Commutative Algebra and Algebraic Geometry

Part I

Orlando Marigliano

January 31, 2023

Contents

Introduction

These are lecture notes for the course *Commutative Algebra and Algebraic Geometry*, held in Stockholm in Fall 2022. These notes cover the part of the course dealing with commutative algebra. They are a self-contained introduction to the subject, following the textbook *Introduction to Commutative Algebra* by Atiyah and Macdonald.

The supplementary material at the end of these notes rounds out some parts of the theory that are either not mentioned in the textbook or used out of sequence.

Each section of these notes corresponds to two lectures in the course. We start with the definition of a ring and end with Hilbert's Nullstellensatz.

1 Rings

Commutative algebra studies *commutative rings*, which we just call *rings* from now on. The subject provides a theoretical common ground for *algebraic geometry* and *algebraic number theory*. The typical example of a ring in algebraic geometry is the polynomial ring $K[t_1, \dots, t_n]$ in finitely many variables over a field K, while the typical example in number theory is the ring of integers $\mathbb{Z}$.

Commutative rings often appear in other subjects, too. In differential geometry for instance, every manifold X has its ring of smooth functions $C^\infty(X, \mathbb{R})$, and *projective modules* over this ring correspond precisely to vector bundles on X.

* * *

A *ring* is a set A together with two binary operations $+$ and $\cdot$ such that

- $(A, +)$ is an abelian group,
- $xy = yx$ for all $x, y \in A$,
- $(xy)z = x(yz)$ and $x(y + z) = xy + xz$ for all $x, y, z \in A$,
- there exists $1 \in A$ such that $1x = x$ for all $x \in A$.

Remark. If $1 = 0$ then $x = 0$ for all $x \in A$. Thus A is the *zero ring* $\{0\}$.

A *ring homomorphism* is a map of rings $f : A \to B$ such that

- f is a homomorphism of abelian groups,
- $f(xy) = f(x)f(y)$ for all $x, y \in A$,
- $f(1) = 1$.

A subset $S \subseteq A$ is a *subring* of A if S is closed under $+, \cdot$ and $1 \in S$. The identity map $S \to A$ is then a ring homomorphism.

If $f : A \to B$ and $g : B \to C$ are ring homomorphisms then so is $g \circ f$.

Ideals and quotient rings

An *ideal* $\mathfrak{a}$ of a ring A is an additive subgroup $\mathfrak{a} \subseteq A$ such that $A\mathfrak{a} \subseteq \mathfrak{a}$.

If $\mathfrak{a} \subseteq A$ is an ideal, then we can form the quotient group $A/\mathfrak{a}$, which comes with its structure group homomorphism $p : A \to A/\mathfrak{a}$ sending $x \in A$ to its equivalence class $[x]$.

There is a unique binary operation $\cdot$ on $A/\mathfrak{a}$ that makes $A/\mathfrak{a}$ into a ring and p into a ring homomorphism.

Proposition 1.1. The map $\{\text{Ideals of } A/\mathfrak{a}\} \to \{\text{Ideals of } A \text{ that contain } \mathfrak{a}\}$ defined by $\bar{\mathfrak{b}} \mapsto p^{-1}(\bar{\mathfrak{b}})$ is an order-preserving bijection.

Proof. The map defines an order-preserving bijection

$$\{\text{Additive subgroups of } A/\mathfrak{a}\} \to \{\text{Additive subgroups of } A \text{ that contain } \mathfrak{a}\}$$

whose inverse is given by $\mathfrak{b} \mapsto p(\mathfrak{b})$. It remains to show that both the map and its inverse send ideals to ideals. The former is true because p is a ring homomorphism. The latter, because p is surjective. □

If $f : A \to B$ is a ring homomorphism then $\ker(f) \subseteq A$ is an ideal, $\operatorname{im}(f) \subseteq B$ is a subring, and f induces a ring isomorphism $A/\ker(f) \simeq \operatorname{im}(f)$.

There's a one-to-one correspondence between ring homomorphisms $\overline{f} : A/\mathfrak{a} \to B$ and ring homomorphisms $f : A \to B$ satisfying $\mathfrak{a} \subseteq \ker(f)$, given by the rule $\overline{f}([x]) := f(x)$.

Zero divisors, nilpotent elements, and units

A *zero divisor* of a ring A is an element $x \in A$ such that $xy = 0$ for some $y \in A \setminus \{0\}$.

An *integral domain* is a nonzero ring with no zero divisors $\neq 0$.

An element $x \in A$ is *nilpotent* if $x^n = 0$ for some $n > 0$.

An element $x \in A$ is a *unit* if $xy = 1$ for some $y \in A$. If such a y exists it is unique and is written x^{-1}. The units in A form an abelian group $(A^\times, \cdot)$.

For $x \in A$, the set $(x) := \{ax \mid a \in A\}$ is an ideal. Such ideals are called *principal*. The element x is a unit if and only if $(x) = A$.

A *field* is a ring $A \neq 0$ where $A^\times = A \setminus \{0\}$. Every field is an integral domain.

Proposition 1.2. Let $A \neq 0$ be a ring. The following are equivalent:

(1) A is a field;
(2) the only ideals in A are (0) and (1);
(3) every ring homomorphism f of A into a ring $B \neq 0$ is injective.

Proof. (1) $\Rightarrow$ (2). Let $\mathfrak{a}$ be an ideal, let $x \neq 0$ in $\mathfrak{a}$. Since x is a unit, $A = (x) \subseteq \mathfrak{a}$.

(2) $\Rightarrow$ (3). The kernel $\ker(f)$ is an ideal which cannot be (1), so it equals (0).

(3) $\Rightarrow$ (1). Let $x \in A$. If $(x) \neq A$ then $A/(x) \neq 0$, thus the structure morphism $A \to A/(x)$ is injective, hence its kernel (x) equals (0), so $x = 0$. □

Prime ideals and maximal ideals

An ideal $\mathfrak{p} \subseteq A$ is *prime* if $\mathfrak{p} \neq A$ and for all $x, y \in A$, if $xy \in \mathfrak{p}$ then $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

An ideal $\mathfrak{m} \subseteq A$ is *maximal* if $\mathfrak{m} \neq A$ and there is no ideal $\mathfrak{a}$ such that $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq A$.

Equivalently,

- $\mathfrak{p}$ is prime $\Leftrightarrow$ $A/\mathfrak{p}$ is an integral domain,
- $\mathfrak{m}$ is maximal $\Leftrightarrow$ $A/\mathfrak{m}$ is a field. (By Prop. 1.1 and 1.2).

A maximal ideal is prime. A ring A is an integral domain if and only if (0) is prime.

Theorem 1.3. Every ring $A \neq 0$ has a maximal ideal.

Proof. Recall Zorn's lemma:

> Let S be a nonempty partially ordered set such that every totally ordered subset $T \subseteq S$ has an upper bound in S. Then S has a maximal element.

Apply this to the set S of all ideals $\neq A$ in A, ordered by inclusion. This set is nonempty because $(0) \in S$. If $T \subseteq S$ is totally ordered then $\bigcup T$ is an ideal $\neq A$, so $\bigcup T \in S$ is an upper bound for T. Hence S has a maximal element. □

Corollary 1.4. If $\mathfrak{a} \neq A$ is an ideal of A, there exists a maximal ideal of A containing $\mathfrak{a}$.

Proof. Apply Thm. 1.3 to $A/\mathfrak{a}$ and use Prop. 1.1. □

Corollary 1.5. Every non-unit x of A is contained in a maximal ideal.

Proof. We have $(x) \neq A$. Now apply Cor. 1.4. □

A *local ring* is a ring A with exactly one maximal ideal $\mathfrak{m}$. Its *residue field* is $A/\mathfrak{m}$.

Proposition 1.6. Let A be a ring and $\mathfrak{m} \subseteq A$ an ideal. If every $x \in A \setminus \mathfrak{m}$ is a unit, then A is a local ring and $\mathfrak{m}$ its maximal ideal.

Proof. If $\mathfrak{a} \neq A$ is an ideal, then $\mathfrak{a} \subseteq A \setminus A^\times \subseteq \mathfrak{m}$, so $\mathfrak{m}$ is the only maximal ideal. □

The nilradical

Proposition 1.7. The set $\operatorname{nil}(A)$ of all nilpotent elements in a ring A is an ideal, and $A/\operatorname{nil}(A)$ has no nilpotent element $\neq 0$.

Proof. Let $x, y \in \operatorname{nil}(A)$ and $a \in A$. Then $x^m = y^n = 0$ for some $n, m > 0$. We have $(ax)^n = 0$, so $ax \in \operatorname{nil}(A)$, and

$$(x+y)^{m+n} = \sum_{r+s=m+n} \binom{r}{m+n} x^r y^s = 0,$$

since if $r + s = m + n$ then $r \geq m$ or $s \geq n$. Hence $x + y \in \operatorname{nil}(A)$.

Let $x \in A$ such that its image $\overline{x}$ in $A/\operatorname{nil}(A)$ is nilpotent. Then $\overline{x}^n = 0$ for some $n > 0$, so $x^n \in \operatorname{nil}(A)$. Hence $0 = (x^n)^m = x^{n+m}$ for some $m > 0$, so $x \in \operatorname{nil}(A)$ and $\overline{x} = 0$. □

The ideal $\operatorname{nil}(A)$ is the *nilradical* of A.

