COMMUTATIVE ALGEBRA

MARKUS LAND

Abstract. These are lecture notes for the lecture *Commutative Algebra* taught at LMU Munich in the summer term 2023. I follow an existing script of Andreas Rosenschon.

Contents

1. Introduction

The purpose of this lecture is to, on the one hand, introduce and study several properties of commutative rings, ideal, and modules, and on the other hand to use this language to prepare for the lectures on algebraic geometry and algebraic number theory.

In particular, we will introduce several notions which will be studied in greater depth in algebraic geometry (like the Zariski spectrum of a commutative ring). Among the topics covered are Noetherian rings, Hilbert's Nullstellensatz, some aspects of affine algebraic geometry, basic properties of modules and the particular the classification of finitely generated modules over principal ideal domains, dimension theory and Artinian rings, integral extensions, Noether's normalization theorem, discrete valuation rings and more generally Dedekind rings.

We now briefly touch on some aspects of the relation between commutative algebra and algebraic geometry and algebraic number theory.

1.1. **Algebraic Geometry.** Basic interesting mathematical objects are polynomials: For instance any polynomial $\mathbb{R}[X_1, \dots, X_n]$ defines a smooth function $\mathbb{R}^n \to \mathbb{R}$, something studied in analysis. One may be interested in the set $f^{-1}(0)$, i.e. the set of solutions of the equation $f(x) = 0$. For instance, the implicit function theorem tells us that if 0 is a regular value, then $f^{-1}(0)$ defines a smooth submanifold of $\mathbb{R}^n$ (if 0 is not regular, then this solution set typically has singularities). In either case, it is interesting to study the function f by studying the geometry (or topology) of the solution set. Particular cases are when f is a polyonmial with integer coefficients. The integral polynomial ring $\mathbb{Z}[X_1, \dots, X_n]$ maps to $K[X_1, \dots, X_n]$ for any field K (in fact for any other ring K) and one can again study the set of solutions of the resulting polynomial equations over K, viewed as subsets of *affine n-space* $\mathbb{A}^n_K$ over K, and

Date: June 1, 2023.

it might be worthwhile to study some sort of geometry of solution sets of integral polynomial equations over different fields.

In classical algebraic geometry, one would consider an algebraically closed field K (this for instance ensures that polynomial equations have solutions). So for ease of presentation let us consider the case $K = \mathbb{C}$. A typical example for instance could be the polynomial $X_2 - X_1^2 \in \mathbb{C}[X_1, X_2]$. Its solution set is given by $V = \{(a, b) \in \mathbb{C}^2 \mid b = a^2\}$. Now, what should an "algebraic" function on this solution set be? An easy answer is to simply say it should be a polynomial function $\mathbb{C}^2 \to \mathbb{C}$, and then we restrict this function to the solution set V. Fair enough. But then it turns out that some functions are zero on the solution set, but not zero outside of it (for instance the function $X_2 - X_1^2$ itself). So let us consider the relation among polynomials in $\mathbb{C}[X_1, X_2]$ given by saying that two are equivalent if they agree on V, or equivalently, that their difference vanishes on V. In the case of interest, this turns out to be precisely the condition that the difference lies in the ideal $(X_2 - X_1^2) \subseteq \mathbb{C}[X, Y]$. We hence arrive at the observation that the ring of algebraic functions on V should be the quotient ring $\mathbb{C}[X_1, X_2]/(X_2 - X_1^2)$.

This leads to the following idea: Given an ideal $I \subseteq \mathbb{C}[X_1, \dots, X_n]$ consider the vanishing set $V(I)$ of all points x in $\mathbb{C}^n$ such that for all $f \in I$, we have $f(x) = 0$. This defines a subset of $\mathbb{C}^n$, the intersection of all solution sets of all elements in I. By analogy to the above, an algebraic function is then precisely an element in $\mathcal{O}(V(I)) = \mathbb{C}[X_1, \dots, X_n]/I(V(I))$, where $I(V(I))$ is the ideal of polynomials which vanish on $V(I)$. Clearly, one has $I \subseteq I(V(I))$ and one formulation of Hilbert's Nullstellensatz is that for any ideal $I \subseteq K[X_1, \dots, X_n]$ and any algebraically closed field K, one has

$$I(V(I)) = \{x \in \mathbb{C}[X_1, \dots, X_n] \mid x^n \in I \text{ for some } n \geq 1\}.$$

The latter in the above equation is called the *radical* of I and is also denoted by $\sqrt{I}$. We will study several equivalent formulations of Hilbert's Nullstellensatz in this course.

The upshot is that radical ideals (that is ideals I which agree with their radical $\sqrt{I}$) in $\mathbb{C}[X_1, \dots, X_n]$ correspond bijectively to certain subsets of $\mathbb{C}^n$ equipped with a ring of algebraic functions on them, which are called affine varieties. The bijection is given by sending an ideal I to the vanishing set $V(I)$ and conversely by sending a variety $V \subseteq \mathbb{C}^n$ to its ring of algebraic functions $\mathcal{O}(V)$. Now, ideals in rings like $\mathbb{C}[X_1, \dots, X_n]$ are the topic of commutative algebra, whereas varieties (and generalizations thereof) are the topic of algebraic geometry. By the just described bijective correspondence, one can try to use algebra to say something about the geometry of the solution sets, or vice versa use the geometry of varieties to say something about their rings of functions.

1.2. **Algebraic Number Theory.** One of the initial goals of algebraic number theory is to study number fields, i.e. finite field extensions of $\mathbb{Q}$. Such finite extensions $K/\mathbb{Q}$ have subrings $\mathcal{O}_K$ (the rings of "integers" in K): Recall that every element in K is a root of a monic polynomial with coefficients in $\mathbb{Q}$ (that is, any finite extension is algebraic). Say that an element x of K lies in $\mathcal{O}_K$ if it is a root of a monic polynomial with coefficients in $\mathbb{Z}$. By the Gauss lemma, we have $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, and the inclusions $\mathbb{Z} \subseteq \mathcal{O}_K$ are ring theoretic analogs of algebraic field extensions (called integral ring extensions) and $\mathcal{O}_K$ is always what is called a Dedekind domain. Now, $\mathbb{Z}$ is a euclidean ring, and last term we have shown the following inclusions:

$$\{\text{Euclidean rings}\} \subseteq \{\text{PIDs}\} \subseteq \{\text{factorial rings}\}$$

Given a number field K, it is an interesting question in number theory to decide what further properties $\mathcal{O}_K$ has, e.g. is it any of the above? For instance, for $K = \mathbb{Q}[\sqrt{-5}]$, one finds $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ which is not factorial, whereas for $K = \mathbb{Q}[\sqrt{-3}]$ we have $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ which is Euclidean.

One can associate to rings A like $\mathcal{O}_K$ (and therefore to a number field) two abelian groups: the Picard group $\mathrm{Pic}(A)$ the Picard group (having to do with line bundles over a geometric object associated to A) and the class group $\mathrm{Cl}(A)$ (having to do with invertible fractional ideals of A). One can then prove an isomorphism $\mathrm{Pic}(A) \cong \mathrm{Cl}(A)$. It turns out that for a number field K the class group $\mathrm{Cl}(\mathcal{O}_K)$ is a finite group and which is trivial if $\mathcal{O}_K$ is factorial. Studying the class group of a number field is a very interesting and difficult problem. For instance, the following is an open question:

$$\text{Is the set } \{d \geq 0 \mid \mathrm{Cl}(\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}) = 0\} \text{ finite?}$$

For $d \leq 0$, the corresponding set is in fact finite, more explicitly Gauss conjectured, and Stark (1952, and later Heegner in 1967) proved that

$$\{d < 0 \mid \mathrm{Cl}(\mathcal{O}_{\mathbb{Q}[\sqrt{d}]}) = 0\} = \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

The relation between the class group and the Picard group is also a first connection between number theory and algebraic K-theory, a relation which in fact goes much much deeper.

2. Rings and ideals

2.1. **Definition** A ring consists of a set A equipped with monoid structures $(+, 0)$ (addition) and $(\cdot, 1)$ (multiplication) such that

(1) $(A, +, 0)$ is an abelian group, and
(2) multiplication distributes over addition, that is, for all $x, y, z \in A$ we have

$$z \cdot (x + y) = z \cdot x + z \cdot y \quad \text{and} \quad (x + y) \cdot z = x \cdot z + y \cdot z.$$

We will often write xy instead of $x \cdot y$. The ring A is called commutative if $(A, \cdot, 1)$ is commutative, i.e. if $xy = yx$ holds for all elements x and y of A.

2.2. **Remark** We do not require that $1 \neq 0$. However, if $1 = 0$, then for any a in A, we have $a = 1 \cdot a = 0 \cdot a = 0$. In other words, $A = \{0\}$ is the only ring in which $1 = 0$.

2.3. **Example** The integers $\mathbb{Z}$ is a commutative ring. Any field K is a commutative ring. Given a commutative ring A and a set M, there exists a polynomial ring $A[X_m; m \in M]$. If $|M| = n$, then this is (isomorphic to) the usual polynomial ring $A[X_1, \ldots, X_n]$ in n variables, and in general it is the filtered colimit over the polynomial rings associated to finite subsets of M. Recall that the polynomial ring comes equipped with a map of sets $\iota_M \colon M \to A[X_m; m \in M]$ given by sending m to X_m, as well as with a map of rings $\iota_A \colon A \to A[X_m; m \in M]$.

2.4. **Definition** A ring homomorphism $f \colon A \to B$ is a map which is a monoid homomorphism with respect to addition and multiplication. That is, one has

$$f(0) = 0, \quad f(x + y) = f(x) + f(y), \quad f(1) = 1, \quad \text{and} f(xy) = f(x)f(y).$$

We write CAlg for the category of commutative rings.

2.5. **Remark** (1) The condition $f(0) = 0$ follows from $f(x + y) = f(x) + f(y)$ since with respect to addition, a ring is a group. Likewise, it follows that $f(-x) = -f(x)$.

(2) The notation CAlg comes from the fact that the category of commutative rings is in fact given by the category $\mathrm{CAlg}(\mathrm{Ab}, \otimes)$ of commutative algebra objects in the symmetric monoidal category of abelian groups (with respect to tensor product of abelian groups). We will come to tensor products in the more general context of modules over rings later.

(3) We recall that the polynomial ring $A[X_m; m \in M]$ satisfies the following universal property: For any commutative ring B, the map

$$\mathrm{Hom}_{\mathrm{CAlg}}(A[X_m; m \in M], B) \longrightarrow \mathrm{Hom}_{\mathrm{CAlg}}(A, B) \times \mathrm{Hom}_{\mathrm{Set}}(M, B)$$

induced by ι_A and ι_M is a bijection.

2.6. **Definition** Let A be a ring. A subset $S \subseteq A$ is a subring if $0, 1 \in S$, and if for any $x, y \in S$ we have that $-x$, $x + y$ and xy are contained in S as well.

2.7. **Remark** The inclusion of a subring $S \subseteq A$ is a ring homomorphism. If $f\colon A \to B$ is a ring homomorphism, then $f(A) \subseteq B$ is a subring.

2.8. **Definition** Let A be a commutative ring. A pair (B, φ) consisting of a commutative ring B and a ring homomorphism $\varphi\colon A \to B$ is called an *A-algebra*. The map φ is called the *structure morphism* of the A-algebra B and is often omitted from the notation. A morphism of A-algebras is a map $B \to B'$ in CAlg compatible with the A-algebra structure morphisms, that is a ring homomorphism making the diagram

$$\begin{array}{ccc} A & \longrightarrow & B' \\ \downarrow & \nearrow & \\ B & & \end{array}$$

commutative.

2.9. **Remark** (1) In other words, we have that the category CAlg_A of commutative A-algebras is equivalent to the slice category $\mathrm{CAlg}_{A/}$ of objects of CAlg under A.

(2) The map $\iota_A\colon A \to A[X_m; m \in M]$ makes the polynomial ring $A[X_m; m \in M]$ an A-algebra. Point (3) of Remark 2.5 then gives the following universal property of the polynomial ring among A-algebras: Namely, the map

$$\mathrm{Hom}_{\mathrm{CAlg}_A}(A[X_m; m \in M], B) \longrightarrow \mathrm{Hom}_{\mathrm{Set}}(M, B)$$

induced by ι_M is a bijection. This means that the association $M \mapsto A[X_m; m \in M]$ assembles into a left adjoint of the forgetful functor $\mathrm{CAlg}_A \to \mathrm{Set}$ given by sending an A-algebra B to the set underlying the commutative ring B. One therefore says that $A[X_m; m \in M]$ is the *free commutative A-algebra on the set M*.

2.10. **Definition** Let A be a commutative ring. A subgroup $\mathfrak{a} \subseteq A$ (under addition) is called an *ideal* if for all $a \in \mathfrak{a}$ and $x \in A$ we have $ax \in \mathfrak{a}$. An ideal $\mathfrak{a}$ strictly contained in A (that is $\mathfrak{a} \neq A$) is called *strict*.

2.11. **Example** Let $f\colon A \to B$ be a morphism in CAlg. Then $\ker(f) \subseteq A$ is an ideal. It is a strict ideal if and only if $B \neq 0$.

The following lemma was proven last term.

2.12. **Lemma** *Let A be a commutative ring and $\mathfrak{a} \subseteq A$ an ideal. Then the quotient ring $A/\mathfrak{a}$ comes equipped with a canonical projection map $\pi_{\mathfrak{a}}\colon A \to A/\mathfrak{a}$. This map satisfies the following universal property, namely that the map*

$$\mathrm{Hom}_{\mathrm{CAlg}}(A/\mathfrak{a}, B) \longrightarrow \mathrm{Hom}_{\mathrm{CAlg}}(A, B)$$

is injective and its image consists of those ring homomorphisms $f\colon A \to B$ for which $\ker(f) \subseteq \mathfrak{a}$.

2.13. **Remark** As any ideal, $\mathfrak{a} \subseteq A$ is a subgroup under addition. Since the addition is commutative, this subgroup is normal. The underlying abelian group of $A/\mathfrak{a}$ (under addition) is then the usual quotient group. The defining property of ideals ensures that the multiplication of A descends to a well-defined multiplication on $A/\mathfrak{a}$ and this turns $A/\mathfrak{a}$ into a commutative ring. In particular, we have $\ker(\pi_{\mathfrak{a}}) = \mathfrak{a}$. Consequently, we deduce that a surjective ring homomorphism $f\colon A \to B$ induces an isomorphism of rings $A/\ker(f) \xrightarrow{\cong} B$.

2.14. **Lemma** *Let $f\colon A \to B$ be a ring homomorphism. If $\mathfrak{b}$ is an ideal of B, then $f^{-1}(\mathfrak{b})$ is an ideal of A. If f is surjective, and $\mathfrak{a}$ is an ideal of A, then $f(\mathfrak{a})$ is an ideal of B.*

Proof. Exercise. □

Let us notice that the set of ideals $\mathfrak{a}$ of A is a partially ordered set (by inclusion).

2.15. **Corollary** *Let A be a commutative ring and $\mathfrak{a}$ an ideal of A. The association*

$$\{\mathfrak{b} \subseteq A/\mathfrak{a} \mid \mathfrak{b} \text{ ideal } \} \xrightarrow{\pi_{\mathfrak{a}}^{-1}} \{\overline{\mathfrak{b}} \subseteq A \mid \overline{\mathfrak{b}} \text{ ideal s.t. } \mathfrak{a} \subseteq \overline{\mathfrak{b}}\}$$

is an isomorphism of partially ordered sets.

Proof. First, we note that the map $\pi_{\mathfrak{a}}^{-1}$ from ideals of $A/\mathfrak{a}$ to ideals of A preserves the partial orders. It then follows that $\mathfrak{a} = \pi_{\mathfrak{a}}^{-1}(0) \subseteq \pi_{\mathfrak{a}}^{-1}(\mathfrak{b})$ for all ideals $\mathfrak{b}$ of $A/\mathfrak{a}$. The map is therefore a well-defined map of posets (partially ordered sets). It remains to see that it is bijective. For this, we note that an inverse is given by sending $\overline{\mathfrak{b}}$ to $\pi_{\mathfrak{a}}(\overline{\mathfrak{b}})$. □

2.16. **Definition** Let A be a commutative ring.

(1) A *unit* of A is an element which is a unit in the multiplicative monoid of A. That is, it is an element a such that there exists b in A with $ab = 1$. We write $A^\times$ for the group of units (under multiplication) of A.
(2) A *field* is a commutative ring $K \neq 0$ such that $K^\times = K \setminus \{0\}$.
(3) An element a of A is called a *zero-divisor* if there exists b in A such that $ab = 0$.
(4) $A \neq 0$ is called a *domain* (sometimes als an *integral domain*) if 0 is the only zero-divisor of A.

Exercise.
(1) Given a in A, there exists at most one element b with $ab = 1$. Hence, for a unit, we write a^{-1} for this unique element and call it the *inverse* of a.
(2) A non-zero commutative ring is a domain if and only if the map $\ell_a\colon A \to A$, with $\ell_a(b) = ab$ is injective for all $a \neq 0$.

(3) A non-zero commutative ring is a field if and only if the map $\ell_a \colon A \to A$ is bijective for all $a \neq 0$.

2.17. **Definition** Let A be a commutative ring, $M \subseteq A$ a subset and $\{\mathfrak{a}_i\}_{i\in I}$, $\mathfrak{a}$ and $\mathfrak{b}$ (a family of) ideals of A.

(1) The intersection $\bigcap_{i\in I} \mathfrak{a}_i$ is an ideal, called the *intersection* of the ideals $\mathfrak{a}_i$. In particular $\mathfrak{a} \cap \mathfrak{b}$ is an ideal of A.
(2) the subset $\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}$ is an ideal, the *sum* of the ideals $\mathfrak{a}$ and $\mathfrak{b}$.
(3) the ideal $(M) = \bigcap_{M\subseteq I\subseteq A} I$ where I ranges through ideals of A containing M is the ideal *spanned by the set* M.
(4) the ideal $\mathfrak{a} \cdot \mathfrak{b} := (\{ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}) \subseteq A$ is the *product* of the ideals $\mathfrak{a}$ and $\mathfrak{b}$.

2.18. **Example** Consider the ring $\mathbb{Z}$ with ideals (n) and (m) generated by integers n and m. Then

$$(n) \cap (m) = \operatorname{lcm}(m, n), \quad (n) + (m) = \gcd(m, n) \quad \text{and} \quad (n)(m) = (nm).$$

In particular, $(n) \cap (m) = (n)(m)$ if and only if $\operatorname{lcm}(n, m) = nm$ and $(n) + (m) = (1)$ if and only if $\gcd(n, m) = 1$.

This "in particular" is true more generally for principal ideals (that is ideals generated by a single element) in factorial rings.

Exercise. For ideals $\mathfrak{a}$ and $\mathfrak{b}$ of a commutative ring A, one has the following properties:

(1) $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$,
(2) $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$, and
(3) $\mathfrak{a} + \mathfrak{b} = A$ implies that $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

2.19. **Lemma** *Let $A \neq 0$ be a commutative ring. TFAE (the following are equivalent)*

(1) *A is a field,*
(2) *the only ideals of A are $\{0\}$ and A,*
(3) *for every $B \neq 0$, every ring homomorphism $f \colon A \to B$ is injective.*

Proof. (1) $\Rightarrow$ (2): Let $\mathfrak{a} \subseteq A$ be a non-zero ideal. Then it contains a unit (A is a field), and therefore 1, so that $\mathfrak{a} = A$. (2) $\Rightarrow$ (3): We have $f(1) = 1$. Therefore (by the assumption that $B \neq 0$), we have $\ker(f) \neq A$, so we have $\ker(f) = \{0\}$ (the kernel is an ideal) and therefore f is injective. (3) $\Rightarrow$ (1): Let $0 \neq a$ be an element of A. We need to show that a is a unit, or equivalently that the ideal (a) spanned by a is equal to A. Consider the ring map $A \to A/(a)$. This map is not injective since $a \neq 0$. Hence $A/(a)$ must be zero and hence $(a) = A$ as needed. □

2.20. **Definition** Let A be a commutative ring and $\mathfrak{a}$ and $\mathfrak{b}$ ideals of A. We say that $\mathfrak{a}$ and $\mathfrak{b}$ are *coprime* if $\mathfrak{a} + \mathfrak{b} = A$.

The following is the *Chinese remainder theorem*. We have proven it last term.

