LECTURE NOTES FOR COMMUTATIVE ALGEBRA, FEBRUARY - APRIL 2023

ANDREA BIANCHI

Abstract. These are the lecture notes for the course "Commutative Algebra" held at the University of Copenhagen between February and April 2023 (blok 3). We refer by [Bos] to the book "S.Bosch, *Algebraic Geometry and Commutative Algebra*, *Springer*, 2013"; many of the arguments contained in these notes are taken from this source. If you spot any mistakes, I would be glad to correct them; so please let me know!

Contents

Date: March 22, 2023.

1. Rings and ring homomorphisms

Since childhood, we have learnt how useful numbers can be in life. The reason for this is that, besides representing "quantities" from the real world, numbers can be combined and manipulated through "operations", allowing "computations" which in turn allow us to make predictions about the reality around us. Two of the most useful operations are the binary operations of "sum" and of "product"; the notion of "ring" arises by abstracting the idea of a set with two such operations, without requiring anymore that the elements of this set correspond to "quantities" in any way.

1.1. **Definition of rings and first examples.**

Definition 1.1. A *ring* R is a set endowed with the following structure:

- two binary operations, i.e. functions $R \times R \to R$, denoted $+\colon R \times R \to R$ and called *sum* and $\cdot\colon R \times R \to R$ and called *product*, and sending a pair $(a, b) \in R \times R$ to an element of R that is denoted $a+b \in R$ and, respectively, $a \cdot b \in R$;
- a special element, denoted $1 \in R$ and called the *multiplicative neutral element*,

satisfying the following properties:

- $(R, +)$ is an abelian group, i.e. the following hold:
  Associativity: for all $a, b, c \in R$ we have $a + (b + c) = (a + b) + c$;
  Commutativity: for all $a, b \in R$ we have $a + b = b + a$;
  Existence of 0: there exists a (unique) element of R, denoted from now on $0 \in R$, such that for all $a \in R$ we have $a + 0 = 0 + a = a$;
  Existence of additive inverses: for all $a \in R$ there is a (unique) element of R, denoted $-a \in R$, such that $a + (-a) = (-a) + a = 0$;
- $(R, \cdot, 1)$ is an associative monoid, i.e. the following hold:
  Associativity: for all $a, b, c \in R$ we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
  1 is neutral: for all $a \in R$ we have $a \cdot 1 = 1 \cdot a = a$;
- the product is distributive with respect to the sum, i.e. for all $a, b, c \in R$ we have $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ and $c \cdot (a + b) = (c \cdot a) + (c \cdot b)$.

A ring R is called *commutative* if moreover the following property holds:

Commutativity of product: for all $a, b \in R$ we have $a \cdot b = b \cdot a$.

We usually denote a ring as a tuple $(R, +, \cdot, 1)$, or whenever there is no reasonable doubt about what additional structure is meant, just as the underlying set R. When

dealing with several rings at the same time we might stress the structure of a ring R by writing $+_R, \cdot_R$ and 1_R.
In Definition 1.1 we use parentheses () just to make clear, as usual, in which order the operations have to be made. The study of commutative rings, i.e. those in which not only the sum, but also the product is commutative, is simpler, and this will be the focus in the entire course; for this reason, we will **from now on always assume that our rings are commutative, and just use the word "ring" to mean "commutative ring"**; but be careful when you read the literature, because "ring" is often used with the meaning of Definition 1.1.

Example 1.2. The set of natural numbers $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is endowed with an element $1 \in \mathbb{N}$ and the two usual operations of sum and product; however the sum doesn't make $\mathbb{N}$ into an abelian group, since for every $a \neq 0$ there is no additive inverse "$-a$" in $\mathbb{N}$. It follows that the set $\mathbb{N}$, with the given structure, is *not* an example of a ring.
Humanity has solved this problem by introducing $\mathbb{Z}$, the integers; $\mathbb{Z}$ is, with the element $1 \in \mathbb{Z}$ and the usual sum and product operations, an example of a ring.
Other familiar examples are $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, again with usual 1 and operations: these rings satisfy an extra property, for which they are called *fields*, as in Definition 1.3.

Definition 1.3. A ring R is a *field* if it satisfies the following properties:

- $0 \neq 1$ (if you are confused about this, see Example 1.10);
- for all $a \in R$ with $a \neq 0$ there exists a (unique) element of R, denoted a^{-1}, such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Example 1.4. For any natural number $n \geq 1$ we can consider the equivalence relation $\equiv_n$ on the set $\mathbb{Z}$, where for $a, b \in \mathbb{Z}$ we say $a \equiv_n b$ if the difference $a - b$ is a multiple of n. The set of equivalence classes is usually denoted $\mathbb{Z}/n$, and we denote by $[a]_n$ the equivalence class of an integer $a \in \mathbb{Z}$.
The set $\mathbb{Z}/n$ "inherits" from $\mathbb{Z}$ a ring structure: one defines the element $1_{\mathbb{Z}/n} \in \mathbb{Z}/n$ as the class $[1_{\mathbb{Z}}]_n$, and for $a, b \in \mathbb{Z}$ one sets $[a]_n + [b]_n = [a+b]_n$ and $[a]_n \cdot [b]_n = [a \cdot b]_n$; these definitions are well-posed, and make $\mathbb{Z}/n$ into a ring.
Now, if we think of $\mathbb{Z}$ as a discrete "line", infinite in both directions, we can think of $\mathbb{Z}/n$ as obtained from $\mathbb{Z}$ by wrapping it along a circle of "length" n; the result is, pictorially, a circle with n points in evidence, representing the n equivalence classes in $\mathbb{Z}/n$. This picture now looks like a ring (the piece of jewelry) with n precious stones...[1]

Exercise 1.5. Check or recall from previous courses that $\equiv_n$ is indeed an equivalence relation, that the given definitions of sum and product on $\mathbb{Z}/n$ are well-posed, and that with this structure $\mathbb{Z}/n$ is indeed a ring, i.e. it satisfies all properties from Definition 1.1.

Exercise 1.6. Check or recall that $\mathbb{Z}/n$ is a field if and only if n is a prime number.

Example 1.7. Given two rings R and S, we can consider the cartesian product of sets $R \times S$; we can put a ring structure on it, by letting the pair $(1_R, 1_S)$ be the multiplicative neutral element, and by letting the operations of sum and product be defined componentwise.

[1] I thought for a long time that this is the historical reason why the word "ring" is used for the mathematical object from Definition 1.1; then I had a quick read on Wikipedia and found out that things are a bit more complicated...

More generally, given a set X and a family of rings $(R_x)_{x\in X}$, we can consider the product $\prod_{x\in X} R_x$, containing families $(a_x)_{x\in X}$ of elements, one for each ring; we can again put a ring structure by letting the family $(1_{R_x})_{x\in X}$ be the multiplicative neutral element, and by defining operations pointwise. A particular case is when all rings R_x are the same ring R: then $\prod_{x\in X} R_x$ is the set R^X of all functions of sets $X \to R$, and we are endowing this set of functions with a ring structure which is defined *pointwise*.

1.2. **Aside: structure versus properties.** It is very important when one gives a definition of a mathematical notion, to distinguish between *structure* and *properties*. With reference to Definition 1.1, we have denoted the binary operations $+, \cdot$ and the element 1 as *structure* that we put on the set: this is to suggest that, once a set R is given, there are possibly several different choices for the operations and for the special element 1, leading to very different rings, yet with same underlying set. Instead, we have denoted the associativity of $+, \cdot$, the neutrality of 1 with respect to $\cdot$, the distributive law, etc., as *properties*: this is to suggest that, once a potential choice of structure is made, either the requirements hold, or not (and in the latter case the choice of structure was bad and we have to change it), but there are not "multiple ways" in which, for instance, associativity of a given sum operations can hold true.
We remark that the element $0 \in R$, i.e. the neutral element of sum, is included among the properties: this is because either there exists such an element, or not, but there cannot be, say, two distinct elements $0, 0' \in R$, both satisfying the property of being neutral for $+$: for one would then run into contradiction when computing $0 + 0'$, which would have to be equal to both 0 and $0'$. This also explains why we put the word "unique" in parentheses in the definition: even without this word, the element would be anyway unique if it exists. Similarly for the existence of additive inverses (so we didn't need to give a map $-: R \to R$ sending $a \mapsto -a$ as a structure, since this map is uniquely determined by its required properties). And similarly for Definition 1.3, where the word "unique" is in parentheses.

Exercise 1.8. Prove that what claimed in the last paragraph holds: that is, the versions of Definitions 1.1 and 1.3 without the occurrences of "(unique)" are equivalent to the versions with the word "(unique)". In this, recall the associative property of both $+$ and $\cdot$.

The distinction between structure and properties is also emphasized in the notation $(R, +, \cdot, 1)$, by which one formally introduces a ring: one has to declare the structure on the set R, but nothing about the properties.
One could now argue: *why did we treat* 0 *and* 1 *differently, by requiring the first as property and the second as structure? After all, one can easily prove that, if the binary operation* $\cdot$ *has a neutral element, this is also unique (this is similar as the argument above with* 0 *and* $0'$*).* The reason for this asymmetry will become clear when we discuss *ring homomorphisms*, see Definition 1.13. For the moment, we content ourselves of the fact that the situation with $(+, 0)$ and with $(\cdot, 1)$ is not precisely the same: indeed $(R, +, 0)$ is required to be an abelian *group*, whereas $(R, \cdot, 1)$ is only required to be a *monoid*.

Exercise 1.9. Prove that for a ring R and for $a \in R$, we always have $a \cdot 0 = 0 \cdot a = 0$. In particular we can *almost never* expect that the element 0 has a multiplicative inverse 0^{-1}, such that $0 \cdot 0^{-1} = 0^{-1} \cdot 0 = 1$; more precisely, the only way this can

happen is the situation of Example 1.10. In particular, in a ring R the monoid $(R, \cdot, 1)$ is almost never a group, and hence the asymmetry between $(R, +, 0)$ and $(R, \cdot, 1)$ is essential to make Definition 1.1 interesting.

Example 1.10. Pay attention to the fact that Definition 1.1 does not impose the inequality $0 \neq 1$. However, if R is a ring with $0 = 1$, then for all $a \in R$ we have $a = a \cdot 1 = a \cdot 0 = 0$ (the last equality usese Exercise 1.9): this means that 0 is the only element of the set R. The ring $\{0 = 1\}$ of one element, known also as "zero ring", is a very boring ring, yet it is convenient to consider it as a ring: this is similar to the convenience of considering 0 as a natural number, or $\emptyset$ as a set.

Exercise 1.11. For a ring R, prove that if $a \in R$ and if -1 and $-a$ are the additive inverses of 1 and a, respectively, then we have $(-1) \cdot a = -a$.

Exercise 1.12. Prove that there are abelian groups $(A, +)$ such that there is no choice of $1 \in A$ and $\cdot \colon A \times A \to A$ which upgrades A to a ring. In other words, not every abelian group is the underlying group of some ring (Hint: take the quotient of abelian groups $\mathbb{Q}/\mathbb{Z}$).
Prove also that there are abelian groups $(A, +)$ admitting more than one ring structure. (Hint: find ring structures on the abelian group $\mathbb{Z}/n$ in which the multiplicative neutral element is any additive generator of $\mathbb{Z}/n$)

1.3. **Ring homomorphisms and categories.** One of the leading principles in modern mathematics, which has become the standard in the last century, is that whenever one introduces a class of mathematical objects, one should also try to define morphisms/maps between two objects in the class. For the notion of ring we have the following convenient definition.

Definition 1.13. Let $(R, +_R, \cdot_R, 1_R)$ and $(S, +_S, \cdot_S, 1_S)$ be two rings. A *ring homomorphism* from R to S is a map of sets $f \colon R \to S$ which "preserves the ring structure", more precisely it satisfies the following properties:

- for all $a, b \in R$ we have $f(a) +_S f(b) = f(a +_R b)$;
- $f(1_R) = 1_S$;
- for all $a, b \in R$ we have $f(a) \cdot_S f(b) = f(a \cdot_R b)$.

You will appreciate how the spirit of Definition 1.13 is: "there are many possible maps of sets $R \to S$, but only some of them, namely those that preserve the ring structure, are considered ring homomorphisms". In particular, morphisms are defined as maps of sets with some properties, but no additional structure on top of a map of sets is specified.
Notice also that one of the requirements is $f(1_R) = 1_S$; the main reason why in Definition 1.1 we put 1 among the structure and 0 among the properties, is that later, in Definition 1.13, we want to remember to put among the properties the equality $f(1_R) = 1_S$, as this property is not in general automatic.

Exercise 1.14. Prove that if $f \colon R \to S$ is a ring homomorphism, then $f(0_R) = 0_S$: for this check that the element $x = f(0_R) \in S$ satisfies the equality $x + x = x$, and by summing $-x$ on both sides one readily gets $x = 0_S$.

Exercise 1.15. Find an example of two rings R, S and a map of sets $f \colon R \to S$ such that $f(a) +_S f(b) = f(a +_R b)$ and $f(a) \cdot_S f(b) = f(a \cdot_R b)$ for all a, b, yet $f(1_R) \neq 1_S$. (Hint: take $S = \mathbb{Z}/6$ and try to arrange that $f(1_R) = [4]_6$)

We make the following observations about Definition 1.13:

- given a ring R, the identity map $\mathrm{Id}_R\colon R \to R$ of the set R is a ring homomorphism;
- given three rings R, S, T and given two ring homomorphisms $f\colon R \to S$ and $g\colon S \to T$, the composition of maps of sets $g \circ f\colon R \to T$ satisfies all requirements of 1.13, i.e. it is again a ring homomorphism.

The above discussion shows that rings and ring homomorphisms form a *category*, in the following sense.

Definition 1.16. A *category* $\mathfrak{C}$ is a choice of the following data:

- a *collection* $\mathrm{Obj}(\mathfrak{C})$, whose elements are called *objects*: here we use the generic word "collection" to emphasize that $\mathfrak{C}$ may not be given by a set (it could be "larger" than any set);
- for all $x, y \in \mathfrak{C}$, a *set* $\mathrm{Hom}_{\mathfrak{C}}(x, y)$ of *morphisms from x to y*;
- for all $x \in \mathfrak{C}$, a special element $\mathbb{1}_x \in \mathrm{Hom}_{\mathfrak{C}}(x, y)$, called the *identity of x*;
- for all $x, y, z \in \mathfrak{C}$, a map of sets $\circ_{x,y,z}\colon \mathrm{Hom}_{\mathfrak{C}}(y, z) \times \mathrm{Hom}_{\mathfrak{C}}(x, y) \to \mathrm{Hom}_{\mathfrak{C}}(x, z)$ sending a pair (g, f) to an element denoted $g \circ f \in \mathrm{Hom}_{\mathfrak{C}}(x, z)$, and called *composition of morphisms*,

such that the following properties hold:

Associativity of composition: for all $x, y, z, w \in \mathrm{Obj}(\mathfrak{C})$ and all $f \in \mathrm{Hom}_{\mathfrak{C}}(x, y), g \in \mathrm{Hom}_{\mathfrak{C}}(y, z), h \in \mathrm{Hom}_{\mathfrak{C}}(z, w)$ we have $(h \circ g) \circ f = h \circ (g \circ f)$;

Neutrality of identities: for all $x, y \in \mathrm{Obj}(\mathfrak{C})$ and all $f \in \mathrm{Hom}_{\mathfrak{C}}(x, y)$ we have $f \circ \mathbb{1}_x = \mathbb{1}_y \circ f = f$.

One usually denotes by $\mathfrak{C}$ also the collection $\mathrm{Obj}(\mathfrak{C})$, and so writes $x \in \mathfrak{C}$ to mean "x is an object of $\mathfrak{C}$". Similarly, one writes $f\colon x \to y$ to mean "f is a morphism (in $\mathfrak{C}$) from x to y", which is the same as saying $f \in \mathrm{Hom}_{\mathfrak{C}}(x, y)$.
Definition 1.16 captures exactly what happens with rings and rings homomorphisms: there is a category, that we will denote by Ring, whose objects are rings[2] $R = (R, +, \cdot, 1)$ and whose set of morphisms $\mathrm{Hom}_{\mathfrak{C}}(R, S)$ is the set of all ring homomorphisms $R \to S$; the identity map Id_R serves as categorical identity $\mathbb{1}_R$, and composition of morphisms is defined using the usual composition of maps of sets.

Example 1.17. Let $R = (R, +_R, \cdot_R, 1_R)$ be a ring, and let $f\colon \mathbb{Z} \to R$ be a ring homomorphism. Then we must have $0 \mapsto 0_R$ and $1 \mapsto 1_R$; moreover any positive integer $n \geq 1 \in \mathbb{Z}$ can be written as a finite sum $1 + \cdots + 1$, which by f must be sent to the element $1_R +_R \cdots +_R 1_R$, where in the last sum there are n summands;[3] similarly, every negative integer $-n$ must be sent to the additive inverse of $f(n)$. It follows that the entire map f is uniquely determined by the requirement that it be a ring homomorphism. Viceversa, one can use the above to define recursively a map of sets $\mathbb{Z} \to R$, and then check that it is always a ring homomorphism.
Conclusion: the ring $\mathbb{Z}$ has the characterising property that for any ring R there is exactly one ring homomorphism $\mathbb{Z} \to R$. In categorical terminology, if an object i of a category $\mathfrak{C}$ has the property that for any object $x \in \mathfrak{C}$ there is exactly one morphism $i \to x$, one says that i is *initial*. We just proved that $\mathbb{Z}$ is initial in Ring.

[2] In this course, we only consider commutative rings; hence also all objects of the category denoted Ring will be commutative rings

[3] Here there is a simple induction argument hidden: spell it out!

Exercise 1.18. Dually, an object t in a category $\mathfrak{C}$ is said to be *terminal* if for any object $x \in \mathfrak{C}$ there is exactly one morphism $x \to t$. Guess which ring is terminal in Ring, and then prove it!

1.4. **Algebras over a ring and rings of polynomials.**

Definition 1.19. Given a ring S, we say that a subset $R \subset S$ is a *subring* if $1 \in R$, R is an additive subgroup of S, and the product restricts on R; in this case the inclusion $R \hookrightarrow S$ is a ring homomorphism.

Exercise 1.20. Prove that the image of a ring homomorphism towards a ring S is a subring of S; converesely, notice that every subring $R \subseteq S$ can be exhibited as the image of the ring homomorphism $R \to S$ given by the inclusion.

Often one is more confident about a subring ring R and is trying to understand properties of the larger ring S, so that one thinks of R as "the easy part" of S. More generally, one may have a (possibly non-injective) ring homomorphism $\phi\colon R \to S$, and still want to consider S as the "easy" ring among the two.

Definition 1.21. Let R be a ring. An *R-algebra* is the datum (S, ϕ) of a ring S and a ring homomorphism $\phi\colon R \to S$. Given two R-algebras (S, ϕ) and (S', ϕ'), a ring homomorphism $f\colon S \to S'$ is said to be a *R-algebra homomorphism* if there is an equality $\phi' = f \circ \phi$ of ring homomorphisms $R \to S'$.

To justify the spirit of Definition 1.21: we can think of an R-algebra as a ring S with an additional structure, namely a choice of ring homomorphism from R; it is then natural to define R-algebra homomorphisms as those ring homomorphisms that "preserve" this additional structure, and this "preservation" is interpreted as commutativity of the following diagram (which is the equality $\phi' = f \circ \phi$):

$$\begin{array}{ccc} R & \xrightarrow{\phi} & S \\ & \searrow^{\phi'} & \downarrow f \\ & & S' \end{array}$$

For every ring R the above yields a category RAlg of R-algebras and homomorphisms of R-algebras.

Exercise 1.22. Describe in detail the category RAlg of R-algebras and homomorphisms of R-algebras. Show that the object (R, Id_R) is initial in this category. Find also a terminal object.

Example 1.23. Every ring is uniquely a $\mathbb{Z}$-algebra, by rephrasing Example 1.17; similarly, every ring homomorphism $f\colon R \to S$ is automatically a $\mathbb{Z}$-algebra homomorphism.
The inclusion of $\mathbb{Q} \hookrightarrow \mathbb{R}$ makes $\mathbb{R}$ into a $\mathbb{Q}$-algebra. For all $m, n \geq 1$ and $m \mid n$, the natural projection $\mathbb{Z}/n \twoheadrightarrow \mathbb{Z}/m$ is a ring homomorphism, making $\mathbb{Z}/m$ into a $\mathbb{Z}/n$-algebra.
Observe that for $n \geq 2$ there can be no ring homomorphism $\mathbb{Z}/n \to \mathbb{Q}$ nor $\mathbb{Q} \to \mathbb{Z}/n$, because in both rings we have $1 \neq 0$, yet any ring homomorphism between these two rings would be in particular an abelian group homomorphism and as such (easy check) would have to send everything to zero. So $\mathbb{Q}$ cannot be made into a $\mathbb{Z}/n$-algebra, nor viceversa. This shows that knowing that a ring S admits an R-algebra structure can put strong constraints on the ring S itself.

Exercise 1.24. Find two rings R, S such that S admits two different structures of R-algebras.

Example 1.25. Given a ring R, a *polynomial* in the variable x with coefficients in R is a formal sum $\sum_{\alpha=0}^{\infty} c_\alpha x^\alpha$, where $(c_\alpha)_{\alpha\geq 0}$ is a sequence of elements of R, called *coefficients*, with all but finitely many terms being 0. The set of all polynomials is denoted $R[x]$, and it becomes a ring by defining $(\sum_{\alpha=0}^{\infty} c_\alpha x^\alpha) + (\sum_{\alpha=0}^{\infty} c'_\alpha x^\alpha) = \sum_{\alpha=0}^{\infty}(c_\alpha + c'_\alpha)x^\alpha$ and $(\sum_{\alpha=0}^{\infty} c_\alpha x^\alpha)\cdot(\sum_{\alpha=0}^{\infty} c'_\alpha x^\alpha) = \sum_{\alpha=0}^{\infty}(\sum_{i=0}^{\alpha} c_i \cdot c'_{\alpha-i})x^\alpha$, and by letting the constant polynomial 1 be the multiplicative neutral element. The inclusion of R into $R[x]$ as constant polynomials is a ring homomorphism, making $R[x]$ into an R-algebra. We will generalise this to several variables in Definition 1.27.

Definition 1.26. Given a set $\mathcal{I}$, we denote by $\mathrm{Mult}(\mathcal{I})$ the set of all functions $\alpha\colon \mathcal{I} \to \mathbb{N}$ that vanish "almost everywhere", in the set that $\mathcal{I} \setminus \alpha^{-1}(0)$ is a finite subset of $\mathcal{I}$. Note that given two such functions $\alpha, \beta \in \mathrm{Mult}(\mathcal{I})$, the pointwise sum $\alpha + \beta$ is again a function $\mathcal{I} \to \mathbb{N}$ that lies in $\mathrm{Mult}(\mathcal{I})$. An element of $\mathrm{Mult}(\mathcal{I})$ is called a *multi-index* labelled by the set $\mathcal{I}$.

Definition 1.27. Let R be a ring. Given a set $\mathcal{I}$, we can create a "variable" x_i for all elements $i \in \mathcal{I}$. With any multi-index $\alpha \in \mathrm{Mult}(\mathcal{I})$ we associate the corresponding *monomial* x^α, which we think of as the formal, *finite* product $\prod_{i\in\mathcal{I}} x_i^{\alpha(i)}$. Given a function $c\colon \mathrm{Mult}(\mathcal{I}) \to R$ that vanishes "almost everywhere", again in the sense that $\mathrm{Mult}(\mathcal{I}) \setminus c^{-1}(0)$ is a finite set, we define the corresponding *polynomial* in the variables $\{x_i\}_{i\in\mathcal{I}}$ and coefficients in R as the formal, *finite* sum $\sum_{\alpha\in\mathrm{Mult}(\mathcal{I})} c_\alpha x^\alpha$. The element $c_\alpha := c(\alpha)$ is called the *coefficient* of the monomial x^α.
We let $R[x_i \mid i \in \mathcal{I}]$ denote the set of all polynomials in the variables $\{x_i\}_{i\in\mathcal{I}}$ and coefficients in R. The sum of polynomials $\sum_\alpha c_\alpha x^\alpha$ and $\sum_\alpha c'_\alpha x^\alpha$ is defined as the polynomial $\sum_\alpha (c_\alpha + c'_\alpha)x^\alpha$, i.e. the polynomial corresponding to the pointwise sum of the functions c and c'. The product of the same polynomials is defined as the polynomial corresponding to the function $d\colon \mathrm{Mult}(\mathcal{I}) \to \mathbb{N}$ sending

$$\alpha \mapsto d(\alpha) = d_\alpha = \sum_{(\beta,\beta')\in\mathrm{Mult}(\mathcal{I})^2\,:\,\beta+\beta'=\alpha} c_\beta \cdot c'_{\beta'}$$

(check that in the latter sum almost all terms are zero).
We define a map $\iota\colon R \to R[x_i \mid i \in \mathcal{I}]$ by sending the element $a \in R$ to the "constant polynomial" a, corresponding to the function $\mathrm{Mult}(\mathcal{I}) \to R$ sending the zero multi-index to a, and every other multi-index to $0 \in R$; this provides us in particular with an element $1_{R[x_i \mid i\in\mathcal{I}]} := \iota(1_R) \in R[x_i \mid i \in \mathcal{I}]$.

Exercise 1.28. Prove that the set $R[x_i \mid i \in \mathcal{I}]$ from Definition 1.27, together with the operations of sum, product and the element $1_{R[x_i \mid i\in\mathcal{I}]}$, is a ring. Prove also that ι is a ring homomorphism, i.e. $(R[x_i \mid i \in \mathcal{I}], \iota)$ is an R-algebra.

The most familiar instance of Definition 1.27 is when $\mathcal{I}$ is a finite set of the form $\{1, \ldots, n\}$: then the corresponding polynomial ring is usually denoted $R[x_1, \ldots, x_n]$.

Exercise 1.29. There is a useful characterising property of the R-algebra of polynomials $(R[x_i \mid i \in \mathcal{I}], \iota)$: prove that for any R-algebra (S, ϕ) and for any family $(s_i)_{i\in\mathcal{I}}$ of elements of S, there exists a *unique* homomorphism of R-algebras $f\colon R[x_i \mid i \in \mathcal{I}] \to S$ such that for all $i \in \mathcal{I}$ we have $f(x_i) = s_i$. You first have to

prove that the assignment

$$f\left(\sum_{\alpha\in\mathrm{Mult}(\mathcal{I})} c_\alpha x^\alpha\right) = \sum_{\alpha\in\mathrm{Mult}(\mathcal{I})} \phi(c_\alpha)\cdot\prod_{i\in\mathcal{I}} s_i^{\alpha_i}$$

gives a well-defined R-algebra homomorphism; you then have to argue that, since every polynomial can be "constructed" via iterated sums and products using only the elements of the set $\{x_i \mid i\in\mathcal{I}\}\cup R\subset R[x_i\mid i\in\mathcal{I}]$ as starting "building blocks", and since the behaviour of f is forced on these building blocks, f is also uniquely determined. This last idea is expanded in Definition 1.30.

Definition 1.30. Let (S,ϕ) be an R-algebra and let $X\subset S$ be a subset. The *sub-R-algebra of S generated by X* is the smallest subring of S containing the image of ϕ and X: it contains all elements that can be constructed starting from elements in $\Im(\phi)\cup X$ by repeated sums and products.[4]
We say that S is *generated by X as an R-algebra* if the entire S is the sub-R-algebra generated by X. And we say that S is *finitely generated as an R-algebra* if there exists a finite subset $X\subset S$ such that S is generated by X as an R-algebra.

One reason to look for generators of R-algebras is the following: if we have two R-algebras S,S' and two homomorphisms of R-algebras $f,g\colon S\to S'$ and we want to check whether $f=g$, it suffices to find a generating set X for S as R-algebra and check whether f and g agree on X or not. Moreover, one can often prove that certain properties enjoyed by a ring R are also enjoyed by any finitely generated R-algebra: if one is lucky enough, one sets an induction argument and reduces the proof to checking that whenever there is *a single element* $x\in S$ generating an R-algebra S, if R enjoys the property then also S does.

Exercise 1.31. Prove that if $f\colon S\to S'$ is a surjective R-algebra homomorphism and S is finitely generated over R, then so is S'.
Use the previous to prove the following: an R-algebra S is finitely generated if and only if there exists $n\geq 0$ and a surjective homomorphism of R-algebras $R[x_1,\dots,x_n]\twoheadrightarrow S$.

1.5. **Functions induced from polynomials.** One of the reasons why polynomials have been invented is that they give us a supply of functions, taking as input one or more elements of a ring R, and giving as output an element of R.

Definition 1.32. Let $\mathcal{I}$ be a set, and let $R^{\mathcal{I}}$ denote the set of all functions of sets $\mathcal{I}\to R$. Given a polynomial $P=\sum_{\alpha\in\mathrm{Mult}(\mathcal{I})} c_\alpha x^\alpha\in R[x_i\mid i\in\mathcal{I}]$, we define the corresponding function $P_*\colon R^{\mathcal{I}}\to R$ as follows: given a function $a\colon\mathcal{I}\to R$, which we see as an indexed family $(a_i)_{i\in\mathcal{I}}$ of elements of R, we define $P_*(a)=\sum_{\alpha\in\mathrm{Mult}(\mathcal{I})} c_\alpha\cdot\prod_{i\in\mathcal{I}} a_i^{\alpha_i}$.

The principle used here is the same as the one used in Exercise 1.29: the "variables" x_i can be regarded as place-holders for elements of the ring R, and replacing them with a choice of such elements yields a new element of R, obtained after a finite computation. The most familiar instance of Definition 1.32 is when $\mathcal{I}=\{1,\dots,n\}$,

[4]Someone will argue: don't you have to put 0? Don't you have to adjoin $-a$ whenever you have a? Answer: $\mathrm{Im}(\phi)$ already contains 0 and also -1, now think of Exercise 1.11... If it makes you more comfortable, however, you can always remember to put zero and additive inverses in the ingredients of the recipe!

yielding the familiar fact that every polynomial $P \in R[x_1, \dots, x_n]$ gives rise to a funcion $P_* \colon R^n \to R$.
Considering all polynomials at the same time, and considering the set $R^{R^{\mathcal{I}}}$ of *all* functions $R^{\mathcal{I}} \to R$, we obtain a map of sets $-_* \colon R[x_i \,|\, i \in \mathcal{I}] \to R^{R^{\mathcal{I}}}$. If we consider on $R^{R^{\mathcal{I}}}$ the ring structure given by pointwise addition and multiplication, then $-_*$ is even a homomorphism of rings.

Example 1.33. Take $R = \mathbb{R}$ and $\mathcal{I} = \{1\}$; then the above gives a map $-_*\mathbb{R}[x] \to \mathbb{R}^{\mathbb{R}}$, which is the usual map that associates with a polynomial in one variable with coefficients in $\mathbb{R}$ the corresponding function $\mathbb{R} \to \mathbb{R}$. Note that the right hand side $\mathbb{R}^{\mathbb{R}}$ contains *all* functions, and not only, say, the continuous or differentiable ones (a very small portion of which is hit by the map $-_*$). This is to say that the map $-_*$ is not surjective in general.

Exercise 1.34. Let R be a finite field, e.g. $R = \mathbb{Z}/p$ for some prime number p, and let $n \geq 0$; show that the map $R[x_1, \dots, x_n] \to R^{R^n}$ is surjective in this case. It cannot be injective because the target is a finite set, but the source is infinite.

The above suggests that, in general, a polynomial is more than its associated function!

2. Ideals and modules

2.1. **Definition of ideals.** Recall that the kernel of a group homomorphism $\psi \colon G \to H$ is a normal subgroup of G, and in fact every normal subgroup $N \triangleleft G$ arises as kernel of some group homomorphism. What is the analogous statement for rings?

Definition 2.1. Let R be a ring. A subset $I \subseteq R$ is an *ideal* if it satisfies the following properties:

- I is an additive subgroup of R (in particular, $0 \in I$ and hence I is non-empty);
- for all $a \in R$ and all $b \in I$ we have $a \cdot b \in I$.

The most basic examples of ideals in a ring R are the entire ring R, and the zero ideal $\{0\} \subseteq R$. Every ideal $I \subseteq R$ which is not the entire ring is called a *proper* ideal. Note that the zero ring $\{0\}$ has no proper ideal.
Another example is the following: if $a \in R$ is an element, we let $aR \subseteq R$ be the subset of elements of the form $a \cdot b$ for some $b \in R$; then aR is easily checked to be an ideal. Such an ideal is called a *principal* ideal; for $a = 0$ or $a = 1$ we recover the previous examples.

Exercise 2.2. We say that an element of a ring $a \in R$ is *invertible* if there is another element $a^{-1} \in R$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Prove that if $I \subseteq R$ is an ideal and if I contains an invertible element of R, then $I = R$. Deduce that the only ideals in a field are the zero ideal and the entire field.

Example 2.3. Using the Euclidean algorithm for division, one can show that all ideals of the ring $\mathbb{Z}$ are principal: more precisely, for all $n \geq 0$ we have an ideal $n\mathbb{Z} \subseteq \mathbb{Z}$.

Example 2.4. Let $R = \mathbb{R}[x, y]$, the ring of polynomials in two variables with real coefficients, and let $I \subseteq R$ be the subset of those polynomials with vanishing constant term. It is easy to check that I is an ideal, yet the degree 1 polynomials

x and y both belong to I and have no common divisor belonging to I. It follows that I is not a principal ideal.

The previous example shows that even if Definition 2.1 abstracts the properties of the set of multiples of an element $a \in R$, as a subset of R, in general not all subsets $I \subseteq R$ with the given properties are of the form "multiples of a" for some $a \in R$. One can then imagine that for every such I there is an "ideal" element of the ring R (i.e., not necessarily an actual element of R), whose "multiples" ought to be the set I: and that is, more or less, the historical reason for the use of the word "ideal".[5]

Lemma 2.5. *Let $f\colon R \to S$ be a ring homomorphism; then $\ker(f) := f^{-1}(0_S)$ is an ideal.*

Proof. Since f is in particular a homomorphism of abelian groups, $\ker(f)$ is an abelian subgroup of R; moreover, if $a \in R$ and $b \in \ker(f)$, then $f(a{\cdot}b) = f(a){\cdot}f(b) = f(a) \cdot 0 = 0$, witnessing that $a \cdot b \in \ker(f)$. □

Exercise 2.6. Prove similarly that if $f\colon R \to S$ is a ring homomorphism and $J \subseteq S$ is an ideal, then $f^{-1}(J)$ is an ideal of R.

Conversely to Lemma 2.5, let R be a ring and $I \subseteq R$ be an ideal, and consider the quotient R/I. This is defined, as usual, as the quotient abelian group whose elements are the cosets $[a]_I = \{a + b \,|\, b \in I\} \subseteq R$, for a ranging in R. Now we can define a product on R/I by setting $[a]_I \cdot [a']_I = [a \cdot a']_I$; Definition 2.1 is designed for this assignment to be well-posed: if we pick$b, b' \in I$ and change our representatives a, a' of the classes $[a]_I, [a']_I$ to $a + b, a' + b'$, the formula above would give the class $[(a + b) \cdot (a' + b')]_I = [a \cdot a' + (a \cdot b' + b' \cdot a + b \cdot b')]_I$, and since $(a \cdot b' + b' \cdot a + b \cdot b')$ belongs to I, we get indeed the same class. We thus obtain a ring structure on the abelian group R/I; moreover the quotient map $R \twoheadrightarrow R/I$ is a ring homomorphism, whose kernel is R/I. Thus we have proved the following:

Proposition 2.7. *Let R be a ring; then every ring homomorphism out of R has an ideal of R as kernel, and conversely, every ideal of R can be exhibited as kernel of some ring homomorphism out of R.*

In fact, if $f\colon R \to S$ is a ring homomorphism, then as we saw $\ker(f) \subseteq R$ is an ideal of R, and $\mathrm{Im}(f) \subseteq S$ is a subring of S. Since f vanishes on $\ker(f)$, it induces a map of abelian groups $\bar{f}\colon R/\ker(f) \to \mathrm{Im}(f)$; this map is not only bijective, but it is also a ring homomorphism (where the source is given the ring structure discussed above). We obtain the following diagram, which factors a generic ring homomorphism f as a composition of a surjective ring homomorphism, followed by a surjective one

$$\begin{array}{ccc} R & \xrightarrow{\quad f \quad} & S \\ \downarrow & & \uparrow \\ R/\ker(f) & \xrightarrow{\quad \bar{f} \quad} & \mathrm{Im}(f) \end{array}$$

Exercise 2.8. Give a solution of Exercise 2.6 considering the composition of ring homomorphisms $R \xrightarrow{f} S \twoheadrightarrow S/J$ and Lemma 2.5.

Example 2.9. Let $n \geq 0$ and let $n\mathbb{Z} \subseteq \mathbb{Z}$ be the ideal of multiples of n; then the quotient ring $\mathbb{Z}/n\mathbb{Z}$ is nothing but the ring $\mathbb{Z}/n$ from Example 1.4.

[5] In this case Wikipedia supports my story!

Exercise 2.10. Let $f\colon R \to S$ be a ring homomorphism and let $I \subseteq R$ be an ideal. Prove that the following are equivalent:

(1) f vanishes on I, i.e. $I \subseteq f^{-1}(0)$;
(2) there exists a unique ring homomorphism $\bar{f}\colon R/I \to S$ such that f is the composite $R \twoheadrightarrow R/I \xrightarrow{\bar{f}} S$.

Before continuing talking of ideals, it is convenient to introduce/recall the notion of module.

2.2. **Modules.** Modules are to rings what vector spaces are to fields: abelian groups in which one can also multiply by scalars.

Definition 2.11. Let R be a ring. A *module* over R is an abelian group $(M, +)$ endowed with a map of sets $\cdot_M\colon R \times M \to M$, called *multiplication by scalars*, satisfying the following properties:

- for all $m \in M$ we have $1 \cdot_M m = m$;
- for all $a, a' \in R$ and $m, m' \in M$ we have $(a + a') \cdot_M (m + m') = (a \cdot_M m) + (a \cdot_M m') + (a' \cdot_M m) + (a' \cdot_M m')$;
- for all $a, a' \in R$ and $m \in M$ we have $(a \cdot_R a') \cdot_M m = a \cdot_M (a' \cdot_M m)$.

A homomorphism of R-modules from $(M, \cdot_M)$ to $(M', \cdot_{M'})$ is a homomorphism of abelian groups $f\colon M \to M'$ satisfying the following property:

- for all $a \in R$ and $m \in M$ we have $f(a \cdot_M m) = a \cdot_{M'} f(m)$.

Whenever there is no risk for confusion, we simply write $\cdot$, or even nothing at all, for multiplication by scalars, instead of $\cdot_M$. Similarly, from now on, for the product $\cdot$ in a ring, we will from now on just remove the $\cdot$ as is usual. And we will often present an R-module just by M instead of $(M, \cdot_M)$, i.e. we will leave the operation $\cdot_M$ implicit.
For every ring R we obtain a category RMod of R-modules and homomorphisms of R-modules.

Example 2.12. If R is a field, then an R-module is precisely an R-vector space, and a homomorphism of R-modules is precisely an R-linear map. In fact, homomorphisms of R-modules are often called "R-linear maps" even for R not a field.

Example 2.13. Every abelian group M is (uniquely) a $\mathbb{Z}$-module: given $m \in M$, for $n \geq 0$ one is forced to define $n \cdot_M m = (1 + \cdots + 1) \cdot_M m = m + \cdots + m$, where the last sum has n occurrences of m, and similarly the value of $n \cdot_M m$ is forced for $n < 0$, as it must be equal to $-((-n) \cdot_M m)$. One can then check that the above formulas give indeed a $\mathbb{Z}$-module structure on M; one can also check that every homomorphism of abelian groups is $\mathbb{Z}$-linear.

Exercise 2.14. Find an example of a ring R and an abelian group M such that M cannot be made into an R-module. (Hint: take $R = \mathbb{Z}/2$, and M containing some element m with $m + m \neq 0$)
Find also an example of a ring R and an abelian group M such that M admits more than one R-module structure. (Hint: take $R = \mathbb{Z}[x]$)

Example 2.15. Let R, S be rings and let $\phi\colon R \to S$ be a ring homomorphism, i.e. (S, ϕ) is an R-algebra. Then we can define an R-module structure on the abelian group S by setting, for all $a \in R$ and $s \in S$, $a \cdot_S s := \phi(a) \cdot_S s$, where the right

hand side uses the product of the ring S. Thus every R-algebra gives rise to an R-module with same underlying abelian group.
A particular case is when $R = S$ and $\phi = \mathrm{Id}_R$: every ring is a module over itself. Another particular case is when $S = R/I$ for some ideal $I \subseteq R$, and $\phi\colon R \to R/I$ is the projection to the quotient (which we saw is a ring homomorphism): in analogy with *cyclic abelian groups* (i.e. those of the form $\mathbb{Z}/n$ for some $n \geq 0$), one calls an R-module of the form R/I also a *cyclic* R-module.[6]

Lemma 2.16. *Let M be an R-module. Then there is a bijection between the set M and the set of R-linear maps $R \to M$.*

Proof. Given an element $m \in M$, we can define a map of sets $f_m\colon R \to M$ by sending $a \mapsto a \cdot m$; one easily checks that this map is R-linear. Viceversa, given an R-linear map $g\colon R \to M$, one can evaluate g at the element $1 \in R$, obtaining an element $g(1) \in M$. The two operations extablish inverse bijections between the set M and the set of R-linear maps $R \to M$. □

Exercise 2.17. Elaborate on Example 2.15 and construct a functor $R\mathrm{Alg} \to R\mathrm{Mod}$ sending each object $(S, \phi) \in R\mathrm{Alg}$ to the R-module defined there. What is a reasonable assignment on morphisms? For your convenience, here follows the definition of functor.

Definition 2.18. Given two categories $\mathfrak{C}$ and $\mathfrak{C}'$, a *functor* F from $\mathfrak{C}$ to $\mathfrak{C}'$, denoted $F\colon \mathfrak{C} \to \mathfrak{C}'$, is a choice of data as following:

- for each object $x \in \mathrm{Obj}(\mathfrak{C})$, an object $F(x) \in \mathrm{Obj}(\mathfrak{C})$;
- for each objects $x, y \in \mathrm{Obj}(\mathfrak{C})$, a map of sets $\mathrm{Hom}_{\mathfrak{C}}(x, y) \to \mathrm{Hom}_{\mathfrak{C}}(F(x), F(y))$, denoted $f \mapsto F(f)$,

satisfying the following properties:

- for all $x \in \mathrm{Obj}(\mathfrak{C})$ we have $F(\mathbb{1}_x) = \mathbb{1}_{F(x)}$;
- for all $x, y, z \in \mathrm{Obj}(\mathfrak{C})$ and all morphisms $f\colon x \to y$ and $g\colon y \to z$ in $\mathfrak{C}$, we have $F(g \circ f) = F(g) \circ F(f)$.

Exercise 2.19. Find an example of a ring R and an R-module M such that there is no R-algebra S which is sent along the functor from Exercise 2.17 to an R-module isomorphic to M. (Hint: you can recycle Exercise 1.12, but there should be simpler examples)

Many of the familiar definitions and lemmas related to the theory of abelian groups carry over to analogous definitions for R-modules, for a given ring R, in particular:

- given an R-module M, if $N \subseteq M$ is a sub-abelian group and if the map $\cdot_M\colon R \times M \to M$ restricts to a map $R \times N \to N$, we say that N is a sub-R-module of M (or just submodule, if the ring is implicit);
- if N is a submodule of M, then the quotient abelian group M/N carries a natural R-module structure, by setting, for $a \in R$ and $m \in M$, $a \cdot [m]_N = [a \cdot m]_N$;
- if M, M' are R-modules and $f\colon M \to M'$ is an R-linear map, then $\ker(f)$ is a submodule of M and $\mathrm{Im}(f)$ is a submodule of M', so that we can

[6]It is clear why the word "cyclic" is used for the abelian groups $\mathbb{Z}/n$, at least when $n \geq 2$: one thinks of the elements of $\mathbb{Z}/n$ as assembled along a cycle... But now there is no geometric/visual meaning left in the terminology when applied to a generic R/I, as a module over R

define $\operatorname{coker}(f)$ as the quotient $M'/\operatorname{Im}(f)$, which is again endowed with an R-module structure;
- if $N, N' \subseteq M$ are submodules, then also the intersection $N \cap N'$ is a submodule;
- if $N \subseteq M$ is a submodule and $f\colon P \to M$ is an R-linear map, then $f^{-1}(N)$ is a submodule of P;
- if $N \subseteq M$ is a submodule, then every other submodule $P \subseteq M$ with $N \subseteq P$ gives rise to a submodule $P/N \subseteq M/N$, and viceversa, every submodule $P' \subseteq M/N$ gives rise to a submodule of M by taking its preimage under the projection map $M \twoheadrightarrow M/N$;
- we can talk of short and long exact sequences of R-modules: in fact, whether a sequence $M \to M' \to M''$ of R-modules and R-linear maps is exact at M' is a property of the underlying sequence of abelian groups (i.e., exactness does not involve multiplication by scalars in R);
- given a set X and a family $(M_x)_{x\in X}$ of R-modules, we can consider the product $\prod_{x\in X} M_x$ and put on it an R-module structure, by defining $a \cdot ((m_x)_{x\in X}) = (a \cdot m_x)_{x\in X}$;
- inside $\prod_{x\in X} M_x$ we can consider the subset of those families $(m_x)_{x\in X}$ such that for all but finitely many $x \in X$ we have $m_x = 0 \in M_x$; this subset of $\prod_{x\in X} M_x$ is denoted $\bigoplus_{x\in X} M_x$, is called the *direct sum* of the R-modules $(M_x)_{x\in X}$, and it is indeed a submodule of the direct product $\prod_{x\in X} M_x$.

Exercise 2.20. Prove all of the previous claims.

Exercise 2.21. There are useful characterising properties for the direct product and the direct sum. Given a family $(M_x)_{x\in X}$ of R-modules, and another R-module N, prove that an R-linear map $f\colon N \to \prod_{x\in X} M_x$ is uniquely determined by the maps $f^x\colon N \to M_x$ obtained by postcomposing f with the projections of the product onto each of its factors. Similarly, prove that an R-linear map $g\colon \bigoplus_{x\in X} M_x \to N$ is uniquely determined by the maps $g_x\colon M_x \to N$ obtained by precomposing g with the inclusions of each direct summand into the direct sum.

Definition 2.22. An R-module M is *free* if there exists a set X and an isomorphism of R-modules $M \cong \bigoplus_{x\in X} R$, where the right hand side is the direct sum of several copies of R as a module over itself, one copy for each $x \in X$.
A *basis* for a (free) R-module M is a collection of elements $\{m_x\}_{x\in X}$ such that the map of R-modules $\bigoplus_{x\in X} R \to M$ given by sending the element $1_R \in R$ in the x^{th} summand to m_x is an isomorphism of R-modules.

Example 2.23. Let R be a field and M be an R-module, i.e. an R-vector space. We can pick a basis $(m_x)_{x\in X}$ of M over R, and use it to exhibit an isomorphism $\bigoplus_{x\in X} R \cong M$. This shows that every vector space is free over the corresponding field.
Let instead $R = \mathbb{Z}$; then for all sets X, the $\mathbb{Z}$-module $\bigoplus_{x\in X} \mathbb{Z}$ is either the zero module (if X is empty), or has infinite cardinality (if X is non-empty): this shows that $\mathbb{Z}$-modules such as $\mathbb{Z}/n$ for $n \geq 2$ are not free, since they cannot be isomorphic to any direct sum $\bigoplus_{x\in X} \mathbb{Z}$.

Example 2.24. The $\mathbb{Z}$-module $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$ is free over $\mathbb{Z}$; examples of bases are the sets $\{(1,0),(0,1)\}$, $\{(1,1),(0,1)\}$, $\{(2,3),(1,2)\}$ and in general any pair of elements $\{(a,b),(c,d)\}$ such that $ad - bc = \pm 1$. This shows that if a module is free, i.e. it admits at least one basis, there are usually several bases.

Example 2.25. Let $n \geq 0$ and let $R^n = R \times \cdots \times R$ be the n-fold cartesian power of R. Then R^n is free, with standard basis given by the elements $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, where the only occurrence of 1 is in position i, for $1 \leq i \leq n$.

As for R-algebras, we have a notion of *generation* for R-modules. Compare the following with Definition 1.30

Definition 2.26. Let M be an R-module and let $X \subseteq M$ be a subset. The *sub-R-module of M generated by M*, denoted $\mathrm{Span}_R(X)$, is the smallest sub-R-module of M containing X: it contains all elements that can be expressed as $\sum_{i=1}^{n} a_i \cdot m_i$ for some $n \geq 0$ and elements $a_1, \ldots, a_n \in R$ and $m_1, \ldots, m_n \in X$.
We say that M is *generated by X as an R-module* if $M = \mathrm{Span}_R(X)$, and we say that M is *finitely generated as an R-module* if there exists a finite subset $X \subseteq M$ such that M is generated by X as an R-module.

Recall Example 2.15, let (S, ϕ) be an R-algebra, and let $X \subseteq S$; then:

- if X generates S as an R-module, it also generates S as an R-algebra;
- if X generates S as an R-algebra, it need not generate S as an R-module: consider the case $S = R[x, y]$, then $\{x, y\}$ generates S as an R-algebra, but not as an R-module.

Example 2.27. The polynomial ring $R[x_i \,|\, i \in \mathcal{I}]$ is generated, as an R-module, by the set of all monomials x^α, for $\alpha \in \mathrm{Mult}(\mathcal{I})$. In fact these elements also form a basis for $R[x_i \,|\, i \in \mathcal{I}]$, thus exhibiting it as a free R-module.

Example 2.28. Given an R-module M and two submodules $N, N' \subseteq M$, the sum $N + N' := \{m + m' \,|\, m \in N, m' \in N\} \subseteq M$ coincides with the submodule $\mathrm{Span}_R(N \cup N')$, and in particular is again a submodule.

Exercise 2.29. Let M be an R-module; prove that the following are equivalent:

- M is finitely generated over R;
- there exist $n \geq 0$ and a surjective R-linear map $R^n \twoheadrightarrow M$.

Prove also that the following are equivalent:

- M can be generated by a single element $m \in M$;
- M is isomorphic to a cyclic R-module, i.e. one of the form R/I for some ideal $I \subseteq R$.

2.3. **Back to ideals.** We can now give a new definition of ideal: an ideal $I \subseteq R$ is a sub-R-module of the R-module R.

Definition 2.30. Given a subset $X \subseteq R$, we denote by $(X) \subseteq R$ the ideal generated by X, i.e. $(X) = \mathrm{Span}_R(X)$. If $X = \{a_1, \ldots, a_n\}$ is finite, we also write $(X) = (a_1, \ldots, a_n) \subseteq R$.

Note that for $a \in R$ the ideal (a) is the same as the ideal aR.

Example 2.31. Given two ideals $I, J \subseteq R$, we can form three new ideals as follows:

- we can take their *intersection*, i.e. the ideal $I \cap J \subseteq R$;
- we can take their *product*, i.e. the ideal $I \cdot J = \mathrm{Span}_R(\{a \cdot b \,|\, a \in I, b \in J\})$;
- we can take their *sum*, i.e. the ideal $I + J = \mathrm{Span}_R(I \cup J) \subseteq R$.

If $R = \mathbb{Z}$, these operations have a very familiar description: let $n, n' \geq 0$, and consider the two ideals $(n) = n\mathbb{Z}$ and $(n') = n'\mathbb{Z}$ of $\mathbb{Z}$:

- the ideal $(n) \cap (n')$ is the ideal $(\mathrm{lcm}(n, n'))$, generated by the *least common multiple* of n and n';
- the ideal $(n) \cdot (n')$ is the ideal $(n \cdot n')$, generated by the *product* of the two natural numbers n and n';
- the ideal $(n) + (n')$ is the ideal $(\gcd(n, n'))$, generated by the *greatest common divisor* of n and n'.

Here we declare $\mathrm{lcm}(n, 0) = 0$ and $\gcd(n, 0) = n$ for all $n \geq 0$.

In the same way as the operations of intersection and sum of ideals correspond to the classical operations of lcm and gcd on natural numbers, we should think of containment $I \subseteq J$ of ideals as the relation corresponding to divisibility $n \mid n'$ of numbers, as shown in the following, easy lemma.

Lemma 2.32. *Let R be a ring and let $a, b \in R$ be two elements; then the following are equivalent:*

(1) $a \mid b$, by which we mean that there exists some (not necessarily unique) $c \in R$ such that $ca = b$;
(2) the ideal (a) contains the ideal (b).

Proof. If (1) holds, then the element $b = ca$ belongs to $(a) \subseteq R$, and since (b) is by definition the smallest submodule of R containing b, we must have $(b) \subseteq (a)$. Conversely, if (2) holds, then in particular $b \in (a)$, and every element of (a) is of the form ca for some $c \in R$. □

In particular, besides studying single ideals in a ring R, it is interesting to study how ideals are related to each other by containment.

Exercise 2.33. This exercise should be compared with Exercise 2.6. Let $f \colon R \to S$ be a ring homomorphism and let $I \subseteq R$ be an ideal:

- prove that if f is surjective, then the image $f(I) \subseteq S$ is an ideal of S;
- find an example in which f is not surjective and in which $f(I)$ is not an ideal of S (though of course one can always consider the ideal $(f(I)) \subseteq S$ generated by $f(I)$: the point is that $(f(I))$ may be strictly larger than $f(I)$).

Lemma 2.34. *Let R be a ring and let $I \subseteq R$ be an ideal. Then the natural ring homomorphism $\pi \colon R \twoheadrightarrow R/I$ induces a bijection between ideals in R containing I, and ideals in R/I.*

Proof. Given an ideal $I \subseteq J \subseteq R$, we can take the image $\pi(J) \subseteq R/I$, which by Exercise 2.33 is an ideal of R/I; viceversa, given an ideal $J \subseteq R/I$, the preimage $f^{-1}(J)$ is an ideal of R by Exercise 2.6, and it contains $f^{-1}(0) = I$. The two operation give inverse bijections between the set of ideals of R containing I, and the set of ideals of R/I. □

Example 2.35. Let k be a field, and let $n \geq 0$. As we saw in Definition 1.32, each polynomial $P \in k[x_1, \ldots, x_n]$ gives rise to a function $P_* \colon k^n \to k$; this gave us a map of rings $-_* \colon k[x_1, \ldots, x_n] \to k^{k^n}$.
Now, if $X \subset k^n$ is any subset, we can consider the subset

$$\mathfrak{I}(X) = \{f \colon k^n \to k \mid f|_X \equiv 0\} \subset k^{k^n};$$

we have that $\mathfrak{I}(X)$ is an ideal in the ring k^{k^n}, since for all functions $f, g \colon k^n \to k$ we have:

- if $f|_X \equiv 0$, then also $-f|_X \equiv 0$ and $(g \cdot f)|_X \equiv (g|_X) \cdot (f|_X) \equiv (g|_X) \cdot 0 \equiv 0$;
- if moreover also $g|_X \equiv 0$, then also $(g + f)|_X \equiv (g|_X) + (f|_X) \equiv 0 + 0 \equiv 0$.

We can now consider the preimage $\mathbb{I}(X)$ of $\mathfrak{I}(X)$ along the ring homomorphism $-_*$, and obtain an ideal $\mathbb{I}(X) \subseteq k[x_1, \dots, x_n]$: it contains all polynomials whose associated function vanishes on X. This gives a way to construct ideals in polynomial rings.

Somewhat more interesting is the opposite construction, starting from an ideal and yielding a subset of k^n.

Definition 2.36. Given an ideal $I \subset k[x_1, \dots, x_n]$, we define $\mathbb{V}(I) \subset k^n$ as the subset of all elements $(a_1, \dots, a_n)$ such that for each $P \in I$ we have $P_*(a_1, \dots, a_n) = 0 \in k$. A subset of k^n of the form $\mathbb{V}(I)$ is called an *affine algebraic set*.

The previous definition should be rather familiar when $k = \mathbb{R}$, $n = 2$ and $I = (P)$ is the principal ideal in $\mathbb{R}[x, y]$ generated by a single polynomial. Then $\mathbb{V}(I) = \mathbb{V}(P)$ is the set of points (a, b) in the plane on which the function induced by the polynomial vanishes; it is usually a curve, and in general the geometric properties of $\mathbb{V}(P)$ contain information about the polynomial P.

Exercise 2.37. If k is a finite field, prove that every subset of k^n is an affine algebraic set. Prove that this is not true, instead, if k is an infinite field and $n \geq 1$.

