subset of $\mathbb{A}^n$ is closed, and this has the following immediate consequence.

Corollary 1.2.10. *If the field $\Bbbk$ is finite, then the Zariski topology on $\mathbb{A}^n$ is discrete.*

Proof. Indeed, if the field $\Bbbk$ is finite, then the set $\mathbb{A}^n$ is finite and thus all its subsets are closed. □

In general, though, the Zariski topology is much more interesting. The only one that we can

describe in simple terms is the one on the affine line.

Proposition 1.2.11. *A proper subset of $\mathbb{A}^1$ is closed if and only if it is finite.*

In other words, the topology on $\mathbb{A}^1$ is the so-called ***co-finite topology*** on that set.

Proof. We already know that the finite subsets of $\mathbb{A}^1$ are closed. Let, on the other hand, X be a proper and closed subset of $\mathbb{A}^1$, so that there is a subset S of $\Bbbk[x_1]$ such that $X = \mathrm{V}(S)$. Since X is not $\mathbb{A}^1$, we have that $S \nsubseteq \{0\}$, and there is therefore an element f of $\Bbbk[x_1]$ in S. The zero locus $\mathrm{V}(f) = \{p \in \Bbbk^1 : f(p) = 0\}$ of f is finite, since it is precisely the set of roots of f in $\Bbbk$ and, since $\mathrm{V}(S) \subseteq \mathrm{V}(f)$ because $f \in S$, so is the set $X = \mathrm{V}(S)$. □

Using this we can show that, in general, the Zariski topology is not Hausdorff.

Example 1.2.12. Let us suppose that the field $\Bbbk$ is infinite, so that so is the affine line $\mathbb{A}^1$. According to Proposition 1.2.11, any non-empty open subset of $\mathbb{A}^1$ has finite complement, and it follows from this that any two non-empty open subsets of $\mathbb{A}^1$ have non-empty intersection. This implies, in particular, that the elements 0 and 1 of $\mathbb{A}^1$ do not have disjoint neighborhood, so that the Zariski topology on $\mathbb{A}^1$ is not Hausdorff.

A useful consequence of the description of the topology of $\mathbb{A}^1$ is that we can show that polynomial functions are continuous with respect to Zariski topologies, in the following precise sense.

Proposition 1.2.13. *Any polynomial function $\mathbb{A}^n \to \mathbb{A}^1$ is continuous with respect to the Zariski topologies on $\mathbb{A}^n$ and on $\mathbb{A}^1$.*

Proof. Let f be an element of $\Bbbk[x_1, \ldots, x_n]$, and let us view f as a polynomial function $p \in \mathbb{A}^n \mapsto f(p) \in \mathbb{A}^1$. To prove that this function is continuous it is enough that we show that the preimage of any closed subset F of $\mathbb{A}^1$ is closed in $\mathbb{A}^n$, and in fact, in view of Proposition 1.2.11, it is enough to do this in the special case in which the set F is of the form $\{a\}$ for some element a of $\Bbbk$. This is easy: if a is an element of $\Bbbk$, then the preimage of $\{a\}$ is the set $\mathrm{V}(f - a)$, the zero locus of the polynomial $f - a$, and is therefore closed in $\mathbb{A}^n$. □

Exercise 1.2.14. Let us consider on the field $\Bbbk$ the topology $\tau \coloneqq \{\varnothing, \{0\}, \Bbbk\}$ or the cofinite topology. Show that in both cases the Zariski topology on $\mathbb{A}^n$ is the coarsest topology on that set with respect to which all polynomial functions $\mathbb{A}^n \to \Bbbk$ are continuous.

The fields $\mathbb{R}$ and $\mathbb{C}$ have standard topologies, determined by their Euclidean metrics. As the affine spaces $\mathbb{A}^n_{\mathbb{R}}$ and $\mathbb{A}^n_{\mathbb{C}}$ are, as sets, simply cartesian products of n copies of $\mathbb{R}$ and of $\mathbb{C}$, respectively, we can endow them with the product topologies coming from those factors: we call

these topologies the ***Euclidean topologies*** on $\mathbb{A}^n_{\mathbb{R}}$ and on $\mathbb{A}^n_{\mathbb{C}}$. These topologies are strictly finer than the corresponding Zariski topologies. That they are different is an immediate consequence of the fact that the Euclidean topologies are Hausdorff while the Zariski ones are not, and that they are finer follows from the following observation and the result of Exercise 1.2.6.

Exercise 1.2.15. Let $\mathbb{k}$ be either $\mathbb{R}$ or $\mathbb{C}$. Show that the algebraic subsets of $\mathbb{A}^n$ are closed with respect to the Euclidean topology.

Another observation that one should make is the following. As sets, the affine space $\mathbb{A}^n$ coincides with the cartesian product $\mathbb{A}^1 \times \cdots \times \mathbb{A}^1$, but the Zariski topology on $\mathbb{A}^n$ and the topology on that set obtained as the product of the Zariski topologies on the factors $\mathbb{A}^1$ are not the same, unless the ground field $\mathbb{k}$ is finite — for in this special case the two topologies are clearly both discrete. The following example shows why this is so in the case of the plane.

Example 1.2.16. Let us suppose that the field $\mathbb{k}$ is infinite, and consider the ***diagonal*** of $\mathbb{A}^2$, namely, its subset

$$\Delta \coloneqq \{(p_1, p_2) \in \mathbb{A}^2 : p_1 = p_2\}.$$

This diagonal is an algebraic subset of $\mathbb{A}^2$, since it manifestly coincides with $\mathrm{V}(x_1 - x_2)$, and thus a closed subset of the Zariski topology on $\mathbb{A}^2$. We claim that, on the other hand, it is not a closed subset for the product topology on $\mathbb{A}^2$ coming from the Zariski topology on $\mathbb{A}^1$.

To see this, let $q = (q_1, q_2)$ be a point in $\mathbb{A}^2 \smallsetminus \Delta$. If U is a neighborhood of q with respect to the product topology, then there are open subsets U_1 and U_2 in the Zariski topology of $\mathbb{A}^1$ such that $q \in U_1 \times U_2 \subseteq U$. The subsets $\mathbb{A}^1 \smallsetminus U_1$ and $\mathbb{A}^1 \smallsetminus U_2$ of $\mathbb{A}^1$ are then both proper and closed, so they are finite: since the set $\mathbb{A}^1$ is infinite, there is therefore a point t in $\mathbb{A}^1$ that does not belong to their union or, equivalently, such that $t \in U_1 \cap U_2$. We then have that $(t, t) \in U_1 \times U_2 \subseteq U$ and thus that $\Delta \cap U \neq \varnothing$. This shows that the point q does not have a neighborhood in the product topology of $\mathbb{A}^2$ that is disjoint from Δ, and therefore that the interior of $\mathbb{A}^2 \smallsetminus \Delta$ is empty with respect to that topology. Of course, this tells us that, in particular, Δ is not closed with respect to that topology.

Exercise 1.2.17. Show that the Zariski topology on $\mathbb{A}^n$ is coarser than the product topology on that set obtained as the product of the Zariski topologies of the n factors $\mathbb{A}^1$.

More generally, we cannot "factor" the topology of $\mathbb{A}^n$ in any of the obvious ways.

Exercise 1.2.18. Let $n_1, \ldots, n_k$ be non-negative integers such that $n = n_1 + \cdots + n_k$. Show that the Zariski topology on $\mathbb{A}^n$ is different from the product topology on $\mathbb{A}^{n_1} \times \cdots \times \mathbb{A}^{n_k}$. Here, of course, we are identifying this last cartesian product with $\mathbb{A}^n$ as a set in the natural way.

Nonetheless, the following proposition does hold, and it is very useful.

Proposition 1.2.19. *Let X and Y be algebraic subsets of $\mathbb{A}^m$ and of $\mathbb{A}^n$, respectively. The subset $X \times Y$ is an algebraic subset of $\mathbb{A}^{m+n}$.*

Here, as before, we are identifying in the natural way the sets $\mathbb{A}^{m+n}$ and $\mathbb{A}^m \times \mathbb{A}^n$.

Proof. There are subsets S and T of $\Bbbk[x_1, \dots, x_m]$ and of $\Bbbk[x_1, \dots, x_n]$, respectively, such that $X = \mathrm{V}(S)$ and $Y = \mathrm{V}(T)$. On the other hand, according to Proposition A.1.1, there are morphisms of algebras

$$\alpha\colon \Bbbk[x_1, \dots, x_m] \to \Bbbk[x_1, \dots, x_{m+n}], \qquad \beta\colon \Bbbk[x_1, \dots, x_n] \to \Bbbk[x_1, \dots, x_{m+n}]$$

such that $\alpha(x_i) = x_i$ for each i in $[\![m]\!]$ and $\beta(x_i) = x_{m+i}$ for each i in $[\![n]\!]$. For each element $p = (p_1, \dots, p_{m+n})$ of $\mathbb{A}^{m+n}$ let us write $p' \coloneqq (p_1, \dots, p_m)$ and $p'' \coloneqq (p_{m+1}, \dots, p_{m+n})$, which are points of $\mathbb{A}^m$ and of $\mathbb{A}^n$, respectively; we then have, in view of our identifications, that $p = (p', p'')$. For all p in $\mathbb{A}^{m+n}$ we have

$$\alpha(f)(p) = f(p'), \qquad \beta(g)(p) = g(p'')$$

for all f in $\Bbbk[x_1, \dots, x_m]$ and all g in $\Bbbk[x_1, \dots, x_n]$. Indeed, to check the first of these two equalities it is enough to note that the subset $\{f \in \Bbbk[x_1, \dots, x_m] : \alpha(f)(p) = f(p')\}$ of $\Bbbk[x_1, \dots, x_m]$ is in fact a subalgebra that contains $x_1, \dots, x_m$, so that it in fact coincides with $\Bbbk[x_1, \dots, x_m]$, and the second equality can be checked in the same way.

To prove the proposition, we consider the subset $U \coloneqq \alpha(S) \cup \beta(T)$ of $\Bbbk[x_1, \dots, x_{m+n}]$ and show that $X \times Y = \mathrm{V}(U)$.

- Let p be an element of $X \times Y$, so that $p' \in X$ and $p'' \in Y$. If h is an element of U, then either there is an f in S such that $h = \alpha(f)$, and thus $h(p) = \alpha(f)(p) = f(p') = 0$, or there is a g in T such that $h = \beta(g)$, and this $h(p) = \beta(g)(p) = g(p'') = 0$. In any case we have that $h(p) = 0$, and since this is true for all h in U, we see that $p \in \mathrm{V}(U)$. This shows that $X \times Y \subseteq \mathrm{V}(U)$.
- Let now p be an element of $\mathrm{V}(U)$. If f is an element of S, then $\alpha(f)$ is an element of U and therefore $f(p') = \alpha(f)(p) = 0$: this tells us that $p' \in \mathrm{V}(S) = X$. A similar argument proves that $p'' \in \mathrm{V}(T) = Y$, of course, and thus we have that $p = (p', p'') \in X \times Y$. This proves that $\mathrm{V}(U) \subseteq X \times Y$, and completes the proof of the proposition. □

Exercise 1.2.20. Let F be a finite subset of $\mathbb{A}^n$. It follows from Proposition 1.2.9 that is algebraic and, therefore, that there is a subset S of $\Bbbk[x_1, \dots, x_n]$ such that $F = \mathrm{V}(D)$. Show that if the field $\Bbbk$ is infinite, then it is possible to choose such a subset S of cardinal n.

1.3. Ideals

If X is an algebraic subset of $\mathbb{A}^n$, then there is a subset S of $\Bbbk[x_1, \ldots, x_n]$ such that $X = \mathrm{V}(S)$, but this set S is usually not uniquely determined by X. In this section we consider this phenomenon in some detail.

Proposition 1.3.1. *Let S be a subset of $\Bbbk[x_1, \ldots, x_n]$, and let $\langle S \rangle$ be the ideal generates by S in $\Bbbk[x_1, \ldots, x_n]$. We have $\mathrm{V}(S) = \mathrm{V}(\langle S \rangle)$.*

Proof. Since $S \subseteq \langle S \rangle$, we have that $\mathrm{V}(S) \supseteq \mathrm{V}(\langle S \rangle)$. Let, on the other hand, p be an element of $\mathrm{V}(S)$. If f is an element of $\langle S \rangle$, then there are a non-negative integer k, elements $f_1, \ldots, f_k$ of S, and elements $g_1, \ldots, g_k$ of $\Bbbk[x_1, \ldots, x_n]$ such that $f = \sum_{i=1}^{k} g_i f_i$, and therefore we have that $f(p) = \sum_{i=1}^{k} g_i(p) f_i(p) = 0$ because $f_i(p) = 0$ for each i in $[\![k]\!]$. This tells us that p is in $\mathrm{V}(\langle S \rangle)$ and, therefore, that $\mathrm{V}(S) \subseteq \mathrm{V}(\langle S \rangle)$. □

It follows from this proposition that if two subsets of $\Bbbk[x_1, \ldots, x_n]$ generate the same ideal, then their corresponding zero loci coincide. Thus, for example, for all choices of f, g, and h in $\Bbbk[x_1, \ldots, x_n]$ we have that $\mathrm{V}(f, g) = \mathrm{V}(f, g + hf)$, and using this it is very easy to see that an algebraic set is, in general, the zero locus of many different subsets of $\Bbbk[x_1, \ldots, x_n]$.

An immediate consequence of the proposition is that every algebraic subset is the zero locus of an ideal, of course.

Corollary 1.3.2. *If X is an algebraic subset of $\mathbb{A}^n$, then there is an ideal I of $\Bbbk[x_1, \ldots, x_n]$ such that $X = \mathrm{V}(I)$.*

Proof. If X is an algebraic subset of $\mathbb{A}^n$, then there is a subset S of $\Bbbk[x_1, \ldots, x_n]$ such that $X = \mathrm{V}(S)$, and the ideal $I \coloneqq \langle S \rangle$ is therefore such that $X = \mathrm{V}(I)$. □

Starting from this observation and using a bit of non-trivial algebra — the *Basis Theorem* of David Hilbert — we can prove that every algebraic subset is the zero locus of a *finite* set of polynomials.

Proposition 1.3.3. *Let X be an algebraic subset of $\mathbb{A}^n$. There are a non-negative integer k and polynomials $f_1, \ldots, f_k$ in $\Bbbk[x_1, \ldots, x_n]$ such that $X = \mathrm{V}(f_1, \ldots, f_k)$.*

Proof. Corollary 1.3.2 tells us that there is an ideal I of $\Bbbk[x_1, \ldots, x_n]$ such that $X = \mathrm{V}(I)$ and, since the algebra $\Bbbk[x_1, \ldots, x_n]$ is Noetherian according to Corollary A.4.6, there are a non-negative integer k and elements $f_1, \ldots, f_k$ of I such that $I = \langle f_1, \ldots, f_k \rangle$. We then have that $X = \mathrm{V}(I) = \mathrm{V}(\langle f_1, \ldots, f_k \rangle) = \mathrm{V}(f_1, \ldots, f_k)$. □

Just as an algebraic set is the zero locus of many different sets of polynomials, it is usually also the zero locus of many different ideals. For example, it is clear that the subsets $\mathrm{V}(x_1)$ and $\mathrm{V}(x_1^2)$ of $\mathbb{A}^1$ coincide, so that $\mathrm{V}(\langle x_1\rangle) = \mathrm{V}(\langle x_1^2\rangle)$, yet the ideals $\langle x_1\rangle$ and $\langle x_1^2\rangle$ of $\Bbbk[x_1]$ are different. We can understand this example using the notion of radical presented in Section A.3.

Proposition 1.3.4. *If I is an ideal of $\Bbbk[x_1,\dots,x_n]$, then $\mathrm{V}(\sqrt{I}) = \mathrm{V}(I)$.*

This is why, as we observed above, in $\mathbb{A}^1$ we have that $\mathrm{V}(x_1) = \mathrm{V}(x_1^2)$: the radical of the ideal $\langle x_1^2\rangle$ of $\Bbbk[x_1]$ is the ideal $\langle x_1\rangle$.

Proof. Let I be an ideal of $\Bbbk[x_1,\dots,x_n]$. Since $I \subseteq \sqrt{I}$, we have that $\mathrm{V}(I) \supseteq \mathrm{V}(\sqrt{I})$. On the other hand, if p is an element of $\mathrm{V}(I)$ and f is an element of $\sqrt{I}$, then there is a positive integer k such that $f^k \in I$, so that $f(p)^k = f^k(p) = 0$, and thus $p \in \mathrm{V}(\sqrt{I})$. This shows that $\mathrm{V}(I) \subseteq \mathrm{V}(\sqrt{I})$. □

This proposition allows us to improve the result of Corollary 1.3.2, of course.

Corollary 1.3.5. *If X is an algebraic subset of $\mathbb{A}^n$, then there is a radical ideal I of $\Bbbk[x_1,\dots,x_n]$ such that $X = \mathrm{V}(I)$.*

Proof. Let X be an algebraic subset of $\mathbb{A}^n$. According to Corollary 1.3.2, there is an ideal I of $\Bbbk[x_1,\dots,x_n]$ such that $X = \mathrm{V}(I)$ and Proposition 1.3.4 tells us that we also have $X = \mathrm{V}(\sqrt{I})$. According to Proposition A.3.2, the ideal $\sqrt{I}$ is radical, so this proves the corollary. □

An ideal I of $\Bbbk[x_1,\dots,x_n]$ determines a subset of $\mathbb{A}^n$. Conversely, each subset of $\mathbb{A}^n$ determines an ideal of that algebra as follows.

Definition 1.3.6. The ***ideal*** of a subset X of $\mathbb{A}^n$ is the set

$$\mathrm{I}(X) \coloneqq \{f \in \Bbbk[x_1,\dots,x_n] : f(p) = 0 \text{ for all } p \text{ in } X\}.$$

Luckily, the ideal of a subset is an ideal — things would be somewhat confusing if not.

Proposition 1.3.7. *Let X be a subset of $\mathbb{A}^n$. The ideal $\mathrm{I}(X)$ of X is a radical ideal of $\Bbbk[x_1,\dots,x_n]$ that contains every subset S of $\Bbbk[x_1,\dots,x_n]$ such that $X \subseteq \mathrm{V}(S)$.*

Proof. For each element p of $\mathbb{A}^n$ the evaluation map $\varepsilon_p\colon f \in \Bbbk[x_1,\dots,x_n] \mapsto f(p) \in \Bbbk$ is a morphism of algebras, so its kernel $\ker \varepsilon_p$ is an ideal of $\Bbbk[x_1,\dots,x_n]$. As clearly $\mathrm{I}(X) = \bigcap_{p\in X} \ker \varepsilon_p$, it follows immediately from this that $\mathrm{I}(X)$ is also an ideal of $\Bbbk[x_1,\dots,x_n]$.

Its very definition implies that $\mathrm{I}(X)$ contains every subset S of $\Bbbk[x_1,\dots,x_n]$ such that $X \subseteq \mathrm{V}(S)$. On the other hand, let us suppose that f is an element of $\Bbbk[x_1,\dots,x_n]$ such that

there is a positive integer k for which f^k is in $\mathrm{I}(X)$. For each element p of X we then have that $f(p)^k = f^k(p) = 0$, so that in fact $f(p) = 0$. This tells us that $f \in \mathrm{I}(X)$, and thus that the ideal $\mathrm{I}(X)$ of $\Bbbk[x_1, \ldots, x_n]$ is radical. □

We will need the following result, similar to the first part of Proposition 1.2.2.

Exercise 1.3.8. Let X and Y be two subsets of $\mathbb{A}^n$.
(a) Show that if $X \subseteq Y$, then $\mathrm{I}(X) \supseteq \mathrm{I}(Y)$.
(b) Show that $\mathrm{I}(X \cup Y) = \mathrm{I}(X) \cap \mathrm{I}(Y)$.

An easy consequence of this observation is that we cannot distinguish a subset of $\mathbb{A}^m$ from its Zariski closure using their ideals.

Proposition 1.3.9. *For any subset X of $\mathbb{A}^m$ we have that* $\mathrm{I}(X) = \mathrm{I}(\overline{X})$.

The closure of X is taken here, of course, with respect to the Zariski topology of $\mathbb{A}^n$.

Proof. Let X be a subset of $\mathbb{A}^m$. We have that $\mathrm{I}(\overline{X}) \subseteq \mathrm{I}(X)$ because $\overline{X} \supseteq X$. On the other hand, if f is an element of $\mathrm{I}(X)$, then the function $\overline{f}\colon p \in \mathbb{A}^n \mapsto f(p) \in \mathbb{A}^1$, as in Proposition 1.2.13, is continuous and vanishes on X: as $\{0\}$ is a closed subset of $\mathbb{A}^1$, the function $\bar{f}$ also vanishes on $\overline{X}$, and this means precisely that $f \in \mathrm{I}(\overline{X})$. □

Using this we can describe the zero locus of the ideal of a subset of $\mathbb{A}^n$.

Proposition 1.3.10. *For each subset X of $\mathbb{A}^n$ we have that* $\mathrm{V}(\mathrm{I}(X)) = \overline{X}$.

Proof. It is clear that X is contained in $\mathrm{V}(\mathrm{I}(X))$, since for each element f of $\mathrm{I}(X)$ and each element p of X we have that $f(p) = 0$. As $\mathrm{V}(\mathrm{I}(X))$ is a closed subset of $\mathbb{A}^n$, we therefore have that $\overline{X} \subseteq \mathrm{V}(\mathrm{I}(X))$. On the other hand, since the subset $\overline{X}$ of $\mathbb{A}^n$ is closed, there is an ideal J of $\Bbbk[x_1, \ldots, x_n]$ such that $\overline{X} = \mathrm{V}(J)$. Since $\mathrm{I}(\mathrm{V}(J)) \supseteq J$, the first part of Proposition 1.2.2 and Proposition 1.3.9 imply that

$$\mathrm{V}(\mathrm{I}(X)) = \mathrm{V}(\mathrm{I}(\overline{X})) = \mathrm{V}(\mathrm{I}(\mathrm{V}(J))) \subseteq \mathrm{V}(J) = \overline{X}.$$

The combination of the two inclusions that we have obtained proves the proposition. □

This proposition implies, in particular, that we have $\mathrm{V}(\mathrm{I}(X)) = X$ for all algebraic subsets X of $\mathbb{A}^n$. It is natural to wonder what the relation between an ideal I of $\Bbbk[x_1, \ldots, x_n]$ and the ideal $\mathrm{I}(\mathrm{V}(I))$ is. It is clear that $I \subseteq \mathrm{I}(\mathrm{V}(I))$, but that in general equality will not hold: the ideal $\mathrm{I}(\mathrm{V}(I))$ is radical, while I need not be. In fact, we actually have that $\sqrt{I} \subseteq \mathrm{I}(\mathrm{V}(I))$, since $\sqrt{I}$ is the smallest radical ideal of $\Bbbk[x_1, \ldots, x_n]$ that contains I and $\mathrm{I}(\mathrm{V}(I))$ is a radical ideal that contains I.

The following example shows that this last inclusion need not be an equality, in general.

Example 1.3.11. Let us suppose that $\Bbbk = \mathbb{R}$, and let us consider the ideal $I \coloneqq \langle x_1^2 + 1 \rangle$ of $\mathbb{R}[x_1]$, which is radical because it is prime. We have that $\mathrm{V}(I) = \mathrm{V}(x_1^2 + 1) = \varnothing$, so that $\mathrm{I}(\mathrm{V}(I)) = \mathrm{I}(\varnothing) = \Bbbk[x_1]$, which is different from $\sqrt{I} = I$.

This one-dimensional example works because the field $\mathbb{R}$ is *not* algebraically closed. In fact, this is the only obstruction. Indeed, if I is a proper ideal of $\Bbbk[x_1]$, then there is a non-constant polynomial f in $\Bbbk[x_1]$ such that $I = \langle f \rangle$, and the set $\mathrm{V}(I)$ is equal to the set $\mathrm{V}(f)$ of the roots of f in $\Bbbk$, which is non-empty if $\Bbbk$ is algebraically closed. We can extend this to affine spaces of all dimensions using the *Nullstellensatz*.

Proposition 1.3.12. *Let us suppose that the ground field $\Bbbk$ is algebraically closed. If I is a proper ideal of $\Bbbk[x_1, \ldots, x_n]$, then the set $\mathrm{V}(I)$ is not empty.*

Proof. Let I be a proper ideal of $\Bbbk[x_1, \ldots, x_n]$. As I is proper, there is a maximal ideal $\mathfrak{m}$ of $\Bbbk[x_1, \ldots, x_n]$ that contains I and, according to Corollary A.11.3, there is a point $p = (p_1, \ldots, p_n)$ of $\mathbb{A}^n$ such that $\mathfrak{m} = \langle x_1 - p_1, \ldots, x_n - p_n \rangle$. Since I is contained in $\mathfrak{m}$ and $\mathfrak{m}$ is the set of elements of $\Bbbk[x_1, \ldots, x_n]$ that vanish on p, we see that $p \in \mathrm{V}(I)$. In particular, the set $\mathrm{V}(I)$ is not empty. □

Using a stronger version of the *Nullstellensatz* we can describe the ideal $\mathrm{I}(\mathrm{V}(I))$ for any ideal I of $\Bbbk[x_1, \ldots, x_n]$.

Proposition 1.3.13. *Let us suppose that the ground field $\Bbbk$ is algebraically closed. For any ideal I of $\Bbbk[x_1, \ldots, x_n]$ we have that $\mathrm{I}(\mathrm{V}(I)) = \sqrt{I}$.*

Proof. Let I be an ideal of $\Bbbk[x_1, \ldots, x_n]$, and let f be an element of $\Bbbk[x_1, \ldots, x_n]$ that does not belong to $\sqrt{I}$. According to Corollary A.11.5, there exists then a maximal ideal $\mathfrak{m}$ of $\Bbbk[x_1, \ldots, x_n]$ such that $I \subseteq \mathfrak{m}$ and $f \notin \mathfrak{m}$, and Corollary A.11.3 tells us that there is then a point $p = (p_1, \ldots, p_n)$ in $\mathbb{A}^n$ such that $\mathfrak{m} = \langle x_1 - p_1, \ldots, x_n - p_n \rangle$, so that $\mathfrak{m}$ is the ideal of all elements of $\Bbbk[x_1, \ldots, x_n]$ that vanish on p. As I is contained in $\mathfrak{m}$, the point p is in $\mathrm{V}(I)$, and since f is not in $\mathfrak{m}$, we have that $f(p) \neq 0$, so that $f \notin \mathrm{I}(\mathrm{V}(I))$. This shows that $\mathrm{I}(\mathrm{V}(I)) \subseteq \sqrt{I}$ and, as we already know that $\sqrt{I} \subseteq \mathrm{I}(\mathrm{V}(I))$, proves the proposition. □

This has the following useful special case.

Corollary 1.3.14. *Let us suppose that the ground field $\Bbbk$ is algebraically closed. If f is an irreducible element of $\Bbbk[x_1, \ldots, x_n]$, then $\mathrm{I}(\mathrm{V}(f)) = \langle f \rangle$.*

Proof. Let f be an irreducible element of $\Bbbk[x_1, \ldots, x_n]$, which is prime there because that algebra is a unique factorization domain. The ideal $\langle f \rangle$ is therefore prime, so radical, and we have, according to Proposition 1.3.13, that $\mathrm{I}(\mathrm{V}(f)) = \sqrt{\langle f \rangle} = \langle f \rangle$. □

Another very useful consequence the following property of the function I.

Corollary 1.3.15. *Let us suppose that the ground field $\Bbbk$ is algebraically closed. If X and Y are algebraic subsets of $\mathbb{A}^n$, then $\mathrm{I}(X \cap Y) = \sqrt{\mathrm{I}(X) + \mathrm{I}(Y)}$.*

Proof. Let X and Y be two algebraic subsets of $\mathbb{A}^n$. Since the ideal $\mathrm{I}(X) + \mathrm{I}(Y)$ is generated by its subset $\mathrm{I}(X) \cup \mathrm{I}(Y)$, it follows from Propositions 1.2.2 and 1.3.10 that

$$\mathrm{V}(\mathrm{I}(X) + \mathrm{I}(Y)) = \mathrm{V}(\mathrm{I}(X) \cup \mathrm{I}(Y)) = \mathrm{V}(\mathrm{I}(X)) \cap \mathrm{V}(\mathrm{I}(Y)) = X \cap Y,$$

so that, in view of Proposition 1.3.13, $\sqrt{\mathrm{I}(X) + \mathrm{I}(Y)} = \mathrm{I}(\mathrm{V}(\mathrm{I}(X) + \mathrm{I}(Y))) = \mathrm{I}(X \cap Y)$. □

The radical that appears in the statement of this corollary is necessary.

Example 1.3.16. Let us suppose that the field $\Bbbk$ is algebraically closed, and consider the algebraic subsets $X \coloneqq \mathrm{V}(x)$ and $Y \coloneqq \mathrm{V}(x - y^2)$ of $\mathbb{A}^2$. Since the ideals $\langle x \rangle$ and $\langle x - y^2 \rangle$ are prime, so radical, they are $\mathrm{I}(X)$ and $\mathrm{I}(Y)$, respectively. The ideal $\mathrm{I}(X) + \mathrm{I}(Y) = \langle x, x - y^2 \rangle = \langle x, y^2 \rangle$ is not the ideal of the intersection $X \cap Y$ because it is not radical. Indeed, one can easily check that it contains y^2 and not y.

This example shows that the sum of radical ideals need not be radical. We will see later that elaborating on this observation leads us to a very useful theory of intersection multiplicity. The hypothesis that the field be algebraically closed that appears in Corollary 1.3.15 is also needed for the conclusion to hold.

Example 1.3.17. Let $\Bbbk$ be $\mathbb{R}$, and let us consider the algebraic sets $X \coloneqq \mathrm{V}(x^2 - y)$ and $Y \coloneqq \mathrm{V}(y + 1)$. We have that $X \cap Y = \varnothing$, so that $\mathrm{I}(X \cap Y) = \mathbb{R}[x, y]$.

We need to find $\mathrm{I}(X)$ and $\mathrm{I}(X)$.

- Let us suppose first that f is an element of $\mathrm{I}(X)$. We can find elements g in $\Bbbk[x, y]$ and h in $\Bbbk[x]$ such that such that $f = (x^2 - y)g + h$. As f is in $\mathrm{I}(X)$ for all t in $\mathbb{R}$ we have that

  $$0 = f(t, t^2) = (t^2 - t^2)g(t, t^2) + h(t) = h(t),$$

  since the point (t, t^2) of $\mathbb{A}^2$ is in X, and this implies at once, since the field $\mathbb{R}$ is infinite, that $h = 0$, so that $f = (x^2 - y)g \in \langle x^2 - y \rangle$. As $\langle x^2 - y \rangle \subseteq \mathrm{I}(X)$, this lets us conclude that, in fact, $\mathrm{I}(X) = \langle x^2 - y \rangle$.
- Let now f be an element of $\mathrm{I}(Y)$. There are elements g in $\Bbbk[x, y]$ and h in $\Bbbk[x]$ such that

$f = (y+1)g + h$, and for every t in $\mathbb{R}$ we have that

$$0 = f(t,-1) = ((-1)+1)g(t,-1) + h(t) = h(t)$$

because $(t,-1)$ is in Y, and this tells us that $h = 0$ and, thus, that f is in $\langle y+1\rangle$. It follows from this that $\mathrm{I}(Y) = \langle y+1\rangle$.

In view of this, we have that

$$\mathrm{I}(X) + \mathrm{I}(Y) = \langle x^2 - y, y+1\rangle = \langle x^2+1, y+1\rangle.$$

Since $\mathbb{R}[x,y]/\langle x^2+1, y+1\rangle \cong \mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}$, the ideal $\langle x^2+1, y+1\rangle$ is proper and prime, so radical. We thus see that in this situation we have $\mathrm{I}(X \cap Y) \neq \sqrt{\mathrm{I}(X) + \mathrm{I}(Y)}$.

Combining Propositions 1.3.10 and 1.3.13 we obtain a parametrization of the algebraic subsets of $\mathbb{A}^n$ by radical ideals of $\Bbbk[x_1,\dots,x_n]$ when the ground field is algebraically closed. Let us write

- $\mathrm{Cl}(\mathbb{A}^n)$ for the set of all algebraic subsets of $\mathbb{A}^n$, and
- $\mathrm{Rad}(\Bbbk[x_1,\dots,x_n])$ for the set of all radical ideals of $\Bbbk[x_1,\dots,x_n]$.

We know that for each element X of $\mathrm{Cl}(\mathbb{A}^n)$ the ideal $\mathrm{I}(X)$ belongs to $\mathrm{Rad}(\Bbbk[x_1,\dots,x_n])$, and for each element I of $\mathrm{Rad}(\Bbbk[x_1,\dots,x_n])$ the set $\mathrm{V}(I)$ belongs to $\mathrm{Cl}(\mathbb{A}^n)$, and this tells us that the two functions mentioned in the following corollary actually exist.

Corollary 1.3.18. *Let us suppose that the ground field $\Bbbk$ is algebraically closed. The functions*

$$\mathrm{I}\colon X \in \mathrm{Cl}(\mathbb{A}^n) \mapsto \mathrm{I}(X) \in \mathrm{Rad}(\Bbbk[x_1,\dots,x_n])$$

and

$$\mathrm{V}\colon I \in \mathrm{Rad}(\Bbbk[x_1,\dots,x_n]) \mapsto \mathrm{V}(I) \in \mathrm{Cl}(\mathbb{A}^n)$$

are mutually inverse bijections that reverse inclusions.

Proof. Propositions 1.3.10 and 1.3.13 tell us that the compositions $\mathrm{V}\circ\mathrm{I}$ and $\mathrm{I}\circ\mathrm{V}$ are identities, and the first part of Proposition 1.2.2 and Exercise 1.3.8 tell us that the functions I and V reverse inclusions. □

Under the bijections of this corollary the subsets $\varnothing$ and $\mathbb{A}^n$, which are the unique minimal element and the unique maximal element of $\mathrm{Cl}(\mathbb{A}^n)$, correspond to the improper ideal and to the zero ideal 0 of $\Bbbk[x_1,\dots,x_n]$, respectively, as these are the unique maximal element and the unique minimal element of $\mathrm{Rad}(\Bbbk[x_1,\dots,x_n])$. On the other hand, the subsets of the form $\{p\}$ with p in $\mathbb{A}^n$ are closed in $\mathbb{A}^n$, and they are the elements of $\mathrm{Cl}(\mathbb{A}^n)$ that cover $\varnothing$ so the corresponding ideals in $\mathrm{Rad}(\Bbbk[x_1,\dots,x_n])$ are those that are covered by the improper ideal, that is, the maximal

ideals of $\Bbbk[x_1, \dots, x_n]$. We can rephrase this observation as follows.

Corollary 1.3.19. *Let us suppose that the ground field $\Bbbk$ is algebraically closed.*

(*i*) *If p is a point of $\mathbb{A}^n$, then $\mathfrak{m}_p \coloneqq \mathrm{I}(\{p\})$ is a maximal ideal of $\Bbbk[x_1, \dots, x_n]$.*

(*ii*) *Conversely, if $\mathfrak{m}$ is a maximal ideal of $\Bbbk[x_1, \dots, x_n]$, then there is exactly one point $p_\mathfrak{m}$ of $\mathbb{A}^n$ such that $\mathrm{V}(\mathfrak{m}) = \{p_\mathfrak{m}\}$.*

(*iii*) *The functions*

$$p \in \mathbb{A}^n \mapsto \mathfrak{m}_p \in \operatorname{Spm} \Bbbk[x_1, \dots, x_n], \qquad \mathfrak{m} \in \operatorname{Spm} \Bbbk[x_1, \dots, x_n] \mapsto p_\mathfrak{m} \in \mathbb{A}^n$$

are mutually inverse bijections.

Proof. The claims of (*i*) and of (*ii*) are exactly those of Corollary A.11.3, and that of (*ii*) follows at once from Corollary 1.3.18 together with (*i*) and (*ii*). □

From now on we will make the following convention.

Convention 1.3.20. The ground field $\Bbbk$ is algebraically closed, unless we explicitly say so.

As algebraically closed fields are infinite, in all that follows we will identify the elements of $\Bbbk[x_1, \dots, x_n]$ with the polynomial functions on $\mathbb{A}^n$ that they determine using the isomorphism of Proposition 1.1.8 and, in particular, we will most often write $\Bbbk[\mathbb{A}^n]$ instead of $\Bbbk[x_1, \dots, x_n]$.

Computing the ideal of a subset of affine space or the radical of an ideal can be difficult — the *Nullstellensatz* is often of help in doing that.

Example 1.3.21. Let us find the radical of the ideal $I \coloneqq \langle x^3 - y^6, xy - y^3 \rangle$ of $\Bbbk[x, y]$. If $p = (p_1, p_2)$ is an element of $\mathrm{V}(I)$, then either $p_2 = 0$, and then $p_1 = 0$, or $p_2 \neq 0$, and then $p_1 = p_2^2$. This tells us that $\mathrm{V}(I) = \{(t^2, t) \in \mathbb{A}^2 : t \in \Bbbk\} = \mathrm{V}(x - y^2)$. Since $x - y^2$ is irreducible in $\Bbbk[x, y]$, it follows from this that $\sqrt{I} = \mathrm{I}(\mathrm{V}(I)) = \mathrm{I}(\mathrm{V}(x - y^2)) = \langle x - y^2 \rangle$.

Exercise 1.3.22. Let f be an element of $\Bbbk[x]$, and let us consider the subset

$$X \coloneqq \{(t, f(t)) \in \mathbb{A}^2 : t \in \Bbbk\}$$

of $\mathbb{A}^2$. Show that X is algebraic and find $\mathrm{I}(X)$.

Exercise 1.3.23.

(a) Show that the union X of the two coordinate axes in $\mathbb{A}^2$ is an algebraic subset and that the ideal $\mathrm{I}(X)$ can be generated by one polynomial.

(b) Show that the union Y of the three coordinate axes in $\mathbb{A}^3$ is an algebraic subset and that the

ideal $\mathrm{I}(Y)$ can be generated by three polynomials but not with two.

Exercise 1.3.24. Show that the subset

$$X \coloneqq \{(t, t^2, t^3) \in \mathbb{A}^3 : t \in \Bbbk\}$$

of $\mathbb{A}^3$ is algebraic and find a generating set for the ideal $\mathrm{I}(X)$ of the minimum possible cardinality.

Exercise 1.3.25. Show that the subset

$$X \coloneqq \{(t^2 - 1, t^3 - t) \in \mathbb{A}^2 : t \in \Bbbk\}$$

of $\mathbb{A}^2$ coincides with $\mathrm{V}(y^2 - x^3 - x^2)$, and find $\mathrm{I}(X)$.

1.4. Coordinate algebras of algebraic subsets

We now extend the notion of polynomial functions to functions defined on algebraic subsets of affine space.

Definition 1.4.1. Let X be a subset of $\mathbb{A}^n$.

- A function $\phi\colon X \to \Bbbk$ is a ***polynomial function*** if there exists a polynomial function $f\colon \mathbb{A}^n \to \Bbbk$ such that $\phi = f|_X$.
- We write $\Bbbk[X]$ for the subset of $\mathrm{Fun}(X)$ of all polynomial functions on X.

Let us notice that when the subset X in this definition is empty there is a unique function $X \to \Bbbk$, the empty function, and it is a polynomial function. The algebra $\Bbbk[X]$ is then the zero algebra — in which we have that $1 = 0$.

Let X be a subset of $\mathbb{A}^n$. The function

$$f \in \mathrm{Fun}(\mathbb{A}^n) \mapsto f|_X \in \mathrm{Fun}(X)$$

given by restriction to X is a morphism of algebras. As $\Bbbk[\mathbb{A}^n]$ is a subalgebra of $\mathrm{Fun}(\mathbb{A}^n)$, its image by this function, which is precisely the set $\Bbbk[X]$, is therefore a subalgebra of $\mathrm{Fun}(X)$, and the function above restricts to a surjective morphism of algebras

$$\phi\colon \Bbbk[\mathbb{A}^n] \to \Bbbk[X].$$

The kernel of this map is the ideal $\mathrm{I}(X)$ of $\Bbbk[\mathbb{A}^n]$, and the *First Isomorphism Theorem* then allows us to conclude that the map

$$\bar{\phi}\colon \Bbbk[\mathbb{A}^n]/\mathrm{I}(X) \to \Bbbk[X]$$

induced by ϕ, which has $\bar{\phi}(f + \mathrm{I}(X)) = \phi(f)$ for each f in $\Bbbk[\mathbb{A}^n]$, is an isomorphism. We will often view this isomorphism as an identification.

Definition 1.4.2. The ***coordinate algebra*** of an algebra subset X of $\mathbb{A}^n$ is the algebra $\Bbbk[X]$.

Let us remark that a polynomial function on $\mathbb{A}^n$, when we view this set as an algebraic subset of $\mathbb{A}^n$, is the same as a polynomial function on $\mathbb{A}^n$ in the sense of Definition 1.1.7, so that the notation $\Bbbk[\mathbb{A}^n]$ refers here and in Section 1.1 to the same algebra.

Exercise 1.4.3. Show that the coordinate algebra of a non-empty algebraic subset X of $\mathbb{A}^n$ is a field if and only if X has exactly one point.

The first observation that we have to make about coordinate algebras is the following one.

Proposition 1.4.4. *The coordinate algebra of an algebraic subset X of $\mathbb{A}^n$ is a finitely generated algebra with no non-zero nilpotent elements.*

In particular, that algebra is Noetherian.

Proof. If X is an algebraic subset of $\mathbb{A}^n$, then $\Bbbk[X]$ is the quotient $\Bbbk[\mathbb{A}^n]/\mathrm{I}(X)$ and it is therefore finitely generated because $\Bbbk[\mathbb{A}^n]$ is finitely generated, and it has no non-zero nilpotent elements because the ideal $\mathrm{I}(X)$ is radical. □

This proposition has the following partial converse.

Exercise 1.4.5. Show that every finitely generated algebra without non-zero nilpotent elements is isomorphic to the coordinate algebra of some algebraic subset of $\mathbb{A}^n$ for some non-negative integer n.

The coordinate algebra of a closed subset plays the same role as the algebra of polynomial functions on affine space. In particular, Corollaries 1.3.18 and 1.3.19 have analogues for algebraic subsets.

Definition 1.4.6. Let X be an algebraic subset of $\mathbb{A}^n$.

- For each subset S of $\Bbbk[X]$ we put $\mathrm{V}_X(S) \coloneqq \{p \in X : f(p) = 0 \text{ for all } f \text{ in } S\}$.
- For each subset Y of X we put $\mathrm{I}_X(Y) \coloneqq \{f \in \Bbbk[X] : f(p) = 0 \text{ for all } p \text{ in } Y\}$.

These two constructions have properties entirely similar to the corresponding constructions on affine space.

Exercise 1.4.7. Let X be an algebraic subset of $\mathbb{A}^n$.

(*i*) If S and T are subsets of $\Bbbk[X]$ such that $S \subseteq T$, then, $\mathrm{V}_X(S) \supseteq \mathrm{V}_X(T)$.
(*ii*) If S and T are subsets of $\Bbbk[X]$, then $\mathrm{V}_X(S) \cup \mathrm{V}_X(T) = \mathrm{V}_X(ST)$.
(*iii*) If $\mathscr{S}$ is a set of subsets of $\Bbbk[X]$, then $\bigcap_{S\in\mathscr{S}} \mathrm{V}_X(S) = \mathrm{V}_X(\bigcup_{S\in\mathscr{S}} S)$.
(*iv*) If S is a subset of $\Bbbk[X]$ and $\langle S\rangle$ is the ideal of $\Bbbk[X]$ that it generates, then $\mathrm{V}_X(S) = \mathrm{V}_X(\langle S\rangle)$.
(*v*) If I is an ideal of $\Bbbk[X]$, then $\mathrm{V}_X(\sqrt{I}) = \mathrm{V}_X(I)$.