Lemma 1.8. Let $f : A \to B$ be a ring homomorphism and $\mathfrak{p} \subseteq B$ a prime ideal. Then $\mathfrak{p}^c := f^{-1}(\mathfrak{p})$ is a prime ideal.

Proof. We have $\mathfrak{p}^c \neq (1)$ since $\mathfrak{p} \neq (1)$ and $\mathfrak{p}^c = \ker(A \to B/\mathfrak{p})$, so $A/\mathfrak{p}^c$ is isomorphic to a subring of $B/\mathfrak{p}$, which is an integral domain. □

Lemma 1.9. Let A be a ring, $f \in A$, and $A_f := A[t]/(tf - 1)$. Then $A_f = 0$ if and only if f is nilpotent.

Proof. For "$\Leftarrow$", the image of f under $A \to A_f$ is nilpotent and a unit, thus $A_f = 0$.

For "$\Rightarrow$", if $A_f = 0$ then $-1 \in (tf - 1)$ in $A[t]$. Thus there exists a polynomial $g(t) = a_0 + a_1 t + \ldots + a_n t^n$ such that $tfg(t) - g(t) + 1 = 0$. By comparing coefficients, we find $a_0 = 1$, $a_1 = f$, …, $a_n = f^n$, $fa_n = 0$, so $f \in \operatorname{nil}(A)$. □

Proposition 1.10. Let N be the intersection of all prime ideals of A. Then $\operatorname{nil}(A) = N$.

Proof. If $f \in A$ and $\mathfrak{p}$ is prime, $f^n = 0$ implies $f \in \mathfrak{p}$ since $0 \in \mathfrak{p}$. Hence $\operatorname{nil}(A) \subseteq N$.

Next, if $f \notin \operatorname{nil}(A)$, then $A_f \neq 0$. Let $\mathfrak{m} \subseteq A_f$ be a maximal ideal and $\mathfrak{p} := s^{-1}(\mathfrak{m})$, where $s : A \to A_f$ is the natural homomorphism. Then $s(f) \notin \mathfrak{m}$ since $s(f)$ is a unit. So $f \notin \mathfrak{p}$. Since $\mathfrak{p}$ is prime, $f \notin N$. □

Operations on ideals

The *intersection* $\bigcap_{i\in I}\mathfrak{a}_i$ of any family $(\mathfrak{a}_i)_{i\in I}$ of ideals is an ideal. Thus for any subset $E\subseteq A$ the set $(E) := \bigcap_{\mathfrak{a}\supseteq E}\mathfrak{a}$, where $\mathfrak{a}$ runs over all ideals containing E, is an ideal, the *ideal generated by* E. It is the smallest ideal containing E. We have

$$(E) = AE := \left\{ \sum_{i=1}^n a_i x_i \mid n\in\mathbb{N}, a_i\in A, x_i\in E \right\}.$$

If $E=\{x_1,\dots,x_n\}$ is finite, we write $(E)=(x_1,\dots,x_n)$.

If $(\mathfrak{a}_i)_{i\in I}$ is a family of ideals, their *sum* $\sum_{i\in I}\mathfrak{a}_i$ is the ideal generated by $\bigcup_{i\in I}\mathfrak{a}_i$. If $I=\{1,\dots,n\}$ is finite, the sum is $\mathfrak{a}_1+\dots+\mathfrak{a}_n=\{x_1+\ldots+x_n \mid x_i\in\mathfrak{a}_i\}$.

For I finite, the *product* $\mathfrak{a}_1\cdots\mathfrak{a}_n$ is the ideal generated by all products $x_1\cdots x_n$ with $x_i\in\mathfrak{a}_i$. In particular $\mathfrak{a}^n$ is defined for any ideal $\mathfrak{a}$ and $n\geq 0$, where $\mathfrak{a}^0=(1)$.

If $\mathfrak{a}+\mathfrak{b}=(1)$, the ideals $\mathfrak{a}$ and $\mathfrak{b}$ are called *coprime.*

Let $A_1,\dots,A_n$ be rings. Their *direct product*

$$A=\prod_{i=1}^n A_i=\{(x_1,\dots,x_n)\mid a_i\in A_i\}$$

is a ring with componentwise addition and multiplication, and $1=(1,\dots,1)$. It comes with ring homomorphisms ('projections') $p_i : A\to A_i$ with $p_i(x)=x_i$.

Proposition 1.11. Let A be a ring and $\mathfrak{a}_1,\dots,\mathfrak{a}_n\subseteq A$ ideals. Define the homomorphism

$$\varphi : A\to\prod_{i=1}^n(A/\mathfrak{a}_i)$$

by applying the structure morphisms $A\to A/\mathfrak{a}_i$ componentwise.

(1) If $\mathfrak{a}_i$, $\mathfrak{a}_j$ are coprime for all $i\neq j$, then $\prod_i\mathfrak{a}_i=\bigcap_i\mathfrak{a}_i$.
(2) φ is surjective if and only if $\mathfrak{a}_i,\mathfrak{a}_j$ are coprime for all $i\neq j$.
(3) φ is injective if and only if $\bigcap_i\mathfrak{a}_i=0$.

Proof. (1) We have $\prod_i\mathfrak{a}_i\subseteq\bigcap_i\mathfrak{a}_i$. For "$\supseteq$", use induction on n.

Let $n=2$ and $b_1\in\mathfrak{a}_1$, $b_2\in\mathfrak{a}_2$ with $b_1+b_2=1$. Let $a\in\mathfrak{a}_1\cap\mathfrak{a}_2$. Then

$$a=(b_1+b_2)a=b_1a+b_2a\in\mathfrak{a}_1\mathfrak{a}_2.$$

Now let $n>2$ and $\mathfrak{b}=\prod_{i>1}\mathfrak{a}_i$. For $i>1$, let $a_i\in\mathfrak{a}_1$, $b_i\in\mathfrak{a}_i$ with $a_i+b_i=1$. Then $1=(a_2+b_2)\cdots(a_n+b_n)\in\mathfrak{a}_1+b_2\cdots b_n$, thus $\mathfrak{a}_1+\mathfrak{b}=(1)$. Hence,

$$\bigcap_{i\geq 1}\mathfrak{a}_i=\mathfrak{a}_1\cap\bigcap_{i>1}\mathfrak{a}_i=\mathfrak{a}_1\cap\mathfrak{b}=\mathfrak{a}_1\mathfrak{b}=\prod_{i\geq 1}\mathfrak{a}_i.$$

(2) For "$\Rightarrow$", let $i\neq j$. Let $x\in A$ with $x\equiv 1 \pmod{\mathfrak{a}_i}$ and $x\equiv 0 \pmod{\mathfrak{a}_j}$. Then

$$1=1-x+x\in\mathfrak{a}_i+\mathfrak{a}_j.$$

For "$\Leftarrow$", note that each $y \in \prod_i A/\mathfrak{a}_i$ can be written as $y = \sum_{i=1}^n \varphi(a_i)e_i$ for some $a_1, \dots, a_n \in A$, where $e_i := (\delta_{ij})_{j=1}^n \in \prod_i A/\mathfrak{a}_i$. So, it suffices to show that all the e_i have a preimage x. Let $i \in \{1, \dots, n\}$. For all $j \neq i$, let $a_j \in \mathfrak{a}_i$, $b_j \in \mathfrak{b}_j$ with $a_j + b_j = 1$. Then $1 = \prod_{i \neq j}(a_j + b_j)$, so $x := \prod_{i \neq j} b_j$ does the job.

(3) This follows since $\ker(\varphi) = \bigcap_i \mathfrak{a}_i$. □

Proposition 1.12. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be prime ideals, let $\mathfrak{a}$ be an ideal with $\mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$. Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i.

Proof. Use induction on n. For $n = 1$ the statement is true. For $n > 1$, suppose $\mathfrak{a} \not\subseteq \mathfrak{p}_i$ for all i. Then for all i and all $j \neq i$ we have $\mathfrak{a} \not\subseteq \mathfrak{p}_j$. By the inductive assumption, for all i we have $\mathfrak{a} \not\subseteq \bigcup_{j \neq i} \mathfrak{p}_j$. So for all i there exists $x_i \in \mathfrak{a}$ such that for all $j \neq i$ we have $x_i \notin \mathfrak{p}_j$. If for any particular i we have $x_i \notin \mathfrak{p}_i$ then we are done, since we found an element $x_i \in \mathfrak{a} \setminus \bigcup_{i=1}^n \mathfrak{p}_i$. Thus we may assume that $x_i \in \mathfrak{p}_i$ for all i. Now let $y = \sum_{i=1}^n \prod_{j \neq i} x_j$. Then $y \in \mathfrak{a}$ and for all i we have $y \equiv \prod_{j \neq i} x_j \not\equiv 0 \pmod{\mathfrak{p}_i}$. Thus for all i we have $y \notin \mathfrak{p}_i$. So $\mathfrak{a} \not\subseteq \bigcup_{i=1}^n \mathfrak{p}_i$. □

Proposition 1.13. Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals and let $\mathfrak{p}$ be a prime ideal with $\mathfrak{p} \supseteq \bigcap_{i=1}^n \mathfrak{a}_i$. Then $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i. If $\mathfrak{p} = \bigcap_{i=1}^n \mathfrak{a}_i$, then $\mathfrak{p} = \mathfrak{a}_i$ for some i.