In general we have the containment $I \subseteq \mathbb{I}(\mathbb{V}(I))$, for any ideal $I \subseteq k[x_1, \dots, x_n]$, and $X \subseteq \mathbb{V}(\mathbb{I}(X))$, but both containments can be strict.

Example 2.38. Let $X = \mathbb{N} \subset \mathbb{R} = \mathbb{R}^1$; then $\mathbb{I}(X) = (0)$, indeed if a polynomial $P \in \mathbb{R}[x]$ vanishes on all natural numbers, it must have infinitely many roots and hence $P = 0$; this implies in turn that $\mathbb{V}(\mathbb{I}(X)) = \mathbb{V}(0) = \mathbb{R}$, which is strictly larger than X.

Example 2.39. Let $I = (x^2) \subset \mathbb{R}[x]$; then $\mathbb{V}(I) = \{0\} \subset \mathbb{R}$, and the polynomials $P \in \mathbb{R}[x]$ whose associated function vanishes at $0 \in \mathbb{R}$ are precisely the polynomials without constant terms, i.e. all polynomials that are multiples of x; it follows that $\mathbb{I}(\mathbb{V}(I)) = (x)$, which is strictly larger than I.
The situation becomes even worse if we consider $I = (x^2+1) \subset \mathbb{R}[x]$; then $\mathbb{V}(I) = \emptyset$, and hence $\mathbb{I}(\mathbb{V}(I))$ is the entire ring $\mathbb{R}[x]$!

The previous examples show that in general not all subsets of k^n and not all ideals of $k[x_1, \dots, x_n]$ are in the image of the operations $\mathbb{V}$ and $\mathbb{I}$, respectively. When $k = \mathbb{R}$ or $\mathbb{C}$, many nice and interesting subsets of k^n can be defined by polynomial equalities, i.e. have the form $\mathbb{V}(I)$ for some ideal I; one can then notice that each element in the ring $k[x_1, \dots, x_n]/I$ gives a function from $\mathbb{V}(I)$ to k, and one can try to translate algebraic properties of $\mathbb{V}(I)$ into geometric properties of $\mathbb{V}(I)$; but there is also a viceversa: one might be mainly interested in the ring $k[x_1, \dots, x_n]/I$ (after all, according to Exercise 1.31, any finitely generated k-algebra has this form), and one can hope to translate geometric properties of $\mathbb{V}(I)$ into algebraic properties of $k[x_1, \dots, x_n]/I$. Algebraic geometry is, more or less, the systematic study of the correspondence between what happens on the algebraic side and what happens on the geometric side.

3. Various types of ideals

We have seen the definition of ideals in a ring R, and how containment of ideals generalises the notion of divisibility. We also saw that given an ideal $I \subseteq R$, we get a quotient ring R/I. In this section we will study different types of ideals. We will introduce several properties that an ideal in a ring may or may not have; a common feature of these properties P(with P being prime, maximal, radical) is that $I \subseteq R$ has the property P if and only if $(0) \subseteq R/I$ has the property P. One then has parallel designations for rings whose ideal (0) satisfies P.

3.1. **Prime ideals and the spectrum of a ring.**

Definition 3.1. An ideal $I \subseteq R$ is *prime* if:

- I is proper, i.e. $I \neq R$;
- for all $a, b \in R$, if $ab \in I$ then at least one among a, b already lies in I.

A ring R is a *domain* if (0) is a prime ideal in R; in other words, R is a domain if for all $a, b \in R$, if $ab = 0$ then $a = 0$ or $b = 0$ (or both).

We notice that if $I \subseteq R$ is an ideal, then $I \neq R$ if and only if $(0) \neq R/I$. Moreover, for any $a, b \in R$, the conditions $a \in I$, $b \in I$ and $ab \in I$ are equivalent to $[a]_I = 0$, $[b]_I = 0$ and $[ab]_I = 0$, so that any pair a, b of elements of R witnessing that I is not prime gives a pair $[a]_I, [b]_I$ of elements of R/I witnessing that R/I is not a domain, and viceversa.
It is standard to denote prime ideals by letters such as $\mathfrak{p}$ and $\mathfrak{q}$.

Lemma 3.2. *Let $\mathfrak{p} \subset S$ be a prime ideal and let $f\colon R \to S$ be a ring homomorphism. Then $f^{-1}(\mathfrak{p})$ is a prime ideal in R.*

Proof. Denote $\mathfrak{q} = f^{-1}(\mathfrak{p}) \subseteq R$, which is an ideal by Exercise 2.6. Let $a, b \in R$ and suppose that $ab \in \mathfrak{q}$; then $f(ab) = f(a)f(b) \in \mathfrak{p}$, and since $\mathfrak{p}$ is prime, at least one among $f(a), f(b)$ lies in $\mathfrak{p}$, which implies that at least one among a, b lies in $\mathfrak{q}$. We conclude by noticing that $1 \notin \mathfrak{q}$, since $f(1) = 1 \notin \mathfrak{p}$ (otherwise $\mathfrak{p}$ would not be proper). □

Definition 3.3. For a ring R, we denote by $\mathrm{Spec}(R)$, called the "spectrum of R", the set of all prime ideals of R.

Exercise 3.4. Starting from Lemma 3.2, construct a contravariant functor from Ring to Set (the category of sets), sending each ring R to $\mathrm{Spec}(R)$.

One may ask: *Why don't we consider the even larger contravariant functor sending R to the set of all of its ideals, and not only the prime ideals? We could use Exercise 2.6 instead of Lemma 3.2 for this!* Sure, one could do that; and in fact, it is convenient to do *both things* at the same time. The standard way to do this is to use the collection of all ideals of R to define a *topology* on R: one declares, for each ideal $I \subseteq R$, a *closed* subset $\mathbb{V}(I) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid I \subseteq \mathfrak{p}\}$, and checks that this is actually the collection of closed sets for a topology on the set $\mathrm{Spec}(R)$, which is called the *Zariski topology*; then one can enhance $\mathrm{Spec}(-)$ to a contravariant functor from Ring to Top, the category of topological spaces.

Exercise 3.5. Check that the previous makes sense. That is, check that:

- for a ring R, the sets $\mathbb{V}(I) \subseteq \mathrm{Spec}(R)$ give the collection of closed subset of a topology;

- for a ring homomorphism $f\colon R \to S$, the induced map of sets between the spaces $\mathrm{Spec}(S)$ and $\mathrm{Spec}(R)$ is actually continuous.

You must have appreciated how I used the letter $\mathbb{V}$ both in the previous discussion and in Definition 2.36; this is not a chance! I leave you the pleasure to reflect about what the connection is, and just give a hint: if k is a field and $n \geq 0$, each point $(a_1, \dots, a_n) \in k^n$ gives rise to the ideal $(x_1 - a_1, \dots, x_n - a_n) \subseteq k[x_1, \dots, x_n]$: the latter is a prime ideal (it is even a maximal ideal, see Definition 3.6), but beware that not all prime ideals of $k[x_1, \dots, x_n]$ have this form.

3.2. **Maximal ideals.**

Definition 3.6. An ideal $I \subset R$ is called *maximal* if it is a proper ideal and it is maximal with respect to inclusion among proper ideals of R.

By Lemma 2.34, we know that $I \subset R$ is maximal if and only if $(0) \subset R/I$ is maximal. It is standard to denote maximal ideals by letters as $\mathfrak{m}$.
In general, if S is a ring such that $(0) \subset S$ is a maximal ideal, then for all $a \neq 0$ in S we have that the principal ideal $(a) \subseteq S$, being an ideal strictly larger than (0), must be non-proper, i.e. we must have $(a) = S$; this implies that $1 \in (a)$, that is, there exists $b \in S$ with $ab = 1$, which is to say that a has a multiplicative inverse. We conclude that a ring S is a field if and only if (0) is maximal in S.

Lemma 3.7. *Every maximal ideal in a ring R is also a prime ideal.*

Proof. Let $\mathfrak{m} \subset R$ be a maximal ideal and let $a, b \in R$ with $ab \in \mathfrak{m}$. Suppose both $a, b \notin \mathfrak{m}$; then both ideals $(a, \mathfrak{m})$ and $(b, \mathfrak{m})$ must be all of R, and in particular there must exist elements $c, d \in R$ and $m, m' \in \mathfrak{m}$ such that $1 = ca + m = db + m'$. We can now compute $1 = 1 \cdot 1 = (ca+m)(db+m') = cd \cdot ab + ca \cdot m' + db \cdot m + mm'$, and the last expression witnesses that $1 \in \mathfrak{m}$, contradicting that $\mathfrak{m}$ is a proper ideal. □

Exercise 3.8. Give another proof of Lemma 3.7 containing the sentence "every field is a domain".

Example 3.9. What are prime and maximal ideals in $\mathbb{Z}$? Let $n \geq 0$ and consider the ideal $(n) \subseteq \mathbb{Z}$.

- if $n = 0$, the ideal (0) is prime, since the product of two non-vanishing integers is also non-zero; yet (0) is not maximal, since $(0) \subset (n)$ for all $n \geq 2$;
- if $n = 1$, the ideal (1) is the entire ring $\mathbb{Z}$, so (1) is not proper;
- if $n = p$ is a prime number, then $\mathbb{Z}/(p)$ is a field (check/remember it!), hence (p) is a maximal ideal;
- if n is not a prime number, we can factor $n = ab$ with both $a, b \geq 2$; then we have $a, b \notin (n)$, yet $ab \in (n)$, showing that (n) is not a prime ideal (and hence also not maximal).

Exercise 3.10. Prove that if $f\colon R \to S$ is a surjective ring homomorphism, then for any maximal ideal $\mathfrak{m} \subset S$ we have that $f^{-1}(S) \subset R$ is also maximal. Find an example of a non-surjective ring homomorphism $f\colon R \to S$ such that some maximal ideal of S pulls back to a non-maximal (yet prime!) ideal of R. (Hint: $\mathbb{Z} \hookrightarrow \mathbb{Q}$)

An important proposition is the following: it guarantees that every non-zero ring R admits some maximal ideal, and therefore also some prime ideal (instead, the spectrum of the zero ring is the empty set). We will prove it in a generalised form

in order to appeal to it also later; the case we are interested in right now is when $I = (0)$ and $T = \{1\}$.

Proposition 3.11. *Let R be a ring, let $I \subseteq R$ be any ideal and let $T \subseteq R$ be a subset that is disjoint from I. Let Σ be the family of all ideals J of R that contain I and are disjoint from T. Then Σ admits at least one maximal element with respect to containment. If moreover T is closed under multiplication, then all maximal elements of Σ are prime ideals.*

Proof. Recall Zorn's lemma:

- a *partially ordered set (poset)* is a set P together with a relation $\preceq \subseteq P \times P$ and denoted "$a \preceq b$" whenever $(a, b) \in \preceq$, satisfying the following properties:
  - $a \preceq a$ for all $a \in P$;
  - if $a, b \in P$ satisfy $a \preceq b$ and $b \preceq a$, then $a = b$;
  - if $a, b, c \in P$ satisfy $a \preceq b$ and $b \preceq c$, then $a \preceq c$;
- a *chain* in a poset $(P, \preceq)$ is a subset $C \subseteq P$ such that for all $a, b \in C$ we have $a \preceq b$ or $b \preceq a$ (or both, if $a = b$);
- an *upper bound* for a subset $S \subseteq P$ is an element $u \in P$ such that for all $a \in S$ we have $a \preceq u$;
- a *maximal element* is an element $m \in P$ such that there is no element $a \in P$ with $m \neq a$ and $m \preceq a$;
- Zorn's lemma says that if $(P, \preceq)$ is a *non-empty* poset such that every chain $C \subseteq P$ admits an upper bound, then there exists at least one maximal element in P.

We will not prove Zorn's lemma (but if you have never seen the proof, go and read it in the literature!). We will apply it to the poset $(\Sigma, \subseteq)$. In order to do it, we have to prove that every chain admits an upper bound. So let $\{I_i\}_{i \in \mathcal{I}}$ be a chain of nested ideals in R, all belonging to Σ, and parametrised by a set $\mathcal{I}$. Denote by $\bar{I} \subseteq R$ the union $\bigcup_{i \in \mathcal{I}} I_i$. We claim that $\bar{I} \in \Sigma$:

- $\bar{I}$ is disjoint from T and contains I, as every I_i has these properties;
- $\bar{I}$ is an ideal: for all $m, m' \in \bar{I}$ and $a \in R$ we want to check that $am + m' \in \bar{I}$ (think about why this is enough); we can pick indices $i_a, i_b \in \mathcal{I}$ such that $a \in I_{i_a}$ and $b \in I_{i_b}$; one of the containments $I_{i_b} \subseteq I_{i_a}$ or $I_{i_a} \subseteq I_{i_b}$ holds (here we use that the ideals I_i form a chain), and hence there is a unique index $\hat{i} \in \mathcal{I}$ with $a, b \in I_{\hat{i}}$; it follows that $am + m' \in I_{\hat{i}}$, and hence $am + m' \in \bar{I}$.

By Zorn's lemma, we conclude that there is are maximal elements in Σ.
We now assume that T is closed under product, and we fix a maximal element $\tilde{I} \in \Sigma$. To prove that $\tilde{I}$ is a prime ideal, we mimic the argument from Lemma 3.7. Let $a, b \in R$ with $ab \in \tilde{I}$, and suppose both $a, b \notin \tilde{I}$; then both ideals $(a, \tilde{I})$ and $(b, \tilde{I})$ do not belong to Σ, and since they contain I they must both intersect T in some element. This means that there must exist elements $c, d \in R$, $m, m' \in \tilde{I}$ amd $t, t' \in T$ such that $t = ca + m$ and $t' = db + m'$. We can now compute the product $t \cdot t' = (ca + m)(db + m') = cd \cdot ab + ca \cdot m' + db \cdot m + mm'$, and the last expression witnesses that $tt' \in \tilde{I}$, contradicting that $\tilde{I}$ is disjoint from T. □

In particular, if $I = (0)$ and $T = \{1\}$, Proposition 3.11 guarantees the existence of ideals $\tilde{I}$ that don't contain 1 (and are therefore proper ideals) and are maximal among proper ideals for containment, i.e. we have proved that maximal ideals in the sense of Definition 3.6 exist. Of course, we must also check the tiniest of the

assumptions in Zorn's lemma, namely the poset has to be non-empty: in the case of the zero ring, there is no ideal which doesn't contain 1 (and that justifies that the zero ring has also no maximal ideal, and in fact no prime ideal).

3.3. **Radical ideals.**

Definition 3.12. An ideal $I \subseteq R$ is *radical* if the following holds: for all $a \in I$ and $n \geq 1$, if $a^n \in I$ then $a \in I$.
A ring R is *reduced* if $(0) \subseteq R$ is a radical ideal. In other words, for all $a \in R$, if $a^n = 0$ for some $n \geq 1$, then $a = 0$.

We observe that if $I \subseteq R$ is radical, then R/I is reduced: if $[a]_I \in R/I$ is an element and $[a]_I^n = [a^n]_I$ is a power of $[a]_I$ that vanishes in R/I, then we must have $a^n \in I$, and since I was a radical ideal of R we then have $a \in I$, i.e. $[a]_I$ is zero.
In general, an element a of a ring R admitting a vanishing power a^n for some $n \geq 1$ is called a *nilpotent* element.

Example 3.13. Let $n \geq 1$ be a natural number, and write $n = p_1^{a_1} \dots p_r^{a_r}$ for the factorisation of n into prime factors, with $p_1, \dots, p_r$ different primes numbers and $a_1, \dots, a_r$ all positive. Then (n) is a radical ideal if and only if $a_1 = \dots = a_r = 1$, i.e. if and only if $n = p_1 \dots p_r$ is the product of distinct prime numbers. Indeed, let $q := p_1 \dots p_r$ and let $a = \max_{i=1}^r a_i$; then q^a is a multiple of n, so $q^a \in (n)$, and if we assume (n) radical we must have $q \in (n)$, implying the equality $a_1 = \dots = a_r = 1$; conversely, if $n = p_1 \dots p_r$, then for any $b \in \mathbb{Z}$ and any $c \geq 1$, if $n \mid b^c$ we must have that each prime factor p_i occurs with positive exponent in the factorisation of b, and this implies $n \mid b$.

Example 3.14. Let $X \subset k^n$ be a subset, and consider the ideal $\mathbb{I}(X) \subseteq k[x_1, \dots, x_n]$; we claim that $\mathbb{I}(X)$ is a radical ideal: for if $P \in k[x_1, \dots, x_n]$ is a polynomial with $(P_*|_X)^n = (P^n)_*|_X \equiv 0$ for some $n \geq 1$, for each point $x \in X$ we have that the element $P_*(x) \in k$ vanishes when raised to the n^{th} power; since k is a field, we just have $P_*(x) = 0$ for all $x \in X$, and this implies that$P_*|_X = (P^n)_*|X$, implying that $P \in \mathbb{I}(X)$.

Exercise 3.15. Prove that a prime ideal $\mathfrak{p} \subset R$ is always a radical ideal. Prove also that if $(I_i)_{i \in \mathcal{I}}$ is a family of radical ideals, then the intersection $\bigcap_{i \in \mathcal{I}} I_i$ is again a *radical* ideal.

Definition 3.16. Let $I \subseteq R$ be an ideal. The *radical* of I, denoted $\sqrt{I} \subseteq R$, is the ideal of all elements $a \in R$ such that $a^n \in I$ for some $n \geq 1$.

The previous definition requires a little check, namely that the set of elements of R admitting a power inside I is indeed an ideal, and not just a subset of R. For this, let $m, m' \in \sqrt{I}$ and let $a \in R$, and let's try to prove that $am + m' \in \sqrt{I}$. Fix integers $n, n' \geq 1$ such that $m^n, m'^{n'} \in I$; then we have

$$(am + m')^{n+n'} = \sum_{i=0}^{n+n'} \binom{n+n'}{i} (am)^i (m')^{n+n'-i};$$

and now we observe that each term of the previous sum is a multiple of at least one among m^n or $(m')^{n'}$, and thus lies in I. This shows that $\sqrt{I} \subset R$ is indeed an ideal.

Exercise 3.17. Let $I \subseteq R$ be an ideal; prove that $\sqrt{I}$ is a radical ideal; and if I is already radical, prove/observe by definition that $\sqrt{I} = I$. Prove also that if $I \subseteq J$ are two ideals in R, then $\sqrt{I} \subseteq \sqrt{J}$.

Example 3.14 also shows that for any ideal $I \subset k[x_1, \dots, x_n]$ we have $\sqrt{I} \subseteq \mathbb{I}(\mathbb{V}(I))$, because we already knew (or it is a simple observation) that $I \subseteq \mathbb{I}(\mathbb{V}(I))$, and now we can apply $\sqrt{-}$ to both sides. This gives an explanation of what is going on in the first part of Example 2.39: the ideal $\mathbb{I}(\mathbb{V}(x^2))$ is not (x^2) but its radical, which turns out to be $(x) = \sqrt{(x^2)}$. But the second part still remains mysterious, as the ideal $(x^2+1) \subseteq \mathbb{R}[x]$ is already radical (it is even a prime, and even a maximal ideal: what kind of field is the quotient $\mathbb{R}[x]/(x^2+1)$?), but we also know that (x^2+1) is a proper ideal... We will see later in the course the Nullstellensatz, explaining what is going on (or rather, giving the fault to $\mathbb{R}$ and the fact that it is not an algebraically closed field).

Example 3.18. In general, if $I, J \subseteq R$ are radical ideals, the intersection $I \cap J$ is radical, but neither the product IJ nor the sum $I + J$ is radical:

- for the first, take $I = J = (n)$ and $R = \mathbb{Z}$;
- for the second, take $R = \mathbb{R}[x, y]$ and let $I = (x^2 - y)$ and $J = (y)$; then both I and J are prime ideals (for instance, prove that both quotients R/I and R/J are isomorphic to the domain $\mathbb{R}[x]$), hence they are radical ideals. Yet the sum $I+J$ contains the element $x^2 = (x^2-y)+y$, but it does not contain the element x. For this last statement, notice that $I + J$ is contained in the even larger ideal $(x^2, y) \subseteq \mathbb{R}[x, y]$, which also does not contain x (prove it!).

After Exercise 3.15 we know that the intersection of a family of prime ideals in a ring R is always a radical ideal. In fact, the converse holds.

Proposition 3.19. *Let I be an ideal in R; then*

$$\sqrt{I} = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(R) \,:\, I \subseteq \mathfrak{p}} \mathfrak{p}.$$

In particular the intersection of all prime ideals of R is precisely the ideal $\sqrt{(0)}$, i.e. the set of all nilpotent elements of R.

Proof. We assume that I is a proper ideal, the case $I = R$ is left as exercise/nodding. The inclusion $\sqrt{I} \subseteq \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p}$ follows from the inclusion $I \subseteq \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p}$ by applying $\sqrt{-}$. For the converse, let $a \in R$ and assume that $a \notin \sqrt{I}$; this means that the set $T = \{1, a, a^2, a^3, \dots\}$ of all powers of a is disjoint from I. By Proposition 3.11 we can then find a maximal ideal among those that contain I and are disjoint from T, and since T is closed under product, we know that this maximal ideal will be a prime ideal, and we denote it $\tilde{\mathfrak{p}}$. We then have $a \notin \tilde{\mathfrak{p}}$, so that $a \notin \bigcap_{I \subseteq \mathfrak{p}} \mathfrak{p}$. □

We showed that (0) is the intersection of all prime ideals in any ring R. What about the intersection of all *maximal* ideals?

Definition 3.20. The *Jacobson ideal* of a ring R is the ideal

$$J(R) := \bigcap_{\mathfrak{m} \in \mathrm{Spec}(R) \,|\, \mathfrak{m} \text{ maximal}} \mathfrak{m}$$

Elements of the Jacobson ideal admit also the following characterisation:

Lemma 3.21. *Let $a \in R$; then $a \in J(R)$ if and only if $1 - ab$ is invertible for all $b \in R$.*

Proof. Suppose first that $a \in J(R)$, and for the sake of contradiction, suppose that $1 - ab$ is not invertible for some $b \in R$; then the principal ideal $(1 - ab) \subseteq R$ is proper, and by Proposition 3.11 it is contained in some maximal ideal $\mathfrak{m}$; it follows that $\mathfrak{m}$ contains both a and $1-ab$, and hence $1 \in \mathfrak{m}$, contradicting that $\mathfrak{m}$ is proper. Conversely, suppose that a is such that $1 - ab$ is invertible for all $b \in R$, and for the sake of contradiction, suppose that $\mathfrak{m}$ is a maximal ideal not containing a; then the ideal $(a, \mathfrak{m})$ is strictly larger than $\mathfrak{m}$, so it has to be the entire ring R: it follows that $1 \in (a, \mathfrak{m})$ can be expressed as $1 = ab + m$, for some $b \in R$ and some $m \in \mathfrak{m}$. In other words, $m = 1 - ab \in \mathfrak{m}$, but since we assumed $1 - ab$ invertible we have again $\mathfrak{m} = R$, contradicting that $\mathfrak{m}$ is proper. □

We conclude with a definition, on which we will have time to elaborate in the future.

Definition 3.22. A ring R is *local* if it admits exactly one maximal ideal $\mathfrak{m}$. In this case we also clearly have $J(R) = \mathfrak{m}$.

4. Localization of rings

Warning: part of the notes in this section are copied from the lecture notes for the course "Homological Algebra" that I taught in 2021-2022. All mistakes contained there (and new ones) are present here.
Recall that, for a ring R, the sum makes R into an additive *group*, but the product only makes R into a multiplicative *monoid*: in particular, not all elements of R need to have a multiplicative inverse (and we saw, for instance, that only in the zero ring the element 0 has an inverse!).
The basic idea behind the notion of *localization* is that given a ring R and a set $T \subset R$ of admissible "denominators", we can construct a new ring R_T (sometimes denoted $T^{-1}R$ or $R[T^{-1}]$) containing fractions of elements of R with an element of T as denominator. This should generalise the construction of $\mathbb{Q}$ as ring of fractions of elements of $\mathbb{Z}$, with an element of $\mathbb{Z} \setminus \{0\}$ as denominator.

4.1. Definition of localization and first examples.

Definition 4.1. Let R be a ring, and recall that $a \in R$ is *invertible* if there is an element $a^{-1} \in R$ with $aa^{-1} = 1$. We denote by $R^\times \subseteq R$ the subset of invertible elements.

For example, if k is a field, then $k^\times = k \setminus \{0\}$; instead $\mathbb{Z}^\times = \{\pm 1\}$; in the zero ring the unique element is $0 = 1$, which is invertible (with itself as inverse). We note the following:

- $R^\times$ is an abelian group, with $1 \in R$ as neutral element and with multiplication in R as group operation;
- every ring homomorphism $f\colon R \to S$ sends $R^\times$ inside $S^\times$, and in fact restricts to a map of abelian group $f\colon R^\times \to S^\times$;
- if $f\colon R \to S$ is a ring homomorphism, then the subset $f^{-1}(S^\times) \subseteq R$ is a *multiplicative subset* in the sense of the following definition.

Definition 4.2. A *multiplicative subset* of a ring R is a subset $T \subseteq R$ such that $1 \in T$ and T is closed under product.

Definition 4.3. Let R be a ring and let $T \subset R$ be a multiplicative subset. We define R_T as the set of equivalence classes of couples $(r,t) \in R \times T$: two couples (r,t) and (r',t') are equivalent if there exists $s \in T$ such that $st'r = str'$. We usually denote the equivalence class of the pair $(r,t) \in R \times T$ as a fraction $\frac{r}{t}$.
We define a sum on the set R_T by setting $\frac{r}{t} + \frac{r'}{t'} = \frac{rt'+r't}{tt'}$; the neutral element of the sum is the class $\frac{0}{1}$, and the additive inverse of $\frac{r}{t}$ is $\frac{-r}{t}$.
We define a product on the set R_T by setting $\frac{r}{t} \cdot \frac{r'}{t'} = \frac{rr'}{tt'}$; the neutral element of the product is $\frac{1}{1}$. With this structure, R_T becomes a commutative ring.
Moreover, we have a map of rings $\tau\colon R \to R_T$, called the *localization map* defined by sending $r \mapsto \frac{r}{1}$.

Exercise 4.4. Check that the equivalence relation on $R \times T$ described in Definition 4.3 is indeed an equivalence relation. Check that the sum and the product are well-defined, and make R_T into a ring. And check that the map of sets $\tau\colon R \to R_T$ is indeed a ring homomorphism.

Example 4.5. Let $T = \mathbb{Z} \setminus \{0\}$, which is a multiplicative subset of $\mathbb{Z}$; then the localization $\mathbb{Z}_T$ coincides with the definition of $\mathbb{Q}$ from school, and the map $\tau\colon \mathbb{Z} \to \mathbb{Q}$ is the obvious inclusion.

Example 4.6. More generally, if R is a domain, then $R \setminus \{0\}$ is a multiplicative subset and we can consider the localization $R_{R\setminus\{0\}}$. The latter is also called the *fraction field* of R, denoted $\mathrm{Frac}(R)$, and, as the name suggests, it is a field: indeed given any fraction $\frac{a}{b} \in R_{R\setminus\{0\}}$, either $a = 0$, and then one easily checks that $\frac{a}{b} = \frac{0}{b} = \frac{0}{1}$ in $R_{R\setminus\{0\}}$, or $a \neq 0$, and then one observes that $\frac{b}{a}$ is a multiplicative inverse for $\frac{a}{b}$; thus every non-zero element in $R_{R\setminus\{0\}}$ is invertible.
A particular instance of the previous is when $R = k[x_1, \ldots, x_n]$, the ring of polynomials in n variables with coefficients in a field k: then we obtain the fraction field $k(x_1, \ldots, x_n)$, whose elements are algebraic fractions (fractions of polynomials) in the variables $x_1, \ldots, x_n$.

4.2. **Localization at a prime and local rings.** If R is a ring and $\mathfrak{p} \subset R$ is a prime ideal, then $R \setminus \mathfrak{p}$ is a multiplicative subset of R (this, in fact, characterises prime ideals among ideals), and hence we can form the localization $R_{R\setminus\mathfrak{p}}$; in this situation there is a sort of convenient but inconsistent custom, namely to denote the latter ring by $R_\mathfrak{p}$. So the standard notation is: if $T \subseteq R$ is a multiplicative subset, write R_T according to Definition 4.3, but if $\mathfrak{p} \subset R$ is instead a prime ideal, write $R_\mathfrak{p}$ for what ought to be written $R_{R\setminus\mathfrak{p}}$ according to Definition 4.3...
In the situation above, we let $\mathfrak{m} := \left\{ \frac{a}{b} \in R_\mathfrak{p} \,|\, a \in \mathfrak{p}, b \in R \setminus \mathfrak{p} \right\} \subset R_\mathfrak{p}$ be the set of all equivalence classes representable by a fraction $\frac{a}{b}$ with $a \in \mathfrak{p}$ and $b \notin \mathfrak{p}$.

Exercise 4.7. Check that $\mathfrak{m}$ is an ideal in $R_\mathfrak{p}$, by using the formulas for sum and product from Definition 4.3.

The ideal $\mathfrak{m}$ is proper: if we had $\frac{1}{1} = \frac{a}{b}$ for some a, b with $a \in \mathfrak{p}$ and $b \notin \mathfrak{p}$, then there would be $c \notin \mathfrak{p}$ with $c \cdot a \cdot 1 = c \cdot b \cdot 1$, yet $ca \in \mathfrak{p}$ whereas $cb \notin \mathfrak{p}$, as $\mathfrak{p}$ is a prime ideal. Incidentally, this also proves that $R_\mathfrak{p}$ is not the zero ring.
We notice further that if $\frac{a}{b} \notin \mathfrak{m}$, then $a, b \notin \mathfrak{p}$ and we can talk of the element $\frac{b}{a} \in R_\mathfrak{p}$ as well: this element is a multiplicative inverse of $\frac{a}{b}$. This proves that $R_\mathfrak{p} \setminus \mathfrak{m} \subseteq R_\mathfrak{p}^\times$, and since no element of $\mathfrak{m}$ can be invertible (for then the ideal $\mathfrak{m}$ could not be proper) we have in fact an equality $R_\mathfrak{p} \setminus \mathfrak{m} = R_\mathfrak{p}^\times$.

Every proper ideal $I \subseteq R_{\mathfrak{p}}$ is disjoint from $R_{\mathfrak{p}}^{\times}$, and therefore is contained in $\mathfrak{m}$: this proves that $\mathfrak{m}$ is the unique maximal ideal of $R_{\mathfrak{p}}$, and thus $R_{\mathfrak{p}}$ is an example of a *local* ring, as in Definition 3.22. This also explains why the words "local ring" and "localization of a ring" are similar; it is however not yet clear what kind of "locus" (place) is hidding in this terminology, but we will see at some point.

Example 4.8. Important instances of the previous discussion are the following

- if p is a prime number, then $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$ is the subring of rational numbers that can be written as a fraction $\frac{a}{b}$ with $p \nmid b$; it has a unique maximal ideal, containing all fractions $\frac{a}{b}$ with $p \mid a$;
- consider the ring $\mathbb{C}[x]$ of polynomials in one variables, and its (maximal, hence prime) ideal (x); then $\mathbb{C}[x]_{(x)}$ is the subring of $\mathbb{C}(x)$ of algebraic fractions $\frac{P}{Q}$ such that $Q_*(0) \neq 0$ (or in other words, the constant term of Q is non-zero); $\mathbb{C}[x]_{(x)}$ has a unique maximal ideal, given by the fractions $\frac{P}{Q}$ in which P is divisible by x (has vanishing constant term); the ring $\mathbb{C}[x]?(x)$ can also be included in the ring $\mathbb{C}[[x]]$ of formal Laurent series in one variable, which is again a local ring (can you prove this latter statement? Hint: the unique maximal ideal contains all $\sum_{i=0}^{\infty} a_i x^i$ with $a_0 = 0 \in \mathbb{C}$)

Exercise 4.9. Let R be a ring and let $I \subset R$ be a proper ideal. Prove that the following are equivalent:

(1) R is a local ring, with unique maximal ideal I;
(2) $R \setminus I \subseteq R^{\times}$;
(3) I is maximal and every element of the form $1 + m$ with $m \in I$ is invertible.

The following is another particular example of localization to keep in mind.

Example 4.10. Let R be a ring, let $t \in R$, and let $T = \{1, t, t^2, \dots\}$ be the multiplicative set of all powers of t. In this case the ring R_T is often denoted R_t; the elements of R_T can be expressed as fractions $\frac{a}{t^n}$ for some $n \geq 0$. In particular we have:

- if $R = \mathbb{Z}$ and $t = n = p_1^{a_1} \dots p_r^{a_r}$ is a positive integer with its prime factorisation, then $\mathbb{Z}_n$ is the subring of $\mathbb{Q}$ of rational numbers that can be expressed as a fraction $\frac{a}{b}$, where all prime factors of b are in the set $\{p_1, \dots, p_n\}$;
- if $R = k[x_1, \dots, x_n]$ and $t = Q$ is a non-zero polynomial, then every element $\frac{P}{Q^r} \in k[x_1, \dots, x_n]_Q$ gives rise to a function $(\frac{P}{Q^r})_* \colon k^n \setminus \mathbb{V}(Q) \to k$, sending a point $(a_1, \dots, a_n) \mapsto \frac{P_*(a_1,\dots,a_n)}{Q_*(a_1,\dots,a_n)^r}$; this is well-defined because the function $Q_* \colon k^n \to k$ attains only non-zero values on $k^n \setminus \mathbb{V}(Q)$; considering all algebraic fractions together, we obtain a map of rings
$$-_* \colon k[x_1, \dots, x_n]_Q \to k^{k^n \setminus \mathbb{V}(Q)},$$
such that the following diagram of ring homomorphisms commutes
$$\begin{array}{ccc} k[x_1, \dots, x_n] & \xrightarrow{-_*} & k^{k^n} \\ \downarrow \tau & & \downarrow \text{restrict} \\ k[x_1, \dots, x_n]_Q & \xrightarrow{-_*} & k^{k^n \setminus \mathbb{V}(Q)} \end{array}$$

Exercise 4.11. Let R be a ring and $t \in R$. We want to prove that R_t is isomorphic, as an R-algebra, to the quotient ring $R[x]/(1 - tx)$:

- Prove that the R-algebra homomorphism $R[x] \to R_t$ sending $x \mapsto \frac{1}{t}$ sends the ideal $(1-tx)$ to 0 and thus factors through an R-algebra homomorphism $f\colon R[x]/(1-tx) \to R_t$;
- Prove that the R-algebra homomorphism $R \to R[x]/(1-tx)$ sends t to an invertible element; deduce that it factors through an R-algebra homomorphism $g\colon R_t \to R[x]/(1-tx)$;
- Prove that f and g are inverse of each other.

Exercise 4.11 can of course be generalised in the following way: if R is a ring, and $T \subseteq R$ is a multiplicative subset, then in particular $(T, \cdot, 1)$ is a multiplicative monoid. We can let $\mathcal{I} \subseteq T$ be a subset generating T as a monoid, and we can consider the quotient R-algebra

$$S := R[x_t \,|\, t \in \mathcal{I}]/(1 - tx_t \,|\, t \in \mathcal{I})$$

where we start from the the polynomial algebra $R[x_t \,|\, t \in \mathcal{I}]$ and we quotient by the ideal generated by all elements of the form $1-tx_t$, for varying $t \in \mathcal{I}$. One can again prove that S is isomorphic to R_T. As the construction suggests in the case in which $\mathcal{I}$ is infinite, one should not expect S to be finitely generated as an R-algebra (and even less as an R-module!). So in general R_T is *not* a finitely generated R-algebra.

Example 4.12. Consider $\mathbb{Q} = \mathbb{Z}_{(0)}$; then for any finite set of fractions

$$\left\{ \frac{a_1}{b_1}, \dots, \frac{a_r}{b_r} \right\} \subset \mathbb{Q},$$

the sub-$\mathbb{Z}$-algebra of $\mathbb{Q}$ generated by $\frac{a_1}{b_1}, \dots, \frac{a_r}{b_r}$ is not the entire $\mathbb{Q}$: for instance, it doesn't contain the fraction $\frac{1}{p}$, where p is a prime number not dividing the product $b_1 \dots b_r$.

4.3. **Properties of the localization map.** We remark the following property of the map $\tau\colon R \to R_T$ from Definition 4.3: the image of the multiplicative set $T \subseteq R$ is contained in $(R_T)^times$: indeed an element $t \in T \subseteq R$ is sent to $\tau(t) = \frac{t}{1}$, which is invertible in R_T with inverse $\frac{1}{t}$.

Exercise 4.13. There is in fact a characterising property for the localization R_T: prove that for any ring S and any ring homomorphism $f\colon R \to S$, if $f(T) \subseteq S^\times$ then there is a unique ring homomorphism $\check{f}\colon R_T \to S$ such that $f = \check{f} \circ \tau$, i.e. the following diagram commutes

$$\begin{array}{ccc} R & \xrightarrow{\tau} & R_T \\ & \searrow^{f} & \downarrow{\scriptstyle \check{f}} \\ & & S. \end{array}$$

(Viceversa, it is clear that if $\check{f}\colon R_T \to S$ is any ring homomorphism then the composite $\check{f} \circ \tau\colon R \to S$ sends T inside $S^\times$)

Lemma 4.14. *The kernel of $\tau\colon R \to R_T$ consists of all elements $a \in R$ for which there exists $s \in T$ with $sa = 0 \in R$.*

Proof. Let $a \in R$; then $\tau(a) = \frac{a}{1}$ vanishes in R_T if it is equal to $\frac{0}{1}$; by the definition of the equivalence relation, this happens if and only if there is $s \in T$ with $s \cdot a \cdot 1 = s \cdot 1 \cdot 0 = 0$. □

In particular, the localization R_T is the zero ring if and only if $\ker(\tau) = R$ (for otherwise at least 1_R would be sent to 1_{R_T}), which happens if and only if $1 \in \ker(\tau)$, which by Lemma 4.14 happens if an only if $0 \in T$.

Lemma 4.15. *The map $\tau\colon R \to R_T$ is bijective if and only if $T \subseteq R^\times$.*

Proof. Assume first that τ is bijective. Then τ is in particular injective, and by Lemma 4.14 this implies that for all $t \in T$ the map $t \cdot -\colon R \to R$ is injective. Let now $t \in T$ and consider the element $\frac{1}{t} \in R_T$; by surjectivity of τ, there must be an element $a \in R$ such that $\frac{1}{t} = \frac{a}{1}$, and by the definition of the equivalence relation giving rise to fractions, we must have, for some $s \in T$, the equality $sat = s$; we now use that $s \cdot -\colon R \to R$ is injective and "cancel" a factor s on both sides, obtaining the equality $at = 1$, that is, $t \in R^\times$.
Viceversa, if $T \subseteq R^\times$, then τ is injective by Lemma 4.14, as each map $s \cdot -\colon R \to R$ is injective for $s \in T$; to prove that τ is surjective, we observe that, given an element $\frac{a}{t} \in R_T$, we have $\frac{a}{t} = \frac{at^{-1}}{1}$, as witnessed, for $s = 1$, by the equality $att^{-1} = a$. □

Example 4.16. Let $R = \mathbb{Z}/6$ and let $T = \{[1]_6, [2]_6, [4]_6\}$. The map of rings $\bar{f}\colon \mathbb{Z}/6 \to \mathbb{Z}/3$ sending $[n]_6 \mapsto [n]_3$ has the property of sending $[2]_6$ to the element $[2]_3$, which is invertible in $\mathbb{Z}/3$, and similarly for $[4]_6 \mapsto [4]_3 \in \mathbb{Z}/3^\times$. By Exercise 4.13 we obtain a ring homomorphism $f\colon \mathbb{Z}/6_{[2]_6} \to \mathbb{Z}/3$; this ring homomorphism sends $1_{\mathbb{Z}/6_{[2]_6}} \mapsto [1]_3$, and since $[1]_3$ is an additive generator of $\mathbb{Z}/3$, we conclude that f is surjective.
To show that f is injective, we notice that every element in $\mathbb{Z}/6_{[2]_6}$ can be written in the form $\frac{[a]_6}{[2]_6}$ with a even: indeed we can start from any fraction $\frac{[b]_6}{[2]_6^n}$ and then force b to be even and n to be positive and odd by multiplying numerator and denominator by a suitable, positive power of $[2]_6$. We then notice that an odd power of $[2]_6$ is equal to $[2]_6$ in $\mathbb{Z}/6$. This shows that $\mathbb{Z}/6_{[2]_6}$ has at most 3 elements, and hence f must be injective.
In particular the map $\tau\colon \mathbb{Z}/6 \to \mathbb{Z}/6_{[2]_6} \cong \mathbb{Z}/3$ is not injective.

Exercise 4.17. Let $T \subseteq T' \subseteq R$ be two multiplicative subsets. Construct a natural homomorphism of R-algebras $R_T \to R_{T'}$ (where both rings have an R-algebra structure given by the two maps called τ); prove in fact that there is exactly one homomorphism of R-algebras $R_T \to R_{T'}$, i.e. the choice you made was actually forced.
Assume now that R is a domain and that $T' = R \setminus \{0\}$. Prove that the natural map $R_T \to R_{(0)}$ is injective; so every localization of a domain is a subring of its fraction field, just as in Example 4.8.

Exercise 4.18. We say that a multiplicative subset T in a ring R is *saturated* if $R^\times \subseteq T$ and if whenever $a, b \in R$ and $ab \in T$, then we have $a, b \in T$. Prove that every multiplicative subset admits a *saturation* $\bar{T}$, i.e. a smallest saturated multiplicative subset containing T. Prove also that the canonical map $R_T \to R_{T'}$ from Exercise 4.17 is an isomorphism of R-algebras.

5. Ideals of localizations and spectra of rings

In Subsection 4.2 we have seen that if R is a ring and if $\mathfrak{p} \subset R$ is a prime ideal, then the ring $R_\mathfrak{p} := R_{R\setminus\mathfrak{p}}$ is local, with maximal ideal given by the fractions $\frac{a}{b}$ with $a \in \mathfrak{p}$.

In the following we ask ourselves the generic questions: how do ideals in R_T compare with the ideals of R?

5.1. **Extension and contraction.** In general, we have seen that a ring homomomorphism $f\colon R \to S$ can be used to "transfer" ideals of one ring to one of the other.

- If $J \subseteq S$ is an ideal, then $f^{-1}(J) \subseteq R$ is also an ideal; we have also seen that if J is proper/prime, then also $f^{-1}(J)$ is proper/prime; after Proposition 3.19, we can observe that if J is radical, i.e. an intersection of prime ideals, then also $f^{-1}(J)$ is an intersection of prime ideals, i.e. radical.
- If $I \subseteq R$ is an ideal, then in general $f(I) \subseteq S$ is not an ideal, but we can always consider the ideal $(f(I)) \subseteq S$ generated by $f(I)$; in general we cannot expect much about the new ideal given knowledge of the old one, for example even if I is proper, $(f(I))$ may well be the entire S.

The two operations on ideals considered above are called "contraction" and "extension"; one sometimes denotes the contraction of J by $J^c = f^{-1}(J)$ and the extension of I by $I^e = (f(I))$.
We now fix a multiplicative subset T of a ring R and focus on the ring homomomorphism $\tau\colon R \to R_T$. In this setting, we have the following.

- If $J \subseteq R_T$ is an ideal, then $J^c \subseteq R$ is the subset of all $a \in R$ such that $\frac{a}{1} \in J$; note that if $\frac{a}{1} \in J$, then in fact $\frac{a}{t} \in J$ for all $t \in T$.
- If $I \subseteq R$ is an ideal, then $I^e \subseteq R_T$ is the ideal generated by all fractions $\frac{a}{1}$ with $a \in I$. This coincides with the subset J of R_T of all elements that can be represented as $\frac{a}{t}$ with $a \in I$ and some $t \in T$: indeed $J \subseteq R_T$ is easily checked to be an ideal (using that I is an ideal) and J contains the generators of I^e, so that $I^e \subseteq J$; conversely, every element of J has the form $\frac{a}{1} \cdot \frac{1}{t}$ with $a \in I$, and hence $J \subseteq I^e$.

The next lemma answers the question: when is I^e proper?

Lemma 5.1. *In the setting above, let $I \subseteq R$ be an ideal; then $I^e = (\tau(I)) \subseteq R_T$ is proper if and only if $I \cap T = \emptyset$.*

Proof. Let us prove that $I^e = R_T$ if and only if there exists an element $t \in I \cap T$. If we assume $I^e = R_T$, then $\frac{1}{1} \in R_T$, and by the characterisation above we have that $\frac{1}{1}$ can be represented as $\frac{a}{s}$ for some $a \in I$ and $s \in T$; the equality $\frac{1}{1} = \frac{a}{s}$ is witnessed by some $s' \in T$ such that $s' \cdot a \cdot 1 = s' \cdot 1 \cdot s$, and this implies that the element $t = s'a = s's$ belongs both to I and to T. If instead we assume the existence of $t \in I \cap T$, then the element $\frac{t}{t}$ belongs to I^e by the description given above, but this element is $1 \in R_T$. □

Lemma 5.2. *In the setting above, let $J \subseteq R_T$ be an ideal. Then $(J^c)^e = J$.*

Proof. In general, for a ring homomomorphism $f\colon R \to S$ and an ideal $J \subseteq S$ we have that $f(f^{-1}(J)) \subseteq J$, and hence also the ideal of S generated by $f(f^{-1}(J))$ is contained in J. In our situation, this proves that $(J^c)^e \subseteq J$. For the other containment, let $\frac{a}{t} \in J$; then also $\frac{a}{1} = \frac{a}{t} \cdot \frac{t}{1} \in J$, and thus $a \in J^c$; it follows that $\frac{a}{1} \in (J^c)^e$, and finally we have $\frac{a}{1} \cdot \frac{1}{t} \in (J^c)^e$. □

In general, for $I \subseteq R$, one has $I \subseteq (I^e)^c$, but equality does not hold: for instance, as soon as $I \cap T \neq \emptyset$ one has $(I^e)^c = R$.

Example 5.3. If you don't like the previous argument because it involves non-proper ideals, consider the following: let $T = \{x^n \mid n \geq 0\}$ be the set of all powers of x in $R = \mathbb{Q}[x, y]$, and consider the principal ideal $I = (xy) \subseteq \mathbb{Q}[x, y]$; then the extension $I^e \subseteq \mathbb{Q}[x, y]_x$ is the principal ideal generated by $\frac{xy}{1}$; this is the same as the principal ideal generate by $\frac{y}{1}$, as we can multiply the generator by an invertible element in $\mathbb{Q}[x, y]_x$, for instance $\frac{1}{x}$. The contraction of I^e is then $(y) \subseteq \mathbb{Q}[x, y]$. So we have $((xy)^e)^x = (y)$, and similarly you can check that $((y)^e)^c = (y)$.

In Example 5.3 it is crucial that (xy) is not a prime ideal in $\mathbb{Q}[x, y]$, as will become clear with the next proposition.

Proposition 5.4. *Let R be a ring, $T \subseteq R$ a multiplicative subset, and consider extension and contraction of ideals along the ring homomomorphism $\tau\colon R \to R_T$. Let $\mathfrak{p} \subset R$ and $\mathfrak{p} \cap T = \emptyset$; then $\mathfrak{p}^e \subset R_T$ is again a prime ideal, and $(\mathfrak{p}^e)^c = \mathfrak{p}$.*

Proof. By Lemma 5.1 we know that $\mathfrak{q} := \mathfrak{p}^e$ is a proper ideal of R_T. Let now $\frac{a}{t}, \frac{b}{t'} \in R_T$ and assume that the product $\frac{ab}{tt'}$ lies in $\mathfrak{q}$; then we can represent the same element $\frac{ab}{tt'}$ by a fraction $\frac{m}{t''}$ with $m \in \mathfrak{p}$. The equality $\frac{ab}{tt'} = \frac{m}{t''}$ must be witnessed by some $s \in T$ for which we have in R the equality $sabt'' = smtt'$; in particular, since $smtt' \in \mathfrak{p}$ (as $m \in \mathfrak{p}$) we must have $sabt'' \in \mathfrak{p}$. Now we use that $\mathfrak{p}$ is prime, so at least one among s, a, b, t'' must lie in $\mathfrak{p}$; the elements s, t'' are excluded, since they lie in T which assumed to be disjoint from $\mathfrak{p}$, so at least one of a, b lies in $\mathfrak{p}$, but this implies that at least one of $\frac{a}{t}, \frac{b}{t'}$ lies in $\mathfrak{q} = \mathfrak{p}^e$. This proves that $\mathfrak{q}$ is a prime ideal.
We now show that $\mathfrak{q}^c = \mathfrak{p}$. The inclusion $\mathfrak{p} \subseteq \mathfrak{q}^c$ is evident, so we focus on the other inclusion. Let now $a \in \mathfrak{q}^c$, then we have $\frac{a}{1} \in \mathfrak{q}$; every element in $\mathfrak{q} = \mathfrak{p}^e$ can be represented as $\frac{b}{t}$ for some $b \in \mathfrak{p}$, and the equality $\frac{a}{1} = \frac{b}{t}$ must be witnessed by some $s \in T$ for which $sat = sb$; again, $sb \in \mathfrak{p}$, hence at least one among s, a, t must lie in $\mathfrak{p}$, and s, t are excluded as they lie in T: we obtain that $a \in \mathfrak{p}$ as desired. □

Recall Subsection 4.2: if $\mathfrak{p} \subset R$ is a prime ideal in a ring, then by Proposition 5.4 prime ideals in $R_\mathfrak{p}$ are in bijection with prime ideals in R that are disjoint from $R \setminus \mathfrak{p}$: of these, $\mathfrak{p}$ is clearly the unique maximal one, and this recovers the fact that $R_\mathfrak{p}$ is a local ring.

5.2. **More on spectra of rings.** Proposition 5.4 has the following striking consequence: the set $\mathrm{Spec}(R_T)$ of prime ideals of R_T is in bijection with the subset of $\mathrm{Spec}(R)$ of those prime ideals that are disjoint from T. The inclusion $\mathrm{Spec}(R_T) \hookrightarrow \mathrm{Spec}(R)$ is moreover given by contraction along the map $\tau\colon R \to R_T$: this map is continuous if we consider on $\mathrm{Spec}(R_T)$ and $\mathrm{Spec}(R)$ the Zariski topology from Subsection 3.1.
We also notice that Lemma 5.2 has the following implication: every ideal $J \subseteq R_T$ can be obtained as extension of some ideal of R, for instance J^c. This implies that not only the map $\mathrm{Spec}(R_T) \hookrightarrow \mathrm{Spec}(R)$ is a continuous injection, but also that the topology on $\mathrm{Spec}(R_T)$ can be recovered as the pullback of the topology of $\mathrm{Spec}(R)$. In other words, if we consider $\mathrm{Spec}(R_T)$ as a subset of $\mathrm{Spec}(R)$, then the Zariski topology on $\mathrm{Spec}(R_T)$ coincides with the subspace topology of the Zariski topology on $\mathrm{Spec}(R)$.

Example 5.5. Let $T = \{1, t, t^2, \dots\} \subseteq R$ and consider the localization $\tau\colon R \to R_t$. Then the above discussion identifies $\mathrm{Spec}(R_T)$ with a subset of $\mathrm{Spec}(R)$, namely

set of those prime ideals $\mathfrak{p}$ of R such that $T \cap \mathfrak{p} = \emptyset$. Notice now that for any prime ideal $\mathfrak{p} \subset R$ we have $1 \notin \mathfrak{p}$, and as soon as some power $t^n \in \mathfrak{p}$ we must also have $t \in \mathfrak{p}$ (prime ideals are radical). Thus for a prime ideal $\mathfrak{p} \subset R$ there are two possibilities:

(1) either $t \notin \mathfrak{p}$, and then $\mathfrak{p} \cap T = \emptyset$ and thus $\mathfrak{p}^e$ is a prime ideal in R_T;
(2) or $t \in \mathfrak{p}$; this is equivalent to the entire principal ideal (t) being contained in $\mathfrak{p}$.

The Zariski topology on $\mathrm{Spec}(R)$ prescribes that the set of primes of type (2) form a closed subset of $\mathrm{Spec}(R)$; it follows that the subset of primes of type (1) forms an open subset; in other words, $\mathrm{Spec}(R_T)$ is an open subset of $\mathrm{Spec}(R)$.

Exercise 5.6. Let R be a ring; prove that the open sets $\mathrm{Spec}(R_t) \subseteq \mathrm{Spec}(R)$, for varying $t \in R$, form a basis for the Zariski topology.

Exercise 5.7. Generalize Example 5.5 to the case in which T is a multiplicative set generated under multiplication by a finite subset of R. Find also an example of a ring R and a multiplicative subset T of R such that $\mathrm{Spec}(R_T)$, considered as a subset of $\mathrm{Spec}(R)$, is not open.

Exercise 5.8. Let R be a ring and $I \subseteq R$ be an ideal, and recall Lemma 2.34. Prove that there is a bijection between prime/maximal/radical ideals of R/I and prime/maximal/radical ideals of R containing I.
Use the previous to show that one can identify $\mathrm{Spec}(R/I)$ with the *closed* subspace of $\mathrm{Spec}(R)$ of all prime ideals containing I. In particular, remember to check that the topology of $\mathrm{Spec}(R/I)$ agrees with the subspace topology of $\mathbb{V}(I)$.

We conclude the subsection by analyzing in detail the spectra of the rings k and $k[x]$, for a field k, as well as $\mathbb{Z}$ and, for a prime number $p \in \mathbb{Z}$, the ring $\mathbb{Z}_{(p)}$.

Example 5.9. Let k be a field. Then, as we have seen, there is a unique proper ideal in k, namely (0), which is therefore also the unique maximal ideal and the unique prime ideal. It follows that $\mathrm{Spec}(k)$ is a topological space with one point. There is exactly one topology on a set with one point, so the Zariski topology is that topology. Someone will say: *What a boring space! How are we going to learn anything about the field k by studying the space with a single point?* That is true, and indeed observe that *all* fields k give rise to the "same" space $\mathrm{Spec}(k)$, where "same" means that these spaces are all homomorphic to each other. But that's just how it is.

Before continuing, let me insert here a definition (that you might have already seen).

Definition 5.10. A *principal ideal domain*, short PID, is a ring R which is a domain (see Definition 3.1) and all of whose ideals are principal, i.e. generated by a single element.

Example 5.11. The ring $\mathbb{Z}$ is a PID, as can be shown using the Euclidean algorithm for division of integers. The elements of $\mathrm{Spec}(\mathbb{Z})$ are (0) and all maximal ideal of the form (p), for (p) a prime number. Each closed subset of $\mathrm{Spec}(\mathbb{Z})$ has the form $\mathbb{V}(n)$, i.e. it is is given by all prime ideals containing a fixed ideal $(n) \subseteq \mathbb{Z}$, for some $n \geq 0$; in particular:

- for $n = 0$ we have $\mathbb{V}(0) = \mathrm{Spec}(\mathbb{Z})$, since (0) is contained in every prime ideal;

- for $n = 1$ we have $\mathbb{V}(1) = \emptyset$, since $(1) = \mathbb{Z}$ is not contained in any prime ideal;
- for $n \geq 2$ we can factor $n = p_1^{a_1} \dots p_r^{a_r}$ into prime factors, with all $a_i \geq 1$: then n is an element of (and with that, (n) is contained in) exactly the prime ideals $(p_1), \dots, (p_r)$.

Notice that any *finite* subset of $\mathrm{Spec}(\mathbb{Z}) \setminus \{(0)\}$ can be obtained as a closed subset of $\mathrm{Spec}(\mathbb{Z})$. Notice also that the only closed subset containing (0) is the entire space $\mathrm{Spec}(\mathbb{Z})$, and this is also the only closed subset with infinite cardinality. The Zariski topology on $\mathrm{Spec}(\mathbb{Z})$ is in particular not Hausdorff.

Example 5.12. Let k be a field and consider the ring $k[x]$ of polynomials in one variable. Using the Euclidean algorithm for division of polynomials, one can prove that $k[x]$ is a PID; more precisely, there are two types of ideals in $k[x]$:

- (0) is an ideal;
- every ideal larger than (0) is generated by some polynomial $P \in k[x]$; up to multiplying P by an element in $k^\times$, we can assume P monic, and in fact for each ideal of $k[x]$ larger than (0) there is a unique monic polynomial $P \in k[x]$ such that the ideal is (P).