The first three parts of this exercise imply, just as in Proposition 1.2.4, that the sets of the form $\mathrm{V}_X(S)$, with S a subset of $\Bbbk[X]$, are the closed sets of a topology on X.

Proposition 1.4.8. *Let X be an algebraic subset of $\mathbb{A}^n$. The set $\tau_X \coloneqq \{X \setminus \mathrm{V}_X(S) : S \subseteq \Bbbk[X]\}$ is a topology on X, which coincides with the topology induced on X by the Zariski topology of $\mathbb{A}^n$.*

From now on we will consider every algebraic subset of $\mathbb{A}^n$ as a topological space with respect to the topology described in this proposition. This topology is T_1, since that of $\mathbb{A}^n$ is T_1, and therefore the topology of every finite algebraic subset of $\mathbb{A}^n$ is discrete.

Proof. That the set τ_X is a topology on X follows immediately from the results of the first three parts of Exercise 1.4.7 and the facts that $\mathrm{V}_X(0) = X$ and $\mathrm{V}_X(1) = X$.

Let $\pi\colon f \in \Bbbk[\mathbb{A}^n] \mapsto f|_X \in \Bbbk[X]$ be restriction map, which is surjective and whose kernel is $\mathrm{I}(X)$.

- Let F be a subset of X that is closed with respect to the topology τ_X, so that there is a subset S of $\Bbbk[X]$ such that $F = \mathrm{V}_X(S)$. According to part (*d*) of Exercise 1.4.7 the ideal $I \coloneqq \langle S\rangle$ is such that $F = \mathrm{V}_X(I)$. Let us consider the ideal $J \coloneqq \pi^{-1}(I)$ of $\Bbbk[\mathbb{A}^n]$. If p is an element of F and g is an element of J, so that $g|_X = \pi(g) \in I$, then we have that $g(p) = g|_X(p) = 0$: this shows that $F \subseteq \mathrm{V}(J)$. Let, on the other hand, p be an element of $\mathrm{V}(J)$. As $\mathrm{I}(X) = \ker\phi \subseteq J$, we have that $p \in X$. Moreover, if f is an element of I, then there is an element g of $\Bbbk[X]$ such that $\pi(g) = f$, so that $g \in J$, and therefore $f(p)$, which makes sense because p is in X, is the same as $g|_F(p) = g(p) = 0$: this shows that $p \in F$, and thus that $F \supseteq \mathrm{V}(J)$.

  We have with with this that the closed subsets of X with respect to τ_X are closed in $\mathbb{A}^n$.
- If F is a closed subset of $\mathbb{A}^n$, so that there is an ideal I of $\Bbbk[\mathbb{A}^n$ such that $F = \mathrm{V}(I)$, then the ideal $J \coloneqq \pi(\mathrm{I}(X) + I)$ is such that $\mathrm{V}_X(J) = \mathrm{V}(I(X) + I) = \mathrm{V}(I(X)) \cap \mathrm{V}(I) = X \cap F$, and this tells us that the intersection $X \cap F$ is closed with respect to the topology τ_X.

These two observations imply that the topology τ_X is the topology induced by the Zariski topology of $\mathbb{A}^n$ on X. □

Exercise 1.4.9. Let X be an algebraic subset of $\mathbb{A}^n$. Show that every polynomial function on X is continuous.

Exercise 1.4.10. Let X be an algebraic subset of $\mathbb{A}^n$.

(*i*) If Y and Z are subsets of X such that $Y \subseteq Z$, then $\mathrm{I}_X(Y) \supseteq \mathrm{I}_X(Z)$.

(*ii*) If Y and Z are subsets of X, then $\mathrm{I}_X(X \cup Y) = \mathrm{I}_X(Y) \cap \mathrm{I}_X(Z)$.

(*iii*) For every subset Y of X the ideal $\mathrm{I}_X(Y)$ is the smallest radical ideal of $\Bbbk[X]$ that contains every subset S of $\Bbbk[X]$ such that $X \subseteq V_X(S)$.

On an algebraic subset of $\mathbb{A}^n$ we have analogues of the *Nullstellensatz*, like the following one.

Proposition 1.4.11. *Let X be an algebraic subset of $\mathbb{A}^n$. If I is an ideal of $\Bbbk[X]$, then $\mathrm{I}_X(\mathrm{V}_X(I)) = \sqrt{I}$.*

Proof. Let I be an ideal of $\Bbbk[X]$. As $I \subseteq \mathrm{I}_X(\mathrm{V}_X(X))$ and the ideal $\mathrm{I}_X(\mathrm{V}_X(X))$ is radical, we have that $\sqrt{I} \subseteq \mathrm{I}_X(\mathrm{V}_X(I))$. In order prove the converse inclusion, let us consider an element f of $\Bbbk[X]$ that is not in $\sqrt{I}$. Corollary A.11.5 tells us that there is a maximal ideal $\mathfrak{m}$ of $\Bbbk[X]$ such that $f \notin \mathfrak{m}$ and $I \subseteq \mathfrak{m}$. Let $\pi\colon \Bbbk[\mathbb{A}^n] \to \Bbbk[X]$ be the restriction map. Since π is surjective, the ideal $\pi^{-1}(\mathfrak{m})$ is maximal in $\Bbbk[\mathbb{A}^n]$ and, according to Corollary A.11.3, there is a point p in $\mathbb{A}^n$ such that $\pi^{-1}(\mathfrak{m}) = \mathrm{I}(\{p\})$. Since $\mathrm{I}(X) = \ker \phi \subseteq \pi^{-1}(\mathfrak{m})$, we have that $p \in \mathrm{V}(\pi^{-1}(\mathfrak{m})) \subseteq \mathrm{V}(\mathrm{I}(X)) = X$. Moreover, there is an element g of $\Bbbk[\mathbb{A}^n]$ such that $\pi(g) = g|_X = f$ and, since $f \notin \mathfrak{m}$, we have that $g \notin \pi^{-1}(\mathfrak{m}) = \mathrm{I}(\{p\})$, so that $f(p) = g|_X(p) = g(p) \neq 0$, and thus $f \notin \mathrm{I}_X(\mathrm{V}_X(I))$. This proves that $\mathrm{I}_X(\mathrm{V}_X(I)) \subseteq \sqrt{I}$ and therefore that $\mathrm{I}_X(\mathrm{V}_X(I)) \sqrt{I}$. □

Just as for the affine space $\mathbb{A}^n$, we can deduce from this result the following description of the closed subsets of an algebraic subset.

Proposition 1.4.12. *Let X be an algebraic subset of $\mathbb{A}^n$, and let us write*

- $\mathrm{Cl}(X)$ *for the set of all algebraic subsets of $\mathbb{A}^n$ contained in X, and*
- $\mathrm{Rad}(\Bbbk[X])$ *for the set of all radical ideals of $\Bbbk[X]$.*

The functions $\mathrm{I}_X\colon \mathrm{Cl}(X) \to \mathrm{Rad}(\Bbbk[X])$ and $\mathrm{V}_X\colon \mathrm{Rad}(\Bbbk[X]) \to \mathrm{Cl}(X)$ are mutually inverse bijections that reverse inclusions.

Proof. That the functions I_X and V_X reverse inclusions follows from the first parts of Exercises 1.4.9 and 1.4.7, respectively, and they are mutually inverse because of the following two observations.

- If I is a radical ideal of $\Bbbk[X]$, then Proposition 1.4.11 tells us that $\mathrm{I}_X(\mathrm{V}_X(I)) = I$.
- If Y is a closed subset of X, so that there is a radical ideal I of $\Bbbk[X]$ such that $Y = \mathrm{V}_X(I)$, then $\mathrm{V}_X(\mathrm{I}_X(Y)) = \mathrm{V}_X(\mathrm{I}_X(\mathrm{V}_X(I))) = \mathrm{V}_X(\sqrt{I}) = \mathrm{V}_X(I) = Y$ thanks to Proposition 1.4.11 and result in the last part of Exercise 1.4.7. □

Similarly, we have a bijective correspondence between the set of points of an algebraic subset and the set of maximal ideals of is coordinate algebra.

Exercise 1.4.13. Let X be an algebraic subset of $\mathbb{A}^n$. Prove the following statements.

(a) If p is an element of X, then $\mathfrak{m}_p \coloneqq \mathrm{I}_X(\{p\})$ is a maximal ideal of $\Bbbk[X]$.

(b) If $\mathfrak{m}$ is a maximal ideal of $\Bbbk[X]$, then there is exactly one point $p_{\mathfrak{m}}$ of X such that $\mathrm{V}_X(\mathfrak{m}) = \{p_{\mathfrak{m}}\}$.

(c) The functions $p \in X \mapsto \mathfrak{m}_p \in \operatorname{Spm} \Bbbk[X]$ and $\mathfrak{m} \in \operatorname{Spm} \Bbbk[X] \mapsto p_{\mathfrak{m}} \in X$ are mutually inverse bijections.

1.5. Affine varieties

Definition 1.5.1. A topological space is ***reducible*** if it is the union of two of its proper closed subsets, and it is ***irreducible*** if it is neither empty not reducible.

Notice that empty topological topological spaces are neither reducible nor irreducible. The topological spaces that we usually encounter in analysis are not irreducible. For example, the space $\mathbb{R}$ with its usual Euclidean topology is not irreducible since, for example, it is equal to $(-\infty, 0] \cup [0, +\infty)$.

Example 1.5.2. An infinite set X endowed with the cofinite topology is an irreducible topological space — indeed, the proper closed subsets of X are finite, so X is not the union of two of them. In particular, the affine line $\mathbb{A}^1$, with its Zariski topology, is an irreducible space.

Example 1.5.3. A non-empty discrete topology space is irreducible if and only if it has exactly one point, and thus a finite algebraic subset of $\mathbb{A}^n$ is irreducible if and only if it has exactly one point.

Irreducibility is a property of a topological space, but our topological spaces are most often constructed as *sub*spaces of another space. This is the reason why the following observation is useful.

Lemma 1.5.4. *Let X be a topological space. A subspace Y of X is irreducible if and only if it is not empty and whenever F and G are two closed subsets of X such that $Y \subseteq F \cup G$ one of F or G contains Y.*

Proof. Let Y be a subspace of X, let us suppose that the condition in the lemma is satisfied, and let F and G be two closed subsets of Y such that $Y = F \cup G$. There are closed subsets F_1 and G_1

of X such that $F = F_1 \cap Y$ and $G = G_1 \cap Y$, and $Y = F \cup G = (F_1 \cap Y) \cup (G_1 \cap Y) = (F_1 \cup G_1) \cap Y$, so that, in fact, $Y \subseteq F_1 \cup G_1$. The hypothesis implies then that one of F_1 or G_1 contains Y, so that one of F o G is actually equal to Y. This shows that Y is irreducible, since it is not empty, and therefore that the condition in the lemma is sufficient.

Let us next suppose that the subspace Y is irreducible, and that F and G are two closed subsets of X such that $Y \subseteq F \cup G$. Since the intersections $F \cap Y$ and $G \cap Y$ are closed subsets of Y and $Y = (F \cup G) \cap Y = (F \cap Y) \cup (G \cap Y)$, the irreducibility of Y implies that one of $F \cap Y$ or $G \cap Y$ is equal to Y, so that one of F or G contains Y. This proves that the condition in the lemma is also necessary. □

Exercise 1.5.5. Let X be a topological space. Prove the following statements.

(a) If X is irreducible and U is a non-empty open subset of X, then U is irreducible and dense.

(b) If Y is an irreducible subspace of X, then the closure $\overline{Y}$ is also irreducible.

Exercise 1.5.6. Let X and Y be two topological spaces, and let $f\colon X \to Y$ be a continuous function. Prove that if the space X is irreducible, then the image $f(X)$ of‘f is also irreducible.

Using the notion of irreducibility we can give the following important definition.

Definition 1.5.7. An ***affine variety*** is an irreducible algebraic subset of an affine space.

Since $\mathbb{A}^1$ is an irreducible algebraic subset, it is an affine variety. Similarly, every set of cardinality 1 of $\mathbb{A}^n$ is an irreducible algebraic subset, so an affine variety. Our next result allows us to produce more interesting examples.

Proposition 1.5.8. *Let X be an non-empty algebraic subset of $\mathbb{A}^n$. The following statements are equivalent:*

(a) The algebraic subset X is irreducible and thus an affine variety.

(b) The ideal $\mathrm{I}(X)$ of X is prime.

(c) The coordinate algebra $\Bbbk[X]$ is an integral domain.

Let us recall that the zero ring is not an integral domain, and that a prime ideal is proper.

Proof. Let us suppose that X is irreducible, and let f and g be two elements of $\Bbbk[\mathbb{A}^n]$ such that $fg \in \mathrm{I}(X)$. This implies that $X \subseteq \mathrm{V}(f) \cup \mathrm{V}(g)$ and, since $\mathrm{V}(f)$ and $\mathrm{V}(g)$ are closed subsets of $\mathbb{A}^n$, we know from Lemma 1.5.4 that one of them contain X, so that one of f or g is in $\mathrm{I}(X)$. We see with this that ideal $\mathrm{I}(X)$ is prime, and therefore that the implication $(a) \Rightarrow (b)$ holds.

The implication $(b) \Rightarrow (c)$ is immediate, since $\Bbbk[X] = \Bbbk[\mathbb{A}^n]/\mathrm{I}(X)$ and the algebra $\Bbbk[\mathbb{A}^n]$ is an integral domain.

Finally, set us suppose that the coordinate algebra $\Bbbk[X]$ is an integral domain, let F and G be two closed subsets of X such that $X = F \cup G$. There are then ideals I and J in $\Bbbk[X]$ such that $F = \mathrm{V}_X(I)$ and $\mathrm{V}_X(J)$, and we have that $X = \mathrm{V}_X(I) \cup \mathrm{V}_X(J) = \mathrm{V}_X(IJ)$, so that

$$0 = \mathrm{V}_X(X) = \mathrm{I}_X(\mathrm{V}_X(IJ)) \supseteq IJ.$$

Since $\Bbbk[X]$ is a domain, this tells us one of I of J is the zero ideal, and thus that one of F or G is equal to X. The algebraic subset X is therefore irreducible and an affine variety. This proves the implication $(c) \Rightarrow (a)$, and completes the proof of the proposition. □

As a consequence of this proposition we can parametrize the affine varieties contained in a given affine space. In fact, we can do this more generally for the varieties contained in a given algebraic subset of an affine space.

Corollary 1.5.9. *Let X be an algebraic subset of $\mathbb{A}^n$, and let $\mathrm{Sub}(X)$ be the set of all affine varieties of $\mathbb{A}^n$ that are contined in X.*

(i) For each element $\mathfrak{p}$ of $\operatorname{Spec}\Bbbk[X]$ we have that $\mathrm{V}_X(\mathfrak{p}) \in \mathrm{Sub}(X)$, and for each element Y of $\mathrm{Sub}(X)$ we have that $\mathrm{I}_X(Y) \in \operatorname{Spec}\Bbbk[X]$.

(ii) The functions $\mathfrak{p} \in \operatorname{Spec}\Bbbk[X] \mapsto \mathrm{V}_X(\mathfrak{p}) \in \mathrm{Sub}(X)$ and $Y \in \mathrm{Sub}(X) \mapsto \mathrm{I}_X(Y) \in \operatorname{Spec}\Bbbk[X]$ that we obtain in this way are mutually inverse bijections that reverse inclusions.

Proof. Hacer. □

Using Proposition 1.5.8, it is now easy to give examples of affine varieties.

Example 1.5.10. Let $f \in \Bbbk[\mathbb{A}^n]$ be any irreducible polynomial. The ideal $I \coloneqq \langle f \rangle$ of $\Bbbk[\mathbb{A}^n]$ is then prime and the corresponding algebraic subset of $\mathbb{A}^n$,

$$\mathrm{V}(I) = \mathrm{V}(f)$$

is an affine variety. We call it the ***hypersurface*** defined by f.

Example 1.5.11. Let us consider the function $\sigma\colon t \in \Bbbk \mapsto (t^2, t^3) \in \mathbb{A}^2$ and its image $X \coloneqq \sigma(\Bbbk)$. It is clear that X is contained in $\mathrm{V}(x^3 - y^2)$ and, in fact, the two sets coincide. Indeed, it (p_1, p_2) is an element of $\mathrm{V}(x^3 - y^2)$, then $p_1^3 = p_2^2$: if $p_1 = 0$, then $p = \sigma(0)$, and if $p_1 \neq 0$, then $p_1 = (p_2/p_1)^2$ and $p_2 = (p_2/p_1)^3$, so that $p = \sigma(p_2/p_1)$.

Let us suppose for a moment that the polynomial $x^3 - y^2$ is reducible in $\Bbbk[x, y]$. Since it is clearly not divisible by any non-constant element of $\Bbbk[x]$, there are then elements g_0, g_1, h_0, and h_1 of $\Bbbk[x]$ such that $x^3 - y^2 = (g_0 + g_1 y)(h_0 + h_1 y)$. This implies first that $g_1 h_1 = -1$, so that $g_1 \in \Bbbk$ and $h_1 = -1/g_1$; then, that $g_0 h_1 + g_1 h_0 = 0$, so that $g_0 = g_1^2 h_0$; and finally, that $g_1^2 h_0^2 = g_0 h_0 = x^3$.

As x^3 is not a square in $\Bbbk[x]$, this is absurd.

The polynomial $x^3 - y^2$ is therefore irreducible in $\Bbbk[x, y]$,

$$\mathrm{I}(X) = \mathrm{I}(\mathrm{V}(x^3 - y^2)) = \sqrt{\langle x^3 - y^3 \rangle} = \langle x^3 - y^2 \rangle.$$

As this is prime, the algebraic subset X is irreducible and, therefore, an affine variety.

Example 1.5.12. Let us show that, more generally, if r and s are coprime positive integers, then the subset

$$X \coloneqq \{(t^r, t^s) : t \in \Bbbk\}$$

of $\mathbb{A}^2$ coincides with $\mathrm{V}(x^s - y^r)$ and is an affine variety. It is clear that X is contained in $\mathrm{V}(x^s - y^r)$. Let, on the other hand, $p = (p_1, p_2)$ be an element of this last set, so that $p_1^s = p_2^r$. Since the integers r and s are coprime, there are integers u and v such that $ur + vs = 1$. If $p_1 p_2 \neq 0$, we can consider the scalar $t \coloneqq p_1^v p_2^u$: we then have

$$t^r = p_1^{vr} p_2^{ur} = p_1^{vr} p_1^{us} = p_1, \qquad t^s = p_1^{vs} p_2^{us} = p_2^{vr} p_2^{us} = p_2,$$

and this tells us that p belongs to the set X. We therefore have that $X = \mathrm{V}(x^s - y^r)$. To prove that X is an affine variety it is enough then that we show that the polynomial $x^s - y^r$ is irreducible in $\Bbbk[x, y]$. We will present several arguments for this.

First argument. Let us suppose then that there are two non-constant polynomials g and h in $\Bbbk[x, y]$ such that

$$x^s - y^r = gh. \tag{1.2}$$

The polynomial g is not in $\Bbbk[x]$: were that the case, we could find a root ξ of g and evaluate the equality (1.2) when (x, y) is $(\xi, 1)$ to find a contradiction. In fact, the same argument shows that both variables x and y actually appear both in g and in h.

Viewing now the equality (1.2) first in $\Bbbk[x][y]$ and then in $\Bbbk[y][x]$ tells us that in g and in h the variable x appears with degree at most $s-1$ and the variable y appears with degree at most $r-1$, so that there are scalars $a_{i,j}$ and $b_{i,j}$ in $\Bbbk$ for each i in $[\![0, s-1]\!]$ and each j in $[\![0, r-1]\!]$ such that

$$g = \sum_{i=0}^{s-1} \sum_{j=0}^{r-1} a_{i,j} x^i y^j, \qquad h = \sum_{i=0}^{s-1} \sum_{j=0}^{r-1} b_{i,j} x^i y^j.$$

Let z be a new variable, and let us evaluate both sides of the equality (1.2) when (x, y) is (z^r, z^2): we get the equality $0 = (z^r)^s = (z^r)^r = g(z^r, z^s) h(z^r, z^s)$ in $\Bbbk[z]$. As $\Bbbk[z]$ is an integral domain,

we can the suppose that $g(z^r, z^s) = 0$, so that

$$0 = g(z^r, z^s) = \sum_{i=0}^{s-1}\sum_{j=0}^{r-1} a_{i,j} z^{ir+js} = \sum_{k=0}^{(s-1)r+(r-1)s} \left(\sum_{\substack{i\in[\![0,s-1]\!] \\ j\in[\![0,r-1]\!] \\ ir+js=k}} a_{i,j} \right) z^k. \tag{1.3}$$

Let (i, j) and (i', j') be two elements of $[\![0, s-1]\!] \times [\![0, r-1]\!]$ such that $ir + js = i'r + j's$, so that $(i - i')r = (j' - j)s$ and, since r and s are coprime, $s \mid i - i'$ and $r \mid j - j'$. As i and i' are both in $[\![0, s-1]\!]$ and j and j' are both in $[\![0, r-1]\!]$, this implies that $i = i'$ and $j = j'$. This tells us that each of the sums that appears between parentheses in (1.3) has at most one term, so that term is actually zero. As every coefficient of g appears in one of those sums, we can conclude from this that, in fact, the polynomial g is zero. This is absurd, of course, and this contradiction proves what we want.

Second argument. Let $\Bbbk(x, y)$ be the field of fractions of $\Bbbk[x, y]$, as usual. We start by establishing the following auxiliary fact:

> *there is an isomorphism of algebras $\alpha\colon \Bbbk(x, y) \to \Bbbk(x, y)$ such that $\alpha(x) = x$ and $\alpha(y) = xy$.*

It is clear that there is a morphism of algebras $\alpha_0\colon \Bbbk[x, y] \to \Bbbk[x, y]$ such that $\alpha_0(x) = x$ and $\alpha_0(y) = xy$, and it is injective. Indeed, if f is an element of $\Bbbk[x, y]$ such that $\alpha_0(f) = 0$, then for all s and t in $\Bbbk$ such that $s \neq 0$ we have

$$g(s, t) = g(s, s(t/s)) = \alpha_0(f)(s, t) = 0,$$

and this tells us that the polynomial function g vanishes on the non-empty open subset $\mathbb{A}^2 \smallsetminus \mathrm{V}(x)$: as that function is continuous and that open set is dense in $\mathbb{A}^2$, we see that in fact, $g = 0$. It follows from the fact that α_0 is injective that it has a unique extension to a $\Bbbk$-linear morphism of algebras $\alpha\colon \Bbbk(x, y) \to \Bbbk(x, y)$ to field $\Bbbk(x, y)$. This extension is an isomorphism: it is injective because its domain is a field, and it is surjective because it image contains $x = \alpha(x)$ and $y = \alpha(y/x)$.

Let us suppose for a moment that r and s are two non-negative integers such that $r < s$ and there are non-constant elements g and h in $\Bbbk[x, y]$ such that $x^s - y^r = gh$. We then have that

$$x^r(x^{s-r} - y^r) = x^s - x^r y^r = g(x, xy)h(x, xy).$$

Since x is a prime element in $\Bbbk[x, y]$, it follows from this that there are two non-negative integers k and l such that $r = k + l$ and x^k and x^l divide $g(x, xy)$ and $h(x, xy)$ in $\Bbbk[x, y]$. Let g_1 and h_1 be the elements of $\Bbbk[x, y]$ such that $g(x, xy) = x^k g_1(x, y)$ and $h(x, xy) = x^l h(x, xy)$. We then have that $x^{s-r} - y^r = g_1(x, y)h_1(x, y)$, of course. We claim that the polynomials g_1 and h_1 are not constant. If, for example, g_1 were constant, so an element of $\Bbbk$, we would have that $g(x, xy) = g_1 x^k$.

As g is an element of $\Bbbk(x,y)$ and this tells us that $\alpha(g) = g_1 x^k = \alpha(g_1 x^k)$, we see that, in fact, $g = g_1 x^k$. As g divides $x^s - y^r$, we must then have that $k = 0$, but this is absurd, because the polynomial g is not constant. With this we have shown that

> *if r and s are different positive integers such that $r < s$ and the polynomial $x^s - y^r$ is reducible in $\Bbbk[x,y]$, then the polynomial $x^{s-r} - y^r$ is reducible in $\Bbbk[x,y]$.* (1.4)

It follows from this and the fact that Euclid's algoritm computes the greatest common divisor of two numbers that

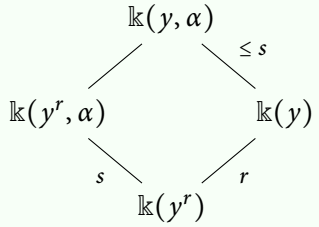
> *if r and s are two coprime positive-integers, then the polynomial $x^s - y^r$ is irreducible in $\Bbbk[x,y]$.*

Let us check this. Suppose that, on the contrary, there exist coprime positive integers r and s such that the polynomial $x^s - y^r$ is reducible in $\Bbbk[x,y]$, and let us choose them so that their sum $r+s$ is as small as possible. We can suppose with any loss of generality that $r < s$. Since $s - r$ and r are two coprime positive integers and their sum is $(s-r) + r = s < s + r$, the way we chose r and s implies at once that the polynomial $x^{s-r} - y^r$ is irreducible in $\Bbbk[x,y]$. This is absurd, as it contradicts our observation (1.4).

Third argument. Let us consider the ring $\Bbbk[y]$, its field of fractions $\Bbbk(y)$, and an algebraic closure Ω of $\Bbbk(y)$. The polynomial $x^s - y^r$ is in $\Bbbk(y)[x]$, so it has a root α in Ω. We consider in Ω the subfield $\Bbbk(y^r, \alpha)$ and its subfield $\Bbbk(y^r)$. As $\Bbbk[y^r]$ is a unique factorization domain in which y^r is a prime element, *Eisenstein's criterion* A.8.15 at the prime ideal $\langle y^r \rangle$ tells us at once that the polynomial $x^s - y^r$ is irreducible in $\Bbbk(y^r)[x]$. As the extension $\Bbbk(y^r, \alpha)$ of $\Bbbk(y^r)$ is generated by a root of that polynomial, it follows that the degree of that extension is $[\Bbbk(y^r, \alpha) : \Bbbk(y^r)] = s$.

The subfield $\Bbbk(y)$ of Ω is also an extension of $\Bbbk(y^r)$, and since y is a root of the polynomial $x^r - y^r$ of $\Bbbk(y^r)[x]$, which is irreducible for the same reason as before, the degree of that extension is $[\Bbbk(y) : \Bbbk(y^r)] = r$. Finally, si α is a root of the polynomial $x^s - y^r$ of $\Bbbk(y)[x]$, we have that $[\Bbbk(y,\alpha) : \Bbbk(y)] \leq s$.

Putting everything together, we see that we have the following diagram of extensions between subfields of Ω and their degrees:



The multiplicativity of the degree tells us that $[\Bbbk(y,\alpha) : \Bbbk(y^r)] \leq rs$ and that that degree is divisible by thje coprime numbers r and s, so that it is also divisible by their product. Of course, this allows

us to conclude that, in fact, $[\Bbbk(y,\alpha):\Bbbk(y^r)] = rs$ and therefore that $[\Bbbk(y,\alpha):\Bbbk(y)] = s$. The minimal polynomial of α over $\Bbbk(y)$ therefore has degree s: since α is a root of $x^s - y^r \in \Bbbk(y)[x]$, this polynomial is that minimal polynomial and, in particular, is irreducible in $\Bbbk(y)[x]$. Since $\Bbbk(y)$ is the fraction field of $\Bbbk[y]$, and the polynomial $x^s - y^r$ is primitive in $\Bbbk[y][x]$, Corollary A.8.12, one of the corollaries of *Gauss's Lemma*, tells us that $x^s - y^r$ is irreducible in $\Bbbk[y][x] = \Bbbk[x,y]$.

Fourth argument. Let us consider the function $\sigma\colon t \in \mathbb{A}^1 \mapsto (t^r, t^s) \in \mathbb{A}^2$, whose image is exactly the set X. Since $\mathbb{A}^1$ is an irreducible space, the result of Exercise 1.5.6 tells us that to pove that X is irreducible it is enough that we show that the function σ is continuous. Let F be a closed subset of $\mathbb{A}^2$, so that there is an ideal I of $\Bbbk[\mathbb{A}^2]$ such that $F = \mathrm{V}(I) = \bigcap_{f\in I}\mathrm{V}(f)$. As $\sigma^{-1}(F) = \bigcap_{f\in I}\sigma^{-1}(\mathrm{V}(f))$, to show that $\sigma^{-1}(f)$ is closed in $]\mathbb{A}^1$ we need only show that for each f in I the set

$$\sigma^{-1}(\mathrm{V}(f)) = \{t \in \mathbb{A}^1 : f(\sigma(t))\}$$

is closed in $\mathbb{A}^1$. Now this is obvious, since for each f in I, the function $t \in \mathbb{A}^1 \mapsto f(\sigma(t)) \in \Bbbk$ is the polynomial function $f(x^r, x^s)$.

Exercise 1.5.13. Show that if r and s are positive integers that are *not* coprime, then the polynomial $x^s - y^r$ is reducible in $\Bbbk[x,y]$ and find its factorization as a product of irreducible elements.

Exercise 1.5.14. As in Example 1.5.12, let us consider the set $X \coloneqq \mathrm{V}(x^s - y^r)$ of $\mathbb{A}^2$. Show that the function $\sigma\colon t \in \mathbb{A}^1 \mapsto (t^r, t^s) \in X$ is a homeomorphism.

1.6. Irreducible components

In general, algebraic subsets of $\mathbb{A}^n$ are not irreducible, so they are not affine varieties. Our objective in this section is to show that, in any case, such an algebraic subset can be written in exactly one way as a union of affine varieties.

It is convenient to prove this in greater generality that what we really need. The set up in which we will work is that of Noetherian spaces, defined as follows.

Definition 1.6.1. A topological space is ***Noetherian*** if the set of its closed subsets, when ordered with the relation of inclusion $\subseteq$, satisfies the descending chain condition.

The topological spaces of analysis usually do not satisfy this condition. For example, in $\mathbb{R}$ we

have the infinite strictly decreasing chain of closed subsets

$$[0,1] \supsetneq [0,1/2] \supsetneq [0,1/2^2] \supsetneq [0,1/2^3] \supsetneq [0,1/2^4] \supsetneq \cdots$$

The spaces that we care about, though, are Noetherian.

Proposition 1.6.2. *An affine variety is a Noetherian topological space.*

Proof. □

Appendix A

Commutative algebra

A.1. Polynomial algebras

Proposition A.1.1. *Let R be a ring, let A be an R-algebra, and let $a = (a_1, \dots, a_n)$ be an element of A^n. There is exactly one morphism of R-algebras $\phi\colon R[x_1, \dots, x_n] \to A$ such that $\phi(x_i) = a_i$ for each i in $[\![n]\!]$.*

Proof. The function $(i_1, \dots, i_n) \in \mathbb{N}_0^n \mapsto x_1^{i_1} \cdots x_n^{i_n} \in R[x_1, \dots, x_n]$ is injective and its image is a basis of $R[x_1, \dots, x_n]$ as a R-module, and it follows from this that there is exactly one R-linear function $\phi\colon R[x_1, \dots, x_n] \to A$ such that $\phi(x_1^{i_1} \cdots x_n^{i_n}) = a_1^{i_1} \cdots a_n^{i_n}$ for each choice of $(i_1, \dots, i_n)$ in $\mathbb{N}_0^n$. This function is a morphism of R-algebras. Indeed, it is clear that

$$\phi(1_{R[x_1,\dots,x_n]}) = x_1^0 \cdots x_n^0 = a_1^0 \cdots a_n^0 = 1_A,$$

and, on the other hand, whenever $(i_1, \dots, i_n)$ and $(j_1, \dots, j_n)$ are two elements of $\mathbb{N}_0^n$ we have that

$$\begin{aligned}\phi(x_1^{i_1} \cdots x_n^{i_n}) \cdot \phi(x_1^{j_1} \cdots x_n^{j_n}) = a_1^{i_1} \cdots a_n^{i_n} \cdot a_1^{j_1} \cdots a_n^{j_n} = a_1^{i_1+j_1} \cdots a_n^{i_n+j_n} = \phi(x_1^{i_1+j_1} \cdots x_n^{i_n+j_n}) \\ = \phi(x_1^{i_1} \cdots x_n^{i_n} \cdot x_1^{j_1} \cdots x_n^{j_n}),\end{aligned}$$

so that ϕ is a morphism of R-algebras follows from Exercise A.1.2 below. This proves the existence claim of the proposition.

To prove now the uniqueness claim, let us suppose that $\phi, \psi\colon R[x_1, \dots, x_n] \to A$ are two morphisms of R-algebras such that $\phi(x_i) = a_i$ and $\psi(x_i) = a_i$ for each choice of i in $[\![n]\!]$. The subset $E \coloneqq \{f \in R[x_1, \dots, x_n] : \phi(f) = \psi(f)\}$ of $R[x_1, \dots, x_n]$ is then a R-subalgebra that

contains the set $\{x_1, \ldots, x_n\}$: since $R[x_1, \ldots, x_n]$ is generated as an R-algebra by this set, we have that, in fact, $E = R[x_1, \ldots, x_n]$, and this means precisely that $\phi = \psi$. □

Exercise A.1.2. Let R be a ring, let A and B be two R-algebras, let X be a subset of A that spans A as an R-module, and let $\phi\colon A \to B$ be a R-linear map. If $\phi(1_A) = 1_B$ and $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$ for all choices of x and y in X, then ϕ is a morphism of R-algebras.

Exercise A.1.3. Let R be a ring, let A and B be two R-algebras, and let $\phi, \psi\colon A \to B$ be two morphisms of R-algebras. Show that the subset $E \coloneqq \{a \in A : \phi(a) = \psi(a)\}$ is an R-subalgebra of A. We call it the ***equalizer*** of ϕ and ψ.

A.2. Localization

In this section we will present one of the main tools of commutative algebra, localization.

A.2.1. Localization of rings

The whole theory starts with the following definition.

Definition A.2.1.1. A subset S of a ring A is ***multiplicatively closed*** if it contains 1 and for all a and b in A we have that

$$a, b \in S \implies ab \in S.$$

There are many examples of multiplicatively closed sets readily available.

Example A.2.1.2. Let A be a ring.

- The set S of all elements of A that are not zero-divisors is multiplicatively closed. In particular, if A is an integral domain, then the set $A \setminus 0$ is multiplicatively closed in A.
- More generally, if $\mathfrak{p}$ is a prime ideal of a ring A, then the set $A \setminus \mathfrak{p}$ is multiplicatively closed in A.
- If f is an element of A, then the set $\{f^n : n \in \mathbb{N}_0\}$ is multiplicatively closed in A.
- The set $S \coloneqq A^\times$ of all units of A is multiplicatively closed.
- If I is an ideal of A, then the set $\{1 + x : x \in I\}$, which we usually write simply $1 + I$, is multiplicatively closed.

Exercise A.2.1.3. Let A be a ring. Show that if S and T are two multiplicatively closed subsets of A, then so is their product $ST \coloneqq \{st : s \in S,\ t \in T\}$.

Exercise A.2.1.4. Let A be a ring, and let X be a subset of A.

(a) Show that there is a multiplicatively closed subset of A that contains X, and that is contained in every multiplicatively closed subset of A that contains X. We call it the multiplicatively closed subset of A ***generated*** by the set X.

(b) Show that that multiplicatively closed subset is the set of all elements of A of the form $s_1^{k_1} \cdots s_n^{k_n}$ with n in $\mathbb{N}_0$, $s_1, \ldots, s_n$ in S, and $k_1, \ldots, k_n$ in $\mathbb{N}_0$.

Exercise A.2.1.5. Let A be a ring. We say that a multiplicatively closed subset S of A is ***saturated*** if for all a and b in A we have that

$$ab \in S \implies a \in S.$$

(a) Show that for any multiplicatively closed subset S of A the set of all saturated multiplicatively closed subsets of A that contain S has a unique minimal element. We call it the ***saturation*** of S.

(b) Show that the group of units $A^\times$ of A is contained in every saturated multiplicatively closed subset of A, and that it is therefore the minimal saturated multiplicatively closed subset of A.

(c) Show that if S is a multiplicatively closed subset of A, then the saturation $\overline{S}$ of S is such that

$$A \setminus \overline{S} = \bigcup \{\mathfrak{p} \in \operatorname{Spec} A : \mathfrak{p} \cap S = \varnothing\}.$$

(d) Let I be an ideal of A. Show that the saturation of the multiplicatively closed subset $1 + I$ is the set $\{a \in A : a + I \in (A/I)^\times\}$.

Hint: To prove (b), start by showing that if a is an element of $A \setminus S$, then there is among the ideals of A that contain a and are disjoint from S a maximal one, and that it is prime.

The first step in the construction of the localization of a ring is the following observation.

Lemma A.2.1.6. *Let A be a ring, and let S be a multiplicatively closed subset of A. The relation $\sim$ on the set $A \times S$ for which*

$$(a, s) \sim (b, t) \iff \textit{there is an element } u \textit{ in } S \textit{ such that } u(at - bs) = 0$$

is an equivalence relation.

Proof. □

As we will see, this equivalence relation does all that we want from it and does it well. The

following remark explains why we do not use a probably more natural alternative.

Exercise A.2.1.7. Let A be a ring, and let S be a multiplicatively closed subset of A.

(a) Show the relation $\sim'$ on the set $A \times S$ that for all elements (a, s) and (b, t) of $A \times S$ satisfies

$$(a, s) \sim' (b, t) \iff at - bs = 0.$$

is reflexive and symmetric, but not, in general, transitive.

(b) Show that the relations $\sim$ of Lemma A.2.1.6 and $\sim'$ of (a) coincide when the ring A is an integral domain or, more generally, when the elements of S are all non-zero divisors.

As any equivalence relation does, the relation $\sim$ defined in Lemma A.2.1.6 determines a set of equivalence classes.

Definition A.2.1.8. Let A be a ring, and let S be a multiplicatively closed subset of A.

- We write A_S for the set of equivalence classes of the relation $\sim$ of Lemma A.2.1.6 in $A \times S$.
- If (a, s) is an element of $A \times S$, then we write a/s for the equivalence class of (a, s) in A_S.

We call an equivalence class a/s in A_S a ***fraction***. In view of the way we defined these fractions, when a and b are elements of A and s and t are elements of S, we have that

$$a/s = b/t \iff \text{there is an element } u \text{ of } S \text{ such that } u(ta - sb) = 0.$$

In particular, of course, we have that

$$a/s = (ta)/(ts) \text{ whenever } a \text{ is an element of } A \text{ and } s \text{ and } t \text{ are elements of } S.$$

The following exercise shows that if we want this to be true — and we certainly do! — then we are more or less forced to proceed as we did to construct the set A_S.

Exercise A.2.1.9. Let A be a ring, and let S be multiplicatively closed subset of A, and let us consider the relation

$$Q \coloneqq \{((a, s), (ta, ts)) \in (A \times S) \times (A \times S) : a \in A, s, t \in S\}$$

on the set $A \times S$. Show that the equivalence relation $\sim$ of Lemma A.2.1.6 is the smallest equivalence relation on the set $A \times S$ that contains the set Q.

The next step in the construction of the localization is to turn the set A_S into a ring.

Lemma A.2.1.10. *Let A be a ring, and let S be a multiplicatively closed subset of A.*

(i) There is exactly one function $+ \colon A_S \times A_S \to A_S$ such that

$$a/s + b/t = (ta + sb)/(st)$$

for each choice of (a,s) *and* (b,t) *in* $A \times S$.

(*ii*) *There is exactly one function* $\cdot\colon A_S \times A_S \to A_S$ *such that*

$$a/s \cdot b/t = (ab)/(st)$$

for each choice of (a,s) *and* (b,t) *in* $A \times S$.

(*iii*) *The set* A_S*, when endowed with the operations* $+$ *and* $\cdot$ *described here as addition and multiplication, is a commutative ring in which the zero and unit elements are* $0/1$ *and* $1/1$*, respectively.*

(*iv*) *The function* $\lambda\colon a \in A \mapsto a/1 \in A_S$ *is a morphism of rings and the image* $\lambda(s)$ *of every element* s *of* S *is a unit of* A_S.

Proof. □

This ring we have just constructed is the localization that we want to study.

Definition A.2.1.11. Let A be a ring, and let S be a multiplicatively closed subset of A. The ring A_S is the ***localization*** of A at the multiplicatively closed set S, and the map $\lambda\colon A \to A_S$ in the last part of Lemma A.2.1.10 is the ***localization map*** of A at S.

If it is useful, we will sometimes write $\lambda_{A,S}$ to denote the localization map of A at S. There are two special cases of this construction that have their own special notations.

- If $\mathfrak{p}$ is a prime ideal of A, then we write $A_{\mathfrak{p}}$ for the localization of A at the multiplicatively closed $A \setminus \mathfrak{p}$ and we call it the ***localization at*** $\mathfrak{p}$.
- If f is an element of A, then we write A_f for the localization of A at the multiplicatively closed subset $\{f^n : n \in \mathbb{N}_0\}$ and we call it the ***localization at*** f.

Our first task is to describe the key property of the localization map, which we usually call its *universal property*. We need first a definition.

Definition A.2.1.12. Let A be a ring, and let S be a multiplicatively closed subset of A. We say that a morphism of rings $\phi\colon A \to B$ ***inverts*** S if for every element s of S the image $\phi(s)$ is a unit of B.

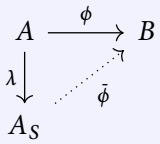
With this definition at hand, we can state the universal property of localizations.

Lemma A.2.1.13. *Let* A *be a ring, let* S *be a multiplicatively closed subset of* A*, and let* $\lambda\colon A \to A_S$ *be the localization map of* A *at* S.

(*i*) *The localization map* $\lambda\colon A \to A_S$ *inverts* S.

(*ii*) *If* $\phi\colon A \to B$ *is a morphism of rings that inverts* S*, then there is exactly one morphism of*

rings $\bar{\phi}\colon A_S \to B$ such that $\bar{\phi} \circ \lambda = \phi$.



In fact, we have that $\bar{\phi}(a/s) = \phi(a)\phi(s)^{-1}$ for each element (a, s) of $A \times S$.

The second part of this lemma says that a morphism of rings defined on A which inverts S factors in a unique way through the localization map. In fact, abusing a little language, we often say that the morphism *extends* to the localization, imagining that the map $\lambda\colon A \to A_S$ is an inclusion.

Proof. □

This universal property of the localization map is so strong that it determines it up to a unique isomorphism. The following lemma spells out in detail what we mean by this.

Lemma A.2.1.14. *Let A be a ring, let S be a multiplicatively closed subset of A, and let $\lambda\colon A \to A_S$ be the localization map of A at S. Let $\kappa\colon A \to B$ be a morphism of rings that satisfies the following two conditions:*

- *The morphism $\kappa\colon A \to B$ inverts S.*
- *If $\phi\colon A \to C$ is a morphism of rings that inverts S, then there is exactly one morphism of rings $\bar{\phi}\colon B \to C$ such that $\bar{\phi} \circ \kappa = \phi$.*

There exists exactly one isomorphism $\alpha\colon A_S \to B$ such that $\alpha \circ \lambda = \kappa$.