2.21. **Theorem** *Let A be a commutative ring, and $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ pairwise coprime ideals. Then the canonical map*

$$A \longrightarrow \prod_{i=1}^{n} A/\mathfrak{a}_i$$

is surjective. Its kernel is given by the intersection $\cap_i \mathfrak{a}_i$ of the ideals $\mathfrak{a}_i$, and therefore, the above canonical map induces an isomorphism

$$A/\bigcap_{i=1}^{n} \mathfrak{a}_i \cong \prod_{i=1}^{n} A/\mathfrak{a}_i.$$

2.22. **Example** (1) Consider $\mathbb{Z}$ and $m \geq 2$. Write $m = p_1^{n_1} \cdots p_k^{n_k}$ with pairwise distinct prime numbers p_i. Then, for $i \neq j$, the ideals $(p_i^{n_i})$ and $(p_j^{n_j})$ are coprime (exercise). By the chinese remainder theorem, the map

$$\mathbb{Z} \longrightarrow \prod_{i=1}^{k} \mathbb{Z}/p_i^{n_i}\mathbb{Z}$$

is surjective and its kernel is given by (m) as follows from part (3) of the above exercise together with Example 2.18. In other words, the above map induces an isomorphism

$$\mathbb{Z}/m\mathbb{Z} \cong \prod_{i=1}^{k} \mathbb{Z}/p_i^{n_i}\mathbb{Z}.$$

(2) Let K be a field and $K[X]$ the polynomial ring. Recall that this ring is a euclidean domain and hence in particular factorial. That is polynomial of positive degree can be written as a product of irreducible polynomials. Now let $f \in K[X]$ be of positive degree and write $f = f_1^{n_1} \cdots f_k^{n_k}$ with pairwise distinct irreducible polynomials f_i. Then the same argument as above shows that there is a canonical isomorphism

$$K[X]/(f) \cong \prod_{i=1}^{k} K[X]/(f_i^{n_i}).$$

Exercise. The purpose of this exercise is to deduce the generalized eigenspace decomposition one proves in linear algebra 2. Let V be finite dimensional K-vector space and let $\varphi\colon V \to V$ be an endomorphism of V. Let $f \in K[X]$ be the minimal polynomial of φ and assume that it factors into linear terms (this is automatic for instance if K is algebraically closed) and write $f = \prod_{i=1}^{k} (X - \lambda_i)^{n_i}$ where the λ_i's are the distinct eigenvalues of f. Show that there is a canonical isomorphism

$$V \cong \prod_{i=1}^{k} \ker[(f - \lambda_i \cdot \mathrm{id})^{n_i}].$$

2.23. **Definition** Let A be a commutative ring and $\mathfrak{a}$ a strict ideal. Then $\mathfrak{a}$ is called

(1) a *prime ideal* if $xy \in \mathfrak{a}$ implies that $x \in \mathfrak{a}$ or $y \in \mathfrak{a}$, and
(2) a *maximal ideal* if $\mathfrak{a} \subseteq \mathfrak{b}$ for some ideal $\mathfrak{b}$ implies that $\mathfrak{b} = \mathfrak{a}$ or $\mathfrak{b} = A$.

2.24. **Lemma** *Let A be a commutative ring, $I, J \subseteq A$ ideals and $\mathfrak{p} \subseteq A$ a prime ideal. If $I \cdot J \subseteq \mathfrak{p}$ then $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$.*

Proof. Assume that I is not a subset of $\mathfrak{p}$. We need to show that $J \subseteq \mathfrak{p}$. Pick $i \in \mathfrak{p} \setminus I$ and let $j \in J$. Then $ij \in I \cdot J \subseteq \mathfrak{p}$. Since $i \notin \mathfrak{p}$ and $\mathfrak{p}$ is prime, we have $j \in \mathfrak{p}$ and therefore $J \subseteq \mathfrak{p}$. □

2.25. **Lemma** *Let A be a commutative ring and $\mathfrak{a}$ an ideal. Then $\mathfrak{a}$ is prime if and only if $A/\mathfrak{a}$ is a domain, and $\mathfrak{a}$ is maximal if and only if $A/\mathfrak{a}$ is a field. In particular, maximal ideals are prime.*

Proof. The case of prime ideals follows by definition and the fact that the kernel of $A \to A/\mathfrak{a}$ is equal to $\mathfrak{a}$. The case of maximal ideals follows from Corollary 2.15 and Lemma 2.19. The "in particular" follows since fields are domains. □

2.26. **Lemma** *Let $f\colon A \to B$ be a morphism in* CAlg *and let $\mathfrak{a}$ be an ideal of $\mathbb{A}$ and $\mathfrak{b}$ be an ideal of B.*

(1) *If $\mathfrak{b}$ is prime, then so is $f^{-1}(\mathfrak{b})$.*
(2) *If $\mathfrak{b}$ is maximal, $f^{-1}(\mathfrak{b})$ need not be maximal.*
(3) *If f is surjective and $\ker(f) \subseteq \mathfrak{a}$, then $\mathfrak{a}$ is prime (or maximal) if and only if $f(\mathfrak{a})$ is.*

Proof. (1): Observe that the canonical map $A/f^{-1}(\mathfrak{b}) \to B/\mathfrak{b}$ is injective. Hence if $B/\mathfrak{b}$ is a domain, then so is $A/f^{-1}(\mathfrak{b})$. (2): Consider the map $\mathbb{Z} \to \mathbb{Q}$ and the maximal ideal $\{0\} \subseteq \mathbb{Q}$. Its preimage is again the zero ideal, which is prime but not maximal. (3): We claim that the map $A/\mathfrak{a} \to B/f(\mathfrak{a})$ is an isomorphism, so one is a domain (or a field) if and only if the other is. To see the claim, note that the assumption $\ker(f) \subseteq \mathfrak{a}$ implies that $f^{-1}(f(\mathfrak{a})) = \mathfrak{a}$, so by the argument of (1), the map $A/\mathfrak{a} \to B/f(\mathfrak{a})$ is injective. But it is also surjective, since f is surjective. □

2.27. **Example** Consider the inclusion $\mathbb{Z} \to \mathbb{Z}[i]$ of the integers into the Gaussian integers. Let p be a prime number. Whether or not the ideal of $\mathbb{Z}[i]$ generated by p is a prime ideal depends on p: In $\mathbb{Z}[i]$ we have $2 = (1+i)(1-i)$, so the ideal generated by 2 is not prime. In fact, since $1 - i = -i(1+i)$, we see that $(2) = (1+i)^2$ as ideals of $\mathbb{Z}[i]$. It turns out that for odd primes, there are two cases to consider:

(1) if $p \equiv 1 \mod 4$. In this case (p) is the product of two prime ideals.
(2) if $p \equiv 3 \mod 4$. In this case (p) is a prime ideal.

One way to prove this is to use that $\mathbb{Z}[i]$ is a euclidean domain, see Exercise 3 on the Exercise Sheet 1.

2.28. **Lemma** *Let A be a commutative ring and $\mathfrak{a}$ a strict ideal of A. There exists a maximal ideal $\mathfrak{m}$ of A which contains $\mathfrak{a}$. In particular, every non-unit $a \in A \setminus A^\times$ lies in some maximal ideal.*

Proof. Consider the (partially ordered) set S of strict ideals $\mathfrak{b}$ of A (that is $\mathfrak{b} \neq A$) which contain $\mathfrak{a}$. Given an increasing sequence $\mathfrak{b}_1 \subseteq \mathfrak{b}_2 \subseteq \dots$ in S let us consider the union $\mathfrak{b}$ of all $\mathfrak{b}_i$'s. Then $\mathfrak{b}$ is a member of S: Obviously $\mathfrak{a} \subseteq \mathfrak{b}$. Furthermore, $\mathfrak{b} \neq A$, for else $1 \in \mathfrak{b}$ which implies that $1 \in \mathfrak{b}_i$ for some $i \geq 1$ which it is not. Consequently, by Zorn's lemma, there exists a maximal element $\mathfrak{m}$ of S. To see that $\mathfrak{m}$ is a maximal ideal, suppose given a further ideal $\mathfrak{m}'$ containing $\mathfrak{m}$. Then $\mathfrak{m}'$ also contains $\mathfrak{a}$. Now either $\mathfrak{m}' = A$ or $\mathfrak{m}' \in S$ from which it follows by maximality of $\mathfrak{m}$ is S that $\mathfrak{m}' = \mathfrak{m}$. To see the "in particular" simply consider $\mathfrak{a} = (a)$. □

2.29. **Definition** A domain A is called a *principal ideal domain* (PID) if every ideal $\mathfrak{a}$ in A is principal, that is, if $\mathfrak{a} = (a)$ for some $a \in A$.

2.30. **Example** Every field K is a PID. The rings $\mathbb{Z}$ and $\mathbb{Z}[i]$ are PIDs. For a field K, the polynomial ring $K[X]$ is a PID. In fact, all these examples are Euclidean domains, and any Euclidean domain is a PID as we have shown last term.

2.31. **Proposition** *Let A be a PID and $\mathfrak{a} \neq 0$ an ideal. Then $\mathfrak{a}$ is prime if and only if $\mathfrak{a}$ is maximal.*

Proof. Maximal ideals are always prime by Lemma 2.25. So let us assume $\mathfrak{a}$ is a prime ideal. Pick an ideal $\mathfrak{m}$ containing $\mathfrak{a}$. Let $\mathfrak{m} = (m)$ and $\mathfrak{a} = (a)$. Then there exists $b \in A$ such that $a = mb$. Since $\mathfrak{a}$ is prime we must have $m \in \mathfrak{a}$ or $b \in \mathfrak{a}$. In the former case we conclude that $\mathfrak{a}$ is maximal, so let us assume the latter. Since $\mathfrak{a} = (a)$ there then exists $x \in A$ such that $xa = b$. Together we find $a = mxa$ and hence $a(1 - mx) = 0$. Since $\mathfrak{a} \neq 0$ and A is a domain, we find $mx = 1$ and hence that m is a unit and thus that $\mathfrak{m} = A$. Again, we conclude that $\mathfrak{a}$ is maximal. □

2.32. **Proposition** *Let A be a commutative ring. Then $A[X]$ is a PID if and only if A is a field.*

Proof. If A is a field, we have stated above that $A[X]$ is a PID. Conversely, suppose that $A[X]$ is a PID and hence in particular a domain. Then also A is a domain. Consequently, the ideal (X) is prime because $A[X]/(X) \cong A$. By Proposition 2.31 we conclude that (X) is maximal and hence that $A[X]/(X) \cong A$ is a field. □

2.33. **Remark** In particular, for a field K, the polynomial ring $K[X_1, \ldots, X_n]$ in n variables is not a PID for $n \geq 2$. However, for an element $(x_1, \ldots, x_n)$ in K^n, the ideal $(X_1 - x_1, \ldots, X_n - x_n) \subseteq K[X_1, \ldots, X_n]$ is clearly the kernel of the surjective map $K[X_1, \ldots, X_n] \to K$ sending X_i to x_i. Consequently, this ideal is maximal. If K is algebraically closed, it turns out that every maximal ideal is of this form, and one obtains a bijective correspondence between K^n and the set of maximal ideals in $K[X_1, \ldots, X_n]$ (this is an equivalent formulation of Hilbert's Nullstellensatz which we will prove later in this course).

For non-algebraically closed fields, this is not true: for instance, the ideal $(X^2 + 1) \subseteq \mathbb{R}[X]$ is maximal (it is irreducible and hence prime and hence maximal since $\mathbb{R}[X]$ is a PID), but is not of the form $(X - a)$ for some $a \in \mathbb{R}$.

2.34. **Definition** A commutative ring is called *local* if it contains a unique maximal ideal. For a local ring $(A, \mathfrak{m})$, we call $\kappa = A/\mathfrak{m}$ its *residue field*. We say that a local ring is of *equal characteristic* if it contains a field (and hence necessarily a prime field, i.e. $\mathbb{Q}$ or $\mathbb{F}_p$ for some prime p). Otherwise we say that A is of *mixed characteristic*.

2.35. **Remark** As a generalization of local rings, we call a commutative ring A *semi-local* if it contains only finitely many maximal ideals. We will not talk much about semi-local rings, however.

Exercise. Let $(A, \mathfrak{m})$ be a local domain and F its field of fractions. Show that A is of equal characteristic if and only if $\mathrm{char}(F) = \mathrm{char}(\kappa)$ and of mixed characteristic if and only if $\mathrm{char}(F) = 0$ and $\mathrm{char}(\kappa) > 0$.

2.36. **Example** We note that a local ring is non-zero: The zero ideal is maximal only in fields, and the zero ring is not a field. Conversely, fields are local rings ($\{0\}$ is indeed the unique maximal ideal).

2.37. **Lemma** *Let A be a commutative ring. Then A is local if and only if the set $A \setminus A^\times$ forms an ideal. In this case, $A \setminus A^\times = \mathfrak{m}$ is the unique maximal ideal.*

Proof. Suppose A is local with maximal ideal $\mathfrak{m}$. We show that $\mathfrak{m} = A \setminus A^\times$. By Lemma 2.28 any element of $A \setminus A^\times$ lies in some maximal ideal, and hence in $\mathfrak{m}$, so that $A \setminus A^\times \subseteq \mathfrak{m}$. On the other hand, $\mathfrak{m} \subseteq A \setminus A^\times$ as $\mathfrak{m}$ cannot contain a unit ($\mathfrak{m} \neq A$). Conversely, suppose that the set $A \setminus A^\times$ forms an ideal $\mathfrak{m}$. Then this is maximal, for if $\mathfrak{m} \subseteq \mathfrak{m}'$ is a strict inclusion, $\mathfrak{m}'$ contains a unit and hence $\mathfrak{m}' = A$. As any strict ideal is contained in $A \setminus A^\times$, we find that any maximal ideal is contained in $A \setminus A^\times$, so we conclude that $A \setminus A^\times$ is in fact the unique maximal ideal. □

2.38. **Example**
(1) Let $p \in \mathbb{Z}$ be a prime number an consider the ring $\mathbb{Z}/p^k\mathbb{Z}$. This is a local ring (of mixed characteristic), with maximal ideal generated by p and residue field $\mathbb{F}_p$.
(2) Let K be a field and consider the ring $K[X]/(X)^n$. This is a local ring (of equal characteristic) with maximal ideal generated by X and residue field K.
(3) Let K be a field and consider the ring $K[\![X]\!] = \lim_n K[X]/(X)^n$ – here lim refers to the (cofiltered) inverse limit of the sequence of ring homomorphisms
$$\cdots \to K[X]/(X)^3 \to K[X]/(X)^2 \to K[X]/(X) \cong K.$$
This is the ring of power series in K, we may view elements as expressions $\sum_n^\infty a_n X^n$ with $a_n \in K$ and usual multiplication of power series. This is a local ring (of equal characteristic) with maximal ideal again generated by X and residue field K.
(4) Let $\mathbb{Z}_{(p)} = \{m/n \in \mathbb{Q} \mid n \notin (p)\}$ where p is a prime. This is a local ring (of mixed characteristic) with maximal ideal generated by p.

For (1), the surjection $\mathbb{Z}/p^k\mathbb{Z} \to \mathbb{F}_p$ whose kernel is generated by p shows that (p) is indeed maximal. Moreover, given any surjection to a field $\mathbb{Z}/p^k\mathbb{Z} \to K$, we find that the image x of p satisfies $x^k = 0$ and hence $x = 0$. Therefore, (p) is contained in the kernel of $\mathbb{Z}/p^k \to K$ hence since (p) is maximal it coincides with the kernel, showing that (p) is the unique maximal ideal. To see (2) and (3), note that by Lemma 2.37 it suffices to show that the ideal spanned by X consists precisely of the non-units (one can of course also prove (1) in this way). For this use a geometric series argument to show that $\sum_n^\infty a_n X^n$ is invertible if and only if $a_0 \neq 0$, and the same in the rings $K[X]/(X)^n$. (4) is a special case of a general result about certain localizations of commutative rings: Given a commutative ring A and a prime ideal $\mathfrak{p}$, the localisation $A_{(\mathfrak{p})}$ of A at the subset $A \setminus \mathfrak{p}$ is a local ring with maximal ideal given by the ideal spanned by $\mathfrak{p}$ in the localization $A_{(\mathfrak{p})}$, as we will show later when discussing localizations of rings more thoroughly.

2.39. **Definition** Let A be a commutative ring. The *(Zariski) spectrum* of A is the set of prime ideals of A:
$$\operatorname{Spec}(A) = \{\mathfrak{p} \subseteq A \mid \mathfrak{p} \text{ prime ideal}\}.$$
For a subset $T \subseteq A$, we set
$$V(T) = \{\mathfrak{p} \in \operatorname{Spec}(A) \mid T \subseteq \mathfrak{p}\} \subseteq \operatorname{Spec}(A).$$

2.40. **Remark** Let $T \subseteq T' \subseteq A$ be subsets. Then $V(T') \subseteq V(T)$. Let $I = (T)$ be the ideal generated by the set T, then $T \subseteq I$ and consequently $V(I) \subseteq V(T)$. In fact, we have

$V(T) = V(I)$. Indeed, $T \subseteq \mathfrak{p}$ if and only if $I \subseteq \mathfrak{p}$ since $\mathfrak{p}$ is itself an ideal. Exercise: $V(0) = \mathrm{Spec}(A)$ and $V(T) = \emptyset$ if and only if the ideal generated by T is A.

2.41. **Example** (1) Let K be a field. Then $\mathrm{Spec}(K) = \{0\}$.

(2) Let A be a PID. Then by Proposition 2.31, every non-zero prime ideal is maximal. Therefore we have

$$\mathrm{Spec}(A) = \{0\} \cup \{\mathfrak{m} \subseteq A \mid \mathfrak{m} \text{ maximal ideal}\}.$$

In particular for the integers $\mathbb{Z}$ and the polynomial ring $K[X]$ over a field K, we have

$$\mathrm{Spec}(\mathbb{Z}) = \{0\} \cup \{(p) \mid p \text{ prime number}\} \quad \text{and} \quad \mathrm{Spec}(K[X]) = \{0\} \cup \{(f) \mid f \text{ irreducible}\}$$

since in a PID, every prime ideal is generated by an irreducible (or equivalently prime) element.

(3) Later, we will show the following: let A be a commutative ring with prime ideal $\mathfrak{p}$. Then

$$\mathrm{Spec}(A_{(\mathfrak{p})}) = \{\mathfrak{q} \in \mathrm{Spec}(A) \mid \mathfrak{q} \subseteq \mathfrak{p}\} \subseteq \mathrm{Spec}(A)$$

In particular, $\mathrm{Spec}(\mathbb{Z}_{(p)}) = \{0\} \cup \{(p)\}$.

2.42. **Lemma** *Let A be a commutative ring.*

(1) *Let $(\mathfrak{a}_i)_{i\in I}$ be a family of ideals of A. Then $V(\bigcup_i \mathfrak{a}_i) = \bigcap_i V(\mathfrak{a}_i)$.*

(2) *Let $\mathfrak{a}, \mathfrak{a}'$ be ideals of A. Then $V(\mathfrak{a} \cap \mathfrak{a}') = V(\mathfrak{a} \cdot \mathfrak{a}') = V(\mathfrak{a}) \cup V(\mathfrak{a}')$.*

Proof. (1): By definition, $\mathfrak{p} \in V(\bigcup_i \mathfrak{a}_i)$ if $\cup_i \mathfrak{a}_i \subseteq \mathfrak{p}$. This is equivalent to the condition that for all $i \in I$, $\mathfrak{a}_i \subseteq \mathfrak{p}$ which means that $\mathfrak{p} \in \cap_i V(\mathfrak{a}_i)$. (2): We have $\mathfrak{p} \in V(\mathfrak{a}) \cup V(\mathfrak{a}')$ if $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{a}' \subseteq \mathfrak{p}$. This implies that $\mathfrak{a} \cap \mathfrak{a}' \subseteq \mathfrak{p}$ and hence we find $V(\mathfrak{a}) \cup V(\mathfrak{a}') \subseteq V(\mathfrak{a} \cap \mathfrak{a}')$. Since $\mathfrak{a} \cdot \mathfrak{a}' \subseteq \mathfrak{a} \cap \mathfrak{a}'$ we conclude from Remark 2.40 that

$$V(\mathfrak{a}) \cup V(\mathfrak{a}') \subseteq V(\mathfrak{a} \cap \mathfrak{a}') \subseteq V(\mathfrak{a} \cdot \mathfrak{a}').$$

Now, given $\mathfrak{p} \in V(\mathfrak{a} \cdot \mathfrak{a}')$, we have $\mathfrak{a} \cdot \mathfrak{a}' \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is prime, we deduce from Lemma 2.24 that $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{a}' \subseteq \mathfrak{p}$. This shows that $V(\mathfrak{a} \cdot \mathfrak{a}') \subseteq V(\mathfrak{a}) \cup V(\mathfrak{a}')$. □

2.43. **Corollary** *Let A be a commutative ring. The set of subsets $\{V(T) \mid T \subseteq A\}$ of* $\mathrm{Spec}(A)$ *determine a topology on* $\mathrm{Spec}(A)$*, the* Zariski topology*.*

Proof. Remark 2.40 and Lemma 2.42 say that the sets $V(T)$ are the closed sets of a topology on $\mathrm{Spec}(A)$. □

In the following remark we briefly recall some notions from point-set topology.

2.44. **Remark** We recall that a topology on a set X is usually defined in the following way: It consists of a collection $\mathcal{U}(X) \subseteq \mathcal{P}(X)$ of subsets of X satsifying the following axioms:

(1) $\emptyset, X \in \mathcal{U}(X)$,
(2) given a family $\{U_i\}_{i\in I}$ with $U_i \in \mathcal{U}(X)$ for all $i \in I$, the union $\cup_i U_i$ is an element of $\mathcal{U}(X)$ as well.
(3) given $U, V \in \mathcal{U}(X)$, the intersection $U \cap V$ is an element of $\mathcal{U}(X)$ as well.