An ideal of $k[x]$ is prime if and only if it is (0) or it is (P) with P a monic and irreducible polynomial. Thus $\mathrm{Spec}(k[x])$ is in bijection with the set of irreducible monic polynomials in $k[x]$, together with 0.
The topology on $\mathrm{Spec}(k[x])$ has the following closed subsets:

- $\mathrm{Spec}(k[x])$ and $\emptyset$ are closed;
- every other closed subset has the form $\mathbb{V}(Q)$, for some monic polynomial $Q \in k[x]$, and it contains those prime ideals corresponding to the irreducible factors of Q.

Every finite subset of the set of prime ideals corresponding to monic irreducible polynomials of $k[x]$ can be obtained as $\mathbb{V}(Q)$ for some Q, e.g. take Q equal to the product of the irreducible polynomials whose associated prime ideals belong to the given finite subset. We notice that the only closed subset containing the prime ideal (0) is the entire $\mathrm{Spec}(k[x])$, and all other closed subsets are finite.

Examples 5.11 and 5.12 show a similarity between the rings $\mathbb{Z}$ and $k[x]$: on the one hand both of them are PIDs, on the other hands the spaces $\mathrm{Spec}(\mathbb{Z})$ and $\mathrm{Spec}(k[x])$ have essentially the same description: this tells us that the way in which ideals and prime ideals are nested inside $\mathbb{Z}$ is similar in flavour to the way in which ideals and prime ideals are nested inside $k[x]$.

Exercise 5.13. In fact one can prove that for any PID R the same phenomenon happens: the set $\mathrm{Spec}(R)$ consists of the prime ideal (0) and the maximal ideals of R (i.e., (0) is the only prime ideal which is not maximal); moreover the closed subsets of $\mathrm{Spec}(R)$ are precisely the entire $\mathrm{Spec}(R)$ and all finite subsets not containing (0). Try to prove it!

Example 5.14. Let $p \geq 2$ be a prime number, and let us analyse the spectrum of the ring $\mathbb{Z}_{(p)}$, i.e. the localization of $\mathbb{Z}$ at the multiplicative subset $\mathbb{Z} \setminus (p)$; recall that $\mathbb{Z}_{(p)}$ can also be regarded as the subring of $\mathbb{Q}$ containing all rational numbers that can be represented as $\frac{a}{b}$ with $p \nmid b$.
There are exactly two prime ideals in $\mathbb{Z}_{(p)}$, namely (0) and (p) (here we regard $p = \frac{p}{1}$ as an element of $\mathbb{Z}_{(p)}$), as a consequence of Proposition 5.4. Similarly, using

Lemmas 5.1 and Lemma 5.2, one can show that each ideal of $\mathbb{Z}_{(p)}$ is either (0) or of the form (p^r) for some $r \geq 0$ (the entire ring $\mathbb{Z}_{(p)}$ arising exactly in the case $r = 0$). For all $r \geq 1$ we have $\mathbb{V}(p^r) = \{(p)\}$, and hence we have exactly three closed subsets in $\mathrm{Spec}(\mathbb{Z}_{(p)})$, namely $\emptyset$, $\{(p)\}$ and $\{(0), (p)\}$.
So $\mathrm{Spec}(\mathbb{Z}_{(p)})$ is the topological space with two points, (0) and (p), such that (0) is an open but not closed point, whereas (p) is a closed but not open point. Note that this description does not depend on the prime number p.

Exercise 5.15. Consider the ring $\mathbb{C}[[x]]$ of formal Taylor expansions in the variable x over $\mathbb{C}$, and prove that $\mathrm{Spec}(\mathbb{C}[[x]])$ is also a space with two points, one being open and the other closed, as in Example 5.14.

5.3. **Elements of the ring as functions on the spectrum.** In this subsection we discuss, for a ring R, how to think of an element $a \in R$ as a function defined on the space $\mathrm{Spec}(R)$; this mimics how a polynomial $P \in k[x_1, \ldots, x_n]$ gives rise to a function $P_* \colon k^n \to k$.

Definition 5.16. Let R be a ring and let $\mathfrak{p} \subseteq R$ be a prime ideal; then the ring $R_{\mathfrak{p}}$ is local, with unique maximal ideal given by $\mathfrak{p}^e$. The *residue field* of R at $\mathfrak{p}$ is the field $R_{\mathfrak{p}}/\mathfrak{p}^e$, which we denote by $\mathbf{k}(\mathfrak{p})$.

Notice that for each prime ideal $\mathfrak{p}$ we can also first quotient R by $\mathfrak{p}$, obtaining a domain $R/\mathfrak{p}$, and then take the fraction field $\mathrm{Frac}(R/\mathfrak{p})$, i.e. localize $R/\mathfrak{p}$ at its prime ideal (0). The field $\mathrm{Frac}(R/\mathfrak{p})$ is in fact canonically isomorphic to $\mathbf{k}(\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}^e$. We moreover have a ring homomomorphism $R \to \mathbf{k}(\mathfrak{p})$, given either by the composition $R \xrightarrow{\tau} R_{\mathfrak{p}} \twoheadrightarrow R_{\mathfrak{p}}/\mathfrak{p}^e = \mathbf{k}(\mathfrak{p})$ or $R \twoheadrightarrow R/\mathfrak{p} \hookrightarrow \mathrm{Frac}(R/\mathfrak{p}) = \mathbf{k}(\mathfrak{p})$.
We can now consider the ring $\prod_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathbf{k}(\mathfrak{p})$, i.e. the product of all residue fields of prime ideals of R; an element of $\prod_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathbf{k}(\mathfrak{p})$ can be thought of as a "function" defined on the space $\mathrm{Spec}(R)$ and with field values: yet for each point $\mathfrak{p} \in \mathrm{Spec}(R)$, the value of the function at $\mathfrak{p}$ is an element of the corresponding residue field $\mathbf{k}(\mathfrak{p})$, which depends on the point. We have a canonical ring homomomorphism $\theta \colon R \to \prod_{\mathfrak{p} \in \mathrm{Spec}(R)} \mathbf{k}(\mathfrak{p})$, sending $a \in R$ to the function $\mathfrak{p} \mapsto [a]_{\mathfrak{p}} \in \mathrm{Frac}(R/\mathfrak{p}) = \mathbf{k}(\mathfrak{p})$. Thus we can see elements of R as some sort of functions on the space $\mathrm{Spec}(R)$.
Classically, one is interested in a topological space X and in order to understand its properties one studies a ring of functions defined over X (or possibly functions with some extra properties, e.g. continuous, smooth, holomorphic...). The above shows that, to some extent, also the converse is possible: given a ring R, we can construct a space, namely $\mathrm{Spec}(R)$, such that elements of R can be regarded as functions on $\mathrm{Spec}(R)$.

Example 5.17. Let $R = \mathbb{C}[x]$, and recall from Example 5.12 that $\mathrm{Spec}(\mathbb{C}[x])$ contains the point (0) and a point (P) for each monic, irreducible polynomial $P \in \mathbb{C}[x]$. Now, since $\mathbb{C}$ is algebraically closed, each irreducible monic polynomial in $\mathbb{C}[x]$ has the form $x - a$, for some $a \in \mathbb{C}$: this shows that $\mathrm{Spec}(\mathbb{C}[x])$ is in bijection with the set $\{(0)\} \sqcup \mathbb{C}$. To avoid confusion, we will denote by $\eta \in \mathrm{Spec}(\mathbb{C}[x])$ the point (0), whereas $0 \in \mathbb{C} \subset \mathrm{Spec}(\mathbb{C}[x])$ is really the ideal $(x) = (x - 0)$.
For each $a \in \mathbb{C}$, the residue field $\mathbf{k}(x-a)$ of $\mathbb{C}[x]$ at $(x-a)$ is the quotient $\mathbb{C}[x]/(x-a)$: since $(x-a)$ is already a maximal ideal, the quotient is already a field and we don't need to take the fraction field. Now we can identify the rings $\mathbb{C}[x]/(x-a)$ and $\mathbb{C}$ as follows: the ring homomomorphism $\mathbb{C}[x] \twoheadrightarrow \mathbb{C}$ sending $P \mapsto P_*(a)$ vanishes on the ideal $(x - a)$, and thus it induces a ring homomomorphism $\mathbb{C}[x]/(x - a) \to \mathbb{C}$

which is in fact an isomorphism. We conclude that all residue fields $\mathbf{k}(x-a)$ are isomorphic to $\mathbb{C}$, for all $a \in \mathbb{C}$. Still, we have $\mathbf{k}(\eta) = \mathbb{C}(x)$, i.e. the fraction field of $\mathbb{C}[x]$.
And now let us see what kind of function on $\mathrm{Spec}(\mathbb{C}[x])$ an element $P \in \mathbb{C}[x]$ induces along θ:

- the point η is sent to the element $P = \frac{P}{1} \in \mathbb{C}(x)$;
- every other point $a \in \mathbb{C} \subset \mathrm{Spec}(\mathbb{C}[x])$ is sent to the element $[P]_{(x-a)} \in \mathbb{C}[x]/(x-a)$, which by the above identification is the element $P_*(a) \in \mathbb{C}$.

So if we identify $\prod_{\mathfrak{p}\in\mathrm{Spec}(\mathbb{C}[x])} \mathbf{k}(\mathfrak{p})$ with the ring $\mathbb{C}(x) \times \mathbb{C}^{\mathbb{C}}$, and if we forgett the component relative to η, the function $\theta(P)$ on $\mathrm{Spec}(\mathbb{C}[x])$ recovers the function $P_*\colon \mathbb{C} \to \mathbb{C}$.

Exercise 5.18. For each field k and each $n \geq 0$ there is an inclusion of sets $k^n \subset \mathrm{Spec}(k[x_1, \dots, x_n])$, given by sending $(a_1, \dots, a_n)$ to the maximal ideal $(x_1 - a_1, \dots, x_n - a_n)$. Find an identification of each residue field $\mathbf{k}(x_1 - a_1, \dots, x_n - a_n)$ with the field k, so that for each $P \in k[x_1, \dots, x_n]$ the function $\theta(P)$ restricts on the subset $k^n \subset \mathrm{Spec}(k[x_1, \dots, x_n])$ to the function $P_*\colon k^n \to k$.

Example 5.19. Each element $n \in \mathbb{Z}$ gives rise to a function $\theta(n)$ on $\mathrm{Spec}(\mathbb{Z})$: this function sends the element $\eta := (0)$ to $n \in \mathbb{Q}$, and it sends $(p) \mapsto [n]_p \in \mathbb{Z}/(p)$. In this case all residue fields are pairwise non-isomorphic!

Examples 5.17 and 5.19 look promising, as suggest that we can *identify* elements of a ring R with certain functions on the space $\mathrm{Spec}(R)$. To ensure that this idenfification is completely unproblematic, we would like the ring homomomorphism $\theta\colon R \to \prod_{\mathfrak{p}\in\mathrm{Spec}(R)} \mathbf{k}(\mathfrak{p})$ to be injective. Is this the case?

Lemma 5.20. *Let R be a ring. Then the kernel of the ring homomomorphism $\theta\colon R \to \prod_{\mathfrak{p}\in\mathrm{Spec}(R)} \mathbf{k}(\mathfrak{p})$ is the* nilradical $\sqrt{(0)}$*, i.e. the ideal of all nilpotent elements in R.*

Proof. Let $a \in \sqrt{(0)}$, i.e. $a \in R$ and $a^n = 0$ for some $n \geq 1$. Then $a \in \mathfrak{p}$ for all prime ideals $\mathfrak{p} \subset R$ (compare also with Proposition 3.19). It follows that $[a]_{\mathfrak{p}} = 0 \in R/\mathfrak{p}$, and hence $\theta(a)\colon \mathfrak{p} \mapsto 0 \in \mathbf{k}(\mathfrak{p})$, so a induces the zero function[7] on $\mathrm{Spec}(R)$, or in other words, $a \in \ker(\theta)$.
Viceversa, let $a \in \ker(\theta)$; then for all $\mathfrak{p} \in \mathrm{Spec}(R)$ we have that $[a]_{\mathfrak{p}}$ vanishes as element of $\mathrm{Frac}(R/\mathfrak{p})$. Now the map $\tau\colon R/\mathfrak{p} \to \mathrm{Frac}(R/\mathfrak{p})$ is injective (this is true for any domain: see also Lemma 4.14), so we must have $[a]_{\mathfrak{p}} = 0$ already in $R/\mathfrak{p}$, i.e. $a \in \mathfrak{p}$. We conclude that $a \in \bigcap_{\mathfrak{p}\in\mathrm{Spec}(R)} \mathfrak{p} = \sqrt{(0)}$ by Proposition 3.19. □

Lemma 5.20 puts some limit to the approach to algebraic geometry in which we consider a ring R as a certain ring of function on $\mathrm{Spec}(R)$, especially if the word "function" is interpreted in the usual set-theoretic sense, i.e. something that can be evaluated at each point of $\mathrm{Spec}(R)$ and that is characterised by its evalutation. The way to represent elements of R faithfully, even if R is not reduced, is to consider a certain *sheaf* of rings on the space $\mathrm{Spec}(R)$. The sheaf, usually denoted $\mathcal{O}_{\mathrm{Spec}(R)}$, associates with every open set U of $\mathrm{Spec}(R)$ a certain ring, whose elements are "regular functions" on U, but we no longer think of an element of $\mathcal{O}_{\mathrm{Spec}(R)}(U)$ as something that can be evaluated on points, rather as something

[7]Pay attention: the "zero function" picks for each $\mathfrak{p} \in \mathrm{Spec}(R)$ a "different" zero, namely the element $0 \in \mathbf{k}(\mathfrak{p})$.

that can be restricted to smaller open subsets contained in U. In particular, the ring $\mathcal{O}_{\mathrm{Spec}(R)}(\mathrm{Spec}(R))$ coincides with R. We stop here this discussion and invite you to attend a course in algebraic geometry if you are curious!

6. Localization of modules

Warning: part of the notes in this section are copied from the lecture notes for the course "Homological Algebra" that I taught in 2021-2022. All mistakes contained there (and new ones) are present here.

Before starting the discussion about localization of modules, let me point out that, given a ring homomorphism $f\colon R \to S$, every S-module M can be given an R-module structure by defining $r \cdot m := f(m) \cdot m$, for $r \in R$ and $m \in M$: we say that M becomes an R-module by *restriction of scalars* along f, and we also write f_*M for this module[8]; in fact the above construction gives a functor $f_*\colon S\mathrm{Mod} \to R\mathrm{Mod}$.[9]

6.1. Definition of localization of modules and first examples.

Definition 6.1. Let R be a commutative ring and let $T \subseteq R$ be a multiplicative subset. An R-module M is *T-local* if for all $t \in T$ the map $t \cdot -\colon M \to M$ is bijective.

Example 6.2. Let $R = \mathbb{Z}$; then $\mathbb{Z}/3$ is 2-local but not 3-local; $\mathbb{Z}$ is not n-local for any $n \geq 2$, as multiplication by n on $\mathbb{Z}$ is injective but not surjective; and $\mathbb{Q}$ is $\mathbb{Z} \setminus \{0\}$-local.

Example 6.3. Let R be a ring and T a multiplicative subset. Let M be an R_T-module, and consider M as an R-module by restriction of scalars along $\tau\colon R \to R_T$. Then M is a T-local R-module: indeed for every element $t \in T$ the map $t \cdot -\colon M \to M$ coincides with the map $\frac{t}{1} \cdot -\colon M \to M$, which has as inverse the map $\frac{1}{t} \cdot -\colon M \to M$ (one of the maps that we might have forgotten).

In fact the converse also holds: if M is a T-local R-module, it is *because* it is obtained from a R_T-module by restriction of scalars. Concretely, for a fraction $\frac{a}{t} \in R_T$ we can define the map $\frac{a}{t} \cdot -\colon M \to M$ as the composition of $a \cdot -\colon M \to M$ and the inverse of the bijection $t \cdot -\colon M \to M$:

$$\tfrac{a}{t} \cdot -\colon M \xrightarrow{a\cdot -} M \xrightarrow{(t\cdot -)^{-1}} M.$$

Check that two equivalent fractions induce the same map $M \to M$; check that these maps assemble into an action of R_T on M, so that the abelian group M becomes an R_T-module, and so that the old R-module structure can be retrieved using the restriction of scalars along τ.

The previous example (almost) shows that the information of a T-local R-module is equivalent to the information of a R_T-module. To make this precise (and complete), you can solve the following exercise.

---

[8] I changed the notation, putting here $_*$ and reserving * for another functor discussed later in the course

[9] If you want to dive into category theory, you can also think of the assignment $R \mapsto R\mathrm{Mod}$ as a contravariant functor from the category of rings to the category of... categories! What we have done is to describe, for a map of rings f, what the associated map of categories (i.e. the associated functor) is.

Exercise 6.4. The restriction of scalars functor τ_* is a functor $R_T\text{Mod} \to R\text{Mod}$ with the following properties:

- it is fully faithful (this boils down to proving that a set-theoretic map between two R_T-modules is an R-linear map if and only if it is also an R_T-linear map);
- its essential image is the full subcategory of RMod spanned by T-local R-modules (this means that precisely the T-local modules can be obtained, up to isomorphism, through the functor τ_*).

Localization of modules can be thought of as a way to pick an R-module M and transform it into a new R-module M_T that is T-local, i.e. into a R_T-module (after Exercise 6.4). The idea is essentially the same as in Definition 4.3

Definition 6.5. Let R be a ring and $T \subset R$ be a multiplicative subset, and let M be an R-module. We define M_T as the set of equivalence classes of couples $(m,t) \in M \times T$: two couples (m,t) and (m',t') are equivalent if there exists $s \in T$ such that $smt' = sm't$. The equivalence class of (m,t) is usually denoted as a fraction $\frac{m}{t}$.
We define a sum on the set M_T by setting $\frac{m}{t} + \frac{m'}{t'} = \frac{t' \cdot m + t \cdot m'}{tt'}$; the neutral element of the sum is $\frac{0}{1}$, and the additive inverse of $\frac{m}{t}$ is $\frac{-m}{t}$.
We define an action of R_T by scalar multiplication on M_T by setting $\frac{r}{t} \cdot \frac{m}{t'} = \frac{r \cdot m}{tt'}$. The set M_T becomes in this way an R_T-module, and hence by Exercise 6.4 it can be also considered as a T-local R-module.
Moreover, we have a map of R-modules $\gamma \colon M \to M_T$ given by $m \mapsto \frac{m}{1}$.

Exercise 6.6. This is similar to Exercise 4.4. Check that the equivalence relation on $M \times T$ described in Definition 6.5 is indeed an equivalence relation. Check that the sum and the product by scalars in R_T are well-defined, and make M_T into an R_T-module. And check that the map of sets $\gamma \colon M \to M_T$ is indeed R-linear.

Exercise 6.7. Prove the following characterising property of the localization of a module: if M is an R-module, N is a T-local R-module for some multiplicative subset $T \subseteq R$, and if $f \colon M \to N$ is R-linear, then there exists a unique R-linear map $g \colon M_T \to N$ such that the following diagram commutes:

$$\begin{array}{ccc} M & \xrightarrow{\gamma} & M_T \\ & \searrow^{f} & \downarrow g \\ & & N. \end{array}$$

Notice that g, as any R-linear map between R_T-modules, is automatically R_T-linear.

6.2. **Functoriality and exactness.** We can now explore the functoriality of the construction transforming an R-module M into an R_T-module M_T. Let $g \colon M \to N$ be an R-linear map. Then the composition $M \xrightarrow{g} N \xrightarrow{\gamma} N_T$ is an R-linear map $M \to N_T$ with source M and target a T-local R-module: by Exercise 6.7 there exists a unique R-linear map $\theta \colon M_T \to N_T$ such that the following diagram commutes

$$\begin{array}{ccc} M & \xrightarrow{g} & N \\ \downarrow \gamma & & \downarrow \gamma \\ M_T & \xrightarrow{\theta} & N_T. \end{array}$$

The map θ is usually denoted g_T; concretely, it sends $\frac{m}{t} \mapsto \frac{g(m)}{t}$. This construction gives rise to a functor $-_T \colon R\text{Mod} \to R_T\text{Mod}$, sending $M \mapsto M_T$ and $(g \colon M \to N) \mapsto (g_T \colon M_T \to N_T)$.

Exercise 6.8. Check that all properties needed for $-_T \colon R\text{Mod} \to R_T\text{Mod}$ are fulfilled.

A crucial property of the localization functor $-_T$ is that it sends exact sequences to exact sequences: in particular, it sends injective R-linear maps to injective R_T-linear maps, and surjective R-linear maps to surjective R_T-linear maps.

Proposition 6.9. *Let R be a commutative ring, and let $T \subset R$ be a multiplicative subset. Then the functor $-_T \colon R\text{Mod} \to R_T\text{Mod}$ is exact.*

Proof. We have to prove that if

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

is a sequence of R-modules and R-linear maps which is exact at N, that is $g \circ f = 0$ and $\ker(g) = \mathrm{Im}(f)$, then the sequence

$$M_T \xrightarrow{f_T} N_T \xrightarrow{g_T} P_T$$

obtained by applying the functor $-_T$ is also exact at N_T. We start by checking that the composition $g_T \circ f_T$ is the zero map from M_T to P_T: given an element $\frac{m}{t} \in M_t$, we readily compute $g_T(f_T(\frac{m}{t})) = \frac{g(f(m))}{t} = \frac{0}{t} = 0$, using that $g \circ f$ is the zero map from M to P. This shows also that $\mathrm{Im}(f_T) \subseteq \ker(g_T)$.
For the opposite containment, let $\frac{n}{t} \in \ker(g_T) \subseteq N_T$. Then in P_T we have $\frac{g(n)}{t} = 0$, and by definition of localization this means that there is $s \in T$ such that $s \cdot g(n) = 0$ in P. This is the same as saying that $g(s \cdot n) = 0$, i.e. $s \cdot n \in \ker(g)$, and by exactness of the first sequence we can conclude that there is $m \in M$ such that $f(m) = s \cdot n$. We can then compute $f_T(\frac{m}{st}) = \frac{f(m)}{st} = \frac{s \cdot n}{st} = \frac{n}{t}$, showing that $\frac{n}{t} \in \mathrm{Im}(f_T)$. □

6.3. **Detecting properties after localization.** Localization is in particular a tool to replace a ring R by a *local* ring $R_\mathfrak{p}$, for any prime ideal $\mathfrak{p} \subset R$, and correspondingly replace R-modules by $R_\mathfrak{p}$-modules; as we will see later in the course, studying local rings and local module is often easier than studying rings and modules in general. We would therefore like to be able to use sistematically a strategy as the following:

(1) start with a problem about a ring R and R-modules;
(2) for each prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$, transform the problem into one about the ring $R_\mathfrak{p}$, which is local, and $R_\mathfrak{p}$-modules;
(3) solve the latter problem, leveraging that $R_\mathfrak{p}$ is local;
(4) solve the original problem about R, using knowledge about all $R_\mathfrak{p}$.

Proposition 6.9 is the kind of result that can help us with step (2), as for instance any exactness hypothesis in the formulation of our problem for R will give rise to an analogue exactness hypothesis for the modified problem for $R_\mathfrak{p}$. We would now like something that can help us with step (4), otherwise it would seem that Proposition 6.9 is not so useful.
In fact, proving that a functor is exact does not imply that the functor is also interesting. Think of the zero functor, say from RMod to SMod, for any two rings R, S, sending each R-module M to the zero S-module. Then the zero functor

is exact, but we are hardly ever going to prove something interesting by solely applying the zero functor!
In the following proposition we will see that localization at all prime ideals (in fact, all maximal ideals suffice!) detects triviality of an R-module.

Proposition 6.10. *Let R be a ring and let M be an R-module. If M is not the zero module, then there exists a maximal ideal $\mathfrak{m} \subset R$ such that $M_\mathfrak{m}$ is not the zero $R_\mathfrak{m}$-module.*

Proof. Let $m \in M$ be a non-zero element. Then the set $\mathrm{Ann}(m) := \{a \in R \,|\, am = 0\}$ is an ideal in R, and by hypothesis it doesn't contain $1 \in R$, i.e. it is a proper ideal. By Proposition 3.11 we can find a maximal ideal $\mathfrak{m}$ containing $\mathrm{Ann}(m)$. We claim that $M_\mathfrak{m} \neq 0$, in particular because $\frac{m}{1} \neq \frac{0}{1} \in M_\mathfrak{m}$. For if we had $\frac{m}{1} = \frac{0}{1}$, there would be an element $s \in R \setminus \mathfrak{m}$ for which the equality $s \cdot m \cdot 1 = s \cdot 0 \cdot 1$, that is, $sm = 0$; but this would mean $s \in \mathrm{Ann}(m)$, whereas $s \in R \setminus \mathfrak{m} \subseteq R \setminus \mathrm{Ann}(m)$. □

Proposition 6.10 has the following corollary.

Corollary 6.11. *Let R be a ring and let $M \xrightarrow{f} N \xrightarrow{g} P$ be a sequence of three R-modules and two R-linear maps. Then the sequence is exact at N if and only if for all maximal ideals $\mathfrak{m} \subset R$ the localized sequence $M_\mathfrak{m} \xrightarrow{f_\mathfrak{m}} N_\mathfrak{m} \xrightarrow{g_\mathfrak{m}} P_\mathfrak{m}$ is exact.*

Proof. One implication is Proposition 6.9, so let us prove the converse: we assume that for each maximal ideal $\mathfrak{m} \subset R$ the sequenc $M_\mathfrak{m} \xrightarrow{f_\mathfrak{m}} N_\mathfrak{m} \xrightarrow{g_\mathfrak{m}} P_\mathfrak{m}$ is exact, and prove that $M \xrightarrow{f} N \xrightarrow{g} P$ is also exact.
We observe, as a consequence of Exercise 6.8, that for all $\mathfrak{m}$ the map $g_\mathfrak{m} \circ f_\mathfrak{m}$ is the same as the localization $(g \circ f)_\mathfrak{m} \colon M_\mathfrak{m} \to P_\mathfrak{m}$ of the composite $g \circ f$.
First, we prove that $g \circ f \colon M \to P$ is the zero map. For this, let $m \in M$; then we know that $g_\mathfrak{m} \circ f_\mathfrak{m}(\frac{m}{1}) = \frac{g \circ f(m)}{1} = 0$ for all maximal ideals $\mathfrak{m}$, and this implies that for each $\mathfrak{m} \subset R$ maximal there is $s \notin \mathfrak{m}$ such that $s \cdot g \circ f(m) = 0$; this implies in turn that $\mathrm{Ann}(g \circ f(m))$ is an ideal of R that is not contained in any maximal ideal, so it has to be the entire ring R, and thus $1 \in \mathrm{Ann}(g \circ f(m))$, i.e. $g \circ f(m) = 0$.
Next we prove that $\ker(g) = \mathrm{Im}(f)$. For this, define the R-module $H = \ker(g)/\mathrm{Im}(f)$; then for all maximal ideals $\mathfrak{m}$ we have $H_\mathfrak{m} = \ker(g)_\mathfrak{m}/\mathrm{Im}(f)\mathfrak{m}$, as the localization at $\mathfrak{m}$ of the short exact sequence of R-modules $\mathrm{Im}(f) \hookrightarrow \ker(g) \twoheadrightarrow H$. By hypothesis we thus have $H_\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m}$, and by Proposition 6.10 this implies that the R-module H vanishes. □

In particular, taking the cases $M = 0$ or $P = 0$ in Corollary 6.11, we obtain that an R-linear map is injective/surjective if and only if, for all maximal ideals $\mathfrak{m} \subset R$, the localization at $\mathfrak{m}$ of the map is injective/surjective.
We conclude the section with the following lemma.

Lemma 6.12. *Let R be a ring and let T be a multiplicative subset, and consider extension of ideals along $\tau \colon R \to R_T$. Then $\sqrt{(0)_R}^e = \sqrt{(0)_{R_T}}$, where subscripts indicate in which ring we are taking the zero ideal.*

Proof. Any ring homomorphism sends nilpotent elements to nilpotent elements: this implies that $\sqrt{(0)_R}^e \subseteq \sqrt{(0)_{R_T}}$. Conversely, given a nilpotent element $\frac{a}{t} \in R_T$, there is $n \geq 1$ such that $(\frac{a}{t})^n = \frac{a^n}{t^n} = 0$, and the latter equality is witnessed by some $s \in T$ such that $sa^n = 0$. It follows that $s^n a^n = (sa)^n = 0$, i.e. $sa \in R$ is nilpotent, and now we can write $\frac{a}{t} = \frac{sa}{st}$ as an element in $\sqrt{(0)_R}^e$. □

A crucial remark, which we will implicitly use in the proof of the next corollary, is that in the setting of Lemma 6.12 the extended ideal $\sqrt{(0)_R}^e$ coincides with the localization of the sub-R-module $\sqrt{(0)_R} \subset R$ at the multiplicative set T: here we use again that ideals are submodules of rings, considered as modules over themselves.

Corollary 6.13. *A ring R is reduced if and only if $R_\mathfrak{m}$ is reduced for all maximal ideals $\mathfrak{m} \subset R$.*

Proof. The ring R is reduced, by definition, if and only if $\sqrt{(0)_R}$ is zero; this happens by Proposition 6.10 if and only if for all maximal ideals $\mathfrak{m} \subset R$ we have $(\sqrt{(0)_R})_\mathfrak{m} = \sqrt{(0)_{R_\mathfrak{m}}}$ vanishes, and this is equivalent as requiring that $R_\mathfrak{m}$ is a reduced ring for all maximal ideals $\mathfrak{m} \subset R$. □

7. Noetherian rings and modules

Recall from Definition 2.26 that if R is a ring and M is an R-module, then we may ask whether M is a finitely generated R-module or not; and Exercise 2.29 tells us that, equivalently, we can ask whether M is isomorphic to a quotient of some R-module R^n by a submodule. Finitely generated modules are easy to study, as one can often prove a property by an inductive argument on the number of generators. Notice that if M is a finitely generated R-module and $f\colon M \twoheadrightarrow N$ is a surjective R-linear map, then N is also finitely generated.
On the other hand, very often one is studying a certain module M and then is led to analyze a *submodule* $N \subset M$ (e.g., the kernel of an R-linear map out of M), and in such situations it would help knowing that N is also a finitely generated R-module. This is unfortunately not always the case, as the following example shows.

Example 7.1. Let $R = \mathbb{R}[x_i \,|\, i \in \mathbb{N}]$ be the polynomial ring in countably many variables $x_0, x_1, \dots$ indexed by the natural numbers. Then R is finitely generated (in fact, it is cyclic) as an R-module. The ideal $I = (x_i \,|\, i \in \mathbb{N}) \subset R$, containing all polynomials with vanishing constant terms, is an ideal and hence a sub-R-module of R. Yet I is not finitely generated as an R-module. To see this, we consider the quotient $I/I^2 \subset R/I^2$: it is also an R-module, and since every $P \in I$ kills by scalar multiplication every element in I/I^2, we have in fact that I/I^2 is an R/I-module (and an R-module by restriction of scalars along the surjective ring homomorphism $R \twoheadrightarrow R/I$). Now if I were finitely generated over R, then also I/I^2 would be finitely generated over R, and equivalently I/I^2 would be finitely generated over R/I. Yet $R/I \cong \mathbb{R}$ and I/I^2 can be identified with the $\mathbb{R}$-vector space with basis the infinite set $\{[x_i]_{I^2} \,|\, i \in \mathbb{N}\}$. This vector space is not finite dimensional, which means that I/I^2 is not finitely generated over R/I.

7.1. **Definition of Noetherian modules and rings.** In order to avoid situations as in Example 7.1, one often restricts the attention to situations in which the following definition holds.

Definition 7.2. Let R be a ring and M be an R-module. We say that M is *Noetherian (over R)* if every sub-R-module of M (including M) is finitely generated over R.
A ring R is *Noetherian* if it is Noetherian as a module over itself: that is, if every ideal $I \subseteq R$ is finitely generated.

Recall that if $f\colon R \to S$ is a ring homomorphism and M is an S-module, then M becomes an R-module by restriction of scalars. We notice the following:

- if M is finitely generated over R, then it is also finitely generated over S: in fact, a finite subset $X \subset M$ such that $\mathrm{Span}_R(X) = M$ also satisfies $\mathrm{Span}_S(X) = M$; the converse doesn't hold in general (think of f being the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ and $M = \mathbb{Q}$), but it holds if f is surjective;
- similarly, if M is Noetherian over R, then it is also Noetherian over S: this uses that every sub-S-module of M is also a sub-R-module (but not viceversa, in general, unless again f is surjective).

Example 7.1 shows that $R = \mathbb{R}[x_i \,|\, i \in \mathbb{N}]$ is not a Noetherian ring. Yet, using the notation from the same example, notice that $R/I \cong \mathbb{R}$ is a finitely generated (in fact, cyclic) R-module, and the only proper sub-R-module of R/I is $\{[0]_I\}$, which is surely finitely generated. So R/I is Noetherian as an R-module.
Let us now look at some examples of Noetherian rings.

Example 7.3. All principal ideal rings R are Noetherian: every ideal $I \subset R$ is generated by a single element, hence it is finitely generated. In particular, every field k, every polynomial ring $k[x]$ in one variable over a field, and $\mathbb{Z}$ are Noetherian.

Lemma 7.4. *Let R be a ring and let M be a Noetherian R-module; then every submodule $N \subseteq M$ is Noetherian, and similarly the quotient module M/N is again Noetherian.*

Proof. If N is a submodule of M, then every submodule of N is also a submodule of M, so it is finitely generated because M is Noetherian: this proves that N is Noetherian. Moreover, any submodule of M/N are all of the form P/N for a submodule $P \subseteq M$ containing N; since M is Noetherian we have that P is finitely generated, and hence also the quotient P/N is finitely generated: this proves that M/N is Noetherian. □

An immediate application of Lemma 7.4 is the following.

Corollary 7.5. *Let R be a Noetherian ring and $I \subseteq R$ be an ideal; then R/I is also a Noetherian ring.*

Proof. By Lemma 7.4, R/I is Noetherian as an R-module, i.e. every sub-R-module of R/I is finitely generated; on the other hand, the sub-R-modules of R/I are in fact the same as the sub-R/I-modules of R/I, i.e. the ideals of the ring R/I. □

Thus Noetherianity passes to quotient rings, and as we see now, also to localisations.

Lemma 7.6. *Let R be a Noetherian ring and let $T \subseteq R$ be a multiplicative subset; then R_T is also a Noetherian ring.*

Proof. By Lemma 5.2, every ideal $J \subseteq R_T$ has the form $(J^c)^e$; since J^c is an ideal in R, it is finitely generated; it then follows that also $(J^c)^e = \mathrm{Span}_{R_T}(\tau(J^c))$ is finitely generated. □

The next example gives yet another tool to produce Noetherian rings.

Example 7.7. Recall that given two rings R and S, we have a ring $R \times S$, with coordinatewise operations. The neutral element of the product is the pair $(1, 1)$, which can be written as the sum $e_R + e_S$, with $e_R = (1, 0)$ and $e_S = (0, 1)$. Notice that $e_R^2 = e_R$, $e_S^2 = e_S$ and $e_R e_S = 0$.
Given a $R \times S$-module M, we can write each element $m \in M$ as $m_R + m_S$, with $m_R = (1, 0) \cdot m$ and $m_S = (0, 1) \cdot m$: this shows that $M = e_R M + e_S M$, (i.e.

$M = \mathrm{Span}_{R\times S}(e_R M + e_S M)$, but in fact the two submodules $e_R M$ and $e_S M$ intersect trivially: for if $m \in e_R M \cap e_S M$, then $e_S m = 0 = e_R m$, but then also $m = 1 \cdot m = (e_R + e_S)m = 0$.
The ideal $(e_R) = R\times\{0\} \subset R\times S$ acts trivially on the submodule $e_S M$, which is thus really a module over the quotient ring $R \times S/(e_R) \cong S$; similarly, we can consider $e_R M$ as an R-module, and in the end we have shown that M is the direct sum $e_R M \oplus e_S M$ of an R-module (which becomes an $R \times S$-module under restriction of scalars along the surjection $R\times S \twoheadrightarrow R$) and an S-module (which similarly becomes an $R \times S$-module).
After this analysis, we conclude the following:

- an $R \times S$-module M is Noetherian if and only if $e_R M$ is Noetherian over R and $e_S M$ is Noetherian over S: for every sub-$R \times S$-module $N \subset M$ decomposes as as a direct sum $e_R N \oplus e_S N$ of a sub-R-module of $e_R M$ and a sub-S-module of $e_S M$;
- in particular, the ring $R \times S$ is Noetherian if and only if both R and S are Noetherian rings.

There is a useful characterisation of Noetherian modules (and hence, of Noetherian rings), given by Proposition 7.9, which needs the following definition.

Definition 7.8. Let R be a ring and M be a module. An *ascending chain* of submodules of M is a family $(M_i)_{i\in\mathbb{N}}$ of submodules $M_i \subseteq M$ such that for $i < j$ we have $M_i \subseteq M_j$; one can thus write

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \ldots \quad \subseteq M$$

Proposition 7.9. *Let R be a ring and let M be an R-module. Then the following conditions on M are equivalent:*

(1) M is Noetherian, in the sense of Definition 7.2;
(2) every ascending chain $(M_i)_{i\in\mathbb{N}}$ of submodules of M is eventually constant, i.e. it admits an index $\bar{i} \in \mathbb{N}$ such that for all $i \geq \bar{i}$ one has $M_i = M_{\bar{i}}$;
(3) every non-empty family Σ of submodules of M admits a maximal element with respect to inclusion.

Proof. We first prove that (1) implies (2). Let M be Noetherian and let $(M_i)_{i\in\mathbb{N}}$ be an ascending chain of submodules. Then $M' := \bigcup_{i\in\mathbb{N}} M_i$ is also a submodule of M (this uses that the submodules M_i are nested into each other), and as such it is finitely generated. Let $X \subset M'$ be a finite subset with $\mathrm{Span}_R(X) = M'$; then $X \subset \bigcup_{i\in\mathbb{N}} M_i$, and since X is finite (and the M_i are nested) there is $\bar{i} \in \mathbb{N}$ satisfying $X \subset M_{\bar{i}}$; this implies, for all $i \geq \bar{i}$, the following chain of inclusions

$$M' = \mathrm{Span}_R(X) \subseteq M_{\bar{i}} \subseteq M_i \subseteq M'$$

and evidently all inclusions must be equalities, in particular $M_{\bar{i}} = M_i$.
We now prove that (2) implies (3). For this, let M be such that every ascending chain of submodules is eventually constant, and let Σ be a non-empty family of submodules of M; suppose that Σ has no maximal element; then we can define (using the axiom of choice) a function $\Psi\colon \Sigma \to \Sigma$ with the property that for all $N \in \Sigma$, the submodule $N \subset M$ is strictly contained in $\Psi(N)$. We can now pick $N_0 \in \Sigma$ and define an ascending chain which is not eventually constant by setting $M_i = \Psi^i(N_0)$, contradicting the assumption.

We finally prove that (3) implies (1). For this, let M be such that each family Σ of submodules admits maximal elements. Let $N \subseteq M$ be a submodule and define Σ_N to be the family of finitely generated submodules of N; it is non-empty as it contains $\{0\}$, so it admits a maximal element $\bar{N}$; now $\bar{N}$ is a submodule of N, and if $\bar{N} \neq N$ we can pick $m \in N \setminus \bar{N}$ and consider $\bar{N} + \mathrm{Span}_R(m)$: it is also a finitely generated submodule of N, but it is strictly larger than $\bar{N}$, contradicting its maximality in Σ_N. This shows that $\bar{N} = N$, i.e. N is finitely generated. □

Proposition 7.9 will be used in the next subsection in the proof of the Hilbert basis theorem.
To conclude the subsection, let me propose two exercises. We have seen in Lemma 7.6 that if R is Noetherian, then R_T is also Noetherian. Does the converse hold? It depends on what we mean by "converse". Surely, Example 7.1 gives a non-Noetherian ring R which is a domain, whose fraction field $\mathrm{Frac}(R)$ is an example of a Noetherian localisation. The following are less naive attempts to define a "converse".

Exercise 7.10. Let R be a ring, and let $t_1, \dots, t_r$ be a finite collection of elements of R such that the ideal $(t_1, \dots, t_r)$ is the entire R. Let M be an R-module, and assume that each localisation M_{t_i} is Noetherian over R_{t_i}; prove that R is Noetherian.
As a special case, if each localisation R_{t_i} is a Noetherian ring, then also R is Noetherian.
(Hint: for all $1 \leq i \leq r$, fix a finite set of generators $(m_{i,j}/t_i^{k_{i,j}})_{1 \leq j \leq n_i}$ for the module M_{t_i}; define a submodule $\bar{M} \subset M$ as $\mathrm{Span}_R(\{m_{i,j}\})$; prove that $M/\bar{M}$ is the zero R-module by using Proposition 6.10)

Exercise 7.11. As a pre-exercise, prove that if R and S are rings, then $\mathrm{Spec}(R \times S)$ can be regarded as the disjoint union of $\mathrm{Spec}(R)$ and $\mathrm{Spec}(S)$.
Let now k be a field, and consider the subring $R \subset k^{\mathbb{N}}$ of those functions of sets $f \colon \mathbb{N} \to k$ that are eventually constant, i.e. such that there is $a \in k$ with $f(n) = a$ for n large enough. We want to prove that R is not Noetherian, yet for every prime ideal $\mathfrak{p} \subset R$ the localisation $R_{\mathfrak{p}}$ is Noetherian.
For any subset $\mathcal{I} \subset \mathbb{N}$, define $I_{\mathcal{I}}$ as the ideal of R containing all functions f such that $f|_{\mathcal{I}} \equiv 0$.

- Prove that indeed R is a subring of $k^{\mathbb{N}}$, and each $I_{\mathcal{I}}$ is an ideal of R.
- Prove that R is not Noetherian (consider the ideals $I_{\{n \in \mathbb{N} \,|\, n \geq i\}}$, for $i \in \mathbb{N}$).
- Prove that for each $i \in \mathbb{N}$, the ideal $I_{\{i\}}$ is maximal.
- Prove that the set $J := \{f \in R \,|\, \exists \bar{n} \in \mathbb{N} \ \forall n \geq \bar{n} \colon \ f(n) = 0\} \subset R$ is a maximal ideal.
- Prove that the previous are in fact all prime ideals of R. To do this, let $\mathfrak{p} \in \mathrm{Spec}(R)$ and use the following dichotomy:
  - either there exists $f \in \mathfrak{p}$ which is eventually constant, equal to some $a \neq 0$; prove that $\mathfrak{p} = I_{\{i\}}$ for one of the finitely many $i \in \mathbb{N}$ with $f(i) = 0$ (there is at least one, otherwise f is invertible in R);
  - or for every $f \in \mathfrak{p}$ we have that f is eventually equal to 0; prove then that $\mathfrak{p}$ contains *every* function f that is eventually 0 (for instance, for each such f there is a g which is eventually $1 \in k$ and such that $f \cdot g = 0 \in R$), that is $J \subseteq \mathfrak{p}$ and thus $\mathfrak{p} = J$.
- Prove that $R_{\mathfrak{p}}$ is isomorphic to k for all prime ideals of R.

7.2. **The Hilbert basis theorem for rings.** In this subsection we prove the following Theorem, which together with Examples 7.3 and 7.7, Corollary 7.5 and Lemma 7.6 produces for us a lot of examples of Noetherian rings.

Theorem 7.12 (Hilbert basis theorem)**.** *Let R be a Noetherian ring. Then the polynomial ring $R[x]$ is also Noetherian.*

In the proof of Theorem 7.12 we will use the standard notions of degree and leading coefficient of a polynomial, which we recall now.

Definition 7.13. Let $P \in R[x] \setminus \{0\}$ and write $P = \sum_{i=0}^{n} a_i x^i$, with $a_n \neq 0$. We say that n is the *degree* of P, and $a_n \in R \setminus \{0\}$ is the *leading coefficient* of P. We also write $n = \deg(P)$ and $a_n = \mathrm{lc}(P)$.

The proof of Theorem 7.12 reminds the division algorithm for polynomials in $k[x]$, with k a field: if $A, B \in k[x]$ are polynomials of degrees n and m respectively, with $n \geq m$, in order to divide A by B one considers the leading coefficients of A and B, one divides the leading coefficients of A by that of B, obtaining an element $a \in k$; then ax^{n-m} will be the first term in the quotient, and one proceeds by replacing A with $A - ax^{n-m}B$, which is a new polynomial of degree strictly smaller than n; one proceeds in this fashion until one can (possibly leaving a reminder at the end).

Proof. Let $I \subseteq R[x]$ be an ideal; we want to prove that it is finitely generated. For each $i \in \mathbb{N}$ we define $I_i \subseteq R$ as the ideal generated by all leading coefficients of elements $P \in I$ of degree exactly i:

$$I_i = (\mathrm{lc}(P) \,|\, P \in I, \deg(P) = i) \subseteq R.$$

We observe that in fact, if P, Q are polynomials of degree i and $r \in R$, then there are two possibilities:

- either $\mathrm{lc}(P - rQ) = \mathrm{lc}(P) - r\mathrm{lc}(Q) \neq 0$, in which case $P - rQ$ is also a polynomial of degree exactly i and $\mathrm{lc}(P - rQ) = \mathrm{lc}(P) - r\mathrm{lc}(Q)$,
- or $\mathrm{lc}(P - rQ) = \mathrm{lc}(P) - r\mathrm{lc}(Q) = 0$.

This shows that I_i, as a set, can be characterised as the union

$$\{0\} \cup \{\mathrm{lc}(P) \,|\, P \in I, \deg(P) = i\}.$$

We next observe that if $P \in I$ has degree i, then $xP \in I$ and $\deg(xP) = i + 1$; moreover $\mathrm{lc}(P) = \mathrm{lc}(xP)$. It follows that $I_i \subseteq I_{i+1}$ for all $i \in \mathbb{N}$. By Proposition 7.9, the ascending chain

$$I_0 \subseteq I_1 \subseteq I_2 \ldots$$

is eventually constant, so there is $\bar{i} \in \mathbb{N}$ with $I_i = I_{\bar{i}}$ for all $i \geq \bar{i}$. Moreover, since R is Noetherian, each ideal I_i is finitely generated: for each $0 \leq i \leq \bar{i}$ let therefore $\{a_{i,j}\}_{0 \leq j \leq n_i}$ be generators for I_i as an ideal of R; and for future convenience, let us set $n_i = n_{\bar{i}}$ for all $i > \bar{i}$, and also $a_{i,j} = a_{\bar{i},j}$; we can assume that all $a_{i,j}$ are non-zero, and by the characterisation of I_i as a set we can find, for all $0 \leq i \leq \bar{i}$ and $1 \leq j \leq n_i$, a polynomial $P_{i,j} \in I$ of degree i with $\mathrm{lc}(P_{i,j}) = a_{i,j}$; for future convenience, for all $i > \bar{i}$ we set $P_{i,j} = x^{i-\bar{i}} P_{\bar{i},j}$ for $1 \leq j \leq n_i = n_{\bar{i}}$.
We now claim that the finite set $X := \{P_{i,j} \,|\, 0 \leq i \leq \bar{i}, 1 \leq j \leq n_i\}$ generates I as an ideal of $R[x]$; since each polynomial $P_{i,j}$ with $i > \bar{i}$ is a multiple of the corresponding polynomial $P_{\bar{i},j}$, it is equivalent to prove that I is generated by the set $Y := \{P_{i,j} \,|\, i \geq 0, 1 \leq j \leq n_i\}$.

For the sake of contradiction, let $(Y) \neq I$ and let Q be a polynomial of minimal degree in $I \setminus (Y)$; let $d = \deg(Q)$. We have $\mathrm{lc}(Q) \in I_d$, so there exist elements $r_1, \dots, r_{n_d} \in R$ with $\mathrm{lc}(Q) = r_1 a_{d,1} + \cdots + r_{n_d} a_{d,n_d}$. We then consider the polynomial $Q' := Q - \sum_{j=1}^{n_d} r_j P_{d,j}$: the formula exhibits Q' as an element of I, and moreover either $Q' = 0$ or $\deg(Q') < d$, since the degree-d terms in the linear combination for Q' cancel out. If $Q' = 0$, we have exhibited $Q = \sum_{j=1}^{n_d} r_j P_{d,j}$ as an element of (Y), which is a contradiction; otherwise, by our choice of Q, the element Q' has smaller degree than Q and thus must lie in (Y): then the above formula exhibits again Q as an element of Y, giving again a contradiction. □

An immediate consequence of Theorem 7.12 is that if R is a Noetherian ring and $n \geq 0$, then the polynomial ring $R[x_1, \dots, x_n]$ is Noetherian: this follows by induction on n, after noticing that $R[x_1, \dots, x_n]$ is isomorphic to the ring $(R[x_1, \dots, x_{n-1}])[x_n]$ of polynomials in x_n with coefficients in the ring $R[x_1, \dots, x_{n-1}]$.

7.3. **The Hilbert basis theorem for modules.** So far we have provided tools to construct Noetherian rings, most notably Theorem 7.12. How about constructing/recognising Noetherian modules over a (possibly non-Noetherian) ring? Lemma 7.4 gives us a tool in this direction, but in a certain sense, if M is an R-module, then every submodule or quotient of M is "smaller" than M itself. The following lemma allows us to construct/recognise "bigger" Noetherian modules from "smaller" ones.

Lemma 7.14. *Let R be a ring, and let $N \overset{f}{\hookrightarrow} M \overset{g}{\twoheadrightarrow} P$ be a short exact sequence of R-modules. Then:*

- *if N and P are finitely generated, then also M is finitely generated;*
- *M is Noetherian if and only if both N and P are Noetherian.*

Proof. For the first point, assume that $n_1, \dots, n_a \in N$ and $p_1, \dots, p_b \in P$ generate N and P, respectively, as R-modules, for some $a, b \geq 0$. Let $\tilde{p}_1, \dots, \tilde{p}_b \in M$ be preimages of $p_1, \dots, p_b$ along g. We claim that the finite list of elements $f(n_1), \dots, f(n_a), \tilde{p}_1, \dots, \tilde{p}_b \in M$ generates M as an R-module. To prove this, let $m \in M$; then $g(m) \in P$ can be written as $r_1 p_1 + \cdots + r_b p_b$ for suitable $r_1, \dots, r_b \in R$. We then observe that the element $m' = m - (r_1 \tilde{p}_1 + \cdots + r_b \tilde{p}_b) \in M$ lies in the kernel of g, hence in the image of f; so m' can be written as $s_1 f(n_1) + \cdots + s_a f(n_a)$ for suitable $s_1, \dots, s_a \in R$. It follows that $m = s_1 f(n_1) + \cdots + s_a f(n_a) + r_1 \tilde{p}_1 + \cdots + r_b \tilde{p}_b$ can be generated using the list mentioned above.
For the second point, we notice that if M is Noetherian then both N and P, which are isomorphic to a submodule and a quotient module of M, respectively, are Noetherian by Lemma 7.4. Conversely, suppose that N and P are Noetherian, and let $M' \subseteq M$ be a submodule. Then $g(M')$ is a submodule of P, and $M' \cap f(N)$ is a submodule of $f(N) \cong N$; it follows that both $g(M')$ and $M' \cap f(N)$ are finitely generated. Since $M' \cap f(N) = M' \cap \ker(g)$, we have a short exact sequence of R-modules $(M' \cap f(N)) \hookrightarrow M' \overset{g}{\twoheadrightarrow} g(M')$, and by the previous point we conclude that M' is finitely generated. This concludes the proof that M is Noetherian. □

We present two corollaries of Lemma 7.14.

Corollary 7.15. *Let R be a ring and let M and N be Noetherian R-modules; then the direct sum $M \oplus N$ is also a Noetherian R-module.*

Proof. There is a short exact sequence of R-modules $M \hookrightarrow M \oplus N \twoheadrightarrow N$, so the statement follows from Lemma 7.14. □

Pay attention: a generic sub-R-module of $M \oplus N$ is not of the form $M' \oplus N'$ for $M' \subseteq M$ and $N' \subseteq N$, so one cannot argue by simply invoking Noetherianity of M and N to say that M' and N' are finitely generated: one has to go through a slightly more complicated argument as the one in the proof of Lemma 7.14.

Corollary 7.16. *Let R be a ring, let M be an R-module and let $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r = M$ be a sequence of nested sub-R-modules of M. Suppose that each quotient M_i/M_{i-1} is Noetherian, for $1 \leq i \leq r$; then M is Noetherian.*

Proof. We prove inductively, that M_i is Noetherian. The base case $M_1 \cong M_1/M_0$ is one of the hypotheses. For the inductive step, if M_{i-1} is Noetherian, then there is a short exact sequence $M_{i-1} \to M_i \to M_i/M_{i-1}$ and by Lemma 7.14, since the two extreme R-modules are Noetherian, so is the one in the middle. □

We are now ready to prove the following Theorem, providing a simple criterion to recognise Noetherian R-modules when R is itself a Noetherian ring.

Theorem 7.17. *Let R be a ring. Then the following are equivalent:*

- *R is a Noetherian ring, in the sense of Definition 7.2;*
- *every finitely generated R-module M is a Noetherian R-module (and viceversa!).*

Proof. Let us first assume that R is Noetherian and let M be a finitely generated R-module; by Exercise 2.29 there exists a surjective R-linear map $R^n \twoheadrightarrow M$, for some $n \geq 0$; by assumption R is a Noetherian R-module, and Corollary 7.15 implies that R^n is a Noetherian R-module; it follows that M, which is isomorphic to a quotient of R^n, is by Lemma 7.4 also Noetherian.
Viceversa, if we assume that every finitely generated R-module is Noetherian, then R is a cyclic R-module, so R must be a Noetherian R-module: this is the definition of a Noetherian ring. □

We conclude the subsection with a simple, but useful observation.

Example 7.18. Let k be a field. Then a k-vector space is Noetherian if and only if it is finitely generated, i.e., if and only if it has finite dimension over k, as then every sub-k-vector space has also finite dimension.

7.4. **A glimpse on Artinian rings and modules.** We conclude the section by introducing a natural counterpart to the notion of Noetherian rings and modules: compare the following with Definition 7.8 and Proposition 7.9. We will limit ourselves to the part of the discussion that is completely parallel to the one for Noetherian rings and modules.

Definition 7.19. Let R be a ring and M be a module. A *descending chain* of submodules of M is a family $(M_i)_{i\in\mathbb{N}}$ of submodules $M_i \subseteq M$ such that for $i < j$ we have $M_i \supseteq M_j$; one can thus write

$$M \supseteq \quad M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots$$

Definition 7.20. An R-module M is *Artinian* if every descending chain $(M_i)_{i\in\mathbb{N}}$ of submodules of M is eventually constant, i.e. it admits an index $\bar{i} \in \mathbb{N}$ such that for all $i \geq \bar{i}$ one has $M_i = M_{\bar{i}}$.

A ring R is Artinian if the R-module R is Artinian: equivalently, every descending chain of ideals in R is eventually constant.

Exercise 7.21. Prove that an R-module M is Artinian if and only if every non-empty family Σ of submodules of M admits a minimal element with respect to inclusion. You can in part adapt the proof of Proposition 7.9.

Example 7.22. Let k be a field; then a k-vector space is Artinian if and only if it is finite dimensional: comparing with Example 7.18, we obtain that over a field the notions of Artinian and Noetherian modules coincide.
In particular, as$k$ has dimension 1 over k, k is an Artinian ring.

Example 7.23. $\mathbb{Z}$ is not Artinian: for example the descending chain of ideals $((2^i))_{i\in\mathbb{N}}$ decreases strictly at each step. Similarly, if k is a field and $n \geq 1$, then $k[x_1, \dots, x_n]$ is not Artinian, as witnessed by the chain of ideals $((x_1)^i)_{i\in\mathbb{N}}$.

Example 7.24. Let k be a field and $n \geq 0$; we claim that $R = k[x]/(x^n)$ is an Artinian ring. To see this, notice first that the unique prime ideal in R, corresponding to the unique prime ideal in $k[x]$ containing (x^n), is $([x]_{x^n})$. Hence R is a local ring, and by Exercise 4.9 for every $P \in k[x]$ such that $P_*(0) \neq 0$ we have that $[P]_{x^n} \in R^\times$. Moreover, since $k[x]$ is a principal ideal ring, also R is a principal ideal ring. Given a nonzero ideal $([Q]_{x^n}) \subseteq R$ generated by the class of some $Q \in k[x]$, we can factor Q as $x^i \cdot P$ with $P_*(0) \neq 0$ and $0 \leq i \leq n-1$, and we obtain a factorisation $[Q]_{x^n} = [x^i]_{x^n} \cdot [P]_{x^n}$ in R. Since $[P]_{x^n}$ is invertible, we conclude that our ideal $([Q]_{x^n})$ can also be presented as $([x^i]_{x^n})$. This shows that there are finitely many ideals in R, namely all ideals of the form $([x^i]_{x^n})$ for $0 \leq i \leq n$ (thus we recover also the zero ideal). And a ring with finitely many ideals must be both Noetherian and Artinian (every descending or ascending chain of ideals is eventually constant).