Proof. □

Localization maps are usually neither injective nor surjective. Let us describe their kernels.

Lemma A.2.1.15. *Let A be a ring, let S be a multiplicatively closed subset of A, and let $\lambda\colon A \to A_S$ be the localization map of A at S.*

(*i*) *We have that* $\ker \lambda = \{a \in A : \text{there is an } s \text{ in } S \text{ such that } sa = 0\}$.
(*ii*) *The localization map λ is injective if and only if the set S does not contain zero divisors.*
(*iii*) *In particular, if A is an integral domain and $0 \notin S$, the localization map is injective.*

Proof. The first part follows immediately from the definition of the equivalence relation that defines the set A_S, and the other two parts follow from the first. □

We can characterize the most extreme way in which the localization map can fail to be injective.

Lemma A.2.1.16. *Let A be a ring, and let S be a multiplicatively closed subset of A. The localization A_S is the zero ring if and only if 0 belongs to S.*

Proof. In A_S the unit element is equal to the zero element if and only if $1/1 = 0/1$, and this happens exactly when there is an element s of S such that $0 = s(1 \cdot 1 - 1 \cdot 0)$, which happens exactly when 0 is in S. □

We can also characterize the multiplicatively closed subsets the localizations at which are surjective.

Lemma A.2.1.17. *Let A be a ring, and let S be a multiplicatively closed subset of A.*

(*i*) *The localization map $\lambda\colon A \to A_S$ of A at S is surjective if and only if for every element a of A and every element s of S there are elements b of A and t of S such that $ta = tsb$.*

(*ii*) *In particular, if every element of S is a unit in A then the localization map λ is surjective and, in fact, an isomorphism.*

Proof. (*i*) Let us suppose first that the localization map λ is surjective, and let a and s be elements of A and of S, respectively. The hypothesis implies that there is an element b of A such that $a/s = \lambda(b) = b/1$, so that there is an element t of S such that $t(1 \cdot a - s \cdot b) = 0$ or, equivalently, such that $ta = tsb$. The condition in (*i*) is therefore necessary for the surjectivity of λ.

Let us suppose now that that condition is satisfied, and let x be an element of A_S, so that there are elements a and s of A and of S, respectively, such that $x = a/s$. The hypothesis now tells us that there are an element b of A and an element t of S such that $ta = tsb$, and this implies that

$$x = a/s = (ta)/(ts) = (tsb)/ts = b/1 = \lambda(b) \in \operatorname{img}\lambda.$$

We can then conclude that the localization map λ is surjective.

(*ii*) Let us suppose now that every element of S is a unit of A. If a and s are an element of A and an element of S, respectively, then the elements $t \coloneqq 1$ of S and $b \coloneqq s^{-1}a$ are such that $ta = tsb$. According to (*i*), the localization map λ is therefore surjective. Moreover, since S does not have zero-divisors, we can conclude from the second part of Lemma A.2.1.15 that λ is also injective, so it is an isomorphism. □

The condition in part (*ii*) of this lemma is not necessary for the localization map to be surjective, though, as the following example shows.

Example A.2.1.18. Let B and C be two rings, and let us consider the ring $A \coloneqq B \times C$, its subset $S \coloneqq \{(1,1),(1,0)\}$, which is multiplicatively closed, and the corresponding localization map $\lambda\colon A \to A_S$. This map is surjective, yet not all of its elements are units of A. Indeed, if x is an

element of A_S, then there are an element (b,c) of A and an element $s=(s_1,s_2)$ of S such that $x=(b,c)/s$ and, since $s_1=1$, we have that

$$(1,0)\cdot\big((1,1)\cdot(b,c)-(s_1,s_2)\cdot(b,0)\big)=(0,0),$$

so that $x=(b,c)/(s_1,s_2)=(b,0)/(1,1)=\lambda((b,0))$.

In this example the multiplicatively closed subset S contains zero divisors of A. The result of the next exercise shows that this is actually necessary to construct an example.

Exercise A.2.1.19. Let A be a ring, let S be a multiplicatively closed subset, and let us suppose that the localization map $\lambda\colon A\to A_S$ is surjective. Show that if S does not contain zero-divisors, then every element of S is a unit of A.

The result of the following exercise generalizes the study of surjectivity of localization maps above.

Exercise A.2.1.20. Let A be a ring, and let S and T be two multiplicatively closed subsets of A such that $S\subseteq T$. The localization map $\lambda_{A,T}\colon A\to A_T$ clearly inverts S, so there is exactly one morphism of rings $\phi\colon A_S\to A_T$ such that $\phi(a/1)=a/1$ for each a in A. Show that the following statements are equivalent:

(*a*) The map ϕ is bijective.
(*b*) For every element t of T the faction $t/1$ is a unit of A_S.
(*c*) T is contained in the saturation of S.
(*d*) For every prime ideal $\mathfrak{p}$ of A we have that $\mathfrak{p}\cap S=\varnothing\implies\mathfrak{p}\cap T=\varnothing$.

Many properties of a ring as inherited by its localizations. As a first example of this, we have the following result.

Lemma A.2.1.21. *Let A be a ring, and let S be a multiplicatively closed subset of A that does not contain* 0*. If A is an integral domain, then so is A_S.*

Proof. Let us suppose that the ring A is an integral domain, and let x and y be two elements of A_S such that $xy=0$. There are elements a and b of A and elements s and t of S such that $x=a/s$ and $y=b/t$, and since $0=xy=(ab)/(st)$, there is an element u of S such that $uab=0$. Since $0\notin S$ and A is an integral domain, this implies that one of a or b is 0, so that one of x or y is zero in A_S. This proves that the ring A_S is an integral domain. □

We can easily describe what happens if we localize a ring «twice». Let A be a ring, let S and T be two multiplicatively closed subsets of A. What we want to do is to localize A at S first, and then at T. Of course, the set T is not a subset of A_S, so this does not make sense. Let, though,

$\lambda_{A,S}\colon A \to A_S$ be the localization map of A at S, and let us consider the subset $\overline{T} \coloneqq \lambda_{A,S}(T)$ of A_S. It is a multiplicatively closed subset of A_S, so we can consider the corresponding localization map $\lambda_{A_S,\overline{T}}\colon A_S \to (A_S)_{\overline{T}}$ and the composition

$$\lambda_{A_S,\overline{T}} \circ \lambda_{A,S}\colon A \to (A_S)_{\overline{T}},$$

which for all a in A has

$$(\lambda_{A_S,\overline{T}} \circ \lambda_{A,S})(a) = (a/1)/(1/1).$$

If s and t are an element of S and an element of T, respectively, then in $(A_S)_{\overline{T}}$ we have that

$$\begin{aligned}(1/s)/(t/1) \cdot (\lambda_{A_S,\overline{T}} \circ \lambda_{A,S})(st) &= (1/s)/(t/1) \cdot ((st)/1)/(1/1)\\ &= (1/s \cdot (st)/1)/(t/1)\\ &= ((st)/s)/(t/1)\\ &= (t/1)/(t/1)\\ &= (1/1)/(1/1),\end{aligned}$$

the unit element of $(A_S)_{\overline{T}}$, so that $(\lambda_{A_S,\overline{T}} \circ \lambda_{A,S})(st)$ is invertible there. This tells us that the map $\lambda_{A_S,\overline{T}} \circ \lambda_{A,S}$ inverts the elements of the multiplicatively closed subset ST of A, and thus the universal property of the localization map $\lambda_{A,ST}\colon A \to A_{ST}$ of A at ST implies that there is exactly one morphism of rings $\phi\colon A_{ST} \to (A_S)_{\overline{T}}$ such that $\phi \circ \lambda_{A,ST} = \lambda_{A_S,\overline{T}} \circ \lambda_{A,S}$. This map has

$$\phi(a/1) = (a/1)/(1/1)$$

for each a in A. If s and t are elements of S and of T, respectively, then we also have that

$$\begin{aligned}((st)/1)/(1/1) \cdot \phi(a/st) = \phi((st)/1) \cdot \phi(a/st) = \phi((st)/1 \cdot (a/st)) &= \phi(a/1)\\ &= (a/1)/(1/1),\end{aligned}$$

so that also

$$\begin{aligned}\phi(a/st) &= (1/1)/((st)/1) \cdot ((st)/1)/(1/1) \cdot \phi(a/st)\\ &= (1/1)/((st)/1) \cdot (a/1)/(1/1)\\ &= (1/s \cdot 1/1)/(1/s \cdot (st)/1) \cdot (a/1)/(1/1)\end{aligned}$$

because $1/s$ is a unit of A_S, and this is

$$\begin{aligned}&= (1/s)/(t/1) \cdot (a/1)/(1/1)\\ &= (a/s)/(t/1).\end{aligned}$$

Lemma A.2.1.22. *Let A be a ring, let S and T be two multiplicatively closed subsets of A, let $\lambda_{A,S}\colon A \to A_S$ be the localization map of A at S, and let $\overline{T} \coloneqq \lambda_{A,S}(T)$. The morphism of rings*

$$\phi\colon A_{ST} \to (A_S)_{\overline{T}}$$

constructed above is an isomorphism. For each choice of a, s and t in A, in S, and in T, respectively, we have that

$$\phi(a/st) = (a/s)/(t/1), \qquad \phi^{-1}((a/s)/(t/1)) = a/(st).$$

Proof. Since the localization map $\lambda_{A,ST}\colon A \to A_{ST}$ inverts ST and $S \subseteq ST$ because $1 \in T$, that map inverts S, and the universal property of the localization map $\lambda_{A,S}\colon A \to A_S$ implies that there is a unique morphism of rings $\psi\colon A_S \to A_{ST}$ such that $\lambda_{A,ST} = \psi \circ \lambda_{A,S}$.

If τ is an element of $\overline{T}$, then there is an element t of T such that $\tau = \lambda_{A,S}(t) = t/1$, and then $\psi(\tau) = \psi(t/1) = \lambda_{A,ST}(t)$ is a unit of A_{ST} because t is in ST. This tells us that the map ψ inverts $\overline{T}$, and the universal property of the localization of A_S at that multiplicatively closed subset implies that there is a morphism of rings $\bar{\psi}\colon (A_S)_{\overline{T}} \to A_{ST}$ such that $\psi = \bar{\psi} \circ \lambda_{A_S,\overline{T}}$. This map is such that for each a in A and s in S we have

$$\bar{\psi}((a/s)/(1/1)) = \psi(a/s) = a/s.$$

One should notice that a/s denotes here in the expressions $\bar{\psi}((a/s)/(1/1)$ and $\psi(a/s)$ an element of A_S, while the expression a/s in the last member of this chain of equalities denotes an element of A_{ST}: this makes sense because $S \subseteq ST$. If now t is an element of T, then in the ring A_{ST} we have that

$$\begin{aligned} t/1 \cdot \bar{\psi}((a/s)/(t/1)) &= \bar{\psi}((t/1)/(1/1)) \cdot \bar{\psi}((a/s)/(t/1)) \\ &= \bar{\psi}((t/1)/(1/1) \cdot (a/s)/(t/1)) \\ &= \bar{\psi}((a/s)/(1/1)) \\ &= a/s, \end{aligned}$$

so that

$$\begin{aligned} \bar{\psi}((a/s)/(t/1)) &= 1/t \cdot t/1 \cdot \bar{\psi}((a/s)/(t/1)) \\ &= 1/t \cdot a/s \\ &= a/(st). \end{aligned}$$

Summing up, we have morphisms of rings $\phi\colon A_{ST} \to (A_S)_{\overline{T}}$ and $\bar{\psi}\colon (A_S)_{\overline{T}} \to A_{ST}$ that for all choices of a in A, of s in S, and of t in T have $\phi(a/st) = (a/s)/(t/1)$ and $\bar{\psi}((a/s)/(t/1)) = a/(st)$. It follows immediately from this that these two maps are mutually inverse. □

Just as we can localize rings, we can localize morphisms of rings, in some sense.

Lemma A.2.1.23. *Let $\pi\colon A \to B$ be a morphism of rings, and let S be a multiplicatively closed subset of A.*

(*i*) *The set $\pi(S)$ is a multiplicatively closed subset of B and there is a unique morphism of rings $\pi_S\colon A_S \to B_{\pi(S)}$ such that $\pi_S(a/1) = \pi(a)/1$ for every choice of a in A, and we in fact have that $\pi_S(a/s) = \pi(a)/s$ for all a in A and all s in S.*

(*ii*) *If the map π is surjective, then so is the map π_S.*

Proof. That the set $\pi(S)$ is a multiplicatively closed subset of B is clear. The composition $\lambda_{B,\pi(S)} \circ \pi\colon A \to B_{\pi(S)}$ of the map π with the localization map $\lambda_{B,\pi(S)}\colon B \to B_{\pi(S)}$ of B at $\pi(S)$ is a morphism of rings, and it inverts S. Indeed, if s is an element of S, then $\pi(s)$ is of course an element of $\pi(S)$, so that $\lambda_{B,\pi(S)}(\pi(s))$ is invertible in $B_{\pi(S)}$. The universal property of the localization of A at S implies then that there is a unique morphism of rings $\pi_S\colon A_S \to B_{\pi(S)}$ such that $\pi_S \circ \lambda_{A,S} = \lambda_{B,\pi(S)} \circ \pi$ or, equivalently, such that $\pi_S(a/1) = \pi(a)/1$ for each a in A. This proves the first claim of (*i*). Moreover, if a is an element of A and s one of S, we have that

$$\pi(s)/1 \cdot \pi_S(a/s) = \pi_S(s/1) \cdot \pi_S(a/s) = \pi_S(s/1 \cdot a/s) = \pi_S(a/1) = \pi(a)/1,$$

so that

$$\pi_S(a/s) = 1/\pi(s) \cdot \pi(s)/1 \cdot \pi_S(a/s) = 1/\pi(s) \cdot \pi(a)/1 = \pi(a)/\pi(s).$$

This tells us that the second claim of (*i*) is also true.

Let us suppose now that the map π is surjective. If x is an element of $B_{\pi(S)}$, then there are an element b of B and an element s of S such that $x = b/\pi(s)$ and, since the map π is surjective, there is also an element a of A such that $\pi(a) = b$. We therefore have that $x = b/\pi(s) = \pi(a)/\pi(s) = \pi_S(a/s) \in \operatorname{img} \pi_S$. We see that the map π_S is surjective, and this proves part (*ii*). □

Before continuing with the general theory of localization, let us present some simple examples.

Example A.2.1.24. Let A be an integral domain, so that the set $S \coloneqq A \setminus 0$ is a multiplicatively closed subset of A and we can therefore consider the localization A_S. This ring is, in fact, a field. Let us check this. Let x be a non-zero element of A_S. There are an element a of A and an element s of S such that $x = a/s$ and, since $x \neq 0$, we have that $a \neq 0$. This implies that we can consider the fraction s/a in A_S and, since $x \cdot s/a = a/s \cdot s/a = (as)/(sa) = 1/1$, that fraction is the inverse for x in A_S.

We call the field A_S the ***field of fractions*** of A, and usually write $\operatorname{Frac} A$ to denote it. Since A is an integral domain and 0 is not in S, we know that the localization map $\lambda\colon A \to \operatorname{Frac} A$ of A at S is

injective. It follows immediately from the universal property of the localization of A at S that

> *if $\phi\colon A \to K$ is an injective morphism of rings whose codomain is a field, then there is exactly one morphism $\tilde{\phi}\colon \operatorname{Frac} A \to K$ such that $\tilde{\phi}(a/1) = \phi(a)/1$, and we have that $\tilde{\phi}(a/b) = \phi(a)/\phi(b)$ for all choices of a and b in A such that $b \neq 0$.*

Since the localization map λ is injective, we usually use it to identify A with its image, and therefore consider every integral domain as a subring of its field of fractions. As a consequence of this identification, we can rephrase the property above in the following way:

> *an injective morphism of rings $\phi\colon A \to K$ whose codomain is a field has a unique extension $\tilde{\phi}\colon \operatorname{Frac} A \to K$ to the field of fractions of A.*

There are many well known examples of this construction of fields of quotients. Let us present two important ones.

Example A.2.1.25. Let us consider the ring $\mathbb{Z}$. The inclusion map $\iota\colon \mathbb{Z} \to \mathbb{Q}$ is an injective morphism of rings and its codomain is a field, so the observations above imply that there is a unique morphism of fields $\tilde{\iota}\colon \operatorname{Frac}\mathbb{Z} \to \mathbb{Q}$ such that $\tilde{\iota}(a/b) = \iota(a)/\iota(b) = a/b$ whenever a and b are integers and b is not zero. This map $\tilde{\iota}$ is injective because its domain is a field, and it is clear that it is also surjective, so it is an isomorphism. We therefore have that

$$\operatorname{Frac}\mathbb{Z} \cong \mathbb{Q}.$$

We always regard the isomorphism $\tilde{\iota}$ as an identification.

Exercise A.2.1.26. Let d be a square-free integer. Show that the fraction field of the subring $\mathbb{Z}[\sqrt{d}]$ of $\mathbb{C}$ is isomorphic to the subfield $\mathbb{Q}(\sqrt{d})$ of $\mathbb{C}$.

Exercise A.2.1.27. Let $\Bbbk$ be a field, and let us consider the ring $\Bbbk[x]$ of polynomials with coefficients in $\Bbbk$ and the field $\Bbbk(x)$ of all rational functions with coefficients in $\Bbbk$. Show that the inclusion $\Bbbk[x] \to \Bbbk(x)$ extends to an isomorphism of field $\operatorname{Frac}\Bbbk[x] \to \Bbbk(x)$.

Example A.2.1.28. Let Ω be a connected and non-empty subset of $\mathbb{C}$, let $H(\Omega)$ be the ring of holomorphic functions on Ω, and let $M(\Omega)$ be the field of meromorphic functions on Ω. As a holomorphic function is meromorphic, we have an inclusion map $\iota\colon H(\Omega) \to M(\Omega)$, which is a morphism of rings. Since $H(\Omega)$ is an integral domain and ι is clearly injective, the map ι induces an injection of fields $\tilde{\iota}\colon \operatorname{Frac} H(\Omega) \to M(\Omega)$. In fact, it is a consequence of the *Weierstraß factorization theorem* that every meromorphic function on Ω is equal to the quotient of two

holomorphic functions on Ω — this is Corollary 5.20 in John B. Conway's book [Con1973] — and this implies at once that this map $\tilde{\iota}$ is an isomorphism.

The following exercise deals with a generalization of the construction of fields of fractions that is sometimes useful.

Exercise A.2.1.29.

(a) Show that if A is a ring, then the set S of all non-zero-divisors of A is a multiplicatively closed subset of A.

We may therefore consider the localization A_S: we call it the ***total ring of fractions*** of A and we write it $\operatorname{Frac} A$. Notice that if A is an integral domain, then the total ring of fractions of A is simply the field of fractions of A, so the notation $\operatorname{Frac} A$ is unambiguous.

(b) Show that for any ring A the localization map $A \to \operatorname{Frac} A$ is injective, and that every element of $\operatorname{Frac} A$ is either a zero divisor or a unit.

(c) Show that if A and B are two rings, then there is a canonical isomorphism

$$\operatorname{Frac}(A \times B) \to \operatorname{Frac} A \times \operatorname{Frac} B.$$

(d) A (possibly non-commutative) ring A is ***von Neumann regular*** if for any element a of A there exists an element x in A such that $a = xax$. Show that if A is a commutative von Neumann regular ring, then the localization map $A \to \operatorname{Frac} A$ is an isomorphism.

Let us look now at some examples at non-total multiplicatively closed subsets.

Example A.2.1.30. Let A be an integral domain, and let S be a multiplicatively closed subset of A. If 0 is in S, then we know that the localization A_S is the zero ring, so we suppose in what follows that $0 \notin S$. Let $\lambda\colon A \to A_S$ be the localization map, which is injective because of Lemma A.2.1.15. The inclusion map $\iota\colon A \to \operatorname{Frac} A$ of A in its field of fractions is a morphism of rings that inverts every element of S, so there is a unique morphism of rings $\phi\colon A_S \to \operatorname{Frac} A$ such that $\iota = \phi \circ \lambda$.

The map ϕ is injective. Indeed, if x is an element of A_S such that $\phi(x) = 0$, then there are elements a of A and s of S such that $x = a/s$ and $0 = \phi(x) = \phi(a/s) = \iota(a)/\iota(s) = a/s$ in $\operatorname{Frac} A$, and this implies that $a = 0$ and thus that $x = 0$. In view of this, we can use the map ϕ to identify the localization A_S with its image under ϕ, which is the subring

$$\phi(A_S) = \{a/s \in \operatorname{Frac} A : a \in A, s \in S\}$$

of all fractions in $\operatorname{Frac} A$ whose denominator is in S.

As simple concrete instances of this we can mention the following.

- If $A = \mathbb{Z}$ and $S = \{p^n : n \in \mathbb{N}_0\}$ is the multiplicatively closed subset generated by a prime number p, then the localization $\mathbb{Z}_S$, which we usually write $\mathbb{Z}_p$, is the subring of $\operatorname{Frac} \mathbb{Z} = \mathbb{Q}$ of all those fractions whose denominator is a power of p.

- If again $A = \mathbb{Z}$ but now $S = \mathbb{Z} \setminus \langle p \rangle$ is the complement of the prime ideal $\mathfrak{p} \coloneqq \langle p \rangle$ generated by a prime number p, then the localization $\mathbb{Z}_S$, which we usually write $\mathbb{Z}_\mathfrak{p}$, is the subring of $\mathbb{Q}$ of all those fractions whose denominator is not divisible by p.

This example shows that all non-zero localizations of an integral domain are subrings of the fraction field of that domain — this is a stronger conclusion than that of Lemma A.2.1.21, which asserts that all those localization are integral domains.

Exercise A.2.1.31. Let A be an integral domain, let $\mathscr{S}$ be the set of all multiplicatively closed subsets of A that do not contain 0, and, as usual, let $\operatorname{Spec} A$ and $\operatorname{Spm} A$ be the sets of all prime ideals of A and of all maximal ideals of A. Show that as subrings of $\operatorname{Frac} A$ we have

$$A = \bigcap_{S \in \mathscr{S}} A_S = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} A_\mathfrak{p} = \bigcap_{\mathfrak{m} \in \operatorname{Spec} A} A_\mathfrak{m}.$$

Hint: In order to show that an element x of this last intersection belongs to A show that the set $\{a \in A : ax \in A\}$ is an ideal of A that is not contained in any maximal ideal of A.

Example A.2.1.32. Let now $\Bbbk$ be a field, let $\Bbbk[x]$ be the ring of polynomials with coefficients in $\Bbbk$, which is an integral domain, and let $S \coloneqq \{x^n : n \in \mathbb{N}_0\}$ be the multiplicatively closed subset of $\Bbbk[x]$ generated by the variable x. Our general discussion tells us that the localization $\Bbbk[x]_x$ is the subring of $\Bbbk(x) = \operatorname{Frac} \Bbbk[x]$ whose fractions are a power of x.

Now such a fraction is of the form f/x^n for a polynomial f in $\Bbbk[x]$ and a non-negative integer n. If the fraction is not zero, then f is not zero and there are a non-negative integer d and elements $a_0, \ldots, a_d$ of $\Bbbk$ such that $f = a_0 + a_1 x + \cdots + a_d x^d$. The fraction is then

$$f/x^n = (a_0 + a_1 x + \cdots + a_d x^d)/x^n = a_0/x^n + a_1 x/x^n + \cdots + a_d x^d/x^n$$

and we can write this in the way

$$a_0 x^{-n} + a_1 x^{-n+1} + \cdots + a_d x^{d-n}.$$

We see with this that every non-zero element of the localization $\Bbbk[x]_x$ can be written in the form

$$a_m x^m + a_{m+1} x^{m+1} + \cdots + a_n x^n \tag{A.1}$$

for some integers m and n such that $m \leq n$ and some scalars $a_m, \ldots, a_n$ of $\Bbbk$.

Expressions such as the one in (A.1) are called ***Laurent polynomials*** — they are, essentially, polynomials in which we allow negative powers — and therefore we call the localization $\Bbbk[x]_x$ the ***ring of Laurent polynomials***. We often write $\Bbbk[x, x^{-1}]$ or $\Bbbk[x^{\pm 1}]$ to denote it

Exercise A.2.1.33. Let $\Bbbk$ be a field. Show that every non-zero element of the ring $\Bbbk[x, x^{-1}]$ of Laurent polynomials can be written in a unique way in the form

$$a_m x^m + a_{m+1} x^{m+1} + \cdots + a_n x^n$$

for some integers m and n such that $m \leq n$ and some scalars $a_m, \ldots, a_n$ of $\Bbbk$ such that $a_m \neq 0$ and $a_n \neq 0$, so that, in fact, the function $n \in \mathbb{Z} \mapsto x^n \in \Bbbk[x, x^{-1}]$ is injective and its image is a basis of its codomain as a $\Bbbk$-vector space.

Exercise A.2.1.34. Let $\Bbbk$ be a field, let $\Bbbk[\![x]\!]$ be the ring of formal series with coefficients in $\Bbbk$, and let

- $S \coloneqq \{x^n : n \geq 0\}$ be the multiplicatively closed subset of $\Bbbk[\![x]\!]$ generated by x and
- $\mathfrak{m}$ be the subset of $\Bbbk[\![x]\!]$ of all those series with zero constant term.

Describe concretely the localization $\Bbbk[\![x]\!]_S$, show that $\mathfrak{m}$ is a maximal ideal of $\Bbbk[\![x]\!]$, and prove that there is an isomorphism of rings $\Bbbk[\![x]\!]_S \to \Bbbk[\![x]\!]_{\mathfrak{m}}$ that extends the identity map of $\Bbbk[\![x]\!]$.

Exercise A.2.1.35. Let n be a positive integer, let x_0 be an element of $\mathbb{R}^n$, and let $\mathrm{C}(\mathbb{R}^n)$ be the ring of all continuous functions $\mathbb{R}^n \to \mathbb{R}$. We say that two elements f and g of $\mathrm{C}(\mathbb{R}^n)$ ***have the same germ at*** x_0 if there is an open subset U of $\mathbb{R}^n$ such that $x_0 \in U$ and $f|_U = g|_U$, and in that case we write $f \sim_{x_0} g$.

(a) Show that $\sim_{x_0}$ is an equivalence relation on the set $\mathrm{C}(\mathbb{R}^n)$.

We write $\mathrm{C}_{x_0}(\mathbb{R}^n)$ for the quotient set $\mathrm{C}(\mathbb{R}^n)/\!\sim_{x_0}$ and $[f]_{x_0}$ for the equivalence class corresponding to an element f of $\mathrm{C}(\mathbb{R}^n)$ in $\mathrm{C}_{x_0}(\mathbb{R}^n)$, and call the class $[f]_{x_0}$ the ***germ*** of f at x_0.

(b) Show that the set $I_{x_0} \coloneqq \{f \in \mathrm{C}(\mathbb{R}^n) : f \sim 0\}$ is an ideal of $\mathrm{C}(\mathbb{R}^n)$, and that for all f and g in $\mathrm{C}(\mathbb{R}^n)$ we have that $f \sim_{x_0} g \iff f \cong g \mod I_{x_0}$. Deduce from this that the sets $\mathrm{C}_{x_0}(\mathbb{R}^n)$ and $\mathrm{C}(\mathbb{R}^n)/I_{x_0}$ coincide and that, in particular, there is exactly one ring structure on the set $\mathrm{C}_{x_0}(\mathbb{R}^n)$ with respect to which we have

$$[f]_{x_0} + [g]_{x_0} = [f+g]_{x_0}, \qquad [f]_{x_0} \cdot [g]_{x_0} = [fg]_{x_0}$$

for all f and g in $\mathrm{C}(\mathbb{R}^n)$.

(c) Let $\mathfrak{m}_{x_0}$ be the set of all elements of $\mathrm{C}(\mathbb{R}^n)$ that vanish at x_0. Show that $\mathfrak{m}_{x_0}$ is a maximal ideal of $\mathrm{C}(\mathbb{R}^n)$, and that whenever f and g are elements of $\mathrm{C}(\mathbb{R}^n)$ we have that $f \sim_{x_0} g$ exacly when there is an element h of $\mathrm{C}(\mathbb{R}^n) \setminus \mathfrak{m}_{x_0}$ such that $h \cdot (f - g) = 0$ in $\mathrm{C}(\mathbb{R}^n)$.

(d) Show that the function $\gamma_{x_0} \colon f \in \mathrm{C}(\mathbb{R}^n) \mapsto [f]_{x_0} \in \mathrm{C}_{x_0}(\mathbb{R}^n)$ is a morphism of rings that inverts the set $\mathrm{C}(\mathbb{R}^n) \setminus \mathfrak{m}_{x_0}$, and deduce from that that there is exactly one morphism of rings $\bar{\gamma}_{x_0} \colon \mathrm{C}(\mathbb{R}^n)_{\mathfrak{m}_{x_0}} \to \mathrm{C}_{x_0}(\mathbb{R}^n)$ such that $\bar{\gamma}_{x_0}(f/1) = [f]_{x_0}$ for all f in $\mathrm{C}(\mathbb{R}^n)$.

(e) Prove that that morphism $\bar{\gamma}_{x_0}$ is, in fact, an isomorphism.

This gives a purely algebraic construction of the ring of germs at x_0 of continuous functions $f\colon \mathbb{R}^n \to \mathbb{R}$ as the localization of the ring $\mathrm{C}(\mathbb{R}^n)$ at the maximal ideal $\mathfrak{m}_{x_0}$.

(f) Show that, more generally, all these results are true if we replace the space $\mathbb{R}^n$ with any completely regular and Hausdorff topogical space.

A.2.2. Localization of modules

The theory of localization of rings that we have just presented has a parallel theory for modules. We will leave many of its details to the reader.

Exercise A.2.2.1. Let A be a ring, let S be a multiplicatively closed subset of A, and let M be an A-module. Show the relation $\sim$ on the set $M \times S$ for which

$$(m,s) \sim (n,t) \iff \text{there is an element } u \text{ in } S \text{ such that } u(mt - ns) = 0$$

is an equivalence relation.

Just as with rings, we use this equivalence relation to construct the set that will underlie the localization of the module M.

Definition A.2.2.2. Let A be a ring, let S be a multiplicatively closed subset of A, and let M be a left A-module.

- We write M_S for the set of equivalence classes of the relation $\sim$ of Exercise A.2.2.1 in $M \times S$.
- If (m,s) is an element of $M \times S$, then we write m/s for the equivalence class of (m,s) in M_S.

The next step is to turn that set into an module.

Exercise A.2.2.3. Let A be a ring, let S be a multiplicatively closed subset of A, let $\lambda\colon A \to A_S$ be the localization map of A at S, and let M be an A-module. Prove the following statements:

(a) There is exactly one function $+\colon M_S \times M_S \to M_S$ such that

$$m/s + n/t = (tm + sn)/(st)$$

for each choice of (m,s) and (n,t) in $M \times S$.

(b) There is exactly one function $\cdot\colon A \times M_S \to M_S$ such that

$$a \cdot m/t = (am)/t$$

for each choice of a in A and of (m,t) in $M \times S$.

(c) The set M_S, when endowed with the operations $+$ and $\cdot$ described here as addition and multiplication by A, is an A-module in which the zero elements is $0/1$.

(d) The function $\lambda_M\colon m \in M \mapsto m/1 \in M_S$ is a morphism of A-modules.

The module that we have described in this exercise is the localization we were after.

Definition A.2.2.4. Let A be a ring, and let S be a multiplicatively closed subset of A, let $\lambda\colon A \to A_S$ be the localization map of A at S, and let M be an A-module. The A-module M_S is the ***localization*** of M at the multiplicatively closed set S, and the map $\lambda_M\colon M \to M_S$ in the last part of Exercise A.2.2.3 is the ***localization map*** of M at S.

Just as for rings, we use special notation for the localization in two cases: if $\mathfrak{p}$ is a prime ideal, then we write $M_\mathfrak{p}$ for the localization of M at the multiplicatively closed subset $A \smallsetminus \mathfrak{p}$, and if f is an element of A, then we write M_f for the localization of M at the multiplicatively closed subset $\{f^n : n \geq 0\}$.

Remark A.2.2.5. We should note that in the situation of this definition we have the localization A_S of the ring A at S and, at the same time, the localization A_S of the regular A-module A at S. In principle these are two different things. As sets, both are obtained from the set $A \times S$ by taking equivalence classes with respect to equivalence relations, and it is immediate to observe that those equivalence relations coincide: this implies that, as sets, at least, the two constructions coincide. We will see below that the A-module A_S has a canonical A_S-module structure, and with that structure it is precisely the regular module of the ring A_S. There is therefore no ambiguity.

The localization of a module has a universal property similar to that of rings: just as localizing at a ring at a multiplicatively closed subset S makes the elements of S invertible, localizing a module at such a set S makes the elements of that set S act bijectively on the resulting module.

Definition A.2.2.6. Let A be a ring, and let S be a multiplicatively closed subset of A. An A-module M is ***S-local*** if for every element s of S the function

$$\mu_{M,s}\colon m \in M \mapsto sm \in M$$

is bijective.

Let us notice that the function $\mu_{M,s}$ that appears in this definition is, in any case, a morphism of A-modules. Morphisms of that form play an important role in the very definition of modules, in fact.

Exercise A.2.2.7. Let A be a ring. For each abelian group M let us write, as usual, $\mathrm{Hom}_\mathbb{Z}(M, M)$ for the ring of all morphisms of groups $M \to M$ — we should remark here that this ring is, usually, not commutative.

(a) Show that if M is an A-module, then the map $a \in A \mapsto \mu_{M,a} \in \mathrm{Hom}_\mathbb{Z}(M, M)$ is a morphism of rings.

(b) Show that, conversely, if M is an abelian group and $\rho\colon A \to \mathrm{Hom}_\mathbb{Z}(M, M)$ is a morphism

of rings, then there exists exactly one structure of A-module on the abelian group M with respect to which we have that $\mu_{M,a} = \rho(a)$ for all a in A.

Exercise A.2.2.8. Let A be a ring, let S be a multiplicatively closed subset of A, let M be an A-module, and let $\lambda\colon A \to A_S$ and $\lambda_M\colon M \to M_S$ be the localization maps of A and of M at S. Prove the following statements:

(a) The A-module M_S is S-local.

(b) If N is an S-local A-module and $\phi\colon M \to N$ is a morphism of A-modules, then there is exactly one morphism of A-modules $\tilde{\phi}\colon M_S \to N$ such that $\phi = \tilde{\phi} \circ \lambda_M$ or, equivalently, such that $\phi(m) = \tilde{\phi}(m/1)$ for all m in M.

$$\begin{array}{ccc} M & \xrightarrow{\phi} & N \\ {\scriptstyle \lambda_M}\downarrow & \nearrow_{\tilde{\phi}} & \\ M_S & & \end{array}$$

This morphism is such that $\tilde{\phi}(m/s) = \phi(m)/s$ for all m in M and all s in S.

Just as for rings, this universal property in fact characterizes the localization of a module.

Lemma A.2.2.9. *Let A be a ring, let S be a multiplicatively closed subset of A, let M be an A-module, and let $\lambda_M\colon M \to M_S$ be the localization maps of M at S. If $\mu\colon M \to L$ is a morphism of modules such that*

- *the A-module L is S-local, and*
- *if N is an S-local A-module and $\phi\colon M \to N$ is a morphism of A-modules, then there is exactly one morphism of A-modules $\tilde{\phi}\colon M_S \to N$ such that $\phi = \tilde{\phi} \circ \mu$,*

then there exists exactly one isomorphism of A-modules $\iota\colon M_S \to L$ such that $\mu = \iota \circ \lambda_M$.

Proof. □

Let us recall that whenever we have a commutative[1] ring A and two A-modules M and N there is a canonical structure of A-module on the abelian group $\mathrm{Hom}_A(M, N)$, which is such that for all choices of a, f and m are in A, $\mathrm{Hom}_A(M, N)$, and M, respectively, we have that

$$(a \cdot f)(m) = af(m) = f(am).$$

Exercise A.2.2.10. Let A be a ring, let S be a multiplicatively closed subset of A, let M be an A-module, and let $\lambda_M\colon M \to M_S$ be the localization map of M at S. Show that for any S-local

[1] If the ring A is not commutative, there is in general no way to turn $\mathrm{Hom}_A(M, N)$ into a left A-module when M and N are left A-modules.

A-module N the funtion

$$f \in \mathrm{Hom}_A(M_S, N) \mapsto f \circ \lambda_M \in \mathrm{Hom}_A(M, N)$$

is an isomorphism of A-modules.

One consequence of this is that localizing a module at a multiplicatively closed subset at which it is local does not really do anything. The following result makes this precise.

Lemma A.2.2.11. *Let A be a ring, let S be a multiplicatively closed subset of A, and let M be an A-module. If M is S-local, then the localization map $\lambda_M \colon M \to M_S$ of M at S is an isomorphism of A-modules.*

Proof. Let us suppose that the A-module M is S-local, and consider its identity map $\mathrm{id}_M \colon M \to M$, which is a morphism of A-modules with S-local codomain. Moreover, if N is an S-local A-modules and $\phi \colon M \to N$ is a morphism of A-modules, then there is clearly exactly one morphism of A-module $\tilde{\phi} \colon M \to N$ such that $\phi = \tilde{\phi} \circ \mathrm{id}_M$, namely, the morphism ϕ itself.

It follows then from Lemma A.2.2.9 that there is exactly one isomorphism of A-modules $\iota \colon M_S \to M$ such that $\mathrm{id}_M = \iota \circ \lambda_M$, and we then have that $\lambda_M = \iota^{-1}$ is itself an isomorphism. □

In particular, this tells us that localization is an idempotent operation.

Corollary A.2.2.12. *Let A be a ring, let S be a multiplicatively closed subset of A, and let M be an A-module. The localization map $\lambda_{M_S} \colon M_S \to (M_S)_S$ is an isomorphism.*

For the most part, we will view this isomorphism λ_{M_S} as an identification. Let us notice that it maps a fraction m/s in M_S to the fraction $(m/s)/1$ in $(M_S)_S$, and that its inverse maps a fraction $(m/s)/t$ in $(M_S)_S$ to the fraction $m/(st)$ in M_S.

Proof. Indeed, this follows immediately from Lemma A.2.2.11 since the module M_S is S-local. □

In general, submodules and quotients of S-local modules need not be S-local themselves. The result of the following exercise tells us exactly when they are.

Exercise A.2.2.13. Let A be a ring, and let S be a multiplicatively closed subset of A, and let M be an S-local A-module.

(a) Show that an A-submodule N of M is S-local if and only if it is ***S-saturated*** in M, in the sense that

> *whenever m and s are elements of M and of S, respectively, such that sm is in N we in fact have that m is in N.*

(b) Show that an A-submodule N of M is such that the quotient A-module M/N is S-local if

and only if N is S-local.

(c) Show that if N is an A-submodule of M, then the set of all S-saturated A-submodules of M has a unique minimal element. We call it the ***S-saturation*** of N in M.

Exercise A.2.2.14. Let A be a ring, and let S be a multiplicatively closed subset of A, and let us consider a short exact sequence of A-modules

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$$

Prove that if two of the three modules M, N, and P are S-local, then so is the remaining one.

Because of this, we say that the S-local A-modules form a *Serre class in the weak sense*. This notion comes essentially from the paper [Ser1953] of Jean-Pierre Serre, where it plays a key role in the proof of his ground-breaking theorem, presented there, that the homotopy groups of spheres are finite, except for those of the form $\pi_n(S^n)$ and $\pi_{4n-1}(S^{2n})$ with n a positive integer — one of the key reasons that resulted in his being awarded the Fields Medal in 1954.

If $\phi\colon A \to B$ is a morphism of rings and M is a B-module, then one can easily check that there is an A-module $\phi^*(M)$ which coincides with M as an abelian group, and on which we have

$$a \cdot m = \phi(a)m$$

for all choices of a and of m in A and in $\phi^*(M)$, respectively — on the right of this equality the product $\phi(a)m$ denotes the action of the element $\phi(a)$ of B on m. We say that the A-module $\phi^*(M)$ is obtained from the B-module M by ***restriction of scalars*** along the morphism ϕ.

Lemma A.2.2.15. *Let A be a ring, let S be a multiplicatively closed subset of A, and let $\lambda\colon A \to A_S$ be the localization map of A at S.*

(*i*) *The underlying abelian group of a S-local A-module M has a unique structure of an A_S-module such that*

$$a/s \cdot m = \mu_{M,s}^{-1}(am)$$

whenever a is in A, s is in S, and m is in M. If M' denotes the resulting A_S-module, then $M = \lambda^*(M')$.

(*ii*) *A morphism of A-modules $f\colon M \to N$ whose domain and codomain are S-local is A_S-linear when we view that domain and codomain as A_S-modules as in* (*i*).

From now on we will view every S-local A-module as an A_S-module in the way described in the first part of this lemma. In particular, from now on the localization M_S of every A-module M will be considered as an A_S-module, since it is surely S-local. The second part of the lemma tells us that this convention is compatible with morphisms.

Proof. (*i*) Let M be an S-local module, and let us consider the function

$$\mu_M \colon a \in A \mapsto \mu_{M,a} \in \mathrm{Hom}_{\mathbb{Z}}(M, M).$$

The fact that M is an A-module implies that this is a morphism of rings and, since M is S-local, it inverts S. Let $\lambda \colon A \to A_S$ be the localization map of A at S. The universal property of the localization of A at S implies then that there exists a unique morphism of rings

$$\tilde{\mu}_M \colon A_S \to \mathrm{Hom}_{\mathbb{Z}}(M, M)$$

such that $\tilde{\mu}_M \circ \lambda = \mu_M$. This equality means precisely that $\tilde{\mu}_M(a/1) = \mu_{M,a}$ for each element a of A, and, in turn, this means that for each element a of A and each element m of M we have

$$\tilde{\mu}_M(a/1)(m) = \mu_{M,a}(m) = am.$$

As the map $\tilde{\mu}_M$ is a morphism of rings, it determines an A_S-module structure on the abelian group M with respect to which we have, for each x in A_S and each m in M, that

$$x \cdot m = \tilde{\mu}_M(x)(m)$$

It follows from this that whenever a and s are elements of A and of S, respectively, and m is an element of M, we have that

$$\mu_{M,s}(a/s \cdot m) = \tilde{\mu}_M(s/1)\big(\tilde{\mu}_M(a/s)(m)\big) = \tilde{\mu}_M(s/1 \cdot a/s)(m) = \tilde{\mu}_M(a/1)(m) = am,$$

so that $a/s \cdot m = \mu_{M,s}^{-1}(am)$. This proves the existence claim in (*i*), and the uniquess claim is clear, since every element of A_S is of the form a/s for some a in A and some s in S.

The final claim of (*i*) is true because when a and m are elements of A and of M, respectively, the product $a \cdot m$ in $\lambda^*(M')$ is, by definition, the product $\lambda(a) \cdot m$ in M, and this is $a/1 \cdot m = am$.

(*ii*) Let now M and N be two S-local A-modules, let $f \colon M \to N$ be a morphism of A-modules, and let us view M and N as A_S-modules as in (*i*). If a, s, and m are elements of A, of S, and of M, respectively, then we have that

$$\begin{aligned}\mu_{N,s}(f(a/s \cdot m)) = s \cdot f(a/s \cdot m) = f(s \cdot (a/s \cdot m)) = f(\mu_{M,s}(\mu_{M,s}^{-1}(am))) = f(am) \\ = af(m),\end{aligned}$$

so that $f(a/s \cdot m) = \mu_{N,s}^{-1}(af(m)) = a/s \cdot f(m)$. This tells us that the function f, which is certainly a morphism of abelian groups, is A_S-linear. □

Using this lemma we can characterize the A-modules that are obtained from A_S-modules by restriction of scalars along the localization map of A at S.