Proof. We have $\mathfrak{p} \supseteq \bigcap_{i=1}^n \mathfrak{a}_i \supseteq \prod_{i=1}^n \mathfrak{a}_i$. Assume there exists $x_i \in \mathfrak{a}_i \setminus \mathfrak{p}$ for all i. Then $\prod_{i=1}^n x_i \notin \mathfrak{p}$ because $\mathfrak{p}$ is prime. So $\mathfrak{p} \not\supseteq \bigcup_{i=1}^n \mathfrak{a}_i$. For the second statement, let $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i. Then $\mathfrak{a}_i \supseteq \bigcap_{i=1}^n \mathfrak{a}_i = \mathfrak{p} \supseteq \mathfrak{a}_i$, so $\mathfrak{p} = \mathfrak{a}_i$. □

If $\mathfrak{a}, \mathfrak{b} \subseteq A$ are ideals, the *ideal quotient* of $\mathfrak{a}$ by $\mathfrak{b}$ is the ideal

$$(\mathfrak{a} : \mathfrak{b}) := \{x \in A \mid x\mathfrak{b} \subseteq \mathfrak{a}\}.$$

In particular, $(0 : \mathfrak{b})$ is the *annihilator* $\operatorname{ann}(\mathfrak{b})$ of $\mathfrak{b}$.

The *radical* of an ideal $\mathfrak{a} \subseteq A$ is

$$\sqrt{\mathfrak{a}} = \operatorname{rad}(\mathfrak{a}) = r(\mathfrak{a}) := \{x \in A \mid x^n \in \mathfrak{a} \text{ for some } n > 0\}.$$

It is the inverse image of $\operatorname{nil}(A/\mathfrak{a})$ under the structure homomorphism $A \to A/\mathfrak{a}$, hence an ideal by Proposition 1.7.

Proposition 1.14. (1) $\mathfrak{a} \subseteq r(\mathfrak{a})$

(2) $r(r(\mathfrak{a})) = r(\mathfrak{a})$

(3) $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$

(4) $r(\mathfrak{a}) = (1) \Leftrightarrow \mathfrak{a} = (1)$

(5) $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$

(6) if $\mathfrak{p}$ is prime then $r(\mathfrak{p}^n) = \mathfrak{p}$ for all $n > 0$.

Proof. Exercise. □

Proposition 1.15. We have $\operatorname{rad} \mathfrak{a} = \bigcap \mathfrak{p}$, where $\mathfrak{p}$ runs through the prime ideals $\supseteq \mathfrak{a}$.

Proof. Apply Prop. 1.10 to $A/\mathfrak{a}$. □

Extension and contraction

Let $f : A \to B$ be a ring homomorphism, $\mathfrak{a} \subseteq A$ and $\mathfrak{b} \subseteq B$ ideals. The *extension* of $\mathfrak{a}$ is $\mathfrak{a}^e := Bf(\mathfrak{a})$. It is an ideal of B while $f(\mathfrak{a})$ is not. We have $\mathfrak{a}$ prime $\not\Rightarrow$ $\mathfrak{a}^e$ prime.

The *contraction* of $\mathfrak{b}$ is $\mathfrak{b}^c := f^{-1}(\mathfrak{b})$. It is an ideal of A. We have $\mathfrak{b}$ prime $\Rightarrow$ $\mathfrak{b}^c$ prime.

Exercise 0. Let K be a field and $f \in K[t_1, \dots, t_n]$ be a polynomial in n variables. Then we can see f as a function $K^n \to K$ by sending a point $x = (x_1, \dots, x_n)$ to $f(x) := f(x_1, \dots, x_n)$. The *vanishing set* of f is $V(f) := \{x \in K^n \mid f(x) = 0\}$.

(1) Let K be infinite. Show that $V(f) = K^n$ if and only if $f = 0$.
(2) Let K be algebraically closed. Show that $V(f) = \emptyset$ if and only if f is a unit.

Exercise 1. Let $A := K[t_1, \dots, t_n]$, where K is a field, and let $x \in K^n$ be a point.

(1) Show that the evaluation map $\varphi_x : A \to K$ defined by $\varphi_x(f) = f(x)$ is a surjective ring homomorpism.
(2) Let $\mathfrak{m}_x := \ker(\varphi_x)$. Give a finite set of generators for $\mathfrak{m}_x$.
(3) Show that $\mathfrak{m}_x$ is a maximal ideal of A.
(4) Let $y \in K^n$ be another point. Show that if $x \neq y$ then $\mathfrak{m}_x \neq \mathfrak{m}_y$.
(5) Let

$$A_x := \left\{ \frac{f}{g} \mid f, g \in A,\ g(x) \neq 0 \right\},$$

seen as a subring of the function field $K(t_1, \dots, t_n)$. Show that A_x is a local ring.

Exercise 2. Let K be a field and $A := K[t_1, \dots, t_n]$. The *variety* of a subset $E \subseteq A$ is

$$V(E) := \{x \in K^n \mid f(x) = 0 \text{ for all } f \in E\}.$$

(1) Let $E \subseteq A$ be a subset and $\mathfrak{a}$ the ideal generated by E. Show that

$$V(E) = V(\mathfrak{a}) = V(\operatorname{rad} \mathfrak{a}).$$

(2) Show that $V((0)) = K^n$ and $V((1)) = \emptyset$.
(3) Let $(\mathfrak{a}_i)_{i \in I}$ be a family of ideals of A. Show that $V(\sum_{i \in I} \mathfrak{a}_i) = \bigcap_{i \in I} V(\mathfrak{a}_i)$.
(4) Let $\mathfrak{a}, \mathfrak{b}$ be ideals of A. Show that $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$.
(5) Let $\mathfrak{a}$ be an ideal of A and $x \in K^n$. Show that $x \in V(\mathfrak{a})$ if and only if $\mathfrak{m}_x \supseteq \mathfrak{a}$. Deduce that $V(\mathfrak{m}_x) = \{x\}$.

2 Modules

For any ring A we can define the class of A-*modules*, which can be seen as "linear objects" over A. Modules are a quite general kind of object. They allow us to consider many common constructions in algebra on the same footing. For instance, the ideals $\mathfrak{a} \subseteq A$, the ring A itself, and the quotient rings $A/\mathfrak{a}$ are all A-modules, as well as all rings B which have a ring homomorphism $A \to B$ pointing to them.

If $A = K$ is a field, then the class of A-modules coincides with that of K-vector spaces. If $A = \mathbb{Z}$, then the A-modules are precisely the abelian groups. We will see in the exercises that if $A = K[t_1, \dots, t_n]$, then every A-module can be seen as a family of K-vector spaces indexed by the elements of K^n. This interpretation helps us visualize modules over polynomial rings, although it does not give a one-to-one correspondence.

* * *

A *module* over a ring A is an abelian group $(M, +)$ together with a map $\cdot : A \times M \to M$ such that for all $a, b \in A$ and $x, y \in M$,

- $a(x + y) = ax + ay$,
- $(a + b)x = ax + bx$,
- $(ab)x = a(bx)$,
- $1x = x$.

An *A-module homomorphism* between two A-modules M and N is a map $f : M \to N$ such that for all $a \in A$ and $x, y \in M$,

- $f(x + y) = f(x) + f(y)$,
- $f(ax) = af(x)$.

The composition of two A-module homomorphisms is an A-module homomorphism.

We may turn the set of all A-module homomorphism from M to N into an A-module by setting, for $f, g : M \to N$, $a \in A$, and $x \in M$,

- $(f + g)(x) := f(x) + g(x)$,
- $(af)(x) := af(x)$.

This A-module is denoted by $\mathrm{Hom}_A(M, N)$ or $\mathrm{Hom}(M, N)$.

An A-module homomorphism $f : N_1 \to N_2$ induces an A-module homomorphism

$$f \circ - : \mathrm{Hom}(M, N_1) \to \mathrm{Hom}(M, N_2)$$

by composing with f. A homomorphism $g : M_1 \to M_2$ induces a homomorphism

$$- \circ g : \mathrm{Hom}(M_2, N) \to \mathrm{Hom}(M_1, N)$$

by pre-composing with g. Thus, the constructions $\mathrm{Hom}(-, N)$ and $\mathrm{Hom}(M, -)$ can be applied to modules and to module homomorphisms. This makes them *functors*.

Examples 2.1. (1) A is an A-module.

(2) If $\mathfrak{a} \subseteq A$ is an ideal, then $\mathfrak{a}$ and $A/\mathfrak{a}$ are A-modules.

(3) If $f : A \to B$ is a ring homomorphism, then B is an A-module via $a \cdot b := f(a)b$.

(4) $\mathrm{Hom}_A(A, M) \simeq M$ as A-modules via $f \mapsto f(1)$.