Example 7.25. If R is an Artinian ring and $I \subseteq R$ is an ideal, then R/I is also Artinian: every descending chain of ideals in R/I corresponds to a descending chain of ideals containing I in R, so it must stabilise.
If R and S are Artinian rings, then Example 7.7 shows that every $R \times S$-module decomposes uniquely as a direct sum of an R-module and an S-module, both considered as $R \times S$-modules by restriction of scalars along the two projections. It follows that an $R \times S$-module is Artinian if and only if its corresponding R-module and S-module are both Artinian. And in particular, $R \times S$ is an Artinian ring if and only if both R and S are Artinian.

The following is analogue to Lemma 7.14.

Lemma 7.26. *Let R be a ring, and let $N \overset{f}{\hookrightarrow} M \overset{g}{\twoheadrightarrow} P$ be a short exact sequence of R-modules. Then M is Artinian if and only if both N and P are Artinian.*

Proof. Let us first assume that M is Artinian. Then every descending chain of submodules of N is mapped injectively along f to a descending chain of submodules of M; one chain stabilises if and only if the other does (use that f is injective), so N is Artinian. Similarly, every descending chain of submodules of P pulls back along g to a descending chain of submodules of M containing $\ker(g)$, and again one chain stabilises if and only if the other does (use that g is surjective, so submodules of P are in bijection with submodules of M containing $\ker(g)$), so P is Artinian.

Viceversa, let us assume that N and P are Artinian, and let $(M_i)_{i\in\mathbb{N}}$ be a descending chain of submodules of M. Then $(P_i)_{i\in\mathbb{N}} := (g(M_i))_{i\in\mathbb{N}}$ is a descending chain of submodules of P, and $(N_i)_{i\in\mathbb{N}} := (f^{-1}(M_i))_{i\in\mathbb{N}}$ is a descending chain of submodules of N. For all $i \in \mathbb{N}$ we have a short exact sequence $N_i \xrightarrow{f} M_i \xrightarrow{g} P_i$.
By assumption on N and P, there is an index $\bar{i}$ such that $N_i = N_{\bar{i}}$ and $P_i = P_{\bar{i}}$ for all $i \geq \bar{i}$; we obtain, for all $i \geq \bar{i}$, a commutative diagram as follows, whose vertical maps are inclusions and whose horizontal maps are restrictions of f and g:

$$\begin{array}{ccccc} N_i & \xrightarrow{f} & M_i & \xrightarrow{g} & P_i \\ \downarrow\subseteq & & \downarrow\subseteq & & \downarrow\subseteq \\ N_{\bar{i}} & \xrightarrow{f} & M_{\bar{i}} & \xrightarrow{g} & P_{\bar{i}}. \end{array}$$

By assumption, the left and the right vertical maps are isomorphisms (in fact, identities); by the five lemma, also the middle inclusion is an isomorphism, i.e. $M_i = M_{\bar{i}}$ for all $i \geq \bar{i}$. This concludes the proof that M is Artinian. □

A straightforward consequence of Lemma 7.26 is that the direct sum of a finite collection of Artinian R-modules is again an Artinian R-module. The following is analogue to Corollary 7.16.

Exercise 7.27. Let R be a ring, let M be an R-module and let $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r = M$ be a sequence of nested sub-R-modules of M. Suppose that each quotient M_i/M_{i-1} is Artinian, for $1 \leq i \leq r$; then M is Artinian.

8. Primary decomposition

As we have seen in Proposition 3.19, every radical ideal I in a ring R can be expressed as an intersection of prime ideals (namely, all prime ideals containing it). In the case $R = \mathbb{Z}$, this theorem reads as follows: let $n \geq 1$ be a positive integer and assume that $n = p_1 \cdot \cdots \cdot p_r$ is a product of distinct prime numbers, then $(n) \subseteq \mathbb{Z}$ is a radical ideal and $(n) = (p_1) \cap \cdots \cap (p_r)$. We would like to express generic ideals (possibly, non-radical ones) in terms of "simpler" ideals, where for instance prime ideals are to be considered "simple".

8.1. **Irreducible ideals.** For generic $n \geq 1$ we can similarly write

$$n = p_1^{a_1} \cap \cdots \cap p_r^{a_r},$$

and in fact we have $(n) = (p_1^{a_1}) \cap \cdots \cap (p_r^{a_r})$; moreover the ideals $(p_i^{a_r})$ are of a special type, at least because of the following reasons:

- they have a prime ideal as radical, i.e. $\sqrt{(p_i^{a_i})} = (p_i)$ is a prime ideal of $\mathbb{Z}$;
- they are *irreducible* ideals in the sense of the following definition.

Definition 8.1. An ideal I in a ring R is irreducible if it is proper and it cannot be written as $I_1 \cap I_2$ such that both I_1 and I_2 are strictly bigger than I.

We observe that $I \subseteq R$ is irreducible if and only if $(0) \subseteq R/I$ is irreducible.

Exercise 8.2. Prove that the irreducible ideals of $\mathbb{Z}$ are precisely (0) and all ideals of the form (p^a) for p a prime number and $a \geq 1$.
Deduce that for $n = p_1^{a_1} \dots p_r^{a_r}$, the *unique* way to write $(n) \subseteq \mathbb{Z}$ as an intersection of irreducible ideals with different prime ideals as radicals is $(n) = (p_1^{a_1}) \cap \cdots \cap (p_r^{a_r})$.

It would be interesting to investigate whether something similar holds more generally, i.e. if in general every ideal I in any ring R can be written as an intersection of irreducible ideals, possibly in a unique way: this would be a generalisation to other rings and ideals of the familiar fact that integers admit a unique factorisation. If we were able to express every ideal I as a *finite* intersection of irreducible ideals, this would be even better!
The following lemma will be needed a few times later, but starts showing that at least prime ideals are always examples of irreducible ideals.

Lemma 8.3. *Let $\mathfrak{p}$ be a prime ideal in a ring R, and let $I_1, \dots, I_r$ be a finite collection of ideals of R such that $I_1 \cap \dots \cap I_r \subseteq \mathfrak{p}$. Then there is an index $1 \leq i \leq r$ such that $I_i \subseteq \mathfrak{p}$. In particular $\mathfrak{p}$ is irreducible in the sense of Definition 8.1.*

Proof. Suppose for the sake of contradiction that for all $1 \leq i \leq r$ we can pick an element $a_i \in I_i \setminus \mathfrak{p}$; then the product $a_1 \dots a_r$ belongs to each I_i, so it belongs to $I_1 \cap \dots \cap I_r$, yet it cannot belong to the prime ideal $\mathfrak{p}$, and this contradicts the inclusion $I_1 \cap \dots \cap I_r \subseteq \mathfrak{p}$. In particular if $\mathfrak{p} = I \cap J$, we have $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$, and since $\mathfrak{p} \subseteq I$ and $\mathfrak{p} \subseteq J$ we must have $I = \mathfrak{p}$ or $J = \mathfrak{p}$. □

Example 8.4. One could alternatively say: *In $\mathbb{Z}$, for $n = p_1^{a_1} \dots p_r^{a_r}$ as above, we also have that the ideal (n) is the product $(p_1)^{a_1} \dots (p_r)^{a_r}$, and the prime ideals (p_i) are "product-irreducible" in the sense that they cannot be written as product of two strictly larger ideals. Why don't we try to generalise to other rings using product of ideals instead of intersection as basic operation?* One possible reason to prefer intersection to product is that an intersection of a family of ideals only depends on *which* ideals belong to the family, whereas in order to specify a product we also need to specify *exponents* for each ideal considered: for instance, for every ring R and every two ideals $I, J \subseteq R$, the intersection $I \cap J$ is equal to $I \cap I \cap J$, but the products I^2J and IJ may (or may not) be different. This makes intersection of ideals into a somewhat simpler notion than product.
The lack of exponents when dealing with intersection of ideals has also the advantage of making it more likely that a decomposition of an ideal is unique; in the following example we see directly that even existence of product decomposition into product-irreducible ideals is not satisfied for some very basic rings.
Let k be a field and let $R = k[x]/(x^2 - x)$. There are exactly three proper ideals in R, namely $([x])$, $([x-1])$ and (0), and each of them is equal to its own square; hence *no ideal* of R can be written as a product of product-irreducible ideals.
Using intersections, instead, we would just have that $([x])$ and $([x-1])$ are irreducible (they are prime ideals, and we apply Lemma 8.3), whereas $(0) = ([x^2 - x]) = ([x]) \cap ([x-1])$ can be written as an intersection of two irreducible ideals.

The following exercise shows that for a generic ring there is little hope to express generic ideals as interesections of irreducible ideals.

Exercise 8.5. Let k be a field, and let $R \subset k^{\mathbb{N}}$ be the subring of those functions $f \colon \mathbb{N} \to k$ that satisfy at least one of the following:

(1) f is constant;
(2) there is $\bar{n} \geq 0$ such that $f(n) = 0$ for all $n \geq \bar{n}$.

For every subset $\mathcal{I} \subset \mathbb{N}$, define $I_{\mathcal{I}} \subset R$ as the ideal containing all functions f that vanish on $\mathcal{I}$.

- Prove that indeed R is a subring of $k^{\mathbb{N}}$, and $I_{\mathcal{I}}$ is an ideal in R.

- Prove that every ideal $J \subseteq R$ is of the form $I_{\mathcal{I}}$, where $\mathcal{I} := \{i \in \mathbb{N} \mid \forall f \in J \ f(i) = 0\}$.
- Prove that $I_{\mathcal{I}} \cap I_{\mathcal{I}'} = I_{\mathcal{I} \cup \mathcal{I}'}$. Deduce that the only irreducible ideals of R are those of the form $I_{\{i\}}$, for some $i \in \mathbb{N}$ (which are in fact all prime ideals of R).
- Prove that $I_{\mathbb{N}} = (0) \subset R$ cannot be written as a finite intersection of irreducible ideals.

To avoid situations as the one in Exercise 8.5, we will focus in the rest of the section on Noetherian rings. And here is a first, positive result.

Proposition 8.6. *Let R be a Noetherian ring. Then every ideal of R can be expressed as a finite intersection of irreducible ideals.*

Proof. For the sake of contradiction, let Σ be the family of all ideals of R that cannot be expressed as a finite intersection of irreducible ideals of R, and assume $\Sigma \neq \emptyset$. Since R is Noetherian, we can pick a maximal element $I \in \Sigma$. If I were irreducible, we would be done, as we could express I as a finite intersection indexed over a set of one element. So I is not irreducible; then either $I = R$ (in this case we regard I as an intersection of ideals indexed by the empty set), or $I = I_1 \cap I_2$ with both I_1 and I_2 proper and strictly larger than I: then by maximality of I in Σ we have that both I_1 and I_2 can be expressed as finite intersections of irreducible ideals, and this implies that also I has this property, contradicting $I \in \Sigma$. □

The following example shows that, even if existence is granted, we should not expect *uniqueness* for a decomposition of an ideal as a finite intersection of irreducible ideals. It will also motivate the quest for a type of ideals that is more general than "irreducible" ideals (and we will identify into *primary* ideals a good candidate for that).

Example 8.7. Let k be a field and consider the ring $R = k[x, y]$. Then the ideal (xy, y^2) can be written as the intersection $(y) \cap (x, y^2)$; we have that (y) is prime, hence irreducible, so let us check that (x, y^2) is irreducible; to this aim, it suffices to check that 0 is irreducible in the ring $k[x, y]/(x, y^2)$, and this ring is isomorphic to $k[y]/(y^2)$, where the only ideals are $([y])$ and (0); this shows that $(y) \cap (x, y^2)$ exhibits $(xy, y^2) \subset R$ as intersection of irreducible ideals.
Now, for any $a \in k$, one can also show that $(xy, y^2) = (y) \cap (x + ay, y^2)$ (exercise!) and that $(x + ay, y^2) \subset R$ is also an irreducible ideal (other exercise!). This shows that there are at least as many decompositions of (xy, y^2) as intersection of irreducible ideals as there are elements in k.
To avoid the choice of a, we could try to replace $(x + ay, y^2)$ by the intersection $\bigcap_{a \in k}(x + ay, y^2)$; this intersection is the ideal $(x^2, xy, y^2) = (x, y)^2$. It is not an irreducible ideal: in fact it can be obtained by intersecting $(x+a, y^2) \cap (x+b, y^2)$, for any two distinct elements $a, b \in k$. If one wants, one can also intersect three or four or finitely many such ideals (as long as k contains many elemets). This produces for us yet another example of an ideal in a Noetherian ring with a non-unique decomposition as intersection of irreducible ideals.

To partially solve the problem from Example 8.7, we will introduce a new class of ideals, called *primary* ideals, which at least for Noetherian rings will contain all irreducible ideals; and we will study more generically decompositions of ideals as finite interesections of primary ideals. In the situation of Example 8.7, we will

have that $(x,y)^2$ is primary (though not irreducible), and this will partially solve our problem as this ideal looks more "canonical" than any ideal of the form $(x+ay, y^2)$.

8.2. **Primary ideals.**

Definition 8.8. Let R be a ring and $I \subseteq R$ be an ideal. We say that R is *primary* if it is proper and the following holds: for all $a, b \in R$ such that $ab \in I$, either $a \in I$ or there is $n \geq 1$ such that $b^n \in I$.

Notice that the definition is asymmetric in a and b. In particular, if $ab = ba \in I$, then either at least one between a and b lies in I, or *both* a and b admit a power lying in I. Notice that every prime ideal is also primary, and in fact if an ideal is both primary and radical, then it is a prime ideal. Finally, notice that I is primary in R if and only if (0) is primary in R/I.

Example 8.9. Primary ideals of $\mathbb{Z}$ are precisely (0) and those of the form (p^a) for p a prime number and $a \geq 1$. In particular, they coincide with irreducible ideals. The ideal $(x,y)^2 \subset k[x,y]$, appearing also in Example 8.7, is primary but not prime (check it directly, later we will see a general fact covering this).

Lemma 8.10. *Let R be a ring and let $\mathfrak{q} \subset R$ be a primary ideal. Then $\sqrt{\mathfrak{q}}$ is a prime ideal, and it is the unique minimum, with respect to inclusion, among prime ideals containing $\mathfrak{q}$.*

Proof. If $a, b \in R$ and $ab \in \sqrt{\mathfrak{q}}$, then there is $n \geq 1$ such that $a^n b^n \in \mathfrak{q}$; then, since $\mathfrak{q}$ is primary either $a^n \in \mathfrak{q}$ (implying $a \in \sqrt{\mathfrak{q}}$) or there is $m \geq 1$ such that $b^{nm} \in \mathfrak{q}$ (and this implies $b \in \sqrt{\mathfrak{q}}$). This proves that $\sqrt{\mathfrak{q}}$ is a prime ideal. Moreover, every prime ideal $\mathfrak{p}$ is radical, so if $\mathfrak{p} \supseteq \mathfrak{q}$ then $\mathfrak{p} \supseteq \sqrt{\mathfrak{q}}$. □

As a matter of notation, we say that a primary ideal $\mathfrak{q}$ in a ring R is $\mathfrak{p}$-*primary* if $\sqrt{\mathfrak{q}} = \mathfrak{p}$.

Lemma 8.11. *Let R be a ring, let $\mathfrak{m}$ be a maximal ideal and let I be an ideal. Suppose $\sqrt{I} = \mathfrak{m}$. Then I is primary.*

Proof. Let $a, b \in R$ and assume $ab \in I$. If $b \in \mathfrak{m}$ then there is $n \geq 1$ with $b^n \in I$, so let us assume $b \notin \mathfrak{m}$; then by maximality of $\mathfrak{m}$ we can write $1 = m + cb$ for some $m \in \mathfrak{m}$ and $c \in R$; it follows that $1 - cb = m \in \mathfrak{m} = \sqrt{I}$, so there is $r \geq 1$ with $(1-cb)^r = i \in I$. Multiplying by a and rearranging we obtain $a = ia - [(1-cb)^r - 1]a$, and since $(1-cb)^r - 1$ is a multiple of cb (and in particular of b), we obtain $a \in I$. □

Example 8.12. Recall Example 8.7. Then each of the ideals $(x + ay, y^2)$ and $(x,y)^2$ is primary, as it has the maximal ideal $(x,y) \subseteq k[x,y]$ as radical.

Example 8.13. Lemma 8.11 shows that if an ideal admits a *maximal* ideal as radical, then it must be primary. Instead, if $I \subset R$ is an ideal and $\sqrt{I} = \mathfrak{p}$ is a prime ideal, then I need not be primary. For instance, let k be a field and let $R = k[x,y,z]/(xy - z^2)$. Then $\mathfrak{p} = ([x],[z])$ is a prime ideal, and $I := \mathfrak{p}^2$ is an ideal satisfying $\sqrt{I} = \mathfrak{p}$; yet even if the product $[x] \cdot [y] \in I$, as it can be expressed as $[z] \cdot [z]$ in R, we have that neither $[x] \in I$ nor any power of $[y]$ is in I. To see the first, notice that R/I further quotients to $k[x,y,z]/(x,y,z)^2$; to see the second, use that R/I further quotients to $R/\mathfrak{p} \cong k[x,y,z]/(x,z) \cong k[y]$.

We conclude the subsection by proving that the notion of primary ideal can be thought of as a generalisation of that of irreducible ideal, at least in Noetherian rings.

Lemma 8.14. *Let R be a Noetherian ring and let $I \subset R$ be an irreducible ideal. Then I is primary.*

Before proving the theorem, we give a definition that will turn out to be very useful in a few contexts.

Definition 8.15. Let R be a ring, let M be an R-module, let $m \in M$ and let $N \subset M$ be a submodule. We denote by $(N\colon m) \subseteq R$ the ideal of all elements $a \in R$ such that $am \in N$. If N is the zero submodule, we write in particular $(N\colon m) = \mathrm{Ann}(m) \subseteq R$ (as we already did in the proof of Proposition 6.10).

We will often use Definition 8.15 for $M = R$ and $N = I$ being an ideal. We observe that $(I\colon a) \supseteq I$ always, that $(I\colon a) = R$ if $a \in I$, and that if $(I_i)_{i\in\mathcal{I}}$ is a family of ideals, then $(\bigcap_{i\in\mathcal{I}} I_i\colon a) = \bigcap_{i\in\mathcal{I}}(I_i\colon a)$ (thus "$(-\colon a)$" commutes with intersections, just as "$\sqrt{-}$"). Finally, if $I \subseteq J$, then $(I\colon a) \subseteq (J\colon a)$.

Proof of Lemma 8.14. Let $a, b \in R$ and assume $ab \in I$. For each $n \geq 1$ we have an ideal $(I\colon b^n)$, and these ideals fit into an ascending chain

$$(I\colon b) \subseteq (I\colon b^2) \subseteq (I\colon b^3) \subseteq \dots.$$

Since R is Noetherian, the previous chain must stabilise, in particular there is $\bar{n}$ with $(I\colon b^{\bar{n}}) = (I\colon b^{\bar{n}+1})$. We now claim that $(a, I) \cap (b^{\bar{n}}, I) = I$: if this is the case, since I is irreducible we would have $a \in I$ or $b^{\bar{n}} \in I$, and this would conclude the proof that I is primary.
So let $x = ca + m = db^{\bar{n}} + m' \in (a, I) \cap (b^{\bar{n}}, I)$ be an element in the intersection, with $c, d \in R$ and $m, m' \in I$. Then, multiplying by b, we obtain $cab + mb = db^{\bar{n}+1} + m'b$, and since $cab, mb, m'b \in I$ we conclude that $db^{\bar{n}+1} \in I$; this implies that $d \in (I\colon b^{\bar{n}+1})$, and by out choice of $\bar{n}$ we then also have $d \in (I\colon b^{\bar{n}})$. This in turn implies that our element $x = db^{\bar{n}} + m'$ already lies in I. □

8.3. **Primary decompositions.** A primary decomposition of an ideal I in a ring R is a description of I as a finite intersection of primary ideals $\mathfrak{q}_i$:

$$I = \bigcap_{i=1}^{r} \mathfrak{q}_i.$$

Proposition 8.6 and Lemma 8.14 imply that every ideal in a Noetherian ring admits a primary decomposition. Example 8.7 shows that, in general, this decomposition is not unique. In fact, when working with primary decomposition, one should not expect uniqueness also by thinking of the following simple reason: if $\mathfrak{q} \subset R$ is a primary but not prime ideal, then $\mathfrak{p} := \sqrt{\mathfrak{q}}$ is a prime ideal by Lemma 8.10, and both "$\mathfrak{q}$" and "$\mathfrak{q} \cap \mathfrak{p}$" are primary decompositions of $\mathfrak{q}$. We would then like to say that the second decomposition is redundant, and only the first is "genuine". The following lemma helps us consistently in this direction.

Lemma 8.16. *Let $\mathfrak{p}$ be a prime ideal in a ring R and let $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ be $\mathfrak{p}$-primary ideals of R; then also $\mathfrak{q} := \bigcap_{i=1}^{r} \mathfrak{q}_i$ is a $\mathfrak{p}$-primary ideal.*

Proof. First we observe that $\sqrt{\mathfrak{q}} = \bigcap_{i=1}^r \sqrt{\mathfrak{q}_i}$, as in general the radical of an arbitrary intersection of ideals is the intersection of the radicals of the ideals. This implies $\sqrt{\mathfrak{q}} = \mathfrak{p}$. Let now $a, b \in R$ with $ab \in \mathfrak{q} \subseteq \mathfrak{p}$; then for each $1 \leq i \leq r$, either $a \in \mathfrak{q}_i$ or $b \in \sqrt{\mathfrak{q}_i} = \mathfrak{p}$ or . If for all i we have $a \in \mathfrak{q}_i$, then $a \in \mathfrak{q}$; otherwise there is i forcing $b \in \mathfrak{p}$, and then $b \in \sqrt{\mathfrak{q}} = \mathfrak{p}$. This shows that $\mathfrak{q}$ is also $\mathfrak{p}$-primary. □

It follows from Lemma 8.16 that if we have a primary decomposition $I = \bigcap_{i=1}^r \mathfrak{q}_i$ and some of the ideals $\mathfrak{q}_i$ have the same prime ideal as radical, then we can replace them by their intersection, obtaining a new primary decomposition with fewer primary factors. Similarly, if there is i with $\mathfrak{q}_i \supseteq \bigcap_{j \neq i} \mathfrak{q}_j$, then we may neglect the factor $\mathfrak{q}_i$ and reduce the size of a primary decomposition.

Definition 8.17. Let R be a ring and I and ideal in R. A primary decomposition $I = \bigcap_{i=1}^r \mathfrak{q}_i$ is *minimal* if the following hold:

- for all $1 \leq i, j \leq r$ with $i \neq j$ we have $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$;
- for all $1 \leq i \leq j$ we have $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$.

The previous discussion, together with Lemma 8.16, shows that if an ideal in a ring has a primary decomposition, then it also has a minimal one. We are still somewhat unsatisfied by Example 8.7, as it provides for each $a \in k$ a different primary decomposition of $(xy, y^2) \subset k[x, y]$ as $(y) \cap (x + ay, y^2)$, and all these decompositions are minimal; but we are also a bit happy because also $(y) \cap (x, y)^2$ is a primary decomposition of (xy, y^2), and the latter decomposition feels more "canonical" as it is termwise contained in each of the previous ones. In general, if $I = \bigcap_{i=1}^r \mathfrak{q}_i$ and $I = \bigcap_{i=1}^s \mathfrak{q}'_i$ are two minimal decompositions, then we can also reduce $(\bigcap_{i=1}^r \mathfrak{q}_i) \cap (\bigcap_{i=1}^s \mathfrak{q}'_i)$ to a minimal decomposition $I = \bigcap_{i=1}^t \mathfrak{q}''_i$, such that each $\mathfrak{q}''_i$ is contained in some $\mathfrak{q}_j$ and in some $\mathfrak{q}'_l$. So for every two minimal decomposition there is one that is "finer" than both, and this is a sort of replacement for uniqueness. There are in fact some characteristics of a primary decomposition that are the same for each minimal primary decomposition, and we shall see them in the following. As a teaser, notice that all minimal primary decompositions of (xy, y^2) considered above have exactly two factors, one having the prime ideal (y) as radical, the other having the prime ideal (x, y) as radical. As a bigger teaser, here is a definition.

Definition 8.18. Let R be a ring and let $I \subseteq R$ be an ideal. We denote by $\mathrm{Ass}(I) \subseteq \mathrm{Spec}(R)$ the subset of those prime ideals $\mathfrak{p}$ of the form $\mathfrak{p} = \sqrt{(I \colon a)}$ for some $a \in R$. We say that each prime ideal in $\mathrm{Ass}(I)$ is *associated* to I.

Before proving that $\mathrm{Ass}(I)$ governs how many factors any minimal primary decomposition of I has, and which prime ideals occur as radicals of the factors, we need an exercise and a proposition.

Exercise 8.19. Let R be a Noetherian ring and $I \subseteq R$ be an ideal. Prove that there is $n \geq 1$ such that $\sqrt{I}^n \subseteq I$, where we consider the n-fold product of $\sqrt{I}$ with itself.

Proposition 8.20. *Let R be a ring and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal. Then the following hold.*

(1) for all $x \in \mathfrak{q}$ we have $(\mathfrak{q} \colon x) = R$;
(2) for all $x \in R \setminus \mathfrak{q}$ we have that $(\mathfrak{q} \colon x)$ is $\mathfrak{p}$-primary;
(3) for all $x \in R \setminus \mathfrak{p}$ we have $(\mathfrak{q} \colon x) = \mathfrak{q}$;

(4) if R is Noetherian, then there is some $x \in R \setminus \mathfrak{q}$ such that $(\mathfrak{q}\colon x) = \mathfrak{p}$.

Proof. (1) If $x \in \mathfrak{q}$, for all $a \in R$ we have $ax \in \mathfrak{q}$, i.e. $a \in (\mathfrak{q}\colon x)$.

(2) Suppose $x \notin \mathfrak{q}$. First we prove that $\sqrt{(\mathfrak{q}\colon x)} = \mathfrak{p}$: on the one hand the inclusion $\mathfrak{q} \subseteq (\mathfrak{q}\colon x)$ implies that $\mathfrak{p} \subseteq \sqrt{(\mathfrak{q}\colon x)}$; on the other hand, if $a \in \sqrt{(\mathfrak{q}\colon x)}$, then there is $n \geq 1$ with $xa^n \in \mathfrak{q}$, and since $\mathfrak{q}$ is primary and $x \notin \mathfrak{q}$ we must have $a^n \in \mathfrak{q}$, i.e. $a \in \mathfrak{p} = \sqrt{\mathfrak{q}}$. Second, we prove that $(\mathfrak{q}\colon x)$ is primary: let $a, b \in R$ such that $ab \in (\mathfrak{q}\colon x)$, and let us prove that $a \in (\mathfrak{q}\colon x)$ or $b \in \mathfrak{p}$. By hypothesis $abx = (ax)b \in \mathfrak{q}$, hence either $ax \in \mathfrak{q}$ (which means $a \in (\mathfrak{q}\colon x)$, or $b \in \mathfrak{p}$.

(3) Suppose $x \notin \mathfrak{p}$. We surely have a containment $\mathfrak{q} \subseteq (\mathfrak{q}\colon x)$; if $a \in (\mathfrak{q}\colon x)$, then $ax \in \mathfrak{q}$, and since no power of x lies in $\mathfrak{q}$ (for $\mathfrak{p} = \sqrt{\mathfrak{q}}$), we must have $a \in \mathfrak{q}$.

(4) Since R is Noetherian, by Exercise 8.19 there is a power of $\mathfrak{p}$ which is contained in $\mathfrak{q}$; we can take a minimal $n \geq 1$ with $\mathfrak{p}^n \subseteq \mathfrak{q}$, i.e. $\mathfrak{p}^{n-1} \nsubseteq \mathfrak{q}$ (for $n = 1$, we set $\mathfrak{p}^{n-1} = R$, which is definitely not contained in $\mathfrak{q}$). Let $x \in \mathfrak{p}^{n-1} \setminus \mathfrak{q}$; then by (2) we have $(\mathfrak{q}\colon x) \subseteq \mathfrak{p}$; moreover for all $a \in \mathfrak{p}$ we have $ax \in \mathfrak{p}^n \subseteq \mathfrak{q}$, hence $a \in (\mathfrak{q}\colon x)$.

□

In the following theorem, dealing with "uniqueness" of primary decompositions (as opposed to "existence"), we remarkably do not assume that R is Noetherian.

Theorem 8.21. *Let R be a ring, let I be an ideal of R, and suppose that $I = \bigcap_{i=1}^{r} \mathfrak{q}_i$ is a minimal primary decomposition of I (in particular, suppose that I admits a primary decomposition). Then $\left\{\sqrt{\mathfrak{q}_i}\right\}_{1 \leq i \leq r} = \mathrm{Ass}(I)$, in particular $r = |\mathrm{Ass}(I)|$.*

Proof. Let $\mathfrak{p} \in \mathrm{Ass}(I)$, i.e. there is $x \in R$ with $\sqrt{(I\colon x)} = \mathfrak{p}$; then we have

$$\mathfrak{p} = \sqrt{(I\colon x)} = \sqrt{\left(\bigcap_{i=1}^{r} \mathfrak{q}_i\colon x\right)} = \bigcap_{i=1}^{r} \sqrt{(\mathfrak{q}_i\colon x)}$$

and we can now appeal to Lemma 8.3 to conclude that $\mathfrak{p} = \sqrt{(\mathfrak{q}_i\colon x)}$ for some i; now Proposition 8.20 implies that $\sqrt{(\mathfrak{q}_i\colon x)}$ can only be equal to R or $\sqrt{\mathfrak{q}_i}$, so we must have $\mathfrak{p} = \sqrt{\mathfrak{q}_i}$.

Conversely, let $1 \leq i \leq r$; by minimality of the primary decomposition we can find $x \in \bigcap_{j \neq i} \mathfrak{q}_j \setminus \mathfrak{q}_i$. Then we have

$$\sqrt{(I\colon x)} = \sqrt{\left(\bigcap_{j=1}^{r} \mathfrak{q}_j\colon x\right)} = \bigcap_{j=1}^{r} \sqrt{(\mathfrak{q}_j\colon x)} = \sqrt{\mathfrak{q}_i},$$

since by Proposition 8.20 we have $\sqrt{(\mathfrak{q}_i\colon x)} = \mathfrak{p}$, whereas for all $j \neq i$ we have $\sqrt{(\mathfrak{q}_j\colon x)} = R$.

This concludes the equality of sets $\left\{\sqrt{\mathfrak{q}_i}\right\}_{1 \leq i \leq r} = \mathrm{Ass}(I)$; the equality $r = |\mathrm{Ass}(I)|$ follows again from the assumption that the primary decomposition is minimal, hence all prime ideals $\sqrt{\mathfrak{q}_i}$ are distinct. □

A direct consequence of Theorem 8.21 is that for an ideal I in a Noetherian ring R the set $\mathrm{Ass}(I)$ is finite. We can in fact refine the last step of the proof of Theorem 8.21 in the Noetherian case as follows.

Proposition 8.22. *Let R be a Noetherian ring and I an ideal in R. Then for each $\mathfrak{p} \in \mathrm{Ass}(I)$ there is $y \in R$ such that $(I\colon y) = \mathfrak{p}$ (and not only $x \in R$ such that $\sqrt{(I\colon x)} = \mathfrak{p}$ as the definition of $\mathrm{Ass}(I)$ guarantees).*

Proof. Let $I = \bigcap_{i=1}^{r} \mathfrak{q}_i$ be a minimal primary decomposition of I, and assume by Theorem 8.21 that $\mathfrak{p} = \sqrt{\mathfrak{q}_1}$. Let again $x \in \bigcap_{j\neq i} \mathfrak{q}_j \setminus \mathfrak{q}_i$, so that $\sqrt{(I\colon x)} = \mathfrak{p}$. We also have $(I\colon x) = \bigcap_{i=1}^{r}(\mathfrak{q}_i\colon x)$; using by Proposition 8.20 (1) we have $(I\colon x) = (\mathfrak{q}_1\colon x)$, by (2) we have that $(\mathfrak{q}_1\colon x)$ is $\mathfrak{p}$-primary, and by (4) we can then find x' such that $((\mathfrak{q}_1\colon x)\colon x') = \mathfrak{p}$. We can now identify the latter with $((I\colon x)\colon x')$ and finally with $(I\colon xx')$. □

8.4. **Geometric interpretation.** Let R be a ring; then $\mathrm{Spec}(R)$ is a topological space, in which the closed subsets are the subsets of the form $\mathbb{V}(I)$ for some ideal $I \subseteq R$. In fact, as we have seen, it suffices to consider radical ideals in order to describe all closed subsets.
A consequence of Lemma 8.3 is that for any ideals $I, J \subseteq R$ we have $\mathbb{V}(I \cap J) = \mathbb{V}(I) \cup \mathbb{V}(J)$

Definition 8.23. We say that a closed subset $\mathbb{V}(I) \subset \mathrm{Spec}(R)$ is *irreducible* if it cannot be written as a union of two strictly smaller closed subsets.

Lemma 8.24. *If $\mathfrak{p}$ is a prime ideal in a ring R, then $\mathbb{V}(\mathfrak{p}) \subseteq \mathrm{Spec}(R)$ is irreducible.*

Proof. Suppose that $\mathbb{V}(\mathfrak{p}) = \mathbb{V}(I) \cup \mathbb{V}(J)$; then in particular $\mathfrak{p} \in (\mathbb{V}(I) \cup \mathbb{V}(J))$, and without loss of generality we may assume $\mathfrak{p} \in \mathbb{V}(I)$. This means that $I \subseteq \mathfrak{p}$, and this implies $\mathbb{V}(\mathfrak{p}) \subseteq \mathbb{V}(I)$, so that in the end $\mathbb{V}(\mathfrak{p}) = \mathbb{V}(I)$. □

For $R = k[x_1, \dots, x_n]$, we can try to see whether it is true that, for $\mathfrak{p} \subset R$ a prime ideal, the subset $\mathbb{V}(\mathfrak{p}) \subset k^n$ cannot be written as a union of two smaller algebraic subsets. This turns out to be false at least in the case in which k is finite, and one should think of extending the discrete set k^n to the topological space $\mathrm{Spec}(k[x_1, \dots, x_n])$ as a way to force the statement of Lemma 8.24.
A straightforward consequence of the primary decomposition of ideals in a Noetherian ring R is that *radical* ideals $I \subset R$ admit the following primary decomposition: $I = \bigcap_{\mathfrak{p}\in \mathrm{Ass}(I)} \mathfrak{p}$. In fact this decomposition must be minimal, as it has the correct number of factors as predicted by Theorem 8.21.
Geometrically, this corresponds to the fact that every closed subset $\mathbb{V}(I) \subseteq \mathrm{Spec}(R)$ admits an expression as a union $\mathbb{V}(\mathfrak{p}_1) \cup \dots \mathbb{V}(\mathfrak{p}_r)$ of irreducible closed subsets, such that no $\mathbb{V}(\mathfrak{p}_i)$ is contained in the union $\bigcup_{j\neq i} \mathbb{V}(\mathfrak{p}_j)$. The subsets $\mathbb{V}(\mathfrak{p}_i)$ are called the *irreducible components* of $\mathbb{V}(I)$, and it is again a consequence of Lemma 8.3 that the decomposition of a closed subset $\mathbb{V}(I)$ as a finite union of irreducible closed subsets is unique.
Let now I be any ideal (possibly, a non-radical one) in a Noetherian ring R; then $\mathrm{Ass}(I)$ is a finite set; recall that for any minimal primary decomposition $I = \bigcap_{i=1}^{r} \mathfrak{q}_i$ we require $\mathfrak{q}_i \nsubseteq \mathfrak{q}_j$, but it may happen that $\sqrt{\mathfrak{q}_i} \subseteq \sqrt{\mathfrak{q}_j}$. This happens precisely in the situation of Example 8.7, where the associated primes of (xy, y^2) are $(y) \subseteq (x, y)$.

Definition 8.25. Let R be a ring and $I \subseteq R$ and ideal. We denote by $\mathrm{Ass}'(I) \subseteq \mathrm{Ass}(I)$ the subset of prime ideals that are minimal with respect to inclusion. We call the elements of $\mathrm{Ass}'(I)$ *isolated primes* and the elements in $\mathrm{Ass}(I) \setminus \mathrm{Ass}'(I)$ *embedded primes*.

As observed above, for I radical we have $\mathrm{Ass}'(I) = \mathrm{Ass}(I)$. The viceversa clearly fails (think of I being primary but not prime...). If $I \subseteq R$ is an ideal in a ring that admits a minimal primary decomposition $I = \bigcap_{i=1}^{r} \mathfrak{q}_i$, then Theorem 8.21 tells us that the prime ideals $\sqrt{\mathfrak{q}_i}$ constitute the entire set $\mathrm{Ass}(I)$, which is then finite; if follows that also $\mathrm{Ass}'(I)$ is finite in this case. Moreover we can write

$$\sqrt{I} = \bigcap_{i=1}^{r} \sqrt{\mathfrak{q}_i} = \bigcap_{\mathfrak{p} \in \mathrm{Ass}(I)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathrm{Ass}'(I)} \mathfrak{p},$$

and the last expression gives a minimal primary decomposition for $\sqrt{I}$: it follows that $\mathrm{Ass}'(I) = \mathrm{Ass}(\sqrt{I})$.
We further observe that if $\bar{\mathfrak{p}} \in \mathbb{V}(I)$ is *any* prime ideal, then $\sqrt{I} = \bigcap_{\mathfrak{p} \in \mathrm{Ass}'(I)} \mathfrak{p}$ is contained in $\bar{\mathfrak{p}}$, and by Lemma 8.3 we obtain that $\bar{\mathfrak{p}}$ contains one of the elements of $\mathrm{Ass}'(I)$; this shows that $\mathrm{Ass}'(\mathfrak{p})$ is the set of all minimal elements in $\mathbb{V}(I)$, and not only (as the definition guarantees) in $\mathrm{Ass}(I)$.

8.5. **Two funny exercises.**

Exercise 8.26. Here is a funny exercise, a bit unrelated to the previous discussion, but at least ideals of the form of Definition 8.15 show up. Let R be a ring and suppose that every prime ideal of R is principal; then R is a principal ideal ring! For the proof one can use the following strategy.

- For the sake of contradiction, let Σ be the family of all non-principal ideals of R, and assume $\Sigma \neq 0$. Prove that Σ must have a maximal element using Zorn's lemma.
- Let $I \in \Sigma$ be maximal; we claim that I is a prime ideal, and this would lead to a contradiction. Let therefore $a, n \in R$ with $ab \in I$. Assume $a \notin I$; then (I, a) is principal (why?), say generated by α. Moreover $(I \colon \alpha)$ contains (I, b), so it is also principal, say generated by β, unless $b \in I$ (why?). Justify the two "why?".
- Prove that I is principal, generated by $\alpha\beta$, and get a contradiction.

Exercise 8.27. Here is another funny exercise, similar to the previous. Let R be a ring and suppose that every prime ideal of R is finitely generated; then R is Noetherian! For the proof, one considers again the family Σ of non-finitely-generated ideals and finds a maximal $I \in \Sigma$ by Zorn; the claim is then that I is a prime ideal, contradicting the hypothesis.
For this, let $a, b \in I$ with $ab \in I$, and assume that $a, b \notin I$. Then (a, I) is finitely generated, say by $a_1, \ldots, a_n$. In particular every element of I can be written as $r_1 a_1 + \cdots + r_n a_n$ for some $r_i \in R$.
Consider now, for all $1 \leq i \leq n$, the submodule $N_i \subset R^i$ of those sequences $(r_1, \ldots, r_i)$ such that $r_1 a_1 + \cdots + r_i a_i \in I$; prove that the set $J_i = \{r_i \mid (r_1, \ldots, r_i) \in N_i\}$ of all "last coordinates" of elements in N_i is an ideal of R, containing I but also containing b. Conclude that each J_i is finitely generated, say by elements $c_{i,1}, \ldots, c_{i,n_i} \in J_i$.
Find suitable elements $d_{i,j} \in I$ for $1 \leq j \leq n$ and $1 \leq j \leq n_i$ such that $I = (d_{i,j})$: use here an argument as in the proof of Theorem 7.12.

9. Artinian rings

We resume the discussion started in Subsection 7.4. Our aim is to prove the following theorem.

Theorem 9.1. *Let R be a non-zero ring. Then R is Artinian (in the sense of Definition 7.20) if and only if R is Noetherian and the* Krull dimension *of R is 0.*

The statement of the theorem contains a new notion, that of Krull dimension. We will start by introducing it.

9.1. **Krull dimension.** The Krull dimension is a basic invariant that one can associate with a ring. We introduce it here, and we will study it more closely later in the course.

Definition 9.2. Let R be a ring. For $l \geq 0$, a *proper chain of prime ideals of length* l is a chain $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_l \subset R$ of $l+1$ *distinct* prime ideals in R. The *Krull dimension* of R is defined as

$$\dim(R) = \sup\{l \geq 0 \,|\, \exists \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_l \subset R\}$$

i.e. the supremum of lengths of proper chains of prime ideals. We set the Krull dimension of the zero ring to be $-\infty$. For non-zero rings, we have $\dim(R) \in \mathbb{N} \cup \{+\infty\}$.

Our notation for the Krull dimension in this course is just $\dim(R)$; sometimes one considers also other notions of dimension on a ring, and then one usually writes something like $\mathrm{Krdim}(R)$ to specify the Krull dimension. Note that the length of a chain is one less than the number of prime ideals appearing in it; this is because for all rings (except the zero ring, which doesn't have any prime ideal) we always have at least one prime ideal, so we are more interested in how much *longer* a proper chain of prime ideals can be.

Example 9.3. A field k has a unique prime ideal (0), so $\dim(k) = 0$. A PID R which is not a field, like $\mathbb{Z}$ or $k[x]$, has dimension 1: on the one hand we can find a prime ideal $\mathfrak{p} \subset R$ different from (0) (for otherwise (0) would be maximal), so that $(0) \subset \mathfrak{p}$ is a chain of prime ideals of length 1; on the other hand if $(p_1) \subsetneq (p_2)$ are non-zero prime ideals, generated by $p_1, p_2 \in R$, then $p_1 \mid p_2$, so by the unique factorisation theorem for PIDs we must have $p_2 = ap_1$ for some $a \in R^\times$, so that $(p_1) = (p_2)$.
The ring $k[x_i \,|\, i \in \mathbb{N}]$ has infinite Krull dimension: indeed we can find arbitrarily long proper chains of prime ideals, and even an infinite chain like $(x_1) \subset (x_1, x_2) \subset (x_1, x_2, x_3) \subset \ldots$.

Example 9.4. Let R be a ring of finite Krull dimension $d \geq 0$. Then $\dim(R[x]) \geq d+1$: given a proper chain of prime ideals $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_d \subset R$ of length d, we have a proper chain of prime ideals of length $d+1$

$$\mathfrak{p}_0^e \subset \mathfrak{p}_1^e \subset \cdots \subset \mathfrak{p}_d^e \subset (\mathfrak{p}_d^e, x) \subset R[x]$$

where $\mathfrak{p}_i^e$ is the extension of $\mathfrak{p}_i$ along the inclusion $R \hookrightarrow R[x]$ (check as exercise that all given ideals are indeed prime ideals). In particular we have, for a field k, that $\dim(k[x_1, \ldots, x_n]) \geq n$.
Later in the course, we will see that in fact $\dim(R[x]) = \dim(R)+1$, and in particular $\dim(k[x_1, \ldots, x_n]) = n$.

We can now understand the statement of Theorem 9.1. In particular, it implies that every Artinian ring is Noetherian, so if every descending chain of ideals in a ring stabilises, then also every ascending chain stabilises: this fact is already non-obvious at first glance. Note that the condition $\dim(R) = 0$ is the same as saying that every prime ideal in R is a maximal ideal.

9.2. **Proof of Theorem 9.1.** We split the proof of Theorem 9.1 into a few lemmas. Throughout the subsection we always assume that the rings considered are non-zero rings, without writing it.

Lemma 9.5. *Let R be an Artinian ring. Then $\dim(R) = 0$, and $\mathrm{Spec}(R)$ is finite.*

Proof. Let $\mathfrak{p}$ be a prime ideal in R; we want to prove that it is maximal. Equivalently, we can prove that the domain $R/\mathfrak{p}$ is a field. So let $x \in R/\mathfrak{p}$ be a non-zero element; then the descending chain of principal ideals

$$(x) \supseteq (x^2) \supseteq (x^3) \supseteq \dots$$

stabilises, and in particular there is $\bar{n}$ with $(x^{\bar{n}}) = (x^{\bar{n}+1})$. This means that there is $a \in R/\mathfrak{p}$ with $ax^{\bar{n}+1} = x^{\bar{n}}$, i.e. $x^{\bar{n}}(ax - 1) = 0 \in R/\mathfrak{p}$. And now we use that $R/\mathfrak{p}$ is a domain, and that we assumed $x \neq 0$: we obtain $ax - 1 = 0$, so that $x \in (R/\mathfrak{p})^\times$. Thus every non-zero element in $R/\mathfrak{p}$ is invertible, i.e. $R/\mathfrak{p}$ is a field. As a consequence, $\dim(R) = 0$.
We now prove that $\mathrm{Spec}(R)$ is finite. For the sake of contradiction, suppose that $\mathrm{Spec}(R)$ was infinite, and let $(\mathfrak{p}_i)_{i\in\mathbb{N}}$ be a family of distinct prime ideals in R. We consider the descending chain of ideals

$$\mathfrak{p}_1 \supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3 \supseteq \dots$$

which stabilises at some point. In particular there is $n \geq 1$ with $\bigcap_{i=1}^{n} \mathfrak{p}_i = \bigcap_{i=1}^{n+1} \mathfrak{p}_i$; this implies the inclusion $\bigcap_{i=1}^{n} \mathfrak{p}_i \subseteq \mathfrak{p}_{n+1}$, and now Lemma 8.3 implies that $\mathfrak{p}_i \subseteq \mathfrak{p}_{n+1}$ for some index $1 \leq i \leq n$. If the inclusion is strict, this would imply $\dim(R) \geq 1$, contradicting what we have proved above; hence the inclusion is an equality, contradicting our choice of distinct prime ideals. □

In particular, if R is an Artinian ring and $\mathrm{Spec}(R) = \{\mathfrak{m}_1, \dots, \mathfrak{m}_r\}$, then $J(R) = \bigcap_{i=1}^{r} \mathfrak{m}_i = \sqrt{(0)} \subset R$. By definition of $\sqrt{(0)}$, for each $a \in \sqrt{(0)}$ there is $n \geq 1$ with $a^n = 0$; a priori, n could depend on a and it could be arbitrarily large for varying a; the following lemma shows that this is not the case.

Lemma 9.6. *Let R be an Artinian ring; then then there is an integer $n \geq 1$ such that $\sqrt{(0)}^n = 0$.*

Proof. We have a descending chain of ideals

$$\sqrt{(0)} \supseteq \sqrt{(0)}^2 \supseteq \sqrt{(0)}^3 \supseteq \dots$$

and since R is Artinian we can find $\bar{i} \geq 1$ such that $\sqrt{(0)}^{\bar{i}} = \sqrt{(0)}^{\bar{i}+1}$.
Suppose for the sake of contradiction that $\sqrt{(0)}^{\bar{i}} \neq (0)$, and let Σ be the family of ideals $J \subseteq \sqrt{(0)}^{\bar{i}}$ such that $J \cdot \sqrt{(0)}^{\bar{i}} \neq (0)$. An example of such an ideal is the ring R, so Σ is non-empty. By Exercise 7.21, using again that R is Artinian, we can find an ideal $\bar{J} \in \Sigma$ which is minimal with respect to inclusion. Clearly $\bar{J} \neq (0)$.

Let now $K = \mathrm{Ann}\left(\bar{J}\sqrt{(0)}^{\bar{i}}\right) \subseteq R$ be the ideal of all elements $a \in R$ such that $am = 0$ for all $m \in \bar{J}\sqrt{(0)}^{\bar{i}}$. We claim that K is a radical ideal. For this, let $a \in \sqrt{K}$ and let $n \geq 1$ be minimal such that $a^n \in K$; then $(a)^{n-1}\bar{J}\sqrt{(0)}^{\bar{i}} \neq (0)$, hence the ideal $(a)^{n-1}\bar{J}$ belongs to Σ, and since $(a)^{n-1}\bar{J} \subseteq \bar{J}$, we must have $(a)^{n-1}\bar{J} = \bar{J}$. It follows that $(0) = (a)^n\bar{J}\sqrt{(0)}^{\bar{i}} = (a)\bar{J}\sqrt{(0)}^{\bar{i}}$, i.e. $a \in K$.
Finally, since K is a radical ideal, we have $\sqrt{(0)} \subseteq K$; in particular we have a chain of inclusions

$$\bar{J}\sqrt{(0)}^{\bar{i}} = \bar{J}\sqrt{(0)}^{\bar{i}+1} \subseteq \bar{J}\sqrt{(0)}^{\bar{i}}K = (0),$$

but this contradicts the fact that $\bar{J} \in \Sigma$. □

Lemma 9.6 gives a little evidence that Artinian rings are Noetherian: indeed for any Noetherian ring R there is $n \geq 1$ such that $\sqrt{(0)}^n = (0)$, as follows from Exercise 8.19.
The following lemma provides a bridge between the Artinian and Noetherian worlds; in the end, all that is used is that for a vector space over a field k, both being Noetherian and being Artinian are equivalent to being finite dimensional.

Lemma 9.7. *Let R be a ring and let $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ be (possibly non-distinct) maximal ideals of R such that $\mathfrak{m}_1 \dots \mathfrak{m}_n = 0$. Then R is Artinian if and only if it is Noetherian.*

Proof. We consider the chain of ideals $(0) = \mathfrak{m}_1 \dots \mathfrak{m}_n \subseteq \mathfrak{m}_1 \dots \mathfrak{m}_{n-1} \subseteq \dots \subseteq \mathfrak{m}_1 \subseteq R$ as a chain of sub-R-modules of R. Each quotient $\mathfrak{m}_1 \dots \mathfrak{m}_{i-1}/\mathfrak{m}_1 \dots \mathfrak{m}_i$ is an R-module on which $\mathfrak{m}_i$ acts as zero by scalar multiplication, i.e. it is a $R/\mathfrak{m}_i$-vector space. Applying Corollary 7.16 and Exercise 7.27, we obtain R being Noetherian is equivalent to each R-module $\mathfrak{m}_1 \dots \mathfrak{m}_{i-1}/\mathfrak{m}_1 \dots \mathfrak{m}_i$ being Noetherian, which is equivalent to each $R/\mathfrak{m}_i$-vector space $\mathfrak{m}_1 \dots \mathfrak{m}_{i-1}/\mathfrak{m}_1 \dots \mathfrak{m}_i$ being finite dimensional, which is equivalent to each R-module $\mathfrak{m}_1 \dots \mathfrak{m}_{i-1}/\mathfrak{m}_1 \dots \mathfrak{m}_i$ being Artinian, which is equivalent to R being Artinian. □

We are ready to prove Theorem 9.1

Proof of Theorem 9.1. Let R be a ring, and assume either that R is Artinian, or that R is Noetherian of dimension 0.
First, we prove that $\sqrt{(0)}$ can be written as a finite intersection $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r$ of maximal ideals. For R Artinian, this Lemma 9.5. For R Noetherian of dimension 0, this is a consequence of the existence of primary decompositions in Noetherian rings: as we saw in Subsection 8.4 we can express $\sqrt{(0)} = \bigcap_{\mathfrak{p} \in \mathrm{Ass}((0))} \mathfrak{p}$ as a finite intersection of prime ideals, and if $\dim(R) = 0$ all prime ideals are maximal.
Second, we prove that there is $n \geq 1$ such that $\sqrt{(0)}^n = (0)$. For R Artinian, this is Lemma 9.6. For R Noetherian (of dimension 0), this is an application of Exercise 8.19.
Using the previous, in either hypothesis on R we obtain a chain of inclusions

$$\mathfrak{m}_1^n \dots \mathfrak{m}_r^n \subseteq (\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_r)^n = \sqrt{(0)}^n = (0),$$

and by Lemma 9.7 we conclude that also "the other condition" on R holds. □

9.3. **Local Artinian rings.** If the word "dimension" is not chosen at random, we should expect that a geometric object associated with R, such as $\mathrm{Spec}(R)$, should really look as something of dimension $\dim(R)$. This intuition is for instance compatible with what we claimed in Example 9.4, that for a field k we have $\dim(k[x_1,\dots,x_n]) = n$, as we think of $\mathrm{Spec}(k[x_1,\dots,x_n])$ as a thick version of k^n, which (at least as a k-vector space) has dimension n.
Now, if R is Artinian, then in particular $\dim(R) = 0$, and the space $\mathrm{Spec}(R)$ is a finite, disjoint union of points; moreover the topology is discrete, as every point $\mathfrak{p} \in \dim(R)$ is the unique point in $\mathbb{V}(\mathfrak{p})$ (here we use that all prime ideals are maximal); that is, every singleton in $\mathrm{Spec}(R)$ is a closed subset; using that $\mathrm{Spec}(R)$ is finite, we also have that every singleton is open.
Moreover, our intuition tells us that R should be thought of a ring of "regular functions" defined on the space $\mathrm{Spec}(R)$; we think of "regularity" as a sort of generalisation of continuity (like smoothness or holomorphicity). If now $\mathrm{Spec}(R)$ is totally disconnected, then we expect that to define a regular function on $\mathrm{Spec}(R)$ we just have to declare its restriction on each singleton of $\mathrm{Spec}(R)$, as these form a cover by disjoint open sets.
Going back to algebra, we expect an Artinian ring R to split as a product of Artinian rings having a single point in their spectrum. And... our intuition works!

Theorem 9.8. *Every Artinian ring factors as a product of Artinian rings.*

In order to prove the theorem, we will use the Chinese Reminder Theorem, that we briefly mention.

Proposition 9.9 (Chinese Reminder Theorem)**.** *Let R be a ring and let $I_1,\dots,I_n$ be ideals in R; assume that for all $1 \le i,j \le n$ with $i \ne j$ we have $I_i + I_j = R$, and let $I = \bigcap_{i=1}^n I_i$; consider the canonical projections of rings $p_i\colon R/I \twoheadrightarrow R/I_i$ and let p be the product ring homomorphism*

$$p\colon R/I \to \prod_{i=1}^n R/I_i;$$

then p is an isomorphism.

Proof. We first check that p is injective. If $[x]_I \in \ker(p)$, then $[x]_{I_i} = 0$, i.e. $x \in I_i$ for all $1 \le i \le n$, and this precisely means that $x \in I$, i.e. $[x]_I = [0]_I$.
For surjectivity, for $1 \le j \le n$ let $e_j \in \prod_{i=1}^n R/I_i$ be the element whose R/I_j-component is $[1]_{I_j}$, and whose R/I_i-component for any $i \ne j$ is $[0]_{I_i}$; then the elements $e_1,\dots,e_n$ generate $\prod_{i=1}^n R/I_i$ as an R-module, so it suffices to prove that each e_j is in the image of p.
For this, fix j and for varying $i \ne j$ let $a_i, b_i \in R$ be such that $a_i \in I_i$, $b_i \in I_j$ and $a_i + b_i = 1$; then the element $x_j := 1 - \prod_{i\ne j} a_i = (\prod_{i\ne j}(a_i + b_i) - \prod_{i\ne j} a_i)$ is such that $[x_j]_{I_j} = [0]$, whereas $[x_j]_{I_i} = [1]_{I_i}$. We conclude by noticing that $p\colon \prod_{i\ne j} x_i \mapsto e_j$. □

Proof of Theorem 9.8. Let $\mathfrak{m}_1,\dots\mathfrak{m}_r$ be the list of all maximal ideals in R, and let $(0) = \bigcap_{i=1}^r \mathfrak{q}_i$ be a primary decomposition of (0), with $\mathfrak{q}_i$ being $\mathfrak{m}_i$-primary. Since R is Noetherian, for all $1 \le i \le r$ there is a power of $\mathfrak{m}_i$ contained in $\mathfrak{q}_i$; taking the maximum exponent, we find $n \ge 1$ such that $\mathfrak{m}_i^n \subseteq \mathfrak{q}_i$ for all $1 \le i \le r$. We then have $(0) = \bigcap_{i=1}^r \mathfrak{m}_i^n$ is another primary decomposition of (0).