Corollary A.2.2.16. *Let A be a ring, let S be a multiplicatively closed subset of A, and let $\lambda\colon A \to A_S$ be the localization map of A at S. An A-module M is obtained from an A_S-module by restriction of scalars along λ if and only if it is S-local.*

Proof. The first part of Lemma A.2.2.15 implies that the condition in this corollary is sufficient: if an A-module M that is S-local, then it tells us we can view M as an A_S-module M' in such a way such that $\lambda^*(M') = M$, so M can certainly be obtained by restriction of scalars along λ.

Let, on the other hand, M be an A_S-module and s an element of S. For each m in M we have

$$\mu_{\lambda^*(M),s}(m) = s \cdot m = \lambda(s)m = s/1 \cdot m = \mu_{M,s/1}(m),$$

so that, in fact, $\mu_{\lambda^*(M),s} = \mu_{M,s/1}$. As the functions $\mu_{M,s/1}$ and $\mu_{M,1/s}$ are mutually inverse, they are bijective, and thus so is $\mu_{\lambda^*(M),s}$. This shows that $\lambda^*(M)$ is S-local. □

We have been talking about localizing modules, but we can also localize morphisms of modules.

Lemma A.2.2.17. *Let A be a ring, let S be a multiplicatively closed subset of A, and let $f\colon M \to N$ be a morphism of A-modules. There is a unique morphism of A-modules $f_S\colon M_S \to N_S$ such that $f_S \circ \lambda_M = \lambda_N \circ f$ or, equivalently, such that $f_S(m/1) = f(m)/1$ for each element m of M, and it is A_S-linear.*

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle\lambda_M}\downarrow & & \downarrow{\scriptstyle\lambda_N} \\ M_S & \xrightarrow{f_S} & N_S \end{array}$$

We call the morphism f_S the ***localization*** of the morphism f at S.

Proof. The morphism of A-modules $\lambda_N \circ f\colon M \to N_S$ has as codomain an S-local A-module, so we know from the second part of Exercise A.2.2.8 that there is exactly one morphism of A-modules $f_S\colon M_S \to N_S$ such that $f_S \circ \lambda_M = \lambda_N \circ f$. Moreover, since the domain and codomain of f_S are S-local modules, we know from Lemma A.2.2.15 that f_S is, in fact, A_S-linear. □

The construction described in this lemma from a morphism of A-modules $f\colon M \to N$ to a map of A_S-modules $f_S\colon M_S \to N_S$ is of «functorial nature»: what this means is, precisely, that the two statements of the following lemma are true.

Lemma A.2.2.18. *Let A be a ring, and let S be a multiplicatively closed subset of A.*

(i) If M is an A-module, then the function $(\mathrm{id}_M)_S\colon M_S \to M_S$ is the identity map of M_S.

(ii) If $f\colon M \to N$ and $g\colon N \to P$ are morphisms of A-modules, then $(g \circ f)_S = g_S \circ f_S\colon M_S \to P_S$.

Proof. □

An immediate consequence of the functoriality of the localization of maps is that that operation preserves isomorphisms.

Exercise A.2.2.19. Let A be a ring, and let S be a multiplicatively closed subset of A. Show that if $f\colon M \to N$ is an isomorphism of A-modules, then so is the localization $f_S\colon M_S \to N_S$.

The operation of localization of maps interacts well with the module structures carried by Hom-sets, in the following sense.

Lemma A.2.2.20. *Let A be a ring, let S be a multiplicatively closed subset of A, and let M and N be two A-modules. The function*

$$\phi_{M,N}\colon f \in \mathrm{Hom}_A(M,N) \mapsto f_S \in \mathrm{Hom}_{A_S}(M_S, N_S)$$

is a map of A-modules, and there is exactly one morphism of A_S-modules

$$\tilde{\phi}_{M,N}\colon \mathrm{Hom}_A(M,N)_S \to \mathrm{Hom}_{A_S}(M_S, N_S)$$

such that $\tilde{\phi}_{M,N}(f/1) = f_S$ for each element f of $\mathrm{Hom}_A(M,N)$

As the localizations M_S and N_S are A_S-modules, the abelian group $\mathrm{Hom}_{A_S}(M_S, N_S)$ has a canonical structure of A_S-module and, by restriction of scalars along the localization map of A at S, a canonical structure of A-module. This is why the first claim of the lemma makes sense. On the other hand, $\mathrm{Hom}_A(M,N)$ is an A-module, so we can consider its localization $\mathrm{Hom}_A(M,N)_S$ at S, which is canonically an A_S-module: this is why the second claim makes sense.

Proof. Let f and g be two elements of $\mathrm{Hom}_A(M,N)$, and let a and b be two elements of A. If m is an element of M, then we have that

$$(af+bg)_S(m/1) = (af+bg)(m)/1 = (af(m)+bg(m))/1 = a\cdot f(m)/1 + b\cdot g(m)/1$$

because of the way in which N_S is an A-module, and this is

$$= a\cdot f_S(m/1) + b\cdot g_S(m/1) = (a\cdot f_S + b\cdot g_S)(m/1)$$

because of the way in which $\mathrm{Hom}_{A_S}(M_S, N_S)$ is an A-module. It follows then from the uniqueness claim of Lemma A.2.2.17 that

$$\phi_{M,N}(af+bg) = (af+bg)_S = a\cdot f_S + b\cdot g_S = a\cdot\phi_{M,N}(f) + b\cdot\phi_{M,N}(g).$$

The map $\phi_{M,N}$ is therefore A-linear.

The abelian group $\mathrm{Hom}_{A_S}(M_S, N_S)$ is canonically an A_S-module, as we recalled above, and it is an A-module by restriction of scalars along the localization map of A at S, so it is an S-local A-module. The second claim of the lemma then follows at once from the universal property of the localization of the A-module $\mathrm{Hom}_A(M, N)$ at S and the fact that the map $\phi_{M,N}$ A-linear. □

In general, the map $\tilde{\phi}_{M,N}$ described in this lemma is neither injective nor surjective. We will show later that it is an isomorphism when the module M is finitely presented. When we do that, we will use the result of the following exercise.

Exercise A.2.2.21. Let A be a ring, let S be a multiplicatively closed subset of A, let $u\colon M' \to M$ and $v\colon N \to N'$ be morphisms of A-modules, and let $u_S\colon M'_S \to M_S$ and $v_S\colon N_S \to N'_S$ be their localizations at S. Show that the function

$$\mathrm{Hom}_A(u, v)\colon f \in \mathrm{Hom}_A(M, N) \mapsto v \circ f \circ u \in \mathrm{Hom}_A(M', N')$$

is a morphism of A-modules, so that we can consider its localization

$$\mathrm{Hom}_A(u, v)_S\colon \mathrm{Hom}_A(M, N)_S \to \mathrm{Hom}_A(M', N')_S$$

at S, and that the function

$$\mathrm{Hom}_{A_S}(u_S, v_S)\colon f \in \mathrm{Hom}_{A_S}(M_S, N_S) \mapsto v_S \circ f \circ u_S \in \mathrm{Hom}_{A_S}(M'_S, N'_S)$$

is a morphism of A_S-modules, and prove that the diagram

$$\begin{array}{ccc} \mathrm{Hom}_A(M, N)_S & \xrightarrow{\tilde{\phi}_{M,N}} & \mathrm{Hom}_{A_S}(M_S, N_S) \\ {\scriptstyle \mathrm{Hom}_A(u,v)_S}\downarrow & & \downarrow{\scriptstyle \mathrm{Hom}_{A_S}(u_S, v_S)} \\ \mathrm{Hom}_A(M', N')_S & \xrightarrow{\tilde{\phi}_{M',N'}} & \mathrm{Hom}_{A_S}(M'_S, N'_S) \end{array}$$

comutes. Here $\tilde{\phi}_{M,N}$ and $\tilde{\phi}_{M',N'}$ are maps just as in Lemma A.2.2.20.

The following lemma tells us how the operations of restriction of scalars and localization interact.

Lemma A.2.2.22. *Let $\pi\colon A \to B$ be a morphism of rings, and let S be a multiplicatively closed subset of A.*

(*i*) *The set $\pi(S)$ is a multiplicatively closed subset of B and there is a unique morphism of rings $\pi_S\colon A_S \to B_{\pi(S)}$ such that $\pi_S(a/s) = \pi(a)/\pi(s)$ for every choice of a in A and of s in S, and it is surjective if π is surjective.*

(*ii*) *For every B-module M there is unique isomorphism of A-modules $\phi\colon M_S \to M_{\pi(S)}$ such that*

$$\phi(m/s) = m/\pi(s)$$

whenever m and s are elements of M and of S, respectively.

(*iii*) *If the morphism π is surjective, there the A-module M_S is in a unique way a $B_{\pi(S)}$-module and the map ϕ is an isomorphism of $B_{\pi(S)}$-modules.*

Since here M is a B-module, we can view it as an A-module by restriction of scalars along the morphism π and then construct its localization M_S at S: this is the A-module that appears as the domain of the morphism ϕ in this lemma.

Proof. (*i*) That the set $\pi(S)$ is a multiplicatively closed subset of B is clear. The composition $\lambda_{B,\pi(S)} \circ \pi\colon A \to B_{\pi(S)}$ of the map π with the localization map $\lambda_{B,\pi(S)}\colon B \to B_{\pi(S)}$ of B at $\pi(S)$ is a morphism of rings, and it inverts S. Indeed, if s is an element of S, then $\pi(s)$ is of course an element of $\pi(S)$, so that $\lambda_{B,\pi(S)}(\pi(s))$ is invertible in $B_{\pi(S)}$. The universal property of the localization of A at S implies then that there is a unique morphism of rings $\phi\colon A_S \to B_{\pi(S)}$ such that $\phi \circ \lambda_{A,S} = \lambda_{B,\pi(S)} \circ \pi$. This equality is equivalent to the statement that for each a in A we have $\phi(a/1) = \pi(a)/1$.

(*ii*) We may view the localization $M_{\pi(S)}$ as a B-module by restricting scalars along the localization map $B \to B_{\pi(S)}$, and then as an A-module by further restricting scalars along the morphism π. If s is an element of S, then the map $x \in M_{\pi(S)} \mapsto sx \in M_{\pi(S)}$ coincides with the map $x \in M_{\pi(S)} \mapsto \pi(s)x \in M_{\pi(S)}$, which is bijective because $M_{\pi(S)}$ is $\pi(S)$-local. This tells us that $M_{\pi(S)}$, as an A-module, is S-local.

The localization map $\lambda_M\colon M \to M_{\pi(S)}$ of the B-module M at $\pi(S)$ is A-linear: as its codomain is S-local, there is a morphism of A-modules $\phi\colon M_S \to M_{\pi(S)}$ such that $s \cdot \phi(m/s) = \lambda_M(m) = m/1$ for all m in M and all s in S. In view of the way $M_{\pi(S)}$ is an A-module, this implies that $\phi(m/s) = m/\pi(s)$ for all m in M and all s in S. Let us show ϕ is an isomorphism.

- Let x be an element of M_S such that $\phi(x) = 0$. There are elements m of M and s of S such that $x = m/s$, and we have that $0 = \phi(m/s) = m/\pi(s)$. There is then an element t of S such that $\pi(t)m = 0$ in the B-module M, and this implies that $tm = 0$ in the A-module M, so that $x = m/s = 0$ in M_S.
- On the other hand, if y is an element of $M_{\pi(S)}$, so that there are elements m of M and s of S such that $y = m/\pi(s)$, then we have that $y = \phi(m/s) \in \operatorname{img}\phi$.

Finally, the fact that there is at most a function $\phi\colon M_S \to M_{\pi(S)}$ that satisfies the condition given in the lemma is an immediate consequence of the fact that every element of M_S is of the form m/s for some m in M and some s in S.

(*iii*) Let us suppose now that the map π is surjective. It is then clear that there is a unique

structure of B-module on the A-module M_S such that restricting scalars along π gives its original A-module structure. In order to prove that the map ϕ of (i) is an isomorphism of B-modules we need only check that it is B-homogeneous, as we already know it is an isomorphism of abelian groups. Let x be an element of M_S and let b be an element of B. As π is surjective, there is an element a of A such that $b = \pi(a)$, and the way B acts on M_S implies that $bx = \pi(b)x$, so that $\phi(bx) = \phi(\pi(a)x) = \pi(a)\phi(x) = b\phi(x)$. □

A.2.3. Exactness properties of localization

In this subsection we fix a ring A and a multiplicatively closed subset S of A.

Lemma A.2.3.1. *Let M be an A-module, and let m and s be elements of M and of S, respectively. We have that $m/s = 0$ in M_S if and only if there is an element t in S such that $tm = 0$.*

Proof. If $m/s = 0 = 0/1$ in M_S, then there exists an element t in S such that $tm = t(1m - s0) = 0$, so that the condition of the lemma holds. On the other hand, if there is an element t of S such that $tm = 0$, then $t(1m - s0) = 0$ and therefore $m/s = 0/1 = 0$ in M_S. □

It follows from this lemma that it is very possible that the localization of a non-zero module be zero. Indeed, it is easy to construct examples of this.

Example A.2.3.2. Let us take $A \coloneqq \mathbb{Z}$, $S \coloneqq \{2^n : n \geq 0\}$, and $M \coloneqq \mathbb{Z}/2\mathbb{Z}$. Since every element of M is annihilated by 2 and 2 is in S, we have that $M_S = 0$.

Exercise A.2.3.3. Show that a finitely generated A-module M such that $M_S = 0$ is zero, and that the hypothesis of finite generation is needed to reach this conclusion in general.

There are many properties that «pass to localizations». The following lemma gives a few.

Lemma A.2.3.4.

(i) *If an A-module M is zero, then the localization M_S is zero.*

(ii) *If $f\colon M \to N$ is a morphism of A-modules that is injective, then so is the map $f_S\colon M_S \to N_S$.*

(iii) *If $f\colon M \to N$ is a morphism of A-modules that is surjective, then so is the map $f_S\colon M_S \to N_S$.*

(iv) *If $f\colon M \to N$ is a morphism of A-modules that is bijective, then so is the map $f_S\colon M_S \to N_S$.*

Proof. The statement (i) is obvious.

(ii) Let $f\colon M \to N$ be an injective morphism of A-modules, let $f_S\colon M_S \to N_S$ be its localization at S, and let x be an element of M_S such that $f_S(x) = 0$. There are elements m and s of M and of S such that $x = m/s$, and $f(m)/s = f_S(m/s) = f_S(x) = 0$ in N_S, so that there is an element t of S

such that $tf(m) = 0$. We then have that $f(tm) = 0$ and, since f is injective, that $tm = 0$, so that $x = m/s = 0$ in M_S. The map f_S is therefore injective.

(*iii*) Let $f\colon M \to N$ be a surjective morphism of A-modules, let $f_S\colon M_S \to N_S$ be its localization at S, and let y be an element of N_S, so that there are elements n and s of N and of S, respectively, such that $y = n/s$. Since the map f is surjective, there is an element m of M such that $n = f(m)$, and then $y = n/s = f(m)/s = f_S(m/s) \in \operatorname{img} f_S$. This shows that the map f_S is surjective.

(*iv*) This final statement follows immediately from the statements (*ii*) and (*iii*). □

If M is an A-module and N is a submodule of M, then the inclusion map $\iota\colon N \to M$ is an injective morphism of A-modules so, according to this lemma, its localization $\iota_S\colon N_S \to M_S$ is an injective morphism of A_S-modules. From now on we will identify the localization N_S with its image in M_S under this map ι_S. This will demand some care. For example, it is clear that every element of M_S of the form n/s with n in N and s in S is in the submodule N_S, but there are fractions which are not of that form that are there too.

Lemma A.2.3.5. *Let M be an A-module, let N be a submodule of M, and let m and s be elements of M and of S, respectively. The element m/s of M_S is in N_S if and only if there is an element t of S such that $tm \in N$.*

Proof. If there is an element t of S such that $tm \in N$, then $m/s = (tm)/(ts)$ is clearly an element of the submodule N_S. Conversely, if m/s is an element of N_S, then there are elements n and u in N and S, respectively, such that $m/s = n/u$, and there is therefore an element v of S such that $v(um - sn) = 0$. The element $t \coloneqq uv$ of S is then such that $tm = uvm = vsn \in N$. □

We can describe what happens when we localize a sum or an intersection of two submodules of a module.

Lemma A.2.3.6. *Let M be an A-module. If N and P are two A-submodules of M, then*

$$N_S + P_S = (N + P)_S, \qquad N_S \cap P_S = (N \cap P)_S.$$

Proof. Since we are comparing four submodules of M_S, it is enough that we check the needed inclusions.

- Let x be an element of $N_S + P_S$. There are elements y and z of N_S and of P_S, respectively, such that $x = y + z$, and there are elements n of N, p of P, and s and t of S such that $y = n/s$ and $z = p/t$, and we therefore have that $x = y + z = n/s + p/t = (tn + sp)/(st) \in (N + P)_S$.
- Let x be an element of $(N + P)_S$, so that there are an element y of $N + P$ and an element s of S such that $x = y/s$. Since y is in $N + P$, there are an element n of N and an element p of P such that $y = n + p$, and we have that $x = y/s = (n + p)/s = n/s + p/s \in N_S + P_S$.

- Let x be an element of $N_S \cap P_S$. Since x is in N_S, there are elements n and s of N and of S such that $x = n/s$; similarly, since x is in P_S, there are elements p and t of P and of S such that $x = p/t$. As $n/s = x = p/t$, there is an element u of S such that $u(tn - sp) = 0$ or, equivalently, such that $utn = usp$. This equality tells us that $utn \in N \cap P$, so that $x = n/s = (utn)/(uts) \in (N \cap P)_S$.
- Finally, let x be an element of $(N \cap P)_S$, so that there is an element m of $N \cap P$ and an element s of S such that $x = m/s$. As m is in N, we have that $x = m/s \in N_S$, and as m is in P, we have that $x = m/s \in P_S$. It follows then that $x \in N_S \cap P_S$. □

Being able to describe submodules of localizations, we can improve Lemma A.2.3.4 in the following way.

Lemma A.2.3.7. *Let $f\colon M \to N$ be a morphism of A-modules. The image and the kernel of of the localized map $f_S\colon M_S \to N_S$ are $(\operatorname{img} f)_S$ and $(\ker f)_S$, respectively.*

Proof. If x is an element of the image of f_S, then there are elements m and s of M and of S, respectively, such that $x = f_S(m/s) = f(m)/s$, and then clearly x is in $(\operatorname{img} f)_S$. Conversely, if x is an element of $(\operatorname{img} f)_S$, then there are an element n of $\operatorname{img} f$ and an element s of S such that $x = n/s$, and an element m of M such that $n = f(m)$: it follows from this that $x = f(m)/s = f_S(m/s) \in \operatorname{img} f_S$. We have proved that $\operatorname{img} f_S = (\operatorname{img} f)_S$.

If x is an element of $\ker f_S$, then there are an element m of M and an element s of S such that $x = m/s$, and we have that $0 = f_S(x) = f(m)/s$, so that there is an element t of S such that $f(tm) = tf(m) = 0$. We then have that $tm \in \ker f$ and that $x = (tm)/(ts) \in (\ker f)_S$. Conversely, if x is an element of $(\ker f)_S$, then there are elements m and s of M and of S, respectively, such that $x = m/s$ and $f(m) = 0$, and then $f_S(x) = f(m)/s = 0$, so $x \in \ker f_S$. This shows that $\ker f_S = (\ker f)_S$. □

This description of the kernels and images of localized maps allows us to prove immediately that localization preserves exactness.

Lemma A.2.3.8. *If*

$$M \xrightarrow{f} N \xrightarrow{g} P \tag{A.2}$$

is an exact sequence of A-modules, then the sequence

$$M_S \xrightarrow{f_S} N_S \xrightarrow{g_S} P_S \tag{A.3}$$

is also exact.

Proof. Let us suppose that (A.2) is a short exact sequence of A-modules. Since $g \circ f = 0$, then $g_S \circ f_S = (g \circ f)_S = 0$, and the sequence (A.3) is a complex. On the other hand, we have that $\operatorname{img} f_S = (\operatorname{img} f)_S = (\ker g)_S = \ker g_S$, so the sequence (A.3) is also exact. □

Let us see how localization interacts with quotients of modules. Let M be an A-module and let N be a submodule of M.

Lemma A.2.3.9. *Let M be an A-module and let N be a submodule of M. There is a unique morphism of A-modules $\phi\colon (M/N)_S \to M_S/N_S$ such that*

$$\phi((m+N)/1) = m/1 + N_S$$

for each m in M and each s in S, and it is an isomorphism of A_S-modules.

In the future, when we are in the situation of this lemma we will often identify the localization $(M/N)_S$ with the quotient M_S/N_S using this isomorphism.

Proof. Let $\lambda_M\colon M \to M_S$ be the localization map of M at S, and let $\pi\colon M_S \to M_S/N_S$ be the quotient map, both of which are A-linear. The composition

$$f \coloneqq \pi \circ \lambda_M\colon m \in M \mapsto m/1 + N_S \in M_S/N_S$$

is then a morphism of A-modules, and for each n in N we have that $f(n) = n/1 + N_S = 0 + N_S$ in M_S/N_S, since $n/1 \in N_S$, so that $N \subseteq \ker f$. There is therefore a unique morphism of A-modules $f_1\colon M/N \to M_S/N_S$ such that $f_1(m+N) = m/1 + N_S$ for each m in M. Now, the module M_S/N_S is S-local according to Exercise A.2.2.13, and there is then a unique morphism of A-modules $\phi\colon (M/N)_S \to M_S/N_S$ such that $\phi((m+N)/1) = m/1 + N_S$ for all m in M, and it is A_S-linear.

Let now $\pi_S\colon M_S \to (M/N)_S$ be the localization at S of the quotient map π, which has $\pi_S(m/s) = (m+N)/s$ whenever m is in M and s is in S. If n and s are elements of N and of S, then we have that $\pi_S(n/s) = (n+N)/s = (0+N)/s = 0$, and this tells us that $N_S \subseteq \ker \pi_S$, so that there is a unique morphism of A-modules $\bar{\pi}_S\colon M_S/N_S \to (M/N)_S$ such that $\bar{\pi}_S(m/s + N_S) = (m+N)/s$ for all choices of m and s in M and in S.

Finally, for any m in M and any s in S we have that

$$\bar{\pi}_S(\phi((m+N)/s)) = \bar{\pi}_S(m/s + N_S) = (m+N)/s$$

and

$$\phi(\bar{\pi}_S(m/s + N_S)) = \phi((m+N)/s) = m/s + N_S,$$

and this tells us that ϕ and $\bar{\pi}_S$ are mutually inverse functions. □

As a special case of the lemma we have just proved, we can describe what localization does to cokernels.

Corollary A.2.3.10. *Let $f\colon M \to N$ be a morphism of A-modules. There is exactly one morphism of A-modules $\phi\colon (\operatorname{coker} f)_S \to \operatorname{coker} f_S$ such that $\phi((n + \operatorname{img} f)/1) = (n/1 + \operatorname{img} f_S)$ for all n in N, and it is an isomorphism of A_S-modules.* □

We have seen that by localizing submodules of an A-module M we obtain A_S-submodules of its localization M_S. In fact, we obtain in this way all the A_S-submodules of M_S. The following two lemmas make this precise.

Lemma A.2.3.11. *Let M be an A-module, and let $\lambda_M\colon M \to M_S$ be the localization map of A at S.*

(*i*) *If N is a submodule of M, then the A_S-submodule N_S of M_S is generated by the set $\lambda_M(N)$, so that $N_S = A_S \cdot \lambda_M(N)$.*

(*ii*) *If P is an A_S-submodule of M_S, then $\lambda_M^{-1}(P)$ is an S-saturated A-submodule of M.*

(*iii*) *For each A-submodule N of M the submodule $\lambda_M^{-1}(N_S)$ is the S-saturation of N in M and, in particular, contains N.*

(*iv*) *For each A_S-submodule P of A_S we have that $P = (\lambda_M^{-1}(P))_S$.*

(*v*) *If N is an A-submodule of M and $\overline{N}$ is its S-saturation in M, then for every submodule Q of M such that $N \subseteq Q \subseteq \overline{N}$ we have $Q_S = N_S$.*

Proof. (*i*) Let x be an element of N_S, so that there are elements n of N and s of S such that $x = n/s$. In A_S we then have that $x = n/s = 1/s \cdot \lambda_M(n)$, so that x is in the A_S-submodule $\langle \lambda_M(N) \rangle$ of M_S generated by $\lambda_M(N)$. Conversely, if n is an element of N, then $\lambda_M(n) = n/1 \in N_S$, so that $\lambda_M(N) \subseteq N_S$ and thus also $\langle \lambda_M(N) \rangle \subseteq N_S$.

(*ii*) Let P be an A_S-submodule of M_S. Since P is then also an A-submodule of M_S and the map λ_M is a morphism of A-modules, it is clear that $\lambda_M^{-1}(P)$ is an A-submodule of M. If s and m are an element of S and an element of $\lambda_M^{-1}(P)$, respectively, and we have that $sm \in \lambda_M^{-1}(P)$, then

$$\lambda_M(m) = 1/s \cdot s/1 \cdot \lambda_M(m) = 1/s \cdot s \cdot \lambda_M(m) = 1/s \cdot \lambda_M(s \cdot m) \in P,$$

so that $m \in \lambda_M^{-1}(P)$. This proves that $\lambda_M^{-1}(P)$ is an S-saturated A-submodule of M.

(*iii*) Let N be a A-submodule of M. Since $N_S = \lambda_M(N)$, we have that $N \subseteq \lambda_M^{-1}(N_S)$. As $\lambda_M^{-1}(N_S)$ is an S-saturated A-submodule of M, to prove what we want we need to show that every S-saturated A-submodule of M that contains N contains $\lambda_M^{-1}(N_S)$.

Let then Q be an S-saturated A-submodule of M that contains N, and let m be an element of $\lambda_M^{-1}(N_S)$. Since $\lambda_M(m) \in N_S$, there are elements n in N and s in S such that $m/1 = \lambda_M(m) = n/s$, and this means that there is an element t of S such that $t(sm - n) = 0$. As $tsm = tn \in N \subseteq Q$ and Q is S-saturated, we see that m is in Q. This shows that $\lambda_M^{-1}(N_S) \subseteq Q$, as we want.

(*iv*) Let P be an A_S-submodule of M_S. We have that $(\lambda_M^{-1}(P))_S = \lambda_M(\lambda_M^{-1}(P)) \subseteq P$. Let, on

the other hand, x be an element of P. As x is in M_S, there are an element m of M and an element s of S such that $x = m/s$. We have that $\lambda_M(m) = m/1 = s/1 \cdot m/s \in P$, so that $m \in \lambda_M^{-1}(P)$, and therefore $x = m/s \in (\lambda_M^{-1}(P))_S$. This shows that also $P \subseteq (\lambda_M^{-1}(P))_S$, so that $P = (\lambda_M^{-1}(P))_S$, as we want.

(*v*) If N and Q are A-submodules of M such that $N \subseteq Q \subseteq \lambda_M^{-1}(N_S)$, then we clearly have that $N_S \subseteq Q_S \subseteq \lambda_M^{-1}(N_S)_S = N_S$, so that $Q_S = N_S$. □

Using this information we can bijectively parametrize the A_S of the localization of an A-module M at S.

Lemma A.2.3.12. *Let M be an A-module, and let $\lambda_M \colon M \to M_S$ be the localization map of A at S.*

(*i*) *The functions*

$$\alpha \colon P \in \mathrm{Sub}_{A_S}(M_S) \mapsto \lambda_M^{-1}(P) \in \mathrm{Sub}_A(M)$$

and

$$\beta \colon N \in \mathrm{Sub}_A(M) \mapsto N_S \in \mathrm{Sub}_{A_S}(M_S)$$

preserve inclusions and are such that $\beta \circ \alpha = \mathsf{id}_{\mathrm{Sub}_{A_S}(M)}$.

(*ii*) *The image of α is the set $\mathrm{Sub}_A^S(M)$ of all S-saturated A-submodules of M.*

(*iii*) *The restrictions*

$$\alpha|^{\mathrm{Sub}_A^S(M)} \colon \mathrm{Sub}_{A_S}(M_S) \to \mathrm{Sub}_A^S(M)$$

and

$$\beta|_{\mathrm{Sub}_A^S(M)} \colon \mathrm{Sub}_A^S(M) \to \mathrm{Sub}_{A_S}(M_S)$$

are mutually inverse bijections.

Proof. That the functions α and β preserve inclusions is clear, and that the composition $\beta \circ \alpha$ is an identity is precisely the content of part (*iv*) of Lemma A.2.3.11. This implies, in particular, that the function α is injective. The image of α is contained in the set $\mathrm{Sub}_A^S(M)$ because of part (*ii*) of that same lemma. On the other hand, if N is an S-saturated submodule of M, then $\alpha(N_S) = \lambda_M^{-1}(N_S)$ is the S-saturation of N by part (*iii*) of the lemma, so equal to N itself. The image of α is therefore the set $\mathrm{Sub}_A^S(M)$, and the corestriction of α to that set is a bijection. Since $\beta \circ \alpha$ is an identity, the map β is the inverse of α and, *a fortiori*, it is invertible. □

A.2.4. Localization of ideals

The ideals of a ring are precisely the submodules of the regular module of the ring, so the theory of localization of modules and submodules applies to ideals.

Lemma A.2.4.1. *Let A be a ring, let S be a multiplicatively closed subset of A, and let $\lambda\colon A \to A_S$ be the localization map of A at S.*

(i) If I is an ideal of A, then $I^e \coloneqq I_S$ is the ideal of A_S generated $\lambda(I)$, so that $I^e = I \cdot A_S$.

(ii) If J is an ideal of A_S, then $J^c \coloneqq \lambda^{-1}(J)$ is an S-saturated ideal of A.

(iii) For each ideal I of A the ideal $(I^e)^c$ is the S-saturation of I in A, so that, in particular, $I \subseteq (I^e)^c$.

(iv) For each ideal J of A_S we have that $J = (J^c)^e$.

(v) The function

$$c\colon J \in \mathrm{Sub}_{A_S}(A_S) \mapsto J^c \in \mathrm{Sub}_A(A)$$

is injective and the function

$$e\colon I \in \mathrm{Sub}_A(A) \mapsto I^e \in \mathrm{Sub}_{A_S}(A_S)$$

is surjective, and we have that $e \circ c = \mathsf{id}_{\mathrm{Sub}_{A_S}(A_S)}$.

(vi) An ideal I of A is such that $I^e = A_S$ if and only if $I \cap S \neq \varnothing$.

If I is an ideal of A, then the ideal $I^e = I_S$ is called the ***extension*** of I in A_S, and if J is an ideal of A_S, then the ideal $J^c \coloneqq \lambda^{-1}(J)$ of A is called the ***contraction*** of J to A. We should notice that an element a of A belongs to the contraction J^c of an ideal J of A_S exactly when $a/1$ is in J.

Proof. The statements (i)–(iv) are direct consequences of the statements (i)–(iv) of Lemma A.2.3.11, and the statement (v) follows form the ones that precede it.

Let us prove the statement (vi). Let I be an ideal of A. If there is an element s of S in I, then the fraction $s/1$ is in $I^e = I_S$ and, since that fraction is a unit of A_S, we have that $I^e = A_S$. Conversely, if $I^e = A_S$, then $1/1 \in I^e = I_S$ and there are an element a of I and an element s of S such that $a/s = 1/1$. This means that there is an element t of S such that $ta = ts$, and then $ts \in I \cap S$. □

Contraction and extension of ideals are, in general, not bijective operations. The following lemma tells us that if we restrict them to prime ideals the behaviour of these operations is better.

Lemma A.2.4.2. *Let A be a ring, and let S be a multiplicatively closed subset of A that does not contain* 0.

(i) If $\mathfrak{p}$ is prime ideal of A_S, then the contraction $\mathfrak{p}^c$ is a prime ideal of A such that $\mathfrak{p}^c \cap S = \varnothing$.

(ii) If $\mathfrak{p}$ is a prime ideal of A such that $\mathfrak{p} \cap S = \varnothing$, then the extension $\mathfrak{p}^e$ is a prime ideal of A_S.

(*iii*) *There are functions*

$$\mathfrak{p} \in \operatorname{Spec} A_S \mapsto \mathfrak{p}^c \in \{\mathfrak{q} \in \operatorname{Spec} A : \mathfrak{q} \cap S = \varnothing\}$$

and

$$\mathfrak{p} \in \{\mathfrak{q} \in \operatorname{Spec} A : \mathfrak{q} \cap S = \varnothing\} \mapsto \mathfrak{p}^e \in \operatorname{Spec} A_S,$$

and they are mutually inverse bijections.

Proof. (*i*) Let $\mathfrak{p}$ be a prime ideal of A_S, and let a and b be two elements of A such that $ab \in \mathfrak{p}^c$. As this implies that $a/1 \cdot b/1 = (ab)/1 \in \mathfrak{p}$, one of $a/1$ or $b/1$ is in $\mathfrak{p}$, and thus one of a or b is in $\mathfrak{p}^c$. This tells us that the contraction $\mathfrak{p}^c$ is prime in A. On the other hand, if s is an element of $\mathfrak{p}^c \cap S$, then $s/1 \in (\mathfrak{p}^c)^e = \mathfrak{p}$ and therefore also $1 = 1/s \cdot s/1 \in \mathfrak{p}$: this is absurd, since $\mathfrak{p} \neq A_S$, and we can conclude that $\mathfrak{p} \cap S = \varnothing$.

(*ii*) Let now $\mathfrak{p}$ be an ideal of A such that $\mathfrak{p} \cap S = \varnothing$. The last part of Lemma A.2.4.1 tells us that $\mathfrak{p}^e \subsetneq A_S$, and Lemma A.2.1.21 tells us that the ring $A_S/\mathfrak{p}^e = A_S/\mathfrak{p}_S = (A/\mathfrak{p})_S$ is an integral domain, so that the ideal $\mathfrak{p}^e$ of A_S is prime.

(*iii*) That there are indeed functions as described in the statement of the lemma is a consequence of the first two parts. Lemma A.2.4.1 tells us that for every element $\mathfrak{p}$ of $\operatorname{Spec} A_S$ we have that $(\mathfrak{p}^c)^e = \mathfrak{p}$. Let, on the other hand, $\mathfrak{p}$ be a prime ideal of A such that $p \cap S = \varnothing$. That same lemma tells us that $(\mathfrak{p}^e)^c$ is the S-saturation of $\mathfrak{p}$ in A: since $\mathfrak{p}$ is a prime ideal disjoint from S, that S-saturation is simply $\mathfrak{p}$. We see with this that the two functions of the lemma are mutually inverse. □

Lemma A.2.3.9 tells us that the localization of a quotient of modules is canonically isomorphic to the quotient of their localizations. This isomorphism is of modules, but when we are dealing with ideals the quotients that we have are rings. The following lemma tells us that the maps that we get in this case are, in fact, isomorphisms of ring.

Proposition A.2.4.3. *Let A be a ring, let S be a multiplicatively closed subset of A, let I be an ideal of A, and let $\pi\colon A \to A/I$ be the quotient map.*

(*i*) *The localization I_S is an ideal of A_S, the subset $\pi(S)$ of A/I is multiplicatively closed, there is a unique isomorphism of rings $\alpha\colon A_S/I_S \to (A/I)_{\pi(S)}$ such that $\alpha(a/s + I_S) = (a + I)/\pi(s)$ for all a in A and all s in S.*

(*ii*) *The map $\pi_S\colon A_S \to (A/I)_S$ obtained from π, viewed as a map of A-modules, by localization at S is a surjective morphism of A-modules whose kernel is I_S, and there is therefore a unique isomorphism $\bar{\pi}_S\colon A_S/I_S \to (A/I)_S$ of A-modules such that $\bar{\pi}_S(a/s + I_S) = (a + I_S)/s$ for all a in A and all s in S.*

In (*ii*) we have written $(A/I)_S$ for the localization of the A-module A/I at S: as S is not a subset

of A/I, this is not the localization of the ring A/I at one of its multiplicatively closed subsets.

Proof. (*i*) Since I is, among other things, a submodule of A, then we can consider its localization I_S and it is an A_S-submodule of A_S. As the submodules of the regular module of a ring are precisely the ideals of the ring, this tells us that I_S is an ideal of A_S.

It is clear that the subset $\pi(S)$ of A/I is multiplicatively closed. Let $\lambda_{A/I,\pi(S)}\colon A/I \to (A/I)_{\pi(S)}$ be the corresponding localization map. The composition $\lambda_{A/I,\pi(S)} \circ \pi\colon A \to (A/I)_{\pi(S)}$ inverts S, so there is exactly one morphism of rings $\tilde{\alpha}\colon A_S \to (A/I)_{\pi(S)}$ such that

$$\tilde{\alpha}(a/s) = \lambda_{A/I,\pi(S)}(\pi(a)) = (a+I)/(s+I)$$

for each a in A and each s in S. This morphism is surjective: if x is an element of $(A/I)_{\pi(S)}$, then there are an element a of A and an element s of S such that $x = (a+I)/(s+I)$, and thus $x = \tilde{\alpha}(a/s)$.

If x is an element of I_S, then there are elements a of I and s of S such that $x = a/s$, and therefore

$$\tilde{\alpha}(a/s) = \tilde{\alpha}(1/s \cdot a/1) = \tilde{\alpha}(1/s) \cdot \tilde{\alpha}(a/1) = \tilde{\alpha}(1/s) \cdot (a+I)/1 = \tilde{\alpha}(1/s) \cdot (0+I)/1 = 0,$$

and this tells us that $I_S \subseteq \ker\tilde{\alpha}$. Conversely, if x is an element of $\ker\tilde{\alpha}$, then there are elements a and s of A and of S, respectively, such that $x = a/s$, and we therefore have that in $(A/I)_{\pi(S)}$

$$\begin{aligned} 0 &= \tilde{\alpha}(s/1) \cdot 0 = \tilde{\alpha}(s/1) \cdot \tilde{\alpha}(x) = \tilde{\alpha}(s/1) \cdot \tilde{\alpha}(a/s) = \tilde{\alpha}(s/1 \cdot a/s) = \tilde{\alpha}((sa)/s) \\ &= \tilde{\alpha}(a/1) = (a+I)/1. \end{aligned}$$

This means that there is an element t in S such that $(t+I)\cdot(a+I) = 0$ in A/I or, equivalently, such that $ta \in I$, and that we thus have that $x = a/s = (ta)/(ts) \in I_S$. Thus proves that $\ker\tilde{\alpha} \subseteq I_S$.

We can conclude from all this that $\ker\tilde{\alpha} = I_S$, and that there is therefore exactly one morphism of rings $\alpha\colon A_S/I_S \to (A/I)_{\pi(S)}$ such that $\alpha(a/s + I_S) = \tilde{\alpha}(a/s) = (a+I)/(s+I)$ and that it is injective and, in fact, bijective because $\tilde{\alpha}$ is surjective.

(*ii*) Let us now view the quotient map $\pi\colon A \to A/I$ as a surjective morphism of A-modules and consider its localization $\pi_S\colon A_S \to (A/I)_S$, which is the unique morphism of A_S-modules such that $\pi_S(a/s) = (a+I)/s$ for all a in A and all s in S. This map π_S is surjective.

If x is an element of A_S such that $\pi_S(x) = 0$, and a and s are elements of A and of S, respectively, such that $x = a/s$, then we have that $0 = \pi_S(x) = (a+I)/s$ in $(A/I)_S$, so that there is an element t in S such that $t\cdot(a+I) = 0$ or, equivalently, $ta \in I$, and thus $x = a/s = (ta)/(ts) \in I_S$. Conversely, if x is an element of I_S, then there are an element a of I and an element s of S such that $x = a/s$, and we therefore have that $\pi_S(x) = \pi_S(a/s) = (a+I)/s = (0+I)/s = 0$.

It follows from this that $\ker\pi_S = I_S$, and that there is an isomorphism $\bar{\pi}_S\colon A_S/I_S \to (A/I)_S$ such that $\bar{\pi}_S(a/s + I) = (a+I)/s$ for all a in A and all s in S. □

Let us notice that in the situation of this lemma, we can apply Lemma A.2.1.23 to the quotient map $\pi\colon A \to A/I$: it tells us that there is a morphism of rings $\pi'_S\colon A_S \to (A/I)_{\pi(S)}$ such that

$\pi'_S(a/s) = (a+I)/(s+I)$ for all a in A and all s in S, and that it is surjective. This coincides with with morphism $\tilde{\alpha}$ that we constructed in the proof of the first part of the lemma.

Exercise A.2.4.4. Let A be a ring, let S be a multiplicatively closed subset of A, and let M be a finitely generated A-module. Show that $\operatorname{ann}_A(M)_S = \operatorname{ann}_{A_S}(M_S)$.

A.2.5. Reflection from localizations

In all the results of the previous subsection, we have obtained information about localizations. An important part of the theory of localizations, though, is trying to obtain information *from* localizations. Since we know, for example, that a non-zero module M can have $M_S = 0$ for some multiplicatively closed subsets S of A, in general we cannot expect to extract much information about M from one of its localizations. What we will do next is show that we can extract a lot of information about a module from a well-chosen *set* of its localizations at different multiplicatively closed subsets. This is, in fact, the true *raison d'être* of localizations.

The simplest example of this is the following lemma.

Lemma A.2.5.1. *Let M be an A-module. The following statements are equivalent:*

(*a*) $M = 0$.
(*b*) $M_\mathfrak{p} = 0$ *for all prime ideals* $\mathfrak{p}$ *of* A.
(*c*) $M_\mathfrak{m} = 0$ *for all maximal ideals* $\mathfrak{m}$ *of* A.

Proof. The implications $(a) \Rightarrow (b)$ and $(b) \Rightarrow (c)$ are obvious, so we need only prove the implication $(c) \Rightarrow (a)$. For that, let us suppose that the module M is not zero, so that there is a non-zero element m in M. The subset $\operatorname{ann}(m) \coloneqq \{a \in A : am = 0\}$ of A is then a proper ideal of A, and there is a maximal ideal $\mathfrak{m}$ of A such that $\operatorname{ann}(m) \subseteq \mathfrak{m}$. If now a is an element of $A \setminus \mathfrak{m}$, then $a \notin \operatorname{ann}(m)$ and $am \neq 0$: it follows from Lemma A.2.3.1 that $M_\mathfrak{m} \neq 0$. This proves what we want. □

When a module has all its localizations at prime ideals zero we say that it is *locally zero*, and the lemma tells us that a module is zero if and only if it is locally zero. We therefore call it a *local criterion* for vanishing. We will see many other examples of local criteria like this. First of all, we can check for the injectivity of a morphism locally.

Lemma A.2.5.2. *Let $f\colon M \to N$ be a morphism of A-modules. The following statements are equivalent:*

(*a*) *The map $f\colon M \to N$ is injective.*
(*b*) *The map $f_\mathfrak{p}\colon M_\mathfrak{p} \to N_\mathfrak{p}$ is injective for all prime ideals $\mathfrak{p}$ of A.*
(*c*) *The map $f_\mathfrak{m}\colon M_\mathfrak{m} \to N_\mathfrak{m}$ is injective for all maximal ideals $\mathfrak{p}$ of A.*

Proof. The implication $(a) \Rightarrow (b)$ follows from the second part of Lemma A.2.3.4, and the implication $(b) \Rightarrow (c)$ is obvious. In order to prove the implication $(c) \Rightarrow (a)$, let us suppose that the map $f\colon M \to N$ is not injective, so that there is a non-zero element m in M such that $f(m) = 0$. As m is not-zero, the ideal $\operatorname{ann}(m)$ of A is proper and there is therefore a maximal ideal $\mathfrak{m}$ of A such that $\operatorname{ann}(m) \subseteq \mathfrak{m}$. This implies that $m/1 \neq 0$ in $M_{\mathfrak{m}}$. As $f_{\mathfrak{m}}(m/1) = f(m)/1 = 0/1 = 0$, this tells us that the morphism $f_{\mathfrak{m}}$ is not injective. □

Surjectivity is also a local property.