(5) $M^\vee := \mathrm{Hom}_A(M, A) \not\simeq M$ in general. For instance, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(2), \mathbb{Z}) = 0$.

Submodules and quotient modules

Let M be an A-module. A *submodule* of M is a subgroup $M' \subseteq M$ such that $AM' \subseteq M'$. It is an A-module. The quotient group M/M' is an A-module via $a[x] := [ax]$. It is called the *quotient* of M by M'. The structure map $M \to M/M'$ is an A-module homomorphism. This map induces a one-to-one order-preserving correspondence between the submodules of M/M' and the submodules of M which contain M'.

If $f : M \to N$ is an A-module homomorphism, then $\ker(f)$ and $\operatorname{im}(f)$ are submodules of M, respectively N. The *cokernel* $\operatorname{coker}(f) := N/\operatorname{im}(f)$ is a quotient module of N.

If $M' \subseteq M$ is a submodule, then A-module homomorphisms $\overline{f} : M/M' \to N$ correspond to homomorphisms $f : M \to N$ such that $M' \subseteq \ker(f)$, via $\overline{f}([x]) := f(x)$. We have $\ker(\overline{f}) = \ker(f)/M'$ and $\operatorname{im}(\overline{f}) = \operatorname{im}(f)$. Thus, f induces an A-module isomorphism

$$M/\ker(f) \simeq \operatorname{im}(f).$$

Operations on submodules

For an A-module M and submodules $(M_i)_{i\in I}$ of M, we can form the *sum* $\sum_i M_i$ and the *intersection* $\bigcap_i M_i$, both submodules of M. The sum is the smallest submodule of M which contains all the M_i. It consists of all finite sums of the form $\sum_i x_i$ with $x_i \in M_i$.

Proposition 2.2. Let $N_1, N_2 \subseteq M \subseteq L$ be A-modules. Then

$$(L/N)/(M/N) \simeq L/M,$$
$$(M_1 + M_2)/M_1 \simeq M_2/(M_1 \cap M_2).$$

Proof. Same proof as for abelian groups, once one verifies that the relevant homomorphisms are A-module homomorphisms. □

If M is an A-module and $\mathfrak{a}$ an ideal, the *product* $\mathfrak{a}M$ consists of all the finite sums of the form $\sum a_i x_i$ with $a_i \in \mathfrak{a}$ and $x_i \in M$. It is a submodule of M.

The *annihilator* of M is $\operatorname{ann}(M) := \{a \in A \mid aM = 0\}$. It is an ideal of A. If $\mathfrak{a} \subseteq \operatorname{ann}(M)$ is an ideal, then M can be seen as an $A/\mathfrak{a}$-module via $[x]m := xm$.

If M is an A-module and $x \in M$, then $Ax := (x) := \{ax \mid a \in A\}$ is a submodule. A family $(x_i)_{i\in I}$ of elements $x_i \in M$ is a *set of generators* of M if $M = \sum_{i\in I} Ax_i$. We say that M is *finitely generated* if it has a finite set of generators.

Direct sum and product

Let $(M_i)_{i\in I}$ be a family of A-modules. Their *direct sum* $\bigoplus_{i\in I} M_i$ is the set of finite formal sums of the form $\sum_i x_i$ for $x_i \in M_i$. Their *direct product* $\prod_{i\in I} M_i$ is the set of families $(x_i)_{i\in I}$ with $x_i \in M_i$. Both are A-modules: the latter via componentwise addition and scalar multiplication, the former by seeing it as the submodule

$$\bigoplus_{i\in I} M_i := \{(x_i)_{i\in I} \mid x_i = 0 \text{ for all but finitely many } i\} \subseteq \prod_{i\in I} M_i.$$

Thus, if I is finite then $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$.

Finitely generated modules

An A-module of the form $A^{(I)} := \bigoplus_{i \in I} A$ for some index set I, or one isomorphic to such, is called *free*. If $I = \{1, \dots, n\}$ is finite we write A^n for this, and set $A^0 := \{0\}$.

Proposition 2.3. Let I be an index set. An A-module M is generated by a family $(x_i)_{i \in I}$ if and only if M is isomorphic to a quotient of $A^{(I)}$.

Proof. If $M = \sum_i Ax_i$ then $\sum_i a_i \mapsto \sum_i a_i x_i$ defines a surjective A-module homomorphism $A^{(I)} \to M$. Conversely, If there is a surjective homomorphism $A^{(I)} \to M$ then the images of the elements e_i for $i \in I$ generate M. □

Remark. Every A-module M has a set of generators: just take M itself. Thus every module is a quotient of a free module.

Proposition 2.4 (Nakayama's Lemma). Let M be a finitely generated A-module and $\mathfrak{a} \subseteq A$ an ideal with $\mathfrak{a}M = M$. Then there exists $b \in 1 + \mathfrak{a}$ with $bM = 0$.

Proof. Let $(x_1, \dots, x_n)$ generate M and proceed by induction on n. For $n = 1$, the statement is true. For $n > 1$, let $N := M/Ax_n$. Then there exists $b \in 1 + \mathfrak{a}$ with $bN = 0$, i.e. $bM \subseteq Ax_n$. Write $x_n = \sum_{i=1}^n a_i x_i$ where $a_i \in \mathfrak{a}$. Then $bx_n = \sum_{i=1}^n a_i b x_i \in \mathfrak{a}x_n$. So, let $a \in \mathfrak{a}$ with $bx_n = ax_n$. Then $(b - a)b \in 1 + \mathfrak{a}$ and $(b - a)bM \subseteq (b - a)(x_n) = 0$. □

Proposition 2.5. Let M be a finitely generated A-module and let $\mathfrak{a} \subseteq A$ be an ideal contained in all maximal ideals of A. Then $\mathfrak{a}M = M$ implies $M = 0$.

Proof. Let $b \in 1 + \mathfrak{a}$ be as in Prop. 2.4. Then $bM = 0$. But b is a unit since it is not contained in a maximal ideal of A (Cor. 1.5). Hence $M = 0$. □

Corollary 2.6. Let M be a finitely generated A-module, $N \subseteq M$ a submodule, $\mathfrak{a} \subseteq A$ an ideal contained in all maximal ideals of A. Then $\mathfrak{a}M + N = M$ implies $N = M$.

Proof. We have $\mathfrak{a}(M/N) = (\mathfrak{a}M + N)/N$. Now apply Nakayama's Lemma to M/N. □

Let M be an A-module, $\mathfrak{m} \subseteq A$ a maximal ideal, and $K = A/\mathfrak{m}$. Then the module $M/\mathfrak{m}M$ can be seen as an $A/\mathfrak{m}$-module, i.e. a K-vector space.

Proposition 2.7. Let $(A, \mathfrak{m})$ be a local ring and $K = A/\mathfrak{m}$. Let M a finitely-generated A-module and $x_1, \dots, x_n \in M$ such that $M/\mathfrak{m}M$ is generated by $([x_i])_{i=1}^n$ over K. Then M is generated by $(x_i)_{i=1}^n$ over A.

Proof. Let $N = \sum_{i=1}^n Ax_i$. Then the composite $N \to M \to M/\mathfrak{m}M$ is surjective, hence $N + \mathfrak{m}M = M$, hence $N = M$ by Cor. 2.6. □

Tensor product of modules

Let M, N, L be A-modules. A map $f : M \times N \to L$ is *A-bilinear* if for all $x \in M$ and $y \in N$, the maps $f(x, -) : N \to L$ and $f(-, y) : M \to L$ are A-linear.

A module T together with an A-bilinear map $g : M \times N \to T$ is a *tensor product* of M and N if for all A-modules L and A-bilinear maps $f : M \times N \to L$ there exists a unique A-linear map $f' : T \to L$ such that $f = f' \circ g$.

Proposition 2.8. Let M, N be A-modules. Then there exists a tensor product (T, g) of M and N. If (T', g') is another tensor product, then there exists a unique A-module isomorphism $j : T \xrightarrow{\sim} T'$ such that $j \circ g = g'$.

We thus speak of *the* tensor product of M and N, and denote it by $M \otimes_A N$ or $M \otimes N$. We write $x \otimes y$ for the image of a pair (x, y) under the structure map $M \times N \to M \otimes N$.

Proof. We construct the tensor product T as the quotient module of the free A-module $A^{(M\times N)} = \bigoplus_{(x,y)\in M\times N} Ae_{(x,y)}$ by the submodule R generated by all elements of the form

$$\begin{aligned} e_{(x+x',y)} - e_{(x,y)} - e_{(x',y)}, \\ e_{(x,y+y')} - e_{(x,y)} - e_{(x,y')}, \\ e_{(ax,y)} - ae_{(x,y)}, \\ e_{(x,ay)} - ae_{(x,y)}, \end{aligned}$$

with $x, x' \in M, y, y' \in M', a \in A$. We then define the structure map as the composition $g : M \times N \to A^{(M\times N)} \to T$ with $g(x, y) = [e_{(x,y)}]$. It is an A-bilinear map.