The elements of $\mathcal{U}$ are called the *open sets* of the topology.

A subset $C \subseteq X$ is called *closed* if $X \setminus C$ is an element of $\mathcal{U}$, that is, if $X \setminus C$ is open[1]. A topology is hence also determined by the collection of closed subsets $\mathcal{C}(X)$ which then satisfies the axioms

(1) $X, \emptyset \in \mathcal{C}(X)$,
(2) given a family $\{C_i\}_{i\in I}$ with $C_i \in \mathcal{C}(X)$ for all $i \in I$, the intersection $\cap_i C_i$ is an element of $\mathcal{C}(X)$ as well.
(3) given $U, V \in \mathcal{C}(X)$, the union $U \cup V$ is an element of $\mathcal{C}(X)$ as well.

Given a subset T of a topological space X, one defines its closure $\overline{T}$ as the intersection of all closed sets C of X which contain T:

$$T \subseteq \overline{T} = \bigcap_{C\in\mathcal{C}(X)} C.$$

By definition, a subset is closed if and only if it agrees with its closure. Note that taking closures only makes sense in a fixed ambient topological space (and very much depends on that ambient space).

Let $T \subseteq X$ be a subset of a topological space. The collection $\{T \cap U \mid U \in \mathcal{U}(X)\}$ is a topology on T, the *subspace topology*. Its closed sets are given by $C \cap T$ for $C \in \mathcal{C}$. We will always view subsets of topological spaces as topological spaces (equipped with the subspace topology) and hence sometimes refer to them as subspaces rather than subsets.

For a family $\{X_i\}_{i\in I}$ of topological spaces indexed over a set I, the *coproduct* or *disjoint union* is the topological space $\coprod_{i\in I} X_i$ whose underlying set is the disjoint union of the sets X_i and where a subset of $\coprod_i X_i$ is open if and only if its intersection with each X_i is open.

A topological space X is called *reducible* if there exist $X_1, X_2 \in \mathcal{C}(X) \setminus \{\emptyset, X\}$ with $X = X_1 \cup X_2$, and called *irreducible* otherwise.[2]

A map $f\colon X \to Y$ between topological spaces is called *continuous* if $f^{-1}(\mathcal{U}(Y)) \subseteq \mathcal{U}(X)$, i.e. if preimages of open sets of Y are open sets in X. Equivalently, if preimages of closed sets of Y are closed sets of X. We write Top for the category of topological spaces with continuous maps as morphisms.

Exercise. If $T \subseteq X$ is an irreducible subspace of a topological space X (that is, it is irreducible in the subspace topology), the so is $\overline{T}$.

2.45. **Lemma** *Let A be a commutative ring and $\mathfrak{p} \in \operatorname{Spec}(A)$.*

(1) $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$.
(2) $\{\mathfrak{p}\} \subseteq \operatorname{Spec}(A)$ *is closed if and only if $\mathfrak{p}$ is maximal.*
(3) *The association $\mathfrak{p} \mapsto V(\mathfrak{p})$ is an order reversing bijection between the set of prime ideasl of A and the set of irreducible closed subsets of* $\operatorname{Spec}(A)$.

Proof. (1): By definition, we have

$$\overline{\{\mathfrak{p}\}} = \bigcap_{T\subseteq\mathfrak{p}} V(T) = V(\mathfrak{p})$$

where the last equality holds true because the collection of subsets of $\mathfrak{p}$ has $\mathfrak{p}$ as maximal element and the association $T \mapsto V(T)$ is inclusion reversing. (2): Let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{p}$. Then $\mathfrak{m} \in V(\mathfrak{p})$. Hence, $V(\mathfrak{p}) = \{\mathfrak{p}\}$ implies that $\mathfrak{p}$ is maximal, and conversely,

[1] Keep in mind that sets are not doors: They are not either open or closed!

[2] The emtpy set not irreducible.

if $\mathfrak{p}$ is maximal, then $V(\mathfrak{p}) = \{\mathfrak{p}\}$. (3): By definition $V(\mathfrak{p}) = V(\mathfrak{p}')$ implies $\mathfrak{p} = \mathfrak{p}'$ for two prime ideals: Since $\mathfrak{p} \in V(\mathfrak{p}) = V(\mathfrak{p}')$ we find that $\mathfrak{p} \subseteq \mathfrak{p}'$ and vice versa. The exercise in Remark 2.44 together with (1) implies that for $\mathfrak{p}$ a prime ideal, $V(\mathfrak{p})$ is irreducible (and closed by definition of the topology). The map $\mathfrak{p} \mapsto V(\mathfrak{p})$ is hence well-defined and injective. We now show that it is also surjective, i.e. that every irreducible closed subset of $\mathrm{Spec}(A)$ is of the form $V(\mathfrak{p})$ for a prime $\mathfrak{p}$. For this we need to make use of a Lemma which we will prove later, Lemma 4.8.[3] Using the language there, we first note that $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$ since $\mathfrak{a} \subseteq \mathfrak{p}$ if and only if $\sqrt{\mathfrak{a}} \subseteq \mathfrak{p}$ for a prime $\mathfrak{p}$. Let us therefore assume that $\mathfrak{a}$ is a radical ideal which is not prime. We will show that $V(\mathfrak{a})$ is reducible. Indeed, let $a, a' \in A \setminus \mathfrak{a}$ with $aa' \in \mathfrak{a}$. Then $\mathfrak{a}$ is strictly contained in both $(\mathfrak{a}, a)$ and $(\mathfrak{a}, a')$, and $(\mathfrak{a}, a) \cdot (\mathfrak{a}, a')$ is contained in $\mathfrak{a}$, in particular $(\mathfrak{a}, a)$ and $(\mathfrak{a}, a')$ are both strict ideals. Consequently, $V(\mathfrak{a}) = V(\mathfrak{a}, a) \cup V(\mathfrak{a}, a')$ and $V(\mathfrak{a}, a) \neq \emptyset \neq V(\mathfrak{a}, a')$. It remains to show that $V(\mathfrak{a}, a) \neq V(\mathfrak{a}) \neq V(\mathfrak{a}, a')$. So assume $V(\mathfrak{a}, a) = V(\mathfrak{a})$. This means that every prime $\mathfrak{p}$ which contains $\mathfrak{a}$ also contains a, from which it follows that $a \in \cap\{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{a} \subseteq \mathfrak{p}\}$. Since $\mathfrak{a}$ is a radical ideal, it follows from Lemma 4.8 (3) that $a \in \mathfrak{a}$ which is not the case. The argument for a' is the same. □

2.46. **Example** Let A be a PID. By the above discussion, and the fact that non-zero prime ideals are maximal, we find that $\mathrm{Spec}(A)$ consists of the closed points $\{\mathfrak{p}\}$ where $\mathfrak{p}$ is a non-zero prime, and the point $\{0\}$. Moreover, $\overline{\{0\}} = V(0) = \mathrm{Spec}(A)$, so that the one-element set $\{0\} \subseteq \mathrm{Spec}(A)$ is *dense*. Moreover, for non-zero primes $\mathfrak{p}, \mathfrak{q}$ we have $\mathfrak{q} \in V(\mathfrak{p})$ if and only if $\mathfrak{q} = \mathfrak{p}$. Finally, let $\mathfrak{a}$ be a strict ideal of A and we aim to describe $V(\mathfrak{a})$. Since A is a PID, $\mathfrak{a} = (a)$ for some element a which can be written as a product of primes $p_1 \cdots p_k$ (recall that $\mathfrak{a} \neq A$ and hence a is a non-unit) and write $\mathfrak{p}_i = (p_i)$ for the generated ideals. Then we get

$$V(\mathfrak{a}) = V(\mathfrak{p}_1 \cdots \mathfrak{p}_k) = \bigcup_{i=1}^{k} V(\mathfrak{p}_i)$$

describing $V(\mathfrak{a})$ as a union of closed irreducible subspaces (which are in fact all singleton spaces, since each $\mathfrak{p}_i$ is maximal).

2.47. **Lemma** *Let $f\colon A \to B$ be a morphism in* CAlg. *Then the map $f^{-1}\colon \mathrm{Spec}(B) \to \mathrm{Spec}(A)$, sending $\mathfrak{q}$ to $f^{-1}(\mathfrak{q})$ is a continuous map.*

Proof. If $\mathfrak{q}$ is a prime ideal, the so is $f^{-1}(\mathfrak{q})$. In particular, the map is a well-defined map of sets. To see that it is continuous, we need to show that $f^{-1}(V(T)))$ is a closed subset of $\mathrm{Spec}(B)$ is $T \subseteq A$ is a subset (because the closed subsets of $\mathrm{Spec}(A)$ are of the form $V(T)$). For this we calculate

$$f^{-1}(V(T)) = \{\mathfrak{q} \in \mathrm{Spec}(B) \mid T \subseteq f^{-1}(\mathfrak{q})\} = \{\mathfrak{q} \in \mathrm{Spec}(B) \mid f(T) \subseteq \mathfrak{q}\} = V(f(T)).$$

□

2.48. **Corollary** *We have a functor* $\mathrm{Spec}(-)\colon \mathrm{CAlg}^{\mathrm{op}} \to \mathrm{Top}$.

Proof. It remains to check that $\mathrm{id}^{-1}\colon \mathrm{Spec}(A) \to \mathrm{Spec}(A)$ is in fact the identity (which is clear) and that for two composable maps in CAlg, $f\colon A \to B$ and $g\colon B \to C$, we have that

$$f^{-1} \circ g^{-1} = (gf)^{-1}\colon \mathrm{Spec}(C) \to \mathrm{Spec}(A)$$

which is again clear. □

[3] apologies for this! Note, however, that the proof of Lemma 4.8 is completely elementary and does not use what we are trying to prove here. I will probably change the order in the script sometime in the future.

2.49. **Remark** The above functor Spec(−) loses a lot of information about commutative rings: Any two fields have Spec(−) simply the one-point space, and there are many commutative rings whose spectrum is Sierpinski space (the space consisting of two points, one of which is open) for instance any local PID which is not a field (these are equivalently the discrete valuation rings – we will discuss them at the end of this term). Later, and in algebraic geometry, we will equip the topological space Spec(A) with extra structure, and this extra structure in fact encodes all of the information that A has.

3. Noetherian rings

3.1. **Definition** Let $\mathfrak{a}$ be an ideal of a commutative ring A. We say that $\mathfrak{a}$ is *finitely generated* if there exist elements $a_1, \dots, a_n$ in A such that $\mathfrak{a} = (a_1, \dots, a_n)$.

Exercise. Let $\mathfrak{a}$ be an ideal and consider the set $S = \{(T) \mid T \subseteq \mathfrak{a} \text{ finite subset}\}$ of ideals of A. Show that $\mathfrak{a}$ is finitely generated if and only if S has a maximal element.

3.2. **Proposition** *Let A be a commutative ring. TFAE:*

(1) *Every ideal of A is finitely generated.*
(2) *Every ascending sequence of ideals $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \dots$ stabilizes.*
(3) *Every non-empty collection S of ideals has a maximal element (under inclusion of ideals).*

Proof. (1) ⇒ (2): Let $\mathfrak{a} = \cup_i \mathfrak{a}_i$. By (1), $\mathfrak{a}$ is finitely generated, say by elements $a_1, \dots, a_k$. Then there exists $n \geq 1$ such that all a_i lie in $\mathfrak{a}_n$. Consequently, we find $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \dots$ so that the sequence stabilizes. (2) ⇒ (3): This is a consequence of Zorn's Lemma, since by assumption (2), the union of an ascending sequence of elements in S is again an element of S. (3) ⇒ (1): Follows from the above exercise. □

3.3. **Remark** The implication (2) ⇒ (3) can also be shown without using Zorn's Lemma (and hence the axiom of choice): Indeed, suppose that S is a non-empty collection of ideals which does not have a maximal element. Pick $\mathfrak{a}_1 \in S$ and find $\mathfrak{a}_2 \in S$ containing $\mathfrak{a}_1$. Inductively, we find an ascending sequence of strict inclusions $\mathfrak{a}_n \subseteq \mathfrak{a}_{n+1}$ and hence a non-stabilizing sequence of ideals.

3.4. **Definition** A commutative ring satisfying one of the equivalent conditions of Proposition 3.2 is called *Noetherian*.

3.5. **Example** Every PID is Noetherian since every ideal is even generated by a single element.

3.6. **Definition** An A-algbera B is called *finitely generated* if there exist $n \geq 0$ and elements $b_1, \dots, b_n$ in B such that the unique map $A[X_1, \dots, X_n] \to B$ of A-algebras sending X_i to b_i is surjective.

3.7. **Remark** By Remark 2.13, a finitely generated A-algebra is isomorphic to an A-algebra of the form $A[X_1, \dots, X_n]/\mathfrak{a}$ for some $n \geq 0$ and ideal $\mathfrak{a} \subseteq A[X_1, \dots, X_n]$.

Exercise. Let B be a finitely generated A-algebra and C be a finitely generated B-algebra. Show that C is a finitely generated A-algebra.

The following theorem is called Hilbert's Basissatz.

3.8. **Theorem** *Let A be Noetherian and B be a finitely generated A-algebra. Then B is Noetherian.*

Proof. First, we observe that if the B-algebra structure map $A \to B$ is surjective, then B is Noetherian: Indeed, let $\mathfrak{b}$ be an ideal of B. Then $\mathfrak{b} = f(f^{-1}(\mathfrak{b}))$ and $f^{-1}(\mathfrak{b})$ is finitely generated, say by elements $a_1, \ldots, a_k$, since A is Noetherian. Then $\mathfrak{b}$ is generated by $f(a_1), \ldots, f(a_k)$. It therefore suffices to prove that $A[X_1, \ldots, X_n]$ is Noetherian, and then by induction that $A[X]$ is Noetherian. We prove the contraposition and assume that $A[X]$ is not Noetherian. Choose an ideal $\mathfrak{a}$ of $A[X]$ which is not finitely generated. Choose $f_1 \in \mathfrak{a}$ of minimal degree, and inductively, choose $f_n \in \mathfrak{a} \setminus (f_1, \ldots, f_{n-1})$ of minimal degree. This gives a sequence of polynomials $f_1, f_2, \ldots$ with $d_n = \deg(f_n) \geq \deg(f_{n-1}) = d_{n-1}$. Let a_i be the leading coefficient of f_i. We then consider the following ascending chain of ideals in A:

$$(a_1) \subseteq (a_1, a_2) \subseteq \cdots \subseteq (a_1, \ldots, a_n) \subseteq \ldots$$

If A is Noetherian, this sequence stabilizes, say from term n on, which implies that $a_{n+1} \in (a_1, \ldots, a_n)$ and hence $a_{n+1} = \sum_{i=1}^{n} b_i a_i$ for some b_i in A. Consider the polynomial

$$g = f_{n+1} - \sum_{i=1}^{n} b_i X^{d_{n+1}-d_i} \cdot f_i \in \mathfrak{a}.$$

By construction, we obtain $\deg(g) < d_{n+1} = \deg(f_{n+1})$. Since $f_{n+1} \notin (f_1, \ldots, f_n)$, also $g \notin (f_1, \ldots, f_n)$. But this contradicts the minimality of $\deg(f_{n+1})$ among elements of $\mathfrak{a} \setminus (f_1, \ldots, f_n)$. Therefore, the above sequence cannot stabilize, and A is not Noetherian. □

We now discuss a topological variant of the above ring theoretic definition motivated by the observation that an ascending sequence of ideals in A gives rise to a descending sequence of closed subsets of $\mathrm{Spec}(A)$.

3.9. **Definition** A topological space X is called Noetherian if every descending sequence of closed subsets $A_0 \supseteq A_1 \supseteq A_2 \supseteq \ldots$ stabilizes.

Exercise. Let X be a Noetherian topological space and $Y \subseteq X$ a subset. Then Y, equipped with the subspace topology, is also Noetherian.

3.10. **Lemma** *Let X be a topological space. TFAE:*

(1) *X is Noetherian*
(2) *every non-empty collection of closed subsets has a minimal element*
(3) *every ascending chain of open subsets $U_0 \subseteq U_1 \subseteq \ldots$ stabilizes*
(4) *every non-empty collection of open subsets has a maximal element.*

Proof. Since the operation sending a subset $A \subseteq X$ to $X \setminus A$ determines a order reversing bijection between closed and open subsets, we find that (1) $\Leftrightarrow$ (3) and (2) $\Leftrightarrow$ (4). It therefore suffices to show that (3) $\Leftrightarrow$ (4). The implication (3) $\Rightarrow$ (4) follows as in the proof of Proposition 3.2 by Zorn's lemma or as in Remark 3.3 and for the converse, note that an ascending chain has a maximal element if and only if it stabilizes. □

3.11. **Example** (1) The metric (and hence topological spaces) $\mathbb{R}$ or $\mathbb{R}^n$ for general $n \geq 1$ are not Noetherian: Consider for instance the collection of closed intervals $[-1/n, 1/n]$ with $n \geq 1$.

(2) If A is a Noetherian ring, then $\mathrm{Spec}(A)$ is a Noetherian topological space: A descending chain of closed subsets of $\mathrm{Spec}(A)$ is given by $V(\mathfrak{a}_1) \supseteq V(\mathfrak{a}_2) \supseteq \dots$ (for ideals $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \dots$). Consequently, descending chains of closed subsets in $\mathrm{Spec}(A)$ give rise to ascending chains of ideals in A. Hence, if A is Noetherian, $\mathrm{Spec}(A)$ is Noetherian as well.
(3) There are non-Noetherian commutative rings where $\mathrm{Spec}(A)$ is Noetherian: Let K be a field and consider $A = K[X_1, X_2, \dots]/(X_1^2, X_2^2, \dots)$. Then $(X_1, X_2, \dots)$ is not finitely generated, so A is not Noetherian. However, $(X_1, X_2, \dots)$ is the unique prime ideal of A (Exercise), and hence $\mathrm{Spec}(A) = \{*\}$ is trivially Noetherian.

3.12. **Definition** Let X be a topological space. A maximal irreducible subspace is called an *irreducible component* of X.

3.13. **Proposition** *Let X be a Noetherian topological space and $Y \subseteq X$ a non-empty closed subset. There exists $n \geq 1$ and irreducible closed subsets $Y_1, \dots, Y_n \subseteq X$ such that $Y = Y_1 \cup \dots \cup Y_n$ and $Y_i \not\subseteq Y_j$ for $i \neq j$. The decomposition $Y = Y_1 \cup \dots \cup Y_n$ is unique up to ordering and the Y_i's are the irreducible components of Y.*

Proof. Existence: Let S be the subset of closed subsets of X which does not admit a decomposition into closed irreducible subsets as in the statement of the proposition. If S is non-empty, then it contains a minimal element since X is Noetherian. Then Y is not irreducible, so there exists closed non-empty $Y', Y'' \subseteq Y$ with $Y = Y \cup Y'$. By minimality of Y, both Y' and Y'' can be written as finite unions of closed irreducible subspaces, and hence so can Y be, contradicting that Y is an element of S. Therefore, S is empty.

Uniqueness: Let $Y = Y_1 \cup \dots \cup Y_n = X_1 \cup \dots X_r$ be decomposition of Y into irreducible closed subspaces Y_i and X_k such that $Y_i \not\subseteq Y_j$ for $i \neq j$ and $X_k \not\subseteq X_l$ for $k \neq l$. Then $X_1 = \cup_i (X_1 \cap Y_i)$ so the irreducibility of X_1 implies (after possibly renaming the Y_i's) that $X_1 \subseteq Y_1$. Likewise $Y_1 \subseteq X_k$ for some k, so that $k = 1$ and $X_1 = Y_1$. Then consider the space $\overline{Y \setminus Y_1}$ and iterate the argument.

Now let C be an irreducible component of $Y = Y_1 \cup Y_n$ with Y_i as in the statement. Since C is irreducible, it must be contained in one of the Y_i's and since it is maximal, it must equal one of the Y_i's. Conversely, any Y_i lies in an irreducible component, so the Y_i's are precisely the irreducible components of Y. □

3.14. **Corollary** *Let X be a Noetherian topological space. Then X has only finitely many irreducible components.*

3.15. **Definition** A prime ideal $\mathfrak{p} \subseteq A$ is called *minimal* if for another prime ideal $\mathfrak{q} \subseteq \mathfrak{p}$ it follows that $\mathfrak{q} = \mathfrak{p}$.

3.16. **Lemma** *Let $\mathfrak{p} \subseteq A$ be a prime ideal. There exists a minimal prime ideal $\mathfrak{q} \subseteq \mathfrak{p}$.*

Proof. We again appeal to Zorn's lemma: Given a descending chain of prime ideals $\mathfrak{q}_i$ contained in $\mathfrak{p}$, the intersection of all $\mathfrak{q}_i$'s is again a prime ideal, and a minimal element for this chain. Consequently, there exist a minimal prime ideal contained in $\mathfrak{p}$. □

3.17. **Example** If A is a domain then $\{0\}$ is the unique minimal prime ideal.