Lemma A.2.5.3. *Let $f\colon M \to N$ be a morphism of A-modules. The following statements are equivalent:*

(a) *The map $f\colon M \to N$ is surjective.*
(b) *The map $f_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is surjective for all prime ideals $\mathfrak{p}$ of A.*
(c) *The map $f_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is surjective for all maximal ideals $\mathfrak{p}$ of A.*

Proof. The implication $(a) \Rightarrow (b)$ follows from the third part of Lemma A.2.3.4, and the implication $(b) \Rightarrow (c)$ is obvious. To prove the implication $(c) \Rightarrow (a)$ let us suppose that the map f is not surjective, so that there is an element n of N which is not in the image of f. This implies that the class $n+\operatorname{img} f$ in the quotient A-module $N/\operatorname{img} f$ is not zero, so that the annihilator $\operatorname{ann}(n+\operatorname{img} f)$ is a proper ideal of A, and there is a maximal ideal $\mathfrak{m}$ of A such that $\operatorname{ann}(n + \operatorname{img} f) \subseteq \mathfrak{m}$. If x is an element of $M_{\mathfrak{m}}$, then there are elements m and s of M and of $A \setminus \mathfrak{m}$, respectively, such that $x = m/s$. We claim that $f_{\mathfrak{m}}(x) \neq n/1$. Indeed, if we had that $f_{\mathfrak{m}}(x) = f(m)/s$ is equal to $n/1$, we would have an element t of $A \setminus \mathfrak{m}$ such that $t(f(m) - sn) = 0$, so that $tsn = tf(m) \in \operatorname{img} f$ and $ts \in \operatorname{ann}(n + \operatorname{img} f) \cap (A \setminus \mathfrak{m}) = \varnothing$, which is absurd. This tells us that the element $n/1$ of $N_{\mathfrak{m}}$ is not in the image of the map $f_{\mathfrak{m}}$, which is therefore not surjective. □

Of course, combining these two results we see immediately that we can check that a map is an isomorphism locally.

Corollary A.2.5.4. *Let $f\colon M \to N$ be a morphism of A-modules. The following statements are equivalent:*

(a) *The map $f\colon M \to N$ is an isomorphism.*
(b) *The map $f_{\mathfrak{p}}\colon M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is an isomorphism for all prime ideals $\mathfrak{p}$ of A.*
(c) *The map $f_{\mathfrak{m}}\colon M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is an isomorphism for all maximal ideals $\mathfrak{p}$ of A.* □

We can also check for exactness locally.

Lemma A.2.5.5. *Let $f\colon M \to N$ and $g\colon N \to B$ be two morphisms of A-modules such that $g \circ f = 0$. The following statements are equivalent:*

(*a*) *The sequence*

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0 \tag{A.4}$$

is exact.

(*b*) *The sequence*

$$0 \longrightarrow M_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} N_{\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} P_{\mathfrak{p}} \longrightarrow 0$$

is exact for all prime ideals $\mathfrak{p}$ *of* A.

(*c*) *The sequence*

$$0 \longrightarrow M_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} N_{\mathfrak{m}} \xrightarrow{g_{\mathfrak{m}}} P_{\mathfrak{m}} \longrightarrow 0$$

is exact for all maximal $\mathfrak{m}$ *of* A.

Proof. The implication $(a) \Rightarrow (b)$ follows from Lemma A.2.3.8, and the implication $(b) \Rightarrow (c)$ is obvious. Let us prove the implication $(c) \Rightarrow (a)$, and to do that let us suppose that the statement (c) holds. Since $f_{\mathfrak{m}}$ is injective and $g_{\mathfrak{m}}$ is surjective for all maximal ideals $\mathfrak{m}$ of A, we know from Lemmas A.2.5.2 and A.2.5.3 that f is injective and g is surjective. Finally, if $\mathfrak{m}$ is a maximal ideal of A, then we have that

$$(\ker g/\operatorname{img} f)_{\mathfrak{m}} = (\ker g)_{\mathfrak{m}}/(\operatorname{img} f)_{\mathfrak{m}} = \ker g_{\mathfrak{m}}/\operatorname{img} f_{\mathfrak{m}} = 0,$$

and we can then conclude that $\ker g/\operatorname{img} f = 0$ using Lemma A.2.5.1. Of course, this implies that $\ker g = \operatorname{img} f$, so that the sequence (A.4) is exact. □

A.3. Radicals

Definition A.3.1. Let A be a ring, and let I be an ideal of A. The ***radical*** of I is the set

$$\sqrt{I} \coloneqq \{a \in A : a^n \in I \text{ for some } n \text{ in } \mathbb{N}\}.$$

The ideal I is ***radical*** if $I = \sqrt{I}$.

Proposition A.3.2. *Let A be a ring, and let I be an ideal of A. The radical $\sqrt{I}$ is the smallest radical ideal of A that contains I.*

Proof. It is clear that 0 is in $\sqrt{I}$. If a and b are elements of $\sqrt{I}$, then there are positive integers m and n such that $a^m \in I$ and $b^m \in I$, and we have that $a - b$ is in $\sqrt{I}$ because

$$\begin{aligned}(a-b)^{m+n} &= \sum_{i=0}^{m+n} \binom{m+n}{i} (-1)^{m+n-i} a^i b^{m+n-i} \\ &= b^n \sum_{i=0}^{m} \binom{m+n}{i} (-1)^{m+n-i} a^i b^{m-i} + a^m \sum_{i=m+1}^{m+n} \binom{m+n}{i} (-1)^{m+n-i} a^{i-m} b^{m+n-i} \\ &\in I + I = I.\end{aligned}$$

Finally, if a and b are elements of A and of $\sqrt{I}$, respectively, then there is a positive integer n such that $b^n \in I$ and therefore $(ab)^n = a^n b^n \in I$, so that $ab \in \sqrt{I}$. This shows that $\sqrt{I}$ is an ideal of A, and it is clear that it contains I. If a is an element of the radical of $\sqrt{I}$, then there is a positive integer n such that $a^n \in \sqrt{I}$, and there is therefore a positive integer m such that $a^{mn} = (a^n)^m \in I$, so that $a \in \sqrt{I}$. We see with this that $\sqrt{I} \subseteq \sqrt{\sqrt{I}} \subseteq \sqrt{I}$, so that the ideal $\sqrt{I}$ is radical.

Let now J be a radical ideal of A that contains I. If a is an element of $\sqrt{I}$, then there is a positive integer n such that $a^n \in I \subseteq J$ and, since the ideal J is radical, we have that $a \in J$: this tells us that $\sqrt{I} \subseteq J$. We can conclude that $\sqrt{I}$ is the smallest radical ideal of A that contains I. □

Proposition A.3.3. *Let A be a ring, and let I and J be two ideals of A.*

(*i*) *If $I \subseteq J$, then $\sqrt{I} \subseteq \sqrt{J}$.*
(*ii*) *We have that $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.*
(*iii*) *We have $\sqrt{I} = A$ if and only if $I = A$.*
(*iv*) *We have that $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.*

Proof. (*i*) Let us suppose that $I \subseteq J$. If a is an element of $\sqrt{I}$, then there is a positive integer n such that $a^n \in I$, and therefore also $a^n \in J$, so that $a \in \sqrt{J}$. This proves that $\sqrt{I} \subseteq \sqrt{J}$.

(*ii*) Since $IJ \subseteq I \cap J$, $I \cap J \subseteq I$, and $I \cap J \subseteq J$, we have that $\sqrt{IJ} \subseteq \sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$. Suppose now that a is an element of $\sqrt{I} \cap \sqrt{J}$, so that there are two positive integers m and n such that $a^m \in I$ and $a^n \in J$. We then have that $a^{m+n} \in IJ$, so that $a \in \sqrt{IJ}$. This shows that $\sqrt{I} \cap \sqrt{J} \subseteq \sqrt{IJ}$ and thus that the two equalities that appear in the statement are true.

(*iii*) It is clear that $\sqrt{A} = A$. On the other hand, if $\sqrt{I} = A$, then there is a positive integer n such that $1 = 1^n \in I$, and thus $I = A$.

(*iv*) Since $I + J \subseteq \sqrt{I} + \sqrt{J}$, we have that $\sqrt{I + J} \subseteq \sqrt{\sqrt{I} + \sqrt{J}}$. To prove the converse inclusion, let a be an element of $\sqrt{\sqrt{I} + \sqrt{J}}$, so that there are a positive integer m and elements b and c of $\sqrt{I}$ and $\sqrt{J}$, respectively, such that $a^m = b + c$. There are then positive integers n and p such

that $b^n \in I$ and $c^p \in J$, and therefore

$$\begin{aligned} a^{m(n+p)} &= (b+c)^{n+p} = \sum_{i=0}^{n+p} \binom{n+p}{i} b^i c^{n+p-i} \\ &= b^n \sum_{i=n+1}^{n+p} \binom{n+p}{i} b^{i-n} c^{n+p-i} + c^p \sum_{i=0}^{n} \binom{n+p}{i} b^i c^{n-i} \\ &\in I + J, \end{aligned}$$

so that $a \in \sqrt{I+J}$. We see with this that $\sqrt{\sqrt{I}+\sqrt{J}} \subseteq \sqrt{I+J}$. □

Proposition A.3.4. *Let A be a ring, and let I be an ideal of A. If I is prime, then for each positive integer we have that $\sqrt{I^n} = I$ and, in particular, I is radical.*

Proof. Let us suppose that the ideal I is prime, and let n be a positive integer. If a is an element of I, then of course $a^n \in I^n$, so that $a \in \sqrt{I^n}$: this shows that $I \subseteq \sqrt{I^n}$. On the other hand, if a is an element of $\sqrt{I^n}$, then there is a positive integer m such that $a^m \in I^n$, and since $I^n \subseteq I$ and I is prime, we have that $a \in I$. With this we see that, in fact, $I = \sqrt{I^n}$, as we want. □

Proposition A.3.5. *Let A be a ring, and let I be an ideal of A. The radical of I is the intersection of all the prime ideals of A that contain I and, in particular, a prime ideal is radical.*

Proof. Let $\mathscr{P}$ be the set of all prime ideals of A that contain I. If $\mathfrak{p}$ is an element of $\mathscr{P}$, then for every element a of $\sqrt{I}$ there is a positive integer n such that $a^n \in I \subseteq \mathfrak{p}$ and, since $\mathfrak{p}$ is prime, we have that $a \in \mathfrak{p}$: this shows that $\sqrt{I} \subseteq \bigcap_{\mathfrak{p}\in\mathscr{P}} \mathfrak{p}$.

Let now a be an element of $A \setminus \sqrt{I}$, and let $\mathscr{J}$ be the set of all ideals J of A that contain I and such that $a^n \notin J$ for all positive integers n. Since a is not in $\sqrt{I}$, we have that I is in $\mathscr{J}$, so that this set is not empty. On the other hand, if C is a subset of $\mathscr{J}$ that is totally ordered by inclusion, then $\bigcup C$ is an element of $\mathscr{J}$. This tells us that the set $\mathscr{J}$, ordered by inclusion, satisfies the hypotheses of Zorn's Lemma, so that there it has maximal elements. Let $\mathfrak{p}$ be one of them.

Let b and c be two elements of A that do not belong to $\mathfrak{p}$. The ideals $\mathfrak{p} + (b)$ and $\mathfrak{p} + (c)$ therefore properly contain $\mathfrak{p}$ and, in view of the way we chose $\mathfrak{p}$, do not belong to the set $\mathscr{J}$: this means that there are positive integers m and n such that $a^m \in \mathfrak{p} + (b)$ and $a^n \in \mathfrak{p} + (c)$. We then have that $a^{m+n} \in (\mathfrak{p}+(b))(\mathfrak{p}+(c)) \subseteq \mathfrak{p}+(bc)$ and, as a consequence of this, that the ideal $\mathfrak{p}+(bc)$ does not belong to $\mathscr{J}$. Since that ideal contains $\mathfrak{p}$, we see that in fact $bc \notin \mathfrak{p}$. This shows that the ideal $\mathfrak{p}$ is prime and, therefore, an element of the set $\mathscr{P}$. As $\mathfrak{p} \in \mathscr{J}$, we have that $a \notin \mathfrak{p}$, so that $a \notin \bigcap_{\mathfrak{p}\in\mathscr{P}} \mathfrak{p}$. This proves that $A \setminus \sqrt{I} \subseteq A \setminus \bigcap_{\mathfrak{p}\in\mathscr{P}} \mathfrak{p}$, so that also $\bigcap_{\mathfrak{p}\in\mathscr{P}} \mathfrak{p} \subseteq \sqrt{I}$. With what we did before we see that $\bigcap_{\mathfrak{p}\in\mathscr{P}} \mathfrak{p} = \sqrt{I}$, as we want. □

Definition A.3.6. Let A be a ring. The ***nilradical*** of A is the ideal $\operatorname{Nil} A = \sqrt{0}$, and the ring A is ***reduced*** if $\operatorname{Nil} A = 0$.

It follows immediately from the definition that the nilradical of a ring A is an ideal of A, and the fact $\operatorname{Nil} A$ is a radical ideal of A implies that the quotient ring $A/\operatorname{Nil} A$ is reduced. On the other hand, Proposition A.3.5 tells us that the following is true.

Proposition A.3.7. *The nilradical of a ring A is the intersection of all the prime ideals of A.* □

Exercise A.3.8. Let A be a ring, and let S be a multiplicatively closed subset of A.

(a) Show that if I is an ideal of A, then $\sqrt{I_S} = (\sqrt{I})_S$.

(b) Show that the ring A_S is reduced if A is.

A.4. Noetherian rings

We start with the following very general definition.

Definition A.4.1. We say that an ordered set $(X, \leq)$ satisfies the ***ascending chain condition*** if whenever $(x_i)_{i\geq 1}$ is a sequence of elements of X such that $x_i \leq x_{i+1}$ for each i in $\mathbb{N}$, then there is a positive integer N such that $x_i = x_N$ for all integers i greater than N.

We say that the ordered set $(X, \leq)$ satisfies the ***descending chain condition*** if the opposite ordered set $(X, \leq^{\mathrm{op}})$ satisfies the ascending chain condition.

There are several important concrete specializations of these conditions. For us, the following one is fundamental.

Definition A.4.2. A ring A is ***Noetherian*** if the set of its ideals, ordered with respect to the relation of inclusion, satisfies the ascending chain condition.

There are many ways to characterize Noetherian rings. The following proposition gives two of them, which are the ones most often useful.

Proposition A.4.3. *Let A be a ring. The following statements are equivalent:*

(a) The ring A is Noetherian.

(b) Every non-empty set of ideals of A has a maximal element.

(c) Every ideal of A is finitely generated.

Proof. $(a) \Rightarrow (b)$ Let us suppose that the statement (b) does not hold, so that there is a non-empty set $\mathscr{I}$ of ideals of A that does not have a maximal element. This means precisely that the relation

$$R \coloneqq \{(I, J) \in \mathscr{I} \times \mathscr{I} : I \subsetneq J\}$$

is such that $\{J \in \mathscr{I} : (I, J) \in R\} \neq \varnothing$ for each I in $\mathscr{I}$. As the set $\mathscr{I}$ itself is not empty, the *Principle of Dependent Choice* tells us that there is a sequence $(I_i)_{i\geq 1}$ of elements of $\mathscr{I}$ such that $(I_i, I_{i+1}) \in R$ or, equivalently, $I_i \subsetneq I_{i+1}$ for each i in $\mathbb{N}$, and this tells us that the ring A is not Noetherian, so that the statement (a) does not hold.

$(b) \Rightarrow (c)$ Let us suppose that the statement (b) holds, let I be an ideal of A, and let $\mathscr{I}$ be the set of all finitely generated ideals of A that are contained in I. Since $0 \in \mathscr{I}$, we have that $\mathscr{I} \neq \varnothing$, and the hypothesis implies that there is a maximal element I_0 in $\mathscr{I}$. Of course, we have that $I_0 \subseteq I$. If the inclusion were strict, then we would have an element a in $I \setminus I_0$, and the ideal $I_0 + (a)$ would be an element of $\mathscr{I}$ that strictly contains I_0, which is impossible. We thus have that $I = I_0$ and, in particular, that I is finitely generated.

$(c) \Rightarrow (a)$ Let us suppose, finally, that every ideal of A is finitely generated, and let $(I_i)_{i\geq 1}$ be a sequence of ideals of A such that $I_i \subseteq I_{i+1}$ for each i in $\mathbb{N}$. Of course, we then have that, more generally, $I_i \subseteq I_{i'}$ whenever i and i' are elements of $\mathbb{N}$ such that $i \leq i'$.

It is easy to check that then the union $I \coloneqq \bigcup_{i\geq 1} I_i$ is also an ideal of A and, according to the hypothesis, there are a non-negative integer k and elements $a_1, \ldots, a_k$ in I such that $I = \langle a_1, \ldots, a_k \rangle$. In view of the definition of I, there are positive integers $i_1, \ldots, i_k$ such that $a_j \in I_{i_j}$ for each j in $[\![k]\!]$. Let $N \coloneqq \max\{0\} \cup \{i_1, \ldots, i_k\}$. For each j in $[\![k]\!]$ we have that $i_j \leq N$, so that $a_j \in I_{i_j} \subseteq I_N$, and then $I = \langle a_1, \ldots, a_k \rangle \subseteq I_N \subseteq I$. Using this we can conclude that if i is an integer such that $i \geq N$, then $I_N \subseteq I_i \subseteq I \subseteq I_N$, so that $I_i = I_N$. We see with this that the ring A is Noetherian. □

A field is a Noetherian ring for almost trivial reasons. We will see that starting from this example we can produce many others. The most important way in which we can do this is provided by the following result, the celebrated *Basis Theorem* of David Hilbert.

Theorem A.4.4. *If A is a Noetherian ring, then so is the ring $A[x]$.*

This theorem was first stated and proved by Hilbert in his article [Hil1890] on the invariant theory of forms.

Proof. Let A be a Noetherian ring, let I be an ideal of $A[x]$, and to reach a contradiction let us suppose that I is *not* finitely generated. Let S be the set of all finite sequences of elements of I. If $f = (f_1, \ldots, f_k)$ is an element of S, then the ideal $I_f \coloneqq \langle f_1, \ldots, f_k \rangle$ generated by the components of f is contained in I and not equal to it, since it is finitely generated, and we can therefore consider

the non-negative integer

$$d(f) \coloneqq \min\{\deg g : g \in I \setminus I_f\}$$

and the set

$$D(f) \coloneqq \{g \in I \setminus I_f : \deg g = d(f)\},$$

which is not empty. There is therefore a function $\delta\colon S \to \mathscr{P}(S) \setminus \{\varnothing\}$ whose value on each element $f = (f_1, \ldots, f_k)$ of S is

$$\delta(f) \coloneqq \{(f_1, \ldots, f_k, g) : g \in D(f)\}.$$

Since the set S contains the empty sequence $()$, the *Principle of Dependent Choice* implies that there is a sequence $(\phi_i)_{i\geq 0}$ in S with $\phi_0 = ()$ and such that $\phi_{i+1} \in \delta(\phi_i)$ for each i in $\mathbb{N}_0$. Moreover, in view of the form the function δ is defined, this implies in turn that there is a sequence $(f_i)_{i\geq 1}$ in I such that $\phi_i = (f_1, \ldots, f_i)$ for each i in $\mathbb{N}_0$. Notice that $f_1 \neq 0$ because I is not the zero ideal, and that moreover for each i in $\mathbb{N}$ we have that also $f_{i+1} \neq 0$ because $f_{i+1} \in I \setminus I_{\phi_i} \not\ni 0$.

For each i in $\mathbb{N}$ let a_i be the leading coefficient of the polynomial f_i, and for each i in $\mathbb{N}$ let J_i be the ideal $\langle a_1, \ldots, a_i\rangle$ of A. We of course have that $J_i \subseteq J_{i+1}$ for all i in $\mathbb{N}$ and therefore, since the ring A is Noetherian, there is a positive integer N such that $J_i = J_N$ for all integers i greater than N. In particular, $a_{N+1} \in J_{N+1} = J_N$, so there are elements $b_1, \ldots, b_N$ in A such that $a_{N+1} = \sum_{i=1}^{N} b_i a_i$.

If i is an element of $\mathbb{N}$, then $\deg f_i \leq \deg f_{i+1}$. Indeed, we have that

$$\begin{aligned}\deg f_i &= d(f_1, \ldots, f_{i-1}) = \min\{\deg g : g \in I \setminus \langle f_1, \ldots, f_{i-1}\rangle\}\\ &\leq \min\{\deg g : g \in I \setminus \langle f_1, \ldots, f_{i-1}, f_i\rangle\} = d(f_1, \ldots, f_{i-1}, f_i) = \deg f_{i+1}.\end{aligned}$$

This implies that we can consider the element

$$h \coloneqq f_{N+1} - \sum_{i=1}^{N} b_i x^{\deg f_{N+1} - \deg f_i} \cdot f_i$$

of $A[x]$. Since f_{N+1} is not in the ideal I_{ϕ_N} and $f_1, \ldots, f_N$ are, we have that $h \in I \setminus I_{\phi_N}$, so that we have $\deg h \geq d(f_1, \ldots, f_N)$. On the other hand, the way we chose the elements $b_1, \ldots, b_N$ implies at once that $\deg h < \deg f_{N+1} = d(f_1, \ldots, f_N)$. This is absurd, and this contradiction proves the theorem. □

Hilbert's theorem implies at once that the polynomial algebras that interest us are Noetherian.

Corollary A.4.5. *If A is a Noetherian ring, then so is the ring $A[x_1, \ldots, x_n]$ for any non-negative integer n.*

Proof. Let us suppose that the ring A is Noetherian, and proceed by induction on the number n of variables. If n is 0, then the algebra in question is simply A, which is Noetherian according to the hypothesis. On the other hand, if n is a non-negative integer and the algebra $A[x_1, \ldots, x_n]$ is Noetherian, then the algebra $A[x_1, \ldots, x_n, x_{n+1}]$ is Noetherian because of Hilbert's Basis Theorem A.4.4 and the fact that there is an obvious isomorphism $A[x_1, \ldots, x_n][x] \to A[x_1, \ldots, x_{n+1}]$. □

In particular, since field are Noetherian, we have the following key fact.

Corollary A.4.6. *If $\Bbbk$ is a field, then so is the ring $\Bbbk[x_1, \ldots, x_n]$ for any non-negative integer n.*

Another important fact about Noetherian rings is that their class is closed under quotients.

Proposition A.4.7. *Let A be a Noetherian ring, and let I be an ideal of A. The quotient ring A/I is Noetherian.*

Proof. Let $\pi : A \to A/I$ be the canonical projection onto the quotient A/I, which is a surjective map. If J is an ideal of A/I, then $\pi^{-1}(J)$ is an ideal of A and there are then a non-negative integer k and elements $a_1, \ldots, a_k$ of A such that $\pi^{-1}(J) = \langle a_1, \ldots, a_k \rangle$.

Let b be an element of J. Since the map π is surjective, there is an element a of $\pi^{-1}(J)$ such that $\pi(a) = b$, and there are then elements $c_1, \ldots, c_k$ in A such that $a = \sum_{i=1}^{k} c_i a_i$. We then have that $b = \pi(a) = \sum_{i=1}^{k} \pi(c_i)\pi(a_i) \in \langle \pi(a_1), \ldots, \pi(a_k) \rangle$. This shows that $J \subseteq \langle \pi(a_1), \ldots, \pi(a_k) \rangle$, and the converse inclusion is clear, so that the elements $\pi(a_1), \ldots, \pi(a_k)$ generate J, which is therefore a finitely generated ideal. □

Combining this with Corollary A.4.6 we obtain the following fundamental fact.

Corollary A.4.8. *Every finitely generated algebra over a field is Noetherian.*

Proof. Let $\Bbbk$ be a field, and let A be a finitely generated algebra over $\Bbbk$, so that there are a non-negative integer k and elements $a_1, \ldots, a_k$ of A such that A is generated as a $\Bbbk$-algebra by the set $\{a_1, \ldots, a_k\}$. There is a unique morphism of $\Bbbk$-algebras $\phi : \Bbbk[x_1, \ldots, x_k] \to A$ such that $\phi(x_i) = a_i$ for each i in $[\![k]\!]$, and it is surjective because its image is a $\Bbbk$-subalgebra of A that contains the set $\{a_1, \ldots, a_k\}$. There is therefore an isomorphism of algebras $\Bbbk[x_1, \ldots, x_k]/\ker\phi \to A$: as the quotient $\Bbbk[x_1, \ldots, x_k]/\ker\phi$ is Noetherian because of Corollary A.4.6 and Proposition A.4.7, we see that the algebra A is Noetherian. □

We will prove in the next section that the ring $\mathbb{Z}$ of integers is also Noetherian, and we will then obtain Corollary A.5.11, a result similar to Corollary A.4.8, that tells us that every finitely generated ring is Noetherian.

The following is another important closure property of the class of Noetherian rings.

Proposition A.4.9. *Let A be a ring, and let S be a multiplicatively closed subset of A. If the ring A is Noetherian, then so is the localization A_S.*

Proof. Let us suppose that the ring A is Noetherian, let $\phi\colon A \to A_S$ be the canonical localization map, so that $\phi(a) = a/1$ for each a in A, and let I be an ideal of A_S. Since the map ϕ is a morphism of rings, the preimage $\phi^{-1}(I)$ is an ideal of A and, since the ring A is Noetherian, there are a non-negative integer k and elements $a_1, \ldots, a_k$ of A such that $\phi^{-1}(I) = \langle a_1, \ldots, a_k \rangle$. We have that

$$\langle a_1/1, \ldots, a_k/1 \rangle = \langle \phi(a_1), \ldots, \phi(a_k) \rangle = \phi(\langle a_1, \ldots, a_k \rangle) = \phi(\phi^{-1}(I)) \subseteq I.$$

Let, on the other hand, a/s be an element of I, so that a and s are an element of A and of S, respectively. We have that $\phi(a) = a/1 = s/1 \cdot a/s \in I$, so that $a \in \phi^{-1}(I)$, and there are elements $c_1, \ldots, c_k$ in A such that $a = \sum_{i=1}^{k} c_i a_i$. This implies at once that $a/s = \sum_{i=1}^{k} c_i/s \cdot a_i/1 \in \langle a_1/1, \ldots, a_k/1 \rangle$. This proves that $I = \langle a_1/1, \ldots, a_k/1 \rangle$, so that I is finitely generated. □

A.5. Principal ideal domains and Euclidean domains

A Noetherian ring is a ring in which every ideal is finitely generated. The following definition singles out an extreme case of this.

Definition A.5.1. A ring A is a ***principal ideal domain*** if it is an integral domain and every one of its ideals is of the form (a) for some a in A.

Fields are clearly principal ideal domains. To exhibit other examples we follow a slightly indirect way using the following concept.

Definition A.5.2. A ***Euclidean function*** on an integral domain A is a function $N\colon A \setminus 0 \to \mathbb{N}_0$ that satisfies the following condition:

> *if a and b are elements of A and b is not zero, then there exist elements q and r in A such that $a = qb + r$ and either $r = 0$ or $N(r) < N(b)$.* (A.5)

A ***Euclidean domain*** is an ordered pair (A, N) whose first component is an integral domain A and whose second component is a Euclidean function on A.

If (A, N) is a Euclidean domain and the context allows us to figure out what the Euclidean function N is, then we usually write simply A instead of (A, N). It is important to keep in mind, though, that if a domain admits a Euclidean function it admits many.

Exercise A.5.3. Let (A, N) be a Euclidean domain. Show that for any positive integer k the function $kN\colon a \in A \setminus 0 \mapsto kN(a) \in \mathbb{N}_0$ is also a Euclidean function on A.

Every field F is a Euclidean domain when endowed with the function $N\colon x \in F \setminus 0 \mapsto 0 \in \mathbb{N}_0$, which is a Euclidean function on it. The following proposition gives a more interesting example.

Proposition A.5.4. *The ring $\mathbb{Z}$ is a Euclidean domain with Euclidean function $N\colon a \in \mathbb{Z} \mapsto |a| \in \mathbb{N}_0$.*

Proof. Let a and b be two elements of $\mathbb{Z}$ such that $b \neq 0$, and let us suppose first that $b > 0$. Since $a/b \in \mathbb{R} = \bigcup_{n\in\mathbb{Z}}[n, n+1)$, there is an integer q in $\mathbb{Z}$ such that $a/b \in [q, q+1)$, so that $q \leq a/b < q+1$ or, equivalently, $qb \leq a < qb + b$. This tells us that the number $r \coloneqq a - qb$ is such that $0 \leq r < b$: we then have that $a = qb + r$ and that either $r = 0$ or $N(r) = r < b = |b| = N(b)$.

Let us suppose now that $b < 0$. By what we have already done, we know there are elements q' and r of $\mathbb{Z}$ such that $a = q'(-b) + r$ and either $r = 0$ or $N(r) < N(-b)$. If we put now $q \coloneqq -q$, then we have that $a = qb + r$ and either $r = 0$ or $N(r) < N(b)$. This shows that the condition (A.5) holds in all cases, so that the function N is indeed a Euclidean function on $\mathbb{Z}$. □

Another important example of a Euclidean domain is provided by the following proposition.

Proposition A.5.5. *Let $\Bbbk$ be a field. The ring $\Bbbk[x]$ is a Euclidean domain with respect to the function $N\colon f \in \Bbbk[x] \setminus 0 \mapsto \deg f \in \mathbb{N}_0$.*

Proof. Again, we need to check that the condition (A.5) of Definition A.5.2 is satisfied. Let g be a non-zero element of $\Bbbk[x]$, and, in order to reach a contradiction, let us suppose that the set P of elements f of $\Bbbk[x]$ for which there do not exist polynomials q and r in $\Bbbk[x]$ such that $f = qg + r$ and either $r = 0$ or $\deg r < \deg g$ is not empty. Notice that the zero polynomial is not in P, for clearly $0 = 0g + 0$, and that moreover every element of P has degree at least $\deg g$: if f is a polynomial with $\deg f < \deg g$, then if we set $q \coloneqq 0$ and $r \coloneqq f$ we have that $f = qg + r$ and either $r = 0$ or $\deg r < \deg g$. We can therefore consider the number

$$d \coloneqq \min\{\deg f : f \in P\},$$

and choose a polynomial f in P such that $\deg f = d$. Let a and b be the leading coefficients of f and of g, respectively and let n be the degree of f, and let us consider the polynomial $h \coloneqq f - ax^{n-\deg g}g/b$. We have that either $h = 0$ or $\deg h < \deg f$: in both cases we have that $f \notin P$ and thus there are elements q_1 and r of $\Bbbk[x]$ such that $h = q_1 g + r$ and either $r = 0$ or $\deg r < \deg g$. If we then put $q \coloneqq q_1 + ax^{n-\deg g}/b$, then we have that $f = qg + r$ and either $r = 0$ or $\deg r < \deg g$: this is absurd, because f is in P. This contradiction tells us that our hypothesis is untenable, and thus that the function N makes $\Bbbk[x]$ a Euclidean domain. □

The reader should notice that we did not include in (A.5) the condition that the elements q and r be *uniquely* determined by a and b. In the case of the polynomial ring $\Bbbk[x]$ that we have just treated, this uniqueness does hold, though.

Exercise A.5.6. Let $\Bbbk$ be a field. Show that if f and g are two elements of $\Bbbk[x]$ and g is not 0, then the polynomials q and r such that $f = qg + r$ and either $r = 0$ or $\deg r < \deg g$ are uniquely determined by f and g.

This is rather special. Indeed, the only Euclidean domains in which the elements q and r in condition (A.5) are uniquely determined are the fields and the rings of the form $\Bbbk[x]$ with $\Bbbk$ a field; see [Rha1962] or [Jod1967] for a proof of this surprising result. Notice that in $\mathbb{Z}$, with the Euclidean function of Proposition A.5.4, we do not have such uniqueness: for example, we have that

$$10 = 1 \cdot 7 + 3, \quad |3| < |7|, \qquad\qquad 10 = 2 \cdot 7 - 4. \quad |4| < |7|.$$

There are many other examples of Euclidean domains, of course.

Exercise A.5.7.

(a) Show that the ring $\mathbb{Z}[i]$ is a Euclidean domain when we endow it with the function $N\colon \mathbb{Z}[i] \setminus 0 \to \mathbb{N}_0$ such that $N(a + bi) = a^2 + b^2$ for all a and b in $\mathbb{Z}$.

(b) Show that the ring $\mathbb{Z}[\sqrt{D}]$ is a Euclidean domain for some Euclidean function when D is one of -2, -3, -7, and -11.

It is certainly not the case that for all square-free integers D the ring $\mathbb{Z}[\sqrt{D}]$ has a Euclidean function. We will see below, for example, that the ring $\mathbb{Z}[\sqrt{-5}]$ does not admit any Euclidean function . It is known that the only square-free values of D for which the function $z \in \mathbb{Z}[\sqrt{D}] \mapsto z\bar{z} \in \mathbb{N}_0$ is a Euclidean function are

$$-11,\ -7,\ -3,\ -2,\ -1,\ 2,\ 3,\ 5,\ 6,\ 7,\ 11,\ 13,\ 17,\ 19,\ 21,\ 29,\ 33,\ 37,\ 41,\ 57,\ 73.$$

This is the sequence A048981 in [OEI2026]; we refer to that database entry for more information about this.

Exercise A.5.8. Let (A, N) be a Euclidean domain. Show that the function

$$\tilde{N}\colon a \in A \setminus 0 \mapsto \min\{N(ab) : b \in A \setminus 0\} \in \mathbb{N}_0$$

is a Euclidean function on A such that $\tilde{N}(a) \leq \tilde{N}(ab)$ whenever a and b are non-zero elements of A.

The reason we are interested in Euclidean domains is that, as we hinted above, they allow us to give examples of principal ideal domains.

Proposition A.5.9. *A Euclidean domain is a principal ideal domain.*

Proof. Let A be a Euclidean domain with Euclidean function $N\colon A \setminus 0 \to \mathbb{N}_0$, and let I be an ideal of A. If $I = 0$, then $I = (0)$. Let us then suppose that $I \neq 0$, so that we may consider the number

$$d \coloneqq \min\{N(a) : a \in I \setminus 0\}$$

and choose an element x in I such that $N(x) = d$. We of course have that $(x) \subseteq I$. Let us show that we have an equality. Let a be a non-zero element of I. There are elements q and r of A such that $a = qx + r$ and either $r = 0$ or $N(r) < N(x)$, and we in fact have that $r = 0$, for otherwise $r = a - qx$ would be a non-zero element of I such that $N(r) < N(x) = d$, which is absurd. That r is zero means that $a = qx \in (x)$, and this allows us to conclude that $I \subseteq (x)$. □

One important consequence of this is, of course, the following one.

Corollary A.5.10. *The ring $\mathbb{Z}$ is a principal ideal domains and, in particular, Noetherian.*

Proof. According to Proposition A.5.4, the ring $\mathbb{Z}$ is Euclidean, so Proposition A.5.9 tells us that it is a principal ideal domain. □

From this we can obtain the following analogue of Corollary A.4.8.

Corollary A.5.11. *Every finitely generated ring is Noetherian.*

Proof. Let A be a finitely generated ring, and let $a_1, \ldots, a_n$ be elements of A such that the set $S = \{a_1, \ldots, a_n\}$ generates A. There is a unique morphism of $\mathbb{Z}$-algebras $\phi\colon \mathbb{Z}[x_1, \ldots, x_n] \to A$ such that $\phi(x_i) = a_i$ for each i in $[\![n]\!]$ and, since the image of ϕ is a subring of A that contains the set S, it is a surjective map. The morphism of rings $\bar{\phi}\colon \mathbb{Z}[x_1, \ldots, x_n]/\ker\phi \to A$ induced by ϕ is therefore an isomorphism. Since $\mathbb{Z}$ is a Noetherian ring, so is the ring $\mathbb{Z}[x_1, \ldots, x_n]$ according to Corollary A.4.5 and its quotient $\mathbb{Z}[x_1, \ldots, x_n]/\ker\phi$ according to Proposition A.4.7. The ring A is therefore Noetherian, as we want. □

It is not true that all principal ideal domains are Euclidean, but it is not easy to show this. The most classical example is the ring

$$\mathcal{O}_{\mathbb{Q}(\sqrt{-19})} \coloneqq \left\{ \frac{a + b\sqrt{-19}}{2} : a, b \in \mathbb{Z}, a^2 + b^2 \not\equiv 1 \mod 4 \right\}. \tag{A.6}$$

This was proved by Theodore Motzkin in [Mot1949], and it is, in fact, the first example that was found of this. The argument is based on a non-trivial amount of algebraic number theory; one can find modern and streamlined expositions in the articles [Wil1973] and [Cám1988] of Jack Wilson

and Oscar Cámpoli, respectively. A much simpler example is the quotient ring

$$\mathbb{R}[x, y]/(x^2 + y^2 + 1).$$

Pierre Samuel proved in [Sam1963] that this ring is a unique factorization domain, and starting from that one can show that it is a principal ideal domain. On the other hand, some arithmetical considerations show that this ring is not Euclidean. The reader can find the details of this in Nicolás Allo-Gómez's article [AG2026].

A.6. Unique factorization domains

In this section we seek to extend the extremely useful *Fundamental Theorem of Arithmetic*, that describes how we can *build* all integers from prime numbers, to more general commutative rings.

Definition A.6.1. Let A be an integral domain.

- An element a of A is ***associated*** to another element b of A if there is a unit u of A such that $a = ub$, and in that case we write $a \sim b$.
- An element a of A is ***irreducible*** if it is not zero, not a unit, and whenever b and c are elements of A such that $a = bc$ one of the two is a unit.
- An element a of A is ***prime*** if it is not zero, not a unit, and whenever a divides the product cd of two elements of A it divides one of the factors.

One should notice that an element a of A is prime exactly when the principal ideal (a) of A that it generates is prime.

Exercise A.6.2. Let A be an integral domain.

(a) Show that the relation $\sim$ of association is an equivalence relation on A.

(b) Let a and b be two elements of A. Prove that $a \sim b$ if and only if a divides b and b divides a.

(c) Let a and b be two elements of A such that $a \sim b$. Show that if a is irreducible, then so is b, and that if a is prime, then so is b.

Exercise A.6.3. Let A be an integral domain, and let p and q be two irreducible elements of A. Show that if p divides q, then p is associated to q.

Primality and irreducibility are very close concepts, as the following lemma shows.

Lemma A.6.4. *Let A be an integral domain.*

(i) Every prime element of A is irreducible.

(ii) If A is a principal ideal domain, then every irreducible element of A is prime.

Since $\mathbb{Z}$ is a principal ideal domain, this tells us that irreducible integers are prime: this result is known as *Euclid's Lemma*, because it appears first in Euclid's *Elements* as Proposition 30 of Book VII.

Proof. (*i*) Let A be an integral domain, let p be a prime element of A, and let us suppose that a and b are two elements of A such that $p = ab$. Since p divides ab and is prime, it divides one of the two factors, and we can suppose without loss of generality that it divides a. In that case there is an element c in A such that $a = pc$, and thus $p(1 - bc) = 0$ and, since $p \neq 0$, we see that b is a unit. This shows that p is irreducible.

(*ii*) Let us suppose now that A is a principal ideal domain, and let p be an irreducible element of A. In order to show that p is a prime element, it is enough that we show that the ideal (p) is prime, and for that, that that ideal is maximal. Let then I be a proper ideal of A such that $(p) \subseteq I$. As A is a principal ideal domain and I is proper, there is an element a of A that is not a unit and such that $I = (a)$. As $p \in I$, there is an element b in A such that $p = ab$, and since p is irreducible and a is not a unit, this element b is a unit, so that $I = (a) = (b^{-1}p) = (p)$. This proves that the ideal (p) is maximal, as we want. □

In general, domains have irreducible elements that are not prime, as the following classical example shows.

Example A.6.5. Let us consider the domain $A = \mathbb{Z}[\sqrt{-5}]$. If z is an element of A, then there are integers a and b such that $z = a + b\sqrt{-5}$ and thus $z\overline{z} = a^2 + 5b^2$ is an element of $\mathbb{Z}$. It follows from this that there is a function $v\colon z \in A \mapsto z\overline{z} \in \mathbb{Z}$, and it is easy to check that whenever z and w are elements of A we have that $v(zw) = v(z)v(w)$.

The element 3 of A is irreducible. Indeed, let us suppose that $z = a + b\sqrt{-5}$ and $w = c + d\sqrt{-5}$, with a, b, c, and d in $\mathbb{Z}$, are such that $3 = zw$. We then have that

$$3^2 = v(3) = v(z)v(w) = (a^2 + 5b^2)(c^2 + 5d^2).$$

Both factors in this last product are positive and it is easy to check that neither of them can be equal to 3: this implies that one of them is equal to 1. If, for example, $a^2 + 5b^2 = 1$, then we in fact have that $b = 0$ so that z is either 1 or -1, and thus a unit of A. This proves that 3 is irreducible, as we said. On the other hand, the number 3 divides $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 3^2$ while it clearly divides neither $2 + \sqrt{-5}$ nor $2 - \sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$, so that it is not a prime element of A.

Let us notice that this implies that the ring $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain.

Exercise A.6.6. Show that the ideal $\langle 2, 1 + \sqrt{-5}\rangle$ of the ring $\mathbb{Z}[\sqrt{-5}]$ is not principal.

This section is devoted to the study of rings all of whose elements can be obtained in essentially one way from the irreducible elements. The following definition makes this precise.

Definition A.6.7. A ring A is a ***unique factorization domain*** if it is an integral domain and the following conditions hold:

- If a is a non-zero element of A that is not a unit, then there exist a positive integer n and irreducible elements $p_1, \ldots, p_n$ of A such that $a = p_1 \cdots p_n$.
- If m and n are two positive integers and $p_1, \ldots, p_m$ and $q_1, \ldots, q_n$ are irreducible elements of A such that $p_1 \cdots p_m \sim q_1 \cdots q_n$, then $m = n$ and there is a bijective function $\sigma : [\![n]\!] \to [\![n]\!]$ such that $p_i \sim q_{\sigma(i)}$ for each i in $[\![n]\!]$.

The following two lemmas give useful consequences of the conditions that appear in this definition. The first one will allow us to deal with the form of uniqueness of factorizations given by the first of those conditions in a convenient form.