Now let $f : M \times N \to L$ be A-bilinear. An A-linear map $f' : T \to L$ is uniquely given by an A-linear map $\tilde{f} : A^{(M\times N)} \to L$ with $R \subseteq \ker(\tilde{f})$. In turn, $\tilde{f}$ is uniquely determined by its value $\tilde{f}(e_{(x,y)})$ at each basis element $e_{(x,y)} \in A^{(M\times N)}$, where $(x, y) \in M \times N$. By the definition of tensor product we are forced to take $\tilde{f}(e_{(x,y)}) = f(x, y)$. But since f is bilinear we have $R \subseteq \ker(\tilde{f})$. Hence, the required f' exists and is unique.

Finally, let (T', g') be another tensor product. Applying the tensor product property of T to the bilinear map g' gives a linear map $j : T \to T'$ such that $g' = j \circ g$. By symmetry we get a linear map $j' : T' \to T$ such that $g = j' \circ g'$. Now $\iota := j' \circ j$ is a linear map $T \to T$ satisfying $g = \iota \circ g$. So is the identity. Thus $\iota = \mathrm{id}$ and by symmetry, $j \circ j' = \mathrm{id}$. Thus j is an isomorphism, unique with the property that $j \circ g = g'$. □

Remarks. (1) If $(x_i)_{i\in I}$ and $(y_j)_{j\in J}$ are sets of generators of M resp. N, then the $(x_i \otimes y_j)_{(i,j)\in I\times J}$ generate $M \otimes N$. Indeed, $M \otimes N$ is generated by the images of the $e_{(x,y)}$ for $x \in M$, $y \in N$. Writing $x = \sum_i a_i x_i$ and $y = \sum_j b_j y_j$, we see that

$$[e_{(x,y)}] = x \otimes y = (\sum_i a_i x_i) \otimes (\sum_j b_j y_j) = \sum_{i,j} a_i b_j x_i \otimes y_j.$$

(2) It is tricky to determine whether a specific element of $M \otimes N$ is zero or not. For instance, $2 \otimes 1$ is zero in $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ but not in $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$.

(3) We could construct a 'multilinear' tensor product $M_1 \otimes \cdots \otimes M_r$ of A-modules $M_1, \dots, M_r$ by replacing all bilinear maps in the construction of the tensor product with multilinear ones. But the nested tensor product $M_1 \otimes (M_2 \otimes (\cdots \otimes M_n) \cdots)$ already satisfies the obvious defining property of the 'multilinear' tensor product.

Proposition 2.9. Let M, N, L. There exist isomorphisms

$$M \otimes N \xrightarrow{\sim} N \otimes M \text{ where } x \otimes y \mapsto y \otimes x,$$
$$(M \otimes N) \otimes L \xrightarrow{\sim} M \otimes (N \otimes L) \text{ where } (x \otimes y) \otimes z \mapsto x \otimes (y \otimes z),$$
$$(M \oplus N) \otimes L \xrightarrow{\sim} (M \otimes L) \oplus (N \otimes L) \text{ where } (x + y) \otimes z \mapsto x \otimes z + y \otimes z,$$
$$A \otimes M \xrightarrow{\sim} M \text{ where } a \otimes x \mapsto ax.$$

Proof. For each of these isomorphisms, check that the right-hand side satisfies the tensor product property with respect to the A-modules on the left-hand side. The structure maps that we use on the right-hand side will then give us the concrete isomorphisms. □

Let A, B be rings. An (A, B)-*bimodule* N is a (left) A-module, simultaneously a (right) B-module such that for all $a \in A$, $x \in N$ and $b \in B$ we have $(ax)b = a(xb)$.

Proposition 2.10. Let A, B be rings, M an A-module, L a B-module and N an (A, B)-bimodule. Then $M \otimes_A N$ and $N \otimes_B L$ are naturally (A, B)-bimodules, and we have

$$(M \otimes_A N) \otimes_B L \simeq M \otimes_A (N \otimes_B L)$$

as (A, B)-bimodules.

Proof. Again, check that the B-module on the right-hand side satisfies the tensor product property for the B-modules on the left-hand side, and that the A-module of the left-hand side satisfies the tensor product property for the A-modules on the right-hand side. □

Two A-module homomorphisms $f : M \to M'$ and $g : N \to N'$ induce an A-module homomorphism

$$f \otimes g : M \otimes N \to M' \otimes N'$$

such that $(f \otimes g)(x \otimes y) = f(x) \otimes g(y)$. If $f' : M' \to M''$ and $g' : N' \to N''$ are two further homomorphisms, then $(f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$.

Restriction and extension of scalars

Let $f : A \to B$ be a ring homomorphism, N a B-module. Then N can be made into an A-module ${}_AN$, the *restriction of scalars*, via $ax := f(a)x$ for $a \in A, x \in N$.

Now let M be an A-module. The A-module $B \otimes_A M$ can be made into a B-module M_B, the *extension of scalars*, by requiring $b(b' \otimes x) = bb' \otimes x$ for all $b, b' \in B$ and $x \in M$.

Proposition 2.11. (1) If N is a finitely generated B-module and B is finitely generated as an A-module, then ${}_AN$ is a finitely generated A-module.
(2) If M is a finitely generated A-module then M_B is a finitely generated B-module.

Proof. If $(y_1, \dots, y_n)$ generates N over B, $(b_1, \dots, b_k)$ generates B over A and $(x_1, \dots, x_m)$ generates M over A, then $(b_i y_j \mid (i,j) \in \{1, \dots, k\} \times \{1, \dots, n\})$ generates ${}_A N$ over A and $(1 \otimes x_1, \dots, 1 \otimes x_m)$ generates M_B over B. □

Algebras

An A-*algebra* is a ring B together with a ring homomorphism $f : A \to B$. Equivalently, it is a ring B together with an A-module structure compatible with the ring structure.

An *homomorphism* between two A-algebras B and C is a ring homomorphism $B \to C$ which is compatible with the structure homomorphisms $A \to B$ and $A \to C$. Equivalently, it is a ring homomorphism $B \to C$ which is also an A-module homomorphism.

An A-algebra $f : A \to B$ is *finite* if B is finitely-generated as an A-module. It is *of finite type* if f extends to a *surjective* A-algebra homomorphism $A[t_1, \dots, t_n] \to B$ for some $n \in \mathbb{N}$. In particular, every finite A-algebra is of finite type.

Example 2.12. Let $A \subseteq B$. Then B is finitely-generated as an A-algebra if and only if $B = A[x_1, \dots, x_n]$ for some $x_1, \dots, x_n \in B$. Here, $A[x_1, \dots, x_n]$ denotes the smallest subring of B that contains A and all the x_i, equivalently the image of the ring homomorphism $A[t_1, \dots, t_n] \to B$ that sends t_i to x_i. On the other hand, B is finitely-generated as an A-module if and only if $B = Ay_1 + \dots + Ay_m$ for some $y_1, \dots, y_m \in B$.

Example 2.13. Let K be a field. The K-algebras of finite type are precisely the rings A such that $A \simeq K[t_1, \dots, t_n]/\mathfrak{a}$ for some $n \in \mathbb{N}$ and some ideal $\mathfrak{a} \subseteq K[t_1, \dots, t_n]$. Such a K-algebra A is finite if and only if it is additionally a finite-dimensional K-vector space.

Tensor product of algebras

Let B, C be A-algebras. The A-module $D := B \otimes_A C$ becomes an A-algebra as follows. The ring multiplication on D is given by the A-bilinear map $D \times D \to D$ determined by the A-linear map $D \otimes D \xrightarrow{\sim} B \otimes C \otimes B \otimes C \to D$, where the last map is determined by the A-bilinear map $B \times C \times B \times C \to D$ defined by $(b, c, b', c') \mapsto bb' \otimes cc'$. Thus in D,

$$(b \otimes c) \cdot (b' \otimes c') = bb' \otimes cc'.$$

This makes D into a ring with identity element $1 \otimes 1$. The ring homomorphism $A \to D$ given by $a \mapsto a \otimes 1 = 1 \otimes a$ makes D into an A-algebra.

Exercise 3. Let M be a module over $A := K[t_1, \dots, t_n]$, K a field. For all $x \in K^n$, define

$$M|_x := M/\mathfrak{m}_x M.$$

(1) Show that $M|_x$ can be made into a K-vector space in two equivalent ways, one using the inclusion $K \to A$ and one using the evaluation morphism $\varphi_x : A \to K$.
(2) Find $n \in \mathbb{N}$, an A-module M, and $x, y \in K^n$ such that $\dim M|_x \neq \dim M|_y$.
(3) Find $n \in \mathbb{N}$ and A-modules $M \not\simeq N$ such that $\dim M|_x = \dim N|_x$ for all $x \in K^n$.

(4) Define

$$\mathrm{Supp}(M) := \{x \in K^n \mid M|_x \neq \{0\}\}.$$

Show that $\mathrm{Supp}(M) \subseteq V(\mathrm{ann}(M))$.

(5) Now let M be finitely generated. Show that $\mathrm{Supp}(M) = V(\mathrm{ann}(M))$.

Exercise 4. In this exercise, you'll compute examples of tensor products in various ways.

(1) Show that $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = 0$.

(2) Let K be a field and V, W finite-dimensional K-vector spaces. Show that

$$\dim(V \otimes_K W) = \dim(V)\dim(W).$$

(3) Let K be a field. Show that

$$K[t_1, \dots, t_n] \otimes_K K[s_1, \dots, s_m] \simeq K[t_1, \dots, t_n, s_1, \dots, s_m]$$

as K-algebras.