Now set $I_i = \mathfrak{m}_i^n$ for $1 \leq i \leq r$. Then for all $i \neq j$ we have that $I_i + I_j$ is not contained in any of the maximal ideals (for otherwise there would be a maximal ideal containing both $\mathfrak{m}_i$ and $\mathfrak{m}_j$); it follows that $I_i + I_j = R$. We can thus apply the Chinese Reminder Theorem, and conclude that $R \cong \prod_{i=1}^r R/\mathfrak{m}_i^n$; each of the rings $R/\mathfrak{m}_i^n$ has a unique prime ideal, hence it is Artinian and local. □

Exercise 9.10. Prove uniqueness in Theorem 9.8: if R is also isomorphic to a product $R \cong \prod_{i=1}^{r'} S_i$, for some local Artinian rings S_i, then $r = r'$ and up to permutation of the indices one can find isomorphisms $S_i \cong R/\mathfrak{m}_i^n$, such that the isomorphism $R \cong \prod_{i=1}^{r'} S_i$ is nothing but the composite of the isomorphism $R \cong \prod_{i=1}^r R/\mathfrak{m}_i^n$ followed by the product of the isomorphisms $S_i \cong R/\mathfrak{m}_i^n$.

10. Tensor products of modules and algebras

Warning: part of the notes in this section are copied from the lecture notes for the course "Homological Algebra" that I taught in 2021-2022. All mistakes contained there (and new ones) are present here.

10.1. **Bilinear maps.** In this lecture we ask ourselves the following general question: given an R-module M, is there a natural way to promote it to an R-algebra? That is, can we multiply two elements of M? More generally, given two R-modules M and M', can we compute the product $m \cdot m'$ for $m \in M$ and $m' \in M'$?
A priori, the answer to all of the previous questions is "no": by definition, if M is an R-module, the only defined operations are sum and multiplication of an element of M with an element of the ring R; but given two R-modules M and M' and elements $m \in M$ and $m' \in M'$, the product $m \cdot m'$ just does not make sense (and it is not even clear *where* it should lie). However, there are situations, such as the following, in which a meaningful product is indeed defined.

Example 10.1. As we saw in Example 2.15, if (S, ϕ) is an R-algebra (i.e., if R and S are rings and $\phi\colon R \to S$ is a ring homomorphism), then we can consider S also as an R-module. And for the R-module S we can restore the product of S. So S is an R-module and we have a product map $\mu_S\colon S \times S \to S$.

Example 10.2. Let R be a ring and consider $M = R[x]$ and $M' = R[y]$ as R-modules. Given polynomials $P \in M$ and $Q \in M'$, the product $P \cdot Q$ makes perfectly sense in the bigger polynomial ring $R[x, y]$. We have in fact multiplication map

$$\mu\colon R[x] \times R[y] \to R[x, y].$$

Note that the target is a new R-module, different from both M and M'.

Example 10.3. Let $R = \mathbb{Z}$ and consider $M = \mathbb{Z}/10$ and $M' = \mathbb{Z}/20$ as $\mathbb{Z}$-modules. Then we may define a map

$$\mu\colon M \times M' \to \mathbb{Z}/2, \qquad ([m]_{10}, [m']_{20}) \mapsto [mm']_2.$$

The previous map is essentially given by projecting both M and M' onto $\mathbb{Z}/2$, and then taking the product in the ring $\mathbb{Z}/2$.
Of course, we could also have projected onto $\mathbb{Z}/5$ instead, or even better onto $\mathbb{Z}/10$ (or even worse, onto the 0 module!).

The previous examples are instances of the following definition.

Definition 10.4. Let R be a ring and let M, M', P be R-modules. An *R-bilinear map*

$$\mu\colon M \times M' \to P$$

is a map of sets satisfying the following properties, for all $m_1, m_2 \in M$, $m_1', m_2' \in M'$ and $r \in R$:

(1) $\mu(m_1 + m_2, m_1') = \mu(m_1, m_1') + \mu(m_2, m_1') \in P$;
(2) $\mu(m_1, m_1' + m_2') = \mu(m_1, m_1') + \mu(m_1, m_2') \in P$;
(3) $\mu(r \cdot m_1, m_1') = \mu(m_1, r \cdot m_1') = r \cdot \mu(m_1, m_1') \in P$.

The three properties in the previous definition extrapolate what one usually whishes from a multiplication in an R-algebra: the first two are a form of distributive law with respect to the addition; the third is a form of compatibility of the multiplication μ with the scalar multiplication (multiplication by elements in R).
Given M and M', the question becomes: *what are the possible choices of P and of an R-bilinear map $\mu\colon M \times M' \to P$? Is there a choice which is better than the other ones?* The second part of the question is justified by the trivial example in which we take $P = 0$ and μ the constant, zero map: in this case we do get an R-bilinear map, but it is a quite boring and useless one!
In general, if we want to construct an R-bilinear map $\mu\colon M \times M' \to P$, we need the following: for all $(m, m') \in M \times M'$ we need to identify an element $\mu(m, m') \in P$; up to replacing P with a submodule, it does not harm to assume that P is in fact generated by the set of elements $(\mu(m, m'))_{(m,m') \in M \times M'}$. Moreover the relations (1)-(3) from Definition 10.4 must hold between these elements.
In few words, the tensor product $M \otimes_R M'$ will be constructed in the most direct way to have all the previous properties: it is obtained from a free module with basis the elements (m, m') of the set $M \times M$, by quotienting the suitable submodule that guarantees that (1)-(3) hold.

10.2. **Definition of tensor products by construction.** The following is the "bad definition" of the tensor product. It is an explicit construction, but it produces an R-module that, in principle, is difficult to handle with: it has a lot of generators and a lot of relations. Only after proving Proposition 10.6 we will be able to understand what makes the tensor product so special.

Definition 10.5. Let M and M' be R-modules. We define an R module $M \otimes_R M'$ as follows. We start with the free module $F = \bigoplus_{(m,m') \in M \times M'} R$, and denote simply by (m, m') the element of the standard basis of F corresponding to 1 in the copy of R with index (m, m'). We then consider the submodule N of F generated by all elements of the following forms, for all $m_1, m_2 \in M$, $m_1', m_2' \in M'$ and $r \in R$:

- $(m_1 + m_2, m_1') - (m_1, m_1') - (m_2, m_1')$;
- $(m_1, m_1' + m_2') - (m_1, m_1') - (m_1, m_2')$;
- $(r \cdot m_1, m_1') - r \cdot (m_1, m_1')$;
- $(m_1, r \cdot m_1') - r \cdot (m_1, m_1')$.

Finally, we define $M \otimes_R M'$ as the quotient R-module F/N. The class of the generator (m, m') in F/N is also denoted $m \otimes m' \in M \otimes_R M'$.
The map of sets $\mu_\otimes\colon M \times M' \to M \otimes_R M'$ is defined by $\mu_\otimes(m, m') = m \otimes m'$, and it is by construction an R-bilinear map.

In a sense, Definition 10.5 produces an R-module P which is designed in order to receive a bilinear map from $M \times M'$. The following proposition makes this idea more precise.

Proposition 10.6. *Let $\mu\colon M \times M' \to P$ be any R-bilinear map, with target any R-module P. Then there exists a* unique *R-linear map $\theta\colon M \otimes_R M' \to P$ such that the following diagram of maps (of sets) commutes:*

$$\begin{array}{ccc} M \times M' & \xrightarrow{\mu_\otimes} & M \otimes_R M' \\ & \searrow^{\mu} & \downarrow{\scriptstyle \theta} \\ & & P. \end{array}$$

Proof. Since $M \otimes M'$ is a quotient F/N, giving an R-linear map $\theta\colon F/N \to P$ is equivalent to giving an R-linear map $\tilde{\theta}\colon F \to P$ that vanishes on N: the map $\tilde{\theta}$ is obtained from θ as the composite $F \twoheadrightarrow F/N \xrightarrow{\theta} P$.
If we want the diagram to commute, we must have the equality

$$\tilde{\theta}(m, m') = \theta(m \otimes m') = \mu(m, m')$$

for all $(m, m') \in M \times M'$. Thus the map $\tilde{\theta}$ is forced on the R-basis of F given by the elements (m, m'), and we can conclude that there are two possibilities:

- either $\tilde{\theta}\colon F \to P$ descends to an R-linear map $\theta\colon F/N \to P$, i.e. it vanishes on N;
- or $\tilde{\theta}$ does not descend to an R-linear map $\theta\colon F/N \to P$.

In the first case, we would have that θ exists and is unique; in the second case instead we would have that θ does not exist. Let us rule out the second case.
To prove that $\tilde{\theta}$ vanishes on N, it suffices to prove that it vanishes on generators (1)-(4) of N. Let us compute as example the image of a generator of N of type (3) along $\tilde{\theta}$:

$$\begin{aligned} \tilde{\theta}\big((r \cdot m_1, m_1') - r \cdot (m_1, m_1')\big) &= \tilde{\theta}(r \cdot m_1, m_1') - r \cdot \tilde{\theta}(m_1, m_1') \\ &= \mu(r \cdot m_1, m_1') - r \cdot \mu(m_1, m_1') = 0. \end{aligned}$$

In the first equality we use R-linearity of $\tilde{\theta}\colon F \to P$; in the second we use the definition of $\tilde{\theta}$, i.e. its evaluation on the basis of F; in the third we use that $\mu\colon M \times M' \to P$ is R-bilinear.
In a similar way one can check that all generators of N are sent to 0 along $\tilde{\theta}$. □

10.3. **Definition of tensor product by universal property.** Motivated by Proposition 10.6, we give the following, which is the "good definition" of the tensor product, by *universal property*.

Definition 10.7. Let M and M' be R-modules. A universal bilinear map for $M \times M'$ is the datum of a couple $(\bar{P}, \bar{\mu})$, where $\bar{P}$ is an R-module and where $\bar{\mu}\colon M \times M' \to P$ is an R-bilinear map, satisfying the following property (called *universal property*): whenever (P, μ) is a (possibly different) couple with P being an R-module and $\mu\colon M \times M' \to P$ an R-bilinear map, then there exists a *unique*

R-linear map $\theta\colon \bar{P} \to P$ such that the following diagram of maps of sets commutes:

$$\begin{array}{ccc} M \times M' & \xrightarrow{\bar{\mu}} & \bar{P} \\ & \searrow^{\mu} & \downarrow{\scriptstyle \theta} \\ & & P. \end{array}$$

At first glance, it is not clear why the previous is a definition at all. A priori, such a wonderful $(\bar{P}, \bar{\mu})$ could not exist at all! But here Proposition 10.6 helps us: it tells us that in fact $(M \otimes M', \mu_{\otimes})$ satisfies the property required for $(\bar{P}, \bar{\mu})$. On the other hand, giving a property of an object often does not suffice to *define* the object. We have to check that, in fact, the property of $(\bar{P}, \bar{\mu})$ in Definition 10.7 suffices to determine this couple, at least up to isomorphism.
The argument is as follows. Let $(\bar{P}, \bar{\mu})$ and $(\check{P}, \check{\mu})$ be two couples satisfying the property required by Definition 10.7. If you wish, think that $(\bar{P}, \bar{\mu})$ is the tensor product from Definition 10.5, and $(\check{P}, \check{\mu})$ is instead obtained in another way.
Since $\bar{\mu}\colon M \times M' \to \bar{P}$ is an example of an R-bilinear map with source $M \times M'$, the universal property of $(\check{P}, \check{\mu})$ implies that there is a *unique* R-linear map $\theta_1\colon \check{P} \to \bar{P}$ such that the following commutes

$$\begin{array}{ccc} M \times M' & \xrightarrow{\check{\mu}} & \check{P} \\ & \searrow^{\bar{\mu}} & \downarrow{\scriptstyle \theta_1} \\ & & \bar{P}. \end{array}$$

Viceversa, since $\check{\mu}\colon M \times M' \to \check{P}$ is R-bilinear, the universal property of the couple $(\bar{P}, \bar{\mu})$ implies that there is a *unique* R-linear map $\theta_2\colon \bar{P} \to \check{P}$ such that the following commutes

$$\begin{array}{ccc} M \times M' & \xrightarrow{\bar{\mu}} & \bar{P} \\ & \searrow^{\check{\mu}} & \downarrow{\scriptstyle \theta_2} \\ & & \check{P}. \end{array}$$

Moreover, since $\bar{\mu}\colon M \times M' \to \bar{P}$ is R-bilinear, the universal property of $(\bar{P}, \bar{\mu})$ *itself* implies that there is a *unique* R-linear map $\bar{\theta}\colon \bar{P} \to \bar{P}$ such that the following commutes

$$\begin{array}{ccc} M \times M' & \xrightarrow{\bar{\mu}} & \bar{P} \\ & \searrow^{\bar{\mu}} & \downarrow{\scriptstyle \bar{\theta}} \\ & & \bar{P}. \end{array}$$

In the last diagram we have two natural candidates for $\bar{\theta}$: one is $\mathrm{Id}_{\bar{P}}$, and the other is $\theta_1 \circ \theta_2$: this second map makes the last diagram commute because we can glue the two previous diagrams, in which θ_1 and θ_2 appear.
By *uniqueness* of $\bar{\theta}$, we get that $\mathrm{Id}_{\bar{P}} = \theta_1 \circ \theta_2$. Similarly, using the universal property of $(\check{P}, \check{\mu})$ against $\check{\mu}$, one obtains that $\mathrm{Id}_{\check{P}} = \theta_2 \circ \theta_1$. This means that θ_1 and θ_2 are inverse R-linear isomorphisms between $\bar{P}$ and $\check{P}$, and that along these isomorphisms the bilinear maps $\bar{\mu}$ and $\check{\mu}$ are identified. In this sense, Definition 10.7 characterises a universal bilinear map out of $M \times M'$ up to canonical isomorphism.

Example 10.8. Let $f\colon M \to N$ and $f'\colon M' \to N'$ be R-linear maps. You can check that for any R-bilinear map $\mu_1\colon N \times N' \to P$ the composite map of sets

$$M \times M' \xrightarrow{f\times f'} N \times N' \xrightarrow{\mu_1} P$$

is an R-bilinear map $\mu_2\colon M\times M' \to P$. This holds in particular when $P = N\otimes_R N'$ and $\mu_1 = \mu_\otimes\colon N \times N' \to N \otimes_R N'$ is the universal bilinear map of $N \times N'$. The universal property of $M \otimes_R M'$ implies that there is a *unique* R-linear map $\theta\colon M \otimes_R M' \to N \otimes_R N'$ such that the following diagram commutes

$$\begin{array}{ccc} M \times M' & \xrightarrow{\mu_\otimes} & M \otimes_R M' \\ \downarrow{\scriptstyle f\times f'} & & \downarrow{\scriptstyle \theta} \\ N \times N' & \xrightarrow{\mu_\otimes} & N \otimes_R N. \end{array}$$

The map θ is often denoted as $f \otimes_R f'\colon M \otimes_R M' \to N \otimes_R N'$.

Exercise 10.9. Let $R\mathrm{Mod} \boxtimes R\mathrm{Mod}$ be the category whose objects are couples of R-modules (M, M'), and in which a morphism $(M, M') \to (N, N')$ is a couple of R-linear maps (f, f') with $f\colon M \to N$ and $f'\colon M' \to N'$. Start from Example 10.8 and check that there is a well-defined functor $\otimes_R\colon R\mathrm{Mod}\times R\mathrm{Mod} \to R\mathrm{Mod}$ sending the object $(M, M') \mapsto M \otimes_R M'$ and sending the morphism $(f, f') \mapsto f \otimes_R f'$.
In particular, for fixed M, we obtain a restricted functor $M \otimes_R -\colon R\mathrm{Mod} \to R\mathrm{Mod}$ sending $M' \mapsto M \otimes_R M'$ and $(f'\colon M' \to N') \mapsto \mathrm{Id}_M \otimes_R f'$. Describe similarly a restricted functor $- \otimes_R M'\colon R\mathrm{Mod} \to R\mathrm{Mod}$ for fixed M'.

10.4. **Examples and properties of tensor products.** In the next examples we compute explicitly some tensor products. We will use both Definition 10.5 and Definition 10.7, to show how combining the two leads to very quick arguments of proof.

Example 10.10. One can sometimes also work with Definition 10.5. For instance, let $m, n \geq 0$ and let's compute directly $\mathbb{Z}/m\otimes_\mathbb{Z}\mathbb{Z}/n$. Each generator $[a]_m \otimes [b]_n$ can be written as $ab\cdot[1]_m \otimes [1]_n$: this implies in particular that $\mathbb{Z}/m\otimes_\mathbb{Z}\mathbb{Z}/n$ is generated over $\mathbb{Z}$ by the single element $[1]_m \otimes [1]_n$, and is thus of the form $\mathbb{Z}/l$ for some $l \geq 0$. What is l? Equivalently, what is the ideal $\mathrm{Ann}([1]_m \otimes [1]_n) \subseteq \mathbb{Z}$? On the one hand we have $m \cdot [1]_m \otimes [1]_n = [m]_m \otimes [1]_n = 0$ and $n \cdot [1]_m \otimes [1]_n = \cdot[1]_m \otimes [n]_n = 0$, so that $\mathrm{Ann}([1]_m \otimes [1]_n) \supseteq (m, n) = (d)$, where $d = \gcd(m, n) \geq 0$; on the other hand we have a $\mathbb{Z}$-bilinear map $\mathbb{Z}/m \otimes_\mathbb{Z} \mathbb{Z}/n \to \mathbb{Z}/d$ given by $([a]_m, [b]_n) \mapsto [ab]_d$, which is easily seen to be surjective, hence we have a surjective, $\mathbb{Z}$-linear map $\mathbb{Z}/m\otimes_\mathbb{Z}\mathbb{Z}/n \to \mathbb{Z}/d$ by the universal property. This proves that $\mathbb{Z}/m\otimes_\mathbb{Z}\mathbb{Z}/n \cong \mathbb{Z}/d$.

Exercise 10.11. Generalising the previous example, let R be a ring and let I, J be ideals in R; prove that the map $R/I \times R/J \to R/I + J$ given by $([a]_I, [b]_J) \mapsto ([ab]_{I+J})$ is well-defined and R-bilinear. Prove that the induced R-linear map $R/I \otimes_R R/J \to R/I + J$ is an isomorphism of R-modules (first, show that the source is a cyclic R-module, generated by the element $[1]_I \otimes [1]_J$).

Proposition 10.12. *Let R be a ring, let $(M_i)_{i\in\mathcal{I}}$ be a family of R-modules and let N be an R-module. Then there is an isomorphism*

$$\bigoplus_{i\in\mathcal{I}} (M_i \otimes_R N) \cong \left(\bigoplus_{i\in\mathcal{I}} M_i\right) \otimes_R N.$$

Proof. Recall that, for a family $(M'_j)_{j\in\mathcal{J}}$, an R-linear map from the direct sum $M' \bigoplus_{j\in\mathcal{J}} M'_j$ to any R-module P is the same as a family of R-linear maps $M'_j \to P$, one for each $j \in \mathcal{J}$.
We can define an R-linear map $\phi\colon \bigoplus_{i\in\mathcal{I}}(M_i\otimes_R N) \to \left(\bigoplus_{i\in\mathcal{I}} M_i\right)\otimes_R N$ by declaring its restrictions $\phi_j\colon M_i\otimes_R N \to \left(\bigoplus_{i\in\mathcal{I}} M_i\right)\otimes_R N$ for all $j \in \mathcal{I}$: if $\iota_j\colon M_j \hookrightarrow \bigoplus_{i\in\mathcal{I}} M_i$ is the inclusion of the j^{th} direct summand, then we let $\phi_j = \iota_j \otimes_R \mathrm{Id}_N$, using Example 10.8.
We can also define an R-linear map $\psi\colon \left(\bigoplus_{i\in\mathcal{I}} M_i\right) \otimes_R N \to \bigoplus_{i\in\mathcal{I}}(M_i \otimes_R N)$ by declaring an R-bilinear map $\mu\colon \left(\bigoplus_{i\in\mathcal{I}} M_i\right) \times N \to \bigoplus_{i\in\mathcal{I}}(M_i \otimes_R N)$ as follows: for a finite linear combination $\sum_{i\in\mathcal{I}} m_i \in \left(\bigoplus_{i\in\mathcal{I}} M_i\right)$, with $m_i \in M_i$, and for $n \in N$, we set $\mu(\sum_{i\in\mathcal{I}} m_i, n) = \sum_{i\in\mathcal{I}} m_i \otimes n)$.
The two maps ϕ and ψ are R-linear and are inverse of each other, as can be checked by evaluating $\psi\circ\phi$ and $\phi\circ\psi$ on the generators of the R-modules $\bigoplus_{i\in\mathcal{I}}(M_i \otimes_R N)$ and $\left(\bigoplus_{i\in\mathcal{I}} M_i\right) \otimes_R N$, which are therefore isomorphic. □

Definition 10.13. Let R be a ring, $I \subseteq R$ an ideal and M an R-module; we denote by $IM \subseteq M$ the submodule generated by all elements $i \cdot m$ with $i \in I$ and $m \in M$.

Lemma 10.14. *In the setting of Definition 10.13 we have an isomorphism of R-modules $R/I \otimes_R M \cong M/IM$.*

Proof. The map $\mu\colon R/I \times M \to M/IM$ sending $([a]_I, m) \mapsto [am]_{IM}$ is well-defined and R-bilinear; it induces therefore an R-linear map $\phi\colon R/I \otimes_R M \to M/IM$. Conversely, we can define a map $M \to R/I \otimes M$ by sending $m \mapsto [1]_I \otimes m$: this map is also well-defined and R-linear, and moreover it vanishes on $IM \subseteq M$, as for $i \in I$ and $m \in M$ we have $im \mapsto [1]_I \otimes am = a[1]_I \otimes m = [a]_I \otimes m = [0]_I \otimes m = 0[1]_I \otimes m = 0$. We get therefore an induced R-linear map from the quotient $\psi\colon M/IM \to R/I \otimes_R M$. One can then check on generators that both composites $\psi\circ\phi$ and $\phi\circ\psi$ are the identity. □

Note that Lemma 10.14 specializes to Exercise 10.11 when $M = R/J$, as $R/I + J$ can be identified with $(R/I)/J(R/I)$.

Exercise 10.15. Let M, M', M'' be R-modules.

- Give a definition of *R-trilinear* map from $M \times M' \times M''$ to another R-module P, similar to Definition 10.4.
- Prove that the map $\bar{\mu}\colon M \times M' \times M'' \to (M \otimes_R M') \otimes_R M''$ sending $(m, m', m'') \mapsto (m \otimes m') \otimes m''$, and the map $\check{\mu}\colon M \times M' \times M'' \to M \otimes_R (M' \otimes_R M'')$ sending $(m, m', m'') \mapsto m \otimes (m' \otimes m'')$, are R-trilinear.
- Prove that both $\bar{\mu}$ and $\check{\mu}$ have the following universal property: given any R-trilinear map $\mu\colon M \times M' \times M'' \to P$, there is a unique $\bar{\theta}\colon (M \otimes_R M') \otimes_R M'' \to P$ such that $\mu = \bar{\theta}\circ\bar{\mu}$, and there is a unique $\check{\theta}\colon (M \otimes_R M') \otimes_R M'' \to P$ such that $\mu = \check{\theta}\circ\check{\mu}$.
- Deduce that the R-modules $(M \otimes_R M') \otimes_R M''$ and $M \otimes_R (M' \otimes_R M'')$ are canonically isomorphic.

Leveraging on the Exercise 10.15, one often writes $M \otimes_R M' \otimes M''$ for either $(M \otimes_R M') \otimes_R M''$ and $M \otimes_R (M' \otimes_R M'')$, or for any R-module receiving a universal R-trilinear map from $M \times M' \times M''$, in the spirit of Definition 10.7.

Exercise 10.16. Let R be a ring and let M, N be R-modules. For any R-module P, check that a map $\mu\colon M \times N \to P$ is R-bilinear if and only if the map $N \times M \to P$

sending $(n, m) \mapsto \mu(m, n)$ is R-bilinear. Deduce that there is an isomorphism $t\colon M \otimes_R N \cong N \otimes_R M$, sending $m \otimes n \mapsto n \otimes m$, by showing that these two R-modules have equivalent universal properties.

10.5. **Extension of scalars.** Recall from the beginning of Section 6 that given a ring homomorphism $f\colon R \to S$ and an S-module N, we can consider N as an R-module by restriction of scalars along f: we can write f_*N for this module. In fact this construction gives a functor $f_*\colon S\mathrm{Mod} \to R\mathrm{Mod}$. In this subsection we use the tensor product to transform an R-module into an S-module.
Let M be an R-module, and let $f\colon R \to S$ as above. Then S can be considered as an R-module, and we can form the tensor product $S \otimes_R M$, which a priori is an R-module. We can however define an S-module structure on $S \otimes_R M$ by setting $s \cdot (s' \otimes m) = (ss') \otimes m$: check that this is a good definition!
In the light of Exercise 10.15 one can also argue as follows: there is an R-trilinear map $S \times S \times M \to S \otimes_R M$ given by $(s, s', m) \mapsto ss' \otimes m$, and this induces an R-linear map $S \otimes_R S \otimes_R M \to S \otimes_R M$ which we can then precompose with the universal R-bilinear map $S \times (S \otimes_R M) \to S \otimes_R (S \otimes_R M)$, to obtain a multiplication by scalars in S for $S \otimes_R M$.

Definition 10.17. We denote by f^*M the S-module $S \otimes_R M$ obtained above.

We further observe that if $g\colon M \to M'$ is an R-linear map, then $\mathrm{Id}_S \otimes_R g\colon S \otimes_R M \to S \otimes_R M'$ is an S-linear map, since $s \cdot (s' \otimes m) = (ss' \otimes m)$ is sent to $ss \otimes g(m)$ which is precisely $s \cdot (s' \otimes g(m))$. We usually denote by $f^*(g)$ the map $\mathrm{Id}_S \otimes_R g$.

Exercise 10.18. Prove that there is a functor $f^*\colon R\mathrm{Mod} \to S\mathrm{Mod}$ sending $M \mapsto f^*M$ and $g \mapsto f^*(g)$, i.e. check that identities of R-modules are sent to identities of S-modules, and compositions of R-linear maps are sent to compositions of S-linear maps. You can see this as an application of Exercise 10.9.

Finally, observe that the R-module structure on $S \otimes_R M$ can be recovered from the S-module structure on $S \otimes_R M$ constructed above by restriction of scalars along f.
As a first application of Definition 10.17, we prove the following lemma, which is an analogue of Lemma 10.14 with R/I replaced by R_T.

Lemma 10.19. *Let R be a ring, let $T \subseteq R$ be a multiplicative subset, and M be an R-module. Then there is an isomorphism of R-modules $M_T \cong R_T \otimes_R M$, where we consider R_T as an R-module via the localisation map $\tau\colon R \to R_T$.*

Proof. The map $\mu\colon R_T \times M \to M_T$ sending $(\frac{a}{t}, m) \mapsto \frac{am}{t}$ is the composite of $\mathrm{Id}_{R_T} \times \gamma\colon R_T \times M \to R_T \times M_T$ and the scalar product multiplication $R_T \times M_T \to M_T$ (see Definition 6.5); in particular μ is well-defined and R-bilinear, so it induces an R-linear map $\phi\colon R_T \otimes_R M \to M_T$.
The map $M \to R_T \otimes_R M$ sending $m \mapsto \frac{1}{1} \otimes m$ is R-linear and has a T-local R-module as target: indeed, as explained above, the R-module structure on $R_T \otimes_R M$ extends to an R_T-module structure. Thus, by Exercise 6.7, there is an induced R-linear map $\psi\colon M_T \to R_T \otimes_R M$.
The maps ψ and ϕ are inverse of each other, as can be checked on generators. □

Exercise 10.20. Prove that if $f\colon M \to N$ is an R-linear map, then the two R-linear maps $\mathrm{Id}_{R_T} \otimes_R f$ and f_T correspond to each other along the identifications $R_T \otimes_R M \cong M_T$ and $R_T \otimes_R N \cong N_T$ considered in the proof of Lemma 10.19.

We conclude the subsection by the following observation. If $f\colon R \to S$ is a homomorphism of rings, and if N is an S-module and M and R-module, then given an S-linear map $g\colon S \otimes_R M \to N$ we can compose it with the R-linear map $M \to S \otimes_R M$ sending $m \mapsto 1 \otimes m$, obtaining an R-linear map $M \to S$. Viceversa, given an R-linear map $h\colon M \to N$, we can define an R-bilinear map $S \times M \to N$ by $(s, m) \mapsto s \cdot h(m)$, and check that the induced map $S \otimes_R M \to N$ is in fact S-linear. The two procedures are inverse of each other, and show that there is a natural bijection between S-linear maps $f^*M \to N$ and R-linear maps $M \to f_*N$.

10.6. **Tensor products of algebras.** We conclude the section by showing that the tensor product can give rise not only to new modules, but also to new rings. We first make an observation: if R is a ring and (S, ϕ) is an R-algebra, then in particular we can consider S as an R-module. The multiplication map $S \times S \to S$ is R-bilinear, so it gives rise to an R-linear map $\mu\colon S \otimes_R S \to S$. The fact that the product on S is commutative has the following consequence: if $T\colon S \otimes_R S \to S \otimes_R S$ is the map sending $s \otimes s' \mapsto s' \otimes s$, as in Exercise 10.16, then the following diagram of R-linear maps commutes

$$\begin{array}{ccc} S \otimes_R S, & \xrightarrow{t} & S \otimes_R S \\ & \searrow^{\mu} & \downarrow{\scriptstyle \mu} \\ & & S. \end{array}$$

Moreover the fact that the product in S is associative implies that the following diagram of R-linear maps commutes, where we use Exercise 10.15 to make sense of $S \otimes_R S \otimes_R S$

$$\begin{array}{ccc} S \otimes_R S \otimes_R S & \xrightarrow{\mathrm{Id}_S \otimes_R \mu} & S \otimes_R S \\ \downarrow{\scriptstyle \mu \otimes_R \mathrm{Id}_S} & & \downarrow{\scriptstyle \mu} \\ S \otimes_R S & \xrightarrow{\mu} & S. \end{array}$$

Finally, the fact that $\phi\colon R \to S$ is a ring homomorphism implies that ϕ is an R-linear map, and that the following diagram of R-linear maps commutes, where we identify $R \otimes_R S \cong S$ via $1 \otimes s \mapsto s$.

$$\begin{array}{ccc} R \otimes_R S & \xrightarrow{\phi \otimes_R \mathrm{Id}_S} & S \otimes_R S \\ & \searrow\!\!\searrow & \downarrow{\scriptstyle \mu} \\ & & S. \end{array}$$

Exercise 10.21. Give the opposite construction: given an R-module S with R-linear maps $\psi\colon R \to S$ and $\mu\colon S \otimes_R S \to S$ making all the above diagrams commute, construct a R-algebra structure on S.

Let now (S, ϕ, μ) and (S', ϕ', μ') be R-algebras, presented as in Exercise 10.21 Then the R-module $S \otimes_R S'$ can be given an R-algebra structure by considering

- the map $\phi''\colon R \to S \otimes_R S'$ given as the composite of the identification $R \cong R \otimes_R R$, sending $1 \mapsto 1 \otimes 1$, and $\psi \otimes_R \psi'$;
- the map $\mu''\colon S \otimes_R S' \otimes_R S \otimes_R S' \to S \otimes_R S'$ given as the composite of $\mathrm{Id}_S \otimes_R t \otimes_R \mathrm{Id}_{S'}$, with $t\colon S' \otimes_R S \to S \otimes_R S'$ as in Exercise 10.16, and $\mu \otimes_R \mu'$

In simple terms, the product on $S \otimes_R S'$ is defined on simple tensors by setting $(a \otimes b) \cdot (a' \otimes b') = aa' \otimes bb'$, and extended R-bilinearly; the ring homomorphism $\psi'' \colon R \to S \otimes_R S'$ is defined by $\psi''(a) = \psi(a) \otimes 1 = 1 \otimes \psi'(a)$.
We observe moreover that there is an R-algebra homomorphism $\iota \colon S \to S \otimes_R S'$ given by setting $\iota(a) = a \otimes 1$; similarly we have a homomorphism of R-algebras $\iota' \colon S' \to S \otimes_R S'$ sending $a' \mapsto 1 \otimes a'$; so $S \otimes_R S'$ is an example of an R-algebra receiving a map of R-algebras both from S and from S'. The following proposition characterises it as the "initial" example of such an R-algebra.

Proposition 10.22. *Let R be a ring, let S, S' and S'' be R-algebras, and let $f \colon S \to S''$ and $f' \colon S' \to S''$ be R-algebra homomorphisms. Then there is a unique homomorphism of R-algebras $\theta \colon S \otimes_R S' \to S''$ such that $f = \theta \circ \iota$ and $f' = \theta \circ \iota'$.*

Proof. The algebra $S \otimes_R S'$ is generated as an R-module by the elements $a \otimes a'$. Each such element can be factored as a product $(a \otimes 1) \cdot (1 \otimes a')$. Each element $a \otimes 1$ is in the image of ι, and each element $1 \otimes a'$ is in the image of ι': hence there can be at most one R-algebra homomorphism θ with the required properties.
In fact, one can define an R-bilinear map $S \times S' \to S''$ by sending $(a, a') \mapsto f(a) \cdot f'(a')$. The induced R-linear map $\theta \colon S \otimes_R S' \to S''$ is easily shown to be a ring homomorphism (hence a homomorphism of R-algebras). □

Example 10.23. Recall Example 10.2; then the algebra $R[x] \otimes_R R[y]$ can be identified with the polynomial algebra $R[x, y]$.
Recall Exercise 10.11; then the constructed bijection $R/I \otimes_R R/J \cong R/I + J$ is not only an isomorphism of R-modules, but also an isomorphism of R-algebras.

11. Flatness

Recall from 10.9 that given a ring R and two R-modules M and N, we have introduced a new R-module $M \otimes_R N$. In fact, if we fix M, we can consider $M \otimes_R -$ as a functor $R\mathrm{Mod} \to R\mathrm{Mod}$, sending $N \mapsto M \otimes_R N$ and sending an R-linear map $f \colon N \to N'$ to the R-linear map $\mathrm{Id}_M \otimes_R f \colon M \otimes_R N \to M \otimes_R N'$. As a particular case, discussed in Exercise 10.18, when $M = S$ is an R-algebra, then $S \otimes_R -$ can be regarded/upgraded to a functor $R\mathrm{Mod} \to S\mathrm{Mod}$.

11.1. **Additive and exact functors.** By Proposition 10.12, the functor $M \otimes_R -$ sends a direct sum $N \oplus N'$ of R-modules to the R-module $M \otimes_R (N \oplus N')$, which can be identified with the direct sum $M \otimes_R N \oplus M \otimes_R N'$. Similarly, for S an R-algebra, the functor $S \otimes_R - \colon R\mathrm{Mod} \to S\mathrm{Mod}$ sends the R-module $N \oplus N'$ to the direct sum of S-modules $S \otimes_R N \oplus S \otimes_R N'$.

Definition 11.1. Let R, S be two rings and let $F \colon R\mathrm{Mod} \to S\mathrm{Mod}$ be a functor. We say that F is additive if it sends finite direct sums to finite direct sums. More precisely: for every $M_1, M_2 \in R\mathrm{Mod}$ we have inclusions $\iota_1 \colon M_1 \to M_1 \oplus M_2$ and $\iota_2 \colon M_2 \to M_1 \oplus M_2$, and the requirement is that $F(\iota_1)$ and $F(\iota_2)$ are inclusions and exhibit $F(M_1 \oplus M_2)$ as the direct sum of $F(M_1)$ and $F(M_2)$.

Example 11.2. Let M, M' be R-modules. Recall that given two R-linear maps $f, g \colon M \to M'$, the pointwise sum $f + g \colon M \to M'$ is again an R-linear map. If F is any functor $F \colon R\mathrm{Mod} \to S\mathrm{Mod}$, then $F(f)$, $F(g)$ and $F(f + g)$ are three S-linear maps $F(M) \to F(M')$, however in general $F(f + g) \neq F(f) + F(g)$: for example consider the constant functor sending *every* R-module M to the S-module S, and

sending *every* R-linear map f to Id_S. Notice that this functor is not additive, as $S \oplus S \neq S$ (at least if S is not the zero ring...).
However, if $F\colon R\mathrm{Mod} \to S\mathrm{Mod}$ is additive, then indeed we have $F(f+g) = F(f) + F(g)$. To see this, first notice that, taking $M_1 = M$ and $M_2 = 0$ (the zero R-module) in Definition 11.1, we have that $\iota_1\colon M \to M \oplus 0$ is an isomorphism, hence $F(\iota_1)\colon F(M) \to F(M) \oplus F(0)$ must also be an isomorphism (a functor sends isomorphisms to isomorphisms), implying that $F(0) = 0$ is the zero S-module.
Second, we notice that there is a unique map $\nabla_M\colon M \oplus M \to M$ such that both composites $\nabla \circ \iota_1$ and $\nabla \circ \iota_2$ are equal to Id_M: in fact, ∇_M is the map sending each copy of M identically to M. If we apply F, we obtain that $F(\nabla)\colon F(M \oplus M) \to F(M)$ has the characterising property for being $\nabla_{F(M)}$, up to identifying $F(M \oplus M)$ with $F(M) \oplus F(M)$ as in Definition 11.1.
Finally, we can characterise $f + g\colon M \to M'$ as the unique map $h\colon M \to M'$ such that $h \circ \nabla \circ \iota_1 = f$ and $h \circ \nabla \circ \iota_2 = g$; applying F we obtain that $F(f+g)$ has the characterising property for being $F(f) + F(g)$.

The above discussion shows that for an R-module M the functor $M \otimes_R -\colon R\mathrm{Mod} \to R\mathrm{Mod}$ is additive. Similarly, for any R-algebra S, the functor $S \otimes_R -\colon R\mathrm{Mod} \to S\mathrm{Mod}$ is additive.
Among additive functors, thos that are easiest to work with are the *exact* ones, i.e. the functors that send short exact sequences to short exact sequences. In general the functor $M \otimes_R -$ is not exact, but it is always *right exact*, in the sense of the following definition.

Definition 11.3. Let R, S be rings and let $F\colon R\mathrm{Mod} \to S\mathrm{Mod}$ be an additive functor. We say that F is:

- *exact*, if whenever $0 \to M \overset{f}{\hookrightarrow} N \overset{g}{\twoheadrightarrow} P \to 0$ is a short exact sequence in $R\mathrm{Mod}$, then $0 \to F(M) \overset{F(f)}{\hookrightarrow} F(N) \overset{F(g)}{\twoheadrightarrow} F(P) \to 0$ is a short exact sequence in $S\mathrm{Mod}$;
- *right exact*, if whenever $M \overset{f}{\to} N \overset{g}{\twoheadrightarrow} P \to 0$ is exact in $R\mathrm{Mod}$, then $F(M) \overset{F(f)}{\to} F(N) \overset{F(g)}{\twoheadrightarrow} F(P) \to 0$ is exact in $S\mathrm{Mod}$;
- *left exact*, if whenever $0 \to M \overset{f}{\hookrightarrow} N \overset{g}{\to} P$ is exact in $R\mathrm{Mod}$, then $0 \to F(M) \overset{F(f)}{\hookrightarrow} F(N) \overset{F(g)}{\to} F(P)$ is exact in $S\mathrm{Mod}$.

Example 11.4. If R is a ring and $T \subseteq R$ is a multiplicative subset, then the functor $-_T\colon R\mathrm{Mod} \to R_T\mathrm{Mod}$ is exact, as proved in Proposition 6.9.
A much simpler example of an exact functor is the following: if $f\colon R \to S$ is a ring homomorphism, then by restriction of scalars we have a functor $f_*\colon S\mathrm{Mod} \to R\mathrm{Mod}$; now given a short exact sequence $0 \to M \overset{f}{\hookrightarrow} N \overset{g}{\twoheadrightarrow} P \to 0$ of R-module, the kernels and the images of the maps involved will not change if we consider M, N, P as R-modules: hence f_* is an exact functor.
In fact, given any additive functor $F\colon R\mathrm{Mod} \to S\mathrm{Mod}$, we can consider the functor $\eta_*\colon S\mathrm{Mod} \to \mathbb{Z}\mathrm{Mod}$ induced by the unique ring homomorphism $\eta\colon \mathbb{Z} \to S$; then F is exact if and only if $\eta_* \circ F$ is exact. This is because exactness of a sequence of S-modules and S-linear map is a property of the underlying sequence of abelian groups and abelian group homomorphisms.

Example 11.5. Let $R = \mathbb{Z}$ and consider the functor $\mathbb{Z}/2 \otimes_{\mathbb{Z}} -\colon \mathbb{Z}\mathrm{Mod} \to \mathbb{Z}\mathrm{Mod}$. Then the short exact sequence $0 \to \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{[-]_2} \mathbb{Z}/2 \to 0$ is sent along the functor to the sequence of $\mathbb{Z}$-modules and $\mathbb{Z}$-linear maps

$$0 \to \mathbb{Z}/2 \otimes_{\mathbb{Z}} \mathbb{Z} \xrightarrow{\mathrm{Id}_{\mathbb{Z}/2} \otimes_{\mathbb{Z}} (\cdot 2)} \mathbb{Z}/2 \otimes_{\mathbb{Z}} \mathbb{Z} \xrightarrow{\mathrm{Id}_{\mathbb{Z}/2} \otimes_{\mathbb{Z}} [-]_2} \mathbb{Z}/2 \otimes_{\mathbb{Z}} \mathbb{Z}/2 \to 0,$$

which can be identified (little exercise!) with the sequence

$$0 \to \mathbb{Z}/2 \xrightarrow{\cdot 0} \mathbb{Z}/2 \xrightarrow{\mathrm{Id}} \mathbb{Z}/2 \to 0.$$

Notice that in the previous sequence the composite of any two consecutive maps is zero: this is because $\mathbb{Z}/2 \otimes_{\mathbb{Z}} -$ is an additive functor (think of Example 11.2). Notice also that the last sequence is not exact: the map $\cdot 0$ has kernel equal to $\mathbb{Z}/2$, but the previous map $0 \to \mathbb{Z}/2$ has trivial image. However, exactness holds at the other two places where it can be checked, namely the middle and the right copy of $\mathbb{Z}/2$.

Lemma 11.6. *Let R be a ring and let M be an R-module. Then the functor $M \otimes_R -\colon R\mathrm{Mod} \to R\mathrm{Mod}$ is right exact.*

Proof. Let $N \xrightarrow{f} N' \xrightarrow{g} N'' \to 0$ be an exact sequence of R-modules and R-linear maps. We want to check that also the sequence

$$M \otimes_R N \xrightarrow{\mathrm{Id}_M \otimes_R f} M \otimes_R N' \xrightarrow{\mathrm{Id}_M \otimes_R g} M \otimes_R N'' \to 0$$

is exact; that is, it is exact at $M \otimes_R N''$ and at $M \otimes_R N'$.
For exactness at $M \otimes_R N''$ we need to check that $\mathrm{Id}_M \otimes_R g$ is a surjective map, and to do so it suffices to show that each generator $m \otimes n'' \in M \otimes_R N''$ is in the image of this map; by surjectivity of $g\colon N' \to N''$ we can find $n' \in N'$ with $g(n') = n''$, and thus $\mathrm{Id}_M \otimes_R g$ sends $m \otimes n' \mapsto m \otimes n''$ as desired.
The fact that $M \otimes_R -$ is an additive functor implies that $\mathrm{Im}(\mathrm{Id}_M \otimes_R f) \subseteq \ker(\mathrm{Id}_M \otimes_R g)$, as this inclusion is equivalent to the equality $(\mathrm{Id}_M \otimes_R g) \circ (\mathrm{Id}_M \otimes_R f) = 0$, and indeed $\mathrm{Id}_M \otimes_R (g \circ f) = 0$. To prove that $\mathrm{Im}(\mathrm{Id}_M \otimes_R f) = \ker(\mathrm{Id}_M \otimes_R g)$, we can equivalently prove that the map

$$\overline{\mathrm{Id}_M \otimes_R f}\colon M \otimes_R N'/\mathrm{Im}(\mathrm{Id}_M \otimes_R f) \to M \otimes_R N''$$

induced by $\mathrm{Id}_M \otimes_R g$ is in bijective (we already know it is surjective). We will do it by constructing an inverse map $\phi\colon M \otimes_R N'' \to M \otimes_R N'/\mathrm{Im}(\mathrm{Id}_M \otimes_R f)$. For this, we start with the R-bilinear map $\mu\colon M \times N' \to M \otimes_R N'/\mathrm{Im}(\mathrm{Id}_M \otimes_R f)$ obtained as the composite of the universal R-bilinear map $M \times N' \to M \otimes_R N'$ and the projection to the quotient (which is an R-linear map).
By construction, we have that $\mu(m, n') = 0$ whenever $n' \in \mathrm{Im}(f)$; this implies that μ factors as the composite of the map of sets $M \times N' \to M \times N'/\mathrm{Im}(f)$ and some R-bilinear map $\bar{\mu}\colon M \times N'/\mathrm{Im}(f) \to M \otimes_R N'/\mathrm{Im}(\mathrm{Id}_M \otimes_R f)$. Notice also that $N'/\mathrm{Im}(f) \cong N''$, so we can consider μ as an R-bilinear map $M \times N'' \to M \otimes_R N'/\mathrm{Im}(\mathrm{Id}_M \otimes_R f)$.
And now we apply the universal property *of* $M \otimes_R N''$, to obtain an R-linear map $\phi\colon M \otimes_R N'' \to M \otimes_R N'/\mathrm{Im}(\mathrm{Id}_M \otimes_R f)$. One readily checks that $\overline{\mathrm{Id}_M \otimes_R f}$ and ϕ are inverse of each other. □

11.2. **Flatness.** Even if there are examples as 11.5, one can still hope that for *some* R-modules M the functor $M \otimes_R -\colon R\mathrm{Mod} \to R\mathrm{Mod}$ is exact.

Example 11.7. The R-module R has the property that $R \otimes_R N \cong N$ in a *natural* way, by identifying $1 \otimes n$ with n. The word "natural" refers to the fact that along these identifications, an R-linear map $f\colon N \to N'$ corresponds precisely to the R-linear map $\mathrm{Id}_R \otimes_R f\colon R \otimes_R N \to R \otimes_R N'$, i.e. the following diagram commutes

$$\begin{array}{ccc} R \otimes_R N & \xrightarrow{\cong} & N \\ \downarrow{\scriptstyle \mathrm{Id}_R \otimes_R f} & & \downarrow{\scriptstyle f} \\ R \otimes_R N' & \xrightarrow{\cong} & N'. \end{array}$$

It follows that the entire functor $R \otimes_R -\colon R\mathrm{Mod} \to R\mathrm{Mod}$ can be identified with (one says, *is naturally isomorphic to*) the identity functor of RMod, which is definitely an exact functor. So $R \otimes_R -$ is an exact functor.
Proposition 6.9, together with Lemma 10.19, implies that for any multiplicative subset $T \subseteq R$ the functor $R_T \otimes_R -\colon R\mathrm{Mod} \to R_T\mathrm{Mod}$ is naturally isomorphic to the functor $-_T\colon R\mathrm{Mod} \to R_T\mathrm{Mod}$, which is an exact functor.

Definition 11.8. Let R be a ring and M be an R-module. We say that M is *flat* (over R) if the functor $M \otimes_R -\colon R\mathrm{Mod} \to R\mathrm{Mod}$ is exact.
An ring homomorphism $f\colon R \to S$ is flat if S, considered as an R-module, is flat.

Example 11.7 shows that R and R_T are flat R-modules; since the module structures come from ring homomorphism, we have that Id_R and $\tau\colon R \to R_T$ are flat ring homomorphisms.

Example 11.9. Observe that proposition 10.12, together with the fact that arbitrary direct sums of short exact sequences are short exact sequences, implies that if $(M_i)_{i\in\mathcal{I}}$ is a family of flat R-modules, then also the direct sum $\bigoplus_{i\in\mathcal{I}} M_i$ is flat. In particular, every module of the form $\bigoplus_{i\in\mathcal{I}} R$ (such a module is called a *free* R-module) is flat. And if R is a field, then every vector space is free, and hence flat.

Example 11.10. Let $f\colon R \to S$ be a ring homomorphism and let M be an S-module. If S is flat over S, the R-module f_*M obtained by restriction of scalars may not be flat. For example, consider the map of rings $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/2$: then every $\mathbb{Z}/2$-vector space is flat, but as we saw in Example 11.5 $\mathbb{Z}/2$ is not flat as a $\mathbb{Z}$-module. Similarly, if f_*M is flat over R, then M may not be flat over S. For example, consider the inclusion of rings $k \hookrightarrow k[x]$, where k is a field. Then the $k[x]$-module $k[x]/(x)$ is not flat over $k[x]$ (think of the short exact sequence $k[x] \xrightarrow{\cdot x} k[x] \twoheadrightarrow k[x]/(x)$ and prove this as an exercise!), but $k[x]/(x)$, as a k-vector space, is flat.

In general, every short exact sequence of R-modules arises from an injective R-linear map $f\colon N \to N'$ by defining $g\colon N' \to N'' := N'/N$ to be the projection to the quotient, and then considering $0 \to N' \xrightarrow{f} N' \xrightarrow{g} N'' \to 0$. Since for every R-module M the functor $M \otimes_R -$ sends the short exact sequence $0 \to N \to N' \to N'' \to 0$ to a sequence $0 \to M \otimes_R N \to M \otimes_R N' \to M \otimes_R N'' \to 0$ which is at least exact at $M \otimes_R N'$ and at $M \otimes_R N''$ (by Lemma 11.6), checking whether M is flat or not is equivalent to checking whether every injective R-linear map $f\colon N \to N'$ gives again rise to an injective R-linear map $\mathrm{Id}_M \otimes f\colon M \otimes_R N \to M \otimes_R N'$.

11.3. **Faithful flatness.** We observe that the zero R-module 0 is flat, as the zero functor $0\colon R\mathrm{Mod} \to R\mathrm{Mod}$ sends *any* sequence to an exact sequence. Now, as discussed in Subsection 6.3 when dealing with localisation, functors as $M \otimes_R -$ can help us transforming a problem about R-modules into a problem about simpler R-modules; exactness of $M \otimes_R -$ can be used to translate good hypotheses of the original problem into good hypotheses for the simplified version; but at some point we want to be able to *come back* to the original problem. In this respect, the zero functor is quite useless. In general, we would be happy if $M \otimes_R -$ *detects* differences and equalities between R-modules.

Definition 11.11. Let R be a ring and M be an R-module. We say that M is *faithfully flat* if M is flat and for every non-zero R-module N we have that $M \otimes_R N$ is also non-zero.
Given a ring homomorphism $f\colon R \to S$, we say that f is faithfully flat if S is faithfully flat as an R-module.

Example 11.12. Let k be a field; then every non-zero vector space V is faithfully flat: indeed if $V \cong \bigoplus_{i\in\mathcal{I}} k$, for a non-empty set $\mathcal{I}$, then for each other vector space $W \neq 0$ we have $V \otimes_k W \cong \bigoplus_{i\in\mathcal{I}} W$, using Proposition 10.12, and the last direct sum is again a non-trivial vector space.
In general, if R is a ring and M is a non-zero, free R-module, then M is faithfully flat. This implies for instance that if $S = R[x_1, \dots, x_n]$, then S is a free R-module, with basis given by the monomials, and thus the inclusion of rings $R \hookrightarrow S$ is a faithfully flat ring homomorphism.

Example 11.13. Let R be a ring; then the module $M = \bigoplus_{\mathfrak{m}} R_{\mathfrak{m}}$, where the direct sum is taken over all maximal ideals of R, is faithfully flat: this is a direct consequence of Proposition 6.10.

Example 11.14. In general not every flat module is faithfully flat. For instance, observe that $\mathbb{Q}$ is a flat $\mathbb{Z}$-module (it is the localisation of $\mathbb{Z}$ at the prime ideal (0)), but it is not faithfully flat. To show this, we claim that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n = 0$ for all $n \geq 2$: indeed any generator $\frac{a}{b} \otimes [c]_n$ can be identified with zero via

$$\frac{a}{b} \otimes [c]_n = n \cdot \frac{a}{nb} \otimes [c]_n = \frac{a}{nb} \otimes (n \cdot [c]_n) = \frac{a}{nb} \otimes [0]_n = 0.$$

Exercise 11.15. Let R be a ring and assume that there are at least two distinct maximal ideals $\mathfrak{m}, \mathfrak{m}'$. Prove that $R_{\mathfrak{m}}$ is not faithfully flat, though it is flat. (Hint: think of $R/\mathfrak{m}'$.)

The following proposition gives a characterisation of faithfully flat modules.

Proposition 11.16. *Let R be a ring and M be a flat R-module. Then the following are equivalent:*

1. *M is faithfully flat in the sense of Definition 11.11;*
2. *for all non-zero R-linear maps $f\colon N \to N'$, also $\mathrm{Id}_M \otimes_R f\colon M \otimes_R N \to M \otimes_R N'$ is non-zero;*
3. *for all sequences $N \xrightarrow{f} N' \xrightarrow{g} N''$ of three R-modules and two R-linear maps, if $M \otimes_R N \xrightarrow{\mathrm{Id}_M \otimes_R f} M \otimes_R N' \xrightarrow{\mathrm{Id}_M \otimes_R g} M \otimes_R N''$ is exact at $M \otimes_R N'$, then also $N \xrightarrow{f} N' \xrightarrow{g} N''$ is exact at N';*
4. *for every maximal ideal $\mathfrak{m} \subset R$ we have $\mathfrak{m}M \neq M$.*

Proof. (**1**) ⇒ (**2**). Let $f\colon N \to N'$ be a non-zero R-linear map. Then we can factor f as a composition of a surjection $s\colon N \twoheadrightarrow \mathrm{Im}(f)$ and an injection $i\colon \mathrm{Im}(f) \hookrightarrow N$. We have that $\mathrm{Id}_M \otimes_R s\colon M \otimes_R N \to M \otimes_R \mathrm{Im}(f)$ is surjective by Lemma 11.6, and since M is flat we also have that $\mathrm{Id}_M \otimes_R i$ is injective. Finally, the assumption on f tells us that $\mathrm{Im}(f)$ is a non-zero R-module, and since M is assumed faithfully flat we obtain that also $M \otimes_R \mathrm{Im}(f)$ is non-zero; it follows that $\mathrm{Id}_M \otimes_R f$ is a non-zero map, as its image contains the image of $M \otimes_R \mathrm{Im}(f)$ along $\mathrm{Id}(M) \otimes_R i$.

(**2**) ⇒ (**3**). The composition $g \circ f$ is the zero map, as witnessed by the fact that the composition $\mathrm{Id}_M \otimes_R (g \circ f) = (\mathrm{Id}_M \circ_R g) \circ (\mathrm{Id}_M \otimes_R f)$ is the zero map. Moreover, using that M is flat, we obtain that the exact sequence $N \xrightarrow{f} N' \xrightarrow{\pi} N'/\mathrm{Im}(f) \to 0$ gives rise to an exact sequence $M \otimes_R N \xrightarrow{\mathrm{Id}_M \otimes_R f} M \otimes_R N' \xrightarrow{\mathrm{Id}_M \otimes_R \pi} M \otimes_R (N'/\mathrm{Im}(f)) \to 0$; so we can identify $M \otimes_R (N'/\mathrm{Im}(f))$ with the quotient $M \otimes_R N'/\mathrm{Im}(\mathrm{Id}_M \otimes_R f)$. Similarly, the exact sequence $0 \to \ker(g) \xhookrightarrow{\iota} N' \xrightarrow{g} N''$ leads to the exact sequence $0 \to M \otimes_R \ker(g) \xhookrightarrow{\mathrm{Id}_M \otimes_R \iota} M \otimes_R N' \xrightarrow{\mathrm{Id}_M \otimes_R g} M \otimes_R N''$, and therefore we can identify $M \otimes_R \ker(g)$ with $\ker(\mathrm{Id}_M \otimes_R g)$. By hypothesis we have $\ker(\mathrm{Id}_M \otimes_R g) = \mathrm{Im}(\mathrm{Id}_M \otimes_R f)$ as submodules of $M \otimes_R N'$; using the previous identifications, we obtain that the composite map

$$M \otimes_R \ker(g) \xrightarrow{\mathrm{Id}_M \otimes_R \iota} M \otimes_R N' \xrightarrow{\mathrm{Id}_M \otimes_R \pi} M \otimes_R (N'/\mathrm{Im}(f))$$

can be identified with the composite map, which obviously vanishes

$$\ker(\mathrm{Id}_M \otimes_R g) = \mathrm{Im}(\mathrm{Id}_M \otimes_R f) \hookrightarrow M \otimes_R N' \twoheadrightarrow M \otimes_R N'/\mathrm{Im}(\mathrm{Id}_M \otimes_R f).$$

This shows that $\mathrm{Id}_M \otimes_R (\pi \circ \iota)$ is zero, and by assumption this implies that $\pi \circ \iota\colon \ker(g) \to N'/\mathrm{Im}(f)$ is zero as well.