3.18. **Proposition** *Let A be a Noetherian commutative ring. Then A has only finitely many minimal prime ideals.*

Proof. By Lemma 2.45 (3), the association $\mathfrak{a} \mapsto V(\mathfrak{a})$ gives an order reversing bijection between prime ideals and irreducible closed subsets of $\mathrm{Spec}(A)$. Hence minimal primes are bijective to irreducible components of $\mathrm{Spec}(A)$ of which there are only finitely many if A, and hence $\mathrm{Spec}(A)$, is Noetherian. □

4. Radicals

We begin with the nilradical of a commutative ring.

4.1. **Definition** Let A be a commutative ring. An element $x \in A$ is called *nilpotent* if $x^n = 0$ for some $n \geq 1$. The collection of all nilpotent elements is denoted by $\mathcal{N}_A$. The ring A is called *reduced* if $\mathcal{N}_A = \{0\}$, i.e. 0 is the only nilpotent elements.

4.2. **Remark** Nilpotent elements x are zero-divisors, for if n is minimal such that $x^n = 0$, then $x \cdot x^{n-1} = 0$. In particular, domains are reduced.

Exercise. Determine the nilpotent elements in the ring $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 2$ a natural number. Are the nilpotent elements the same as the zero-divisors? Give an explicit example of a reduced ring which is not a domain.

4.3. **Lemma** *The collection of nilpotent elements $\mathcal{N}_A \subseteq A$ is an ideal, the* nilradical *of A.*

Proof. Let $a, b \in \mathcal{N}_A$, and let $n, m \geq 1$ such that $a^n = 0 = b^m$. Then $(a+b)^{m+n} = 0$ and $(-a)^n = 0$. Therefore $\mathcal{N}_A$ is a subgroup of A. Moreover, if $x \in A$ is arbitrary, then $(ax)^n = a^n x^n = 0$ so $\mathcal{N}_A$ is indeed an ideal. □

4.4. **Definition** Let A be commutative ring. We denote by A_{red} the quotient ring $A/\mathcal{N}_A$ of A by its nilradical.

4.5. **Proposition** *Let A be a commutative ring. Then*

(1) *A_{red} is reduced, and*
(2) *$\mathcal{N}_A = \bigcap\{\mathfrak{p} \mid \mathfrak{p} \subseteq A$ prime ideal $\}$.*

Proof. (1): Assume $x \in A_{\mathrm{red}}$ is nilpotent, say $x^n = 0$ for $n \geq 1$. Choose $a \in A$ lifting x along the projection map $\pi\colon A \to A_{\mathrm{red}}$. Then $\pi(a^n) = x^n = 0$ and therefore $a^n \in \mathcal{N}$. Pick $m \geq 1$ such that $0 = (a^n)^m = a^{nm}$. This shows that $a \in \mathcal{N}$ and hence $x = \pi(a) = 0$.

(2): First, let $x \in \mathcal{N}_A$ and $\mathfrak{p}$ a prime ideal. Let $n \geq 1$ such that $x^n = 0 \in \mathfrak{p}$. Inductively, we deduce that $x \in \mathfrak{p}$, which shows one inclusion. To see the converse inclusion, let $x \in A \setminus \mathcal{N}_A$. We aim to show that there exists a prime $\mathfrak{p}$ such that $x \notin \mathfrak{p}$. Let S be the set of ideals $\mathfrak{a}$ of A such that no power x^n of x lies in $\mathfrak{a}$:

$$S = \{\mathfrak{a} \mid \forall n \geq 1 : x^n \notin \mathfrak{a}\}.$$

Then $\{0\} \in S$ (since x is not nilpotent) and therefore S is non-empty. An application of Zorn's lemma shows that S contains a maximal element $\mathfrak{p}$ (for an ascending chain of elements in S, the union is again an element in S). By construction, $x \notin \mathfrak{p}$, so it suffices to show that $\mathfrak{p}$ is prime. To do so, let $a, a' \in A \setminus \mathfrak{p}$. We need to show that $aa' \in A \setminus \mathfrak{p}$. Consider the ideals $(\mathfrak{p}, a)$ and $(\mathfrak{p}, a')$. Both contain $\mathfrak{p}$, so the maximality of $\mathfrak{p}$ in S shows that $(\mathfrak{p}, a)$ and $(\mathfrak{p}, a')$ are not contained in S. Pick $n, n' \geq 1$ such that $x^n \in (\mathfrak{p}, a)$ and $x^{n'} \in (\mathfrak{p}, a')$. Then $x^{n+n'} \in (\mathfrak{p}, aa')$ so that $(\mathfrak{p}, aa') \notin S$, showing that $aa' \notin \mathfrak{p}$ as needed. □

4.6. **Definition** Let A be a commutative ring and $\mathfrak{a}$ an ideal. The *radical* of $\mathfrak{a}$ is the set

$$\sqrt{\mathfrak{a}} = \{x \in A \mid \exists n \geq 1 \text{ such that } x^n \in \mathfrak{a}\}.$$

This is again an ideal of A and contains $\mathfrak{a}$. We say that $\mathfrak{a}$ is a radical ideal if $\mathfrak{a} = \sqrt{\mathfrak{a}}$.

4.7. **Example** Let A be a commutative ring. Then the nilradical $\mathcal{N}_A$ is a radical ideal and any prime ideal is a radical ideal.

4.8. **Lemma** *Let A be a commutative ring, $\mathfrak{a}$ an ideal and let $\pi\colon A \to A/\mathfrak{a}$ be the projection.*

(1) $\sqrt{0} = \mathcal{N}_A$,
(2) $\sqrt{\mathfrak{a}} = \pi^{-1}(\mathcal{N}_{A/\mathfrak{a}})$. *In particular, $\mathfrak{a}$ is a radical ideal if and only if $A/\mathfrak{a}$ is reduced.*
(3) $\sqrt{\mathfrak{a}} = \cap\{\mathfrak{p} \in \operatorname{Spec}(A) \mid \mathfrak{a} \subseteq \mathfrak{p}\}$.

Proof. (1): This is the definition of $\mathcal{N}_A$. (2): Is again simply spelling out definitions. The "in particular" follows since $\mathfrak{a} = \pi^{-1}(0)$ so $\mathfrak{a}$ being radical indeed is equivalent to $0 = \mathcal{N}_{A/\mathfrak{a}}$ which is the definition of $A/\mathfrak{a}$ being reduced. (3): We have

$$\sqrt{\mathfrak{a}} = \pi^{-1}\Big(\bigcap_{\mathfrak{p}\in\operatorname{Spec}(A/\mathfrak{a})} \mathfrak{p}\Big) = \bigcap_{\mathfrak{p}\in\operatorname{Spec}(A/\mathfrak{a})} \pi^{-1}(\mathfrak{p}) = \bigcap_{\mathfrak{p}\in\operatorname{Spec}(A),\mathfrak{a}\subseteq\mathfrak{p}} \mathfrak{p}$$

where the first equality is (2) together with Proposition 4.5, and the last equality is Corollary 2.15 combined with Lemma 2.26. □

4.9. **Lemma** *Let $f\colon A \to B$ be a morphism in* CAlg *and let $\mathfrak{a}, \mathfrak{a}'$ be ideals of A and $\mathfrak{b}$ be an ideal of B. Then the following assertions hold true:*

(1) *$\sqrt{\mathfrak{a}}$ is a radical ideal,*
(2) $\sqrt{\mathfrak{a}\cdot\mathfrak{a}'} = \sqrt{\mathfrak{a}\cap\mathfrak{a}'} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{a}'}$,
(3) $\sqrt{\mathfrak{a}+\mathfrak{a}'} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{a}'}}$.
(4) *$\sqrt{\mathfrak{a}} = A$ if and only if $\mathfrak{a} = A$,*
(5) *$\sqrt{\mathfrak{a}}$ and $\sqrt{\mathfrak{a}'}$ are coprime if and only if $\mathfrak{a}$ and $\mathfrak{a}'$ are coprime,*
(6) $f^{-1}(\sqrt{\mathfrak{b}}) = \sqrt{f^{-1}(\mathfrak{b})}$, *and*
(7) $(f(\sqrt{\mathfrak{a}})) \subseteq \sqrt{(f(\mathfrak{a}))}$.

Proof. (1): assume $x \in A$ and $n \geq 1$ such that $x^n \in \sqrt{\mathfrak{a}}$. Then there is $m \geq 1$ such that $x^{nm} \in \mathfrak{a}$ and hence $x \in \sqrt{\mathfrak{a}}$. (2): The inclusion $\mathfrak{a}\cdot\mathfrak{a}' \subseteq \mathfrak{a}\cap\mathfrak{a}'$ induces an inclusion of associated radicals. The other inclusion follows from the observation that $(\mathfrak{a}\cap\mathfrak{a}')^2 \subseteq \mathfrak{a}\cdot\mathfrak{a}'$. For the latter equality, the inclusion $\subseteq$ holds by definition. For the inclusion $\supseteq$ let x be such that there are n and m such that $x^n \in \mathfrak{a}$ and $x^m \in \mathfrak{a}'$. Then $x^{\max\{n,m\}} \in \mathfrak{a}\cap\mathfrak{a}'$ as needed. (3): The inclusion $\subseteq$ follows again because taking radicals preserves inclusions of ideals. Conversely, we first note that $\sqrt{a}+\sqrt{b} \subseteq \sqrt{\mathfrak{a}+\mathfrak{b}}$ since $\sqrt{\mathfrak{a}+\mathfrak{b}}$ is an ideal which contains $\sqrt{a}$ and $\sqrt{b}$. Applying radicals on both sides gives the desired inclusion. (4): This follows from the observation that if $x^n = 1$, then x is a unit. (5): Follows by combining (3) and (4). (6): $x \in \sqrt{f^{-1}(\mathfrak{b})}$ means that there is an $n \geq 1$ such that $x^n \in f^{-1}(\mathfrak{b})$ which is equivalent to the condition that $f(x) \in \sqrt{\mathfrak{b}}$ as needed (since f is a ring homomorphism). (7): Let $x \in \sqrt{\mathfrak{a}}$. Then $f(x)^n \in f(\mathfrak{a}) \subseteq (f(\mathfrak{a}))$ and so $f(x) \in \sqrt{(f(\mathfrak{a}))}$ as needed. □

4.10. **Example** (1) Consider the ring $\mathbb{Z}$ and $\mathfrak{a} = (n)$. Let $p_1, \dots, p_n$ be the distinct prime divisors of n. Then $\sqrt{\mathfrak{a}} = (p_1 \cdots p_n) = \cap_i(p_i)$. In particular, (n) is a radical ideal if

and only if every prime divisor of n divides n precisely once. For instance, we have $\sqrt{(6)} = (6)$ and $\sqrt{(18)} = (6)$ and $\sqrt{(8)} = (2)$.

(2) Let K be a field and $T \subseteq K^n$ a subset. Then the vanishing ideal $\mathcal{I}(T) = \{f \in K[X_1, \ldots, X_n] \mid \forall x \in T : f(x) = 0\}$ is a radical ideal. This is because the nilradical of a field is the zero ideal.

4.11. **Definition** Let A be a commutative ring. We define its *Jacobson radical* $\mathcal{J}_A$ to be

$$\mathcal{J}_A = \bigcap \{\mathfrak{m} \subseteq A \mid \mathfrak{m} \text{ maximal ideal}\}.$$

4.12. **Remark** Since maximal ideals are prime, there is an inclusion $\mathcal{N}_A \subseteq \mathcal{J}_A$. Furthermore, since every maximal ideal is a radical ideal, we find that $\mathcal{J}_A$ is also a radical ideal.

4.13. **Lemma** *Let A be a commutative ring. Then $x \in \mathcal{J}_A$ if and only if for all $y \in A$, we have $1 - xy \in A^\times$.*

Proof. ($\Rightarrow$): If there is $y \in A$ such that $1 - xy \in A \setminus A^\times$, then there is a maximal ideal $\mathfrak{m}$ such that $1 - xy \in \mathfrak{m}$ and therefore such that $xy \notin \mathfrak{m}$ (since $1 \notin \mathfrak{m}$). Consequently, $x \notin \mathfrak{m}$. ($\Leftarrow$): Conversely, if there exists a maximal ideal with $x \notin \mathfrak{m}$, then the image of x in the field $A/\mathfrak{m}$ is non-zero and hence invertible. Thus, there exists $y \in A$ such that $1 - xy \in \mathfrak{m} \subseteq A \setminus A^\times$. □

4.14. **Example** Consider the ring $A[X]$ for a commutative ring A. For an element $f = \sum_{i=0}^n a_i X^i$, the following assertions hold true:

(1) $f \in \mathcal{N}_{A[X]}$ if and only if for all $i \geq 0$, $a_i \in \mathcal{N}_A$.
(2) $f \in A[X]^\times$ if and only if $a_0 \in A^\times$ and for $i \geq 1$, $a_i \in \mathcal{N}_A$.

If $f \in \mathcal{J}_{A[X]}$, then Lemma 4.13 says that $1 - fX$ is a unit, and hence by (1) above all coefficients of f are nilpotent. Thus by (2), we find $\mathcal{N}_{A[X]} = \mathcal{J}_{A[X]}$. If A is reduced, we furthermore conclude from (2) that $A[X]$ is also reduced, so that $\mathcal{N}_{A[X]} = \mathcal{J}_{A[X]} = 0$.

4.15. **Example** Let K be a field and let $K[\![X]\!]$ be the power series ring over K. This is a domain (in particular reduced) so that $\mathcal{N}_{K[\![X]\!]} = 0$. On the other hand, in Example 2.41 we have observed that it is also a local ring with maximal ideal given by the ideal generated by (X). Hence, $\mathcal{J}_{K[\![X]\!]} = (X)$.

4.16. **Definition** A commutative ring A is called a *Jacobson ring* if for all prime ideals $\mathfrak{p}$ of A, one has

$$\mathfrak{p} = \bigcap \{\mathfrak{m} \subseteq A \mid \mathfrak{m} \text{ maximal with } \mathfrak{p} \subseteq \mathfrak{m}\}.$$

4.17. **Example** A field K is a Jacobson ring and $\mathbb{Z}$ is a Jacobson ring. A PID A is a Jacobson ring if and only if $\mathcal{J}_A = 0$. Indeed, all non-zero primes are maximal, so the condition is satisfied for non-zero primes. For the 0-ideal, the definition simply says $0 = \mathcal{J}_A$.

4.18. **Remark** Let A be a Jacobson ring and $\mathfrak{a}$ an ideal of A. Then $\mathcal{N}_A = \mathcal{J}_A$ and $A/\mathfrak{a}$ is also a Jacobson ring. Indeed, first we note that the definition implies that $\mathcal{J}_A \subseteq \mathfrak{p}$ for all prime ideals $\mathfrak{p}$, so that $\mathcal{J}_A \subseteq \mathcal{N}_A$ as well. The fact that $A/\mathfrak{a}$ is a Jacobson ring follows from Lemma 2.26 (3). In particular, one has $\mathcal{N}_{A/\mathfrak{a}} = \mathcal{J}_{A/\mathfrak{a}}$ for all $\mathfrak{a} \subseteq A$. Taking preimages along

the projection map $\pi\colon A \to A/\mathfrak{a}$, we get

$$\sqrt{\mathfrak{a}} = \pi^{-1}(\mathcal{N}_{A/\mathfrak{a}}) = \pi^{-1}(\mathcal{J}_{A/\mathfrak{a}}) = \bigcap\{\mathfrak{m} \mid \mathfrak{m} \text{ maximal with } \mathfrak{a} \subseteq \mathfrak{m}\}.$$

4.19. **Corollary** *A commutative ring A is a Jacobson ring if and only if for any ideal $\mathfrak{a}$ of A, one has $\mathcal{N}_{A/\mathfrak{a}} = \mathcal{J}_{A/\mathfrak{a}}$.*

Proof. The condition for each $\mathfrak{a}$ is a valid in a Jacobson ring by Remark 4.18. Conversely, if the condition holds for each $\mathfrak{a}$ it also holds for prime ideals $\mathfrak{p}$ and taking preimages as in Remark 4.18 one gets that A is a Jacobson ring. □

4.20. **Proposition** *Let A be a Noetherian domain in which every non-zero prime ideal is maximal and which contains infinitely many maximal ideals. Then A is a Jacobson ring.*

Proof. It suffices to prove that $\mathcal{J}_A = 0$, compare Example 4.17, since all non-zero primes are maximal. To do so, let $0 \neq x \in A \setminus A^\times$. We show that x only lies in finitely many prime ideals, and in particular in only finitely many maximal ideals. Since A has infinitely many maximal ideals, x is not contained in the Jacobson radical as needed. Consider the map $A \to A/(x)$. Then the prime ideals which contain x are precisely the prime ideals of $A/(x)$. Consider such a prime ideal $\mathfrak{q} \subseteq A/(x)$ and suppose $\mathfrak{q}' \subseteq \mathfrak{q}$ is a further prime ideal. Then both preimages under $A \to A/(x)$ are non-zero prime ideals, and hence must agree since the non-zero primes in A are maximal. We deduce that all prime ideals of $A/(x)$ are minimal. Since $A/(x)$ is Noetherian, there are only finitely many such minimal primes and the proposition follows. □

4.21. **Example** A PID is a Noetherian domain whose non-zero primes are maximal. Hence, a PID with infinitely many maximal ideals is a Jacobson ring. Moreover, by definition, for a local ring $(A, \mathfrak{m})$, we have $\mathcal{J}_A = \mathfrak{m} \neq 0$, so a local PID is not a Jacobson ring (unless it is a field). Local PIDs are also called discrete valuation rings, we will study them in more detail at the end of the term. This shows that the condition in Proposition 4.20 that A has infinitely many maximal ideals cannot be dropped in general.

4.22. **Example** Let A be a semi-local domain, with maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_n$. Since any two maximal ideals are coprime or equal, we deduce from the Chinese remainder theorem that $A/\cap\mathfrak{m}_i \cong \prod_i A/\mathfrak{m}_i$. If A is a Jacobson ring, then $\cap\mathfrak{m}_i = \mathcal{J}_A = \mathcal{N}_A$, and the condition that A is a domain implies that $\mathcal{N}_A = 0$. Consequently $A \cong \prod A/\mathfrak{m}_i$, which in turn implies $n = 1$ (again since A is a domain), i.e. that A is in fact local. But a local ring is Jacobson if and only if it is a field. We deduce that a semi-local domain is Jacobson if and only if it is a field.

We end this section with two further topological spaces associated to commutative rings.

4.23. **Definition** Let A be a commutative ring. We define the following subspaces of $\operatorname{Spec}(A)$:

(1) $\operatorname{Spec}_{\max}(A) = \{\mathfrak{m} \in \operatorname{Spec}(A) \mid \mathfrak{m} \text{ maximal}\}$, the *maximal spectrum* and
(2) $\operatorname{Spec}_{\mathrm{rab}}(A) = \{\mathfrak{m} \cap A \in \operatorname{Spec}(A) \mid \mathfrak{m} \subseteq A[X] \text{ maximal}\}$, the *Rabinowitsch spectrum*

4.24. **Remark** For a commutative ring A, one has that $\operatorname{Spec}_{\max}(A) \subseteq \operatorname{Spec}_{\mathrm{rab}}(A)$, since for all maximal ideals $\mathfrak{m}$ of A, one has $\mathfrak{m} = (\mathfrak{m}, X) \cap A$ and $(\mathfrak{m}, X)$ is a maximal ideal of $A[X]$.

4.25. **Lemma** *Let A be a commutative ring and $\mathfrak{a}$ a strict ideal of A. Then*

$$\sqrt{\mathfrak{a}} = \bigcap\{\mathfrak{p} \in \operatorname{Spec}_{\mathrm{rab}}(A) \mid \mathfrak{a} \subseteq \mathfrak{p}\}.$$

5. Affine algebraic geometry

5.1. **Definition** Let A be a commutative ring and B an A-algebra. An A-subalgebra of B is a subring B' whose inclusion to B is a morphism of A-algebras. For $T \subseteq B$ a subset, we denote by $A[T] \subseteq B$ the image of the tautological A-algebra morphism $A[X_t; t \in T] \to B$. The subset $T \subseteq B$ is called *algebraically independent (over A)* if the tautological map $A[X_t; t \in T] \to B$, whose image is $B[T]$, is injective. An element b of B such that $\{b\}$ is algebraically independent is called *transcendental*.

5.2. **Remark** The A-subalgebra $A[T]$ is the smallest A-subalgebra of B which contains the set T. The notation is of course misleading, since $A[T]$ does not only depend on the set T, but also the inclusion of this set as a subset of B.