(4) Let M be an A-module and $\mathfrak{a} \subseteq A$ an ideal. Show that

$$A/\mathfrak{a} \otimes_A M \simeq M/\mathfrak{a}M$$

as A-modules.

(5) Let M, N be modules over $A := K[t_1, \dots, k_n]$, K a field. Show that for all $x \in K^n$,

$$(M \otimes_A N)|_x \simeq M|_x \otimes_K N|_x$$

as K-vector spaces.

3 Localizations

Localization of a ring A is an algebraic construction similar to taking quotient rings or rings of polynomials over A. While the former sets a collection of elements to zero and the latter adds new elements to the ring, a localization makes a collection of elements $S \subseteq A$ invertible. Here, care has to be taken because S might contain zero divisors, which may force some elements $\neq 0$ in A to become zero in the localization.

Most common are the localization A_f at an element $f \in A$ and the localization $A_{\mathfrak{p}}$ away from a prime ideal $\mathfrak{p} \subseteq A$. If $A = K[t_1, \dots, t_n]$ for a field K, then the former is the ring of rational functions defined on the complement $D(f)$ of $V(f) \subseteq K^n$, while the latter is the ring of rational functions defined at least somewhere on $V(\mathfrak{p})$.

* * *

A *multiplicative subset* of a ring A is a subset $S \subseteq A$ such that

- $1 \in S$
- If $x, y \in S$ then $xy \in S$.

A *localization* of A at S is an A-algebra $f : A \to T$ such that

- $f(S) \subseteq T^\times$;
- For all $t \in T$ there exist $a \in A$, $s \in S$ such that $t = f(a)f(s)^{-1}$;
- For all $a \in \ker(f)$ there exists $s \in S$ such that $sa = 0$.

Construction 3.1. We construct a localization of A at S, the *ring of fractions* $S^{-1}A$.

As a set, $S^{-1}A = (A \times S)/{\sim}$, where

$$(a, s) \sim (b, t) \text{ if and only if } u(at - bs) = 0 \text{ for some } u \in S.$$

This is an equivalence relation. If $(a, s) \in A \times S$, we write a/s for its image in $S^{-1}A$. If $(b, t) \in A \times S$ is another element, then

$$\frac{a}{s} = \frac{b}{t} \text{ if and only if } uat = ubs \text{ for some } u \in S.$$

The ring operations are defined as follows:

$$\begin{aligned} (a/s) + (b/t) &= (at + bs)/(st), \\ (a/s)(b/t) &= (ab)/(st). \end{aligned}$$

These are well-defined, and make $S^{-1}A$ into a ring, with $0 \coloneqq 0/1$ and $1 \coloneqq 1/1$.

The structure morphism $A \to S^{-1}A$ is defined by $f(x) = x/1$.

It can now be checked that $S^{-1}A$ is a localization of A at S.

Proposition 3.2. Let $S \subseteq A$ be a multiplicative subset and $f : A \to T$ an A-algebra. If $f(S) \subseteq T^\times$ then there exists a unique A-algebra homomorphism $h : S^{-1}A \to T$. If additionally f is a localization of A at S, then h is an isomorphism.

Proof. Since $(a/s)(s/1) = a/1$, we are forced to take $h(a/s) \coloneqq g(a)g(s)^{-1}$ for all $a/s \in S^{-1}A$. This is well-defined since if $a/s = 0$ then $ua = 0$ for some $u \in S$, thus $g(u)g(a) = 0$, so $g(a) = 0$. It can now be verified that h is a ring homomorphism. Surjectivity resp. injectivity of h are equivalent to the second resp. third property of a localization. □

Examples 3.3. (1) Let $\mathfrak{p} \subseteq A$ be an ideal. Then $\mathfrak{p}$ is prime if and only if $S \coloneqq A \setminus \mathfrak{p}$ is multiplicative. In this case, $A_\mathfrak{p} \coloneqq S^{-1}A$ is the *localization* of A at $\mathfrak{p}$.

(2) If A is an integral domain, then $\mathrm{Frac}(A) \coloneqq A_{(0)}$ is the *fraction field* of A.

(3) For example, $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$ and $\mathrm{Frac}(k[t_1, \dots, t_n]) = k(t_1, \dots, t_n)$.

(4) We have $S^{-1}A = 0$ if and only if $0 \in S$.

(5) If $f \in A$ then $S \coloneqq \{f^n \mid n \geq 0\}$ is multiplicative and $A_f \coloneqq S^{-1}A \simeq A[t]/(tf - 1)$.

Proposition 3.4. Let A be a ring and S a multiplicative subset. Let $\mathfrak{a} \subseteq A$, $\mathfrak{b} \subseteq S^{-1}A$ be ideals. Then:

(1) $\mathfrak{a}^e = \{a/s \mid a \in \mathfrak{a}, s \in S\}$.

(2) $(\mathfrak{a}^e)^c = \{x \in A \mid sx \in \mathfrak{a} \text{ for some } s \in S\}$.

(3) $\mathfrak{a}^e = (1)$ if and only if there exists $s \in \mathfrak{a} \cap S$.

(4) $\mathfrak{b} = (\mathfrak{b}^c)^e$.

Proof. (1) '$\supseteq$' is clear. For '$\subseteq$', bring the sum $\sum_i a_i/s_i$ to a common denominator.

(2) If $x \in (\mathfrak{a}^e)^c$, then $x/1 \in \mathfrak{a}^e$. Thus, $x/1 = x'/s$ for some $x' \in \mathfrak{a}, s \in S$, so there exists $u \in S$ with $usx = ux' \in \mathfrak{a}$. Conversely, if $sx \in \mathfrak{a}$ for some $s \in S$, then $x/1 = sx/s \in \mathfrak{a}^e$, so $x \in (\mathfrak{a}^e)^c$.

(3) Follows from (2) and the fact that $\mathfrak{b}^c = (1)$ if and only if $\mathfrak{b} = (1)$.

(4) $(b^c)^e = \{b/s \mid b \in \mathfrak{b}^c\} = \{b/s \mid b/1 \in \mathfrak{b}\} = \mathfrak{b}$. □

Proposition 3.5. There is an order-preserving one-to-one correspondence

$$\{\text{Prime ideals } \mathfrak{q} \text{ of } S^{-1}A\} \overset{1:1}{\longleftrightarrow} \{\text{Prime ideals } \mathfrak{p} \text{ of } A \text{ such that } \mathfrak{p} \cap S \neq \emptyset\}$$

given by the mutually inverse maps $\mathfrak{q} \mapsto \mathfrak{q}^c$ and $\mathfrak{p} \mapsto \mathfrak{p}^e$.

Proof. If $\mathfrak{q}$ is prime, then so is $\mathfrak{q}^c$. If $s \in \mathfrak{q}^c \cap S$ then $(1) = (\mathfrak{q}^c)^e = \mathfrak{q}$, so $\mathfrak{q}^c \cap S = \emptyset$.

If $\mathfrak{p}$ is prime with $\mathfrak{p} \cap S = \emptyset$, then $(\mathfrak{p}^e)^c = \mathfrak{p}$ and $\mathfrak{p}^e \neq (1)$. If $(a/s)(b/t) \in \mathfrak{p}^e$, then $ab/1 \in \mathfrak{p}^e$, so $ab \in (\mathfrak{p}^e)^c = \mathfrak{p}$. Hence $a/s \in \mathfrak{p}^e$ or $b/t \in \mathfrak{p}^e$. So $\mathfrak{p}^e$ is prime. □

Corollary 3.6. Let $\mathfrak{p} \subseteq A$ be a prime ideal and $f \in A$ an element. Then there are two order-preserving one-to-one correspondences

$$\{\text{Prime ideals of } A_{\mathfrak{p}}\} \overset{1:1}{\longleftrightarrow} \{\text{Prime ideals } \mathfrak{q} \text{ of } A \text{ such that } \mathfrak{q} \subseteq \mathfrak{p}\};$$

$$\{\text{Prime ideals of } A_f\} \overset{1:1}{\longleftrightarrow} \{\text{Prime ideals } \mathfrak{q} \text{ of } A \text{ such that } f \notin \mathfrak{q}\}.$$

In particular, $A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$. □

Localization of modules

Let A be a ring, M an A-module, S a multiplicative subset, and $f : A \to T$ a localization of A at S. A *localization* of M along f is a T-module P together with an A-module homomorphism $g : M \to P$ such that

- For all $y \in P$ there exist $x \in M, s \in S$ such that $y = f(s)^{-1}g(x)$;
- For all $x \in \ker(g)$ there exists $s \in S$ such that $sx = 0$.

Construction 3.7. We construct a localization of M along $f : A \to S^{-1}A$, the *module of fractions* $S^{-1}M$.

The construction is analogous to the one for $S^{-1}A$, so that $S^{-1}M$ is identified with the set of fractions $\{x/s \mid x \in M, s \in S\}/\!\sim$, where

$$\frac{x}{s} = \frac{y}{t} \text{ if and only if } utx = usy \text{ for some } u \in S.$$

Addition and scalar multiplication are defined analogously as in $S^{-1}A$, and the structure morphism $g : M \to S^{-1}M$ is defined by $g(x) = x/1$.