(**3**) ⇒ (**4**). Let $\mathfrak{m} \subset R$ be a maximal ideal, and denote by $i\colon \mathfrak{m} \to R$ the inclusion, which is injective but not surjective. Then the sequence $\mathfrak{m} \xrightarrow{i} R \to 0$ is not exact at R, so after tensoring with M we must get a non-exact sequence $M \otimes_R \mathfrak{m} \xrightarrow{\mathrm{Id}_M \otimes_R i} M \otimes_R R \to 0$. After identifying $M \otimes_R R \cong M$ in the usual way, the image of $\mathrm{Id}_M \otimes_R i$ is generated by the elements $am \in M$ with $a \in \mathfrak{m}$ and $m \in M$; in other words, the image corresponds to the submodule $\mathfrak{m}M \subseteq M$, and by non-exactness we must have $\mathfrak{m}M \neq M$.

(**4**) ⇒ (**1**). Let N be a non-zero R-module, and let $n \in N$ be a non-zero element. Then the injective map $\mathrm{Span}_R(n) \hookrightarrow N$ given by the inclusion is sent after tensoring with the flat R-module M to an injective map $M \otimes_R \mathrm{Span}_R(n) \hookrightarrow M \otimes_R N$, so if we prove that $M \otimes_R \mathrm{Span}_R(n) \neq 0$ we also have that $M \otimes_R N \neq 0$, as desired. The module $\mathrm{Span}_R(n)$ is cyclic, so for some ideal $I \subseteq R$ we have $\mathrm{Span}_R(n) \cong R/I$; moreover, if $\mathfrak{m}$ is a maximal ideal containing I, we have a surjection $\mathrm{Span}_R(n) \cong R/I \twoheadrightarrow R/\mathfrak{m}$, which after tensoring with M becomes a surjection $M \otimes_R \mathrm{Span}_R(n) \twoheadrightarrow M \otimes_R R/\mathfrak{m}$, so it suffices to prove that $M \otimes_R R/\mathfrak{m}$ is non-zero. Using again that M is flat, we have that the short exact sequence $0 \to \mathfrak{m} \to R \to R/\mathfrak{m} \to 0$ gives rise to a short exact sequence $0 \to M \otimes_R \mathfrak{m} \to M \otimes_R R \to M \otimes_R R/\mathfrak{m} \to 0$; the image of the injective map $M \otimes_R \mathfrak{m} \to M \otimes_R R$ is the submodule $\mathfrak{m}M \subseteq M$ if we identify $M \otimes_R R \cong M$ as usual. By hypothesis, this is not the entire M, so by exactness we have $M \otimes_R R/\mathfrak{m} \neq 0$ as desired. □

12. Flatness and localisations

Let R be a ring, let M be an R-module and let $T \subseteq R$ be a multiplicative subset. By Lemma 10.19 the R-module M_T can be identified with the tensor product $M \otimes_R R_T$, and an application of exercise 10.15 is that the functor $(M \otimes_R R_T) \otimes_R - \colon R\mathrm{Mod} \to R\mathrm{Mod}$ can be identified with the composite functor $(M \otimes_R -) \circ (R_T \otimes_R -)$; if M is flat over R, then both functors in the composition preserve exact sequences, hence the composite does: this shows that if M is a flat R-module, then M_T is also a flat R-module.

Exercise 12.1. More generally, prove that if M, M' are flat R-modules, then $M \otimes_R M'$ is also a flat R-module; and if M, M' are faithfully flat R-modules, then $M \otimes_R M'$ is also a faithfully flat R-module.

As observed in Example 11.14, $\mathbb{Q} = \mathbb{Z}_{(0)}$ is flat but not faithfully flat as a $\mathbb{Z}$-module, even if it is a localisation of $\mathbb{Z}$ which is faithfully flat as a $\mathbb{Z}$-module. So in general, even if M is faithfully flat *over* R, M_T may only be flat *over* R.

12.1. Tensor product "commutes" with localisation.

Lemma 12.2. *Let R be a ring, let $T \subseteq R$ be a multiplicative subset, let M, M', P be R_T-modules and let $\mu \colon M \times M' \to P$ be a map of sets; then μ is R-bilinear if and only if it is R_T-bilinear.*

Proof. If μ is R_T-bilinear, then it is also R-bilinear: this is an instance of the more general fact that if $f \colon R \to S$ is a ring homomorphism and $\mu \colon M \times M' \to P$ is an S-bilinear map, with M, M', P being S-modules, then the same map μ, considered as a map $f_*M \times f_*M' \to f_*P$, is R-bilinear.
Viceversa, suppose that μ is R-bilinear. We have to check that for $\frac{a}{t} \in R_T$, for $m \in M$ and for $m' \in M'$ we have in P the equality $\mu(\frac{a}{t}m, m') = \mu(m, \frac{a}{t}m') = \frac{a}{t}\mu(m, m')$. Since multiplication by t is invertible, it suffices to check in P the equality $t\mu(\frac{a}{t}m, m') = t\mu(m, \frac{a}{t}m') = a\mu(m, m')$; and now we can use that μ is R-bilinear and replace $t\mu(\frac{a}{t}m, m') = \mu(t\frac{a}{t}m, m')$ and $t\mu(m, \frac{a}{t}m') = \mu(m, t\frac{a}{t}m')$, thus reducing ourselves to checking that $\mu(am, m') = \mu(m, am') = a\mu(m, m')$, which again is true because μ is R-bilinear. □

Lemma 12.3. *Let R be a ring, $T \subseteq R$ a multiplicative subset, and let M, N be R-modules. If either M or N (or both) are T-local, then also $M \otimes_R N$ is T-local*

Proof. Suppose that M is T-local; then for $t \in T$ the map $t \cdot - \colon M \to M$ is an R-linear isomorphism. Since $- \otimes_R N$ is a functor, it follows that $(t \cdot -) \otimes_R \mathrm{Id}_N \colon M \otimes_R N \to M \otimes_R N$ is also an isomorphism, and the latter map can be identified with $t \cdot - \colon M \otimes_R N \to M \otimes_R N$. □

A straightforward corollary of Lemmas 12.2 and 12.3 is the following.

Corollary 12.4. *Let R be a ring, $T \subseteq R$ a multiplicative subset, and M, M' be R_T-modules; then there is an isomorphism of T-local R-modules $M \otimes_R M' \cong M \otimes_{R_T} M'$.*

Proof. We check that $M \otimes_R M'$ satisfies the universal property characterising $M \otimes_{R_T} M'$. First, by Lemma 12.3 we have that $M \otimes_R M'$ is T-local, so we can consider it as an R_T-module; moreover $\mu^R_\otimes \colon M \times M' \to M \otimes_R M'$ is R-bilinear, so by Lemma 12.2 it is also R_T-bilinear.

Let now $\mu\colon M \times M' \to P$ be an R_T-bilinear map, with P some R_T-module. Then μ is also R-bilinear by Lemma 12.2, so by the universal property of $M \otimes_R N$ there is a unique R-linear map $\theta\colon M \otimes_R N \to P$ such that $\theta \circ \mu^R_\otimes = \mu$; the map θ is an R-linear map between R_T-modules, so it is R_T-linear. □

Proposition 12.5. *Let R be a ring, $T \subseteq R$ a multiplicative subset and M be an R-module. Then for any R_T-module N there is a natural isomorphism of R-modules $M \otimes_R N \cong M_T \otimes_R N \cong M_T \otimes_{R_T} N$. In particular:*

(1) If M is flat over R, then M_T is flat over R_T;
(2) If M is faithfully flat over R, then M_T is faithfully flat over R_T;

Proof. The isomorphism $M_T \otimes_R N \cong M_T \otimes_{R_T} N$ follows from Corollary 12.4. For the first isomorphism, observe that the map $M \times N \to M_T \otimes_{R_T} N$ sending $(m, n) \mapsto \frac{m}{1} \otimes n$ is R-bilinear, so it gives rise to an R-linear map $\phi\colon M \otimes_R N \to M_T \otimes_{R_T} N$. Viceversa, the map $M_T \times N \to M \otimes_R N$ sending $(\frac{m}{t}, n) \mapsto m \otimes \frac{1}{t} \cdot n$ is R-linear, so it induces an R-linear map $\psi\colon M_T \otimes_R N \to M \otimes_R N$. One can check on generators that ϕ and ψ are inverse isomorphisms.
By Lemma 12.3, we can consider $M \otimes_R -$, $M_T \otimes_R -$ and $M_T \otimes_{R_T} -$ as functors $R_T\mathrm{Mod} \to R_T\mathrm{Mod}$, and the previous argument, which is natural in N, shows that these functors are isomorphic to each other; in particular, if the first functor is exact, so is the third. If M is flat over R, then the functor $M \otimes_R -\colon R_T\mathrm{Mod} \to R_T\mathrm{Mod}$ can be regarded as the restriction of $M \otimes_R -\colon R\mathrm{Mod} \to R\mathrm{Mod}$ to the subcategory of RMod consisting of all T-local R-modules and all R-linear maps between them. This concludes the proof of (1).
If M is moreover faithfully flat over R, then for any non-zero R_T-module N (which is in particular a non-zero R-module) we have that $M \otimes_R N$ is also non-zero; the above isomorphism then tells us that also $M_T \otimes_{R_T} N$ is non-zero, and this proves (2). □

12.2. **Characterisation of faithfully flat ring homomorphisms.** The previous discussion can be applied to prove the following theorem, characterising faithfully flat homomorphisms of rings among the flat ones.

Theorem 12.6. *Let $\phi\colon R \to S$ be a flat homomorphism of rings. Then the following are equivalent:*

(1) ϕ is faithfully flat, in the sense of Definition 11.11;
(2) every maximal ideal $\mathfrak{m} \subset R$ is of the form $\phi^{-1}(\mathfrak{n})$ for some maximal ideal $\mathfrak{n} \subset S$;
(3) the map $\mathrm{Spec}(\phi)\colon \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is surjective.

Proof. (**1**) ⇒ (**3**). Let $\mathfrak{p} \in \mathrm{Spec}(R)$ be a prime ideal, and let $T := R \setminus \mathfrak{p}$. The T-localisation of S as an R-module can be identified with the localisation of S at the multiplicative subset $\phi(T) \subseteq S$, and we get a ring homomorphism $\phi_T\colon R_T \to S_T := S_{\phi(T)}$. Since we assume that ϕ is faithfully flat, we have by Proposition 12.5 that also the ring homomorphism ϕ_T is faithfully flat. Consider now the unique maximal ideal $\mathfrak{m} \subset R_T$ (which is the extension of $\mathfrak{p}$ along the localisation map $R \to R_T$). Then by Proposition 11.16 we have that $\mathfrak{m}S_T \neq S_T$, as S_T is a faithfully flat R_T-module; we can in fact identify $\mathfrak{m}S_T$ with the ideal $\mathfrak{m}^e := (\phi_T(\mathfrak{m})) \subset S_T$, i.e. the extension along ϕ_T of $\mathfrak{m}$. It follows that, since $\mathfrak{m}^e \subset S_T$ is a proper ideal, it is contained in some maximal ideal $\mathfrak{n} \subset S_T$; the contraction $\mathfrak{n}^c := \phi^{-1}(\mathfrak{n})$ is a prime ideal of R_T containing $\mathfrak{m}$, and since $\mathfrak{m}$ is maximal it must be the entire $\mathfrak{m}$.

The contraction of $\mathfrak{n}$ along the localisation map $S \to S_T$ is some prime ideal $\mathfrak{q} \subset S$, whose contraction along ϕ must be $\mathfrak{p}$.

(**3**) $\Rightarrow$ (**2**). If $\mathrm{Spec}(\phi)$ is surjective, in particular for every maximal ideal $\mathfrak{m} \subset R$ there is a prime ideal $\mathfrak{q} \subset S$ such that $\phi^{-1}(S) = \mathfrak{m}$. We can extend $\mathfrak{q}$ to a maximal ideal $\mathfrak{n} \subset S$; the contraction $\phi^{-1}(S)$ is a prime ideal of R that contains $\mathfrak{m}$, so it has to be $\mathfrak{m}$.

(**2**) $\Rightarrow$ (**1**). Using Proposition 11.16, we have to prove that for each maximal ideal $\mathfrak{m} \subset R$ the sub-R-module $\mathfrak{m}S$ is different from the entire S. If $\mathfrak{n} \subset S$ is a maximal ideal such that $\phi^{-1}(\mathfrak{n}) = \mathfrak{m}$, we have that $\mathfrak{m}S \subseteq \mathfrak{n}$, and thus $\mathfrak{m}S \neq S$. □

Example 12.7. In general a ring homomorphism $\phi\colon R \to S$ inducing a surjective map $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ need not be flat. For instance, consider the ring homomorphism $k[x]/(x^2) \twoheadrightarrow k[x]/(x) \cong k$, for k a field: it induces a bijection between spectra (both consisting of a single point), but $k[x]/(x)$ is not a flat $k[x]/(x^2)$-module, as for instance the $k[x]/(x^2)$-linear map $k[x]/(x) \to k[x]/(x^2)$ sending $[1]_x \mapsto [x]_{x^2}$ is injective, yet after tensoring with $k[x]/(x)$ over $k[x]/(x^2)$ we obtain a map that can be identified with the zero map $k[x]/(x) \xrightarrow{0} k[x]/(x)$, in particular a non-injective map.

We conclude by reading Example 11.14 in the light of Theorem 12.6: the ring homomorphism $\mathbb{Z} \to \mathbb{Q}$ makes $\mathbb{Q}$ into a flat $\mathbb{Z}$-module; however the induced map $\mathrm{Spec}(\mathbb{Q}) \to \mathrm{Spec}(\mathbb{Z})$ is not surjective, as $\mathrm{Spec}(\mathbb{Q})$ consists of a single point, hitting the point $(0) \in \mathrm{Spec}(\mathbb{Z})$, and every other point $(p) \in \mathrm{Spec}(\mathbb{Z})$ is not in the image.

12.3. **Detecting flatness.** Proposition 12.5 tells us that flatness is preserved after localisation: if M is a flat R-module, then for any multiplicative subset $T \subseteq R$ we have that M_T is a flat R_T-module (it is also a flat R-module, and proving this is an application of Exercise 12.1). We are now interested in the converse statement: if enough localisations M_T of an R-module M are flat, can we conclude that M is flat (over R)? In asking that M_T is flat "for enough T", we have a priori to specify whether we want M_T to be flat over R or over R_T. Fortunately these two requirements are equivalent, as the following corollary of Proposition 12.5 shows.

Corollary 12.8. *Let R be a ring, $T \subseteq R$ a multiplicative subset and N an R_T-module. Then N is flat over R if and only if it is flat over R_T.*

Proof. If N is flat over R, then $N \cong N_T$ is flat over R_T by Proposition 12.5. Viceversa, if N is flat over R_T, then again by Proposition 12.5 the functor $- \otimes_R N$ can be regarded as the composite functor $(-)_T \otimes_{R_T} N$, so it is a composition of exact functors and hence exact. □

In the spirit of Proposition 6.10, we would like a statement of the form "an R-module is flat if and only if each localisation $R_\mathfrak{m}$ at a maximal ideal is flat". The following proposition generalises a bit this statement.

Proposition 12.9. *Let $\phi\colon R \to S$ be a ring homomorphism and let M be an S-module. Then the following statements are equivalent.*

1. *The R-module $\phi_* M$ is flat.*
2. *For every maximal ideal $\mathfrak{n} \subset S$, the R-module $\phi_*(M_\mathfrak{n})$ is flat.*

We observe that condition (2) in Proposition 12.9 can be rephrased as follows, thanks to Corollary 12.4: for every maximal ideal $\mathfrak{n} \subset S$, denoting $\mathfrak{p} = \phi^{-1}(\mathfrak{n}) \in$

$\mathrm{Spec}(R)$, we have that the R-module $\phi_*(M_\mathfrak{n})$ is $R \setminus \mathfrak{m}$-local, so we can consider it as a $R_\mathfrak{p}$-module; we can then ask that $\phi_*(M_\mathfrak{n})$ be flat over $R_\mathfrak{p}$.
We also observe that, taking $R = S$ and $\phi = \mathrm{Id}_R$, Proposition 12.9 tells us that an R-module M is flat if and only $R_\mathfrak{m}$ is flat for every maximal ideal $\mathfrak{m} \subset R$.
To prove Proposition 12.9 it is convenient to consider triple tensor products of the form $N \otimes_R M \otimes_S P$, where N is an R-module and M, P are S-modules (so M is also an R-module, as it is identified with f_*M). The following exercise makes this idea precise.

Exercise 12.10. Let $\phi\colon R \to S$ be a ring homomorphism and let M be an S-module. For an R-module N, consider the tensor product $N \otimes_R \phi_*M$: for every $a \in S$, the map $s \cdot -\colon M = \phi_*M \to M = \phi_*M$ is R-linear, so it induces an R-linear map $\mathrm{Id}_N \otimes_R (s \cdot -)\colon N \otimes_R \phi_*M \to N \otimes_R \phi_*M$.

- Prove that the maps $\mathrm{Id}_N \otimes_R (s \cdot -)$, for varying $s \in S$, assemble into an S-module structure on $N \otimes_R \phi_*M$.
- Prove that if $f\colon M \to M'$ is an S-linear map, then the map $\mathrm{Id}_N \otimes_R f$ (constructed using that f is also R-linear $\phi_*RM \to \phi_*M'$) is S-linear.
- Prove that $N \otimes_R \phi_*(-)$ can be made into a functor $S\mathrm{Mod} \to S\mathrm{Mod}$.
- Prove that in fact the entire construction is also natural in N: if $g\colon N \to N'$ is an R-linear map and $f\colon M \to M'$ is S-linear, we get that $g \otimes_R f\colon N \otimes_R \phi_*M \to N' \otimes_R \phi_*M'$ is S-linear. So we really get a functor $- \otimes_R \phi_*(-)\colon R\mathrm{Mod} \boxtimes S\mathrm{Mod} \to S\mathrm{Mod}$. We often leave ϕ_* implicit and just write $- \otimes_R -$ for this functor.
- Prove that if M and P are two S-modules and N is an R-module, there is a "natural" isomorphism of S-modules between $N \otimes_R (M \otimes_S P)$ and $(N \otimes_R M) \otimes_S P$; that is, prove that the two functors $- \otimes_R (- \otimes_S -)$ and $(- \otimes_R -) \otimes_S -$, from $R\mathrm{Mod} \boxtimes S\mathrm{Mod} \boxtimes S\mathrm{Mod}$ to $S\mathrm{Mod}$, are naturally isomorphic.

Proof of Proposition 12.9. (**1**) $\Rightarrow$ (**2**). Let $\mathfrak{n}$ be a maximal ideal in S. We can identify $M_\mathfrak{n}$ with the tensor product $M \otimes_S S_\mathfrak{n}$. By Exercise 12.10 we can express the functor $- \otimes_R M_\mathfrak{n}$ as $(- \otimes_R M) \otimes_S S_\mathfrak{n}$, that is, as the composition of the two functors $- \otimes_R M\colon R\mathrm{Mod} \to S\mathrm{Mod}$, and $- \otimes_S S_\mathfrak{n}\colon S\mathrm{Mod} \to S\mathrm{Mod}$. The first functor is exact by hypothesis on M (here we use that exactness is a property of a sequence of modules that can be checked on the underlying sequence of abelian groups); the second is exact by Example 11.7.

(**2**) $\Rightarrow$ (**1**). Let $i\colon N \hookrightarrow N'$ be an injective R-linear map. By Exercise 12.10, the induced map $i \otimes_R \mathrm{Id}_M$ is an *S-linear* map between the *S-modules* $N \otimes_R M \to N' \otimes_R M$; if $i \otimes_R \mathrm{Id}_M$ is not injective, by Corollary 6.11 there is some maximal ideal $\mathfrak{n} \subset S$ such that $(i \otimes_R \mathrm{Id}_M)_\mathfrak{n}\colon (N \otimes_R M)_f n \to (N' \otimes_R M)_\mathfrak{n}$ is not injective. We can now rewrite the previous map as $i \otimes_R \mathrm{Id}_M \otimes_S \mathrm{Id}_{S_\mathfrak{n}}\colon N \otimes_R M \otimes_S S_\mathfrak{n} \to N' \otimes_R M \otimes_S S_\mathfrak{n}$, and finally as $i \otimes_{\mathrm{Id}_{M_\mathfrak{n}}}\colon N \otimes_R M_\mathfrak{n} \to N' \otimes_R M_\mathfrak{n}$; the non-injectivity of the last map contradicts the assumption that $M_\mathfrak{n}$ be a flat R-module. □

Exercise 12.11. Generalise the statements (1) and (2) in Proposition 12.5 to the following setting. Let $\phi\colon R \to S$ be a ring homomorphism, making S into an R-algebra. Let M be an R-module. Prove the following:

- if M is flat over R, then $\phi^*M = S \otimes_R M$ is flat over S;
- if M is faithfully flat over R, then $\phi^*M = S \otimes_R M$ is faithfully flat over S.

In doing this, Exercise 12.10 may be useful.

13. Integral dependence

In school we have learnt that not all real numbers are rational. In fact, the prompt to enlarge rational numbers to real numbers comes usually from geometric situations in which one wants to measure an actual length, but there is not suitable rational number for that. The first example of an "irrational" number one encounters is usually something like $\sqrt{2}$, expressing the length of the diagonal of a square of side length 1; the second famous example is π, expressing half of the length of a circle of radius 1. One also learns that $\sqrt{2}$, though irrational, satisfies the equality $\sqrt{2}^2 - 2 = 0$; that is, the polynomial $t^2 - 2 \in \mathbb{Z}[x]$ is such that, when evaluated at $t = \sqrt{2}$, vanishes. One learns also that there is no such polynomial for π, not even if one looks for it inside $\mathbb{Q}[t]$. The invention of complex numbers, generalising real numbers, follows a similar pattern as introducing $\sqrt{2}$, thus extending $\mathbb{Q}$: there is no real number i such that $i^2 + 1 = 0$, so one just invents it! In a certain sense, both complex numbers $\sqrt{2}$ and i are more close to being rational than π: even if they are not rational, they at least satisfy a polynomial equation with coefficients in $\mathbb{Q}$.

13.1. **Definition of integral (and algebraic) dependence.** We want to study general situations in which we have a ring homomorphism $f\colon R \to S$ (in the examples above, it was an inclusion like $\mathbb{Q} \hookrightarrow \mathbb{C}$), and we want to distinguish elements of S satisfying some polynomial equation "with coefficients in R": more precisely, we will consider those polynomials in $S[t]$ in the image of the ring homomorphism $F\colon R[t] \to S[t]$ induced by f, and ask which elements of s are sent to zero by the function $S \to S$ induced by one such polynomial.

Notation 13.1. Given a ring homomorphism $f\colon R \to S$, by abuse of notation we will often denote by f also the ring homomorphism $f \otimes_R \mathrm{Id}_{R[t]}\colon R[t] = R \otimes_R R[t] \to S[t] \cong S \otimes_R R[t]$, i.e. the induced ring homomorphism between polynomial rings. By even bigger abuse of notation, whenever f is injective we will just consider R as a subring of S and thus consider $R[t]$ as a subring of $S[t]$.

Definition 13.2. Let $f\colon R \to S$ be a ring homomorphism, and consider thus S as an R-algebra. Let $b \in S$. We say that:

- b is *algebraic*, or *algebraic dependent* over R if there is a non-zero polynomial $P \in R[t]$ such that $f(P)_*(a) = 0 \in S$;
- b is *integral*, or *integral dependent* over R if there is a *monic* polynomial $P \in R[t]$ such that $f(P)_*(a) = 0 \in S$.

In the previous definition, recall that a polynomial $P \in R[t]$ is *monic* if $\mathrm{lc}(P) = 1$, as in Definition 7.13; concretely, we have $P = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$ for some $n \geq 0$ and some $a_0, \ldots, a_{n-1} \in R$. Apart when coefficients are in the zero ring, monic polynomials are non-zero, so that being integral implies being algebraic.
In the light of 13.2, $\sqrt{2}$ and i are integral over $\mathbb{Z}$ whereas π is not. At first glance, the notion of algebraic dependence looks both more genuine and more general than that of integral dependence, but the following two examples will motivate our focus on the latter notion in the entire section.

Example 13.3. Let k is a field and let S be a non-zero k-algebra, so we can regard k as a subring of S; then an element $b \in S$ is algebraic over k if and only if b is

also integral over k: indeed if $P \in k[t]$ is non-zero and such that $P_*(b) = 0$, then $P/\mathrm{lc}(P)$ is monic and still satisfies $(P/\mathrm{lc}(P))_*(P) = 0$.
More generally, if $f\colon R \to S$ is a ring homomorphism and $b \in S$ is algebraic over R, with witnessing polynomial $P \in R[t]$, then at least the element $\frac{b}{1}$ in the localisation $S_{\mathrm{lc}(P)}$ is integral over R, as witnessed by the monic polynomial $\frac{P}{\mathrm{lc}(P)} \in S_{\mathrm{lc}(P)}[t]$.

Example 13.4. Let $f\colon R \to S$ be a ring homomorphism, let $I \subseteq R$ and $J \subseteq S$ be ideals, and assume $f(I) \subseteq J$; then there is an induced ring homomorphism $\bar{f}\colon R/I \to S/J$. If $b \in S$ is integral over R, then $[b]_J$ is integral over R/I: for if $P \in R[t]$ is monic with $f(P)_*(b) = 0$, then also the polynomial $[P]_I \in R/I[t]$ is monic, and $\bar{f}([P]_I)_*([b]_J) = [f(P)_*(b)]_J = [0]_J = 0$.
In general, if we only assume that b is algebraic over R, then $[b]_J$ is not algebraic over R/I. For example, let $R = \mathbb{Z}$, let $S = \mathbb{Z}[x]/(2x)$, and let f be the unique ring homomorphism; then $[x]_{2x}$ is algebraic over $\mathbb{Z}$, as witnessed by the polynomial $2t \in \mathbb{Z}[t]$. We can now consider the ideals $J = ([2]_{2x}) \subset S$ and $I = (2) \subset \mathbb{Z}$; then we have $R/I = \mathbb{Z}/2$, $S/J \cong \mathbb{Z}[x]/(2x, 2) = \mathbb{Z}[x]/(2) = \mathbb{Z}/2[x]$, and $\bar{f}\colon \mathbb{Z}/2 \hookrightarrow \mathbb{Z}/2[x]$ is the natural inclusion. The element $x \in \mathbb{Z}/2[x]$, corresponding to $[[x]_{2x}]_2 \in S/J$, is no longer algebraic.

Example 13.5. Similarly, let $f\colon R \to S$ be a ring homomorphism, let $T \subseteq R$ and $T' \subseteq S'$ be multiplicative subsets such that $f(T) \subset T'$; then there is an induced ring homomorphism $\check{f}\colon R_T \to S_{T'}$. If $b \in S$ is integral over R, then $\frac{b}{1} \in S_{T'}$ is integral over R_T: for if $P \in R[t]$ witnesses that b is integral over R, then the monic polynomial $\frac{P}{1} \in R_T[t]$ witnesses that $\frac{b}{1}$ is integral over R_T.
Consider instead the case of the inclusion or rings $R = \mathbb{Z}/6 \hookrightarrow S = \mathbb{Z}/6[x]/(2x) = \mathbb{Z}[x]/(6, 2x)$; then $[x] \in S$ is algebraic over R, as witnessed by the non-zero polynomial $[2]_6 t$. After localisation at the element $[3]_6 \in R \subset S$, we obtain up to easy identifications the inclusion of rings $\mathbb{Z}/2 \hookrightarrow \mathbb{Z}/2[x]$, and now x is no longer algebraic over $\mathbb{Z}/2$.

The previous examples show that over a field algebraic and integral dependence are equivalent notions, and that integral dependence is preserved when passing to quotient rings or localisations, whereas algebraic dependence may be lost. From now on we will focus only on integral dependence. Just beware of the phenomenon appearing in the following example.

Example 13.6. Let $R = \mathbb{Z}$ and $S = \mathbb{Z}[x]/(2x, x^2)$; then $[x] \in S$ is both algebraic over R, as witnessed by the polynomial $2t$, and integral, as witnessed by the polynomial t^2; however the minimal degree of a polynomial wintessing the algebraic dependence of x is 1, which is strictly smaller than the minimal degree of a polynomial witnessing integral dependence of x, which is in fact 2.
This of course has to do with the fact that, in general, if $f\colon R \to S$ is a ring homomorphism and $b \in S$ is an ideal, then the set of polynomials $P \in R[t]$ such that $f(P)_*(b) = 0$ is an ideal in $R[t]$; such an ideal is in general not principal, and if it contains monic polynomials it may not *be generated* by monic polynomials.

13.2. **Finite, finite type and integral algebras.** Given a ring homomorphism $f\colon R \to S$, we can consider S as an R-algebra or as an R-module. One says that

- S is an R-algebra *of finite type* if S is finitely generated as an R-algebra;
- S is a *finite* R-algebra if S is finitely generated as an R-module.

Similarly f is said to be a ring homomorphism of finite type, or a finite ring homomorphism. We already observed in Subsection 2.2 that if an R-algebra is finite, then it is also of finite type (but the viceversa doesn't hold in general). In light of Definition 13.2, we give the following definition.

Definition 13.7. An R-algebra S is said to be *integral* (respectively, the structure ring homomorphism $R \to S$ is *integral*, or an *integral extension*) if every element of S is integral over R.

Example 13.8. Looking at familiar fields, $\mathbb{C}$ is integral over $\mathbb{R}$, as every complex number z admits a conjugate complex number $\bar{z}$ such that both $s = z + \bar{z}$ and $p = z\bar{z}$ are real, and such that the polynomial $t^2 - st + p$ vanishes when evaluated at z. Instead, $\mathbb{R}$ is not integral over $\mathbb{Q}$, as witnessed by real numbers such as π.
A more subtle example is that of $\mathbb{Q}$ as a $\mathbb{Z}$-algebra: for the element $\frac{1}{2} \in \mathbb{Q}$ one can easily find a non-zero polynomial $P \in \mathbb{Z}[t]$ such that $P_*(\frac{1}{2}) = 0$, for instance $P = 2t - 1$; but no monic polynomial has this property! So $\mathbb{Q}$ is not integral as a $\mathbb{Z}$-algebra.

Exercise 13.9. Prove the last claim of Example 13.8. More generally, prove that if R is a unique factorisation domain and $\frac{a}{b} \in \mathrm{Frac}(R)$ is an element which is integral over R (considered as a subring of $\mathrm{Frac}(R)$), then in fact $\frac{a}{b} \in R$.

Exercise 13.10. Prove that every surjective ring homomorphism is integral. Prove also that if $f\colon R \to S$ is a ring homomorphism and $\bar{f}\colon R/\ker(f) \hookrightarrow S$ is the induced ring homomorphism from the quotient $R/\ker(f)$, then f is integral if and only if $\bar{f}$ is integral (in fact, each element of S is integral over R if and only if it is integral over $R/\ker(f)$).

There are some implications among the notions of integral, finite and finite type algebra: the first is given by the following lemma.

Lemma 13.11. *Let $f\colon R \to S$ be a ring homomorphism making S into an integral R-algebra of finite type; then S is a finite R-algebra.*

Proof. A way to express that S is of finite type is that there is a surjective R-algebra homomorphism $g\colon R[x_1, \dots, x_n] \to S$ from a finitely generated polynomial ring; letting $b_i = g(s_i) \in S$, we can equivalently require that S is generated as an R-module by *all* products $b_1^{e_1} \dots b_n^{e_n}$, for varying exponents $e_1, \dots, e_n \geq 0$. In principle, thus, one needs infinitely many elements to generate S as an R-module. However, if S is integral over R, then for each $1 \leq i \leq n$ there is a *monic* polynomial $P_i \in R[t]$ such that $f(P_i)_*(b_i) = 0$.
Now we appeal to the division algorithm for polynomials: if coefficients are taken in a generic ring R, we can still divide succesfully by any monic polynomial: for any $Q, P \in R[t]$ with P monic, there exist unique $A, B \in R[t]$ with $B = 0$ or $\deg(B) < \deg P$ such that $Q = AP + B$. This holds in particular for any polynomial Q of the form t^{e_i}, and for $P = P_i$. Applying $f(-)_*(b_i)$ to the equality $t^{e_i} = A_{i,e_i}P_i + B_{i,e_i}$, we obtain in S the equality $b_i^{e_i} = (B_{i,e_i})_*(b_i)$; using that B_{i,e_i} is a linear combination over R of $1, t, \dots, t^{\deg P_i - 1}$, we thus obtain that each power $b_i^{e_i}$ can be expressed as a linear combination over R of the *finitely many* powers $1, b_i, \dots, b_i^{\deg P_i - 1}$. Taking products over $1 \leq i \leq n$, we finally obtain that every product $b_1^{e_1} \dots b_n^{e_n}$ can be expressed as an R-linear combination of the *finitely many* products $b_1^{j_1} \dots b_n^{j_n}$, for varying $0 \leq j_i \leq \deg P_i - 1$. □

In fact the argument of proof of Lemma 13.11 shows the following statement, that we keep for future reference.

Lemma 13.12. *Let $f\colon R \to S$ be a ring homomorphism. Assume that there is a surjective R-algebra homomorphism $g\colon R[x_1, \dots, x_n] \twoheadrightarrow S$, for some $n \geq 1$, such that $g(x_i)$ is integral over R. Then S is a finite R-algebra.*

Example 13.13. Both hypotheses "integral" and "finite type" are necessary in Lemma 13.11. For instance:

- $k[x]$ is of finite type but not integral over k (x is not integral), and in fact $k[x]$ is not finite over k;
- $S = k[x_1, x_2, \dots]/(x_1, x_2, \dots)^2$ is integral over k: indeed every element $b = a + \sum_{i \geq 0} c_i[x_i]$, with $a, c_i \in k$, satisfies the equality $b^2 - 2ab + a^2 = (b-a)^2 = 0$; yet S is not of finite type, and hence also not finite over k.

We will see later that in fact also the converse to Lemma 13.11 holds, in Corollary 13.19

13.3. **Two manipulations of polynomials.** One of the simplest and yet most beautiful applications of the notion of integral dependence is that if $f\colon R \to S$ is integral, then one can detect whether an element of S is invertible by looking at the monic polynomial(s) in $R[t]$ that vanish when evaluated at the element.

Lemma 13.14. *Let $f\colon R \to S$ be an integral extension and let $b \in S$ be an element. Then $b \in S^\times$ if and only if there exists a monic polynomial $P = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in R[t]$ with $a_0 \in R^\times$ and such that $f(P)_*(b) = 0$.*

Proof. Suppose first that there is an equality $b^n + f(a_{n-1})b^{n-1} + \cdots + f(a_1)b + f(a_0) = 0$ with $a_0 \in R^\times$ and $a_1, \dots, a_{n-1} \in R$. Then also $f(a_0)$ is invertible in S, and the equality $1 = b \cdot \frac{-1}{f(a_0)}(f(a_{n-1})b^{n-1} + \cdots + f(a_1)b)$ shows that $b \in S^\times$.
Viceversa, assume that $b \in S^\times$. Let $P = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$ and $Q = t^m + c_{n-1}t^{n-1} + \cdots + c_1 t + c_0$ be monic polynomials such that $f(P)_*(b) = f(Q)_*(b^{-1}) = 0$. Then the polynomial $Q' := c_0 t^m + c_1 t^{m-1} + \cdots + c_{n-1}t + 1$ is possibly not monic, but it is such that $f(Q')_*(b) = 0$. We can now consider the polynomial $t^m P + Q'$: it is monic of degree $m + n$, its constant term is 1, and its evaluation at b vanishes. □

Example 13.15. Let $R \subseteq S$ be an injective, integral extension of domains. Then R is a field if and only if S is a field. To see this, if R is a field then for every $b \in S$ we can find a monic polynomial $P \in R[t]$ with $P_*(b) = 0$. If $b \neq 0$, we can factor $P = t^m P'$ with P' monic having non-zero constant term, and the equality $P_*(b) = b^m P'_*(b) = 0$, together with S being a domain, implies that $P'_*(b) = 0$; now Lemma 13.14 ensures that $b \in S^\times$.
Viceversa, if S is a field, then for every $b \in R$ with $b \neq 0$ we have $b \in S^\times$, so by Lemma 13.14 we can find an equality $b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$ with $a_0 \in R^\times$ and $a_1, \dots, a_{n-1} \in R$; note that all terms involved in the equality are in the ring $R \subseteq S$. We then have $b \cdot (b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) = -a_0 \in R$, hence b is a divisor of an invertible element of R, and is therefore also invertible.

The following lemma will be needed at least twice in the future: in the proof of Nakayama lemma 14.10, and in the characterisation of integral elements in any ring extension given in Proposition 13.18.

Lemma 13.16. *Let R be a ring and let M be an $R[x]$-module which is finitely generated also when considered as an R-module. Let $I \subseteq R$ be an ideal (possibly $I = R$) and suppose that $xM \subseteq IM$. Then there is a monic polynomial $P \in R[x]$ of the form $P = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ such that $PM = 0$ and such that $a_0, \ldots, a_{n-1} \in I$.*

Proof. The proof will be based on the Cayley-Hamilton theorem (or a variation of that argument, depending on what one means by "Cayley-Hamilton". Let S be a commutative ring, and for $n \geq 1$ denote by $\mathrm{Mat}_n(S)$ the set of $n \times n$ matrices with coefficients in S. Given a matrix $C = (c_{i,j}) \in \mathrm{Mat}_n(S)$, the determinant $\det(C) \in S$ can be defined using the Leibniz formula as the sum

$$\det(C) = \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) \left(\prod_{i=1}^{n} c_{i,\sigma(i)} \right),$$

where $\mathfrak{S}_n$ is the n^{th} symmetric group, i.e. the group of permutations of the set $\{1, \ldots, n\}$, and the sign of a permutation σ is 1 if σ is even, and -1 if σ is odd.
For $n \geq 2$, given a matrix $C \in \mathrm{Mat}_{n-1}(S)$, for all fixed $1 \leq i, j \leq n$ we denote by $\hat{C}_{i,j} \in \mathrm{Mat}n-1(S)$ the matrix obtained by removing the i^{th} row and the j^{th} column from the matrix A (and by reindexing the entries in the most natural way): this is usually called the $(i,j)^{\text{th}}$ "minor" of the matrix C. Then the Laplace rule tells us that for any fixed $1 \leq \bar{i} \leq n$, or for any fixed $1 \leq \bar{j} \leq n$, we can compute

$$\det(C) = (-1)^{\bar{i}-1} \sum_{j=1}^{n} (-1)^{j-1} c_{\bar{i},j} \det(\hat{C}_{\bar{i},j}) = (-1)^{\bar{j}-1} \sum_{i=1}^{n} (-1)^{i-1} c_{i,\bar{j}} \det(\hat{C}_{i,\bar{j}}).$$

We can now define, for a given matrix $C \in \mathrm{Mat}_n(S)$, with $n \geq 2$, a new matrix $\tilde{C} = (\tilde{c}_{i,j}) \in \mathrm{Mat}_n(S)$, usually called the "adjugate matrix" of C, by setting $\tilde{c}_{i,j} = (-1)^{i+j} \det(\hat{C}_{i,j})$. For $n = 1$ we also set $\tilde{C} = (1)$. The usual rule for matrix multiplication, together with the Laplace rule, tells us that $C \cdot \tilde{C} = \tilde{C} \cdot C = \det(C)\mathrm{Id}_n \in \mathrm{Mat}_n(C)$ (this is known as the "Cramer rule").
Now we start the actual proof of the lemma. Let $m_1, \ldots, m_n \in M$ be generators of M over R, with $n \geq 1$ (if $M = 0$ there is not much to prove...). The hypothesis $xM \subseteq IM$ allows us to find, for each $1 \leq i \leq n$, coefficients $a_{i,j} \in I$ for $1 \leq j \leq n$ such that $xm_i = \sum_{j=1}^{n} a_{i,j} m_j$. Let $A = (a_{i,j}) \in \mathrm{Mat}_n(R) \subset \mathrm{Mat}_n(R[x])$, let $C = (c_{i,j}) = x\mathrm{Id}_n - A \in \mathrm{Mat}_n(R[x])$, and let $\tilde{C} = (\tilde{c}_{i,j}) \in \mathrm{Mat}_n(R[x])$ be the adjugate matrix. Notice that for all $1 \leq k \leq n$ we have in M the equality $\sum_{j=1}^{n} c_{k,j} m_j$. Fix now $1 \leq i \leq n$; then we have the following chain of equalities in M

$$0 = \sum_{k=1}^{n} \tilde{c}_{i,k} \left(\sum_{j=1}^{n} c_{k,j} m_j \right) = \sum_{j=1}^{n} \left(\sum_{k=1}^{n} \tilde{c}_{i,k} c_{k,j} \right) m_j = \sum_{j=1}^{n} \left(\det(C)\mathrm{Id}_n \right)_{i,j} m_j = \det(C) m_i$$

where the third equality is given by the usual rule for computing the entries of a product matrix. Hence $\det(C) = \det(x\mathrm{Id}_n - A) \in R[x]$ is an element that kills all generators m_i of M. We also notice that the only contribution of degree n to $\det(C)$ comes from choosing the identity permutation in $\mathfrak{S}_n$, according to the Leibniz rule; in other words, $\det(C)$ is the sum of $\prod_{i=1}^{n}(x - ai, i)$ and other terms of degree $\leq n-1$ in x; as such, $\det(C)$ is a monic polynomial. We finally observe that the ring homomorphism $R[x] \to R[x]/(I)$ sends C to the matrix $[C]_{(I)} := ([a_{i,j}]_{(I)}) \in \mathrm{Mat}_n(R[x]/(I))$, and we have the equality $\det([C]_{(I)}) = [\det(C)]_{(I)}$;

since $[C]_{(I)} = [x\mathrm{Id}_n]_{(I)}$, we have that $[\det(C)]_{(I)} = [\det(x\mathrm{Id}_n)]_{(I)} = [x^n]_{(I)}$: this proves that all non-leading coefficients of $\det(C)$ lie in I. □

Exercise 13.17. Let $f\colon R \to S$ be a ring homomorphism, and let $b \in S$ be an element which is integral over R.

- Prove that the set I of all elements $a \in R$ such that there exists $P \in R[t]$ monic with $P_*(0) = a$ and $f(P)_*(b) = 0$ is an ideal of R; prove also that $I \subseteq f^{-1}((b))$ (the preimage along f of the principal ideal $(b) \subseteq S$).
- Prove that in general $I \neq f^{-1}((b))$. Hint: consider the case $R = \mathbb{Z} \hookrightarrow S = \mathbb{Z}[\sqrt{2}]$ and $b = 3\sqrt{2}$; prove that $6 \in (b)$ but $6 \notin I$.

Observe that Lemma 13.14 essentially proves that the ideal I from Exercise 13.17 is the entire ring R if and only if b is invertible.

13.4. **Characterisation of integral elements.** We can now characterise integral elements in a ring extension, and prove the converse of Lemma 13.11.

Proposition 13.18. *Let $f\colon R \to S$ be a ring homomorphism, and let $b \in S$. Then the following are equivalent:*

(1) b is integral over R, in the sense of Definition 13.2;
(2) the subring $f(R)[b] \subseteq S$ generated by b and the image of f is finitely generated as an R-module;
(3) there exists a finitely generated R-module $M \subseteq S$ containing $f(R)$ and such that $b \cdot M := \{bm \mid m \in M\} \subseteq M$ (in the latter we use the product operation of S);
(4) there is an $f(R)[b]$-module M which is finitely generated over R and such that the action of $f(R)[b]$ on M does not factor through any ideal of $f(R)[b]$ (one says that M is a "faithful" $f(R)[b]$-module).

Proof. (**1**) ⇒ (**2**). If b is integral, let $P = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in R[t]$ be a monic polynomial with $f(P)_*(b) = 0$. As in the proof of Lemma 13.11, we can invoke the division algorithm for polynomials and prove that every polynomial in $R[t]$ can be written as the sum of a multiple of P and another polynomial of degree at most $n-1$. Changing coefficients via f and then evaluating at b gives by definition of $f(R)[b]$ a surjective ring homomorphism $f(-)_*(b)\colon R[t] \to f(R)[b]$, and the previous argument shows that $(-)_*(b)$ is surjective also when restricted to the sub-R-module of $R[t]$ spanned by polynomials of degree $\leq n-1$; this is a finitely generated R-module, hence $f(R)[b]$ is also a finitely generated R-module.

(**2**) ⇒ (**3**). If $f(R)[b]$ is finitely generated as an R-module, then by definition it is also such that $b \cdot f(R)[b] \subseteq f(R)[b]$ and $f(R) \subseteq f(R)[b]$, so we just take $M = f(R)[b]$.

(**3**) ⇒ (**4**). If there is a finitely generated R-module $M \subseteq S$ such that $b \cdot M \subseteq M$ and $f(R) \subseteq M$, then the first condition allows us to consider M as an $f(R)[b]$-module; moreover if an element $c \in f(R)[b]$ acts as zero on the entire M, the second condition, implying $1_S \in M$, tells us that $c \cdot 1_S = 0$, so $c = 0$.

(**4**) ⇒ (**1**). Let M be an $f(R)[b]$-module which is finitely generated over R; the surjective R-algebra homomorphism $R[x] \twoheadrightarrow f(R)[b]$ sending $a \in R$ to $f(a) \in f(R) \subseteq f(R)[b]$ and sending $x \mapsto b$ allows us to consider M as an $R[x]$-module, which is still finitely generated over R. By Lemma 13.16 there is a monic polynomial $P \in R[x]$ such that $PM = 0$. This implies that the element $f(P)_*(b)$ acts trivially

on M, and if we assume that the action of $f(R)[b]$ on M doesn't factor through any ideal of $f(R)[b]$, we conclude that $f(P)_*(b) = 0$, whence b is integral over R. □

Proposition 13.18 has a number of corollaries.

Corollary 13.19. *Let $f\colon R \to S$ be a finite ring homomorphism. Then f is integral and of finite type.*

Proof. We have already observed several times that a finite ring homomorphism is also of finite type (an R-algebra which is finitely generated as an R-module is also finitely generated as an R-algebra). If f is finite, then $M = S$ satisfies (3) in Proposition 13.18 for any $b \in S$, hence any b in S is integral over R. □

Corollary 13.20. *Let $f\colon R \to S$ be an integral ring homomorphism.*

1. *If $I \subseteq R$ and $J \subseteq S$ are ideals with $f(I) \subseteq J$, then the induced ring homomorphism $\bar{f}\colon R/I \to S/J$ is again integral.*
2. *If $T \subseteq R$ is a multiplicative subset, then the induced ring homomorphism $f_T\colon R_T \to S_{f(T)}$ is again integral.*

Proof. Part (1) is a direct consequence of Example 13.4. For part (2), let $\frac{b}{f(s)} \in S_{f(T)}$; then b is integral over R, and this is witnessed by some monic polynomial $t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in R[t]$. The monic polynomial $t^n + \frac{a_{n-1}}{s}t^{n-1} + \cdots + \frac{a_0}{s^n} \in R_T[t]$ then witnesses that $\frac{b}{f(s)}$ is integral over R_T. □

Corollary 13.21. *Let $f\colon R \to R'$ and $f'\colon R' \to R''$ be ring homomorphisms.*

1. *If f and f' are of finite type, then $f' \circ f$ is of finite type.*
2. *If f and f' are finite, then $f' \circ f$ is finite.*
3. *If f and f' are integral, then $f' \circ f$ is integral.*

Proof. For (1), let $g\colon R[x_1, \dots, x_n] \twoheadrightarrow R'$ and $g'\colon R'[y_1, \dots, y_m] \twoheadrightarrow R''$ be surjective homomorphisms of R-algebras and R'-algebras, respectively. Then the ring homomorphism $\tilde{g}\colon R[x_1, \dots, x_n][y_1, \dots, y_m] \to R'[y_1, \dots, y_m]$ induced by g is also surjective. The composition $g' \circ \tilde{g}\colon R[x_1, \dots, x_n, y_1, \dots, y_m] \twoheadrightarrow R''$ shows that R'' is an R-algebra of finite type.
For (2), let similarly $r'_1, \dots, r'_n \in R'$ and $r''_1, \dots, r''_m \in R''$ be elements such that R' is generated by $r'_1, \dots, r'_n \in R'$ as an R-module and R'' is generated by $r''_1, \dots, r''_m \in R''$ as an R'-module. Then the elements $g'(r'_i)r''_j$ exhibit R'' as a finitely generated R-module.
For (3), let $b \in R''$; since R'' is integral over R', we can find an equality $b^n + g'(a_{n-1})b^{n-1} + \cdots + g'(a_1)b + g'(a_0) = 0$ in R'', with $a_0, \dots, a_{n-1} \in R'$. Denoting by $R[a_0, \dots, a_{n-1}] \subseteq R'$ the sub-R-algebra generated by the elements $a_0, \dots, a_{n-1}$, we have by Lemma 13.12 that both ring homomorphisms $R \to R[a_0, \dots, a_{n-1}]$ and $R[a_0, \dots, a_{n-1}] \to R''$ are finite, hence by (2) also their composition is finite, and by Corollary 13.19 we have that R'' is integral over R. □

13.5. **Integral closure along a ring homomorphism.**

Notation 13.22. Given a ring homomorphism $f\colon R \to S$ making S into an R-algebra, one often denotes by $\tilde{R}$ the subset of S of all elements that are integral over R. This notation is mostly used in contexts where the ring homomorphism f (often an injection) is understood.

As the next Lemma 13.23 shows, $\tilde{R}$ is a subring of S and contains $f(R)$: therefore $\tilde{R}$ is often called the *integral closure* of R in S, especially when f is an inclusion, so that one has $R \subseteq \tilde{R} \subseteq S$.

Corollary 13.23. *Let $f\colon R \to S$ be a ring homomorphism. Then $\tilde{R}$ is a subring of S and $f(R) \subseteq \tilde{R}$.*

Proof. For every element $b \in f(R)$ there is $a \in R$ such that $f(a) = b$; the polynomial $t - a \in R[t]$ witnesses that b is integral over R. This shows that $f(R) \subseteq \tilde{R}$. To show that $\tilde{R}$ is a subring of S, we have to prove that product and sum of elements in $\tilde{R}$ are again in $\tilde{R}$ (this is enough also to settle differences, as we already have checked that $-1 \in \tilde{R}$). Let therefore $b, b' \in \tilde{R}$ and consider the subring $f(R)[b, b'] \subseteq S$, i.e. the image of the R-algebra homomorphism $R[x, x'] \to S$ sending $x \mapsto b$ and $x' \mapsto b'$. Then by Lemma 13.12 we have that $f(R)[b, b']$ is a finite R-algebra, and by Corollary 13.19 we have that $f(R)[b, b']$ is an integral R-algebra: that is, every element of $f(R)[b, b']$, in particular $b + b'$ and bb', are integral over R. □

In general, if $b, b' \in S$ are integral and $P, P' \in R[t]$ are monic polynomials witnessing that, it is not immediate to find a monic polynomial $P'' \in R[t]$ witnessing that $b+b'$ is integral. With a little work, involving the theory of symmetric polynomials, one can in fact show that there is such a P'' of degree equal to $\deg(P) \cdot \deg(P')$, whose coefficients are expressed as polynomial functions of the coefficients of P and P'. A similar statement holds for the integral element bb'. This leads to an alternative proof of Lemma 13.23, which we will not discuss here.

Lemma 13.24. *Let $f\colon R \to S$ be a ring homomorphism and let $\tilde{R} \subseteq S$ be the integral closure of R as in Notation 13.22. Consider S as an $\tilde{R}$-algebra, and thus consider the integral closure $\tilde{\tilde{R}} \subseteq S$ of $\tilde{R}$ in S. Then $\tilde{R} = \tilde{\tilde{R}}$.*

Proof. By Corollary 13.21, the composite $R \xrightarrow{f} \tilde{R} \hookrightarrow \tilde{\tilde{R}}$ is an integral ring homomorphism, as it is a composition of integral maps, and thus we have $\tilde{\tilde{R}} \subseteq \tilde{R}$; the inclusion $\tilde{R} \subseteq \tilde{\tilde{R}}$ is a consequence of Lemma 13.23. □

Definition 13.25. If R is a domain and $S = \mathrm{Frac}(R)$, the integral closure $\tilde{R}$ is also called the *normalisation* of R. A domain R is *normal* if it coincides with its normalisation (as a subring of $\mathrm{Frac}(R)$).

We conclude the subsection with some examples of domains ant their normalisation.

Example 13.26. Let R be a unique factorisation domain; then the normalisation of R, i.e. the integral closure of R in $\mathrm{Frac}(R)$, coincides with R. This is the case, for instance, for $\mathbb{Z}$, $\mathbb{Z}[x_1, \ldots, x_n]$, $k[x_1, \ldots, x_n]$.

Example 13.27. Let $\mathbb{Q}[\sqrt{3}] \subset \mathbb{R}$ be the subfield containing all elements $a + b\sqrt{3}$ with $a, b \in \mathbb{Q}$, and consider the inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}[\sqrt{3}]$. Then $\tilde{\mathbb{Z}}$ contains all elements $a + b\sqrt{3}$ with $a, b \in \mathbb{Z}$, and this already shows that $\mathbb{Z} \neq \tilde{\mathbb{Z}}$; but $\tilde{\mathbb{Z}}$ is even larger than that: for example the element $\frac{1}{2} + \frac{\sqrt{3}}{2}$ belongs to $\tilde{\mathbb{Z}}$, as witnessed by the polynomial $t^2 - t + 2$. In fact all elements of $\tilde{\mathbb{Z}}$ have the form $\frac{a}{2} + \frac{b\sqrt{3}}{2}$ with $a + b$ even.

Example 13.28. Let k be a field and let $R = k[x^2, x^3] \subseteq k[x]$ be the subring spanned by polynomials whose degree-1 monomial vanishes. One often presents $k[x^2, x^3]$ as the ring $k[y, z]/(y^2 - z^3)$, by identifying $y = x^3$ and $z = x^2$. Then

$\mathrm{Frac}(R) = \mathrm{Frac}(k[x]) = k(x)$, and the element x is integral over R, as the polynomial $t^2 - x^2$ witnesses. Thus, by Lemma 13.23, $\tilde{R}$ is at least as large as $k[x]$; by Example 13.26 we have that $k[x]$ is normal, and therefore $\tilde{R} = k[x]$.

13.6. **Integral closure and localisation.** We conclude by analysing the interaction between localisation and integral closure along a ring homomorphism.

Lemma 13.29. *Let $f\colon R \to S$ be a ring homomorphism and let $T \subseteq R$ be a multiplicative subset, and consider the induced ring homomorphism $\bar{f}\colon R_T \to S_{f(t)}$; let $\widetilde{(R_T)} \subseteq S_{f(t)}$ be the integral closure of R_T in $S_{f(t)}$. Let moreover $\tilde{R} \subseteq S$ be the integral closure of R in S, and let $(\tilde{R})_{f(T)}$ be the localisation of $\tilde{R}$ at the multiplicative subset $f(t) \subseteq \tilde{R}$. Then $\widetilde{(R_T)} = (\tilde{R})_{f(T)}$.*

Proof. For the inclusion $\widetilde{(R_T)} \subseteq (\tilde{R})_{f(T)}$, let $\frac{b}{f(s)} \in S_{f(T)}$ be integral over R_T, with $b \in S$ and $s \in T$, and let $t^n + \frac{a_{n-1}}{s_{n-1}} t^{n-1} + \cdots + \frac{a_0}{s_0} \in R_T[t]$ be a monic polynomial witnessing that. The equality

$$\left(\frac{b}{f(s)}\right)^n + \frac{f(a_{n-1})}{f(s_{n-1})}\left(\frac{b}{f(s)}\right)^{n-1} + \cdots + \frac{f(a_0)}{f(s_0)} = 0 \in S_{f(T)}$$

can be rewritten, after setting $s' := s^n s_0 \dots s_{n-1} \in T$ and $a_i' = a_i s^{n-i} \prod_{j\neq i} s_j \in R$, as

$$\frac{1}{f(s')}\left(b^n + f(a_{n-1}')b^{n-1} + \cdots + f(a_0')\right) = 0 \in S_{f(T)}.$$

The last equality must be witnessed by some $s'' \in T$ such that in S we have the equality

$$f(s'')\left(b^n + f(a_{n-1}')b^{n-1} + \cdots + f(a_0')\right) = 0 \in S.$$

Multiplying further by $(f(s''))^{n-1}$, we obtain that $f(s'')b \in S$ is integral over R. Thus $\frac{b}{f(s)} = \frac{f(s'')b}{f(s''s)} \in (\tilde{R})_{f(T)}$.