5.3. **Example**
(1) Consider $\mathbb{C}$ as a $\mathbb{Z}$-algebra and the set $\{i\} \subseteq \mathbb{C}$. Then $\mathbb{Z}[\{i\}] = \mathbb{Z}[i]$ is the ring of Gaussian integers.
(2) Consider $\mathbb{C}$ as a $\mathbb{Q}$-algebra and $a \in \mathbb{C}$. If a is algebraic, let q be its minimal polynomial. Then $\mathbb{Q}[\{a\}] = \mathbb{Q}[X]/(q)$ and this is a finite field extension of $\mathbb{Q}$. If a is not algebraic (i.e. transcendental in the above sense), then the map $\mathbb{Q}[X] \to \mathbb{C}$ is injective, and $\mathbb{Q}[\{a\}] \cong \mathbb{Q}[X]$.
(3) Let K be a field and consider the function field $K(X) = \mathrm{Quot}(K[X])$ as a K-algebra. Then $K[\{X\}] = K[X]$.

Exercise. Let K be a field and $n \geq 1$. Show that there are infinitely many irreducible elements (even up to units) in $K[X_1, \ldots, X_n]$.

5.4. **Lemma** *Let K be a field and let $n \geq 1$. Then the function field $L = K(X_1, \ldots, X_n) = \mathrm{Quot}(K[X_1, \ldots, X_n])$ is not finitely generated over K.*

Proof. Pick an arbitrary finite subset $\{y_1, \ldots, y_m\}$ of L. We will show that the inclusion $K[y_1, \ldots, y_m] \subseteq L$ is strict, so L is not finitely generated over K. To do so, for $1 \leq i \leq m$, we write $y_i = f_i/g_i$ for $f_i, g_i \in K[X_1, \ldots, X_n]$. Pick an irreducible element $p \in K[X_1, \ldots, X_n]$ coprime to $g_1 \cdots g_m$. We claim that $1/p$ (which is an element of L) is not contained in $K[y_1, \ldots, y_m]$. Indeed, to the contrary, suppose it is. Then there is an equation

$$1/p = \sum_{I=(i_1,\ldots,i_m)} \alpha_I (y_1 \cdots y_m)^I = f/g \in L = K(X_1, \ldots, X_n)$$

where $(y_1 \cdots y_m)^I = y_1^{i_1} \cdots y_m^{i_m}$ and $\alpha_I \in K$ and the irreducible factors of g are contained in the set of irreducible factors of $g_1 \cdots g_m$.. Multiplying by p and g we obtain

$$g = p \cdot f \in K[X_1, \ldots, X_n]$$

showing that p divides g in $K[X_1, \ldots, X_n]$. However, by construction p and g are coprime, so we arrive at a contradiction. □

The following is often referred to as Zariski's main lemma:

5.5. **Lemma** *Let L/K be a field extension such that L is finitely generated as K-algebra. Then L/K is a finite field extension.*

Proof. We can choose $x_1, \ldots, x_n$ in L such that $L = K[x_1, \ldots, x_n]$. Let r be the largest number such that r many of the x_i's are algebraically independent over K, by possibly

reordering, we may assume that $x_1, \dots, x_r$ are algebraically independent, in other words, so that $K[x_1, \dots, x_r] \subseteq L$ is isomorphic to a polynomial K-algebra on r variables. Since L is a field, this inclusion factors through the function field $E = K(x_1, \dots, x_r)$ and we obtain a factorization of the field extension L/K as follows:

$$K \longrightarrow E \longrightarrow L.$$

By construction, L/E is finitely generated by the elements $x_{r+1}, \dots, x_n$ and each of these generators is algebraic over E. Consequently, L/E is finitely generated algebraic field extension and hence finite (see last terms notes). Choose a basis $\{y_1, \dots, y_d\}$ of the E-vector space L, without loss of generality we may assume that $y_1 = 1$ the unit of E. Let us denote by $\pi\colon L \to E$ the E-linear map determined by sending y_1 to 1, and for $i \geq 2$, sending y_i to zero. Then $\pi_{|E} = \mathrm{id}_E$ by construction. For $1 \leq i \leq n$, we can write

$$x_i = \sum_{j=1}^{d} \alpha_{ij} \cdot y_j \tag{1}$$

with $\alpha_{ij} \in E$. Likewise, for all $1 \leq i, j \leq d$, we can write

$$y_i \cdot y_j = \sum_{k=1}^{d} \beta_{ijk} \cdot y_k \tag{2}$$

again with $\beta_{ijk} \in E$. Let $R = K[\alpha_{ij}, \beta_{ijk}] \subseteq E$ be the sub K-algebra of E generated by all α_{ij}'s and β_{ijk}'s. By construction, R is a finitely generated K-algebra. Now let $e \in E$ be an arbitrary element. Since $E \subseteq L$ and L is finitely generated, we can write e as a polynomial in the x_i's:

$$e = \sum_I \gamma_I (x_1 \cdots x_n)^I.$$

Now substitute (1) for each x_i appearing above. Then, iteratively substituting (2), we find that e can be expressed as a linear combination of the elements $y_1, \dots, y_d$ with coefficients in the ring R. Applying π to such a presentation and using that π is E-linear (in particular it preserves multiplication by elements of R), we find that E is a finitely generated R-algebra. Since R is a finitely generated K-algebra, we deduce that E is a finitely generated K-algebra. Recalling that $E = K(x_1, \dots, x_r)$ is a function field, we deduce from Lemma 5.4 that $r = 0$, or in other words that $K = E$, so that L is indeed finite over K. □

5.6. **Proposition** *Let K be a field, let $f\colon A \to B$ be a map of K-algebras and $\mathfrak{m} \subseteq B$ a maximal ideal. If B is a finitely generated K-algebra, then $f^{-1}(\mathfrak{m})$ is maximal.*

Proof. We observe that the canonical map of K-algebras $A/f^{-1}(\mathfrak{m}) \to B/\mathfrak{m}$ is injective and that $B/\mathfrak{m}$ is a field and finitely generated over K since B is finitely generated over K. By Zariski's main lemma, we deduce that $B/\mathfrak{m}$ is a finite dimensional K-vector space. Consequently, $A/f^{-1}(\mathfrak{m})$ is also a finite dimensional K-vector space. Since it is domain (it is a subring of a field), it is a field: multiplication by any non-zero element of $A/f^{-1}(\mathfrak{m})$ is a K-linear map which is injective, and hence, by the fact that $A/f^{-1}(\mathfrak{m})$ is a finite dimensional K-vector space, also surjective. □

5.7. **Remark** For the above proposition all assumptions are necessary: If one drops the assumption that K is a field, consider the ring map $\mathbb{Z}_{(p)} \to \mathbb{Q}$. It makes $\mathbb{Q}$ a finitely generated $\mathbb{Z}_{(p)}$-algebra (exercise). Then consider $\{0\} \subseteq \mathbb{Q}$ the unique maximal ideal. Its preimage is

again $\{0\}$ which is not maximal in $\mathbb{Z}_{(p)}$. If one drops the assumption that B is finitely generated as K-algebra, consider $K[X] \to K(X)$ and again the ideal $\{0\} \subseteq K(X)$.

5.8. **Definition** Let K be a field and $n \geq 1$. We write $\mathbb{A}^n_K = K^n$ for the set of n-tuples of elements of K and call $\mathbb{A}^n_K$ the *n-dimensional affine space over K*.

The following is often referred to as the weak Nullstellensatz.

5.9. **Proposition** *Let K be an algebraically closed field and $\mathfrak{m} \subseteq K[X_1, \ldots, X_n]$ a maximal ideal. Then there exists $a = (a_1, \ldots, a_n) \in \mathbb{A}^n_K$ such that $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$.*

Proof. First, we note that the result is true for $n = 1$: Indeed, maximal ideals of $K[X_1]$ are generated by a single monic and irreducible polynomial. Since K is algebraically closed, an irreducible polynomial has degree one, hence is of the form $X - a$ if monic. Now in general, for $i \in \{1, \ldots, n\}$, let $j_i \colon K[X_i] \to K[X_1, \ldots, X_n]$ be the inclusion. By Proposition 5.6, $j_i^{-1}(\mathfrak{m})$ is a maximal ideal of $K[X_i]$ and hence of the form $(X_i - a_i)$. It follows that the elements $X_i - a_i$ of $K[X_1, \ldots, X_n]$ are contained in $\mathfrak{m}$. We deduce that $(X_1 - a_1, \ldots, X_n - a_n) \subseteq \mathfrak{m}$. Since the former is already a maximal ideal, this inclusion is an equality. □

5.10. **Definition** Let K be a field and $S \subseteq K[X_1, \ldots, X_n]$ be a subset. We set

$$V(S) = \{(a_1, \ldots, a_n) \in \mathbb{A}^n_K \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in S\} \subseteq \mathbb{A}^n_K.$$

A subset $V \subseteq \mathbb{A}^n_K$ of affine n-space is called an *affine subvariety of $\mathbb{A}^n_K$* if there is a subset $S \subseteq K[X_1, \ldots, X_n]$ such that $V = V(S)$.

5.11. **Remark** Let $S \subseteq K[X_1, \ldots, X_n]$ be a subset.

(1) Let $\mathfrak{a}_S$ be the ideal generated by S. Then $V(S) = V(\mathfrak{a}_S)$.
(2) By Hilbert's Basissatz, $K[X_1, \ldots, X_n]$ is Noetherian, so any ideal $\mathfrak{a}$ is finitely generated. Consequently, $V(S) = V(f_1, \ldots, f_n)$ for appropriate polynomials $f_1, \ldots, f_n$.
(3) Finally, we have $V(f_1, \ldots, f_n) = V(f_1) \cap \cdots \cap V(f_n)$.

5.12. **Example** (1) $\mathbb{A}^n_k$ and $\emptyset$ are affine subvarieties.

(2) Let $S = \{f_1, \ldots, f_m\}$ and all f_i are linear polynomials in $K[X_1, \ldots, X_n]$, i.e. $f_i = \sum_j a_{ij} X_j$. Then $V(S)$ is an affine subspace of $\mathbb{A}^n_K$: It is the set of solutions of the linear equations given by the f_i as we study them in linear algebra. One collects the coefficients $\{a_{ij}\}$ into a matrix (of size $m \times n$). let r be its rank. Then the affine subspace $V(S)$ has dimension $n - r$ and is given by the translate by a special solution of the equation system of the kernel of the homomorphism $K^n \to K^m$ represented by the matrix (a_{ij}).
(3) A subvariety of $\mathbb{A}^n_K$ of the form $V(f)$ for a single element $f \in K[X_1, \ldots, X_n]$ is called a *hypersurface*. By Remark 5.11 (3), any subvariety is an intersection of hypersurfaces. A hypersurface in $\mathbb{A}^2_K$ is often called a *curve*, and a hypersurface in $\mathbb{A}^3_K$ a *surface*. Interesting examples are given by $f = Y^2 - X^3 - aX - b \in K[X, Y]$, in which case $V(f)$ is an *affine elliptic curve*. Elliptic curves are very beautiful and quite well understood objects of algebraic and arithmetic geometry and have played a prominent role in the solution of Fermat's last theorem.
(4) Let V be a subvariety of $\mathbb{A}^n_K$ and W a subvariety of $\mathbb{A}^m_K$. Then the cartesian product $V \times W$ is naturally a subvariety of $\mathbb{A}^{n+m}_K$. Indeed, if $V = V(\mathfrak{a})$ and $W = V(\mathfrak{b})$, then $V \times W = V(\mathfrak{a}, \mathfrak{b})$.

5.13. **Lemma** *Let K be a field and $S \subseteq K[X_1, \dots, X_n]$. Let $\mathcal{M}_S$ denote the set of maximal ideals of $K[X_1, \dots, X_n]$ containing S. Then the association*

$$V(S) \longrightarrow \mathcal{M}_S\ , \quad a = (a_1, \dots, a_n) \mapsto (X_1 - a_1, \dots, X_n - a_n) = \mathfrak{m}_a$$

is well-defined and injective. If K is algebraically closed, it is bijective.

Proof. Consider $a = (a_1, \dots, a_n)$ and $b = (b_1, \dots, b_n)$ with $a, b \in V(S)$. We need to show that $\mathfrak{m}_a \in \mathcal{M}_S$, that is, that $S \subseteq \mathfrak{m}_a$. This is the case if for all $f \in S$, we have that $f(a_1, \dots, a_n) = 0$ since $\mathfrak{m}_a$ is the kernel of the *evaluation at a* homomorphism $K[X_1, \dots, X_n] \to K$. This is true since $a \in V(S)$. The map under consideration is therefore well-defined. To see that it is injective, assume that $\mathfrak{m}_a = \mathfrak{m}_b$. Since $X_i - a_i \in \mathfrak{m}_a$ and $X_i - b_i \in \mathfrak{m}_b$, we deduce that $a_i - b_i \in \mathfrak{m}_a \cap K = \{0\}$ for all $1 \leq i \leq n$. This shows that $a = b$, so the map is injective. Now assume that K is algebraically closed and let $\mathfrak{m} \in \mathcal{M}_S$ (i.e. $\mathfrak{m}$ is maximal and $S \subseteq \mathfrak{m}$). By Proposition 5.9 $\mathfrak{m} = \mathfrak{m}_a$ for some $a \in \mathbb{A}^n_K$. It then remains to show that $a \in V(S)$. For this, we need to see that for all $f \in S$, we have $f(a) = 0$ which follows from the assumption that $S \subseteq \mathfrak{m}_a$. □

5.14. **Remark** By definition, $\mathcal{M}_S$ is a subset of $\operatorname{Spec}(K[X_1, \dots, X_n])$. Consequently, for any $S \subseteq K[X_1, \dots, X_n]$, $V(S)$ is also a subset of $\operatorname{Spec}(K[X_1, \dots, X_n])$. In particular, any affine variety over K is a topological space (with the subspace topology of $\operatorname{Spec}(K[X_1, \dots, X_n])$. We refer to this topology on an affine variety as the *Zariski topology*. By construction, an affine variety V is a subspace of affine space $\mathbb{A}^n_K$, and the affine varieties are precisely the closed subspaces of $\mathbb{A}^n_K$. In fact, since $K[X_1, \dots, X_n]$ is Noetherian, we have seen that $\mathbb{A}^n_K$ is Noetherian and any affine variety is also Noetherian. Sometimes, people define an affine variety to be irreducible, but we shall not do so.

The following theorem is a frequently stated version of Hilbert's Nullstellensatz.

5.15. **Theorem** *Let K be an algebraically closed field and $\mathfrak{a} \subseteq K[X_1, \dots, X_n]$ a strict ideal. Then $V(\mathfrak{a})$ is not empty.*

Proof. By Lemma 5.13, $V(\mathfrak{a})$ is bijective to $\mathcal{M}_\mathfrak{a}$, the set of maximal ideals containing $\mathfrak{a}$. Since $\mathfrak{a}$ is strict, the set $\mathcal{M}_\mathfrak{a}$ is not empty, see Lemma 2.28. □

We recall the following definition.

5.16. **Definition** Let K be a field, $n \geq 1$ and $T \subseteq \mathbb{A}^n_K$ a subset. The *vanishing ideal of T* is the ideal

$$\mathcal{I}(T) = \{f \in K[X_1, \dots, X_n] \mid f(x) = 0 \text{ for all } x \in T\}.$$

Note that $\mathcal{I}(T)$ is a radical ideal of $K[X_1, \dots, X_n]$.

Given an ideal $\mathfrak{a} \subseteq K[X_1, \dots, X_n]$, there are two radical ideals we can associate to $\mathfrak{a}$: Its radical $\sqrt{\mathfrak{a}}$ on the one hand, and the vanishing ideal $\mathcal{I}(V(\mathfrak{a}))$ of the affine variety associated to $\mathfrak{a}$. By construction $\mathfrak{a} \subseteq \mathcal{I}(V(\mathfrak{a}))$, and since the latter is a radical ideal, one obtains an inclusion $\sqrt{\mathfrak{a}} \subseteq \mathcal{I}(V(\mathfrak{a}))$. The following is again a frequently stated version of Hilbert's Nullstellensatz.

5.17. **Theorem** *Let K be an algebraically closed field and $\mathfrak{a} \subseteq K[X_1, \dots, X_n]$ be an ideal. Then there is an equality*

$$\mathcal{I}(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$

We will use the following lemma for the proof of this version of Hilbert's Nullstellensatz.

5.18. **Lemma** *Let K be a field and A a finitely generated K-algebra. Then A is a Jacobson ring.*

Proof. We consider the following claims:

$$\begin{aligned}\mathfrak{p} &\subseteq \bigcap\{\mathfrak{m} \in \operatorname{Spec}_{\max}(A) \mid \mathfrak{p} \subseteq \mathfrak{m}\}\\ &\subseteq \bigcap\{\mathfrak{m}' \cap A \mid \mathfrak{p} \subseteq \mathfrak{m}' \cap A, \mathfrak{m}' \in \operatorname{Spec}_{\max}(A[X])\}\\ &= \mathfrak{p}\end{aligned}$$

The first is obvious, the second follows from Proposition 5.6 (applied to the map $A \to A[X]$), and the final claim is Lemma 4.25. Hence all inclusions are in fact equalities, which shows the lemma. □

Proof of Theorem 5.17. First assume that $\mathfrak{a} = A$. Since $V(A) = \emptyset$, we find $\mathcal{I}(V(A)) = A$. We may now restrict our attention to strict ideals $\mathfrak{a} \subseteq K[X_1, \dots, X_n]$. By Lemma 5.18, $K[X_1, \dots, X_n]$ is a Jacobson ring, so that $\sqrt{\mathfrak{a}} = \bigcap\{\mathfrak{m} \in \operatorname{Spec}_{\max}(A) \mid \mathfrak{a} \subseteq \mathfrak{m}\}$, see Remark 4.18. It therefore suffices to show that if $f \in \mathcal{I}(V(\mathfrak{a}))$ and $\mathfrak{m} \in \operatorname{Spec}_{\max}(A)$ with $\mathfrak{a} \subseteq \mathfrak{m}$, then $f \in \mathfrak{m}$. Since K is algebraically closed, Lemma 5.13 says that there is $a \in V(\mathfrak{a})$ such that $\mathfrak{m} = \mathfrak{m}_a$. Moreover, $f \in \mathfrak{m}_a$ if and only if $f(a) = 0$. But this is true since $f(x) = 0$ for all $x \in V(\mathfrak{a})$ by definition of $\mathcal{I}(V(\mathfrak{a}))$. □

5.19. **Corollary** *Let K be an algebraically closed field. Then the maps*

$$\{\mathfrak{a} \subseteq K[X_1 \dots, X_n] \mid \mathfrak{a} \text{ radical ideal }\} \underset{\mathcal{I}}{\overset{V}{\rightleftarrows}} \{V \subseteq \mathbb{A}^n_K \mid V \text{ affine subvariety of } \mathbb{A}^n_K\}$$

are order reversing inverse bijections.

Proof. Both sets are ordered by inclusion. The maps V and $\mathcal{I}$ are order reversing by construction. Now, for a radical ideal $\mathfrak{a}$, Theorem 5.17 says that $\mathcal{I}(V(\mathfrak{a})) = \mathfrak{a}$. Conversely, let $V = V(\mathfrak{a}) \subseteq \mathbb{A}^n_K$ be an affine variety. By construction, $V(\mathfrak{a}) \subseteq V(\mathcal{I}(V(\mathfrak{a}))) = V(\sqrt{\mathfrak{a}}) \subseteq V(\mathfrak{a})$, the middle equality again being Hilbert's Nullstellensatz. Therefore, all inclusions are equalities, showing the corollary. □

5.20. **Definition** Let K be a field and $V \subseteq \mathbb{A}^n_K$ an affine variety. The *coordinate ring* of V is the K-algebra

$$\mathcal{O}(V) = K[X_1, \dots, X_n]/\mathcal{I}(V).$$

Note that $\mathcal{O}(V)$ is a finitely generated and reduced K-algebra.

5.21. **Remark**

(1) We may think of $\mathcal{O}(V)$ as the ring of K-valued algebraic functions on V: First, note that $\mathcal{O}(\mathbb{A}^n_K) = K[X_1, \dots, X_n]$. Any polynomial $K[X_1, \dots, X_n]$ determines a function on $\mathbb{A}^n_K$ which can be restricted to V. Now, the ideal $\mathcal{I}(V)$ consists precisely of those functions on $\mathbb{A}^n_K$ which vanish on V, so an element of $\mathcal{O}(V)$ determines a well-defined function on V. The ring $\mathcal{O}(V)$ is sometimes also called the ring of regular functions.

(2) Let $V = V(\mathfrak{a})$ for some radical ideal $\mathfrak{a} \subseteq K[X_1, \dots, X_n]$. Then $\mathfrak{a} \subseteq \mathcal{I}(V(\mathfrak{a}))$ so that $\mathcal{O}(V(\mathfrak{a}))$ is a quotient of $K[X_1, \dots, X_n]/\mathfrak{a}$. If K is algebraically closed, then $\mathcal{I}(V(\mathfrak{a})) = \mathfrak{a}$, so $\mathcal{O}(V(\mathfrak{a})) = K[X_1, \dots, X_n]/\mathfrak{a}$.