As one can check, $S^{-1}M$ is a localization of M along f.

Proposition 3.8. Let $S \subseteq A$ be a multiplicative subset, $f : A \to S^{-1}A$ the corresponding localization, N an $S^{-1}A$-module, and $g : M \to N$ an A-module homomorphism. There exists a unique $S^{-1}A$-module homomorphism $h : S^{-1}M \to N$ such that $g = h \circ f$. If additionally g is a localization of M along f, then h is an isomorphism.

Proof. Since $(s/1)(x/s) = x/1$, we must take $h(x/s) \coloneqq (1/s)g(x)$. As in the analogous statement for $S^{-1}A$, this is well-defined and an isomorphism if and only if g is a localization along f. □

Proposition 3.9. We have $S^{-1}M \simeq S^{-1}A \otimes_A M$ as $S^{-1}A$-modules.

Proof. We show that $S^{-1}M$ satisfies the universal property of $S^{-1}A \otimes_A M$. First, we have an A-bilinear map $\sigma : S^{-1}A \times M \to S^{-1}M$ where $\sigma(a/s, x) \coloneqq ax/s$. Next, let $\tau : S^{-1}A \times M \to N$ be A-bilinear. We show that there exists a unique A-linear map $f : S^{-1}M \to N$ with $f \circ \sigma = \tau$. We are forced to take $f(x/s) \coloneqq \tau(1/s, x)$, which is well-defined since if $x/s = y/t$ then $utx = usy$ for some $u \in S$, thus

$$f(x/s) = \tau(ut/uts, x) = \tau(1/uts, utx) = \tau(1/uts, usy) = \tau(us/uts, y) = f(y/t).$$

Since τ is A-bilinear, f is A-linear. □

Remark. Let M be an A-module and $f : A \to T$ any localization. Then we can construct a localization of M along f, namely the T-module $M_T = T \otimes_A M$. To see that this is a localization, consider M_T as an $S^{-1}A$-module using the unique isomorphism $S^{-1}A \xrightarrow{\sim} T$. Then $M_T \simeq S^{-1}A \otimes_A M \simeq S^{-1}M$ as $S^{-1}M$-modules. Thus M_T is a localization along $A \to S^{-1}A$, so it is also a localization along f, using the unique isomorphism $T \xrightarrow{\sim} S^{-1}A$.

Examples 3.10. The module analogues of $A_\mathfrak{p}$ and A_f when $S = A \setminus \mathfrak{p}$ or $\{f^n\}_{n \geq 0}$ are denoted by $M_\mathfrak{p}$ and M_f, respectively.

If $f : M \to N$ is an A-module homomorphism, then we have an $S^{-1}A$-module homomorphism $S^{-1}f : S^{-1}M \to S^{-1}N$ defined by $S^{-1}f(x/s) = f(x)/s$. The assignment $f \mapsto S^{-1}f$ is again a *functor*, i.e. compatible with identities and composition.

A sequence of A-modules and A-module homomorphisms of the form

$$\cdots \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \cdots$$

is *exact* if $\ker(f_{i+1}) = \operatorname{im}(f_i)$ for all i. A *short exact sequence* is an exact sequence

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0.$$

It says that f is injective, g surjective, and that $M'' \simeq M/M'$ via f and g.

Proposition 3.11. The functor S^{-1} is *exact*, i.e. it preserves exact sequences.

Proof. It suffices to check that if $M' \xrightarrow{f} M \xrightarrow{g} M''$ is exact, then the induced sequence

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$$

is exact. We have $\ker(g) = \operatorname{im}(f)$ and have to show $\ker(S^{-1}g) = \operatorname{im}(S^{-1}f)$.

For '$\supseteq$', note that $g(f(x))/s = 0$ for all $x \in M'$.

For '$\subseteq$', let $g(y)/s = 0$ for some $y \in M, s \in S$. Then $g(uy) = ug(y) = 0$ for some $u \in S$. Thus $uy = f(x)$ for some $x \in M'$, so $f(x)/us = y/s$. Hence $y/s \in \operatorname{im}(S^{-1}f)$. □

Corollary 3.12. (1) If $f : M \to N$ is injective then so is $S^{-1}f : S^{-1}M \to S^{-1}N$.

(2) If f is surjective then so is $S^{-1}f$.

(3) If $N \subseteq M$ is a submodule, then $S^{-1}(M/N) \simeq S^{-1}M/S^{-1}N$ as A-modules.

Proof. Apply Proposition 3.11 to the exact sequences $0 \to M \to N$, $M \to N \to 0$, and $0 \to N \to M \to M/N \to 0$, respectively. □

Proposition 3.13. Let M, N be A-modules. Then

$$S^{-1}M \otimes_{S^{-1}A} S^{-1}N \simeq S^{-1}(M \otimes_A N)$$

as $S^{-1}A$-modules via $x/s \otimes y/t \mapsto (x \otimes y)/st$.

Proof. Follow the isomorphisms

$$\begin{aligned} S^{-1}(M \otimes_A N) &\simeq S^{-1}A \otimes_A (M \otimes_A N) \\ &\simeq (S^{-1}A \otimes_A M) \otimes_A N \\ &\simeq (S^{-1}A \otimes_A M) \otimes_{S^{-1}A} (S^{-1}A \otimes_A N) \\ &\simeq S^{-1}M \otimes_{S^{-1}A} S^{-1}N. \end{aligned}$$

□

Corollary 3.14. Let $\mathfrak{p} \subseteq A$ be a prime ideal. Then

$$M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}} \simeq (M \otimes_A N)_{\mathfrak{p}}$$

as $A_{\mathfrak{p}}$-modules. □

Local properties

Proposition 3.15. Let M be an A-module. The following are equivalent:

(1) $M = 0$;

(2) $M_{\mathfrak{p}} = 0$ for all prime ideals $\mathfrak{p} \subseteq A$;

(3) $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m} \subseteq A$.

Proof. The only nontrivial part is '(3) $\Rightarrow$ (1)'. Let $x \in M \setminus \{0\}$. Then $\operatorname{ann}(x) \subsetneq A$. Let $\mathfrak{m} \supseteq \operatorname{ann}(x)$ be a maximal ideal. Then $x/1 \neq 0$ in $M_{\mathfrak{m}}$ since $\operatorname{ann}(x) \subseteq A \setminus (A \setminus \mathfrak{m})$. □

Proposition 3.16. Let $f : M \to N$ be an A-module homomorphism. The following are equivalent:

(1) f is injective (resp. surjective);

(2) $f_{\mathfrak{p}}$ is injective (resp. surjective) for all prime ideals $\mathfrak{p} \subseteq A$;

(3) $f_{\mathfrak{m}}$ is injective (resp. surjective) for all maximal ideals $\mathfrak{m} \subseteq A$.

Proof. For all prime ideals $\mathfrak{p}$ we have $\ker(f)_{\mathfrak{p}} \simeq \ker(f_{\mathfrak{p}})$ and $\operatorname{coker}(f)_{\mathfrak{p}} \simeq \operatorname{coker}(f_{\mathfrak{p}})$ because S^{-1} is exact. The statement now follows from Prop. 3.15. □

Exercise 5. (1) Let A be a ring. Show that the set of units $S := A^{\times}$ is a multiplicative subset and that the structure map $A \to S^{-1}A$ is an isomorphism.

(2) Let A be a ring and S, $T \subseteq A$ multiplicative subsets such that $S \subseteq T$. Show that there exists a unique ring homomorphism $f : S^{-1}A \to T^{-1}A$ that commutes with the structure maps. That is, if $s : A \to S^{-1}A$ and $t : A \to T^{-1}A$ are the structure maps, then $f \circ s = t$.

(3) Now let A be an integral domain and S, T as in (2), where additionally $0 \notin T$. Show that the homomorphism f from (2) is *injective.* Deduce that if A is an integral domain, then the structure morphism $A \to S^{-1}A$ is injective and $S^{-1}A$ can be regarded as a subring of $\operatorname{Frac}(A)$.

(4) Let $A = K[t_1, \ldots, t_n]$, $f \in A$, and $x \in K^n$. Show that

$$\bigcup_{g \in A \setminus \mathfrak{m}_x} A_g = A_{\mathfrak{m}_x}$$

as subrings of $\operatorname{Frac}(A)$, and that if $f^k = ag$ for some $a, g \in A$ ($k \geq 0$) then $A_g \subseteq A_f$.

(5) Let A be a ring, $f \in A$, and $S := \{f^k\}_{k \geq 0}$. Show that

$$A_f \simeq A[t]/(tf - 1).$$

Exercise 6. Recall that if $f : A \to B$ is a ring homomorphism and $\mathfrak{a} \subseteq A$, $\mathfrak{b} \subseteq B$ ideals, then $\mathfrak{b}^c$ is the ideal $f^{-1}(\mathfrak{b})$ and $\mathfrak{a}^e$ is the ideal generated by the set $f(\mathfrak{a}) \subseteq B$.