For the other inclusion $(\tilde{R})_{f(T)} \subseteq \widetilde{(R_T)}$, let $\frac{b}{f(s)} \in S_{f(T)}$ with $b \in \tilde{R}$ and $s \in T$. Then $\frac{b}{1}$ is integral over R and hence also over R_T, whereas $\frac{1}{f(s)}$ is integral over R_T as witnessed by the polynomial $t - \frac{1}{s}$. By Lemma 13.23 the product $\frac{a}{f(s)} = \frac{a}{1}\frac{1}{f(s)}$ is also integral over R_T. □

We can use Lemma 13.29 to prove that being normal is a local property of a domain, in the following, strong sense. We observe that if R is a domain and $T \subseteq R \setminus \{0\}$ is a multiplicative subset, then R_T is again a domain and $\mathrm{Frac}(R_T)$ can be canonically identified with $\mathrm{Frac}(R)$.

Proposition 13.30. *Let R be a domain. Then the following are equivalent:*

1. *R is normal in the sense of Definition 13.25;*
2. *$R_{\mathfrak{p}}$ is normal for any $\mathfrak{p} \in \mathrm{Spec}(R)$;*
3. *$R_{\mathfrak{m}}$ is normal for any maximal ideal $\mathfrak{m} \subset R$.*

Proof. (**1**) ⇒ (**2**). By Lemma 13.29, letting $T = R \setminus \mathfrak{p}$ and $S = \mathrm{Frac}(S)$, we have $\widetilde{(R_T)} = (\tilde{R})_T = R_T$.

(**2**) ⇒ (**3**). Every maximal ideal is in particular a prime ideal.

(**3**) ⇒ (**1**). Let $\frac{a}{s} \in \mathrm{Frac}(R)$ be integral over R. Then $\frac{a}{s}$ is also integral over $R_{\mathfrak{m}}$ for any maximal ideal $\mathfrak{m} \subset R$, and thus we have $\frac{a}{s} \in R_{\mathfrak{m}} \subseteq \mathrm{Frac}(R)$. For each maximal

ideal $\mathfrak{m}$ we can therefore find $a_\mathfrak{m} \in R$ and $s_\mathfrak{m} \in R \setminus \mathfrak{m}$ with $\frac{a}{s} = \frac{a_\mathfrak{m}}{s_\mathfrak{m}} \in \mathrm{Frac}(R)$. Moreover the ideal $I \subseteq R$ generated by all elements $s_\mathfrak{m}$, for varying $\mathfrak{m}$ maximal in R, is not contained in any maximal ideal of R, and thus it must be equal to R and in particular contain $1 \in R$: so there exist maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ and elements $c_1, \dots, c_n \in R$ such that $c_1 s_{\mathfrak{m}_1} + \cdots + c_n s_{\mathfrak{m}_n} = 1$. We then have an equality in $\mathrm{Frac}(R)$

$$\frac{a}{s} = 1 \cdot \frac{a}{s} = \sum_{i=1}^{n} c_i b_{\mathfrak{m}_i} \frac{a_{\mathfrak{m}_i}}{s_{\mathfrak{m}_i}} = \sum_{i=1}^{n} c_i a_{\mathfrak{m}_i},$$

and the last expression clearly gives an element in $R \subseteq \mathrm{Frac}(R)$. □

Exercise 13.31. Let $f\colon R \to S$ be a ring homomorphism, let $s_1, \dots, s_r \in R$ be elements such that the ideal $(s_1, \dots, s_r) = R$. Suppose that each induced ring homomorphism $R_{s_i} \to S_{f(s_i)}$ is integral; prove that f is already integral. (Hint: for $b \in S$, consider the ideal of leading coefficients of polynomials $P \in R[t]$ satisfying $f(P)_*(b) = 0$, and prove that this ideal is the entire R.)

14. The "Going up" theorem and Nakayama lemma

Given a ring homomorphism $f\colon R \to S$, we have seen that there is an induced map $\mathrm{Spec}(f)\colon \mathrm{Spec}(S) \to \mathrm{Spec}(R)$; and we have seen that if f is faithfully flat, then $\mathrm{Spec}(f)$ is surjective: every prime ideal of R is the contraction along f of some prime ideal of S. For a generic ring homomorphism it is difficult to characterise the image of $\mathrm{Spec}(f)$: surely it is contained in $\mathbb{V}(\ker(f)) \subseteq \mathrm{Spec}(R)$, but in the example $i\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$ we see that $\mathbb{V}(\ker(i)) = \mathbb{V}(0) = \mathrm{Spec}(\mathbb{Z})$, yet the image of $\mathrm{Spec}(i)$ is only the point $(0) \in \mathrm{Spec}(\mathbb{Z})$.

14.1. **The "Lying over" theorem.** The "Lying over" theorem settles the question about the image of $\mathrm{Spec}(f)$ when f is an integral ring homomorphism.

Theorem 14.1 (Lying over)**.** *Let $f\colon R \to S$ be an integral ring homomorphism. Then* $\mathrm{Im}(\mathrm{Spec}(f)) = \mathbb{V}(\ker(f)) \subseteq \mathrm{Spec}(R)$.

In order to prove Theorem 14.1 we need the following proposition.

Lemma 14.2. *Let $f\colon R \to S$ be an integral ring homomorphism. Then: a prime ideal $\mathfrak{q} \in \mathrm{Spec}(S)$ is maximal if and only if $\mathrm{Spec}(f)(\mathfrak{q}) \in \mathrm{Spec}(R)$ is maximal.*

Proof. Let $\mathfrak{p} := \mathrm{Spec}(f))(\mathfrak{q}) = f^{-1}(\mathfrak{q})$. Then there is an induced ring homomorphism $\bar{f}\colon R/\mathfrak{p} \to S/\mathfrak{q}$, which is injective between domains and is still integral by Corollary 13.20. By Example 13.15, $R/\mathfrak{p}$ is a field if and only if $S/\mathfrak{q}$ is a field. □

Proof of Theorem 14.1. The inclusion $\mathrm{Im}(\mathrm{Spec}(f)) \subseteq \mathbb{V}(\ker(f))$ follows from the generic fact that if $J \subseteq S$ is an ideal, then $f^{-1}(J)$ is an ideal of R containing $\ker(f)$. Let now $\mathfrak{p} \subset R$ be some prime ideal containing $\ker(f)$; we want to show that there is some prime ideal $\mathfrak{q} \in \mathrm{Spec}(R)$ "lying over" $\mathfrak{p}$. For this, we use a similar strategy as in the proof of Theorem 12.6: we let $T := R \setminus \mathfrak{p}$ and consider the induced ring homomorphism $f_T\colon R_T \to S_{f(T)}$, which by Corollary 13.20 is still an integral extension. We observe that $f(T)$ does not contain 0, as $T \cap \ker(f) = \emptyset$, and this implies that $S_{f(T)}$ is not the zero ring, so there is some maximal ideal $\mathfrak{n} \subset S_{f(T)}$. By Lemma 14.2, since f_T is integral, we have that $\mathrm{Spec}(f_T)(\mathfrak{n})$ is a maximal ideal of R_T; the ring R_T is local, with unique maximal ideal $\mathfrak{m}$ being is the extension of $\mathfrak{p}$ along the localisation map $\tau_T\colon R \to R_T$, and hence we must

have $\mathrm{Spec}(f_T)(\mathfrak{n}) = \mathfrak{m}$. If we denote by $\tau_{f(T)}\colon S \to S_{f(T)}$ the localisation map and set $\mathfrak{q} = \mathrm{Spec}(\tau_{f(T)})(\mathfrak{q}) \in \mathrm{Spec}(S)$, we have that $\mathrm{Spec}(f)\colon \mathfrak{q} \mapsto \mathfrak{p}$since the following diagram of rings is commutative (we also write next to each ring the relevant prime ideal that it contains)

$$\begin{array}{ccccccc} \mathfrak{p} & \subset & R & \xrightarrow{f} & S & \supset & \mathfrak{q} \\ & & \downarrow{\scriptstyle \tau_T} & & \downarrow{\scriptstyle \tau_{f(T)}} & & \\ \mathfrak{m} & \subset & R_T & \xrightarrow{f_T} & S_{f(T)} & \supset & \mathfrak{n}. \end{array}$$

□

We observe that if $f\colon R \to S$ is an injective, integral ring homomorphism, then Theorem 14.1 implies that $\mathrm{Spec}(f)\colon \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is surjective. By Theorem 12.6 we then have that f is flat if and only if it is faithfully flat.

Example 14.3. For a field k, the inclusion of rings $k \hookrightarrow k[x]$ is faithfully flat, but it is not integral.

14.2. **The "Going up" theorem.** The "Going up" theorem is a refinement of the "Lying over" theorem, as it concerns the spectra $\mathrm{Spec}(R)$ and $\mathrm{Spec}(S)$ involved in an integral extension of rings not just as sets, but as posets (with inclusion of prime ideals giving the partial order).

Theorem 14.4 (Going up)**.** *Let $f\colon R \to S$ be an integral extension, let $\mathfrak{q} \in \mathrm{Spec}(S)$, denote $\mathfrak{p} = \mathrm{Spec}(f)(\mathfrak{q}) \in \mathrm{Spec}(R)$, and let $\mathfrak{p}' \in \mathrm{Spec}(R)$ be a prime ideal of R with $\mathfrak{p} \subseteq \mathfrak{p}'$. Then there is $\mathfrak{q}' \in \mathrm{Spec}(S)$ with $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathrm{Spec}(f)(\mathfrak{q}') = \mathfrak{p}'$.*

Proof. Let $g\colon R \to S/\mathfrak{q}$ be the composite ring homomorphism $R \xrightarrow{f} S \twoheadrightarrow S/\mathfrak{q}$. Then g is a composite of integral morphisms, so it is again integral by Corollary 13.21. By Theorem 14.1, since $\mathfrak{p}'$ is a prime ideal of R containing $\ker(g) = \mathfrak{p} = f^{-1}(\mathfrak{q}) = g^{-1}(0)$, we can find a prime ideal $\bar{\mathfrak{q}}' \in \mathrm{Spec}(R/\mathfrak{q})$ with $\mathrm{Spec}(g)(\bar{\mathfrak{q}}') = \mathfrak{p}'$. We then take $\mathfrak{q}'$ to be the preimag of $\bar{\mathfrak{q}}'$ in S. □

An immediate consequence of Theorem 14.4 is the following: let $f\colon R \to S$ be an integral ring homomorphism, and let $\mathfrak{p}_0 \subset \cdots \subseteq \mathfrak{p}_l$ be a chain of prime ideals in R; then for any "lift" $\mathfrak{q}_0$ of $\mathfrak{p}_0$ to a prime ideal in S, we can find a chain of prime ideals $\mathfrak{q}_0 \subseteq \cdots \subseteq \mathfrak{q}_l \subset S$ such that $\mathrm{Spec}(f)\colon \mathfrak{q}_i \mapsto \mathfrak{p}_i$ for all $0 \leq i \leq l$, by "going up" the chain. This last statement is sometimes known as the "Going up" theorem.
Recall now the definition of Krull dimension of a ring (Definition 9.2). A direct consequence of the "Going up" theorem is the following.

Corollary 14.5. *Let $f\colon R \to S$ be an injective integral ring homomorphism. Then $\dim(R) \leq \dim(S)$.*

Proof. Let $\mathfrak{p}_0 \subset \mathfrak{p}_q \subset \cdots \subset \mathfrak{p}_l \subset R$ be a strictly increasing chain of prime ideals in R. By Theorem 14.1 we can find $\mathfrak{q}_0 \in \mathrm{Spec}(S)$ with $\mathrm{Spec}(f)(\mathfrak{q}_0) = \mathfrak{p}_0$, and by Theorem 14.4 we can lift the entire chain to a chain of prime ideals $\mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_l \subset S$; no equality $\mathfrak{q}_i = \mathfrak{q}_{i+1}$ can occur, for otherwise we would also have $\mathfrak{p}_i = \mathrm{Spec}(f)(\mathfrak{q}_i) = \mathrm{Spec}(f)(\mathfrak{q}_{i+1}) = \mathfrak{p}_{i+1}$. This shows that for any strictly increasing chain of prime ideals in R we can find a strictly increasing chain of prime ideals in S of the same length, and this implies $\dim(R) \leq \dim(S)$. □

To prove the converse of Corollary 14.5 we need a lemma.

Lemma 14.6. *Let $f\colon R \to S$ be an integral ring homomorphism, and let $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ be nested prime ideals in $\operatorname{Spec}(S)$ such that $\operatorname{Spec}(f)(\mathfrak{q}_1) = \operatorname{Spec}(f)(\mathfrak{q}_2)$. Then $\mathfrak{q}_1 = \mathfrak{q}_2$.*

Proof. The argument is similar to the one of the proof of Theorem 12.6 and Theorem 14.1. Let $\mathfrak{p} := \operatorname{Spec}(f)(\mathfrak{q}_1) = \operatorname{Spec}(f)(\mathfrak{q}_2)$ and let $T := R \setminus \mathfrak{p}$; then $f(T)$ is disjoint from both $\mathfrak{q}_1$ and $\mathfrak{q}_2$, so that the extensions $\mathfrak{q}_1' = (\tau_{f(T)}(\mathfrak{q}_1))$ and $\mathfrak{q}_2' = (\tau_{f(T)}(\mathfrak{q}_2)$ are prime ideals in $S_{f(T)}$ (in particular, they are proper). The map $f_T\colon R_T \to S_{f(T)}$ is integral by Corollary 13.20; moreover $\mathfrak{q}_1' \subseteq \mathfrak{q}_2'$, and $\operatorname{Spec}(f_T)(\mathfrak{q}_i)$, for $i = 1, 2$ is a prime ideal of R_T whose contraction to R is $\mathfrak{p}$: the only such prime ideal is the (unique) maximal ideal of R_T. It follows from Lemma 14.2 that both $\mathfrak{q}_1'$ and $\mathfrak{q}_2'$ are maximal, since $\mathfrak{q}_1' \subseteq \mathfrak{q}_2'$ we must have $\mathfrak{q}_1' = \mathfrak{q}_2'$; we then have $\mathfrak{q}_1 = \operatorname{Spec}(\tau_{f(T)})(\mathfrak{q}_1') = \operatorname{Spec}(\tau_{f(T)})(\mathfrak{q}_2') = \mathfrak{q}_2$ as desired. □

Corollary 14.7. *Let $f\colon R \to S$ be an integral ring homomorphism. Then $\dim(S) \leq \dim(R)$.*

Proof. Let $\mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_l \subset S$ be a strictly increasing chain of prime ideals in S; applying $\operatorname{Spec}(f)$ we obtain a chain of prime ideals $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_l \subset R$; this chain must also be strictly increasing, for if $\mathfrak{p}_i = \mathfrak{p}_{i+1}$, Lemma 14.6 implies that $\mathfrak{q}_i = \mathfrak{q}_{i+1}$, against our assumption. Hence for every strictly increasing chain of prime ideals in S we can find a strictly increasing chain of prime ideals in R of the same length, and this implies $\dim(S) \leq \dim(R)$. □

Example 14.8. For a non-injective integral ring homomorphism $f\colon R \to S$ we can have a strict inequality $\dim(S) < \dim(R)$: for instance the surjection $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p$, for p a prime, is integral (as any surjective ring homomorphism), and $\dim(\mathbb{Z}/p) = 0 < \dim(\mathbb{Z}) = 1$. What "goes wrong" in the argument leading to Corollary 14.5 is the application of the "Lying over" theorem to the prime ideal $(0) \in \operatorname{Spec}(\mathbb{Z})$, since $(0) \notin \mathbb{V}(\ker(\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p)) = \mathbb{V}(p) = \{(p)\}$. In general, if $f\colon R \to S$ is integral and $\ker(f) \subseteq \sqrt{(0)} \subseteq R$, then $\dim(R) = \dim(S)$.

Example 14.9. If $f\colon R \to S$ is not a ring homomorphism, then the statement of the "Going up" theorem in general fails. For instance, take the inclusion $i\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$; then $(0) \in \operatorname{Spec}(\mathbb{Q})$ is sent via $\operatorname{Spec}(i)$ to $(0) \in \operatorname{Spec}(\mathbb{Z})$; for any maximal ideal $(p) \in \operatorname{Spec}(\mathbb{Z})$ we have $(0) \subseteq (p)$, yet (p) is not in the image of $\operatorname{Spec}(i)$.

14.3. **Nakayama lemma.** On a different note, we now discuss Nakayama lemma.

Lemma 14.10 (Nakayama)**.** *Let R be a ring, $I \subseteq R$ an ideal and M a finitely generated R-module. Suppose that $IM = M$. Then there is an element $a \in R$ with $aM = 0$ and $[a]_I = [1]_I \in R/I$.*

Proof. Consider the R-algebra homomorphism $f\colon R[x] \to R$ sending $x \mapsto 1$; then f_*M is an $R[x]$-module which is finitely generated as an R-module, so we may apply Lemma 13.16 and find a monic polynomial $P \in R[t]$ whose non-leading coefficients are in I and such that $P \cdot f_*M = 0$. It follows that $P_*(1) \cdot M = f(P) \cdot M = 0$, and $[P_*(1)]_I = [1]_I$. □

The following are corollaries of Nakayama lemma, that sometimes are also known under the name of Nakayama lemma.

Corollary 14.11. *Let R be a local ring with maximal ideal $\mathfrak{m}$, and let M be a finitely generated R-module with $\mathfrak{m}M = M$. Then $M = 0$.*

Proof. By Lemma 14.10, we can find $a \in R$ with $[a]_f m = [1]_{\mathfrak{m}}$ and $aM = 0$; in particular $a \notin \mathfrak{m}$, so $a \in R^\times$ (here we use that R is local) and thus $M = 0$. □

Corollary 14.12. *Let R be a ring, $I \subseteq R$ an ideal and M a finitely generated R-module. Let $N \subseteq M$ be a sub-R-module such that $M = N + IM$; then there is $a \in R$ with $[a]_I = [1]_I$ and $aM \subseteq N$. In particular, if R is local and $I = \mathfrak{m}$ is its maximal ideal, the conclusion is that $N = M$.*

Proof. The condition $M = N + IM$ is equivalent to the requirement that $M/N = I(M/N)$; since M/N is also finitely generated over R, we can apply Lemma 14.10 and find $a \in R$ with $[a]_I = [1]_I$ and $a(M/N) = 0$; the last condition is equivalent to $aM \subseteq N$. In the case of R local and $I = \mathfrak{m}$, we have $a \in R^\times$ and thus we have $M/N = 0$, i.e. $N = M$. □

Corollary 14.13. *Let R be a local ring with maximal ideal $\mathfrak{m}$, and let M be a finitely generated R-module. Let $m_1, \dots, m_n$ be elements of M; then $m_1, \dots, m_n$ generated M over R if and only if $[m_1]_{\mathfrak{m}M}, \dots, [m_n]_{\mathfrak{m}M}$ generated $M/\mathfrak{m}M$ as a vector space over $R/\mathfrak{m}$.*

Proof. If the elements m_i generated M over R, then the elements $[m_i]_{\mathfrak{m}M}$ generated $M/\mathfrak{m}M$ over R and, equivalently, over $R/\mathfrak{m}$. Viceversa, assume that the elements $[m_i]_{\mathfrak{m}M}$ generated $M/\mathfrak{m}M$ over $R/\mathfrak{m}$, and let $N = \mathrm{Span}_R(m_1, \dots, m_n)$; then $M = N + \mathfrak{m}M$, as this equality is equivalent to the surjectivity of the map $N/\mathfrak{m}N \to M/\mathfrak{m}M$ induced by the inclusion $N \subseteq M$. By Corollary 14.12 we then have $M = N$ as desired. □

Example 14.14. Recall that $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-module. For every non-zero ideal $I = (n) \subseteq \mathbb{Z}$ we have $\mathbb{Q} = (n)\mathbb{Q}$, yet, at least for $n \geq 2$, any $a \in \mathbb{Z}$ with $a \equiv 1 \pmod{n}$ also satisfies $a \neq 0$, so that we have $a\mathbb{Q} = \mathbb{Q}$ instead of $a\mathbb{Q} = 0$.

Example 14.15. If M is a finitely generated module over a local ring R with maximal ideal $\mathfrak{m}$, Corollary 14.13 gives us a way to compute the *minimal* number of generators necessary to generated M over R: this is the dimension of $M/\mathfrak{m}M$ over $R/\mathfrak{m}$.
If we now pick a basis $[m_1]_{\mathfrak{m}M}, \dots, [m_n]_{\mathfrak{m}M}$ of $M/\mathfrak{m}M$ over $R/\mathfrak{m}$, we can consider the R-module homomorphism $f\colon R^n \to M$ sending the i^{th} standard generator of R^n to m_i. By Corollary 14.13 we have that f is surjective; is it also an isomorphism? In general not: think of the example in which $M = R/\mathfrak{m}$, then the dimension n will be 1, m_1 will be some element of $R^\times = R \setminus \mathfrak{m}$, and the map $f\colon R \to R/\mathfrak{m}$ given by $f(a) = [m_1 a]_{\mathfrak{m}}$ is not injective.
If one however assumes that R is Noetherian and M is... flat, then with a little homological algebra it is possible to prove that f is in fact an isomorphism; here is for your curiosity the argument. If $N = \ker(f)$, then the short exact sequence $0 \to N \to R^n \to M \to 0$ gives rise to a long exact sequence $\cdots \to \mathrm{Tor}_1^R(M, R/\mathfrak{m}) \to N \otimes_R R/\mathfrak{m} \to (R/\mathfrak{m})^n \to M/\mathfrak{m}M \to 0$ (if you don't know what "Tor" means, you will learn it when studying homological algebra). Since M is flat, we have $\mathrm{Tor}_1^R(M, R/\mathfrak{m}) = 0$, and moreover the last map $(R/\mathfrak{m})^n \to M/\mathfrak{m}M$, induced by f, is an isomorphism. It follows that $N \otimes_R R/\mathfrak{m} = N/\mathfrak{m}N$ vanishes, and since R is Noetherian we have that N is finitely generated over R and we can apply Corollary 14.11 to conclude that $N = 0$.
So for a finitely generated module over a local Noetherian ring, being flat is the same as being free!

14.4. **A glimpse on the "Going down" theorem.** Theorem 14.4 allows one, in presence of an integral morphism $f\colon R \to S$, to lift a chain of prime ideals $\mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_l$ in R to a chain of prime ideals $\mathfrak{q}_0 \subseteq \cdots \subseteq \mathfrak{q}_l$ in S, provided that a lift $\mathfrak{q}_0$ of the smallest prime ideal $\mathfrak{p}_0$ is given. Is it possible to find lifts that *end* with a given prime ideal $\mathfrak{q}_l$ lifting $\mathfrak{p}_l$? Under quite strong assumptions, the answer is yes.

Theorem 14.16 (Going down)**.** *Let $f\colon R \to S$ be an injective, integral map of domains, with R normal (see Definition 13.25). Let $\mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_l$ be a chain of prime ideals in R, and let $\mathfrak{q}_l$ be a prime ideal in S with $f^{-1}(\mathfrak{q}_l) = \mathfrak{p}_l$. Then there exists a chain of prime ideals $\mathfrak{q}_0 \subseteq \cdots \subseteq \mathfrak{q}_l$ in S with $f^{-1}(\mathfrak{q}_i) = \mathfrak{p}_i$.*

The strategy of the proof is the following. First, since f is injective, let us assume that $R \subseteq S$ is a subring. By Theorem 14.1 we can find some lift $\hat{\mathfrak{q}}_0$ of $\mathfrak{p}_0$, and by Theorem 14.4 we can extend this to a chain $\hat{\mathfrak{q}}_0 \subseteq \cdots \subseteq \hat{\mathfrak{q}}_l$ of prime ideals in S lifting the original chain of prime ideals in R. If we are very lucky, we get that $\hat{\mathfrak{q}}_l$ is precisely the desired lift $\mathfrak{q}_l$, and we are done.
Unfortunately we cannot expect to be lucky; the next idea is to look for an automorphism of rings $g\colon S \to S$ fixing R pointwise and such that $g(\hat{\mathfrak{q}}_l) = \mathfrak{q}_l$: in this case we can apply g to the entire chain $\hat{\mathfrak{q}}_0 \subseteq \cdots \subseteq \hat{\mathfrak{q}}_l$, and we win again.
In this light, it would be desirable if S admits many automorphisms as an R-algebra. We next notice that enlarging S to an even larger domain S' which is still an integral extension of R, cannot harm: indeed S' is also integral over S, and by Theorem 14.1 we can lift $\mathfrak{q}_l$ to a prime ideal $\mathfrak{q}'_l$; if we are able to solve the Going-down problem for the extension $R \subseteq S'$, finding a chain of prime ideals $\mathfrak{q}'_0 \subseteq \cdots \subseteq \mathfrak{q}'_l$ lifting the given chain in R, then we can intersect this chain with S and obtain a chain of prime ideals in S with the desired properties.
What we do is to consider the algebraic closure $\overline{\mathrm{Frac}(R)}$ of the field $\mathrm{Frac}(S)$ (which is also the algebraic closure of $\mathrm{Frac}(S)$), and inside here consider the integral closure $S' = \tilde{R}$ of R. The Galois group G of $\overline{\mathrm{Frac}(R)}$ over $\mathrm{Frac}(R)$ acts on $\overline{\mathrm{Frac}(R)}$ by field automorphisms that fix $\mathrm{Frac}(R)$, and in particular R, pointwise. It follows that G acts on $\overline{\mathrm{Frac}(R)}$ preserving S'. One then has to prove that G acts transitively on the set of prime ideals $\mathfrak{q}' \subset S'$ satisfying $\mathfrak{q}' \cap R = \mathfrak{p}_l$. See Section 3.3 in [Bos] for the rest of the proof!

15. Nullstellensatz

Recall that, given a field k and an ideal $I \subseteq k[x_1, \ldots, x_n]$, we defined the associated affine algebraic set $\mathbb{V}(I) \subset k^n$ in Definition 2.36. We observed that $\mathbb{V}(-)$, considered as a function from ideals of $k[x_1, \ldots, x_n]$ to subsets of k^n, is in general not injective; one reason, corresponding to the first half of Example 2.39, is that one always has $\mathbb{V}(I) = \mathbb{V}(\sqrt{I})$; but even if we restrict $\mathbb{V}(-)$ to radical ideals, we have situations like the one in the second half of Example 2.39, in which we even see a *proper* ideal I satisfying $\mathbb{V}(I) = \mathbb{V}(k[x_1, \ldots, x_n]) = \emptyset$. The Hilbert Nullstellensatz tells us that if k is an *algebraically closed* field, then radical ideals of $k[x_1, \ldots, x_n]$ are faithfully represented by their associated affine algebraic sets. We repeat the definition of algebraically closed field.

Definition 15.1. A field k is *algebraically closed* if for every non-zero polynomial $P \in k[t]$ of degree ≥ 1 there is $a \in k$ with $P_*(a) = 0$.

If a field k is algebraically closed, then every integral extension $k \to R$ in which R is also a field is in fact a bijection $k \cong R$.

In the formulation of the Nullstellensatz we will use the notation $\mathbb{V}(-)$. It is time to make this notation unambiguous, as for an ideal $I \subset k[x_1, \dots, x_n]$, we have denoted by "$\mathbb{V}(I)$" both a subset of k^n (Definition 2.36) and a subspace of $\mathrm{Spec}(k[x_1, \dots, x_n])$ (end of Subsection 3.1).

Definition 15.2. For a ring R, we denote by $\mathrm{Spec}_{\max}(R) \subset \mathrm{Spec}(R)$ the subset consisting of all maximal ideals of R.

Notation 15.3. For a generic ideal I in a generic ring R, we denote by $\mathbb{V}(I) \subseteq \mathrm{Spec}(R)$ the set of all prime ideals of R containing I, and by $\mathbb{V}_{\max}(I) = \mathbb{V}(I) \cap \mathrm{Spec}_{\max}(R)$ the set of all maximal ideals of R containing I.
Given any subset $X \subseteq \mathrm{Spec}(R)$, we denote by $\mathbb{I}(X) \subset R$ the (radical) ideal obtained as intersection of all prime ideals in X.
If R is a k-algebra (e.g. $R = k[x_1, \dots, x_n]$, we denote by $\mathrm{Spec}^k_{\max}(R) \subset \mathrm{Spec}_{\max}(R)$ the set of all maximal ideals $\mathfrak{m}$ of R such that the composite $k \to R \to R/\mathfrak{m}$ is an isomorphism of fields; equivalently, $\mathrm{Spec}^k_{\max}(R)$ contains kernels of k-algebra homomorphisms $R \to k$; and we denote by $\mathbb{V}^k_{\max}(R) = \mathbb{V}_{\max}(I) \cap \mathrm{Spec}^k_{\max}(R)$.

Observe that the subset $k^n \subseteq \mathrm{Spec}(k[x_1, \dots, x_n])$ is precisely $\mathrm{Spec}^k_{\max}(k[x_1, \dots, x_n])$.

Theorem 15.4 (Nullstellensatz)**.** *Let k be a field. Then the following are equivalent:*

(1) k is algebraically closed;
(2) for all $n \geq 0$, if $I \subset k[x_1, \dots, x_n]$ is a proper ideal, then $\mathbb{V}^k_{\max}(I) \neq \emptyset$;
(3) for all $n \geq 0$, if $\mathfrak{m} \subset k[x_1, \dots, x_n]$ is a maximal ideal, then for suitable $a_1, \dots, a_n \in k$ we have $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$; in other words $\mathrm{Spec}^k_{\max}(k[x_1, \dots, x_n]) = \mathrm{Spec}_{\max}(k[x_1, \dots, x_n])$;
(4) for all $n \geq 0$, if $I \subseteq k[x_1, \dots, x_n]$ is an ideal, then $\sqrt{I} = \mathbb{I}(\mathbb{V}^k_{\max}(I))$.

Observe that non-zero polynomials of degree ≥ 1 in $k[t]$ are precisely the non-invertible elements in $k[t]$. This immediately tells us that (1) is equivalent to (2) for $n = 1$: an proper ideal in $k[t]$ is the principal ideal generated by a non-invertible $P \in k[t]$, and for $a \in k = \mathrm{Spec}^k_{\max}(k[t])$ we have $a \in \mathbb{V}^k_{\max}((P))$ if and only if $P_*(a) = 0$.
We also observe that (3) implies (2): if I is proper, we can include it into a maximal ideal $\mathfrak{m} \subset k[x_1, \dots, x_n]$, which assuming (3) has the form $(x_1 - a_1, \dots, x_n - a_n)$: then at least the point $(a_1, \dots, a_n) \in k^n$ lies in $\mathbb{V}^k_{\max}(I)$, which is therefore non-empty. Similarly, (4) implies (2): if I is an ideal with $\mathbb{V}(I) = \emptyset$, then $\mathbb{I}(\mathbb{V}(I)) = \mathbb{I}(\emptyset) = k[x_1, \dots, x_n]$, and assuming (4) we would have $\sqrt{I} = k[x_1, \dots, x_n] \ni 1$, implying that a power of 1 is in I, so $I = k[x_1, \dots, x_n]$ and I is not proper.
For the other implications more work is needed! The rest of the proof of Theorem 15.4 is the content of the rest of the section.

15.1. **Noether normalisation lemma.** The standard proof of the Nullstellensatz goes through the Noether normalisation lemma, stating that each k-algebra of finite type is a finite extension of a polynomial ring.

Lemma 15.5 (Noether normalisation lemma)**.** *Let k be a field and let R be a non-zero finitely generated k-algebra. Then there is $m \geq 0$ for which there is an injective, finite k-algebra homomorphism $f \colon k[y_1, \dots, y_m] \hookrightarrow R$.*

The idea of the proof is the following. The hypothesis allows us to identify R as a k-algebra with one of the form $k[x_1,\dots,x_n]/I$ for some $n\geq 0$ and some ideal I. If we are lucky, then there is $0\leq m\leq n$ such that the natural map $k[x_1,\dots,x_m]\to k[x_1,\dots,x_n]/I$ is injective and finite; if we are not lucky... this will be true after taking a "change of variables": we can pick polynomials $P_i\in k[x_1,\dots,x_n]$ for $1\leq i\leq n$, such that the induced k-algebra homomorphism $g\colon k[x_1,\dots,x_n]\to k[x_1,\dots,x_n]$ sending $x_i\mapsto P_i$ is bijective (we will discuss later how to ensure this by cleverly choosing P_i). The image of the ideal I is a new ideal $g(I)\subset k[x_1,\dots,x_n]$, and we can equivalently study the finitely generated k-algebra $k[x_1,\dots,x_n]/g(I)$: if we are lucky, this new quotient satisfies that the natural map $k[x_1,\dots,x_m]\to k[x_1,\dots,x_n]/g(I)$ is injective and finite.
It is in general hard to say a priori, given a sequence $P_1,\dots,P_n\in k[x_1,\dots,x_n]$ of polynomials, whether the induced k-algebra homomorphism $g\colon k[x_1,\dots,x_n]\to k[x_1,\dots,x_n]$ is bijective or not. However, if we fix natural numbers $e_1,\dots,e_{n-1}$, then the k-algebra homomorphism

$$g_{e_1,\dots,e_{n-1}}\colon k[x_1,\dots,x_n]\to k[x_1,\dots,x_n],\quad x_i\mapsto x_i+x_n^{e_i}\ \forall 1\leq i\leq n-1,\quad x_n\mapsto x_n$$

is indeed bijective, with inverse given by the homomorphism

$$g^-_{e_1,\dots,e_{n-1}}\colon k[x_1,\dots,x_n]\to k[x_1,\dots,x_n],\quad x_i\mapsto x_i-x_n^{e_i}\ \forall 1\leq i\leq n-1,\quad x_n\mapsto x_n$$

Lemma 15.6. *Let $P\in k[x_1,\dots,x_n]$ be a non-zero polynomial. Then there are $e_1,\dots,e_{n-1}$ and there is $\lambda\in k^\times$ such that $\lambda\cdot g_{e_1,\dots,e_{n-1}}(P)$ is monic when considered as a polynomial in x_n with coefficients in $k[x_1,\dots,x_{n-1}]$.*

Proof. The polynomial P can be written as a finite sum $\sum_{i=1}^r c_i x^{\alpha_i}$, where $r\geq 1$, $c_i\in k^\times$, $\alpha_i=(\alpha_i(1),\dots,\alpha_i(n))\in\mathbb{N}^n$ and we abbreviate $x^{\alpha_i}=x_1^{\alpha_i(1)}\dots x_n^{\alpha_i(n)}$. We may assume that α_1 is the maximum among the α_i with respect to the lexicographic order on $\mathbb{N}^n$: concretely this means that for all $i\geq 2$, if $1\leq j\leq n$ is minimal with $\alpha_1(j)\neq\alpha_i(j)$, then $\alpha_1(j)>\alpha_i(j)$.
Let N be a natural number which is larger than $\sum_{i=1}^r\sum_{j=1}^n\alpha_i(j)$, and consider the k-algebra automorphism $g=g_{e_1,\dots,e_{n-1}}$ of $k[x_1,\dots,x_n]$ induced by the sequence $e_i=N^{n-i}$, for $1\leq i\leq n-1$. We claim that $\frac{1}{c_1}g(P)$ is monic in x_n, and it has degree in x_n precisely equal to $d_1:=\sum_{j=1}^n\alpha_1(j)N^{n-j}$. To see this, write

$$g(P)=\sum_{i=1}^r c_i\prod_{j=1}^{n-1}\left(x_j+x_n^{N^{n-i}}\right)^{\alpha_i(j)}x_n^{\alpha_i(n)}.$$

Then the degree in x_n of the i^{th} summand is $d_i:=\sum_{j=1}^n\alpha_i(j)N^{n-j}$, as can be seen by selecting in each binomial $x_j+x_n^{N^{n-i}}$ the power of x_n rather than x_j. By choice of N, each $\alpha_i(j)$ is strictly smaller than N, so we can interpret the previous expression as the base-N-expansion of the natural number d_i; the lexicographic maximality of α_1 now implies that $d_1>d_i$ for any $i\geq 2$; so the first summand dictates the degree in x_n of $g(P)$, which is d_1, and also what is the coefficient of $x_n^{d_1}$ in $g(P)$, namely c_1. □

Proof or Lemma 15.5. By hypothesis we can identify the finitely generated k-algebra R with a quotient algebra $k[x_1,\dots,x_n]/I$ for some $n\geq 0$ and some ideal $I\subset k[x_1,\dots,x_n]$; there are a priori several possible choices of n and of I. We proceed by induction on n, showing the following statement, depending on n:

If $I \subset k[x_1, \dots, x_n]$ is an ideal, then there is $0 \leq m \leq n$ and a finite injective k-algebra map $f\colon k[y_1, \dots, y_m] \hookrightarrow k[x_1, \dots, x_n]/I$.

For $n = 0$ we have the only case $I = (0) \subset k = k[\,]$, so $k[\,]/I$ is already finite over k, and we take $m = 0$.

Let now $n \geq 1$; and let $I \subset k[x_1, \dots, x_n]$; if $I = (0)$ we can again take $m = n$ and consider the bijective map $k[y_1, \dots, y_n] \cong k[x_1, \dots, x_n]$ sending $y_i \mapsto x_i$. Let us now assume that $I \neq 0$, and let $P \in I$ be a non-zero element. If P is not monic in x_n when considered as a polynomial with coefficients in $k[x_1, \dots, x_n]$, then we may choose an automorphism g of $k[x_1, \dots, x_n]$ and $\lambda \in k^\times$ as in Lemma 15.6, so that $\lambda g(P)$ is monic in x_n; up to replacing P by $\frac{P}{\lambda} \in I$, we may then assume that $g(P)$ is already monic in x_n. Moreover g induces an isomorphism of k-algebras $\bar{g}\colon k[x_1, \dots, x_n]/I \cong k[x_1, \dots, x_n]/g(I)$, so we may as well prove the existence of an injective finite k-algebra map $f'\colon k[y_1, \dots, y_m] \to k[x_1, \dots, x_n]/g(I)$, and then set $f = \bar{g}^{-1} \circ f'$.

So we may assume that P is already monic in x_n. Let then $I' = I \cap k[x_1, \dots, x_{n-1}]$; then the map $h\colon k[x_1, \dots, x_{n-1}]/I' \to k[x_1, \dots, x_n]/I$ is injective and finite (indeed the powers of x_n up to $\deg_{x_n} P$ suffice to generate $k[x_1, \dots, x_n]/I$ as a module over $k[x_1, \dots, x_{n-1}]/I'$). By inductive hypothesis we can find $0 \leq m \leq n-1$ and an injective, finite map of k-algebras $f'\colon k[y_1, \dots, y_m] \to k[x_1, \dots, x_{n-1}]/I'$; we then take $f = h \circ f'$. □

Recall that $\mathrm{Spec}(k[x_1, \dots, x_n])$ contains k^n as a subset in a natural way; then the automorphism $g_{e_1,\dots,e_n}$ considered in Lemma 15.6 induces a homeomorphism of $\mathrm{Spec}(k[x_1, \dots, x_n])$ which restricts to the bijection $k^n \to k^n$ sending $(a_1, \dots, a_n) \mapsto (a_1 + a_n^{e_1}, a_2 + a_n^{e_2}, \dots, a_n)$. This bijection is not as nice as a *linear automorphism* of k^n; when k is infinite, in fact, there is an alternative proof of Lemma 15.5 using only "linear" change of variable automorphisms of $k[x_1, \dots, x_n]$ (i.e. each x_i is sent to a homogeneous polynomial of degree 1).

Exercise 15.7. Carry out the alternative proof of Lemma 15.5 when k is infinite, by proving the following statements:

- if $P \in k[x_1, \dots, x_n]$ is a non-zero, homogeneous polynomial of total degree $d \geq 0$, then there are $a_1, \dots, a_{n-1} \in k$ with $P_*(a_1, \dots, 1) \neq 0$;
- if $P \in k[x_1, \dots, x_n]$ is a non-zero polynomial, then there are $a_1, \dots, a_{n-1} \in k$ such that the automorphism g of $k[x_1, \dots, x_n]$ sending $x_i \mapsto x_i + a_i x_n$ for $1 \leq i \leq n-1$ and $x_n \mapsto x_n$ sends P to a polynomial $g(P)$ which, up to multiplying by an element in $k^\times$, is monic in x_n.

15.2. **Maximal ideals and residue fields in finitely generated algebras.** An immediate application of Lemma 15.5 is the following.

Lemma 15.8 (Zariski lemma)**.** *Let $k \hookrightarrow K$ be an extension of fields (i.e. a ring homomorphism between fields). Then K is finite over k if and only if it is of finite type over k.*

Proof. If K is finite over k, then it is also of finite type. Assume now that K is of finite type over k. By Lemma 15.5 we have that there is an injective, finite k-algebra homomorphism $k[y_1, \dots, y_m] \hookrightarrow K$ for some $m \geq 0$; by Example 13.15 we then have that $k[y_1, \dots, y_m]$ is a field, and this clearly implies $m = 0$. □

In Definition 5.16 we introduced the notion of *residue field*. A corollary of Lemma 15.8 is the following.

Corollary 15.9. *Let k be a field and let R be a non-zero finitely generated k-algebra; then for every maximal ideal $\mathfrak{m} \subset R$, the residue field $R/\mathfrak{m}$ is finite over k.*

Proof. By Corollary 13.21, the composite map $k \to R \to R/\mathfrak{m}$ is a field extension of finite type. By Lemma 15.8 we obtain that $R/\mathfrak{m}$ is finite over k. □

We can use Corollary 15.8 to prove that (1) implies (3) in Theorem 15.4: if $\mathfrak{m} \subset k[x_1, \dots, x_n]$ is a maximal ideal, then the composite ring homomorphism $k \to k[x_1, \dots, x_n] \to k[x_1, \dots, x_n]/\mathfrak{m}$ is a finite extension of k *which is again a field*; assuming k algebraically closed, this implies that $k \to k[x_1, \dots, x_n]/\mathfrak{m}$ is an isomorphism. In particular, for each $1 \leq i \leq n$, the class $[x_i]_{\mathfrak{m}}$ is the image of some element $a_i \in k$; we then have $x_i - a_i \in \mathfrak{m}$, so that $(x_1 - a_1, \dots, x_n - a_n) \subseteq \mathfrak{m}$, and by maximality of both ideals we must have an equality.

15.3. **Radical ideals and zero loci.** So far we have proved that (1), (2) and (3) are equivalent and implied by (4) in Theorem 15.4. We will now prove that (3) implies (4) as well; this will follow almost immediately from the following, general proposition.

Proposition 15.10. *Let k be a field and let R be a k-algebra of finite type. Then we have $\sqrt{I} = \mathbb{I}(\mathbb{V}_{\max}(I))$.*

Proof. Recall from Proposition 3.19 that $\sqrt{I}$ is the intersection of all prime ideals in R containing I; in the light of Notation 15.3, we have $\sqrt{I} = \mathbb{I}(\mathbb{V}(I))$. Since $\mathbb{V}_{\max}(I) \subseteq \mathbb{V}(I)$, we have $\sqrt{I} = \mathbb{I}(\mathbb{V}(I)) \subseteq \mathbb{I}(\mathbb{V}_{\max}(I))$.
Let now $a \in R \setminus \sqrt{I}$, let $T = \{1, a, a^2, \dots\} \subset R$, and consider the localisation $\tau\colon R \to R_T$; we immediately observe that R_T is of finite type over R, as it is generated by $\frac{1}{a}$ as an R-algebra. By Corollary 13.21 we have that R_T is also of finite type over k.
Since $T \cap I = \emptyset$, by Lemma 5.1 we have that the extended ideal $I^e \subset R_T$ is a proper ideal; as such it is contained in a maximal ideal $\mathfrak{m} \subset R_T$; the preimage $\mathfrak{p} := \mathfrak{m}^c \subset R$ is a prime ideal containing I. We can consider the composition of ring homomorphisms $k \to R/\mathfrak{p} \to R_T/\mathfrak{n}$. Both morphisms and their composition are of finite type, and in particular the field $R_T/\mathfrak{n}$ is a field extension of k of finite type over k; by Lemma 15.8 we have that $R_T/\mathfrak{n}$ is finite over k, and a fortiori $R_T/\mathfrak{n}$ is finite also over the domain $R/\mathfrak{p}$; it follows from Example 13.15 that $R/\mathfrak{p}$ is in fact a field, that is $\mathfrak{p} \subset R$ is in fact maximal. Since $\tau(a)$ is invertible and $\tau(\mathfrak{p}) \subset \mathfrak{m}$, we have $a \notin \mathfrak{p}$; thus $a \notin \mathbb{I}(\mathbb{V}_{\max}(I))$, as the latter is the intersection of all maximal ideals of R containing I, and $\mathfrak{p}$ is one of them. □

Recall that (3) in Theorem 15.4 is the requirement that for all $n \geq 0$ one has $\mathrm{Spec}^k_{\max}(k[x_1, \dots, x_n]) = \mathrm{Spec}_{\max}(k[x_1, \dots, x_n])$; under this assumption, by Proposition 15.10 we immediately have $\sqrt{I} = \mathbb{I}(\mathbb{V}_{\max}(I)) = \mathbb{I}(\mathbb{V}^k_{\max}(I))$, which is (4).
A particular case of Proposition 15.10 is the following: taking $I = (0)$, we obtain that the Jacobson ideal $J(R)$ of a finitely generated k-algebra R, introduced in Definition 3.20, coincides with the nilradical $\sqrt{(0)}$.

16. Artin-Rees lemma and Krull intersection theorem

It is well-known that the only integer $n \in \mathbb{Z}$ which is a multiple of 2^m for all $m \geq 0$ is zero. In the language of ideals in rings, we have $\bigcap_{m \geq 0} (2)^m = 0$, where we take

a *descending* intersection. This observation turns out useful in concrete situation by rephrasing it as the following principle: if $n \neq 0 \in \mathbb{Z}$, then there is a value of m such that $2^m \mid n$ but $2^{m+1} \nmid m$.[10] Is it a general phenomenon that the (descending) intersection of all powers of a *proper* ideal I in a ring R is zero?[11] As shown in Example 8.4, the ring $R = k[x]/(x^2 - x)$ has a proper ideal $I = ([x])$ such that $I^m = I$ for all $m \geq 0$, so in general we cannot expect this. Krull intersection theorem provides a criterion for when this holds.

Theorem 16.1 (Krull intersection theorem)**.** *Let R be a Noetherian ring and let $I \subseteq J(R) \subset R$ be an ideal contained in the Jacobson ideal (see Definition 3.20), and let M be a finitely generated R-module. Then*

$$\bigcap_{i \geq 0} I^i M = 0.$$

The proof of Theorem 16.1 will be based on the Artin-Rees lemma; we will prove this other remarkable result first, then prove Theorem 16.1, and finally give a first application, which will be needed in the general study of dimensions of Noetherian rings.

16.1. **Ther Artin-Rees lemma.** Before stating the Artin-Rees lemma, it is convenient to introduce a few definitions.

Definition 16.2. Let R be a ring, $I \subseteq R$ an ideal and M an R-module. An *I-filtration* on M is a descending sequence of sub-R-modules

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots$$

such that $M = M_0$ and such that $IM_i \subseteq M_{i+1}$ for $i \geq 0$.
An I-filtration is *I-stable* if there is $\bar{i}$ such that $M_{i+1} = IM_i$ for all $i \geq \bar{i}$.

For example, given R, I, M as in Definition 16.2, one can set $M_i = I^i M$: then one gets an I-stable I-filtration on M; clearly one could also just set $M_i = M$ for all i: this gives an I-filtration on M, which is often not I-stable.
Observe also that if $(M_i)_{i \geq 0}$ is an I-filtration of the R-module M, then for all $i, j \geq 0$ we have $I^j M_i \subseteq M_{i+j}$.

Example 16.3. Let R, I, M as in Definition 16.2 and let $N \subseteq M$ be a sub-R-module. Given an I-filtration $(M_i)_{i \geq 0}$ of M, we can define an I-filtration $(N_i)_{i \geq 0}$ of N by setting $N_i := N \cap M_i$.
If $(M_i)_{i \geq 0}$ is I-stable, then $(N_i)_{\geq 0}$ as above is not necessarily I-stable. For instance, let $R = \mathbb{Z}$, $I = (2)$, $M = \mathbb{Z}[x]$ and let $N \subset M$ be the sub-$\mathbb{Z}$-module spanned by the elements $2^n x^n$, for varying $n \geq 0$; let $M_i = (2)^i M$, so that $(M_i)_{i \geq 0}$ is (2)-stable; then $(2^i)M \cap N$ is spanned over $\mathbb{Z}$ by the elements $2^{\max(i,n)} x^n$, and $(2^{i+1})M \cap N$ is strictly larger than $(2)\big((2^i)M \cap N\big)$, as it contains the element $2^{i+1} x^{n+1}$ (which is in N, but is not divisible by 2 in N).

The Artin-Rees lemma is essentially the statement that what goes wrong in Example 16.3 is that M is not finitely generated.

[10] One says that "2^m exactly divides m", or that "m is the 2-adic evaluation of n".
[11] If $I = R$, the conclusion clearly fails unless R is the zero ring!

Lemma 16.4 (Artin-Rees)**.** *Let R be a Noetherian ring, let $I \subseteq R$ be an ideal, let M be a finitely generated R-module and let $N \subseteq M$ be a sub-R-module. Then there is $\bar{i} \geq 0$ such that for all $i \geq \bar{i}$ we have an equality*

$$I^i M \cap N = I^{i-\bar{i}}(I^i M \cap N).$$

In particular the I-filtration $(I^i M)_{i\geq 0}$ on M restricts to a stable *I-filtration on N.*

Lemma 16.4 is a clever application of Theorem 7.12; let us see how.

Definition 16.5. Let R be a ring and $I \subseteq R$ be an ideal. We definte $R[Ix] \subseteq R[x]$ as the sub-R-algebra containing all polynomials $P = a_n x^n + \cdots + a_0$ such that $a_i \in I^i$ for all $i \geq 0$. Using that I is an ideal, and using the very definition of powers I^i of an ideal I, we obtain that $R[Ix]$ is indeed a subring of $R[x]$, containing R (by convention $I^0 = R$).

Lemma 16.6. *If R is Noetherian and $I \subseteq R$ is an ideal, then $R[Ix]$ is again Noetherian.*

Proof. Let $a_1, \ldots, a_n$ be generators for I; then the R-algebra homomorphism

$$R[y_1, \ldots, y_n] \to R[Ix]$$

sending $y_i \mapsto a_i x$ is surjective; the ring $R[y_1, \ldots, y_n]$ is Noetherian by Theorem 7.12, and hence also its quotient $R[Ix]$ is Noetherian. □

The importance of Definition 16.5 is that an R-module with an I-filtration gives rise to an $R[Ix]$-module as follows.

Definition 16.7. Let R be a ring, $I \subseteq R$ be an ideal, and M an R-module with an I-filtration $(M_i)_{i\geq 0}$. We define an $R[Ix]$-module structure on the direct sum $M_\bullet := \bigoplus_{i\geq 0} M_i$. Given an element m in the summand $M_i \subset M_\bullet$ and given a monomial $ax^j \in R[Ix]$, with $a \in I^j$, we let $ax^j \cdot m$ be the element $am \in I^j M_i \subseteq M_{i+j}$, considered as an element in the summand $M_{i+j} \subseteq M_\bullet$. This assignment extends to a R-bilinear map $R[Ix] \otimes_R M_\bullet \to M_\bullet$, making $M_\bullet$ into a $R[Ix]$-module.

Exercise 16.8. Prove the last statement of Definition 16.7, i.e. prove that Definition 16.7 is a good definition of an $R[Ix]$-module structure on $M_\bullet$.

In the light of Definitions 16.5 and 16.7, it is particularly easy to characterise I-stable filtrations in the context of finitely generated modules over a Noetherian ring.

Proposition 16.9. *Let R be a Noetherian ring, $I \subseteq R$ an ideal and M a finitely generated R-module. Let $(M_i)_{i\geq 0}$ be an I-filtration on M. Then the following are equivalent:*

(1) $(M_i)_{i\geq 0}$ is an I-stable I-filtration;
(2) the $R[Ix]$-module $M_\bullet$ constructed in Definition 16.7 is finitely generated.

Proof. Assume first that $(M_i)_{i\geq 0}$ is I-stable, and let $\bar{i} \geq 0$ be such that $IM_i = M_{i+1}$ for $i \geq \bar{i}$. We claim that the direct sum $\bigoplus_{j=1}^{\bar{i}} M_j$ generates $M_\bullet$ as an $R[Ix]$-module. A generic element in $M_\bullet$ decomposes as a finite sum of elements contained in a single summand M_i, so it suffices to prove that for all $i \geq 0$ and all $m \in M_i$, we can write m as an $R[Ix]$-linear combination of elements in $\bigoplus_{j=1}^{\bar{i}} M_j$; if $i \leq \bar{i}$ this is obvious, and if $i > \bar{i}$ we can use the hypothesis and write $m \in M_i \subseteq M$ as an I-linear

combination of elements of $M_{i-1} \subseteq M$; the same linear combination, multiplied by x, exhibits $m \in M_i \subset M_\bullet$ as an $R[Ix]$-linear combination of elements in M_{i-1}; we conclude by an easy inductive argument.
Hence $\bigoplus_{j=1}^{\bar{i}} M_j$ generates the entire $M_\bullet$ over $R[Ix]$; since R is Noetherian and M is finitely generated over R, every M_j, for $0 \leq j \leq \bar{i}$ is finitely generated over R; choosing finitely many generators for each M_j, and interpreting them as elements of $M_\bullet$, we obtain a finite generating set of $M_\bullet$ over $R[Ix]$.

Assume now that the $R[Ix]$-module $M_\bullet$ is finitely generated; then there is in particular $\bar{i} \geq 0$ such that $\bigoplus_{j=1}^{\bar{i}} M_j$ generates $M_\bullet$ over $R[Ix]$. Let $i > \bar{i}$ and let $m \in M_i$; then we can find indices $0 \leq j_1, \dots, j_n \leq \bar{i}$ (possibly non-distinct), a sequence of elements $m_1, \dots, m_n$ with $m_l \in M_{j_l}$ and polynomials $P_1, \dots, P_n \in R[Ix]$ such that $m = \sum_{l=1}^n P_i m_i$. Up to replacing each P_l with its homogeneous part of degree $i - j_l$, we can assume that $P_l = a_l x^{i-j_l}$ for some $a_l \in I^{i-j_l}$; notice that $i - j_l \geq 1$, as we assume $i > \bar{i} \geq j_l$. Moreover each a_l can be written as a sum of products of the form $b_{l,1} \dots b_{l,i-j_l}$, with $b_{l,1}, \dots, b_{l,i-j_l} \in I$; up to repeating each m_l several times, we may assume that each a_l has the form of a single product $b_{l,1} \dots b_{l,i-j_l}$. We can then write

$$m = \sum_{l=1}^{n} b_{l,1} \cdot (b_{l,2} \dots b_{l,i-j_l} m_l)\,,$$

and since each term in the parenthesis belongs to M_{i-1}, we obtain that $m \in IM_{i-1}$. □

Proof of Lemma 16.4. The I-filtration $(I^i M)_{i \geq 0}$ on M is I-stable, hence by Proposition 16.9 the associated $R[Ix]$-module $M_\bullet$ is finitely generated. We can consider on N the I-filtration $(I^i M \cap N)_{i \geq 0}$, and the associated $R[Ix]$-module $N_\bullet$ can be identified with a sub-$R[Ix]$-module of $M_\bullet$; by Lemma 16.6 we then have that $N_\bullet$ is finitely generated over $R[Ix]$, and by Proposition 16.9 this implies that the I-filtration $(I^i M \cap N)_{i \geq 0}$ on N is I-stable. In other words, there is $\bar{i} \geq 0$ such that for $i \geq \bar{i}$ we have $I(I^{\bar{M}} \cap N) = I^{i+1} M \cap N$, and this is equivalent to saying that for $i \geq \bar{i}$ we have $I^i M \cap N = I^{i-\bar{i}}(I^{\bar{i}} M \cap N)$. □

16.2. **Proof of Krull intersection theorem and an application.** Once Lemma 16.4 has been proved, the proof of Theorem 16.1 becomes quite immediate.