5.22. **Corollary** *Let K be an algebraically closed field and A a finitely generated reduced K-algebra. Then $A \cong \mathcal{O}(V)$ for some affine subvariety $V \subseteq \mathbb{A}^n_K$ for some $n \geq 1$.*

Proof. Choosing a presentation, we find $A \cong K[X_1, \dots, X_n]/\mathfrak{a}$. Since A is reduced $\mathfrak{a}$ is a radical ideal. Then consider $V(\mathfrak{a}) \subseteq \mathbb{A}^n_K$ so that $\mathcal{O}(V(\mathfrak{a})) = K[X_1, \dots, X_n]/\mathfrak{a} \cong A$ by (2) of the above remark. □

5.23. **Remark** Let K be an algebraically closed field. We have now defined and studied (to some extend) the notion of affine subvarieties of $\mathbb{A}^n_K$. Given one such, say $V \subseteq \mathbb{A}^n_K$, we consider affine subvarieties of $V = V(\mathfrak{a})$, that is subsets $W \subseteq V$ which are again of the form $V(\mathfrak{b})$ for some radical ideal $\mathfrak{b}$. Since V reverses inclusions, we find that $V(\mathfrak{b}) \subseteq V(\mathfrak{a})$ implies that $\mathfrak{a} \subseteq \mathfrak{b}$. In particular, affine subvarieties of $V(\mathfrak{a})$ are determined by radical ideals $\mathfrak{b}$ which contain $\mathfrak{a}$, or equivalently, determined by radical ideals of $K[X_1, \dots, X_n]/\mathfrak{a}$ (by considering preimages). One obtains that the maps

$$\{\mathfrak{b} \subseteq K[X_1 \dots, X_n]/\mathfrak{a} \mid \mathfrak{b} \text{ radical ideal } \} \underset{\mathcal{I}}{\overset{V}{\rightleftarrows}} \{W \subseteq V(\mathfrak{a}) \mid W \text{ affine subvariety of } V(\mathfrak{a})\}$$

are order reversing inverse bijections. Note that a subvariety $V \subseteq \mathbb{A}^n_K \subseteq \mathrm{Spec}(A)$ is a topological space and that subvarieties of V are precisely the closed subsets of V in this topology, see Remark 5.14.

5.24. **Lemma** *Let K be an algebraically closed field and $V \subseteq \mathbb{A}^n_K$ an affine subvariety of $\mathbb{A}^n_K$. Then one has bijections*

1. $\{$*closed subspaces of* $V\} \cong \{$*radical ideals in* $\mathcal{O}(V)\}$,
2. $\{$*closed irreducible subspaces of* $V\} \cong \{$*prime ideals in* $\mathcal{O}(V)\}$,
3. $\{$*irreducible components of* $V\} \cong \{$*minimal prime ideals in* $\mathcal{O}(V)\}$, *and*
4. $\{$*points of* $V\} \cong \{$*maximal ideals in* $\mathcal{O}(V)\}$.

Proof. We have argued (1) in the above remark and (4) is a consequence of Hilbert's Nullstellensatz. (3) is implied by (2), so it suffices to show that $V(\mathfrak{a})$ is irreducible if and only if $\sqrt{\mathfrak{a}}$ is prime. This is the same argument as in Lemma 2.45 and in fact holds for arbitrary fields K (not necessarily algebraically closed). □

5.25. **Example**

1. Let K be a field. Then $\mathbb{A}^n_K$ is an irreducible topological space.
2. Let $f \in K[X_1, \dots, X_n]$ be an irreducible polynomial and $V = V(f)$ the associated subvariety of $\mathbb{A}^n_K$. Then V is irreducible. For a general polynomial f of positive degree, it can be written as a product of irreducible polynomials $p_1 \cdots p_n$. Then $V(f) = V(p_1) \cup \cdots \cup V(p_n)$ is the decomposition of $V(f)$ into irreducible components. For instance, consider $f = XY \in K[X, Y]$. Then $V(XY) = V(X) \cup V(Y)$ is the union of the coordinate axes in the plane.
3. Let $V \subseteq \mathbb{A}^n_K$ be an affine subvariety of $\mathbb{A}^n_K$ and let $W_i = V(\mathfrak{a}_i)$ be affine subvarieties of V, for $1 \leq i \leq r$, without loss of generality assume $\mathfrak{a}_i$ are radical ideals. Then $\mathcal{O}(W_i) = \mathcal{O}(V)/\mathfrak{a}_i$ and there is a canonical map
$$\mathcal{O}(V) \longrightarrow \prod_{i=1}^{r} \mathcal{O}(W_i)$$
given by the family of projections. The chinese remainder theorem says that this map is surjective if and only if the ideals $\mathfrak{a}_i$ are pairwise coprime, and is injective if $\cap_i \mathfrak{a}_i = 0$. Geometrically, this is interpreted as follows: The $\mathfrak{a}_i$ are pairwise coprime if and only if the W_i's are pariwise disjoint, and one has $\cap_i \mathfrak{a}_i$ if the union of the W_i's is all of V. In other words, we find that $\mathcal{O}(V)$ is isomorphic to the product over the

$\mathcal{O}(W_i)$'s exactly if V is the disjoint union of the W_i's, as one expect from a ring of functions on a geometric object.

(4) Consider $\mathfrak{a} = (Y^2 - X^3) \subseteq \mathbb{C}[X, Y]$. Then $V(\mathfrak{a}) = \{(a^3, a^2) \subseteq \mathbb{C}^2 \mid a \in \mathbb{C}\}$ is a *cusp*. Consider the map $\mathbb{C}[X, Y] \to \mathbb{C}[T]$ with $X \mapsto T^2$ and $Y \mapsto T^3$. The kernel of this map is the ideal $(Y^2 - X^3)$ (exercise), and let us denote the image by $C \subseteq \mathbb{C}[T]$. In an exercise. we will show that the cusp $V(\mathfrak{a})$ is, as a variety, not isomorphic to affine space $\mathbb{A}^1_{\mathbb{C}}$. We will do so by distinguishing their ring of functions: $\mathcal{O}(\mathbb{A}^1_{\mathbb{C}}) \cong \mathbb{C}[T]$ and by construction, $\mathcal{O}(V(\mathfrak{a})) \cong C$. In other words, we will show that C is not isomorphic to a polynomial ring in a single variable $\mathbb{C}[X]$.

Exercise. Show that C is not isomorphic to $\mathbb{C}[X]$. Hint: Show that C is not a PID by considering the ideal $(T^2, T^3) \subseteq C$.

6. Modules

6.1. **Definition** Let R be a commutative ring. An R-module consists of an abelian group M together with a ring map $R \to \mathrm{End}_{\mathbb{Z}}(M)$ written $r \mapsto (m \mapsto rm)$, and called the *scalar multiplication*. Equivalently, the scalar multiplication is determined by a map $R \times M \to M$, $(r, m) \mapsto rm$ satisfying the following axioms:

(1) $r(m + m') = rm + rm'$,
(2) $(r + r')m = rm + r'm$,
(3) $(rs)m = r(sm)$, and
(4) $1m = m$.

An R-submodule N of an R-module M is a subgroup $N \subseteq M$ closed under the scalar multiplication, that is: for $r \in R$ and $n \in N$, one has $rn \in N$. An R-module homomorphism $f\colon M \to M'$ between R-modules is a map of abelian groups, such that for all $r \in R$ and $m \in M$, one has $f(rm) = rf(m)$, i.e. that f is R-linear. We write $\mathrm{Hom}_R(M, N)$ for the set of R-linear maps from M to N and $\mathrm{Mod}(R)$ for the category of R-modules. Forgetting the scalar multiplication and the abelian group structure gives forgetful functors $\mathrm{Mod}(R) \to \mathrm{Ab} \to \mathrm{Set}$.

6.2. **Example** (1) Let K be a field. Then a K-module is precisely a K-vector space.

(2) Let R be a ring. Then R is an R-module via the multiplication map of R. An R-submodule of R is precisely an ideal of R.

(3) Let $f\colon S \to R$ be a map in CAlg. Then there is a canonical restriction of scalars functor $\mathrm{Mod}(R) \to \mathrm{Mod}(S)$, sending an R module $(M, R \to \mathrm{End}_{\mathbb{Z}}(M))$ to the S-module $(M, S \to R \to \mathrm{End}_{\mathbb{Z}}(M))$. In particular, R is canonically an S-module with module multiplication given by $s \cdot r = f(s)r$.

(4) The forgetful functor $\mathrm{Mod}(R) \to \mathrm{Ab}$ is conservative (that is, it detects isomorphisms). Indeed, if $f\colon M \to N$ is R-linear and bijective, then its inverse f^{-1} satisfies

$$f(f^{-1}(rn)) = rn = r(ff^{-1}(n)) = f(rf^{-1}(n))$$

so that the bijectivity of f implies that $f^{-1}(rn) = rf^{-1}(n)$.

(5) The forgetful functor $\mathrm{Mod}(\mathbb{Z}) \to \mathrm{Ab}$ is an isomorphism of categories (Exercise). Under this isomorphism, the forgetful functor $\mathrm{Mod}(R) \to \mathrm{Ab}$ corresponds to the restriction of scalars functor $\mathrm{Mod}(R) \to \mathrm{Mod}(\mathbb{Z})$ along the unique map of rings $\mathbb{Z} \to R$.

(6) Given an R-linear map $f\colon M \to N$, the kernel of f, $\ker(f) = \{m \in M \mid f(m) = 0\}$ is an R-submodule of M and the Image $\mathrm{Im}(f) = f(M) \subseteq N$ is canonically an R-submodule of N.

(7) Given an R-module M and an R-submodule $N \subseteq M$, the quotient of abelian groups M/N is canonically an R-module vie $r[m] = [rm]$. It satisfies the expected universal property: For any other R-module L, the quotient map induces an injection

$$\mathrm{Hom}_R(M/N, L) \longrightarrow \mathrm{Hom}_R(M, N)$$

whose image consists precisely of those R-linear maps $f\colon M \to N$ whose kernel is contained in N.

(8) Given an R-linear map $f\colon M \to N$, we define its cokernel $\mathrm{coker}(f)$ to be the quotient R-module $N/\mathrm{Im}(f)$. Kernel and cokernel then have the expected universal properties: the maps

$$\mathrm{Hom}_R(L, \ker(f)) \to \mathrm{Hom}_R(L, M) \quad \text{and} \quad \mathrm{Hom}_R(\mathrm{coker}(f), L) \to \mathrm{Hom}_R(N, L)$$

are injective with image given by those maps $L \to M$ or $N \to L$ respectively, whose composite with f is the zero map.

(9) Given an R-module M and an ideal $\mathfrak{a} \subseteq R$, we let $\mathfrak{a}M = \{\sum_i a_i m_i \mid a_i \in \mathfrak{a} \text{ and } m_i \in M\}$. This is an R-submodule of M. Then quotient R-module $M/\mathfrak{a}M$ is in the image of the restriction of scalars functor $\mathrm{Mod}(R/\mathfrak{a}) \to \mathrm{Mod}(R)$, that is, the scalar multiplication map $R \to \mathrm{End}_{\mathbb{Z}}(M/\mathfrak{a}M)$ factors through the projection $R \to R/\mathfrak{a}$.

(10) Given a family of R-modules $\{M_i\}_{i\in I}$ indexed over a set I, then the abelian groups $\bigoplus_i M_i$ and $\prod_i M_i$ canonically admit the structure of R-modules via componentwise scalar multiplication. We have that $\bigoplus_i M_i \subseteq \prod_i M_i$ is an R-submodule. These constructions are coproducts and products in the categorical sense, that is, they satisfy the following universal properties: For each $j \in I$, the canonical maps $M_j \to \bigoplus_i M_i$ and $\prod_i M_i \to M_j$ are R-linear and or another R-module N, one has that the canonical maps

$$\mathrm{Hom}_R(\bigoplus_i M_i, N) \to \prod_i \mathrm{Hom}_R(M_i, N) \quad \text{and} \quad \mathrm{Hom}_R(N, \prod_i M_i) \to \prod_i \mathrm{Hom}_R(N, M_i)$$

are bijections. We write $R^{(I)}$ for $\bigoplus_I R$ and R^I for $\prod_I R$. Modules isomorphic to $R^{(I)}$ are called *free* (on the set I), and *finitely generated free* if I is finite (in which case $R^{(I)} \cong R^I$).

(11) Given R-modules M and N, the set of R-linear maps $\mathrm{Hom}_R(M, N)$ is naturally an R-module. Indeed, first we note that it is an abelian group with monoid structure given as follows. For $f, g \in \mathrm{Hom}_R(M, N)$, define the map $f+g$ via $(f+g)(m) = f(m)+g(m)$. Immediately from the definitions, we find that $f + g \in \mathrm{Hom}_R(M, N)$. The neutral element is the zero map 0 sending all elements of M to 0. The inverse of a map f is then given by $-f$, defined via $(-f)(m) = -f(m)$. This shows that $\mathrm{Hom}_R(M, N)$ is indeed an abelian group. We define a scalar multiplication as follows: For $r \in R$ and $f \in \mathrm{Hom}_R(M, N)$ we set $(rf)(m) = rf(m)$. Since R is commutative, one checks that rf is again R-linear and that this defines an R-module structure on $\mathrm{Hom}_R(M, N)$.

(12) Given an R-linear map $f\colon M \to M'$ and another R-module N, the canonical maps

$$\mathrm{Hom}_R(N, M) \xrightarrow{f_*} \mathrm{Hom}_R(N, M') \quad \text{and} \quad \mathrm{Hom}_R(M', N) \xrightarrow{f^*} \mathrm{Hom}_R(M, N)$$

given by postcomposition and precomposition with f respectively, are R-linear. In particular, the bijections appearing in the display in (10) are isomorphisms of R-modules. These maps induce functors
(a) $\mathrm{Hom}_R(M,-)\colon \mathrm{Mod}(R) \to \mathrm{Mod}(R)$, and
(b) $\mathrm{Hom}_R(-,M)\colon \mathrm{Mod}(R)^{\mathrm{op}} \to \mathrm{Mod}(R)$,
which can in fact be combined to a single functor $\mathrm{Hom}_R(-,-)\colon \mathrm{Mod}(R)^{\mathrm{op}} \times \mathrm{Mod}(R) \to \mathrm{Mod}(R)$. Composing this functor with the forgetful functor $\mathrm{Mod}(R) \to \mathrm{Set}$ gives the usual Hom functor of the category $\mathrm{Mod}(R)$.

Exercise. The category $\mathrm{Mod}(R)$ admits all small limits and colimits and the restriction of scalar functors $\mathrm{Mod}(R) \to \mathrm{Mod}(S)$, for ring maps $S \to R$, commute with all small limits and colimits. Hint: It suffices to consider equalizers and coequalizers.

Exercise. Let M be an R-module. Then the scalar multiplication map $R \to \mathrm{End}_{\mathbb{Z}}(M)$ factors through the forgetful map $\mathrm{End}_R(M) \to \mathrm{End}_{\mathbb{Z}}(M)$, that is, scalar multiplication by a fixed element of R on M is an R-linear map.

6.3. **Definition** An R-module M is called
(1) *finitely generated*, if there exists a finite set I and a surjection $R^I \to M$. In other words, if M is a quotient of a finitely generated free R-module,
(2) *finitely presented*, if there exists a finite set I and a surjection $R^I \to M$ whose kernel is again a finitely generated R-module.
(3) *Noetherian*, if any of the following equivalent conditions are satisfied (the proof that these conditions are equivalent carries over verbatim from the case of Noetherian rings, Proposition 3.2).
   (a) all submodules of M are finitely generated,
   (b) every ascending chain of submodules of M stabilizes,
   (c) every non-empty collection of submodules of M has a maximum.

Exercise. Let M and N be Noetherian R-modules. Show that $M \oplus N$ is also Noetherian.

6.4. **Lemma** *Let R be a Noetherian ring and M an R-module. Then M is Noetherian if and only if M is finitely generated. In particular, finitely generated R-modules are finitely presented.*

Proof. Clearly M being Noetherian implies that M is finitely generated. To see the converse, we first note that R, viewed as an R-module is Noetherian, since R-submodules of R are precisely ideals of R. The above exercise shows that R^n is Noetherian for all $n \geq 1$. Since M is finitely generated, there is a surjection $R^n \to M$. For any ascending chain of R-submodules of M, the preimages along the map $R^n \to M$ now form an ascending chain of R-submodules of R^n which stabilizes since R^n is Noetherian. Consequently, the chain of submodules of M also stabilizes, so M is Noetherian. □

6.5. **Definition** Let M, N and L be R-modules. A map $f\colon M \times N \to L$ is called *R-bilinear* if for all $m, n' \in M$, $n, n' \in N$ and $r \in R$, one has:
(1) $f(m+m', n) = f(m,n) + f(m',n)$,
(2) $f(m, n+n') = f(m,n) + f(m,n')$, and
(3) $f(rm, n) = rf(m,n) = f(m, rn)$.

We denote by $\mathrm{Hom}_{R,R}(M\times N, L)$ the set of R-bilinear maps. Note again, that it is canonically an R-module via $(rf)(m,n) = r\cdot f(m,n)$.

6.6. **Remark** For R-modules M, N and L, the map

$$\mathrm{Hom}_{R,R}(M\times N, L) \to \mathrm{Hom}_R(N, \mathrm{Hom}_R(M,L))$$

sending f to the map $n \mapsto f(-,n)$ is R-linear and a bijection, hence an isomorphism of R-modules.

6.7. **Definition** Let M and N be R-modules. A tensor product of M and N consists of an R-module $M\otimes_R N$ equipped with a R-bilinear map $M\times N \to M\otimes_R N$ satisfying the following universal property: For every R-bilinear map $\varphi\colon M\times N\to L$, there exists a unique R-linear map $\bar\varphi\colon M\otimes_R N\to L$ making the diagram

$$\begin{array}{ccc} M\times N & \xrightarrow{\varphi} & L \\ \downarrow & \nearrow_{\bar\varphi} & \\ M\otimes_R N & & \end{array}$$

commute. In other words, the universal property says that the canonical map

$$\mathrm{Hom}_R(M\otimes_R N, L) \longrightarrow \mathrm{Hom}_{R,R}(M\times N, L)$$

is a bijection.

6.8. **Remark** If a tensor product exists, it is specified up to unique isomorphism by its universal property. The question thus really is, do tensor products exist. The answer is yes:

6.9. **Lemma** *Let M and N be R-modules. Then a tensor product $(M\otimes_R N, M\times N\to M\otimes_R N)$ exists.*

Proof. We define $M\otimes_R N$ by brut-force: First we consider $F(M,N) = R^{(M\times N)}$, the free R-module on the set $M\times N$. This comes with a map of sets $\iota\colon M\times N\to F(M,N)$. The universal property says that the map $\varphi\colon M\times N\to L$ extends uniquely to a map $\tilde\varphi\colon F(M,N)\to L$ of R-modules. The map ι is not R-bilinear: For instance, $\iota(rm,n)\neq r\iota(m,n)$, and likewise $\iota(m,n+n')\neq\iota(m,n)+\iota(m,n')$. So consider the sub R-module V of $F(M,N)$ generated by the set

$$\Big\{\iota(m+m',n)-\iota(m,n)-\iota(m',n), \iota(m,n+n')-\iota(m,n)-\iota(m,n'), \iota(rm,n)-r\iota(m,n), \iota(m,rn)-r\iota(m,n)\Big\}$$

where $m,m'\in M, n,n'\in N, r\in R$ are arbitrary elements. Then define $M\otimes_R N$ as the quotient R-module $F(M,N)/V$. By construction, the composite

$$M\times N \xrightarrow{\iota} F(M,N) \longrightarrow F(M,N)/V = M\otimes_R N$$

is R-bilinear. Moreover, since φ is R-bilinear, the map $\tilde\varphi$ extends uniquely to the quotient $M\otimes_R N$, showing that this object satisfies the required universal property. □

6.10. **Remark** The image under the map $M\times N\to M\otimes_R N$ of an element (m,n) is often written $m\otimes n$ and called an *elementary tensor*. It is important to keep in mind that not all elements of $M\otimes_R N$ are of this form (but they form a generating set, that is, every element is

of a sum of elementary tensors). For instance, $m \otimes n + m' \otimes n'$ is in general not an elementary tensor. But the tensor product is bilinear, so that

$$m \otimes n + m \otimes n' = m \otimes (n + n') \quad \text{and} \quad m \otimes n + m' \otimes n = (m + m') \otimes n.$$

The R-module structure is then given by $r \cdot (m \otimes n) = rm \otimes n = m \otimes rn$, that is, we are allowed to move scalars from R through the tensor sign.