Lemma A.6.8. *Let A be a unique factorization domain, let n be a positive integer, and let $p_1, \ldots, p_n$ be irreducible elements of A no two of which are associated. If $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are non-negative integers such that $p_1^{a_1} \cdots p_n^{a_n} \sim p_1^{b_1} \cdots p_n^{b_n}$, then in fact $a_i = b_i$ for each i in $[\![n]\!]$.*

Proof. Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be non-negative integers such that $p_1^{a_1} \cdots p_n^{a_n} \sim p_1^{b_1} \cdots p_n^{b_n}$, and let us suppose that there is an element j in $[\![n]\!]$ such that $a_j \neq b_j$. Without loss of generality, we can suppose that we in fact have that $a_j > b_j$. Since

$$p_1^{a_1} \cdots p_{j-1}^{a_{j-1}} p_j^{b_j + (a_j - b_j)} p_{j+1}^{a_{j+1}} \cdots p_n^{a_n} = p_1^{a_1} \cdots p_n^{a_n} \sim p_1^{b_1} \cdots p_n^{b_n}$$

and A is an integral domain, we have that

$$p_j \mid p_1^{a_1} \cdots p_{j-1}^{a_{j-1}} p_j^{a_j - b_j} p_{j+1}^{a_{j+1}} \cdots p_n^{a_n} \sim p_1^{b_1} \cdots p_{j-1}^{b_{j-1}} p_{j+1}^{b_{j+1}} \cdots p_n^{b_n}. \tag{A.7}$$

Since A is a unique factorization domain and p_j is an irreducible element of A, we know from Proposition A.6.13 that p_j is a prime element, and therefore, in view of (A.7), that there is an element k in $[\![n]\!] \setminus \{j\}$ such that p_j divides p_k and, according to the result of Exercise A.6.3, we have that $p_j \sim p_k$. This is absurd, because by hypothesis p_j and p_k are not associated since $j \neq k$, and this contradiction proves the lemma. □

In fact, a little more is true.

Exercise A.6.9. Let A be a unique factorization domain, let n be a positive integer, and let $p_1, \ldots, p_n$ be irreducible elements of A no two of which are associated. Prove that if $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are integers such that in the fraction field of A we have $p_1^{a_1} \cdots p_n^{a_n} = q_1^{b_1} \cdots q_n^{b_n}$, then $a_i = b_i$ for each i in $[\![n]\!]$.

If we choose representatives for the association classes of irreducible elements in our ring,

then among the many factorizations of each element of the ring we can single out one, and then several things become easier to deal with. Our second lemma explains this.

Lemma A.6.10. *Let A be a unique factorization domain.*

(*i*) *There is a subset $\mathscr{I}$ of A whose elements are all irreducible and such that every irreducible element of A is associated to exactly one element of $\mathscr{I}$. In particular, no two different elements of $\mathscr{I}$ are associated.*

Let us fix one such set $\mathscr{I}$.

(*ii*) *If p and q are elements of $\mathscr{I}$ and p divides q, then in fact we have that $p = q$.*

(*iii*) *For each non-zero element a of A there exist a unit c_a in A and a function $\varepsilon_a \colon \mathscr{I} \to \mathbb{N}_0$ such that the set $I_a \coloneqq \{p \in \mathscr{I} : \varepsilon_a(p) > 0\}$ is finite and $a = c_a \prod_{p \in I_a} p^{\varepsilon_a(p)}$. Moreover, if c is a unit of A and $\varepsilon \colon \mathscr{I} \to \mathbb{N}_0$ is a function such that the set $I \coloneqq \{p \in \mathscr{I} : \varepsilon(p) > 0\}$ is finite and we have that $a = c \prod_{p \in I} p^{\varepsilon(p)}$, then $c = c_a$ and $\varepsilon = \varepsilon_a$.*

(*iv*) *A non-zero element a of A divides another non-zero element b of A if and only if $\varepsilon_a(p) \leq \varepsilon_b(p)$ for all p in $\mathscr{I}$.*

(*v*) *Two non-zero elements a and b of A are associated if and only if $\varepsilon_a(p) = \varepsilon_b(p)$ for all p in $\mathscr{I}$.*

Proof. (*i*) Let R be the set of all irreducible elements of A and let $\pi \coloneqq R \to R/\!\sim$ is the canonical projection from R to the set of equivalence classes for the relation of association on R. As this function is surjective, the *Axiom of Choice* tells us that there is a function $\sigma \colon R/\!\sim \to R$ such that $\pi \circ \sigma = \mathsf{id}_{R/\sim}$. We put $\mathscr{I} \coloneqq \sigma(R/\!\sim)$. The elements of this set $\mathscr{I}$ are of course all irreducible, and if p is an irreducible element of A, then $\sigma(\pi(p))$ is the unique element of $\mathscr{I}$ that is associated to p.

(*ii*) If p and q are elements of $\mathscr{I}$ and there is an element a of A such that $q = ap$, then the irreducibility of q and the fact that p is not a unit imply together that a is a unit, so that $p \sim q$, and this allows us to conclude that, in fact, $p = q$.

(*iii*) Let a be a non-zero element of A. As A is a unique factorization domain, there exist a unit c in A, a non-negative integer k, and irreducible elements $q_1, \ldots, q_k$ in A such that $a = cq_1 \cdots q_k$. The way we chose the set $\mathscr{I}$ implies that for each i in $[\![k]\!]$ there is exactly one element p_i in $\mathscr{I}$ such that $q_i \sim p_i$, and there is therefore a unit c_i in A such that $q_i = c_i p_i$. Let us consider the function $\varepsilon_a \colon \mathscr{I} \to \mathbb{N}_0$ that on each element p of $\mathscr{I}$ takes the value

$$\varepsilon_a(p) = |\{i \in [\![k]\!] : q_i \sim p\}|.$$

The set $I_a \coloneqq \{p \in \mathscr{I} : \varepsilon_a(p) > 0\}$ is clearly contained in $\{p_1, \ldots, p_k\}$, so it is finite, and for each p in the set I_a we have that $\varepsilon_a(p) = |\{i \in [\![k]\!] : p = p_i\}|$. It follows from this that

$$a = c \prod_{i=1}^{k} q_i = c \prod_{i=1}^{k} c_i p_i = \left(c \prod_{i=1}^{k} c_i \right) \prod_{i=1}^{k} p_i = \left(c \prod_{i=1}^{k} c_i \right) \prod_{p \in I_a} p^{\varepsilon_a(p)},$$

so if we put $c_a \coloneqq c\prod_{i=1}^{k} c_i$ we see that the existence claim of (*iii*) holds.

Let now c be a unit of A, let $\varepsilon\colon \mathscr{I} \to \mathbb{N}_0$ be a function, and let us suppose that the set $I \coloneqq \{p \in \mathscr{I} : \varepsilon(p) > 0\}$ is finite and that we have that $a = c\prod_{p\in I} p^{\varepsilon(p)}$.

We have that $I_a \subseteq I$. To verify this, let q be an element of I_a, so that $\varepsilon_a(q) > 0$. This implies that q divides the product $c_a \prod_{p\in I_a} p^{\varepsilon_a(p)}$, which is equal to a, so that it also divides the product $c\prod_{p\in I} p^{\varepsilon(p)}$, because it is also equal to a. Since q is irreducible and A is a unique factorization domain, Proposition A.6.13 tells us that q is prime, and that it therefore divides one of the factors in this last product. As c is a unit, it is not divisible by q, so there is an element r of I such that q divides $r^{\varepsilon(r)}$: it follows from this that $\varepsilon(r) > 0$, of course, for q cannot divide a unit, and then the primality of q implies that q divides r itself, so that in fact $q = r \in I$.

By symmetry, of course, we also have that $I \subseteq I_a$, so that $I_a = I$. This implies that we have

$$c_a \prod_{p\in I_a} p^{\varepsilon_a(p)} = a = c\prod_{p\in I_a} p^{\varepsilon(p)}, \tag{A.8}$$

so that

$$\prod_{p\in I_a} p^{\varepsilon_a(p)} \sim \prod_{p\in I} p^{\varepsilon(p)},$$

It follows now from Lemma A.6.8 that $\varepsilon = \varepsilon_a$, and, in view of (A.8), that also $c = c_a$. This proves the uniqueness claim of (*iii*).

(*iv*) Let a and b be two non-zero elements of A. If we have that $\varepsilon_a(p) \le \varepsilon_b(p)$ for all p in $\mathscr{I}$, then we have that $I_a \subseteq I_b$ and that therefore

$$\begin{aligned} b &= c_b \prod_{p\in I_b} p^{\varepsilon_b(p)} = c_b \prod_{p\in I_b\setminus I_a} p^{\varepsilon_b(p)} \prod_{p\in I_a} p^{\varepsilon_b(p)-\varepsilon_a(p)} \prod_{p\in I_a} p^{\varepsilon_a(p)} \\ &= c_b c_a^{-1} \prod_{p\in I_b\setminus I_a} p^{\varepsilon_b(p)} \prod_{p\in I_a} p^{\varepsilon_b(p)-\varepsilon_a(p)} \cdot a, \end{aligned}$$

so that a divides b.

To prove the converse implication, we suppose that a divides b and prove that $\varepsilon_a(p) \le \varepsilon_b(p)$ for all p in $\mathscr{I}$ proceeding by induction with respect to the non-negative integer $\mu(a) \coloneqq \sum_{p\in I_a} \varepsilon_a(p)$. If this number is 0, then we in fact have that $\varepsilon_a(p) = 0 \le \varepsilon_b(p)$ for all p, so what we want is true in that case. Let us the suppose that $\mu(a)$ is positive, so that there is an element q of $\mathscr{I}$ such that $\varepsilon_a(q) > 0$ and thus $q \in I_a$. We then have that

$$q \mid c_a \prod_{p\in I_a} p^{\varepsilon_a(p)} = a \mid b = c_b \prod_{p\in I_b} p^{\varepsilon_b(p)}.$$

Since q is irreducible in A and A is a unique factorization domain, q is prime, and therefore this divisibility relation and the fact that c_b is a unit imply that q divides an element of I_b, so that it is in

fact an element of I_b because of the way we chose the set $\mathscr{I}$. This tells us that there are functions $\bar{\varepsilon}_a, \bar{\varepsilon}_b \colon \mathscr{I} \to \mathbb{N}_0$ that on each element p of $\mathscr{I}$ take the values

$$\bar{\varepsilon}_a(p) = \begin{cases} \varepsilon_a(q) - 1 & \text{if } p = q; \\ \varepsilon_a(p) & \text{if } p \neq q; \end{cases} \qquad \bar{\varepsilon}_b(p) = \begin{cases} \varepsilon_b(q) - 1 & \text{if } p = q; \\ \varepsilon_b(p) & \text{if } p \neq q; \end{cases}$$

and the elements $\bar{a} \coloneqq c_a \prod_{p \in I_a} p^{\bar{\varepsilon}_a(p)}$ and $\bar{b} \coloneqq c_b \prod_{p \in I_b} p^{\bar{\varepsilon}_b(p)}$ of A. The uniqueness claim of part (*iii*) of the lemma implies that $\varepsilon_{\bar{a}} = \bar{\varepsilon}_a$ and $\varepsilon_{\bar{b}} = \bar{\varepsilon}_b$. We have that $\bar{a}q = a \mid b = \bar{b}q$, so that $\bar{a} \mid \bar{b}$, and since clearly $I_{\bar{a}} \subseteq I_a$ that also

$$\mu(\bar{a}) = \sum_{p \in I_{\bar{a}}} \varepsilon_{\bar{a}} = \sum_{p \in I_a} \bar{\varepsilon}_a = \sum_{p \in I_a} \varepsilon_a - 1 < \sum_{p \in I_a} \varepsilon_a = \mu(a).$$

The inductive hypothesis then allows us to conclude that $\varepsilon_{\bar{a}}(p) \leq \varepsilon_{\bar{b}}(p)$ for all p in $\mathscr{I}$, and, of course, this implies that $\varepsilon_a(p) \leq \varepsilon_b(p)$ for all p in $\mathscr{I}$, which is what we wanted to prove. This completes the induction.

(*v*) This follows immediately from (*iv*) and the fact that two elements of A are associated if they divide each other. □

The first condition in Definition A.6.7 is a rather weak one. For example, according to the first part of the following proposition it is satisfied by all Noetherian rings.

Proposition A.6.11. *Let A be an integral domain.*

(*i*) *If the set of principal ideals of A satisfies the ascending chain condition, then every non-zero and non-unit element of A is a product of irreducible elements.*

(*ii*) *If A is a unique factorization domain, then the set of principal ideals of A satisfies the ascending chain condition.*

Proof. (*i*) Let us suppose that the set of principal ideals of A satisfies the ascending chain condition, and let us say that a non-zero and non-unit element a of A is *factorizable* if there exist a positive integer n and irreducible elements $p_1, \ldots, p_n$ in A such that $a = p_1 \cdots p_n$. It is clear that the irreducible elements of A are factorizable, and that the product of two factorizable elements of A is itself factorizable. Let us write N for the set of all non-zero and non-unit elements of A that are *not* factorizable, and consider on it the relation

$$R \coloneqq \{(a, b) \in N \times N : b \mid a, a \nmid b\}.$$

Let a be an element of N. As a is not irreducible, there are non-zero and non-unit elements b and c in A such that $a = bc$ and, since a is not factorizable, one of b or c is also not factorizable, so we can suppose with loss of generality that b is in N. We have that $b \mid a$. If we also had that $a \mid b$, so that there is an element d in A such that $b = ad$, then we would have that $b(1 - cd) = 0$ and,

since $b \neq 0$, that $cd = 1$, which is absurd because c is not a unit. We thus see that $(a, b) \in R$.

This shows that for all a in N the set $\{b \in N : (a, b) \in R\}$ is not empty. Let us suppose now for a moment that the set N is not empty. The *Principle of Dependent Choice* implies then implies that there is a sequence $(a_i)_{i\geq 1}$ in N such that for each i in $\mathbb{N}$ we have $(a_i, a_{i+1}) \in R$ or, equivalently, that $a_{i+1} \mid a_i \nmid a_{i+1}$ for each i in $\mathbb{N}$. It follows from this that we have a strictly increasing chain of ideals

$$(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$$

This is absurd, as it contradicts our hypothesis on A, and this contradiction shows that the set N is empty. This means precisely that the first claim of the proposition is true.

(*ii*) Let us now suppose that the ring A is a unique factorization domain, and let $(a_i)_{i\geq 1}$ be a sequence of elements of A such that for each i in $\mathbb{N}$ we have that $\langle a_i \rangle \subseteq \langle a_{i+1} \rangle$. Let us choose a set $\mathscr{I}$ of irreducible elements of A as in the first part of Lemma A.6.10, and for each i in $\mathbb{N}$ let c_i be the unit of A and $\varepsilon_i \colon \mathscr{I} \to \mathbb{N}_0$ be the function such that the set $I_i \coloneqq \{p \in \mathscr{I} : \varepsilon_i(p) > 0\}$ is finite and $a_i = c_i \prod_{p\in I_i} p^{\varepsilon_i(p)}$, as in the thirds part of that lemma. For each i in $\mathbb{N}$ we have that $\langle a_i \rangle \subseteq \langle a_{i+1} \rangle$, so that a_{i+1} divides a_i and, according to the fourth part of the lemma, we therefore have that $\varepsilon_{i+1}(p) \leq \varepsilon_i(p)$ for all p in $\mathscr{I}$.

For each p in $\mathscr{I}$ the sequence $(\varepsilon_i(p))_{i\geq 1}$ is then a non-increasing sequence of non-negative integers, so there exists a positive integer N_p such that $\varepsilon_i(p) = \varepsilon_{N_p}(p)$ for all integers i such that $i \geq N_p$. Let us set $N \coloneqq \max\{N_p : p \in I_1\}$, and let i be an integer such that $i \geq N$. We have that $\varepsilon_i(p) = \varepsilon_N(p)$ for all p in the set $\mathscr{I}$ — if p is an element of I_1 this follows from the way we chose the number N, and if p is not in I_1 then this is because in that case $0 \leq \varepsilon_i(p) \leq \varepsilon_1(p) = 0$ — and therefore the elements a_i and a_N are associated according to the fifth part of the lemma and this the ideals $\langle a_i \rangle = \langle a_N \rangle$ are equal. This proves that the set of principal ideals of A satisfies the ascending chain condition. □

The second condition of Definition A.6.7 is interesting because we insist that the elements p_i and q_i that appear there be irreducible. The condition would becomes non-interesting if we only cared about factorizations into prime elements, as the next result shows.

Lemma A.6.12. *Let A be an integral domain, let m and n be two positive integers, let c be a unit of A, and let $p_1, \ldots, p_m$ be prime elements of A, and let $q_1, \ldots, q_n$ be irreducible elements of A such that $p_1 \cdots p_m = c q_1 \cdots q_n$. We have that $m = n$ and there is a bijective function $\sigma \colon [\![m]\!] \to [\![n]\!]$ such that $p_i \sim q_{\sigma(i)}$ for each i in $[\![m]\!]$.*

Proof. We will prove the lemma proceeding by induction with respect to the integer m. Since p_1 divides the product $c q_1 \cdots q_n$ and is prime and c is a unit, there is an element j in $[\![n]\!]$ such that p_1 divides q_j, so there is an element d in A such that $q_j = d p_1$: as q_j is irreducible and p_1 is not a unit,

this d is a unit and therefore $p_1 \sim q_j$.

Let us suppose for a moment that m is 1. We then have that

$$p_1 = cq_1 \cdots q_n = cq_1 \cdots q_{j-1} d p_1 q_{j+1} \cdots q_n$$

and thus, since A is a domain, that $1 = cq_1 \cdots q_{j-1} d q_{j+1} \cdots q_n$. This tells us that each of the $n-1$ elements $q_1, \ldots, q_{j-1}, q_{j+1}, \ldots, q_n$ is a unit in A: as they are also irreducible, we see that in fact $n = 1$. This implies that $j = 1$ and that the unique function $\sigma\colon [\![m]\!] \to [\![n]\!]$, which has $\sigma(1) = 1$, is a bijection such that $p_i \sim q_{\sigma(i)}$ for each i in $[\![m]\!]$. This starts our induction.

To complete it, let us now suppose that m is greater than 1. As $q_j = dp_1$, we have that

$$p_1 \cdots p_m = cq_1 \cdots q_n = cq_1 \cdots q_{j-1} d p_1 q_{j+1} \cdots q_n$$

and, since A is a domain, that in fact

$$p_2 \cdots p_m = cdq_1 \cdots q_{j-1} q_{j+1} \cdots q_n.$$

The obvious inductive hypothesis then tells us that $m - 1 = n - 1$, so that $m = n$, and that there is a bijective function function $\tau\colon [\![2, m]\!] \to [\![n]\!] \setminus \{j\}$ such that $p_i \sim q_{\tau(i)}$ for each i in $[\![2, m]\!]$. The function $\sigma\colon [\![m]\!] \to [\![n]\!]$ that on each element i of $[\![m]\!]$ takes the value

$$\sigma(i) = \begin{cases} j & \text{if } i = 1; \\ \tau(i) & \text{if } i \geq 2; \end{cases}$$

is then also bijective, and we have that $p_i \sim q_{\sigma(i)}$ for each i in $[\![m]\!]$. This completes the induction and thus the proof of the lemma. □

Proving that a ring is a unique factorization domain is usually difficult when using the definition directly. The following result gives two alternate criteria that are often helpful.

Proposition A.6.13. *Let A be an integral domain. The following statements are equivalent:*

(*a*) *A is a unique factorization domain.*

(*b*) *Every non-zero and non-unit element of A is a product of irreducible elements, and every irreducible element of A is prime.*

(*c*) *Every non-zero and non-unit element of A is a product of prime elements.*

Proof. (*a*) ⇒ (*b*) Let us suppose that A is a unique factorization. Every non-zero and non-unit element of A is therefore a product of irreducible elements, and we need to show that every irreducible element of A is prime.

Let then p be an irreducible element of A, and let a and b be two elements of A such that p divides ab, so that there is another element c in A such that $ab = pc$. Since A is a unique

factorization domain, there are units u, v and w of A, non-negative integers m, n, and k, and irreducible elements $a_1, \ldots, a_m$, $b_1, \ldots, b_n$, and $c_1, \ldots, c_k$ in A such that $a = ua_1 \cdots a_m$, $b = vb_1 \cdots b_n$, and $c = wc_1 \cdots c_k$. We have that $uva_1 \cdots a_m b_1 \cdots b_n = wpc_1 \cdots c_k$ and, since p is irreducible and A is a unique factorization domain, p is prime and thus divides one of the factors appearing on the left of the last equality. It does not divide u or v, for these are units, so it divides one of the elements $a_1, \ldots, a_m, b_1, \ldots, b_n$, and thus also one of a or b. We see with this that p is prime in A.

$(b) \Rightarrow (c)$ Since irreducible elements are prime, this is clear.

$(c) \Rightarrow (a)$ Let us suppose that every non-zero and non-unit element of A is a product of prime elements. Since prime elements are irreducible, this implies that the ring A satisfies the first condition of Definition A.6.7. Let us show now that it also satisfies the second one.

Let m and n be two positive integers, and let $p_1, \ldots, p_m$ and $q_1, \ldots, q_n$ be irreducible elements of A such that $p_1 \cdots p_m \sim q_1 \cdots q_n$, so that there is a unit c in A such that $p_1 \cdots p_m = cq_1 \cdots q_n$. Since we are assuming that the statement (c) holds, there a positive integer k and prime elements $r_1, \ldots, r_k$ in A such that $r_1 \cdots r_k = p_1 \cdots p_m$, and it follows from Lemma A.6.12 that in fact $k = m$ and that there is a bijection $\sigma_1 \colon [\![k]\!] \to [\![m]\!]$ such that $r_i \sim p_{\sigma_1(i)}$ for each i in $[\![k]\!]$.

We also have that $r_1 \cdots r_k = cq_1 \cdots q_n$, so again according to that lemma we have that $k = n$, and that there is a bijection $\sigma_2 \colon [\![k]\!] \to [\![n]\!]$ such that $r_i \sim q_{\sigma_2(i)}$ for each i in $[\![k]\!]$. It follows immediately form this that $m = n$ and that the function $\sigma \coloneqq \sigma_2 \circ \sigma_1^{-1} \colon [\![m]\!] \to [\![n]\!]$ is such that $p_i \sim q_{\sigma(i)}$ for each i in $[\![n]\!]$. This completes the proof of the proposition. □

An application of the criterion of Proposition A.6.13 is the following important result.

Proposition A.6.14. *A principal ideal domain is a unique factorization domain.*

Proof. A principal ideal domain is a Noetherian ring in which irreducible elements are prime, so, according to Proposition A.6.13 and A.6.11, also a unique factorization domain. □

Proposition A.6.14 has as a special case the *Fundamental Theorem of Arithmetic*. Indeed, this is what unique factorization amounts to for the ring $\mathbb{Z}$, since its irreducible elements are the prime numbers and their opposites, and its only units are 1 and −1. It is interesting to note that while the existence claim of this theorem follows from results that are in Euclid's *Elements*, it was first stated and proved by Kamāl al-Dīn al-Fārisī, who died around 1320. On the other hand, the uniqueness claim of the theorem was first stated and proved in detail by Carl Friedrich Gauss in the Article 16 of his *Disquisitiones Arithmeticae*. The long and interesting story of this theorem is told in the article [AÖ2001] of Ahmet Göksel Ağargün and Erdoğan Mehmet Özkan.

Proposition A.6.14 also allows us to conclude that the ring $\mathbb{k}[x]$ of polynomials over a field $\mathbb{k}$ is a unique factorization domain, since that ring is Euclidean according to Proposition A.5.5 and therefore a principal ideal domain because of Proposition A.5.9. Our next objective is to generalize this: we want to prove the imporant fact that the ring $A[x_1, \ldots, x_n]$ is a unique factorization

domain whenever A is a unique factorization domain and n is any non-negative integer. In fact, we will give two different proofs of this, the first one based on ideas of Masayoshi Nagata and the second one due to Carl Friedrich Gauss.

The first step towards Nagata's proof is to establish a new criterion for factoriality. To do that we need the following extremely useful observation, due to Wolfgang Krull [Kru1928] and often called *Krull's Separation Lemma*.

Lemma A.6.15. *Let A be an integral domain, let S be a non-empty multiplicatively closed subset of A, and let I be an ideal of A that is disjoint from S. There is then an ideal P of A that is maximal among those that contain I and are disjoint from S, it is prime, and the ideal P_S is maximal in the localization A_S.*

Proof. Let $\mathscr{P}$ be the set of all ideals of A that contain I and are disjoint from S. This set is not empty, as it contains I itself. Let us show that it satisfies the hypothesis of *Zorn's Lemma*.

Let $\mathscr{C}$ be a non-empty subset of $\mathscr{P}$ that is totally ordered with respect to inclusion, and let $\bigcup\mathscr{C}$ be the union of its elements, which clearly contains I and is disjoint from S. We claim that $\bigcup\mathscr{C}$ is an ideal of A.

- As $\mathscr{C}$ is not empty, and each of its elements is not empty, the set $\bigcup\mathscr{C}$ is also not empty.
- If a and b are elements of $\bigcup\mathscr{C}$, then there are elements C_1 and C_2 of $\mathscr{C}$ such that $a \in C_1$ and $b \in C_2$ and, since $\mathscr{C}$ is totally ordered, we have that $C_1 \cup C_2 \in \mathscr{C}$, so that $a - b \in C_1 \cup C_2 \subseteq \bigcup\mathscr{C}$, since $C_1 \cup C_2$ is an ideal of A.
- Finally, if a and b are an element of A and an element of $\bigcup\mathscr{C}$, respectively, then there is an element C of $\mathscr{C}$ such that $b \in C$ and, since C is an ideal of A, we have that $ab \in C \subseteq \bigcup\mathscr{C}$.

This and the fact that obviously I contains all the elements of $\mathscr{C}$ implies that I is an upper bound for the set $\mathscr{C}$ in $\mathscr{P}$. The ordered set $\mathscr{P}$ is thus inductive, as we want.

It follows now from *Zorn's Lemma* that the set $\mathscr{P}$ has a maximal element P. We will show now that this ideal P is prime, and thereby complete the proof of the lemma. Let a and b be two elements of A such that $ab \in P$ and, to reach a contradiction, let us suppose that $a \notin P$ and $b \notin P$. We then have that the ideals $P + \langle a \rangle$ and $P + \langle b \rangle$ contain I and strictly contain P, so that they do not belong to the set $\mathscr{P}$ and therefore intersect non-vacuously the set S. There are therefore elements u and v of P and x and y of A such that $u + ax \in S$ and $v + by \in S$. Since the set is multiplicatively closed, we then have that

$$uv + uby + axv + abxy = (u + ax)(v + by) \in S$$

This is absurd, as the four terms uv, uby, axv, and $abxy$ belong to P, yet $P \cap S = \varnothing$. This contradiction allows us to conclude that the ideal P is prime.

Let $\operatorname{Spec} A_S$, as usual, be the set of prime ideals of the ring A_S, and let us write $\operatorname{Spec}_S A$ for the set of prime ideals of A that are disjoint from S. If $\mathfrak{p}$ is an element of $\operatorname{Spec}_S A$, then $\mathfrak{p}A_S$ is an

element of Spec A, so there is a function

$$\phi\colon \mathfrak{p} \in \operatorname{Spec}_S A \mapsto \mathfrak{p}A_S \in \operatorname{Spec} A_S,$$

and it is, in fact, an inclusion-preserving bijection. The ideal P is a maximal element of the subset $\{\mathfrak{p} \in \operatorname{Spec}_S A : \mathfrak{p} \supseteq I\}$ of $\operatorname{Spec}_S A$, and therefore P_S is a maximal element of the subset

$$\{\mathfrak{p}A_S \in \operatorname{Spec} A_S : \mathfrak{p} \in \operatorname{Spec}_S A, \mathfrak{p} \supseteq I\}$$

of Spec A_S. Since the map ϕ is surjective, this tells us that, in fact, the localization P_S is a maximal element of Spec A_S, so a maximal ideal of A_S. □

Using this lemma, we can prove the following criterion for factoriality due to Irving Kaplansky [Kap1970, Theorem 5].

Proposition A.6.16. *An integral domain is a unique factorization domain if and only if every one of its proper non-zero prime ideals contains a prime element.*

Proof. Let A be an integral domain, let us suppose that A is a unique factorization domain, and let $\mathfrak{p}$ be a proper non-zero prime ideal of A. There is then a non-zero element x in $\mathfrak{p}$, and it is not a unit and, according to Proposition A.6.13, there are prime elements $p_1, \dots, p_n$ of A such that $x = p_1 \cdots p_n$. Since x is in $\mathfrak{p}$ and the ideal $\mathfrak{p}$ is prime, there is then an element i of $[\![n]\!]$ such that $p_i \in \mathfrak{p}$, and this shows that the condition in the proposition is necessary.

To prove it is also sufficient, let us suppose that every proper-non-zero prime ideal of A contains a prime element, and let S be the set of elements a of A such that there are a unit c in A, a non-negative integer n, and prime elements $p_1, \dots, p_n$ in A such that $a = cp_1 \cdots p_n$. Of course, this set S is multiplicatively closed. Let us show that it is also *saturated*, that is, that whenever a and b are elements of A we have that

$$ab \in S \implies a \in S.$$

Let then a and b be two elements of A such that ab is in S, so that there are a unit c in A, a non-negative integer n, and prime elements $p_1, \dots, p_n$ in A such that $ab = cp_1 \cdots p_n$. Let I be a subset of $[\![n]\!]$ such that the product $\prod_{i \in I} p_i$ divides b and of maximal cardinality, and let b' be the element of A such that $b = b' \prod_{i \in I} p_i$. Since A is an integral domain and $ab' \prod_{i \in I} p_i = ab = c \prod_{i=1}^{n} p_i$, we have that $ab' = c \prod_{i \in [\![n]\!] \setminus I} p_i$. Let now J be a subset of $[\![n]\!] \setminus I$ such that $\prod_{i \in J} p_i$ divides a and of maximal cardinality, and let a' be the element of A such that $a = a' \prod_{i \in J} p_i$. We have that $a'b' \prod_{i \in J} p_i = ab' = c \prod_{i \in [\![n]\!] \setminus I} p_i$, so that also

$$a'b' = c \prod_{i \in [\![n]\!] \setminus (I \cup J)} p_i. \tag{A.9}$$

If there is an element k in $[\![n]\!] \smallsetminus (I \cup J)$, then it divides one of a' or b', and then either $\prod_{i\in I\cup\{k\}} p_i$ divides b or $\prod_{i\in J\cup\{k\}} p_i$ divides a, and both possibilities cannot occur in view of the way we chose the sets I and J. This tells us that $I \cup J = [\![n]\!]$, and thus the equality (A.9) implies that a' is a unit of A and $a = a' \prod_{i\in J} p_i$ is an element of S.

The set S is contained in $A \smallsetminus 0$ and, in fact, it is equal to it. Indeed, let us suppose that there is a non-zero element a of A that is not in S. Since the multiplicatively closed subset S is saturated, it follows then that, in fact, the ideal $\langle a\rangle$ is disjoint from S, and Lemma A.6.15 tells us that there is a prime ideal $\mathfrak{p}$ of A such that $\mathfrak{p} \cap S = \varnothing$. This is absurd, since the hypothesis implies that there is in $\mathfrak{p}$ a prime element and that element belongs to S.

This contradiction allows us to conclude that $S = A \smallsetminus 0$, as we claimed. This means that every non-zero and non-unit element of A is a product of prime elements and, according to Proposition A.6.13, that A is a unique factorization domain. □

We can use this criterion to prove that the class of unique factorization domains is closed under localizations.

Proposition A.6.17. *Let A be a ring, and let S be a multiplicatively closed subset of A. If A is a unique factorization domain, then so is the localization A_S.*

Proof. Let us suppose that A is a unique factorization domain, and let us show that the localization A_S is a unique factorization domain using Kaplansky's criterion A.6.16. Let $\mathfrak{p}$ be a proper non-zero prime ideal of A_S, and let $\iota\colon A \to A_S$ be the canonical map to the localization. The preimage $\iota^{-1}(\mathfrak{p})$ is a proper non-zero prime ideal of A, so Proposition A.6.16 tells us that there is a prime element p of A in it. The element $p/1$ of A_S is then in $\mathfrak{p}$, and to complete the proof we will show that it is prime.

Let α and β be elements of A_S such that $p/1$ divides $\alpha\beta$. There are then elements a, b, and c of A and s, t, and u of S such that $\alpha = a/s$, $\beta = b/t$, and $p/1 \cdot c/u = \alpha\beta = a/s \cdot b/t$ in A_S, so that $pcst = abu$ in A. As p is prime, this tells us that p divides one of a, b, or u. It cannot divide u, though: were that the case, we would have an element u' in A such that $u = u'p$, and then $p/1 \cdot u'/u = 1$ in A_S, so that $p/1$ is a unit of A_S, and this is impossible because $p/1$ is in $\mathfrak{p}$ and the ideal $\mathfrak{p}$ of A_S is proper. Now, if it divides a, then there is an element a' in A such that $a = a'p$ and in A_S we have that $\alpha = a/s = a'/s \cdot p/1$, so that $p/1$ divides α; similarly, if p divides b then $p/1$ divides β. This shows that $p/1$ is prime in A_S, as we want. □

We have now all the tools that we need to prove Nagata's factoriality criterion. The following lemma contains the technical parts of its proof.

Lemma A.6.18. *Let A be an integral domain, let S be a multiplicatively closed subset of A generated by prime elements, and let x be an irreducible element of A.*

(*i*) *The image of x in the localization A_S is either irreducible or invertible.*
(*ii*) *The element x is prime in A if and only if its image in A_S is prime or invertible.*

Proof. (*i*) Let us suppose $x/1$ is not a unit of A_S, and that α and β are elements of A_S such that $x/1 = \alpha\beta$, and let a and b be elements of A and s and t elements of S such that $\alpha = a/s$ and $\beta = b/t$. There are prime elements $p_1, \ldots, p_n$ in A such that $st = p_1 \cdots p_n$ and we have that $stx = ab$ in A. Let I be a subset of $[\![n]\!]$ such that $\prod_{i\in I} p_i$ divides a of maximal cardinality, and let a' be the element of A such that $a = a' \prod_{i\in I} p_i$. Similarly, let J be a subset of $[\![n]\!] \smallsetminus I$ such that $\prod_{i\in J} p_i$ divides b of maximal cardinality, and let b' be the element of A such that $b = b' \prod_{i\in J} p_i$. We then have that

$$\prod_{i=1}^{n} p_i \cdot x = stx = ab = \prod_{i\in I} p_i \cdot a' \cdot \prod_{i\in J} p_i \cdot b'$$

and, since $I \cap J = \varnothing$, this implies that

$$\prod_{i\in[\![n]\!]\smallsetminus(I\cup J)} p_i \cdot x = a'b'.$$

We claim that $I \cup J = [\![n]\!]$. Indeed, if that is not the case and k is an element of $[\![n]\!] \smallsetminus (I \cup J)$, then the last equality tells us that the prime element p_k divides one of a' or b'. If p_k divides a', then $\prod_{i\in I\cup\{k\}} p_i$ divides a, and this is impossible because $I \cup \{k\}$ has one more element than I, and if instead p_k divides b', then $\prod_{i\in J\cup\{k\}} p_i$ divides b, and this is impossible because $J \cup \{k\}$ is contained in $[\![n]\!] \smallsetminus I$ and has one more element than J.

This proves that $x = a'b'$. As x is irreducible in A, one of a' or b' is a unit of A, and thus one of α or β is a unit of A_S. This shows that $x/1$ is irreducible in A_S.

(*ii*) Let us suppose that x is a prime element of A, so that the ideal $\langle x\rangle$ of A is prime and the quotient $A/\langle x\rangle$ is an integral domain. Let $\bar{S}$ be the image of S in this quotient. There is an isomorphism $A_S/xA_S \cong (A/\langle x\rangle)_{\bar{S}}$, and the ring $(A/\langle x\rangle)_{\bar{S}}$ is either zero or an integral domain: this tells us that x is either invertible or prime in A_S. This proves that the condition that appears in (*ii*) is necessary. We prove that it is also sufficient in two steps.

- Let us suppose first that $x/1$ is a unit of A_S, so that there is an element y in A and an element s in S such that $x \cdot y/s = 1/1$ in A_S or, equivalently, such that $xy = s$ in A. There are prime elements $p_1, \ldots, p_n$ of A such that $s = p_1 \cdots p_n$, and thus $xy = p_1 \cdots p_n$. Let I be a subset of $[\![n]\!]$ of maximal cardinality among those such that $\prod_{i\in I} p_i$ divides y, and let y' be the element of A such that $y = y' \prod_{i\in I} p_i$. Since $\prod_{i=1}^{n} p_i = xy = xy' \prod_{i\in I} p_i$, we have that $\prod_{i\in[\![n]\!]\smallsetminus I} p_i = xy'$. We cannot have that $I = [\![n]\!]$, for then this equality would tell us that x is a unit of A, and it is not, since it is irreducible. We can therefore choose an element j in $[\![n]\!] \smallsetminus I$. The prime p_j then divides xy', and it cannot divide y', for in that case the product $\prod_{i\in I\cup\{j\}} p_i$ would divide y, contradicting the maximality with which we chose the set I, so that p_j divides x. As x is irreducible, we in fact have that x is associated to p_j and is thus itself prime.

- Let us suppose now that $x/1$ is prime in A_S, and let a and b be two elements of A such that $x = ab$. As $x/1 = a/1 \cdot b/1$ in A_S, then $x/1$ divides one of $a/1$ or $b/1$ in A_S, and this means that there are an element c of A and an element s of S such that $x/1 \cdot c/s = a/1$ or $x/1 \cdot c/s = b/1$ in A_S or, equivalently, $xc = as$ or $xc = bs$ in A. Let us suppose, for example, that the first equality holds. Since s is in S, there are prime elements $p_1, \dots, p_n$ of A such that $s = p_1 \cdots p_n$.

  Let I be a subset of $[\![n]\!]$ such that $\prod_{i\in I} p_i$ divides c and that is of the maximal possible cardinality, and let c' be the element of A such that $c = c' \prod_{i\in I} p_i$. We then have that

$$xc' \prod_{i\in I} p_i = xc = as = a \prod_{i=1}^{n} p_i,$$

  so that $xc' = a \prod_{i\in[\![n]\!]\setminus I} p_i$. If the set $[\![n]\!]\setminus I$ is not empty, then we can choose an element j in it and we have that p_j divides xc': as p_j does not divide c', for otherwise the product $\prod_{i\in I\cup\{j\}} p_i$ divides c and the set $I \cup \{j\}$ strictly contains I, so p_j divides x and, since x is irreducible, is associated to it: this implies that x is prime. If instead the set $[\![n]\!] \setminus I$ is empty, then we have that $a = xc'$, so that a is divisible by x.

This completes the proof of the lemma. □

The following characterization of factoriality, originally given by Nagata in [Nag1957], is what we are after.

Proposition A.6.19. *Let A be an integral domain, and let S be a multiplicatively closed subset of A generated by prime elements. The ring A is a unique factorization domain if and only if*

- *every non-zero non-unit of A is a product of irreducible elements and*
- *the localization A_S is a unique factorization domain.*

Proof. Let us suppose that every non-zero non-unit of A is a product of irreducible elements and that A_S is a unique factorization domain, so that, according to Proposition A.6.13, every irreducible element of A_S is prime. In that case, if x is an irreducible element of A, then the first part of Lemma A.6.18 tells us that $x/1$ is either irreducible or invertible in A_S, so that either $x/1$ is prime or invertible in A_S, and, according to the second part of the same lemma, the element x is prime in A. This shows that every irreducible element of A is prime and, since we are assuming that every non-zero non-unit of A is a product of irreducible elements, we can conclude from Proposition A.6.13 that A is a unique factorization domain. The condition of the proposition is thus sufficient.

Let us suppose now that A is a unique factorization domain. Of course, every non-zero non-unit element of A is then a product of irreducible elements, and it follows from Proposition A.6.17 that A_S is a unique factorization domain. This shows that the condition of the proposition is also necessary. □

We can now make the key step in the proof that polynomial rings over unique factorization domains are themselves unique factorization domains.

Proposition A.6.20. *If A is a unique factorization domain, then so is the ring $A[x_1, \dots, x_n]$ for any non-negative integer n.*

Proof. Let A be a unique factorization domain. We will only prove that the ring $A[x]$ is a unique factorization domain. That more generally the $A[x_1, \dots, x_n]$ is a unique factorization domain for any non-negative integer n follows from this and a straightforward induction based on the fact that for any such integer there is an isomorphism $A[x_1, \dots, x_n][x] \to A[x_1, \dots, x_{n+1}]$.

We start by proving that

$$\textit{every non-zero and non-unit element of } A[x] \textit{ is a product of irreducible elements} \tag{A.10}$$

In view of Proposition A.6.11, to do that it is enough that we show that the set of principal ideals of $A[x]$ satisfies the ascending chain condition. Let $(I_i)_{i\geq 1}$ be a sequence of principal ideals of $A[x]$ such that for each i in $\mathbb{N}$ we have $I_i \subseteq I_{i+1}$. We need to show that there is a positive integer N such that $I_{i+1} = I_i$ for all integers i such that $i \geq N$. This is obvious if $I_i = 0$ for all i in $\mathbb{N}$, for in that case we can simply take $N = 1$, so we may suppose that there is an i_0 in $\mathbb{N}$ such that $I_{i_0} \neq 0$. Of course, this implies that $I_i \neq 0$ for all integers i such that $i \geq i_0$, too.

Let us choose, for each integer i such that $i \geq i_0$, a non-zero element f_i of $A[x]$ such that $I_i = \langle f_i \rangle$. For each integer i such that $i \geq i_0$ we then have that $\langle f_i \rangle = I_i \subseteq I_{i+1} = \langle f_{i+1} \rangle$, so that f_{i+1} divides f_i and, in particular, $\deg f_{i+1} \leq \deg f_i$. The sequence of non-negative integers $(\deg f_i)_{i\geq i_0}$ is therefore non-increasing and there is a positive integer M such that $M \geq i_0$ and $\deg f_i = \deg f_M$ for all integers i such that $i \geq M$.

For each integer i such that $i \geq M$ let a_i be the leading coefficient of the polynomial f_i. If i is an integer such that $i \geq M$, then we have both $\langle f_i \rangle \subseteq \langle f_{i+1} \rangle$, so that f_{i+1} divides f_i, and $\deg f_{i+1} = \deg f_M = \deg f_i$, so there is an element b_i in A such that $f_i = b_i f_{i+1}$ and thus $a_i = b_i a_{i+1}$. This tells us that we have an increasing chain of principal ideals

$$\langle a_M \rangle \subseteq \langle a_{M+1} \rangle \subseteq \langle a_{M+2} \rangle \subseteq \langle a_{M+3} \rangle \subseteq \cdots$$

As A is a unique factorization domain, Proposition A.6.11 tells us that the set of principal ideals of A satisfies the ascending chain condition, and there is therefore an integer N such that $N \geq M$ and $\langle a_i \rangle = \langle a_N \rangle$ for each integer i such that $i \geq N$. This number N satisfies the condition that we want: if i is an integer such that $i \geq N$, then we have $\langle a_i \rangle = \langle a_N \rangle = \langle a_{i+1} \rangle$ and $a_i = b_i a_{i+1}$, so the element b_i is a unit of A and thus $I_{i+1} = \langle f_{i+1} \rangle = \langle b_i f_{i+1} \rangle = \langle f_i \rangle = I_i$.

Let now S be the multiplicatively closed subset of A generated by the prime elements of A. As A is a unique factorization domain, we have that every irreducible element of A is prime and that every element of A is associated to a product of irreducible elements, and this implies at once that

the localization A_S is the fraction field F of A. Each prime element of A is prime in $A[x]$, so when we view S as a subset of $A[x]$ it is a multiplicatively closed subset generated by prime elements. Moreover, the localization $A[x]_S$ clearly coincides with $A_S[x] = F[x]$ and is therefore a unique factorization domain because F is a field. In view of this and (A.10), we can conclude, thanks to Nagata's factoriality criterion A.6.19, that the ring $A[x]$ is a unique factorization domain. □

A.7. Greatest common divisors

One of the reasons that underlie our interest in unique factorization domains is that in them we have a good notion of *greatest common divisor*.