Proof of Theorem 16.1. Consider the sub-R-module $N := \bigcap_{i \geq 0} I^i M \subseteq M$: Lemma 16.4 implies that there is $\bar{i}$ such that for all $i \geq \bar{i}$ we have a chain of inclusions

$$N = I^i M \cap N = I^{i-\bar{i}}(I^{\bar{i}} M \cap N) \subseteq I^{i-\bar{i}} N \subseteq N$$

and thus setting $i = \bar{i} + 1$ we obtain $N = IN$. We can now apply Lemma 14.10 (using again that R is Noetherian and N is finitely generated) to find $a \in R$ with $[a]_I = [1]_I$ and $aN = 0$. The hypothesis $I \subseteq J(R)$ implies that $a \in R^\times$ by Lemma 3.21, and thus we have $N = 0$ as desired. □

Example 16.10. A particular application of Theorem 16.1 is the following: if R is a Noetherian local ring with maximal ideal $\mathfrak{m}$, then $J(R) = \mathfrak{m}$ and thus for any finitely generated R-module M we have $\bigcap_{n \geq 0} \mathfrak{m}^i M = 0$.
An application of the previous remark is the following: if R is a Noetherian domain (not necessarily local!) and $\mathfrak{m}$ is a maximal ideal of R, then $\bigcap_{i \geq 0} \mathfrak{m}^i = 0$. To see this, observe that the localisation map $R \hookrightarrow R_\mathfrak{m}$ is injective, and it restricts for all i

to an injection $\mathfrak{m}^i \hookrightarrow \mathfrak{m}^i R_\mathfrak{m}$, and eventually to an injection $\bigcap_{i\geq 0} \mathfrak{m}^i \hookrightarrow \bigcap_{i\geq 0} \mathfrak{m}^i R_\mathfrak{m}$. The ring $R_\mathfrak{m}$ is local Noetherian with maximal ideal $\mathfrak{m}R_\mathfrak{m}$, so we have by the above remark that $\bigcap_{i\geq 0}(\mathfrak{m}R_\mathfrak{m})^i = \bigcap_{i\geq 0} \mathfrak{m}^i R_\mathfrak{m} = 0$.
We can of course also take any proper ideal I in a Noetherian domain R, and still obtain $\bigcap_{i\geq 0} I^i = 0$ by including I in a maximal ideal $\mathfrak{m}$ and running the previous argument. This generalises the observation about multiples of powers of 2 in $\mathbb{Z}$ at the beginning of the section.

As a final application of Theorem 16.1, which will be needed when studying dimensions of Noetherian rings, we prove the following lemma, preceeded by a definition.

Definition 16.11. Let R be a ring, $\mathfrak{p} \in \operatorname{Spec}(R)$ a prime ideal, and $n \geq 1$. Consider extensions and contractions of ideals with respect to the localisation map $\tau\colon R \to R_\mathfrak{p}$. We denote by $\mathfrak{p}^{(n)}$ the ideal $((\mathfrak{p}^n)^e)^c \subseteq R$, i.e. $\tau^{-1}((\tau(\mathfrak{p}^n)))$; it is called the n^{th} *symbolic power* of $\mathfrak{p}$, and it contains $\mathfrak{p}^n$.

Lemma 16.12. *Let R be a Noetherian ring and let $\mathfrak{p} \subset R$ be a prime ideal; let $\tau\colon R \to R_\mathfrak{p}$ be the localisation map. Then*

$$\ker(\tau) = \bigcap_{i\geq 0} \mathfrak{p}^{(i)}$$

Proof. Let $\mathfrak{m} = \mathfrak{p}^e = \mathfrak{p}R_\mathfrak{p}$ denote the maximal ideal of $R_\mathfrak{p}$, and note that for $i \geq 0$ we have that the ideal $(\mathfrak{p}^i)^e = \mathfrak{p}^i R_\mathfrak{p}$ coincides with $\mathfrak{m}^i$. Since $R_\mathfrak{p}$ is local Noetherian we have by Theorem 16.1 that $\bigcap_{i\geq 0} \mathfrak{m}^i = 0$. We can then write

$$\ker(\tau) = \tau^{-1}(\{0\}) = \tau^{-1}\left(\bigcap_{i\geq 0} \mathfrak{m}^i\right) = \bigcap_{i\geq 0} \tau^{-1}(\mathfrak{m}^i) = \bigcap_{i\geq 0} \mathfrak{p}^{(i)}.$$

□

Exercise 16.13. The ideals $\mathfrak{p}^{(i)}$ as in Definition 16.11 show up also when considering primary decompositions.

- Prove that $\mathfrak{p}^{(i)}$ is a $\mathfrak{p}$-primary ideal (Hint: use Lemma 8.11 and that preimages of primary ideals are again primary).
- Prove that $\mathfrak{p}$ is the only element in $\operatorname{Ass}'(\mathfrak{p}^i)$, and that every minimal primary decomposition of $\mathfrak{p}^i$ has precisely $\mathfrak{p}^{(i)}$ as $\mathfrak{p}$-primary factor.[12]

Beware: in general $\mathfrak{p}^i$ is not itself primary, and $\operatorname{Ass}(\mathfrak{p}^i)$ may contain other (necessarily embedded) prime ideals.

17. Krull dimension theorem

Recall from Definition 9.2 that every ring R has a numerical invariant, $\dim(R) \in \mathbb{N} \cup \{\infty\}$, called the dimension of the ring. We also saw that the Noetherian rings of dimension 0 are precisely the Artinian rings. In this and the following section we ask ourselves, in great generality, how to compute the dimension of a generic ring. The combination of Corollaries 14.5 and 14.7 also shows that if $f\colon R \hookrightarrow S$ is an injective, integral ring homomorphism, then $\dim(R) = \dim(S)$.

[12]This is an instance of a more general fact, that we didn't prove: if I is an ideal in a ring that admits a primary decomposition, then for each $\mathfrak{p} \in \operatorname{Ass}'(I)$ the $\mathfrak{p}$-primary factor of each minimal primary decomposition is the same for all such decompositions, and it agrees with $(I^e)^c$, where extension and contraction are relative to the localisation map $\tau\colon R \to R_\mathfrak{p}$.

Example 17.1. Let k be a field and let R be a finitely generated k-algebra. Then by Lemma 15.5 there exists an injective, integral ring homomorphism $k[y_1, \dots, y_m] \hookrightarrow R$. We then have that $\dim(R) = \dim(k[y_1, \dots, y_m]$, so the computation of dimensions of finitely generated k-algebras reduces to the computation of dimensions of finitely generated polynomial rings over k.
We will moreover see later that $\dim(k[y_1, \dots, y_m]) = m$; thus the number $m \geq 0$ making the statement of Lemma 15.5 hold true for R only depends on R, and it is equal to $\dim(R)$.

Exercise 17.2. Let R, S be rings; prove that $\dim(R \times S) = \max\{\dim(R), \dim(S)\}$.

The Krull dimension theorem will give us means to bound from above the dimension of a ring, using knowledge about how many generators are actually needed to generate its ideals; as the latter condition suggests, the applicability will be restricted to Noetherian rings.

17.1. **Height and coheight.** To give the statement of Krull dimension theorem, let us introduce the notion of *height*, together with the "dual" notion of *coheight*.

Definition 17.3. Let R be a ring.

- For a prime ideal $\mathfrak{p} \subset R$, we define the *height* of $\mathfrak{p}$ as $\mathrm{ht}(\mathfrak{p}) := \dim(R_{\mathfrak{p}}) \in \mathbb{N} \cup \{\infty\}$.
- For a generic *proper* ideal $I \subset R$, we define the height of I, denoted $\mathrm{ht}(I) \in \mathbb{N} \cup \{\infty\}$, as $\min\{\mathrm{ht}(\mathfrak{p}) \mid I \subseteq \mathfrak{p} \in \mathrm{Spec}(R)\}$.
- For a proper ideal $I \subset R$ we define the *coheight* of I, denoted $\mathrm{coht}(I) \in \mathbb{N} \cup \{\infty\}$, as $\dim(R/I)$.

The notions of height and coheight generalise that of dimension: for instance, for a prime ideal $\mathfrak{p} \subset R$, we have that $\mathrm{ht}(\mathfrak{p})$ is the supremum of lengths $l \geq 0$ of proper chains of prime ideals $\mathfrak{p}_0 \subset \dots \mathfrak{p}_l = \mathfrak{p} \subset R$ ending with $\mathfrak{p}$, whereas $\mathrm{coht}(\mathfrak{p})$ is the supremum of lengths $l \geq 0$ of proper chains of prime ideals $\mathfrak{p} = \mathfrak{p}_0 \subset \dots \mathfrak{p}_l \subset R$ beginning with $\mathfrak{p}$. This implies the inequality $\mathrm{ht}(\mathfrak{p}) + \mathrm{coht}(\mathfrak{p}) \leq \dim(R)$, as the first sum is the supremum of lengths of proper chains of prime ideals *passing through* $\mathfrak{p}$.

Exercise 17.4. Prove that for any $I \subset R$ we have $\mathrm{ht}(I) + \mathrm{coht}(I) \leq \dim(R)$ holds.

Observe also that $\mathrm{coht}(\{0\}) = \dim(R)$ and that if R is local with maximal ideal $\mathfrak{m}$, then $\mathrm{ht}(\mathfrak{m}) = \dim(R)$.

Theorem 17.5 (Krull dimension theorem)**.** *Let R be a Noetherian ring and let $I \subset R$ be an ideal. Suppose that I can be generated by r elements; then for every $\mathfrak{p} \in \mathrm{Ass}'(I)$, i.e. for every minimal prime ideal lying over I, we have $\mathrm{ht}(\mathfrak{p}) \leq r$. In particular we have $\mathrm{ht}(I) \leq r$.*

A straigthforward consequence of Theorem 17.5 is that if R is a Noetherian ring and $I \subset R$ is an ideal, then $\mathrm{ht}(I)$ is finite. In particular, if R is a local Noetherian ring with maximal ideal $\mathfrak{m}$, then $\dim(R) = \mathrm{ht}(\mathfrak{m})$ is finite.
In general it is not true that if R is a Noetherian ring, then $\dim(R)$ is finite! In Subsection 17.3 we will discuss the famous example of Nagata.

17.2. **Proof of Krull dimension theorem.** The proof of Theorem 17.5 is a bit technical and is preceeded by the following proposition.

Proposition 17.6. *Let R be a Noetherian domain and let $a \in R$ be an element which is neither 0 nor invertible. Let $\mathfrak{p} \in \mathrm{Ass}'((a))$ be a minimal prime ideal containing (a). Then* $\mathrm{ht}(\mathfrak{p}) = 1$.

Proof. The proper chain of prime ideals $(0) \subset \mathfrak{p}$ shows that $\mathrm{ht}(\mathfrak{p}) \geq 1$. To prove equality, we need to show that the only prime ideal properly contained in $\mathfrak{p}$ is (0). We can localise R at the prime ideal $\mathfrak{p}$: by doing so, we still have a Noetherian domain $R_{\mathfrak{p}}$ and we still have that $\frac{a}{1}$ is neither zero (for the localisation map is injective, R being a domain) nor invertible (for $a \in \mathfrak{p}$ is sent inside $\mathfrak{p}R_{\mathfrak{p}}$ along the localisation map) in $R_{\mathfrak{p}}$; by Proposition 5.4 all prime ideals contained in $\mathfrak{p}$ are witnessed by prime ideals of $R_{\mathfrak{p}}$.
So it is no harm to *replace* R by $R_{\mathfrak{p}}$, or equivalently, assume that R is *already* a local ring, that $\mathfrak{p}$ is its maximal ideal, and that $\mathfrak{p}$ is minimal among prime ideals lying over (a). Under this extra assumption, we have that $\mathfrak{p}$ is in fact the *unique* prime ideal of R containing (a), for any other prime ideal $(a) \subseteq \mathfrak{p}' \subset R$ would be contained in $\mathfrak{p}$, the unique maximal ideal of R, and thus would prevent $\mathfrak{p}$ from being a minimal prime ideal containing (a). It follows that $R/(a)$ is a Noetherian ring of dimension 0 (it has exactly one prime ideal), and by Theorem 9.1 we have that $R/(a)$ is Artinian; this has a consequence also for the ring R: every descending chain of ideals of R *that contain* (a) stabilises.
Let now $\mathfrak{p}_0 \subset R$ be a prime ideal strictly contained in $\mathfrak{p}$; as observed above, $a \notin \mathfrak{p}_0$. We can consider the descending chain of ideals $I_i := \mathfrak{p}_0^{(i)} + (a)$, where we consider the i^{th} symbolic power of $\mathfrak{p}_0$, as in Definition 16.11. In particular, recall from Exercise 16.13 that $\mathfrak{p}_0^{(i)}$ is a $\mathfrak{p}_0$-primary ideal. All ideals I_i contain (a), and so we can find $\bar{i} \geq 0$ such that for all $i \geq \bar{i}$ we have $\mathfrak{p}_0^{(i)} + (a) = \mathfrak{p}_0^{(\bar{i})} + (a)$. Let us also assume $\bar{i} \geq 1$.
We claim that for all $i \geq \bar{i}$ we have $\mathfrak{p}_0^{(\bar{i})} = \mathfrak{p}_0^{(i)} + a\mathfrak{p}_0^{(\bar{i})}$. The inclusion $\mathfrak{p}_0^{(\bar{i})} \supseteq \mathfrak{p}_0^{(i)} + a\mathfrak{p}_0^{(\bar{i})}$ is evident. For the other inclusion, let $b \in \mathfrak{p}_0^{(\bar{i})} \subset I_{\bar{i}}$; then $b \in I_i$ so we can find $c \in \mathfrak{p}_0^{(i)} \subseteq \mathfrak{p}_0^{(\bar{i})}$ and $d \in R$ with $b = c + ad$; it follows that $b - c = ad \in \mathfrak{p}_0^{(\bar{i})}$, and since $\mathfrak{p}_0^{(\bar{i})}$ is $\mathfrak{p}_0$-primary and $a \notin \mathfrak{p}_0$, we must have $d \in \mathfrak{p}_0^{(\bar{i})}$; this implies that $b \in \mathfrak{p}_0^{(i)} + a\mathfrak{p}_0^{(\bar{i})}$, completing the proof of the claim.
Since $a \in \mathfrak{p}$, the equality $\mathfrak{p}_0^{(\bar{i})} = \mathfrak{p}_0^{(i)} + a\mathfrak{p}_0^{(\bar{i})}$ implies the equality $\mathfrak{p}_0^{(\bar{i})} = \mathfrak{p}_0^{(i)} + \mathfrak{p}\mathfrak{p}_0^{(\bar{i})}$ for all $i \geq \bar{i}$; we can now set $M = \mathfrak{p}_0^{(\bar{i})}$ and $N = \mathfrak{p}_0^{(i)} \subseteq N$, and apply Corollary 14.12 to conclude that $\mathfrak{p}_0^{(\bar{i})} = \mathfrak{p}_0^{(i)}$ for all $i \geq \bar{i}$.
And now it is time to invoke Lemma 16.12: the kernel of the localisation map $R \to R_{\mathfrak{p}_0}$ is trivial, since R is a domain, and hence $\bigcap_{i \geq 0} \mathfrak{p}_0^{(i)} = 0$; by the above, the previous intersection is equal to $\mathfrak{p}_0^{(\bar{i})}$, which is therefore zero. Taking radicals, and remembeding again that we are in a domain, we have $\mathfrak{p}_0 = \sqrt{\mathfrak{p}_0^{(\bar{i})}} = \sqrt{(0)} = 0$ as desired. □

Proof of Theorem 17.5. We proceed by induction on the number $r \geq 0$ of elements used to generate $I \subseteq R$. For $r = 0$ we have $I = (0)$, and any minimal prime ideal $\mathfrak{p} \subset R$ (i.e. any $\mathfrak{p} \in \mathrm{Ass}'(0)$) has height 0.
Let now $r \geq 1$ and let $a_1, \ldots, a_r \in I$ be generators of I. Let moreover $\mathfrak{p} \in \mathrm{Ass}'(I)$ be a minimal prime ideal containing I; we want to prove that $\mathrm{ht}(\mathfrak{p}) \leq r$; for this aim, let $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_t = \mathfrak{p}$ be a proper chain of prime ideals of some length $t \geq 0$

ending with $\mathfrak{p}$: the supremum of t for varying chain gives $\mathrm{ht}(\mathfrak{p})$, and hence we want to prove that $t \leq r$.
For this aim, we can again replace R by $R_{\mathfrak{p}}$, replace I by $IR_{\mathfrak{p}}$ (which can be generated by the r elements $\frac{a_i}{1}$), and consider the proper chain of prime ideals $\mathfrak{p}_0 R_{\mathfrak{p}} \subset \cdots \subset \mathfrak{p}_t R_{\mathfrak{p}} = \mathfrak{p} R_{\mathfrak{p}}$. We still want to prove the inequality $t \leq r$. Just as in the proof of Proposition 17.6, we will henceforth assume that R is already a local ring with maximal ideal $\mathfrak{p}$, and that $\mathfrak{p}$ is minimal among prime ideals containing I.
If $t = 0$, the inequality $t \leq r$ is evident, so let us assume $t \geq 1$. We also want to assume that there is no prime ideal $\mathfrak{q}$ with $\mathfrak{p}_{t-1} \subset \mathfrak{q} \subset \mathfrak{p}$, i.e. $\mathfrak{p}_{t-1}$ is maximal among prime ideals strictly contained in $\mathfrak{p}$. To achieve this situation, we consider the family Σ of all prime ideals $\mathfrak{q}$ with $\mathfrak{p}_{t-1} \subseteq \mathfrak{q} \subset \mathfrak{p}$; since R is Noetherian we may find a maximal $\mathfrak{q} \in \Sigma$, and then we may replace $\mathfrak{p}_{t-1}$ by $\mathfrak{q}$ in our original proper chain of prime ideals. Henceforth we assume that there is no prime ideal strictly between $\mathfrak{p}_{t-1}$ and $\mathfrak{p}$.
Since $\mathfrak{p}$ is minimal among prime ideals containing I, and since $\mathfrak{p}$ is now assumed maximal, we have that $\mathfrak{p}$ is in fact the *unique* prime ideal of R containing I; in particular $I \nsubseteq \mathfrak{p}_{t-1}$. This has two interesting consequences: first, by Proposition 3.19 we have $\mathfrak{p} = \sqrt{I}$; second, at least one of the generators of I is not in $\mathfrak{p}_{t-1}$, and without loss of generality we may assume that $a_r \notin \mathfrak{p}_{t-1}$.
Consider now the ideal $J = (a_r) + \mathfrak{p}_{t-1}$; then every prime ideal containing J is a prime ideal strictly larger than $\mathfrak{p}_{t-1}$, yet contained in the unique maximal ideal $\mathfrak{p}$: by our assumption it follows that $\mathfrak{p}$ is the unique prime ideal containing J, and in particular $\sqrt{J} = \mathfrak{p}$. Since $I \subseteq \mathfrak{p}$, each generator a_i of I admits a power in J; in particular there are exponents $n_1, \ldots, n_{r-1} \geq 0$, elements $a'_1, \ldots, a'_{r-1} \in \mathfrak{p}_{t-1}$ and elements $b_1, \ldots, b_{r-1} \in R$ such that $a_i^{n_i} = a'_i + b_i a$.
Let now $I' = (a'_1, \ldots, a'_{r-1})$; by construction I' can be generated by $r-1$ elements, and it is contained in $\mathfrak{p}_{t-1}$; moreover we have $I^n \subset I' + (a_r)$ for n large enough, say $n = \sum_{i=1}^{r-1} n_i$ (compare with Exercise 8.19). Let finally $\mathfrak{p}'$ be a minimal prime ideal among the prime ideals containing I' and contained in $\mathfrak{p}_{t-1}$ (the existence of such $\mathfrak{p}'$ is guaranteed by the inclusion $I' \subseteq \mathfrak{p}_{t-1}$); then we have a chain of inclusions

$$\mathfrak{p} = \sqrt{I} = \sqrt{I^n} \subseteq \sqrt{I' + (a_r)} \subseteq \sqrt{\mathfrak{p}' + (a_r)} \subseteq \sqrt{\mathfrak{p}_{t-1} + (a_r)} \subseteq \mathfrak{p}$$

which has to be a chain of equalities. In particular we have that $\mathfrak{p}$ is the unique prime ideal containing $\mathfrak{p}' + (a_r)$. Consider now the ring $R/\mathfrak{p}'$: it is a local domain with maximal ideal $\mathfrak{p}/\mathfrak{p}'$, and it contains an element $[a_r]_{\mathfrak{p}'}$ which is neither zero (for $a_r \notin \mathfrak{p}_{t-1} \supseteq \mathfrak{p}'$) nor a unit (for $a_r \in \mathfrak{p}$, so $[a_r]_{\mathfrak{p}'} \in \mathfrak{p}/\mathfrak{p}'$). By Proposition 17.6 evert minimal prime ideal in $R/\mathfrak{p}'$ that contains $[a_r]_{\mathfrak{p}'}$ has height 1: in fact $\mathfrak{p}/\mathfrak{p}'$ is the unique such prime ideal, yet we have a chain of inclusions of prime ideals $\mathfrak{p}'/\mathfrak{p}' \subseteq \mathfrak{p}_{t-1}/\mathfrak{p}' \subset \mathfrak{p}/\mathfrak{p}'$. We conclude that the first inclusion must be an equality, i.e. $\mathfrak{p}' = \mathfrak{p}_{t-1}$.
And now we may apply the inductive hypothesis: $\mathfrak{p}_{t-1} = \mathfrak{p}'$ is a minimal prime ideal containing I', which is an ideal generated by $r-1$ elements; it follows that $t - 1 \leq \mathrm{ht}(\mathfrak{p}_{t-1}) = \mathrm{ht}(\mathfrak{p}') \leq r - 1$, finally proving that $t \leq r$. □

We will see many applications of Theorem 17.5 in the next section.

17.3. **The counterexample of Nagata.** Let k be a field and let $\mathcal{I} \subset \mathbb{N}^2$ be the set of pairs (i, j) with $i \geq j \geq 0$. Consider the polynomial ring $R = k[x_{i,j} \mid (i, j) \in \mathcal{I}]$;

for each $i \geq 0$ let $\mathfrak{p}_i \subset R$ be the prime ideal $\mathfrak{p}_i = (x_{i,1}, x_{i,2}, \ldots, x_{i,i})$. Let $T \subset R$ be the complement in R of the union $\bigcup_{i\geq 0} \mathfrak{p}_i$.

Lemma 17.7. *The subset $T \subset R$ is a multiplicative subset of R.*

Proof. We have $1 \in T$, as 1 belongs to no prime ideal; moreover if $P, Q \in R$ are polynomials belonging to T, then $P, Q \notin \mathfrak{p}_i$ for all $i \geq 0$, hence $PQ \notin \mathfrak{p}_i$ for all $i \geq 0$, and thus $PQ \in T$. □

We now consider the ring R_T; we claim that this ring is Noetherian, and yet $\dim(R_T) = \infty$. The fact that $\dim(R_T) = \infty$ is relatively easy: for each $i \geq 0$ we can produce a proper chain of prime ideals of length $i + 1$ in R by taking

$$(0) \subset (x_{i,0}) \subset (x_{i,0}, x_{i,1}) \subset \cdots \subset (x_{i,0}, x_{i,1}, \ldots, x_{i,i-1}) \subset \mathfrak{p}_i;$$

all prime ideals in the chain are disjoint from T, and hence by Proposition 5.4 the extended prime ideals form a chain of length $i + 1$ in R_T. Since i is arbitrary, this shows that $\dim(R_T) = \infty$.
The difficult part is of course to prove that R_T is Noetherian.

Lemma 17.8. *Let Σ be the collection of ideals of R that are disjoing from T; then the prime ideals $\mathfrak{p}_i$, for varying $i \geq 0$, are precisely all maximal elements with respect to inclusion in Σ.*

Proof. We observe that $P \in R$ does not belong to $\mathfrak{p}_i$ if and only if at least one monomial of P is a product of an element of $k^\times$ and variables $x_{i',j}$ for varying $i' \neq i$ and $0 \leq j \leq i'$. In particular every polynomial in R with non-vanishing constant term belongs to T.
We use this to prove that each $\mathfrak{p}_i$ is maximal among ideals that are disjoint from T: indeed for any proper inclusion of ideals $\mathfrak{p}_i \subset I$ we can pick $P \in I \setminus \mathfrak{p}_i$; then P has at least one monomial containing only variables $x_{i',j}$ with $i' \neq i$; summing a suitable k-multiple of $x_{i,0} \in \mathfrak{p}_i \subset I$, we obtain that $P' = P + \lambda x_{i,0} \in I$ is a polynomial with at least one monomial witnessing that $P' \notin \mathfrak{p}_i$, and at least one monomial (the one we added) witnessing that $P' \notin \mathfrak{p}_{i'}$ for any $i' \neq i$, i.e. $P' \in T$.
Conversely, let $I \subset R$ be any ideal, and assume that $I \cap T = \emptyset$; for any $P \in I$ let $s(P) \subset \mathbb{N}$ be the subset of all $i \geq 0$ such that $P \in \mathfrak{p}_i$, and let $s(I) = \{s(P) \mid P \in I\}$ be the family of all $s(P)$ for $P \in I$. We observe that $s(I)$ consists of $\mathbb{N} = s(0)$ and of finite subsets, as each $0 \neq P \in I$ has at least a non-trivial monomial, containing finitely many variables and thus witnessing that $P \notin \mathfrak{p}_i$ for almost all $i \geq 0$. The hypothesis $I \cap T = \emptyset$ implies that $\emptyset \notin s(I)$. Moreover, if $P, P' \in I$ are polynomials, we can find an exponent $e \geq 0$ such that the sum of the elements P^e and P' has no cancellation among monomials of P^e and monomials of P' (here we use that P has vanishing constant term), so that $s(P^e + P') = s(P) \cap s(P')$. This implies that $s(I)$ has a unique minimal element with respect to inclusion: if $I = \{0\}$, then $s(I) = \{\mathbb{N}\}$ so $\mathbb{N}$ is the unique minimal element; otherwise $s(I)$ contains some finite set and there is a unique set of minimal cardinality, which is also the unique minimum of $s(I)$ with respect to inclusion.
This minimum is non-empty, and this shows that there is $i \geq 0$ such that each $s(P)$ contains i, i.e. $P \in \mathfrak{p}_i$ for all $P \in I$. □

Applying Lemma 5.1 and Proposition 5.4, we obtain that the extended ideals $\mathfrak{m}_i := \mathfrak{p}_i^e = \mathfrak{p}_i R_T \subset R_T$ are precisely all maximal ideals of R_T. We also observe that the

localisations $(R_T)_{\mathfrak{m}_i}$ coincide with $R_{\mathfrak{p}_i}$, and we have

$$(R_T)_{\mathfrak{m}_i} \cong R_{\mathfrak{p}_i} \cong k(x_{i',j} \,|\, (i',j) \in \mathcal{I}, i' \neq i)[x_{i_0}, x_{i,1}, \dots, x_{i,i}]_{(x_{i_0}, x_{i,1}, \dots, x_{i,i})};$$

The latter is a Noetherian ring: indeed $k(x_{i',j} \,|\, (i',j) \in \mathcal{I}, i' \neq i)$ is a field, and we are taking a localisation of a finitely generated algebra over this field, which is Noetherian by Theorem 7.12 and Lemma 7.6.
Of course we remember Exercise 7.11, so we are not tempted to conclude that R_T is Noetherian just because all of its localisations at maximal ideals are Noetherian. So let $I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$ be an ascending chain of ideals in R_T; without loss of generality, we can assum $I_0 \neq \{0\}$, and pick $0 \neq P \in I_0$; then the set $s(P)$, as in the proof of Lemma 17.8, is finite.
For each $i \in s(P)$ we can identify the ascending chain of extended ideals $I_0(R_T)_{\mathfrak{m}_i} \subseteq I_1(R_T)_{\mathfrak{m}_i} \subseteq \dots$ with the ascending chain of $(R_T)_{\mathfrak{m}_i}$-modules $(I_0)_{\mathfrak{m}_i} \subseteq (I_1)_{\mathfrak{m}_i} \subseteq \dots$; since $(R_T)_{\mathfrak{m}_i}$ is Noetherian, this sequence stabilises, i.e. there is $\bar{j}_i \geq 0$ such that for each $j \geq \bar{j}_i$ the inclusion $I_{\bar{j}_i} \subseteq I_j$ becomes a bijection $(I_{\bar{j}_i})_{\mathfrak{m}_i} \cong (I_j)_{\mathfrak{m}_i}$ after localisation.
Let now $\bar{j} = \max \bar{j}_i \,|\, i \in s(P)$: we claim that for all $j \geq \bar{j}$ the inclusion $I_{\bar{j}} \subseteq I_j$ is... surjective, that is it is a bijection; we can check this after localisation at *all* maximal ideals of R_T, thanks to Corollary 6.11. For $i \in s(P)$ this is immediate, by how we defined $\bar{j}$. For $i \notin s(P)$ the situation is even better: the chain of inclusions $I_{\bar{j}} \subseteq I_j \subseteq R_T$ becomes a chain of bijections after localisation at $\mathfrak{m}_i$, since $P \notin \mathfrak{m}_i$ but $P \in I_{\bar{j}}$; here we appeal to Lemma 5.1.

18. Applications of Krull dimension theorem

In this last section we see some applications of the Krull dimension theorem.

18.1. **Bound on dimension of local rings.** The first immediate consequence of Theorem 17.5 is that every ideal I in a Noetherian ring R has finite height: already this simple statement is not completely obvious before proving Theorem 17.5. In the case of a local ring we obtain the following.

Corollary 18.1. *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Then $\dim(R) \leq \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$. In particular $\dim(R)$ is finite.*

Proof. Corollary 14.13 implies that $\mathfrak{m}$ can be generated by $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$-many elements, and the statement follows by applying Theorem 17.5 to the ideal $\mathfrak{m}$, using that $\mathrm{ht}(\mathfrak{m}) = \dim(R)$. □

Already the fact that the dimension of a Noetherian *local* ring is finite is not completely obvious a priori: the example of Nagata from Subsection 17.3 shows that (non-local) Noetherian rings may have infinite dimension.

Example 18.2. In general, for a local Noetherian ring R with maximal ideal $\mathfrak{m}$, we may have $\dim(R) < \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$. For instance let k be a field and let $R = k[x^2, x^3]_{(x^2,x^3)}$. Then the maximal ideal (x^2, x^3) of $k[x^2, x^3]$ cannot be generated by less than 2 elements, and similarly the extended ideal (x^2, x^3) of R needs at least two generators. To prove this formally, use Corollary 14.13 and notice that $(x^2, x^3)/(x^2, x^3)^2$ is 2-dimensional over $R/(x^2, x^3)$, generated by the vectors $[x^2]$ and $[x^3]$.

Yet $\dim(R) = 1$, since the normalisation of R is $k[x]$, which is a PID and has therefore dimension 1, and $\dim(R) = \dim(k[x])$ by combining Corollaries 14.5 and 14.7.

Exercise 18.3. Let k be a field, let $n \geq 3$ and let $R = k[x_1, \ldots, x_n]/(x_1^2 + \cdots + x_n^2)$. Prove that $\dim(R) = n - 1$, yet for the maximal ideal $\mathfrak{m} = (x_1, \ldots, x_n) \subset R$ we have $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = 0$.

Example 18.2 and Exercise 18.3 motivate the following definition.

Definition 18.4. A local Noetherian ring R with maximal ideal $\mathfrak{m}$ is *regular* if $\dim(R) = \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$; equivalently, using Corollary 14.13, if $\mathfrak{m}$ can be generated by exactly (i.e. no more than) $\dim(R)$-many elements.

18.2. **Krull principal ideal theorem.** In the case of a principal ideal $(a) \subset R$, Krull dimension theorem tells us that $\mathrm{ht}((a)) \leq 1$. The inequality can be strict (for instance if $a = 0$), but under suitable assumptions on a we have an equality, as in the following theorem.

Theorem 18.5 (Krull principal ideal theorem)**.** *Let R be a Noetherian ring and let $a \in R$ be an element which is neither invertible nor a zero-divisor. Then* $\mathrm{ht}((a)) = 1$.

Proof. We have to show that $\mathrm{ht}((a)) \geq 1$; the opposite statement is $\mathrm{ht}(a) = 0$, i.e. there is some prime ideal $\mathfrak{p} \supseteq (a)$ with $\mathrm{ht}(\mathfrak{p}) = 0$. We then have that $\mathfrak{p}$ is a minimal prime in the ring R, i.e. it is one of the prime ideals in $\mathrm{Ass}'((0))$. Let therefore $\mathrm{Ass}'((0)) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, and assume $\mathfrak{p} = \mathfrak{p}_1$. We have $\sqrt{(0)} = \bigcap_{i=1}^r \mathfrak{p}_i$, and since R is Noetherian there is $n \geq 1$ large enough so that $(\bigcap_{i=1}^r \mathfrak{p}_i)^n = (0)$, and hence also $\prod_{i=1}^r \mathfrak{p}_i^n = 0$. Now this implies that a is a zero-divisor: indeed the product $\prod_{i=2}^r \mathfrak{p}_i^n$ doesn't vanish (otherwise $\mathfrak{p}_1$ would not be in $\mathrm{Ass}'(0)$), and there is a minimal $1 \leq j \leq n$ with $\mathfrak{p}_1^j \prod_{i=2}^r \mathfrak{p}_i^n = 0$; then for any $0 \neq b \in \mathfrak{p}_1^{j-1} \prod_{i=2}^r \mathfrak{p}_i^n = 0$ we have $ab = 0$. □

18.3. **Parameters in a local ring.** Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$. From Example 18.2 and Exercise 18.3 we see that, in general, we cannot expect that $\mathfrak{m}$ be generated by only $\dim(R)$-many elements. We can nevertheless hope that equality in Krull dimension theorem holds at least for some other ideal of R: in particular, if $I \subset R$ is an $\mathfrak{m}$-primary ideal (which, by Lemma 8.11, is the same as saying that I is such that $\sqrt{I} = \mathfrak{m}$), we can ask whether I can be generated by $\mathrm{ht}(I)$-many elements; and by the very definition of height, since $\mathfrak{m}$ is the unique prime ideal containing I, we have $\mathrm{ht}(I) = \mathrm{ht}(\mathfrak{m}) = \dim(R)$.

Definition 18.6. Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$. A set of elements $a_1, \ldots, a_d \in \mathfrak{m}$ is called a *system of parameters* for R if $d = \dim(R)$ and the ideal $I := (a_1, \ldots, a_d)$ is $\mathfrak{m}$-primary, i.e. $\mathfrak{m}$ is the unique minimal prime ideal lying over I, i.e. $\mathrm{ht}(I) = \mathrm{ht}(\mathfrak{m}) = d$.

We will see that every Noetherian local ring R admits a system of parameters; in particular $\dim(R)$ is equal to the minimum number $d \geq 0$ such that there is some $\mathfrak{m}$-primary ideal generated by exactly d elements, where $\mathfrak{m}$ is the maximal ideal of R. This gives a new characterisation of the dimension of Noetherian local rings, which was originally defined in terms of proper chains of prime ideals. In particular we have the following, for a local Noetherian ring R:

- for every $\mathfrak{m}$-primary ideal $I = (a_1, \dots, a_r)$ and every proper chain of prime ideals $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_l$ we have $l \leq r$;
- for a suitable choice of I and of the chain of prime ideals, equality holds.

In particular one can *prove* that a given Noetherian local ring R has dimension precisely $d \geq 0$ by *exhibiting* an $\mathfrak{m}$-primary ideal generated by d elements and a proper chain of prime ideals of length d.

Example 18.7. Let us prove again that $\dim(k[x^2, x^3]_{(x^2,x^3)} = 1$: the chain of ideals $(0) \subset (x^2, x^3)$ has length 1, and the ideal (x^2) is (x^2, x^3)-primary and is generated by 1 element.

The existence of a system of parameters will follow from the following more general proposition, which is a sort of converse of Theorem 17.5.

Proposition 18.8. *Let R be a Noetherian ring, let $I \subset R$ be an ideal, and let $r := \operatorname{ht}(I)$ (which is finite by Theorem 17.5). Let $1 \leq s \leq r$ and let $a_1, \dots, a_{s-1} \in I$ be elements such that $\operatorname{ht}((a_1, \dots, a_{s-1}) = s-1$ (the inequality $\geq$ always holds by Theorem 17.5). Then there exists a further element $a_s \in I$ such that $\operatorname{ht}((a_1, \dots, a_s)) = s$. In particular, there are elements $a_1, \dots, a_r \in I$ such that $\operatorname{ht}((a_1, \dots, a_r)) = r = \operatorname{ht}(I)$.*

The proof of Proposition 18.8 is subject to the following basic lemma, which is a counterpart to Lemma 8.3.

Lemma 18.9. *Let R be a ring, $I \subset R$ an ideal and $\mathfrak{p}_1, \dots, \mathfrak{p}_n \in \operatorname{Spec}(R)$ be prime ideals, for some $n \geq 1$. Assume that I is contained in the set $\bigcup_{i=1}^n \mathfrak{p}_i$ (which is not necessarily an ideal). Then there is $1 \leq i \leq n$ such that $I \subseteq \mathfrak{p}_i$.*

Proof. We proceed by induction over n. If $n = 1$ the statement is obvious. Assume now $n \geq 2$. If there exists an index $1 \leq j \leq n$ such that $I \subseteq \bigcup_{i \neq j} \mathfrak{p}_i$, we may reduce our collection of prime ideals and apply the inductive hypothesis to find an index $i \neq j$ such that $I \subseteq \mathfrak{p}_i$.
Let us therefore assume that for all $1 \leq j \leq n$ we have $I \nsubseteq \bigcup_{i \neq j} \mathfrak{p}_i$, and find a contradiction. We can pick elements $a_j \in I \setminus \bigcup_{i \neq j} \mathfrak{p}_i$, for $1 \leq j \leq n$; we must have $a_j \in \mathfrak{p}_j$. For all $1 \leq l \leq n$ we then have that the product $b_l := \prod_{j \neq l} a_j$ belongs to I, belongs to $\mathfrak{p}_i$ for $i \neq l$, and doesn't belong to $\mathfrak{p}_l$. It follows that the sum $\sum_{l=1}^n b_l$ is an element in I which doesn't belong to any of the ideals $\mathfrak{p}_i$. □

Proof of Proposition 18.8. Let $\operatorname{Ass}'((a_1, \dots, a_{s-1}) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ be the set of minimal prime ideals lying over $(a_1, \dots, a_{s-1})$. By Theorem 17.5 we have $\operatorname{ht}(\mathfrak{p}_i) \leq s-1$, and by the hypothesis $\operatorname{ht}((a_1, \dots, a_{s-1})) = s-1$ we have in fact $\operatorname{ht}(\mathfrak{p}_i) = s-1$ for all $1 \leq i \leq n$. Since $\operatorname{ht}(I) = r > s-1$, we must have that I is not contained in any of the prime ideals $\mathfrak{p}_i$; it follows from Lemma 18.9 that $I \nsubseteq \bigcup_{i=1}^n \mathfrak{p}_i$, and so we may pick an element $a_s \in I \setminus \bigcup_{i=1}^n \mathfrak{p}_i$. Then every prime ideal $\mathfrak{p}$ containing $(a_1, \dots, a_s)$ is not one of the ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$, yet since $\mathfrak{p} \supseteq (a_1, \dots, a_{s-1})$ we have that $\mathfrak{p} \supseteq \mathfrak{p}_i$ for some $1 \leq i \leq n$, and this implies that $\operatorname{ht}(\mathfrak{p}) \geq s$, so that $\operatorname{ht}((a_1, \dots, a_s)) \geq s$; again by Theorem 17.5 we have $\operatorname{ht}((a_1, \dots, a_s)) = s$. □

Once Proposition 18.8 is proved, we can apply it to the case of a Noetherian local ring R with maximal ideal $\mathfrak{m}$: if $\dim(R) = d \geq 0$, we can find elements $a_1, \dots, a_d \in \mathfrak{m}$ such that the ideal $I := (a_1, \dots, a_d)$ satisfies $\operatorname{ht}(I) = d$; by definition of height of an ideal, it follows that every prime ideal $\mathfrak{p}$ containing I has height $\geq d$; since

$\mathfrak{p} \subseteq \mathfrak{m}$ and $\mathrm{ht}(\mathfrak{m}) = \dim(R) = d$, we must have $\mathfrak{p} = \mathfrak{m}$, i.e. $\mathfrak{m}$ is the unique prime ideal containing I. It follows that $\sqrt{I} = \mathfrak{m}$, i.e. I is $\mathfrak{m}$-primary.

Corollary 18.10. *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$ and let $a_1, \dots, a_r \in \mathfrak{m}$. Then $\dim(R/(a_1, \dots, a_r)) \geq \dim(R) - r$.*

Proof. Let $I = (a_1, \dots, a_r)$, and consider the ring R/I: it is again local, with maximal ideal $\mathfrak{m}/I$, so we can find by Proposition 18.8 a system of parameters $[c_1]_I, \dots, [c_s]_I \in R/I$, where $s = \dim(R/I)$. The ideal $([c_1]_I, \dots, [c_s]_I)$ is $\mathfrak{m}/I$-primary, i.e. $\mathfrak{m}/I$ is the only prime ideal lying over it; pulling back to R, we obtain that the ideal $(a_1, \dots, a_r, c_1, \dots, c_s)$ is $\mathfrak{m}$-primary, as $\mathfrak{m}$ is the only prime ideal containing it. It follows from Theorem 17.5 that $r + s \geq \dim(R)$, i.e. $\dim(R/I) \geq \dim(R) - r$. □

We can combine Theorem 18.5 and Corollary 18.10 to prove the following corollary.

Corollary 18.11. *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$, and let $a \in \mathfrak{m}$. Then $\dim(R/(a)) = \dim(R) - 1$.*

Proof. Theorem 18.5 implies that $\mathrm{ht}((a)) = 1$, and the inequality $\mathrm{ht}((a)) + \mathrm{coht}((a)) \leq \dim(R)$ translates to $\dim(R/(a)) \leq \dim(R) - 1$. Viceversa, Corollary 18.10 implies that $\dim(R/(a)) \geq \dim(R) - 1$. □

In fact, we can improve Proposition 18.8 to the following in the case of a local ring.

Proposition 18.12. *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$, and let $0 \leq r \leq d := \dim(R)$. Let $a_1, \dots, a_r \in \mathfrak{m}$. Then the following are equivalent:*

1. *there exist $a_{r+1}, \dots, a_d \in \mathfrak{m}$ such that $a_1, \dots, a_d$ are a system of parameters for R;*
2. *$\dim(R/(a_1, \dots, a_r)) = d - r$.*

Proof. Assume first (1), let $I = (a_1, \dots, a_r)$ and let $\mathfrak{q} = (a_1, \dots, a_d)$, which is $\mathfrak{m}$-primary; passing to the quotient by I, we have that $\mathfrak{q}/I = ([a_{r+1}]_I, \dots, [a_d]_I) \subset R/I$ is a $\mathfrak{m}/I$-primary in the Noetherian local ring R/I; since $\mathfrak{q}/I$ is generated by $d - r$ elements, we obtain $\dim(R/I) \leq d - r$ by Theorem 17.5; the inequality $\dim(R/I) \geq d - r$ follows from Corollary 18.10.

Assume now (2), and let again $I = (a_1, \dots, a_r)$. By Proposition 18.8 we can find a system of parameters $[c_{r+1}]_I, \dots, [c_d]_I \in \mathfrak{m}/I$ for R/I, and as in the proof of Corollary 18.10 we have that $\mathfrak{q} := (a_1, \dots, a_r, c_{r+1}, \dots, c_d) \subset R$ is an $\mathfrak{m}$-primary ideal, as $\mathfrak{m}$ is the only prime ideal containing it. By definition, this means that $a_1, \dots, a_r, c_{r+1}, \dots, c_d$ is a system of parameters for R. □

18.4. **Dimension of polynomial rings.** We can now compute the dimension of polynomial rings over a generic ring.

Proposition 18.13. *Let R be a Noetherian ring and let $n \geq 0$. Then*

$$\dim(R[x_1, \dots, x_n]) = \dim(R) + n.$$

Proof. For $n = 0$ there is nothing to prove. For $n = 1$, the inequality $\dim(R[x]) \geq \dim(R) + 1$ was already proved in Example 9.4. For the other inequality, let $\mathfrak{m}$ be a maximal ideal of $R[x]$ and let $\mathfrak{p} = \mathfrak{m} \cap R \in \mathrm{Spec}(R)$; it suffices to prove that $\mathrm{ht}(\mathfrak{m}) \leq \mathrm{ht}(\mathfrak{p}) + 1$, where the two heights are computed with respect to the two rings $R[x]$ and R, respectively. We observe that the multiplicative subset

$T := R \setminus \mathfrak{p} \subset R \subset R[x]$ is disjoint from $\mathfrak{m}$, so we may replace R by $R_T = R_{\mathfrak{p}}$, replace $R[x]$ by $R[x]_T \cong R_{\mathfrak{p}}[x]$, replace $\mathfrak{m}$ by the extended ideal $\mathfrak{m}R_{\mathfrak{p}}[x]$ (which is again maximal and has same height as $\mathfrak{m}$), and replace similarly $\mathfrak{p}$ by $\mathfrak{p}R_{\mathfrak{p}}$ (also these two ideals have the same height in their respective rings). We may thus assume that $\mathfrak{p}$ is *already* maximal in R, and in fact we may assume that R is local Noetherian with maximal ideal $\mathfrak{p}$.
Observe now that $\mathfrak{p}R[x]$ is a prime ideal in $R[x]$, as the quotient $R[x]/\mathfrak{p}R[x] \cong R/\mathfrak{p}[x]$ is a domain. In fact, $R/\mathfrak{p}$ is a field, and hence $R/\mathfrak{p}[x]$ is a principal ideal domain. It follows that the maximal ideal $\mathfrak{m}/\mathfrak{p}R[x] \subset R/\mathfrak{p}[x]$ is a principal ideal, generated by some class $[P]_{\mathfrak{p}R[x]}$; it further follows that $\mathfrak{m}$ is generated by $\mathfrak{p} \subset R$ together with $P \in R[x]$.
Since R is local Noetherian, by Proposition 18.8 there are elements $a_1, \dots, a_d \in \mathfrak{p}$, with $d = \mathrm{ht}(\mathfrak{p})$, such that $(a_1, \dots, a_d) \subset R$ is a $\mathfrak{p}$-primary ideal, i.e. $\mathfrak{p}$ is the only prime ideal containing $(a_1, \dots, a_d)$. Consider now a prime ideal $\mathfrak{q} \subset R[x]$ containing $(a_1, \dots, a_d, P)$: then $\mathfrak{q}$ must intersect R in a prime ideal containing $(a_1, \dots, a_d)$, i.e. $\mathfrak{q} \cap R = \mathfrak{p}$, and hence $\mathfrak{m} = \mathfrak{p} + (P) \subseteq \mathfrak{q}$; by maximality of $\mathfrak{m}$ we conclude $\mathfrak{q} = \mathfrak{m}$, i.e. $\mathfrak{m}$ is the only prime ideal containing $(a_1, \dots, a_d, P)$, which is thus $\mathfrak{m}$-primary. By Theorem 17.5, since $(a_1, \dots, a_d, P)$ is generated by $d + 1$ elements, we obtain $\mathrm{ht}(\mathfrak{m}) \leq d + 1$.
The case $n \geq 2$ follows by applying n times the case $n = 1$, using also Theorem 7.12 along the way. □

Example 18.14. Particular applications of Proposition 18.13 are the following:

- $\dim(\mathbb{Z}[x_1, \dots, x_n]) = n + 1$, for all $n \geq 0$;
- if k is a field, then $\dim(k[x_1, \dots, x_n]) = n$; this completes the discussion about dimensions of k-algebras of finite type started in Example 17.1.

Exercise 18.15. Give an alternative proof of the equality $\dim(k[x_1, \dots, x_n]) = n$, for k a field, as follows:

- in the case in which k is algebraically closed, prove that $\mathrm{ht}(\mathfrak{m}) \leq n$ for every $\mathfrak{m} \in \mathrm{Spec}_{\max}(k[x_1, \dots, x_n])$ by combining Theorems 15.4 and 17.5;
- in the case in which k is not algebraically closed, let $\bar{k}$ be an algebraic closure of k, and consider the inclusion of rings $k[x_1, \dots, x_n] \subseteq \bar{k}[x_1, \dots, x_n]$; prove that it is an injective integral extension of domains, and use Corollaries 14.5 and 14.7 to conclude.

We can in fact analyze more closely the maximal ideals of polynomial rings over *any* field: the following proposition is immediate for k algebraically closed, using Theorem 15.4, but less obvious for generic k.

Proposition 18.16. *Let k be a field and let $\mathfrak{m} \in \mathrm{Spec}_{\max}(k[x_1, \dots, x_n])$ for some $n \geq 0$; then the following hold:*

(1) $\mathfrak{m}$ can be generated by n elements;
(2) $\mathrm{ht}(\mathfrak{m}) = n$;
(3) the localisation $k[x_1, \dots, x_n]_{\mathfrak{m}}$ is a regular local ring, in the sense of Definition 18.4.

Proof. We start by proving (1) and (2) by induction on $n \geq 0$. For $n = 0$ there is nothing to prove, as $\mathfrak{m} = (0) \subset k$. Let now $n \geq 1$, and let $\mathfrak{p} = \mathfrak{m} \cap k[x_1, \dots, x_{n-1}]$. Then the composition $k \hookrightarrow k[x_1, \dots, x_{n-1}]/\mathfrak{p} \hookrightarrow k[x_1, \dots, x_n]/\mathfrak{m}$ exhibits $k[x_1, \dots, x_n]/\mathfrak{m}$ as an integral extension of k by Corollary 15.9; it follows

that $k[x_1,\dots,x_n]/\mathfrak{m}$ is also integral over the domain $k[x_1,\dots,x_{n-1}]/\mathfrak{p}$, which is therefore a field by Example 13.15. Hence $\mathfrak{p}$ is actually a maximal ideal, and we may assume by inductive hypothesis that $\mathfrak{p}$ is generated by $n-1$ elements and has height $n-1$ in $k[x_1,\dots,x_{n-1}]$.
Moreover the ideal $\mathfrak{m}/\mathfrak{p} \subset (k[x_1,\dots,x_{n-1}]/\mathfrak{p})[x_n]$ is maximal, and since the ring $(k[x_1,\dots,x_{n-1}]/\mathfrak{p})[x_n]$ is a PID, we have that there is an element $[P]_{\mathfrak{p}} \in k[x_1,\dots,x_{n-1}]/\mathfrak{p})[x_n]$ generating $\mathfrak{m}/\mathfrak{p}$; it follows that $\mathfrak{m}$ is generated by n elements, namely the $n-1$ elements generating $\mathfrak{p}$ together with P, proving (1). By Theorem 17.5 we immediately obtain $\mathrm{ht}(\mathfrak{m}) \leq n$; conversely, if $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_{n-1} = \mathfrak{p} \subset k[x_1,\dots,x_{n-1}]$ is a proper chain of prime ideals witnessing that $\mathrm{ht}(\mathfrak{p}) = n-1$, then $\mathfrak{p}_i k[x_1,\dots,x_n] \subset k[x_1,\dots,x_n]$ is a prime ideal which is not maximal, as the quotient is the ring $(k[x_1,\dots,x_{n-1}]/\mathfrak{p}_i)[x_n]$, which is a domain but not a field; all such ideals are thus strictly contained in $\mathfrak{m}$, and witness that $\mathrm{ht}(\mathfrak{m}) \geq n$; this concludes the proof of (2). Part (3) is then a direct consequence of (1) and (2) and the definitions of regularity and height, together with the fact that the maximal ideal in $k[x_1,\dots,x_n]_{\mathfrak{m}}$ is generated by the image of any system of generators of $\mathfrak{m}$ under the localisation map. □

18.5. **Regular local rings are domains.** We conclude with the following proposition.

Proposition 18.17. *Let R be a regular local Noetherian ring. Then R is a domain.*

Proof. We denote by $\mathfrak{m}$ the maximal ideal of R, and argue by induction on $d := \dim(R)$. The hypothesis says that $\mathfrak{m}$ can be generated by d elements. For $d = 0$ we hence have that $\mathfrak{m} = (0)$, so that R is in fact a field, hence a domain.
Assume now $d \geq 1$. Since R is regular, we can find a system of d generators $a_1,\dots,a_d$ for $\mathfrak{m}$. Let moreover $\mathfrak{p}_1,\dots,\mathfrak{p}_r$ be the list of the minimal prime ideals of R, i.e. the primes in $\mathrm{Ass}'(0)$.
We prove by induction on $0 \leq t \leq r$ that there exists an element b_t of the form

$$b_t = a_1 + \sum_{i=2}^{d} c_{t,i} a_i$$

such that $b_t \notin \bigcup_{j=1}^{t} \mathfrak{p}_j$. For $t = 0$ we just take $b_0 = a_1$, and the last condition is void. Let now $t \geq 1$ and fix by inductive hypothesis an element b_{t-1} satisfying the above property; if $b_{t-1} \notin \mathfrak{p}_t$ we can just take $b_t = b_{t-1}$, so let us assume $b_{t-1} \in \mathfrak{p}_t$. By Lemma 8.3, using that none of $\mathfrak{p}_1,\dots,\mathfrak{p}_{t-1}$ is contained in $\mathfrak{p}_t$, we can find an element $c \in \bigcap_{j=1}^{t-1} \mathfrak{p}_j \setminus \mathfrak{p}_t$; the hypothesis $c \notin \mathfrak{p}_t$, together with the fact that $\mathfrak{m} \nsubseteq \mathfrak{p}_t$ (for otherwise $\mathfrak{m} = \mathfrak{p}_t$ would be also a minimal prime ideal, implying that $\dim(R) = 0$), implies that $c\mathfrak{m} \nsubseteq \mathfrak{p}_t$; since $\mathfrak{m}$ can be generated using $b_{t-1}, a_2, \dots, a_d$, and since $b_t \in \mathfrak{p}_t$, we must have that $ca_{\bar{i}} \notin \mathfrak{p}_t$ for some $2 \leq \bar{i} \leq d$. We can then set $b_t := b_{t=1} + ca_{\bar{i}}$, which evidently is not contained in any of $\mathfrak{p}_1,\dots,\mathfrak{p}_t$.
In particular we may find an element $b = b_r$ which is not contained in any of the minimal primes $\mathfrak{p}_1,\dots,\mathfrak{p}_r$. Observe also that $\mathfrak{m} = (b, a_2, \dots, a_d)$. We can now consider the local ring $R/(b)$: its maximal ideal $\mathfrak{m}/(b)$ can be generated by the $d-1$ elements $[a_2]_b,\dots,[a_d]_b$, and moreover, since the set $\{a\}$ extends to a system of parameters for R, namely $b, a_2, \dots, a_d$, by Proposition 18.12 we have $\dim(R/(b)) = d-1$. Hence $R/(b)$ is a regular local Noetherian ring, and by inductive hypothesis it is a domain. This implies that the principal ideal (b) is in fact a prime ideal.

We next use that b is not contained in any minimal prime $\mathfrak{p}_i$ as follows. Let $\mathfrak{p}_{\bar{i}}$ be a minimal prime of R contained in the prime ideal (b). We claim that $\mathfrak{p}_{\bar{i}} = b\mathfrak{p}_{\bar{i}}$; one inclusion follows from $\mathfrak{p}_{\bar{i}}$ being an ideal; for the other inclusion, let $c \in \mathfrak{p}_{\bar{i}}$; then, since $\mathfrak{p}_{\bar{i}} \subseteq (b)$, there is $d \in R$ with $db = c$; since $b \notin \mathfrak{p}_{\bar{i}}$, we must have $d \in \mathfrak{p}_{\bar{i}}$ as desired. Since $b \in \mathfrak{m}$, we have in particular $\mathfrak{p}_{\bar{i}} = \mathfrak{m}\mathfrak{p}_{\bar{i}}$, and Corollary 14.11 implies that $\mathfrak{p}_{\bar{i}} = 0$. We thus learn that (0) is a prime ideal, i.e. R is a domain. A posteriori, we learn also that that $r = 1$, i.e. (0) was the unique minimal prime in R. □

Mathematics Institute, University of Copenhagen, Universitetsparken 5, Copenhagen, Denmark
Email address: anbi@math.ku.dk