6.11. **Example** Let p and q be different prime numbers. Then $\mathbb{Z}/p\mathbb{Z} \otimes \mathbb{Z}/q\mathbb{Z} = 0$. Indeed, it suffices to show that any biadditive map $f\colon \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \to M$, for an arbitrary abelian group M, is the zero map. Since $f(m,n) = mn \cdot f(1,1)$, this map is determined by $x = f(1,1)$. Moreover, this element satisfies $px = qx = 0$ since $pf(1,1) = f(p,1) = f(0,1) = 0$ and likewise $qf(1,1) = f(1,q) = f(1,0) = 0$. But since p and q are coprime, there exists n, m such that $np + mq = 1$, and consequently that

$$x = (np + mq)x = npx + mqx = 0.$$

6.12. **Example** Let p be a prime number. Then $\mathbb{Z}/p\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$. Indeed, by the same argument as above, any biadditive map $f\colon \mathbb{Z}/p\mathbb{Z} \times \mathbb{Q} \to M$ is determined by $m = f(1,1)$. Then we have

$$m = pf(1, 1/p) = f(p, 1/p) = f(0, 1/p) = 0.$$

6.13. **Lemma** *There are canonical isomorphisms $\alpha_{M,N,L}\colon (M \otimes_R N) \otimes_R L \cong M \otimes_R (N \otimes_R L)$ and canonical isomorphisms $\tau_{M,N}\colon M \otimes_R N \to N \otimes_R M$. Furthermore, there are canonical isomorphisms $R \otimes_R M \cong M \cong M \otimes_R R$. These isomorphisms make* $(\mathrm{Mod}(R), \otimes_R, R)$ *into a* symmetric monoidal category*, that is, they satisfy various coherence axioms.*

Proof. The isomorphisms α and τ are inherited from the corresponding isomorphisms for the cartesian product. Finally, the scalar multiplication map $R \times M \to M$ is R-bilinear and satisfies the universal property of a tensor product. The coherence axioms for the τ is that $\tau_{M,N} \circ \tau_{N,M} = \mathrm{id}_{N \otimes_R M}$ for all N, M and that $\tau_{R,M}$ interchanges the two isomorphisms $R \otimes_R M \cong R$ and $M \otimes_R R \cong R$. There is also a coherence axiom for the interplay of τ and α. Furthermore, there is a coherence axiom for α involving 4 objects. Have a look at the wikipedia page for (symmetric) monoidal categories. All of these coherence axioms follow from the versions for the cartesian products. □

Recall that an adjunction of categories consists of functors $F\colon \mathcal{C} \to \mathcal{D}$ and $G\colon \mathcal{D} \to \mathcal{C}$ together with a natural isomorphism

$$\tau\colon \mathrm{Hom}_{\mathcal{D}}(F(-), -) \cong \mathrm{Hom}_{\mathcal{C}}(-, G(-))\colon \mathcal{C}^{\mathrm{op}} \times \mathcal{D} \to \mathrm{Set}.$$

Given a functor $G\colon \mathcal{D} \to \mathcal{C}$, recall also that it *admits* a left adjoint if and only if for each $c \in \mathcal{C}$, the functor

$$\mathrm{Hom}_{\mathcal{C}}(c, G(-))\colon \mathcal{D} \to \mathrm{Set}$$

is corepresentable, i.e. isomorphic to $\mathrm{Hom}_{\mathcal{D}}(F(c), -)$ for some object $F(c) \in \mathcal{D}$ which is called a corepresenting object. If this is the case, choices of corepresenting objects $F(c)$ assemble into a functor $F\colon \mathcal{C} \to \mathcal{D}$ which is then left adjoint to G. This says that checking whether or not a given functor admits an adjoint is a "pointwise" question. See chapter 6 in my lecture notes "Algebra" for further details. We will freely use these notions in what follows.

6.14. **Corollary** *Let R be a commutative ring and M an R-module. Then the functor* $\mathrm{Hom}_R(M, -)\colon \mathrm{Mod}(R) \to \mathrm{Mod}(R)$ *admits a left adjoint $M \otimes_R -\colon \mathrm{Mod}(R) \to \mathrm{Mod}(R)$.*

Proof. The bilinear map $M \times N \to M \otimes_R N$ part of the tensor product corresponds to a unique linear map $N \to \mathrm{Hom}_R(M, M \otimes_R N)$. Consider the composite

$$\mathrm{Hom}(M \otimes_R N, L) \longrightarrow \mathrm{Hom}_R(\mathrm{Hom}_R(M, M \otimes_R N), \mathrm{Hom}_R(M, L)) \longrightarrow \mathrm{Hom}_R(N, \mathrm{Hom}_R(M, L)).$$

Postcomposing the final term with the canonical bijection to $\mathrm{Hom}_{R,R}(M \times N, L)$ from Remark 6.6, the composite becomes restriction along the bilinear map $M \times N \to M \otimes_R N$ and is therefore a bijection by the universal property of the tensor product. Consequently, the above composite is also a bijection, and natural in L by inspection. This precisely says that sending N to $M \otimes_R N$ assembles into a left adjoint of $\mathrm{Hom}_R(M, -)$. □

6.15. **Remark** Given a map $f\colon N \to N'$, the resulting map $\mathrm{id} \times f\colon M \times N \to M \times N' \to M \otimes_R N$ is R-bilinear and therefore extends uniquely to an R-linear map $\mathrm{id} \otimes f\colon M \otimes_R N \to M \otimes_R N'$. Unravelling the definitions, this map is indeed the effect of the functor $M \otimes_R -$ on the morphism f.

6.16. **Corollary** *Let R be a commutative ring and M an R-module. Then the functor $M \otimes_R -\colon \mathrm{Mod}(R) \to \mathrm{Mod}(R)$ preserves colimits, and the functor $\mathrm{Hom}_R(M, -)\colon \mathrm{Mod}(R) \to \mathrm{Mod}(R)$ preserves limits.*

Exercise. The functor $\mathrm{Hom}_R(-, M)\colon \mathrm{Mod}(R)^{\mathrm{op}} \to \mathrm{Mod}(R)$ also preserves limits.

6.17. **Remark** One says that a symmetric monoidal category is *closed* if for all objects M, the tensor product functor $M \otimes -$ admits a right adjoint. Consequently, $(\mathrm{Mod}(R), \otimes_R, R)$ is a closed symmetric monoidal category.

6.18. **Lemma** *Let $f\colon R \to S$ be a morphism in* CAlg *and M an R-module. Then the R-modules $S \otimes_R M$ and $\mathrm{Hom}_R(S, M)$ are canonically the restriction of S-modules with the same name.*

Proof. We need to construct S-module structures on $S \otimes_R M$ and $\mathrm{Hom}_R(S, M)$ giving rise to the canonical R-module structures via the map f. We first, consider $S \otimes_R M$. For this we consider the following composite:

$$S \times (S \otimes_R M) \longrightarrow S \otimes_R (S \otimes_R M) \cong (S \otimes_R S) \otimes_R M \longrightarrow S \otimes_R M$$

where the last map is given by the multiplication map of S (note that it is R-bilinear). On elementary tensors, this map sends $(s, s' \otimes m)$ to $ss' \otimes m$. One then checks that this indeed defines an S-module structure on $S \otimes_R M$ whose restricted R-module structure is the canonical one since $r \cdot (s \otimes m) = rs \otimes m$ by definition of the tensor product. Likewise, we define a map $S \times \mathrm{Hom}_R(S, M) \to \mathrm{Hom}_R(S, M)$ by sending (s, f) to the map sf defined by $(sf)(s') = f(ss')$. Again, one checks that this is well-defined and gives an S-module structure on $\mathrm{Hom}_R(S, M)$. The restricted R-module structure is then the canonical one, since $(rf)(s) = f(rs) = r \cdot f(s)$ by R-linearity of f. □

6.19. **Proposition** *Let $R \to S$ be a map of commutative rings. Then the restriction of scalars functor $\mathrm{Mod}(S) \to \mathrm{Mod}(R)$ admits left and right adjoint, given by $S \otimes_R -$ and $\mathrm{Hom}_R(S, -)$.*

Proof. It remains to verify natural (in S-modules N and R-modules M) bijections

$$\mathrm{Hom}_S(S \otimes_R M, N) \cong \mathrm{Hom}_R(M, N) \quad \text{and} \quad \mathrm{Hom}_R(N, M) \cong \mathrm{Hom}_S(N, \mathrm{Hom}_R(S, M)).$$

The first bijection is induced by sending a map $f\colon S \otimes_R M \to N$ to its restriction along $M \xrightarrow{\iota(1,-)} S \otimes_R M$. An inverse is given as follows: Let $g\colon M \to N$ be R-linear. Then the map

$S \times M \to N$, $(s, m) \mapsto s \cdot g(m)$ is R-bilinear, and therefore descends to a map $S \otimes_R M \to N$, which, on elementary tensors sends $s \otimes m$ to $s \cdot g(m)$. This map is evidently S-linear. The second bijection for instance is given by sending $f\colon N \to M$ to the map $N \to \mathrm{Hom}_R(S, M)$, $n \mapsto (s \mapsto f(sn))$. Its inverse is given by postcomposing with the evaluation at 1 map $\mathrm{Hom}_R(S, M) \to M$ (sending g to $g(1)$). It is a direct check to see that these maps are natural in N and M. □

Exercise. Let M be an R-module and $\mathfrak{a}$ an ideal of R. There is a canonical isomorphism $R/\mathfrak{a} \otimes_R M \to M/\mathfrak{a}M$ of $R/\mathfrak{a}$-modules.

The terms appearing in the statement of the following lemma will be explained in the proof.

6.20. **Lemma** *Let $f\colon R \to S$ be a map of commutative rings. Then the extension of scalars functor $\mathrm{Mod}(R) \to \mathrm{Mod}(S)$ canonically admits the structure of a symmetric monoidal functor. In particular, given a commutative R-algebra A, the tensor product $S \otimes_R A$ is a commutative S-algebra.*

Proof. Giving the functor $S \otimes_R -$ a symmetric monoidal structure amounts to specifying isomorphisms $S \otimes_R R \cong S$ and $\rho_{M,N}\colon (S \otimes_R M) \otimes_S (S \otimes_R N) \to S \otimes_R (M \otimes_R N)$ compatible with the associativity and symmetry isomorphisms in $\mathrm{Mod}(R)$ and $\mathrm{Mod}(S)$, respectively, see again the Wikipedia page for the exact compatibilities that are required. For the first, we use the multiplication map $S \times R \to S$, $(s, r) \mapsto sf(r)$, note that it is R-bilinear and satisfies the universal property of the tensor product. The isomorphism $\rho_{M,N}$ is given by the composite The isomorphism is given as follows:

$$\begin{aligned}(S \otimes_R M) \otimes_S (S \otimes_R N) &\cong (M \otimes_R S) \otimes_S (S \otimes_R M)\\ &\cong M \otimes_R (S \otimes_S S) \otimes_R M\\ &\cong M \otimes_R S \otimes_R M\\ &\cong S \otimes_R (M \otimes_R N).\end{aligned}$$

where all isomorphisms are associativity isomorphisms and symmetry isomorphisms (and the unitality isomorphism $S \otimes_S S \cong S$ we have also seen earlier). It then follows that $(S \otimes_R A)$ is a commutative ring with multiplication given by

$$(S \otimes_R A) \otimes_S (S \otimes_R A) \cong S \otimes_R (A \otimes_R A) \to S \otimes_R A$$

where the first is the isomorphism just discussed and the second is the multiplication map of A: Note that the multiplication map $A \times A \to A$ is R-bilinear since A is an R-algebra. Moreover, the R-algebra structure map $R \to A$ induces a ring map $S \cong S \otimes_R R \to S \otimes_R A$, making the latter an S-algebra. □

Exercise. The category of commutative R-algebras CAlg_R admits pushouts. A pushout of $B \leftarrow A \to C$ is given by $B \otimes_A C$.

6.21. **Corollary** *Let R be a commutative ring and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ pairwise coprime ideals of R. Let M be an R-module. Then the canonical map*

$$M/\bigcap_{i=1}^{n} \mathfrak{a}_i M \longrightarrow \prod_{i=1}^{n} M/\mathfrak{a}_i M$$

is an isomorphism.

Proof. Using the above exercise, this follows from the case of rings, Theorem 2.21, by applying the functor $- \otimes_R M$, and using that this functor preserves finite products (since the are also finite coproducts and this functor, as a left adjoint, preserves all colimits). Here, we use that the map used in Theorem 2.21 is a map of R-modules (which is true by construction). □

6.22. **Definition** A chain complex (M, d) of R-modules consists of a sequence

$$\dots \overset{d_{n+2}}{\to} M_{n+1} \overset{d_{n+1}}{\to} M_n \overset{d_n}{\to} M_{n-1} \to \dots$$

of composable maps of R-modules such that $\mathrm{Im}(d_{n+1}) \subseteq \ker(d_n)$ for all $n \in \mathbb{Z}$. For every $n \in \mathbb{Z}$ we can then define the nth homology module

$$H_n(M, d) = \ker(d_n)/\mathrm{Im}(d_{n+1}).$$

The chain complex is called *acyclic* if all its homology modules vanish, and acyclic at M_n if $H_n(M, d) = 0$. Acyclic chain complexes are also called *exact sequences*. Motivated by this, we shall call a chain complex simply a sequence (which is an exact sequence if and only if it is exact at each step, which means that the chain complex is acyclic). A sequence $M \overset{f}{\to} N \overset{g}{\to} L$ hence from here on means that $\mathrm{Im}(f) \subseteq \ker(g)$. An exact sequence of the form

$$0 \to M \to N \to L \to 0$$

is called a *short exact sequence*.

6.23. **Example** (1) $0 \to M \to N$ is exact (at M) if and only if $M \to N$ is injective.
(2) $M \to N \to 0$ is exact (at N) if and only if $M \to N$ is surjective.
(3) $0 \to M \overset{f}{\to} N \overset{g}{\to} L \to 0$ is exact, if f is injective, $\mathrm{Im}(f) = \ker(g)$ and g is surjective.

The following is useful Yoga involving exact sequences:

6.24. **Lemma** (Snake Lemma) *Consider the following commutative diagram of R-modules*

$$\begin{array}{ccccccc} (0 & \longrightarrow &)M' & \longrightarrow & M & \xrightarrow{p} & M'' \longrightarrow 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} \\ 0 & \longrightarrow & N' & \xrightarrow{i} & N & \longrightarrow & N''(\longrightarrow 0) \end{array}$$

Then there is a canonical exact sequence

$$(0 \to) \ker(f') \to \ker(f) \to \ker(f'') \overset{\delta}{\to} \mathrm{coker}(f') \to \mathrm{coker}(f) \to \mathrm{coker}(f'')(\to 0).$$

where δ is called the boundary map.

Proof. The boundary map is defined as follows: Pick $m'' \in \ker(f'')$ and $m \in M$ with $p(m) = m''$. By exactness of the bottom row, $f(m) \in \mathrm{Im}(i)$, we have $f(m) \in N$. Define $\delta(m'') = [f(m)] \in \mathrm{coker}(f')$. This construction depends only on m'', as one checks directly. We will then only show exactness at the spots involving δ. That any two composites involving δ are zero is clear. There are then two further cases to consider: For exactness at $\ker(f')$ it remains to show that an element of $\ker(\delta)$ can be lifted to to an element of $\ker(f)$. Second, given an element in $\mathrm{coker}(f')$ which maps to zero in $\mathrm{coker}(f)$, we need to show it is in the image of δ. Both are clear once one spells everything out. □

6.25. **Lemma** (5 Lemma) *Consider a commutative diagram*

$$\begin{array}{ccccccccc} M_0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 \\ \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_4} \\ N_0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 \end{array}$$

consisting of horizontal exact sequences. Then

(1) *f_0 surjective, f_1, f_3 injective $\Rightarrow$ f_2 injective, and*
(2) *f_4 injective, f_1, f_3 surjective $\Rightarrow$ f_2 surjective.*

Proof. We indicate (2) and leave (1) and the details as an exercise (which will also be discussed in the tutoriums). Let $x \in N_2$ and y be its image in N_3. Pick $\bar{y} \in M_3$ with $f_3(\bar{y}) = y$. The image of $\bar{y}$ in M_4 is zero since f_4 is injective and the image of y in N_4 is zero (by exactness of the lower sequence). There is thus $\tilde{y} \in M_2$ whose image in M_3 is $\bar{y}$. Consider $x - f_2(\tilde{y})$. Its image in N_3 is zero, and hence it comes from N_1. Lift this element in N_1 along f_1 to $z \in M_1$. Denote by j the map $M_1 \to M_2$. Then

$$f_2(\tilde{y} + j(z)) = f_2(\tilde{y}) + f_2(j(z)) = f_2(\tilde{y}) + x - f_2(\tilde{y}) = x$$

as needed. □

6.26. **Lemma** *Let R be a commutative ring and M an R-module. Suppose that*

$$0 \to N' \to N \to N'' \to 0$$

is a short exact sequence of R-modules. Then the sequences

(1) $0 \to \mathrm{Hom}_R(M, N') \to \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N'')$,
(2) $0 \to \mathrm{Hom}_R(N'', M) \to \mathrm{Hom}_R(N, M) \to \mathrm{Hom}_R(N', M)$, *and*
(3) $M \otimes_R N' \to M \otimes_R N \to M \otimes_R N'' \to 0$

are exact. We therefore say that $\mathrm{Hom}_R(M, -)$ *is left exact and that $M \otimes_R -$ is right exact.*

Proof. (1): The statement is equivalent to the statement that the canonical map

$$\mathrm{Hom}_R(M, \ker(N \to N'')) \longrightarrow \ker(\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N'))$$

is an isomorphism. This follows from the fact that $\mathrm{Hom}_R(M, -)$ is a right adjoint and hence preserves limits, recalling that a kernel is a limit (it is the equalizer of the given map with the zero map). Same argument works for (2) by passing to opposite categories (exercise). For (3), we now use that $M \otimes_R -$ is a left adjoint and hence preserves cokernels (these are coequalizers of the given map with the zero map). Moreover, as in (1), the exactness of (3) is equivalent to the statement that the canonical map

$$\mathrm{coker}(M \otimes_R N \to M \otimes_R N'') \longrightarrow M \otimes_R (\mathrm{coker}(N \to N''))$$

is an isomorphism. □

6.27. **Definition** Let R be a commutative ring and M an R-module. We say that M is *(1) projective, (2) injective, or (3) flat*, if for all short exact sequences

$$0 \to N' \to N \to N'' \to 0$$

we have

(1) $\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N'') \to 0$ is exact,
(2) $\mathrm{Hom}_R(N, M) \to \mathrm{Hom}_R(N', M) \to 0$ is exact, or
(3) $0 \to M \otimes_R N' \to M \otimes_R N$ is exact,

respectively.

6.28. **Remark** Together with Lemma 6.26, we find that a module M is projective if and only if the functor $\mathrm{Hom}_R(M,-)$ preserves exact sequences, is injective if and only if the functor $\mathrm{Hom}_R(-,M)$ preserves exact sequences, and flat if and only if the functor $M\otimes_R -$ preserves exact sequences.

6.29. **Definition** Let M be a flat R-module. We say that M is *faithfully flat* if a sequence $N'\to N\to N''$ which is exact after applying $M\otimes_R -$ is in fact exact.

Exercise. Let I be a filtered category and let

$$0\to A_i\to B_i\to C_i\to 0$$

denote the value at i of a functor from I to the category of short exact sequences in $\mathrm{Mod}(R)$. Show that the sequence

$$0\to \operatorname*{colim}_i A_i\to \operatorname*{colim}_i B_i\to \operatorname*{colim}_i C_i\to 0$$

is again exact. One therefore says that filtered colimits in $\mathrm{Mod}(R)$ are exact.

Exercise. Let $F\colon \mathrm{Mod}(R)\to\mathrm{Mod}(R)$ be an exact functor (i.e. one sending short exact sequences to short exact sequences). We say that F is strongly exact if a sequence $N'\to N\to N''$ is exact provided the sequence $F(N)\to F(N)\to F(N'')$ is exact. Show that F is strongly exact if and only if $F(N)=0$ implies that $N=0$ and if and only if F is conservative (that is if $F(f)$ is an isomorphism, then f is an isomorphism).

We note that the functor $M\otimes_R -$, is strongly exact if and only if M is faithfully flat.

Exercise. Show that retracts in $\mathrm{Mod}(R)$ are direct summands: Given R-module maps $M\to N$ and $N\to M$ such that $M\to N\to M$ is an isomorphism, there is an R-module N' and an isomorphism $M\oplus N'\to N$. Show that a projective module is a retract and hence in fact a direct summand of a free module.

Exercise. A finitely generated and projective R-module is finitely presented.

6.30. **Example**
(1) Free modules are projective and flat. Free, projective and flat modules are closed under direct sums.
(2) Flat modules are closed under filtered colimits (because filtered colimits are exact – exercise).
(3) Retracts (i.e. directt summands) of flat, projective, or injective modules are flat, projective, or injective, respectively. Consequently, projective modules are flat.
(4) Products of injective modules are injective.
(5) Over fields, every module is free (hence projective and flat) and injective (exercise).
(6) Rings in which free modules are injective are called self-injective, and in particular in the context of non-commutative rings do come up in nature, e.g. the quasi-Frobenius algebras which appear in representation theory.
(7) Free modules are typically not injective, see the next Lemma.

The next Lemma is called Baer's criterion for injective modules.