Definition A.7.1. Let A be an integral domain, and let S be a subset of A. We say that an element d of A is a ***greatest common divisor*** of S if

- d divides all the elements of S, and
- d is divisible by any element of A that divides all elements of S.

We write $\gcd S$ for the set of all greatest common divisors of S.

In general, a set that has a greatest common divisor has many, but they are all related in a simple way, as the result of the following exercise shows.

Exercise A.7.2. Show that if a subset S of a domain A admits a greatest common divisor, then the set $\gcd S$ of all its greatest common divisors is in fact an equivalence class for the relation of association.

In general, we are interested mostly in finding greatest common divisors for *finite* sets of elements of integral domains. There are integral domains in which this is not possible, though.

Example A.7.3. Let us consider the ring $A \coloneqq \mathbb{Z}[\sqrt{-3}]$, and the *norm* function $N\colon z \in A \mapsto z\overline{z} \in \mathbb{N}_0$, which has the property that

$$N(xy) = N(x)N(y) \text{ for all choices of } x \text{ and } y \text{ in } A.$$

If u is a unit of A, and a and b are the integers such $u = a + b\sqrt{-3}$, then we have that

$$1 = N(1) = N(u \cdot u^{-1}) = N(u) \cdot N(u^{-1}),$$

so that the integer $N(u) = a^2 + 3b^2$ divides 1, and thus $a \in \{\pm 1\}$ and $b = 0$. This tells us that the units of A are 1 and -1. On the other hand, we have that

$$\text{if } u \text{ and } v \text{ are elements of } A \text{ such that } u \text{ divides } v \text{ and } N(u) = N(v), \text{ then } u \sim v.$$

Indeed, in that situation there is an element w in A such that $uw = v$ and thus $N(u)N(w) = N(v)$, so that $N(w) = 1$ and therefore w is a unit of A.

Let us now consider the subset $S \coloneqq \{4, 2 + 2\sqrt{-3}\}$ of A. Since

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}), \qquad 2 + 2\sqrt{-3} = 2 \cdot (1 + \sqrt{-3}),$$

we see that 2 and $1 + \sqrt{-3}$ are common divisors of the elements of S. We will show below that they are in fact *maximal* common divisors, in the sense that every common divisor of the elements of S that is divisible by 2 is associated to it, and every common divisor of the elements of S that is divisible by $1 + \sqrt{-3}$ is associated to it. Since they are not associated to each other, this implies that the set S does not have a greatest common divisor.

First, let us note that 4 does not divide $2 + 2\sqrt{-3}$ and that $2 + 2\sqrt{-3}$ does not divide 4: indeed, they are not associated and they have the same norm.

- Let x be a common divisor of the elements of S that is divisible by 2. There are then integers a and b such that $x = 2a + 2b\sqrt{-3}$ and, since x divides 4, the number

  $$\frac{4}{2a + 2b\sqrt{-3}} = \frac{2a - 2b\sqrt{-3}}{a^2 + 3b^2}$$

  is in A. In particular, $a^2 + 3b^2$ divides $2b$, so $3b^2 \leq a^2 + 3b^2 \leq 2|b|$ and thus $b = 0$. We then have that $2/a \in \mathbb{Z}$, so that a is one of ± 1 or ± 2, and x one of ± 2 or ± 4. In fact, as 4 does not divide $2 + 2\sqrt{-3}$, the number x is one of ± 2 and therefore is associated to 2.
- Let now x be a common divisor of the elements of S that is divisible by $1 + \sqrt{-3}$, so that there are integers a and b such that $x = (1 + \sqrt{-3})(a + b\sqrt{-3})$. As x divides $2 + 2\sqrt{-3}$, the number

  $$\frac{2 + 2\sqrt{-3}}{(1 + \sqrt{-3})(a + b\sqrt{-3})} = \frac{2}{a + b\sqrt{-3}} = \frac{2a - 2b\sqrt{-3}}{a^2 + 3b^2}$$

  is in A, so $a^2 + 3b^2$ divides $2b$ and we see as before that $b = 0$ and that $2/a \in \mathbb{Z}$. As $2 + 2\sqrt{-3}$ does not divide 4 in A, we must have, in fact, that a is one of ± 1, and thus that x is associated to $1 + \sqrt{-3}$.

Rings in which every finite subset admits a greatest common divisor are convenient for many things. We give them a name.

Definition A.7.4. A ring is a ***GCD domain*** if it is an integral domain and each of its finite subsets admits a greatest common divisor.

When checking that a ring satisfies this condition, the result of the following exercise is useful.

Exercise A.7.5. Let A be an integral domain. If every subset of A with two elements has a greatest common divisor in A, then A is a GCD domain.

The following lemma gives a few facts that are useful when dealing with greatest common divisors.

Lemma A.7.6. *Let A be a GCD domain, and let a, b, and c be elements of A.*

(*i*) *If $x \in \gcd\{a,b\}$ and $y \in \gcd\{b,c\}$, then $\gcd\{x,c\} = \gcd\{a,b,c\} = \gcd\{a,y\}$.*

(*ii*) $\gcd\{ac,bc\} = c\gcd\{a,b\}$.

(*iii*) *If $x \in \gcd\{a,b\}$, then $\gcd\{a,bc\} = \gcd\{a,xc\}$.*

(*iv*) *If $1 \in \gcd\{a,b\}$ and $1 \in \gcd\{a,c\}$, then $1 \in \gcd\{a,bc\}$.*

If we forget for a moment the fact that $\gcd\{a,b\}$ denotes a set and not an element of the ring, then we can write the equalities of the first part of this lemma in the form

$$\gcd\{\gcd\{a,b\},c\} = \gcd\{a,b,c\} = \gcd\{a,\gcd\{b,c\}\},$$

and we can view this as saying that the operation gcd is associative.

Proof. (*i*) By symmetry, it is enough to prove that $\gcd\{x,c\} = \gcd\{a,b,c\}$. Let d be an element of $\gcd\{a,b,c\}$, and let e be an element of $\gcd\{x,c\}$. Since d divides a and b, it divides x, and since it also divides c, we see that d divides e. Conversely, since e divides x, it divides a and b, and since it also divides c, it divides d. We thus see that $d \sim e$, and thus that the sets $\gcd\{a,b,c\}$ and $\gcd\{x,c\}$ are equal, because they are equivalence classes for the relation of association.

(*ii*) Let d_0 and e_0 be elements of $\gcd\{a,b\}$ and of $\gcd\{ac,bc\}$, respectively. Since d_0 divides a and b, the product cd_0 divides ac and bc, and is thus a divisor of e_0 and there is an element f of A such that $e_0 = cd_0f$. There are elements $\bar{a}$ and $\bar{b}$ in A such that $ac = e_0\bar{a}$ and $bc = e_0\bar{b}$, and then $ac = e_0\bar{a} = cd_0f\bar{a}$ and $bc = e_0\bar{b} = cd_0f\bar{b}$, so that $a = d_0f\bar{a}$ and $b = d_0f\bar{b}$. This implies that d_0f divides d_0, and thus that f is a unit. We have shown that $e_0 \sim cd_0$.

If e is an element of $\gcd\{ac,bc\}$, so that $e \sim e_0 \sim cd_0$, then there is a unit u in A such that $e = ucd_0$ and, since $ud_0 \in \gcd\{a,b\}$, we have that $e \in c\gcd\{a,b\}$: we see with this that $\gcd\{ac,bc\} \subseteq c\gcd\{a,b\}$. On the other hand, if d is an element of $\gcd\{a,b\}$, then $d \sim d_0$, so that $cd \sim cd_0 \sim e_0 \in \gcd\{ac,bc\}$ and thus also $cd \in \gcd\{ac,bc\}$: this shows that $c\gcd\{a,b\} \subseteq \gcd\{ac,bc\}$. The two inclusions that we have obtained imply the equality of (*ii*).

(*iii*) Let x be an element of $\gcd\{a,b\}$. Since $a \in \gcd\{a,ac\}$ and $cx \in c\gcd\{a,b\} = \gcd\{ac,bc\}$, we have, according to (*i*), that $\gcd\{a,bc\} = \gcd\{a,ac,bc\} = \gcd\{a,xc\}$.

(*iv*) This follows immediately from (*iii*). □

An infinite subset of a GCD domain need not admit a greatest common divisor. The following proposition tells us that finitely generated ideals, which are usually infinite, do.

Proposition A.7.7. *Let A be a GCD domain, let I be a finitely generated ideal of A, and let S be a finite subset of A such that $I = \langle S \rangle$. The set* $\gcd I$ *coincides with* $\gcd S$ *and is therefore not empty, and the ideal generated by any of its elements is the unique minimal element of the set of principal ideals that contain I.*

Proof. Let $a_1, \ldots, a_n$ be the elements of S, and let d be an element of $\gcd S$. If b is an element of I, then there are elements $b_1, \ldots, b_n$ of A such that $b = \sum_{i=1}^{n} b_i a_i$ and, since d divides each of $a_1, \ldots, a_n$, we see that d divides b. On the other hand, if e is a common divisor for the elements of I, then in particular e divides all the elements of S and thus also d. This shows that $d \in \gcd I$ and, since $\gcd S$ and $\gcd I$ are both equivalence classes for the association relation, this implies that, in fact, $\gcd I = \gcd S$.

Since d divides all the elements of I, we have that $I \subseteq \langle d \rangle$. On the other hand, if J is a principal ideal of A that contains I, then there is an element b of A such that $J = \langle b \rangle$ and, since $I \subseteq J = \langle b \rangle$, the element b divides each element of I: as d is in $\gcd I$, this implies that b divides d and thus that $J = \langle b \rangle \supseteq \langle d \rangle$. The principal ideal $\langle d \rangle$ is therefore the unique minimal element of the set of principal ideals of A that contain I. □

We will prove below, as Proposition A.7.14, that unique factorization domains are GCD domains, and this implies, in view of Proposition A.6.14, that a principal ideal domain is a GCD domain. For such a ring, though, there is a simpler way to prove this which we will now present. In fact, that argument works more generally for rings that satisfy the condition of the following definition.

Definition A.7.8. An integral domain A is a ***Bézout domain*** if every finitely generated ideal of A is principal.

These rings are named after Étienne Bézout. Of course, principal ideal domains are precisely the Bézout domains that are Noetherian. Bézout domains that are not Noetherian do exist. To present an example of this we need the results of the following exercise.

Exercise A.7.9.

(a) Show that an integral domain A is a Bézout domain if any ideal of A that can be generated by two elements is principal.

(b) Show that an ideal $\langle a, b \rangle$ in a ring A is principal if and only if there exist elements u and v of A such that $ua + vb$ divides both a and b.

Example A.7.10. The set A of all elements of $\mathbb{Q}[x]$ whose constant term is an integer is easily seen to be a subring of $\mathbb{Q}[x]$. In this ring, any polynomial with zero constant term is divisible by any non-zero integer. Let us show that it is a non-Noetherian Bézout domain.

- We want to show that every ideal of A that can be generated by two elements is principal. In

order to reach a contradiction, let us suppose that this is not the case, and among all the ordered pairs of non-zero elements of A that generate an ideal which is not principal let (a, b) be one such that the non-negative integer $\deg a + \deg b$ is minimal.

According to the result of Exercise A.7.9, there do not exist elements u and v such that $ua + vb$ is a common divisor of a and b. This implies that

> *the polynomials a and b do not have a common divisor in A that is a non-constant polynomial.* (A.11)

Indeed, let us suppose that d is common divisor of a and b in A that is a non-constant polynomial, and let $\bar{a}$ and $\bar{b}$ be the elements of A such that $a = d\bar{a}$ and $b = d\bar{b}$. As $\deg d > 0$, we have that $\deg \bar{a} + \deg \bar{b} < \deg a + \deg b$ and, since $\bar{a}$ and $\bar{b}$ are non-zero, the way in which we chose the pair (a, b) implies that the ideal $\langle \bar{a}, \bar{b} \rangle$ is principal, so that there are elements u and v in A such that $u\bar{a} + v\bar{b}$ divides $\bar{a}$ and $\bar{b}$: but then $ua + vb = ud\bar{a} + vd\bar{b}$ divides $a = d\bar{a}$ and $b = d\bar{b}$, and this is absurd. This contradiction proves (A.11).

It follows from (A.11) that one of a or b has non-zero constant term. If this were not so, we could find positive integers m, n, r, and s, and elements c and d of A such that $a = x^m c/r$ and $b = x^n d/s$, and then x/rs would be a non-constant common divisor of a and b in A, since $a = x/rs \cdot sx^{m-1}c$ and $b = x/rs \cdot rx^{n-1}d$, and (A.11) tells us this is impossible.

Let now g be the greatest common divisor of a and b in the ring $\mathbb{Q}[x]$. Since one of a or b has non-zero constant term, so does g, and there is therefore a rational number n such that ng has constant term equal to 1 and is thus an element of A. The polynomials e and f in $\mathbb{Q}[x]$ such that $a = nge$ and $b = ngf$ have integer constant term, so they are in A, and thus ng is, in fact, a common divisor of a and b in A. According to (A.11), the polynomial ng is constant and, therefore, equal to 1. This implies that $1 \in a\mathbb{Q}[x] + b\mathbb{Q}[x]$, so that the intersection $\mathbb{Z} \cap (aA + bA)$, which is an ideal of $\mathbb{Z}$, is not zero. There is then a positive integer m such that $\mathbb{Z} \cap (aA + bA) = m\mathbb{Z}$, and elements h and k in A such that $m = ha + kb$. Let us notice that $mA \subseteq aA + bA$.

Let now a_0 and b_0 be the constant terms of a and of b, let w be their non-negative greatest common divisor in $\mathbb{Z}$, and let s and t be integers such that $w = sa_0 + tb_0$. The constant term of the polynomial $sa + tb - w$ is zero, so that m divides $sa + tb - w$ in A, and thus $sa + tb - w \in mA \subseteq aA + bA$, so that $w \in \mathbb{Z} \cap (aA + bA) = m\mathbb{Z}$ and m divides w. On the other hand, we have that $m = h(0)a_0 + k(0)b_0$, so that w also divides m and thus $m = w$. Since clearly w divides both a and b, the result of Exercise A.7.9 lets us conclude that the ideal $\langle a, b \rangle$ of A is principal, which is absurd.

This contradiction arose from our hypothesis that there are 2-generated ideals in A that are not principal, so this is not true: the ring A is thus a Bézout domain.

- Let us consider the subset $X \coloneqq \{x/n : n \in \mathbb{N}\}$ of A, the ideal I that it generates, and suppose that I is finitely generated. Since we have shown above that A is a Bézout domain, then this implies that, in fact, the ideal I is principal, so that there is an element f in I such that

$I = \langle f \rangle$. Since $x \in I$, this polynomial f divides x in I and therefore also in $\mathbb{Q}[x]$, so it is of the form ax for some non-zero rational number a. Let r and s be coprime integers such that $a = r/s$, and let p be a prime number that does not divide s. Since $x/p \in X \subseteq I = \langle rx/s \rangle$, there is an element b of A such that $x/p = rxb/s$. Of course, b is a constant polynomial, so an integer, and that equality implies that in $\mathbb{Z}$ be have $s = rbp$: this is absurd, since p does not divide s. This proves that the ideal I is not finitely generated, and that therefore the ring A is not Noetherian.

The following one is an important example of a non-Noetherian Bézout domain found in the context of complex analysis.

Example A.7.11. Let Ω be a connected open subset of $\mathbb{C}$. Olaf Helmer proved in [Hel1940] that the ring $\mathcal{H}(\Omega)$ of holomorphic functions on Ω is a Bézout domain, and this ring is not Noetherian. This is a consequence of the *Weierstraß Factorization Theorem* and of the *Mittag–Leffler Theorem* on the existence of meromorphic functions with prescribed principal parts. The details and the story of this result are given by Reinhold Remmert in the fourth chapter of his book [Rem1998].

Exercise A.7.12. Let A be a Bézout domain, let F be the field of fractions of A, and let B be any subring of F such that $A \subseteq B$. Show that subset $S \coloneqq \{a \in A : a^{-1} \in B\}$ of A is multiplicatively closed, that B is the localization A_S, and that B is a Bézout domain.

One should note that, in general, a subring of the fraction field of a domain A that contains A is not a localization of A. For example, if $A = \mathbb{Q}[x, y]$, and $A_{(x)}$ and $A_{(y)}$ are the localizations of A at the prime ideals (x) and (y), viewed as subrings of the fraction field $\operatorname{Frac} A = \mathbb{Q}(x, y)$, then the subring $B \coloneqq A_{(x)} \cap A_{(y)}$ of $\operatorname{Frac} A$ contains A and is not a localization of A.

As we said, the reason we are considering Bézout domains is that the following result holds.

Proposition A.7.13. *A Bézout domain is a GCD domain.*

Proof. Let A be a Bézout domain. According to the result of Exercise A.7.5, in order to prove the proposition it is enough that we show that every 2-element subset of A admits a greatest common divisor. Let then a and b be two elements of A. Since A is a Bézout domain, there is an element d in A such that $\langle a, b \rangle = \langle d \rangle$. Let us show that d is a greatest common divisor for the set $\{a, b\}$.

- Since $a, b \in \langle a, b \rangle = \langle d \rangle$, this element d divides both a and b.
- On the other hand, let e be a common divisor of a and b: as d is in $\langle a, b \rangle$, there are elements u and v in A such that $d = ua + vb$, and therefore e clearly divides d. □

Having considered this special result, let us now move to the proof of the important fact that

unique factorization domains are GCD domains. As we will see, most of the technical details needed to do this are contained in Lemmas A.6.8 and A.6.10.

Proposition A.7.14. *A unique factorization domain is a GCD domain.*

There exist GCD domains that are not unique factorization domains. The ring of algebraic integers in $\mathbb{C}$ and the ring of entire functions are examples of this — proving either of these claims is outside of the scope of these notes, though. On the other hand, there exist unique factorization domains that are not Bézout domains: one simple example is the ring $\mathbb{Z}[x]$, which is a unique factorization domain by the Proposition A.6.20 that we will prove later and whose ideal $(2, x)$ is not principal.

Proof. Let A be a unique factorization domain, and let $\mathscr{I}$ be a set of irreducible elements of A as in the first part of Lemma A.6.10. According to the result of Exercise A.7.5, to prove the proposition it is enough that we check that every subset of A with two non-zero elements admits a greatest common divisor.

Let a and b be two elements of A, let S be the subset $\{a, b\}$, and let us show that $\gcd S \neq \varnothing$. If one of a or b is zero, then the other is an element of $\gcd S$, and we may therefore suppose that both a and b are non-zero. According to Lemma A.6.10, there are units c_a and c_b in A and functions $\varepsilon_a, \varepsilon_b \colon \mathscr{I} \to \mathbb{N}_0$ such that the sets $I_a \coloneqq \{p \in \mathscr{I} : \varepsilon_a(p) > 0\}$ and $I_b \coloneqq \{p \in \mathscr{I} : \varepsilon_b(p) > 0\}$ are finite, $a = c_a \prod_{p \in I_a} p^{\varepsilon_a(p)}$, and $b = c_b \prod_{p \in I_b} p^{\varepsilon_b(p)}$. Let us consider the function $\varepsilon \colon \mathscr{I} \to \mathbb{N}_0$ that on each element p of $\mathscr{I}$ takes the value

$$\varepsilon(p) = \min\{\varepsilon_a(p), \varepsilon_b(p)\}.$$

The set $I \coloneqq \{p \in \mathscr{I} : \varepsilon(p) > 0\}$ is contained in I_a, so it is finite, and we may therefore also consider in A the element

$$d \coloneqq \prod_{p \in I} p^{\varepsilon(p)}.$$

According to the uniqueness claim of part (*iii*) of Lemma A.6.10, we have that $c_d = 1$ and $\varepsilon_d = \varepsilon$. To complete the proof of the proposition, we will show that d is a greatest common divisor of $\{a, b\}$.

- Since clearly $\varepsilon(p) \leq \varepsilon_a(p)$ and $\varepsilon(p) \leq \varepsilon_b(p)$ for all p in $\mathscr{I}$, the last part of Lemma A.6.10 tells us that d divides both a and b.
- Let e be an element of A that divides both a and b. As e is therefore non-zero, there are a unit c_e and a function $\varepsilon_e \colon \mathscr{I} \to \mathbb{N}_0$ such that the set $I_e \coloneqq \{p \in \mathscr{I} : \varepsilon_e(p) > 0\}$ is finite and $e = c_e \prod_{p \in I_e} p^{\varepsilon_e(p)}$. Since e divides a and b, the last part of Lemma A.6.10 tells us that $\varepsilon_e(p) \leq \varepsilon_a(p)$ and $\varepsilon_e(p) \leq \varepsilon_b(p)$ for all p in $\mathscr{I}$, so that in fact

  $$\varepsilon_e(p) \leq \min\{\varepsilon_a(p), \varepsilon_b(p)\} = \varepsilon_d(p)$$

  for all p in $\mathscr{I}$ and, therefore, according to the same lemma, d divides e. □

A.8. Gauss's Lemma

In this section we will present two extremely useful results that are valid in GCD domains.

Definition A.8.1. Let A be a ring. The ***content*** of a polynomial f in $A[x]$ is the ideal generated by the set of its coefficients, which we write $\mathrm{cont}(f)$.

In the situation of this definition it is obvious that $\mathrm{cont}(af) = a\,\mathrm{cont}(f)$ for each element a of A. The main observation to be made about these concepts is the following one.

Proposition A.8.2. *Let A be a ring, and let f and g be two elements of $A[x]$. We have that*

$$\mathrm{cont}(fg) \subseteq \mathrm{cont}(f)\cdot\mathrm{cont}(g) \subseteq \sqrt{\mathrm{cont}(fg)}.$$

Proof. If one of f or g is zero, the claim is obvious, so we may suppose that f and g are both not zero. Let m and n be the degrees of f and of g, respectively, and let $a_0, \ldots, a_m$ and $b_0, \ldots, b_n$ be the elements of A such that $f = \sum_{i=0}^{m} a_i x^i$ and $g = \sum_{j=0}^{n} b_j x^j$, so that $fg = \sum_{k=0}^{m+n} c_k x^k$, with

$$c_k = \sum_{l=\max\{0,k-n\}}^{\min\{m,k\}} a_l b_{k-l}$$

for each k in $[\![0, m+n]\!]$. Of course, we then have $\mathrm{cont}(f) = \langle a_0, \ldots, a_m\rangle$, $\mathrm{cont}(g) = \langle b_0, \ldots, b_m\rangle$, and $\mathrm{cont}(fg) = \langle c_0, \ldots, c_{m+n}\rangle$. Since clearly $a_i b_j \in \mathrm{cont}(f)\cdot\mathrm{cont}(g)$ for all choices of i in $[\![m]\!]$ and of j in $[\![n]\!]$, we have that

$$\mathrm{cont}(fg) \subseteq \mathrm{cont}(f)\cdot\mathrm{cont}(g)$$

To complete the proof we need show that $\mathrm{cont}(f)\cdot\mathrm{cont}(g) \subseteq \sqrt{\mathrm{cont}(fg)}$ and, as the radical of an ideal is the intersection of all the prime ideals that contain the ideal, to do this it is enough that we check that for any prime ideal $\mathfrak{p}$ of A we have that

$$\mathrm{cont}(fg) \subseteq \mathfrak{p} \implies \mathrm{cont}(f)\cdot\mathrm{cont}(g) \subseteq \mathfrak{p}.$$

Let then $\mathfrak{p}$ be a prime ideal of A that contains $\mathrm{cont}(fg)$, and let $\pi\colon A[x] \to (A/\mathfrak{p})[x]$ the map induced by the canonical projection $A \to A/\mathfrak{p}$. Since $\mathrm{cont}(fg) \subseteq \mathfrak{p}$, all the coefficients of fg are in $\mathfrak{p}$ and thus $\pi(f)\cdot\pi(g) = \pi(fg) = 0$: as the ideal $\mathfrak{p}$ is prime, the quotient $A/\mathfrak{p}$ is an integral domain, and therefore so is the ring $(A/\mathfrak{p})[x]$, and then one of $\pi(f)$ or $\pi(g)$ is zero, so that one of $\mathrm{cont}(f)$ or $\mathrm{cont}(g)$ is contained in $\mathfrak{p}$ and, as a consequence, $\mathrm{cont}(f)\cdot\mathrm{cont}(g) \subset \mathfrak{p}$. □

In general, in the situation of this proposition no two of the ideals $\mathrm{cont}(fg)$, $\mathrm{cont}(f)\cdot\mathrm{cont}(g)$, and $\sqrt{\mathrm{cont}(fg)}$ need be equal.

Example A.8.3. Let us consider, as Irving Kaplansky does in [Kap1970], the subring $A \coloneqq \mathbb{Z}[2i]$ of $\mathbb{C}$, and the polynomials $f \coloneqq 2 + 2ix$ and $g \coloneqq 2 - 2ix$ in $A[x]$. As $\operatorname{cont}(f) = \operatorname{cont}(g) = \langle 2, 2i\rangle$, we have that $\operatorname{cont}(f) \cdot \operatorname{cont}(g) = \langle 2, 2i\rangle^2 = \langle 4, 4i\rangle$. Since $fg = 4 + 4x^2$, we have that

$$\operatorname{cont}(fg) = \langle 4\rangle = \{4a + 8bi : a, b \in \mathbb{Z}\},$$

and this ideal does not contain $4i$. On the other hand, it is clear that $2 \notin \operatorname{cont}(f) \cdot \operatorname{cont}(g)$ and that $2 \in \sqrt{\operatorname{cont} fg}$. We therefore have that $\operatorname{cont}(fg) \subsetneq \operatorname{cont}(f) \cdot \operatorname{cont}(g) \subsetneq \sqrt{\operatorname{cont}(fg)}$.

By restricting the class of rings under consideration and using a modified version of the content we can improve the result of Proposition A.8.2.

Definition A.8.4. Let A be a GCD domain. If f is an element of $A[x]$, then we write $\underline{\operatorname{cont}}(f)$ for the unique minimal principal ideal of A that contains $\operatorname{cont}(f)$, and we say that f is ***primitive*** if $\underline{\operatorname{cont}}(f) = A$.

The existence of such a unique minimal principal ideal is guaranteed by Proposition A.7.7, since the content of a polynomial is manifestly a finitely generated ideal. If the ring A is a Bézout domain, then $\underline{\operatorname{cont}}(f)$ is simply $\operatorname{cont}(f)$.

Lemma A.8.5. *Let A be a GCD domain, and let F be the field of fractions of A.*

(*i*) *If a is an element of A and f one of $A[x]$, then $\underline{\operatorname{cont}}(af) = a\,\underline{\operatorname{cont}}(f)$.*

(*ii*) *If f is a non-zero element of $A[x]$ and d is an element of A such that $\underline{\operatorname{cont}}(f) = \langle d\rangle$, then there is a primitive element $\bar{f}$ in $A[x]$ such that $f = d\bar{f}$.*

(*iii*) *If f is a non-zero element of $F[x]$, then there is an element a of F and a primitive element $\bar{f}$ of $A[x]$ such that $f = a\bar{f}$, and if a' and $\bar{f}'$ are another element of F and another primitive element of $A[x]$, respectively, such that we also have $f = a'\bar{f}'$, then there is a unit u of A such that $a = ua'$.*

Proof. (*i*) Since $\operatorname{cont}(af) = a \operatorname{cont}(af)$, this is clear.

(*ii*) Let f be a non-zero element of $A[x]$, and let d be an element of A such that $\underline{\operatorname{cont}}(f) = \langle d\rangle$. Since d divides each coefficient of f, there is an element $\bar{f}$ in $A[x]$ such that $f = d\bar{f}$, and it is not zero because f is not zero. Let now $\bar{d}$ be a greatest common divisor for set of coefficients of $\bar{f}$. As $d\bar{d}$ divides all the coefficients of $f = d\bar{f}$, we have that $d\bar{d}$ divides d, and this implies that $\bar{d}$ is a unit of A. This tells us that $\underline{\operatorname{cont}}(\bar{f}) = \langle \bar{d}\rangle = A$, so that $\bar{f}$ is primitive.

(*iii*) Let f be a non-zero element of $F[x]$. There are then an element c of A and an element f_1 of $A[x]$ such that $f = \bar{f}/c$ and, according to (*i*), there are also an element b of A and a primitive element $\bar{f}$ of $A[x]$ such that $\bar{f} = b\bar{f}$. If we now put $a \coloneqq b/c$, which is an element of F, we have that $f = a\bar{f}$. This proves the first claim of (*ii*).

To prove the second one, let a' be an element of F and let $\bar{f}'$ be a primitive element of $A[x]$,

and let us suppose that $f = a'\bar{f}'$. Since $a\bar{f} = a'\bar{f}'$ and the polynomials $\bar{f}$ and $\bar{f}'$ are both primitive, we have that

$$\langle a\rangle = a\,\underline{\mathrm{cont}}(\bar{f}) = \underline{\mathrm{cont}}(a\bar{f}) = \underline{\mathrm{cont}}(a\bar{f}') = a'\,\underline{\mathrm{cont}}(\bar{f}') = \langle a\rangle,$$

so that there is a unit u of A such that $a = ua'$. □

The main result about the content of polynomials with coefficients in a GCD domain is the following one, usually known as *Gauss's Lemma*.

Proposition A.8.6. *Let A be a GCD domain. If f and g are two elements of $A[x]$, then*

$$\underline{\mathrm{cont}}(fg) = \underline{\mathrm{cont}}(f)\cdot\underline{\mathrm{cont}}(g). \tag{A.12}$$

Proof. Let f and g be two elements of $A[x]$. If one of f or g is zero, the equality (A.12) is obvious, so we may suppose that both f and g are not zero. Let m and n be the degrees of f and g, respectively. We will prove that the product fg is primitive by induction with respect to the non-negative integer $m+n$.

If $m+n=0$, so that there are non-zero elements a and b in A such that $f=a$ and $g=b$, then we have that $\underline{\mathrm{cont}}(f)=\langle a\rangle$, $\underline{\mathrm{cont}}(f)=\langle b\rangle$, and $\underline{\mathrm{cont}}(fg)=\underline{\mathrm{cont}}(ab)=\langle ab\rangle$, so that we clearly have that $\underline{\mathrm{cont}}(f)\cdot\underline{\mathrm{cont}}(g)=\langle a\rangle\cdot\langle b\rangle=\langle ab\rangle=\underline{\mathrm{cont}}(fg)$, as we want.

Let us suppose now that the integer $m+n$ is positive. Let d and e be elements of A such that $\underline{\mathrm{cont}}(f)=\langle d\rangle$ and $\underline{\mathrm{cont}}(g)=\langle e\rangle$, let $\bar{f}$ and $\bar{g}$ be the primitive elements of $A[x]$ such that $f=d\bar{f}$ and $g=e\bar{g}$, and let a and b be the leading coefficients of $\bar{f}$ and of $\bar{g}$, respectively.

If $\bar{f}=ax^m$, then the element a is a unit because $\bar{f}$ is primitive and we therefore have that

$$\underline{\mathrm{cont}}(fg)=\underline{\mathrm{cont}}(deax^m\bar{g})=dea\,\underline{\mathrm{cont}}(\bar{g})=\langle dea\rangle=\langle d\rangle\cdot\langle e\rangle=\underline{\mathrm{cont}}(f)\cdot\underline{\mathrm{cont}}(g),$$

and a argument proves the equality (A.12) if $\bar{g}=bx^n$. We can therefore suppose in what follows that both $\bar{f}$ and $\bar{g}$ have each more than one term. Let u be an element of A such that $\underline{\mathrm{cont}}(\bar{f}\bar{g})=\langle u\rangle$.

- Let v be a greatest common divisor of $\{a,u\}$. This element v divides all the coefficients of $(f-ax^m)g$, so that $\underline{\mathrm{cont}}((\bar{f}-ax^m)\bar{g})\subseteq\langle v\rangle$ and, according to the inductive hypothesis,

  $$\underline{\mathrm{cont}}(\bar{f}-ax^m)=\underline{\mathrm{cont}}(\bar{f}-ax^m)\cdot A=\underline{\mathrm{cont}}(\bar{f}-ax^m)\cdot\underline{\mathrm{cont}}(\bar{g})=\underline{\mathrm{cont}}((\bar{f}-ax^m)\bar{g})\subseteq\langle v\rangle.$$

  Since v divides a, this implies us that v divides all the coefficients of $\bar{f}$ and thus that $A=\underline{\mathrm{cont}}(f)\subseteq\langle v\rangle$: this tells us that v is a unit, so that $1\in\gcd\{a,u\}$.
- Similarly, let v' be a greatest common divisor of $\{b,u\}$: it divides the coefficients of $\bar{f}(g-bx^n)$, so $\underline{\mathrm{cont}}(\bar{f}(\bar{g}-bx^n))\subseteq\langle v'\rangle$ and, in view of the inductive hypothesis,

  $$\underline{\mathrm{cont}}(\bar{g}-bx^n)=A\cdot\underline{\mathrm{cont}}(\bar{g}-bx^n)=\underline{\mathrm{cont}}(\bar{f})\cdot\underline{\mathrm{cont}}(\bar{g}-bx^n)=\underline{\mathrm{cont}}(\bar{f}(\bar{g}-bx^n))\subseteq\langle v'\rangle.$$

As v' divides b, this implies that v' divides the coefficients of $\bar{g}$ and, since $\bar{g}$ is primitive, that v' is a unit, so that $1 \in \gcd\{b, u\}$.

We therefore have that $1 \in \gcd\{a, u\}$ and that $1 \in \gcd\{b, u\}$, and we can conclude from the last part of Lemma A.7.6 that also $1 \in \gcd\{ab, u\}$. Since ab is the leading coefficient of $\bar{f}\bar{g}$, it is divisible by u, and thus also $u \in \gcd\{ab, u\}$. We see with this that $u \sim 1$, so that $\bar{f}\bar{g}$ is primitive and

$$\underline{\mathrm{cont}}(fg) = \underline{\mathrm{cont}}(de\bar{f}\bar{g}) = de\,\underline{\mathrm{cont}}(\bar{f}\bar{g}) = \langle de\rangle = \langle d\rangle \cdot \langle e\rangle = \underline{\mathrm{cont}}(f) \cdot \underline{\mathrm{cont}}(g).$$

This completes the induction, and therefore proves the proposition. □

There are many important corollaries of Proposition A.8.6. The first one that we mention is simply one of its special cases.

Corollary A.8.7. *Let A be a GCD domain. If f and g are two primitive elements of $A[x]$, then the product fg is also primitive.* □

The second corollary is a very useful divisibility criterion for polynomials.

Corollary A.8.8. *Let A be a GCD domain, let F be the field of fractions of A, and let f and g be two elements of $A[x]$. The polynomial f divides the polynomial g in $A[x]$ if and only if it divides it in $F[x]$ and $\underline{\mathrm{cont}}(g) \subseteq \underline{\mathrm{cont}}(f)$.*

Proof. If f divides g in $A[x]$, so that there is an element h of $A[x]$ such that $g = fh$, then f divides g in $F[x]$ and, according to Proposition A.8.6, we have that $\underline{\mathrm{cont}}(h) = \underline{\mathrm{cont}}(f) \cdot \underline{\mathrm{cont}}(h) \subseteq \underline{\mathrm{cont}}(f)$.

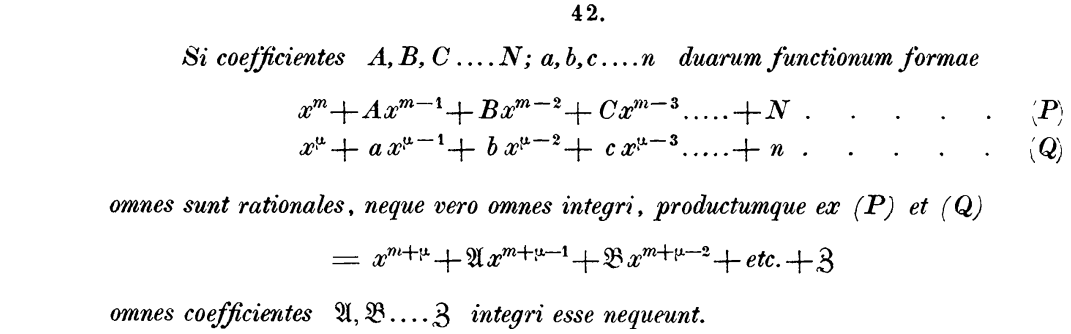
Let us suppose now that f divides g in $F[x]$ and that $\underline{\mathrm{cont}}(g) \subseteq \underline{\mathrm{cont}}(f)$. Let a be a generator of $\underline{\mathrm{cont}}(f)$, and let $\bar{f}$ be the primitive element of $A[x]$ such that $f = a\bar{f}$. As f divides g in $F[x]$, there is an element h of $F[x]$ such that $g = fh$, and there are therefore elements b and c in A and a primitive element $\bar{h}$ of $A[x]$ such that $c \neq 0$ and $h = b\bar{h}/c$. As $cg = ab\bar{f}\bar{h}$ and, according to Corollary A.8.7, the product $\bar{f}\bar{h}$ is primitive, we have that

$$ab \in \langle ab\rangle = ab\,\underline{\mathrm{cont}}(\bar{f}\bar{h}) = \underline{\mathrm{cont}}(ab\bar{f}\bar{h}) = \underline{\mathrm{cont}}(cg) = c\,\underline{\mathrm{cont}}(g) \subseteq c\,\underline{\mathrm{cont}}(f) = \langle ac\rangle,$$

so that ac divides ab in A. This implies, of course, that c divides b in A, so that the fraction b/c is in A and thus $h = b\bar{h}/c$ is an element of $A[x]$. This shows that f divides g in $A[x]$, as we want. □

The third corollary is an integrality criterion.

Corollary A.8.9. *Let A be a GCD domain, let F be the field of fractions of A, and let f and g be two elements of $F[x]$ each of which has a coefficient that is a unit of A. If the fg is a primitive element of $A[x]$, then f and g are in $A[x]$.*



42.

Si coefficientes $A, B, C \ldots . N; a, b, c \ldots . n$ *duarum functionum formae*

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} \ldots . + N \quad . \quad . \quad . \quad . \quad . \quad (P)$$
$$x^\mu + a\,x^{\mu-1} + b\,x^{\mu-2} + c\,x^{\mu-3} \ldots . + n \quad . \quad . \quad . \quad . \quad . \quad (Q)$$

omnes sunt rationales, neque vero omnes integri, productumque ex (P) *et* (Q)

$$= x^{m+\mu} + \mathfrak{A}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + etc. + \mathfrak{Z}$$

omnes coefficientes $\mathfrak{A}, \mathfrak{B} \ldots . \mathfrak{Z}$ *integri esse nequeunt.*

Figure A.1. The original statement of *Gauss's Lemma* in Article 42 of Carl Friedrich Gauss's *Disquisitiones Arithmeticae*.

Proof. There are elements a and b of F and primitive polynomials $\bar{f}$ and $\bar{g}$ in $A[x]$ such that $f = a\bar{f}$ and $g = b\bar{g}$. We know f has a coefficient u which is a unit of A, and u/a is one of the coefficients of $\bar{f}$, so a^{-1} is in fact an element of A; similarly, of course, b^{-1} is in A. Corollary A.8.7 tells us that $\bar{f}\bar{g} = a^{-1}b^{-1}fg$ is a primitive element of $A[x]$, so that $a^{-1}b^{-1}\,\underline{\mathrm{cont}}(fg) = \underline{\mathrm{cont}}(a^{-1}b^{-1}fg) = \underline{\mathrm{cont}}(\bar{f}\bar{g}) = A$. It follows from this that a^{-1} and b^{-1} are units of A, and thus that $f = a\bar{f}$ and $g = b\bar{g}$ have their coefficients in A. □

The following is, again, simply a special case of Corollary A.8.9.

Corollary A.8.10. *Let A be a GCD domain, let F be the field of fractions of A, and let f and g be two monic elements of $F[x]$. If all the coefficients of fg are in A, then all the coefficients of f and of g are in A.*

The contrapositive of this statement is the original lemma of Gauss: its special case over the integers appears as Article 42 in Carl Friedrich Gauss's *Disquisitiones Arithmeticae* — see Figure A.1.

Proof. Let us suppose that all the coefficients of fg are in A. Since that polynomial is monic, it is then primitive in $A[x]$, and Corollary A.8.10 tells us that both f and g are in $A[x]$. □

Corollary A.8.10 implies, for example, that if a complex number α is an algebraic integer, so that it is a root of a monic element of $\mathbb{Z}[x]$, then the minimal polynomial of α over $\mathbb{Q}$, which is, in principle, a monic element of $\mathbb{Q}[x]$, has all its coefficients in $\mathbb{Z}$.

Corollary A.8.11. *Let A be a GCD domain, let F be the field of fractions of A, and let f and g be two elements of $F[x]$. If fg is in $A[x]$, then there is an element d of F such that df and g/d are in $A[x]$.*

Proof. There are elements a and b in F and primitive elements $\bar{f}$ and $\bar{g}$ in $A[x]$ such that $f = a\bar{f}$ and $g = b\bar{g}$. According to Corollary A.8.7, the product $\bar{f}\bar{g}$ is primitive: since we have $fg = ab\bar{f}\bar{g}$, it follows from the last part of Lemma A.8.5 that ab is a unit of A. If we put $d \coloneqq b$, we then have that the polynomials $df = ab\bar{f} = u\bar{f}$ and $g/s = \bar{g}$ are both in $A[x]$. □

Our final corollary is an irreducible criterion.

Corollary A.8.12. *Let A be a GCD domain, and let F be the field of fractions of A. A non-constant polynomial f in $A[x]$ is irreducible if and only if it is irreducible in $F[x]$ and it is primitive.*

Proof. Let f be an irreducible non-constant element of $A[x]$, let c be an element of A such that $\underline{\mathrm{cont}}(f) = c$, and let $\bar{f}$ be the primitive element of $A[x]$ such that $f = c\bar{f}$. The polynomial $\bar{f}$ is not constant, so it is not a unit of $A[x]$: as f is irreducible in $A[x]$, it follows then that c is a unit of $A[x]$ and therefore, since it is constant, of A, so that f is primitive.

Let us suppose now that there are elements g and h in $F[x]$ such that $f = gh$. According to Corollary A.8.11 there is an element d of F such that dg and h/d are both in $A[x]$, and since $f = dg \cdot h/d$ and f is irreducible in $A[x]$, we see that one of dg or h/d is a unit of $A[x]$, so that one of g or h is a unit of $F[x]$. This tells us that f is irreducible in $F[x]$, and we can conclude that the condition given by the corollary for the irreducibility of f in $A[x]$ is necessary.

Let us suppose now that f is a non-constant primitive element of $A[x]$ that is irreducible in $F[x]$ and let g and h be elements of $A[x]$ such that $f = gh$. Since f is irreducible in $F[x]$, one of g or h is a unit there, so that it is constant. My symmetry, we can suppose that it is g that is constant, and since then $A = \underline{\mathrm{cont}}(f) = \underline{\mathrm{cont}}(gh) = g\,\underline{\mathrm{cont}}(h)$, we see that g is a unit of A, so of $A[x]$. This shows that f is irreducible in $A[x]$, and the condition of the corollary sufficient. □

As an application of these results, let us reprove Proposition A.6.20. It is interesting to note that this is the original application made by Gauss of his lemma.

Proposition A.8.13. *If A is a unique factorization domain, then so is the ring $A[x]$.*

Proof. Let f be an element of $A[x]$, and let a and $\bar{f}$ be a generator of the ideal $\underline{\mathrm{cont}}(f)$ and the primitive element of $A[x]$ such that $f = a\bar{f}$.

Let F be the fraction field of A. Since $F[x]$ is a principal ideal domain, it is a unique factorization domain and there are therefore an element b of F, a non-negative integer n, and irreducible elements $g_1, \ldots, g_n$ of $F[x]$ such that $f = bg_1 \cdots g_n$ in $F[x]$. According to Lemma A.8.5, there are elements $b_1, \ldots, b_n$ of F and primitive elements $p_1, \ldots, p_n$ of $A[x]$ such that $g_i = b_i p_i$ for each i in $[\![n]\!]$. It follows from Corollary A.8.12 that $p_1, \ldots, p_n$ are irreducible elements of $A[x]$.

In fact, they are even prime there. Indeed, let us suppose that i is an element of $[\![n]\!]$, and that v

and w are elements of $A[x]$ such that p_i divides the product vw in $A[x]$. Of course, p_i then also divides the product vw in $F[x]$ and, since $F[x]$ is a unique factorization domain, p_i divides one of the factors v or w in $F[x]$. Corollary A.8.10 then implies that p_i divides that same factor in $A[x]$, since that factor has coefficients in A.

Let $c \coloneqq bb_1 \cdots b_n$. As $f = cp_1 \cdots p_n$ and the product $p_1 \cdots p_n$ is primitive, the last part of Lemma A.8.5 tells us that there is a unit u in A such that $c = au \in A$, and the fact that A is a unique factorization domain implies that there are a unit t of A, a non-negative integer m, and prime elements $q_1, \ldots, q_m$ of A such that $c = tq_1 \cdots q_m$. We then have that $f = tq_1 \cdots q_m p_1 \cdots p_n$, and each of the factors that appear in this product are either units of $A[x]$ or prime elements of $A[x]$ — indeed, the units and the prime elements of A are units and prime elements of $A[x]$, respectively.

This shows that if f is an element of $A[x]$, then there exist a unit t of $A[x]$, a non-negative integer n, and prime elements $p_1, \ldots, p_n$ of $A[x]$ such that $f = tp_1 \cdots p_n$. This tells us that the ring $A[x]$ satisfies the first condition of Definition A.6.7, and using Lemma A.6.12 we can see at once that it also satisfies the second one, so that $A[x]$ is a unique factorization domain. □

Another extremely useful application of *Gauss's Lemma* is the well-known *Rational Root Theorem*.

Proposition A.8.14. *Let A be a GCD domain, let F be its field of fractions, and let*

$$f = a_0 + a_1 x + \cdots + a_n x^n$$

be an element of $A[x]$. If p and q are elements of A such that $q \neq 0$, $1 \in \gcd\{p, q\}$ and p/q is a root of f, then p divides a_0 in A and q divides a_n in A.

Proof. Let p and q be elements of A such that $q \neq 0$, $1 \in \gcd\{p, q\}$, and p/q is a root of f. Let d be an element of A that generates $\underline{\text{cont}}(f)$, and let $\tilde{f}$ be the primitive element of $A[x]$ such that $f = d\tilde{f}$. The polynomial $g \coloneqq qx - p$ of $A[x]$ is primitive and divides f in $F[x]$, so Corollary A.8.8 tells us that g divides f in $A[x]$, and this implies immediately that p divides the constant term a_0 of f and that q divides the leading coefficient a_n of f. □

Let us finish our treatment of *Gauss's Lemma* and its consequences with the following irreducibility criterion, known usually as *Eisenstein's criterion*, because Gotthold Eisenstein published a version of the result in [Eis1850], even though the result had been found first by Theodor Schönemann [Sch1846].

Proposition A.8.15. *Let A be an integral domain, let F be the field of fractions of A, and let*

$$f = a_0 + a_1 x + \cdots + a_n x^n$$

be an element of $A[x]$ *with* $a_n \neq 0$ *such that there is a prime ideal* $\mathfrak{p}$ *of* A *such that*

$$a_0, \ldots, a_{n-1} \in \mathfrak{p}, \quad a_n \notin \mathfrak{p}, \quad a_0 \notin \mathfrak{p}^2,$$

(*i*) *The polynomial* f *is not equal to the product of two non-constant elements of* $A[x]$.
(*ii*) *If* f *is primitive, then then* f *is irreducible in* $A[x]$.
(*iii*) *If* A *is a unique factorization domain, then* f *is irreducible in* $F[x]$.

Proof. Since the ideal $\mathfrak{p}$ is prime, the quotient $A/\mathfrak{p}$ is an integral domain and we can consider its field of fractions K. Whenever a and u are elements o A and of $A[x]$, respectively, let us write $\bar{a}$ and $\bar{u}$ for the images of a and of u in K and in $K[x]$. For example, we have that $\bar{f} = \bar{a}_n x^n$.

(*i*) Let g and h be two elements of $A[x]$ of positive degree such that $f = gh$, and let b and c be the leading coefficients of g and of h, respectively. We have that $\bar{g}\bar{h} = \bar{a}_n x^n$ in $K[x]$ and that $\bar{a}_n \neq 0$ in K. Since $K[x]$ is a unique factorization domain and x is an irreducible element there, it follows that there are positive integers r and s such that $r+s = n$, $\bar{g} = \bar{b}x^r$, and $\bar{g} = \bar{c}x^s$. This implies immediately that the constant terms of g and of h are both in the ideal $\mathfrak{p}$, so that the constant term of $f = gh$ is in $\mathfrak{p}^2$. This contradicts the hypothesis, and this contradiction proves the first claim of the proposition.

(*ii*) If there are two non-unit elements gh in $A[x]$ such that $f = gh$, then, in view of (*i*), we can suppose that g is in fact in A, and therefore $\underline{\text{cont}}(f) = \underline{\text{cont}}(gh) = g\,\underline{\text{cont}}(h) \subseteq \langle g \rangle \subsetneq A$, so that A is not primitive in $A[x]$.

(*iii*) Let us suppose that there are elements g and h in $F[x]$ such that $f = gh$. Since it has coefficients in A and A is a GCD domain, Corollary A.8.11 tells us that there is an element d of F such that dg and h/d are both in $A[x]$. Since the product of these two polynomials is also f, part (*i*) of the proposition tells us that one of the two is constant, so that one of g or h is constant and therefore a unit of $F[x]$. This tells us that f is irreducible in $F[x]$. □

A.9. Integral dependence

Our next immediate objective is to present the concept of integral dependence, one of the key tools in commutative algebra, number theory, and algebraic geometry.

Definition A.9.1. Let B be a ring, and let A be s subring of B.

- An element b of B is ***integral*** over A if there is a monic polynomial f in $A[x]$ such that $f(b) = 0$.
- The ring B is ***integral*** over A if every element of B is integral over A.

- The ***integral closure*** of A in B is the subset of B of all those elements that are integral over A.
- The ring A is ***integrally closed*** in B if the integral closure of A in B is A itself.
- Finally, the ring A is ***normal*** if it is a domain and it is integrally closed in its field of fractions.

Let us note that in the situation of this definition it is obvious that the elements of B are integral over B. The simplest situation in which we can see these notions at work is the following one.

Example A.9.2. Let us show that

> *the integral closure of $\mathbb{Z}$ in $\mathbb{Q}$ is $\mathbb{Z}$ itself, so that $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$ and therefore, normal.*

Clearly every element of $\mathbb{Z}$ is integral over $\mathbb{Z}$. On the other hand, if an element q of $\mathbb{Q}$ is integral over $\mathbb{Z}$, then there is a monic polynomial f in $\mathbb{Z}[x]$ that has q as a root, and the *Rational Root Theorem* A.8.14 implies immediately that q is an element of $\mathbb{Z}$.

The argument in this example depends on the *Rational Root Theorem*, and therefore it should not be a surprise that it in fact works over any GCD domain.

Proposition A.9.3. *A GCD domain is normal.*

Proof. Let A be a GCD domain, let F be the field of fractions of A, and let b be an element of F that is integral over A, so that there is a monic polynomial f in $A[x]$ such that $f(b) = 0$. There are elements p and q in A such that $q \neq 0$, $b = p/q$, and $1 \in \gcd\{p, q\}$, and the *Rational Root Theorem* A.8.14 tells us that q divides the leading coefficient of f, which is 1. Of course, this implies that q is a unit of A and b and element of A. □

Using this proposition we can exhibit important examples of normal domains.

Corollary A.9.4. *The algebra $\Bbbk[x_1, \ldots, x_n]$ is a normal domain.*

Proof. Indeed, it is, according to Proposition A.6.20 a unique factorization domain, so a GCD domain. □

Let us now give examples of rings that are *not* normal.

Example A.9.5. Let us consider the subring $A \coloneqq \mathbb{Q}[t^2, t^3]$ of $\mathbb{Q}[t]$ generated by the monomials t^2 and t^3. This is clearly an integral domain and since $t^2/t^3 = t$, the field of fractions of A is $\mathbb{Q}(t)$. The element t of $\mathbb{Q}(t)$ is a root of the monic polynomial $x^2 - t^2 \in A[x]$, it is integral over A. It is clear, though, that t does not belong to A, so the domain A is not normal.

Example A.9.6. Let us now consider the subring $A \coloneqq \mathbb{Q}[\sqrt{5}]$ of $\mathbb{C}$, whose field of fractions can be identified with the field $\mathbb{Q}(\sqrt{-5})$. The element $a \coloneqq (1+\sqrt{5})/2$ of that field manifestly does not belong to A, yet it is a root of the monic polynomial $x^2 - x - 1$ of $A[x]$, and this shows that the ring A is not normal.

The condition that we used to define integrality is not very convenient in practice to show that an element is actually integral. The following proposition gives two more useful conditions.

Proposition A.9.7. *Let B be a ring, let A be a subring of B, and let b be an element of B. The following statements are equivalent:*

(*a*) *The element b is integral over B.*

(*b*) *The subring $A[b]$ of B is a finitely generated A-module.*

(*c*) *The subring $A[b]$ is contained in a subring C of B that is finitely generated as a B-module.*

Proof. (*a*) $\Rightarrow$ (*b*) We are supposing here that there is a monic element f of $A[x]$ such that $f(b) = 0$, so that there are then a positive integer d and elements $a_0, \dots, a_{d-1}$ of A such that $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$, and we have that

$$b^d = -\sum_{i=0}^{d-1} a_i b^i. \tag{A.13}$$

Let M be the A-submodule $\langle 1, b, \dots, b^{d-1}\rangle$ of B, which is manifestly finitely generated. We have that $M \subseteq A[b]$, and to prove what we want we will show that we in fact have here an equality. As $A[b]$ is generated as an A-module by the set $\{b^j : j \in \mathbb{N}_0\}$, to do that we need only show that $b^j \in M$ for all j in $\mathbb{N}_0$. This is clear if $j < d$, of course. On the other hand, if j is an integer such that $j \geq d$ and we know that $b^k \in M$ for all k in $[\![0, j-1]\!]$, then the equality (A.13) implies that

$$b^j = b^{j-d}b^d = -b^{j-d}\sum_{i=0}^{d-1} a_i b^i = -\sum_{i=0}^{k-1} a_i b^{j-d+i} \in M$$

because $j - d + i \in [\![0, j-1]\!]$ whenever $i \in [\![0, d-1]\!]$. The result we want thus follows by induction.

(*b*) $\Rightarrow$ (*c*) This is clear, as we can simply put $C \coloneqq A[b]$.

(*c*) $\Rightarrow$ (*a*) Let us suppose that there is a subring C of B such that $C \supseteq A[b]$ and that is finitely generated as an A-module, so that there are elements $c_1, \dots, c_n$ in C such that $C = \sum_{i=1}^n Ac_i$. Since b is in C and C is a subring of B, for each j in $[\![n]\!]$ there are elements $a_{1,j}, \dots, a_{n,j}$ in A such that $bc_j = \sum_{i=1}^n a_{i,j}c_i$. Let M be the matrix $(a_{i,j})$ in $\mathrm{M}_n(A)$, and let us consider the three maps

$$\lambda_M \colon v \in A^n \mapsto Mv \in A^n, \qquad \lambda_c \colon c \in C \mapsto bc \in C, \qquad \mu \colon (v_1, \dots, v_n) \in A^n \mapsto \sum_{i=1}^n v_i c_i.$$

The square

$$\begin{array}{ccc} A^n & \xrightarrow{\lambda_M} & A^n \\ {\scriptstyle\mu}\downarrow & & \downarrow{\scriptstyle\mu} \\ C & \xrightarrow{\lambda_b} & C \end{array}$$

since for each element $v = (v_1, \dots, v_n)$ of A^n we have that

$$\lambda_b(\mu(v)) = \lambda_b\left(\sum_{j=1}^{n} v_j c_j\right) = \sum_{j=1}^{n} v_j b c_j = \sum_{i=1}^{n}\sum_{j=1}^{n} v_j a_{i,j} c_i = \sum_{j=1}^{n}\left(\sum_{i=1}^{n} a_{i,j} v_j\right) c_j = \mu(\lambda_M(v)).$$

Let now $f \in A[x]$ be the characteristic polynomial of M. The *Cayley–Hamilton Theorem* tells us that f is a monic polynomial of degree n such that $f(M) = 0$, and this implies that also $f(\lambda_M) = 0$. Since 1 is an element of C, there is an element $v = (v_1, \dots, v_n)$ in A such that $1 = \sum_{i=1}^{n} v_i c_i = \mu(v)$, and for each k in $\mathbb{N}_0$ we have that $b^k = b^k 1 = \lambda_b^k(\mu(v)) = \mu(\lambda_M(v))$, so that $f(b) = f(b)1 = \mu(f(\lambda_M)(v)) = 0$. We thus see that b is integral over A. □

The implication $(a) \Rightarrow (b)$ of this proposition has the following useful generalization.

Corollary A.9.8. *Let B be a ring, and let A be a subring of B. If $b_1, \dots, b_n$ are elements of B that are integral over A, then the subring $A[b_1, \dots, b_n]$ of B is a finitely generated A-module and integral over A.*

Proof. Because of the implication $(c) \Rightarrow (a)$ of Proposition A.9.7, we need only prove that the subring $A[b_1, \dots, b_n]$ is finitely generated as an A-module, and we do this by induction with respect to n. When n is 0 there is nothing to prove, of course. Let us then suppose that n is a positive integer and, inductively, that the subring $A' \coloneqq A[b_1, \dots, b_{n-1}]$ of B is finitely generated as an A-module. Since b_n is integral over A, it is integral over A', and the implication $(a) \Rightarrow (b)$ of Proposition A.9.7 tells us that $A'[b_n]$, which coincides with $A[b_1, \dots, b_n]$, is a finitely generated A'-module. We can therefore conclude that $A[b_1, \dots, b_n]$ is finitely generated as an A-module thanks to the result of Exercise A.9.9 below. □

Exercise A.9.9. Let C be a ring, and let A and B be subrings of C such that $A \subseteq B$. Show that if B is finite generated as an A-module, and C is finitely generated as a B-module, then C is finitely generated as an A-module. We refer to this result as the *transitivity of finite generation*.

Armed with the criterion for integrality given by Proposition A.9.7, we can easily establish the main properties of integral dependence. The first of them, the following proposition, is usually referred to as the *transitivity of integral dependence*.

Proposition A.9.10. *Let C be a ring, and let A and B be subrings of C such that $A \subseteq B$. If B is integral over A and C is integral over B, then C is integral over A.*

Proof. Let us suppose that B is integral over A and that C is integral over B, and let c be an element of C. Since c is integral over B, there is a monic polynomial f in $B[x]$ such that $f(c) = 0$, and there are then a positive integer k and elements $b_0, \dots, b_{k-1}$ in B such that $f = x^k + \sum_{i=0}^{k-1} b_i x^i$. As the elements $b_0, \dots, b_{k-1}$ are integral over A, we know from Corollary A.9.8 that the subring $B' \coloneqq A[b_0, \dots, b_{k-1}]$ of B is a finitely generated A-module. Since the polynomial f belongs to $B'[x]$, the element c is integral over B', and thus the ring $B'[c]$ is finitely generated as a B'-module. According to the result of Exercise A.9.9, the ring $B'[c]$ is then also finitely generated as an A-module and, as it contains $A[c]$, we can conclude from the implication $(c) \Rightarrow (a)$ of Proposition A.9.7 that c is integral over A. This is true for all elements c of C, so the ring C itself is integral over A. □

Another key fact that we can prove using Proposition A.9.7 is that the integral closure of a ring is a ring.

Proposition A.9.11. *Let B be a ring, and let A be a subring of B. The integral closure of A in B is a subring of B that is integrally closed in B.*

Proof. Let $\overline{A}$ be the integral closure of A in B. If x and y are two elements of $\overline{A}$, then Corollary A.9.8 tells us that the subring $A[x, y]$ of B is integral over A, so that, in particular, its elements $x - y$ and xy are integral over A and thus belong to $\overline{A}$. Since certaint 1 belongs to $\overline{A}$, this lets us conclude that $\overline{A}$ is a subring of B.

If b is an element of B that is integral over $\overline{A}$, then the subring $\overline{A}[b]$ of B is integral over $\overline{A}$ by Corollary A.9.8 and the transitivity of integral dependence established in Proposition A.9.10 implies that $\overline{A}[b]$ is integral over A, so that b is integral over A and thus belongs to $\overline{A}$. This shows that the subring $\overline{A}$ is integrally closed in B. □

The construction of integral closures is a rather important tool in several areas of mathematics. For example, if F is an ***algebraic number field***, that is, a finite extension of $\mathbb{Q}$, then the integral closure $\mathcal{O}_F$ of $\mathbb{Z}$ in F is what we call the ring of ***algebraic integers*** of F. The study of the rings of numbers that arise in this way is an important part of number theory.

Example A.9.12. Let D be an integer different from 0 and 1 and that is square-free, that is, that is not divisible by a square other than 1, and let us consider the field $F \coloneqq \mathbb{Q}(\sqrt{D})$.

Let z be an element of $\mathbb{Q}(\sqrt{D})$ that is integral over $\mathbb{Z}$, and let a and b be the elements of $\mathbb{Q}$ such that $z = a + b\sqrt{D}$. If b is zero, then in fact z is in $\mathbb{Q}$ and we know from Example A.9.2 that a

is an integer. Let us then suppose that b is not zero. In that case, no polynomial in $\mathbb{Q}[x]$ of degree 1 vanishes on z, and the polynomial $f \coloneqq x^2 - 2ax + (a^2 - b^2D)$ of $\mathbb{Q}[x]$ does, and divides in $\mathbb{Q}[x]$ an polynomial that has z as a root. Since there is a monic element of $\mathbb{Z}[x]$ that has z as a root and it is therefore divisible by f, *Gauss's Lemma* tells us that f has coefficients in $\mathbb{Z}$, that is, that $2a \in \mathbb{Z}$ and $a^2 - b^2D \in \mathbb{Z}$.

If the integer $2a$ is even, then a is in $\mathbb{Z}$ and since $a^2 - b^2D$ is an integer and D is square-free, we also have that $b \in \mathbb{Z}$. Let us suppose for a moment that the integer $2a$ is odd, so that there is an integer c such that $2a = 2c + 1$ and

$$e \coloneqq \frac{1 - 4b^2D}{4} = a^2 - b^2D - c^2 - c \in \mathbb{Z}. \tag{A.14}$$

Let r and s be coprime integers such that $b = r/s$ and $s > 0$, so that $4r^2D = s^2(1 - 4e)$. This equality implies that the square of any odd prime divisor of s divides D, so s is a power of 2, the same equality then implies that s is, in fact, either 1 or 2, and it cannot be 1 because of (A.14). There is an integer d such that $b = (2d + 1)/2$, so that

$$z = a + b\sqrt{D} = \frac{2c + 1}{2} + \frac{2d + 1}{2}\sqrt{D} = (c - d) + (2d + 1)\frac{1 + \sqrt{D}}{2} \in \mathbb{Z}\left[\frac{1 + \sqrt{D}}{2}\right].$$

and $D \equiv 1 \mod 4$ because

$$c^2 + c - d^2D - dD + \frac{1 - D}{4} = \frac{(2c + 1)^2 - (2d + 1)^2D}{4} = a^2 - b^2D \in \mathbb{Z}.$$

We have shown that

> *if a and b are elements of $\mathbb{Q}$ such that $z = a + b\sqrt{D}$ is integral over $\mathbb{Z}$, then either $z \in \mathbb{Z}[\sqrt{D}]$ or $D \equiv 1 \mod 4$ and $z \in \mathbb{Z}[(1 + \sqrt{D})/2]$.* (A.15)

Let us write $\mathcal{O}$ for the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{D})$. If the integer D is such that $D \not\equiv 1 \mod 4$, then our observation (A.15) implies that $\mathcal{O} \subseteq \mathbb{Z}[\sqrt{D}]$ and, since $\sqrt{D}$ is in $\mathcal{O}$ because it is a root of the polynomial $x^2 - D$, we in fact have that $\mathcal{O} = \mathbb{Z}[\sqrt{D}]$ in this case. If instead $D \equiv 1 \mod 4$, then (A.15) tells us that $\mathcal{O} \subseteq \mathbb{Z}[(1 + \sqrt{D})/2]$ and since $(1 + \sqrt{D})/2$ is a root of the polynomial $x^2 - x + (1 - d)/4$, which has integer coefficients, we have equality also in this case. We can therefore conclude from all this that

> *the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{D})$ is $\mathbb{Z}[\omega]$, with* $\omega = \begin{cases} \sqrt{D} & \text{if } D \not\equiv 1 \mod 4; \\ \dfrac{1 + \sqrt{D}}{2} & \text{if } D \equiv 1 \mod 4. \end{cases}$

Exercise A.9.13. Show that the example (A.6) given by Theodore Motzkin of a principal ideal domain that is not Euclidean is in fact the ring of algebraic integers in the field $\mathbb{Q}(\sqrt{-19})$.

When a ring is integral over one of its subrings, there are many properties of one that are reflected on the other. A simple example of this phenomenon is given by the following proposition.

Proposition A.9.14. *Let B be an integral domain, and let A be a subring of B over which B is integral. The ring B is a field if and only if the ring A is field.*

Proof. Let us suppose first that B is a field and that it is integral over A, and let a be a non-zero element of A, so that we can consider the inverse a^{-1} of a in B. Since B is integral over A, there is a monic polynomial f in $A[x]$ such that $f(a^{-1}) = 0$. Let n be the degree of f, and let $a_0, \ldots, a_{n-1}$ be the elements of A such that $f = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$. We then have that

$$\begin{aligned} 0 = f(a^{-1})a^{n-1} &= (a_0 + a_1 a^{-1} + \cdots + a_{n-1}a^{-n+1} + a^{-n})a^{n-1} \\ &= a_0 a^{n-1} + a_1 a^{n-2} + \cdots + a_{n-1} + a^{-1}, \end{aligned}$$

so that, in fact, $a^{-1} = -(a_0 a^{n-1} + a_1 a^{n-2} + \cdots + a_{n-1})$ is an element of A. This shows that A is a field, and thus that the condition given in the proposition is necessary.

Let us now suppose that the ring A is a field, and let b be a non-zero element of B. There are then a positive integer n and elements $a_0, \ldots, a_{n-1}$ in A such that b is a root of the polynomial $f \coloneqq a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ of $A[x]$, and we can in fact suppose that the number n is minimal with respect to this condition. This minimality implies that a_0 is not zero, for otherwise b would be a root of the polynomial $a_1 + a_2 x + \cdots + a_{n-1}x^{n-2} + x^{n-1}$ of $A[x]$ because B is a domain. As

$$b(a_1 + a_2 b + \cdots + a_{n-1}b^{n-2} + b^{n-1}) = -a_0$$

and a_0 is a unit of B, we see that b is invertible in B. □

A.10. Normalization

The second result from commutative algebra that we need is the so called *Normalization Lemma* of Emmy Noether [Noe1926], which is Proposition A.10.2 below. This result tells us that finitely generated algebras over a field are not really that complicated: they contain a relatively large and well-understood subalgebra, a polynomial algebra, over which they are finitely generated modules. We will see later that it also provides useful geometric information — for example, it plays an important role in the development of the idea of dimension.

We start with the following straightforward auxiliary lemma.

Lemma A.10.1. *Let us suppose that the field $\Bbbk$ is infinite, and let f be a non-zero homogeneous element of $\Bbbk[x_1, \ldots, x_n]$. There are scalars $t_1, \ldots, t_{n-1}$ in $\Bbbk$ such that $f(t_1, \ldots, t_{n-1}, 1) \neq 0$.*

Proof. We proceed by induction with respect to the non-negative integer n, noting that when n is 0 there is nothing to prove. Let us then suppose that n is a positive integer, let d be the degree of f, and let $f_0, \ldots, f_d$ be the elements of $\Bbbk[x_2, \ldots, x_n]$ such that $f = \sum_{i=0}^{d} f_i x_1^i$. There is an element j of $[\![0, d]\!]$ such that $f_j \neq 0$, because $f \neq 0$, and since f_j is then a non-zero homogeneous element of $\Bbbk[x_2, \ldots, x_n]$ of degree $d - j$, the obvious inductive hypothesis allows us to conclude that there are scalars $s_2, \ldots, s_{n-1}$ in $\Bbbk$ such that $f_j(s_2, \ldots, s_{n-1}, 1) \neq 0$. It follows from this that $f(x_1, s_2, \ldots, s_{n-1}, 1)$ is a non-zero element of $\Bbbk[x_1]$ and, as the field $\Bbbk$ is infinite, there is a scalar s_1 in $\Bbbk$ such that $f(s_1, s_2, \ldots, s_{n-1}, 1) \neq 0$. This completes the induction, and thus the proof of the lemma. □

With this lemma at hand, we can prove the Normalization Lemma. We will only state it and prove in the case in which the ground field $\Bbbk$ is infinite, but exactly the same is true when the field is finite — a different proof is required, though. We refer to the discussion in David Eisenbud's book [Eis1995], where the full version of this result is Theorem 13.1.

Proposition A.10.2. *Let us suppose that the field $\Bbbk$ is infinite, and let A be a finitely generated algebra. There exist a non-negative integer d and elements $y_1, \ldots, y_d$ of A such that*

- *the elements $y_1, \ldots, y_d$ are algebraically independent, and*
- *the algebra A is integral over its subalgebra $\Bbbk[y_1, \ldots, y_d]$.*

Proof. There exist a non-negative integer n and pairwise different elements $a_1, \ldots, a_n$ of A such that A is generated as an algebra by the set $S \coloneqq \{a_1, \ldots, a_n\}$. We will prove the claim of the proposition proceeding by induction with respect to the integer n.

If the elements $a_1, \ldots, a_n$ are algebraically independent, then clearly the claim of the proposition is true, as we can simply take $k = n$ and $y_i = a_i$ for each $i \in [\![n]\!]$. Let us suppose then that the elements $a_1, \ldots, a_n$ are not algebraically independent, so that there is a non-constant polynomial f in $\Bbbk[x_1, \ldots, x_n]$ such that $f(a_1, \ldots, a_n) = 0$. Let r be the total degree of f, and for each $i \in [\![0, r]\!]$ let f_i be the homogeneous component of degree i in f, so that we have $f = f_r + \cdots + f_0$.

Let $t_1, \ldots, t_{n-1}$ be elements of $\Bbbk$. If $k_1, \ldots, k_n$ are non-negative integers, then the leading term of the polynomial

$$(x_1 + t_1 x_n)^{k_1} \cdots (x_{n-1} + t_{n-1} x_n)^{k_{n-1}} x_n^{k_n},$$

viewed as an element of $\Bbbk[x_1, \ldots, x_{n-1}][x_n]$, is

$$t_1^{k_1} \cdots t_{n-1}^{k_{n-1}} \cdot x_n^{k_1 + \cdots + k_{n-1} + k_n}.$$

This implies that the leading term of the polynomial

$$f(x_1 + t_1 x_n, \ldots, x_{n-1} + t_{n-1} x_n, x_n),$$

viewed as an element of $\Bbbk[x_1, \ldots, x_{n-1}][x_n]$, is

$$f_d(t_1, \ldots, t_{n-1}, 1) \cdot x_n^d.$$

It follows from Lemma A.10.1 that we can choose the scalars $t_1, \ldots, t_{n-1}$ in $\Bbbk$ in such a way that the scalar $s \coloneqq f_d(t_1, \ldots, t_{n-1}, 1)$ is not zero, and therefore the polynomial

$$g(x_1, \ldots, x_n) \coloneqq s^{-1} \cdot f(x_1 + t_1 x_n, \ldots, x_{n-1} + t_{n-1} x_n, x_n),$$

viewed as an element of $\Bbbk[x_1, \ldots, x_{n-1}][x_n]$, is monic of degree d.

For each i in $[\![n-1]\!]$ let us put $a'_i \coloneqq a_i - t a_n$. It is clear that $A = \Bbbk[a'_1, \ldots, a'_{n-1}, a_n]$, and A is integral over its subalgebra $A' \coloneqq \Bbbk[a'_1, \ldots, a'_{n-1}]$ because

$$g(a'_1, \ldots, a'_{n-1}, x)$$

is a monic element of $A'[x]$ whose value at a_n is

$$\begin{aligned} g(a'_1, \ldots, a'_{n-1}, a_n) &= s^{-1} \cdot f(a'_1 + t_1 a_n, \ldots, a'_{n-1} + t_{n-1} a_n, a_n) \\ &= s^{-1} \cdot f(a_1, \ldots, a_{n-1}, a_n) \\ &= 0. \end{aligned}$$

Now the algebra A' can manifestly be generated by $n-1$ elements, so we inductively can suppose that there are a non-negative integer d and elements $y_1, \ldots, y_d$ in A' that are algebraically independent and such that A' is integral over its subalgebra $\Bbbk[y_1, \ldots, y_d]$. In view of the transitivity of integral dependence, we see that A itself is integral over its subalgebra $\Bbbk[y_1, \ldots, y_d]$, and this completes the induction and the proof of the proposition. □

A.11. The *Nullstellensatz*

Here we will finally state and prove the *Nullstellensatz* or, rather, several versions of that result. The first one is the following result, usually known as *Zariski's Lemma*, because Zariski used it in [Zar1947] to prove the *Nullstellensatz*, just as we will do here.

Proposition A.11.1. *Let us suppose that the field $\Bbbk$ is infinite. A finitely generated algebra that is a field is in fact a finite algebraic extension of $\Bbbk$.*

This is also true when the ground field $\Bbbk$ is finite, and to prove that we need a version of the *Normalization Lemma* A.10.2 for finite ground fields.

Proof. Let B be a finitely generated algebra that is a field. According to the *Normalization Lemma* A.10.2, there are a non-negative integer d and elements $b_1, \dots, b_d$ of B that are algebraically independent over $\Bbbk$ and such that B is integral over its subalgebra $A \coloneqq \Bbbk[b_1, \dots, b_d]$. According to Proposition A.9.14, this subalgebra A is a field, and this implies that $d = 0$. This means that the field B is generated by finitely many elements each of which is algebraic over $\Bbbk$, so that it is a finite algebraic extension of $\Bbbk$. □

The most important case of this proposition is the following result.

Corollary A.11.2. *Let us suppose that the field $\Bbbk$ is algebraically closed. If A is a finitely generated algebra that is a field, then $A = \Bbbk$.*

Proof. Since the field $\Bbbk$ is algebraically closed, it is infinite, so a finitely generated algebra that is a field is, according to Proposition A.11.1, a finite algebraic extension of $\Bbbk$ and thus equal to $\Bbbk$ itself. □

Using this we can easily give a description of all maximal ideals of polynomial rings over algebraically closed fields.

Corollary A.11.3. *Let us suppose that the field $\Bbbk$ is algebraically closed, let n be a non-negative integer, and let $A \coloneqq \Bbbk[x_1, \dots, x_n]$.*

(i) If $a = (a_1, \dots, a_n)$ is an element of $\Bbbk^n$, then $\mathfrak{m}_a \coloneqq \langle x_1 - a_1, \dots, x_n - a_n \rangle$ is a maximal ideal of A whose elements are precisely the elements of A that vanish on a.

(ii) If $\mathfrak{m}$ is a maximal ideal of A, then there exists exactly one element a of $\Bbbk^n$ such that $\mathfrak{m} = \mathfrak{m}_a$.

Proof. (*i*) Let $a = (a_1, \dots, a_n)$ be an element of $\Bbbk^n$, let us consider the ideal $\mathfrak{m}_a$ of A described in the statement of the corollary, and let $\phi\colon f \in A \mapsto f(a) \in \Bbbk$ be the morphism of algebras given by evaluation at a. Since $\phi(x_i - a_i) = 0$ for each i in $[\![n]\!]$, we have that $\mathfrak{m}_a \subseteq \ker \phi$. As $\phi(1) \neq 0$, we see that $1 \notin \ker \phi$ and thus that $\mathfrak{m}_a \subsetneq A$.

On the other hand, the quotient $A/\mathfrak{m}_a$ is generated as an algebra by the classes of $x_1, \dots, x_n$ modulo $\mathfrak{m}_a$, and those classes are the same as the classes of $a_1, \dots, a_n$, which are in $\Bbbk$. It follows from this that $A/\mathfrak{m}_a$ is actually equal to $\Bbbk$, so a field, and therefore that the ideal $\mathfrak{m}_a$ is maximal. In particular, we have that $\mathfrak{m}_a = \ker \phi$, so that the elements of $\mathfrak{m}_a$ are precisely the elements of A that vanish on a.

(*ii*) Let $\mathfrak{m}$ be a maximal ideal of A. The quotient $A/\mathfrak{m}$ is then a field that is finitely generated as an algebra over $\Bbbk$, so Corollary A.11.2 tells us that $A/\mathfrak{m} = \Bbbk$. In particular, for each i in $[\![n]\!]$

there is an element a_i of $\Bbbk$ such that $x_i \equiv a_i \mod \mathfrak{m}$, and this implies that the ideal $\mathfrak{m}$ contains the ideal $\mathfrak{m}_a$. As $\mathfrak{m} \neq A$ and $\mathfrak{m}_a$ is maximal, we then have that $\mathfrak{m} = \mathfrak{m}_a$.

Let now $b = (b_1, \dots, b_n)$ be an element of $\Bbbk^n$ that is different from a, so that there is an element j of $[\![n]\!]$ such that $b_j \neq a_j$. The polynomial $x_i - b_j$, which is in $\mathfrak{m}_b$, then does not vanish on the point a, and this means that it does belong to $\mathfrak{m}_a$. We see with this that $\mathfrak{m}_b \neq \mathfrak{m}_a$, and this proves the uniqueness claim made in (*ii*). □

This corollary, in turn, implies that proper ideals of $\Bbbk[x_1, \dots, x_n]$ have common zeroes in $\Bbbk^n$.

Corollary A.11.4. *Let us suppose that the field $\Bbbk$ is algebraically closed. If I is a proper ideal of $\Bbbk[x_1, \dots, x_n]$, then there is a point a of $\Bbbk^n$ such that $f(a) = 0$ for all elements f of I.*

Let us remark that this corollary specializes to the following higher-dimension version of the condition of algebraic closedness:

> *if the field $\Bbbk$ is algebraically closed and f is non-constant element of $\Bbbk[x_1, \dots, x_n]$,*
> *then there is a point p in $\mathbb{A}^n$ such that $f(p) = 0$.*

Indeed, this follows immediately from the corollary by considering the ideal $\langle f \rangle$ generated by f.

Proof. Let I be a proper ideal of $\Bbbk[x_1, \dots, x_n]$. Since it is proper, there is a maximal ideal $\mathfrak{m}$ of $\Bbbk[x_1, \dots, x_n]$ such that $I \subseteq \mathfrak{m}$ and, according to Corollary A.11.3, there is a point $a = (a_1, \dots, a_n)$ in $\Bbbk^n$ such that $\mathfrak{m}$ coincides with the ideal $\mathfrak{m}_a$ of all elements of $\Bbbk[x_1, \dots, x_n]$ that vanish on a. This implies, of course, that all the elements of I vanish on a. □

We can rephrase this last corollary as a purely algebraic statement.

Corollary A.11.5. *Let us suppose that the field $\Bbbk$ is infinite, and let A be a finitely generated algebra. If I is a proper ideal of A, then*

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{m} \in \operatorname{Spm} A \\ I \subseteq \mathfrak{m}}} \mathfrak{m}.$$

We need that the field $\Bbbk$ be infinite here in order to be able to use Proposition A.11.1. As we said, that proposition is also true when $\Bbbk$ is finite, so the same is true of this corollary.

Proof. Let I be a proper ideal of A, and let us write J for the intersection appearing in the statement of the corollary. If $\mathfrak{m}$ is a maximal ideal of A that contains I, then $\mathfrak{m}$ is prime and Proposition **??** tells us that $\sqrt{I} \subseteq \mathfrak{m}$: this shows that $\sqrt{I} \subseteq J$.

Let now f be an element of A that does not belong to $\sqrt{I}$, so that I is disjoint from the multiplicatively closed subset $S \coloneqq \{f^n : n \in \mathbb{N}_0\}$ of A. Let G be a finite subset of A that generates it as an algebra: then the set $Y \coloneqq \{g/1 : g \in G\} \cup \{1/f\}$ generates the algebra A_S, which is therefore

finitely generated.

According to *Krull's Separation Lemma* A.6.15, there is a prime ideal $\mathfrak{p}$ of A such that $I \subseteq \mathfrak{p}$, $\mathfrak{p} \cap S = \varnothing$, and $\mathfrak{p}_S$ is a maximal ideal in A_S. The quotient $A_S/\mathfrak{p}_S$ is a field, and it is finitely generated as an algebra, because A_S is. Proposition A.11.1, the field $A_S/\mathfrak{p}_S$ is a finite algebraic extension of $\Bbbk$ and, in view of Corollary A.9.8, integral over $\Bbbk$. There is a canonical isomorphism $(A/\mathfrak{p})_S \to A_S/\mathfrak{p}_S$ so, of course, $(A/\mathfrak{p})_S$ is integral over $\Bbbk$. Since the ideal $\mathfrak{p}$ is prime and therefore the quotient $A/\mathfrak{p}$ is a domain, the localization map $A/\mathfrak{p} \to (A/\mathfrak{p})_S$ is injective, so we can view it as an inclusion. As we then have inclusions $\Bbbk \subseteq A/\mathfrak{p} \subseteq (A/\mathfrak{p})_S$, the ring $(A/\mathfrak{p})_S$ is integral over $A/\mathfrak{p}$: since it is a field, Proposition A.9.14 tells us that $A/\mathfrak{p}$ is a field and, thus, the ideal $\mathfrak{p}$ is maximal. As $f \notin \mathfrak{p}$, we can conclude that $f \notin J$. This proves that $J \subseteq \sqrt{I}$ and, as a consequence, the corollary. □

Motivated by this result, Wolfgang Krull made in [Kru1951] and [Kru1952] the following definition.

Definition A.11.6. A ring is a ***Jacobson ring*** if every prime ideal is an intersection of maximal ideals.

This rings were also studied by Oscar Goldman in [Gol1951] — he calls them ***Hilbert rings***.

Since every prime ideal is radical, Corollary A.11.5 immediately implies that

Corollary A.11.7. *Let us suppose that the field $\Bbbk$ is infinite. Every finitely generated algebra is a Jacobson ring.* □

Bibliography

[AG2026] Nicolás Allo-Gómez. Other examples of principal ideal domains that are not euclidean domains. *The American Mathematical Monthly*, pages 1–8, 2026. doi:10.1080/00029890.2026.2673805.

[AÖ2001] Ahmet Göksel Ağargün and Erdoğan Mehmet Özkan. A historical survey of the fundamental theorem of arithmetic. *Historia Mathematica*, 28(3):207–214, 2001. doi:10.1006/hmat.2001.2318.

[Cám1988] Oscar A. Cámpoli. A principal ideal domain that is not a Euclidean domain. *Amer. Math. Monthly*, 95(9):868–871, 1988. doi:10.2307/2322908.

[Con1973] John B. Conway. *Functions of one complex variable*, volume 11 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1973.

[Eis1850] Gotthold Eisenstein. über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt. *J. Reine Angew. Math.*, 39:160–179, 1850. doi:10.1515/crll.1850.39.160.

[Eis1995] David Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry. doi:10.1007/978-1-4612-5350-1.

[Gol1951] Oscar Goldman. Hilbert rings and the Hilbert Nullstellensatz. *Math. Z.*, 54:136–140, 1951. doi:10.1007/BF01179855.

[Hel1940] Olaf Helmer. Divisibility properties of integral functions. *Duke Math. J.*, 6:345–356, 1940. URL: http://projecteuclid.org/euclid.dmj/1077491905.

[Hil1890] David Hilbert. Ueber die Theorie der algebraischen Formen. *Math. Ann.*, 36(4):473–534, 1890. doi:10.1007/BF01208503.

[Jod1967] Max A. Jodeit, Jr. Uniqueness in the division algorithm. *Amer. Math. Monthly*, 74:835–836, 1967. doi:10.2307/2315810.

[Kap1970] Irving Kaplansky. *Commutative rings*. Allyn and Bacon, Inc., Boston, MA, 1970.

[Kru1928] Wolfgang Krull. Zur Theorie der zweiseitigen Ideale in nichtkommutativen Bereichen. *Math. Z.*, 28(1):481–503, 1928. doi:10.1007/BF01181179.

[Kru1951] Wolfgang Krull. Jacobsonsche Ringe, Hilbertscher Nullstellensatz, Dimensionstheorie. *Math. Z.*, 54:354–387, 1951. doi:10.1007/BF01238035.

[Kru1952] Wolfgang Krull. Jacobsonsches Radikal und Hilbertscher Nullstellensatz. In *Proceedings of the International Congress of Mathematicians, Cambridge, Mass., 1950, vol. 2*, pages 56–64. Amer. Math. Soc., Providence, RI, 1952.

[Mot1949] Theodore Motzkin. The Euclidean algorithm. *Bull. Amer. Math. Soc.*, 55:1142–1146, 1949. doi:10.1090/S0002-9904-1949-09344-8.

[Nag1957] Masayoshi Nagata. A remark on the unique factorization theorem. *J. Math. Soc. Japan*, 9:143–145, 1957.

[Noe1926] Emmy Noether. Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p. *Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl.*, 1926:28–35, 1926. URL: https://eudml.org/doc/59193.

[OEI2026] OEIS Foundation Inc. The on-line encyclopedia of integer sequences. Published electronically at https://oeis.org, 2026.

[Rem1998] Reinhold Remmert. *Classical topics in complex function theory*, volume 172 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1998. Translated from the German by Leslie Kay. doi:10.1007/978-1-4757-2956-6.

[Rha1962] Tong-Shieng Rhai. Mathematical Notes: A Characterization of Polynomial Domains Over a Field. *Amer. Math. Monthly*, 69(10):984–986, 1962. doi:10.2307/2313196.

[Sam1963] Pierre Samuel. *Anneaux factoriels*. Sociedade de Matemática de São Paulo, São Paulo, 1963. Rédaction de Artibano Micali.

[Sch1846] Theodor Schönemann. Von denjenigen Moduln, welche Potenzen von Primzahlen sind.(Fortsetzung). *J. Reine Angew. Math.*, 32:93–105, 1846. doi:10.1515/crll.1846.32.93.

[Ser1953] Jean-Pierre Serre. Groupes d'homotopie et classes de groupes abéliens. *Ann. of Math. (2)*, 58:258–294, 1953.

[Wil1973] Jack C. Wilson. A principal ideal ring that is not a Euclidean ring. *Math. Mag.*, 46:34–38, 1973. doi:10.2307/2688577.

[Zar1947] Oscar Zariski. A new proof of Hilbert's Nullstellensatz. *Bull. Amer. Math. Soc.*, 53:362–368, 1947. doi:10.1090/S0002-9904-1947-08801-7.

Notations

People

Index