6.31. **Lemma** *Let M be an R-module.Then M is injective if and only if for every ideal $I \subseteq R$ of R, every R-linear map $I \to M$ extends to a map $R \to M$.*

Proof. If M is injective, any R-linear map $I \to M$ extends to R since $I \to R$ is injective. The converse is the interesting part of the statement. So let $L \to N$ be an injection of R-modules and $f\colon L \to M$ an R-linear map. Consider the set S of pairs (N', f') with $L \subseteq N' \subseteq N$ and $f'_{|L} = f$, partially ordered by inclusion: $(N', f') \leq (N'', f'')$ if and only if $N' \subseteq N''$ and $f''_{|N'} = f'$. Then Zorn's lemma implies that this set contains a maximum (for an ascending chain, consider the union), say $(\bar{N}, \bar{f})$. We wish to show that $\bar{N} = N$. So assume that $(N', f') \in S$ with N' strictly included in N. Consider $x \in N \setminus N'$ and let $I = \{i \in R \mid ix \in N'\}$. The canonical map $R \to N$ determined by x then restricts to an R-linear map $I \to N' \subseteq N$. The composite $I \to N' \to M$ can then be extended to R, by assumption, so we obtain a map $\varphi\colon R \to M$ whose restriction to I is given by $i \mapsto f'(ix)$. This defines the following diagram

$$\begin{array}{ccc} N' \oplus R & \xrightarrow{f'-\varphi} & M \\ \downarrow{\scriptstyle i+x} & & \\ N & & \end{array}$$

where $i\colon N' \to N$ denotes the inclusion and $x\colon R \to N$ the map determined by x. Assume (n', r) is in the kernel of the vertical map. Then $r \in I$ by definition of I and hence $\varphi(r) = f(rx)$. This shows that the kernel of the vertical map is contained in the kernel of the horizontal map, and in particular shows that the horizontal map factors over the image of the vertical map, giving an extension of f' to a strictly larger submodule of N. □

6.32. **Corollary** *Let A be an abelian group, viewed as $\mathbb{Z}$-module. Then A is injective if and only if A is divisible, that is, the multiplication by n map on A is surjective for all $n \geq 1$.*

6.33. **Example** The abelian group underlying a $\mathbb{Q}$-module is injective. Quotients of injective abelian groups are again injective, so $\mathbb{Q}/\mathbb{Z}$ is injective as abelian group.

As an extension of what we have seen earlier, we observe that for an R-module M, the abelian group $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ is naturally an R-module, via $rf(m) = f(rm)$. Let us write $M^{\vee\mathbb{Q}/\mathbb{Z}}$ for $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ to indicate that this is some kind of "dual" R-module.

6.34. **Lemma** *Let $M' \xrightarrow{f} M \xrightarrow{g} M''$ maps of R-modules with $\mathrm{Im}(f) \subseteq \ker(g)$. Then this sequence is exact if and only if the induced sequence*

$$(M'')^{\vee\mathbb{Q}/\mathbb{Z}} \longrightarrow M^{\vee\mathbb{Q}/\mathbb{Z}} \longrightarrow (M')^{\vee\mathbb{Q}/\mathbb{Z}}$$

is exact.

Proof. Since exactness of sequences of R-modules is determined by the underlying sequence of abelian groups, we can reformulate the statement using the terminology of the above exercise as follows: The statement is that the functor $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ is strongly exact. By the exercise, this amounts to showing that $\mathbb{Q}/\mathbb{Z}$ is injective (which we have verified above), and that $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ detects the zero abelian group. To do so, we prove the contraposition and assume that $A \neq 0$. Then there is some non-trivial element which gives rise to an inclusion $C \subseteq A$ where C is a cyclic group. Since $\mathbb{Q}/\mathbb{Z}$ is injective, we find that the resulting map

$\mathrm{Hom}(A, \mathbb{Q}/Z) \to \mathrm{Hom}(C, \mathbb{Q}/\mathbb{Z})$ is surjective, so it suffices to show that the latter is non-trivial. This follows from the fact that $\mathbb{Q}/\mathbb{Z}$ contains elements of arbitrary order: The image of the element $1/n \in \mathbb{Q}$ under the projection to $\mathbb{Q}/\mathbb{Z}$ has order n. □

The following Lemma will be used in a proof below:

6.35. **Lemma** *Let M be a finitely presented R-module and N any R-module. Then the canonical map*

$$\gamma_{M,N} \colon M \otimes_R N^{\vee\mathbb{Q}/\mathbb{Z}} \longrightarrow \mathrm{Hom}_R(M,N)^{\vee\mathbb{Q}/\mathbb{Z}}, (m,f) \mapsto (\varphi \mapsto f(\varphi(m))$$

is an isomorphism.

Proof. Let us fix an R-module N. One checks that the map as indicated is well-defined and R-linear (making use of the universal property of the tensor product). Then we observe the map $\gamma_{R,N}$ is an isomorphism (in fact, the identity, using the canonical identifications with $N^{\vee\mathbb{Q}/\mathbb{Z}}$ of source and target). Moreover, $\gamma_{M\oplus M',N}$ canonically identifies with $\gamma_{M,N} \oplus \gamma_{M',N}$. Consequently, $\gamma_{R^n,N}$ is an isomorphism for all $n \geq 1$. Now let M be a finitely presented module. Choose a finite presentation, that is, an exact sequence $R^m \to R^n \to M \to 0$. Consider then the following diagram:

$$\begin{array}{ccccccc}
R^m \otimes_R N^{\vee\mathbb{Q}/\mathbb{Z}} & \longrightarrow & R^n \otimes_R N^{\vee\mathbb{Q}/\mathbb{Z}} & \longrightarrow & M \otimes_R N^{\vee\mathbb{Q}/\mathbb{Z}} & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
\mathrm{Hom}_R(R^m,N)^{\vee\mathbb{Q}/\mathbb{Z}} & \longrightarrow & \mathrm{Hom}_R(R^n,N)^{\vee\mathbb{Q}/\mathbb{Z}} & \longrightarrow & \mathrm{Hom}_R(M,N)^{\vee\mathbb{Q}/\mathbb{Z}} & \longrightarrow & 0
\end{array}$$

A direct check shows that this diagram commutes. Moreover, both horizontal sequences are exact: For the top one, it follows from the right exactness of $- \otimes_R N^{\vee\mathbb{Q}/\mathbb{Z}}$, Lemma 6.26 (3), and for the bottom one it follows from Lemma 6.26 (2) and Lemma 6.34. By what we have already argued, the left and middle vertical maps are isomorphisms. Hence the right vertical map is also an isomorphism (e.g. by the 5-Lemma). □

For an R-module M, let us write $M^\vee = \mathrm{Hom}_R(M,R)$ for its R-linear dual module. The following variant of Lemma 6.35 holds:

6.36. **Lemma** *Let M be a finitely generated projective R-module and N any R-module. Then the canonical map*

$$M^\vee \otimes_R N \longrightarrow \mathrm{Hom}_R(M,N), \quad (f,n) \mapsto (m \mapsto f(m) \cdot n)$$

is an isomorphism.

Proof. Exercise. Hint: Use the same strategy as in the proof of Lemma 6.35. □

6.37. **Remark** R-modules satisfying the concusion of Lemma 6.36 are called dualizable. In general, there is a notion of dualizable objects in symmetric monoidal categories $\mathcal{C}$ as follows: An object $X \in \mathcal{C}$ is dualizable if there exists $Y \in \mathcal{C}$ and maps $\mathbb{1} \to X \otimes Y$ (the coevaluation) and $Y \otimes X \to \mathbb{1}$ (the evaluation) such that the two composites

$$X \longrightarrow (X \otimes Y) \otimes X \cong X \otimes (Y \otimes X) \longrightarrow X$$

$$Y \longrightarrow Y \otimes (X \otimes Y) \cong (Y \otimes X) \otimes Y \longrightarrow Y$$

are the identity of X and Y, respectively. If such a datum exists, it exists uniquely, and one writes $Y = DX$. In case the symmetric monoidal category $\mathcal{C}$ is closed, DX is necessarily of the form $\mathrm{Hom}(X, \mathbb{1})$ and an object is dualizable if and only if the canonical map

$$DX \otimes Y \longrightarrow D(X \otimes Y)$$

is an isomorphism for all Y. Exercise: Show that the dualizable R-modules are precisely the finitely generated projective ones.

There is an even stronger notion than dualizability, namely invertibility: An R-module M is called *invertible* if there exists N such that $M \otimes_R N \cong R$. Show that this implies that M is dualizable (with dual given by N which is then also written M^{-1}).

We come to some basic further relations between these properties (arguably chosen somewhat random).

6.38. **Proposition** *Let M be a finitely presented R-module. Then R is projective if and only if R is flat. In particular, flat ideals in Noetherian rings are projective.*

Proof. Consider a an exact sequence $N \to N'' \to 0$. We wish to show that

$$\mathrm{Hom}_R(M, N) \longrightarrow \mathrm{Hom}_R(M, N'') \longrightarrow 0$$

is exact. By Lemma 6.34 and Lemma 6.36, this is the case if and only if the sequence

$$0 \longrightarrow M \otimes_R (N'')^{\vee\mathbb{Q}/\mathbb{Z}} \longrightarrow M \otimes_R N^{\vee\mathbb{Q}/\mathbb{Z}}$$

is exact, which is the case since M is flat. □

6.39. **Remark** There is another way one can derive Proposition 6.38. Namely, it is a theorem of Lazard (which we shall not prove in this course) that any flat module is a filtered colimit of finitely generated free modules. Recall that a filtered colimit is a colimit indexed over a filtered category, and that a category I is called filtered if for every finite category J (that is, J is small and the cardinality of all morphisms in J is finite), every functor $J \to I$ admits a cone (not necessarily a colimit cone!). Equivalently, a non-empty category I is filtered if and only if for any two objects $x, x' \in I$ there is an object $y \in I$ and morphisms $x \to y$ and $x' \to y$, and for any two morphisms $f, g\colon x \to y$, there is a morphism $h\colon y \to z$ such that $hf = hg$.

Exercise. Show that finitely presented modules M satisfy that the functor $\mathrm{Hom}_R(M, -)$ commutes with *filtered* colimits. Prove or disprove that the same is true for finitely generated R-modules M. Using Lazard's theorem as above, show that a finitely presented and flat module is projective.

In contrast to Proposition 6.38, finitely generated and flat modules need *not* be projective. To explain a nice example, we introduce the following definitions and observations.

6.40. **Definition** A commutative ring R is called *von Neumann regular* if for all $a \in R$ there exists $x \in R$ such that $a = a^2x$.

6.41. **Example**
(1) A field is a von Neumann regular ring.
(2) For a set I and a von Neumann regular ring R_i for all $i \in I$, the product ring $\prod_i R_i$ is von Neumann regular.

(3) If R is von Neumann regular and $R \to S$ is a surjection, then S is von Neumann regular.

In particular, for a field K, the countable infinite product $\prod_{n\geq 0} K$ is von Neumann regular.

6.42. **Lemma** *Let R be a von Neumann regular ring.*

(1) *R is reduced.*
(2) *If R is a domain, then R is a field.*
(3) *Any prime ideal of R is maximal.*

Proof. (1): Suppose $a \in R$ with $a^n = 0$. Pick x such that $a = a^2x$. Then $a^{n-1} = a^n x = 0$, and by induction, $a = 0$. (2): Let $0 \neq a \in R$. Pick x such that $a = a^2x$. Since R is a domain and $a \neq 0$, we find that $1 = ax$ so that a is invertible. (3): Let $\mathfrak{p}$ be a prime ideal. Then $R/\mathfrak{p}$ is a domain and von Neumann regular by Example 6.41 (3) and hence a field by (2). □

The following proposition will be proved after we have discussed localizations, see **??**.

6.43. **Proposition** *Let R be a von Neumann regular ring and M an R-module. Then M is flat.*

In the example which follows we will make use of the following nice exercise:

Exercise. Let R be a commutative ring and I an ideal. Show that if R/I is projective, then so is I and there exists an idempotent element $i \in R$ such that $I = (i)$. In particular, I is principal.

We are now ready to consider the following example of a finitely generated flat module which is not projective.

6.44. **Example** Let K be a field and $R = \prod_{n\geq 0} K$. Then R is von Neumann regular as discussed above. Consider the ideal $I = \bigoplus_{n\geq 0} K \subseteq \prod_{n\geq 0} K = R$ and consider the R-module R/I. This is finitely generated and flat since any module over R is flat. If it were projective, by the above exercise we would have $I = (i)$ for an idempotent $i \in R$. The idempotent elements in R are precisely the elements $(a_n)_{n\geq 0}$ with $a_i \in K$ idempotent, and hence with $a_i = 0, 1$. For such an element to lie in I it must be that only finitely many of the a_i's are 1 and the rest are 0. But the ideal generated by such an element is strictly contained in I.

This example shows also that I is not a finitely generated ideal in R: If it were, then R/I were finitely presented and flat and hence projective. But we have just argued that R/I is not projective.

We now note that every R-module is a quotient of a projective R-module. One says that the category $\mathrm{Mod}(R)$ has *enough projectives*. Dually, one may wonder whether every R-module is a submodule of an injective one, saying that $\mathrm{Mod}(R)$ also has enough injectives. We prove below that this is the case. Having enough projectives/injectives implies that one can *derive additive right/left exact functors*. This is at the heart of homological algebra, and we will not touch on this topic now (but possibly later when defining Tor and Ext groups).

6.45. **Lemma** *Let M be an R-module. Then there exists an injective map $M \to Q$ with Q injective.*

Proof. Consider the R-module $M^{\vee\mathbb{Q}/\mathbb{Z}}$ and choose a surjection $F \to M^{\vee\mathbb{Q}/\mathbb{Z}}$ with F a free R-module, say on a set I. Let $F \to M$ be a surjection from a free R-module. Consider the

composite

$$M \longrightarrow (M^{\vee\mathbb{Q}/\mathbb{Z}})^{\vee\mathbb{Q}/\mathbb{Z}} \longrightarrow F^{\vee\mathbb{Q}/\mathbb{Z}} = \prod_I \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$$

We have seen that the functor $(-)^{\vee\mathbb{Q}/\mathbb{Z}}$ takes surjections to injections, so the latter map in the above composite is injective. The first map, given by sending m to $\varphi \mapsto \varphi(m)$ is also injective (Exercise). Since products of injective R-modules are injective, it therefore suffices to show that $R^{\vee\mathbb{Q}/\mathbb{Z}} = \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ is an injective R-module. This follows from the adjunction isomorphism

$$\mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})) \cong \mathrm{Hom}_{\mathbb{Z}}(N, \mathbb{Q}/\mathbb{Z})$$

and the fact that the forgetful functor $\mathrm{Mod}(R) \to \mathrm{Mod}(\mathbb{Z})$ is stricly exact (i.e. preserves and detects exact sequences). □

We continue with an important technical tool, namely Nakayama's lemma. First, we give the following version of the theorem of Cayley–Hamilton.

6.46. **Lemma** *Let R be a commutative ring and $A \in M_n(R)$ a matrix. Then the characteristic polynomial $\chi_A = \det(X \cdot \mathrm{id} - A) \in R[X]$ satisfies $\chi_A(A) = 0 \in M_n(R)$.*

Proof. First recall the following general situation. Suppose given a map of commutative rings $f\colon R \to S$. Then it induces (by componentwise application) a map $M_n(R) \to M_n(S)$, as well as a canonical map $R[X] \to S[X]$. Given a matrix $A \in M_n(R)$, let $f(A)$ be its image in $M_n(S)$. Then the characteristic polynomials satisfy $\chi_{f(A)} = f(\chi_A)$.

Now let U be the polynomial ring over $\mathbb{Z}$ on variables $\{X_{ij}\}_{1\leq i,j\leq n}$ and consider the tautological matrix $X = (X_{ij})_{1\leq i,j\leq n} \in M_n(U)$. Let $\chi_X \in U[T]$ be the characteristic polynomial of X. On the one hand, the entries of A determine a ring homomorphism $f\colon U \to R$, so that $f(X) = A$. On the other hand, we can consider the embedding $i\colon U \to K$ of U into its fraction field K. Then by the above we find that

$$\chi_A(A) = \chi_{f(X)}(f(X)) = f(\chi_X(X)).$$

Similarly, we have

$$i(\chi_X(X)) = \chi_{i(X)}(i(X)) = 0$$

where the last equality (which is one in $M_n(K)$) follows from the Cayley–Hamilton theorem for matrices over a field we learn in linear algebra. Since $i\colon M_n(U) \to M_n(K)$ is injective, we deduce that $\chi_X(X) = 0$ and hence that $\chi_A(A) = 0$ as well. □

6.47. **Proposition** *Let R be a commutative ring, $\mathfrak{a} \subseteq R$ an ideal, M a finitely generated R-module and $\phi\colon M \to M$ an R-linear endomorphism. Suppose $\varphi(M) \subseteq \mathfrak{a}M$. Then there exists a monic polynomial*

$$P = X^n + a_1X^{n-1} + \ldots a_{n-1}X + a_n \in R[X]$$

such that $a_i \in \mathfrak{a}^i$ and $0 = P(\varphi) \in \mathrm{End}_R(M)$.

Proof. Pick a generating set $m_1, \ldots, m_n$ for M. For each $1 \leq i \leq n$, write $\phi(m_i) = \sum_{j=1}^n a_{ij}m_j$ with $a_{ij} \in \mathfrak{a}$. This determines matrix $(a_{ij})_{1\leq i,j\leq n} = A \in M_n(\mathfrak{a}) \subseteq M_n(R)$ and one obtains a commutative diagram

$$\begin{array}{ccccc} & & R^n & \xrightarrow{p} & M \\ & \swarrow & \downarrow{\scriptstyle A} & & \downarrow{\scriptstyle \phi} \\ \mathfrak{a}^n & \xrightarrow{\subseteq} & R^n & \xrightarrow{p} & M \end{array}$$

where the map p is determined by the generators m_i and the lower horizontal map is the composite of p with the inclusion $\mathfrak{a}^n \to R^n$. The characteristic polynomial P of the matrix A does what we want: First, the map $\mathrm{End}_R(M) \to \mathrm{Hom}_R(R^n, M)$ obtained by precomposition with p, is injective. Moreover, one checks that $P(\varphi) \circ p = p \circ P(A)$. Then, we use that $P(A) = 0$ by Lemma 6.46 to deduce that $P(\varphi) = 0$. Second, expanding out the definition of the characteristic polynomial, we see that the coefficients satisfy the required property. □

6.48. **Corollary** *Let R be a commutative ring and M a finitely generated R-module. Let $\mathfrak{a}$ be an ideal of R such that $\mathfrak{a}M = M$, then there exists $a \in \mathfrak{a}$ such that $am = m$ for all $m \in M$.*

Proof. Consider the identity of M. By Proposition 6.47, there exists a monic polynomial $P = \sum_{i=0}^n a_i X^{n-i}$ with $P(\mathrm{id}) = 0$. Then $a = -\sum_{i=1}^n a_i$ does the job. □

6.49. **Lemma** (Nakayama Lemma) *Let R be a commutative ring and M a finitely generated R-module. Suppose that $\mathfrak{a} \subseteq \mathcal{J}_R$ is an ideal of R contained in the Jacobson radical and that $R/\mathfrak{a} \otimes_R M = 0$. Then $M = 0$.*

Proof. The condition that $R/\mathfrak{a} \otimes_R M = 0$ simply means $\mathfrak{a}M = M$. Therefore, by Corollary 6.48, there exists $a \in \mathfrak{a} \subseteq \mathcal{J}_R$ such that $(1-a)m = 0$ for all $m \in M$. However, since $a \in \mathcal{J}_R$, we find that $(1-a)$ is invertible so that $m = 0$. □

6.50. **Corollary** *Let R be a commutative ring, $\mathfrak{a} \subseteq \mathcal{J}_R$ an ideal and M a finitely generated R-module. If $N \subseteq M$ is a submodule with $N + \mathfrak{a}M = M$, then $N = M$.*

Proof. Consider M/N and apply Nakayama's lemma. □

6.51. **Corollary** *Let $(R, \mathfrak{m})$ be a local ring with residue field κ and M a finitely generated module. Let $m_1, \dots, m_n$ be elements of M which give a basis of the κ-vector space $M/\mathfrak{m}M$. Then $\{m_1, \dots, m_n\}$ is a generating set of M.*

Proof. Consider the submodule N of M generated by $m_1, \dots, m_n$ and apply the previous corollary. □

6.52. **Corollary** *Let R be a commutative ring and M a finitely generated R-module. Then any surjective R-linear map $f\colon M \to M$ is an isomorphism.*

Proof. Exercise. □

6.53. **Corollary** *Let R be a local ring and P a finitely generated projective module. Then P is free.*

Proof. Let κ be the residue field of R. Pick a generating set of P which lifts a basis of $\kappa \otimes_R P$. This determines a map $R^n \to P$ which admits a section $P \to R^n$ (by projectivity of P) and these maps become inverse isomorphisms upon applying $\kappa \otimes_R -$. Therefore $\mathrm{coker}(P \to R^n)$ is a finitely generated R-module which vanishes upon applying $\kappa \otimes_R -$, and is therefore trivial by Nakayama's lemma. □

6.54. **Remark** In fact, over local rings any projective module is free (regardless of finite generation). We will not prove this result here though.

Mathematisches Institut, Ludwig-Maximilians-Universität München, Theresienstrasse 39, 80333 München, Germany

Email address: markus.land@math.lmu.de