(1) Let A be a ring and M a finitely-generated A-module. Let $\mathfrak{p} \subseteq A$ be a prime ideal. Show that $M_\mathfrak{p} = 0$ if and only if there exists $f \in A \setminus \mathfrak{p}$ such that $M_f = 0$.

(2) Let A be a ring and $S \subseteq A$ a multiplicative subset. Show that $\operatorname{nil}(S^{-1}A) = \operatorname{nil}(A)^e$, where the extension is taken with respect to the structure map $A \to S^{-1}A$.

(3) Let A be a ring. We call A *reduced* if $\operatorname{nil}(A) = 0$. Show that A is reduced if and only if $A_\mathfrak{p}$ is reduced for every prime ideal $\mathfrak{p} \subseteq A$.

(4) Let A be a ring and $\mathfrak{p}', \mathfrak{p} \subseteq A$ prime ideals such that $\mathfrak{p}' \subseteq \mathfrak{p}$. Find a ring B and a ring homomorphism $f : A \to B$ such that $\mathfrak{q} \mapsto \mathfrak{q}^c$ gives a bijection

$$\{\mathfrak{q} \subseteq B \mid \mathfrak{q} \text{ prime}\} \xrightarrow{1:1} \{\mathfrak{q}' \subseteq A \mid \mathfrak{q}' \text{ prime}, \mathfrak{p}' \subseteq \mathfrak{q}' \subseteq \mathfrak{p}\}.$$

(5) Let $f : M \to N$ be an A-module homomorphism and $S \subseteq A$ a multiplicative subset. Show that $\ker(S^{-1}f) \simeq S^{-1}\ker(f)$ and $\operatorname{coker}(S^{-1}f) \simeq S^{-1}\operatorname{coker}(f)$.

In particular, $\ker(f_\mathfrak{p}) \simeq \ker(f)_\mathfrak{p}$ *and* $\operatorname{coker}(f_\mathfrak{p}) \simeq \operatorname{coker}(f)_\mathfrak{p}$ *for every prime ideal* $\mathfrak{p} \subseteq A$.

4 Primary Decompositions and Noetherian Rings

Primary decompositions generalize decomposition theorems in number theory and algebraic geometry. Over $A = \mathbb{Z}$, every element $a \in \mathbb{Z}$ can be uniquely written a product of prime powers $p_1^{i_1} \cdots p_m^{i_m}$, and these are simpler objects than a because they only have one prime factor. Over $A = K[t_1, \ldots, t_n]$, every variety $V(\mathfrak{a}) \subseteq K^n$ over a field K decomposes uniquely as a union $V_1 \cup \cdots \cup V_m$ of *irreducible* varieties, i.e. varieties that cannot be decomposed further in this way. These are both examples of decompositions of the form $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$, where the ideals $\mathfrak{q}_i$ are *primary.* In general, such a decomposition is not unique, but some features of it are, and this recovers the uniqueness statements of the previous two examples.

In 1921, Emmy Noether showed that the existence of primary decompositions is always guaranteed if the ambient ring satisfies a certain finiteness property, which is now called *Noetherian* in her honor. Furthermore, David Hilbert showed in 1890 that the class of Noetherian rings includes all polynomial rings $K[t_1, \dots, t_n]$ over a field K, providing thus the first important link between commutative algebra and algebraic geometry.

When the field K is algebraically closed, the second important link was given again by Hilbert through his *Nullstellensatz* in 1893, which in particular provides a one-to-one correspondence between the varieties in K^n and the radical ideals of $K[t_1, \dots, t_n]$.

* * *

Lemma 4.1. Let $f : A \to B$ be a ring homomorphism, $\mathfrak{a}, \mathfrak{b}, \mathfrak{a}_i \subseteq B$ ideals ($i \in I$). Then

(1) $r(\mathfrak{a})^c = r(\mathfrak{a}^c)$.
(2) $r(\mathfrak{a}) = (1)$ if and only if $\mathfrak{a} = (1)$.
(3) $r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$.
(4) r is order-preserving.
(5) $\bigcap_i (\mathfrak{a}_i : \mathfrak{a}) = (\bigcap_i \mathfrak{a}_i : \mathfrak{a})$.
(6) $(\mathfrak{a} \cap \mathfrak{b})^c = \mathfrak{a}^c \cap \mathfrak{b}^c$.

Proof. All of these follow immediately from the definitions. □

Lemma 4.2. Let $S \subseteq A$ be a multiplicative subset and $\mathfrak{a}, \mathfrak{b} \subseteq A$ ideals. Then for $A \to S^{-1}A$:

(1) $r(\mathfrak{a}^e) = r(\mathfrak{a})^e$.
(2) $(\mathfrak{a} \cap \mathfrak{b})^e = \mathfrak{a}^e \cap \mathfrak{b}^e$.

Proof. (1) "$\subseteq$" is clear. For "$\supseteq$", let $(x/s)^k = x'/s'$ where $x' \in \mathfrak{a}$. Then there exists $u \in S$ with $us'x^k = us^k x' \in \mathfrak{a}$, so $x^k/1 \in a^e$, thus $x/s \in r(\mathfrak{a}^e)$.

(2) "$\subseteq$" is clear. For "$\supseteq$", let $x/s = x'/s'$ where $x \in \mathfrak{a}$ and $x' \in \mathfrak{b}$. Then there exists $u \in S$ with $us'x = usx' \in \mathfrak{b}$, so $x/1 \in \mathfrak{b}^e$, thus $x/s \in \mathfrak{b}^e$. □

Also recall some propositions we have already proven:

Proposition 1.12. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be prime ideals, let $\mathfrak{a}$ be an ideal with $\mathfrak{a} \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$. Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some i.

Proposition 1.13. Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals and let $\mathfrak{p}$ be a prime ideal with $\mathfrak{p} \supseteq \bigcap_{i=1}^n \mathfrak{a}_i$. Then $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some i. If $\mathfrak{p} = \bigcap_{i=1}^n \mathfrak{a}_i$, then $\mathfrak{p} = \mathfrak{a}_i$ for some i.

Let A be a ring, $\mathfrak{q}, \mathfrak{p} \subseteq A$ ideals. Then $\mathfrak{q}$ is $\mathfrak{p}$-*primary* if

- $\mathfrak{q} \neq (1)$;
- $r(\mathfrak{q}) = \mathfrak{p}$;
- if $xy \in \mathfrak{q}$ then $x \in \mathfrak{q}$ or $y \in \mathfrak{p}$.

Proposition 4.3. Let $\mathfrak{q}, \mathfrak{p} \subseteq A$ be ideals. If $\mathfrak{q}$ is $\mathfrak{p}$-primary, then $\mathfrak{p}$ is prime.

Proof. We have $\mathfrak{p} \neq (1)$ since $\mathfrak{q} \neq (1)$. If $xy \in \mathfrak{p}$ then $x^k y^k \in \mathfrak{q}$ for some $k \geq 0$, so either $x \in \mathfrak{p}$ or $y^{kk'} \in \mathfrak{q}$ for some $k' \geq 0$, which implies $y \in \mathfrak{p}$. □

Proposition 4.4. Let $\mathfrak{q} \subseteq A$ be an ideal and $\mathfrak{m} = r(\mathfrak{q})$ maximal. Then $\mathfrak{q}$ is $\mathfrak{m}$-primary.

Proof. We have $\mathfrak{q} \subseteq \mathfrak{m} \neq (1)$. Now let $xy \in \mathfrak{q}$. If $y \notin \mathfrak{m}$ then there exists $z \in A$ such that $zy \equiv 1 \pmod{\mathfrak{m}}$. But then $(zy-1)^k \equiv 0 \pmod{\mathfrak{q}}$, so

$$0 \equiv x(zy-1)^k \equiv x \pmod{\mathfrak{q}}.$$ □

Lemma 4.5. If $\mathfrak{q}_1, \dots, \mathfrak{q}_n$ are $\mathfrak{p}$-primary, then so is $\mathfrak{q} \coloneqq \bigcap_i \mathfrak{q}_i$.

Proof. We have $\mathfrak{q} \neq (1)$ and $r(\mathfrak{q}) = \mathfrak{p}$. Now let $xy \in \mathfrak{q}$ and $x \notin \mathfrak{q}$. Then $x \notin \mathfrak{q}_i$ for some i, but then $y \in \mathfrak{p}$ since $\mathfrak{q}_i$ is $\mathfrak{p}$-primary. □

Lemma 4.6. Let $\mathfrak{q}$ be $\mathfrak{p}$-primary, $x \in A$. Then
(1) If $x \in \mathfrak{q}$ then $(\mathfrak{q} : x) = (1)$.
(2) If $x \notin \mathfrak{q}$ then $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary.
(3) If $x \notin \mathfrak{p}$ then $(\mathfrak{q} : x) = \mathfrak{q}$.

Proof. (1) $1x \in \mathfrak{q}$.
(2) If $y \in (\mathfrak{q} : x)$ then $y \in \mathfrak{p}$, so $\mathfrak{q} \subseteq (\mathfrak{q} : x) \subseteq \mathfrak{p}$. Applying r we get $\mathfrak{p} \subseteq r(\mathfrak{q} : x) \subseteq \mathfrak{p}$, so $\operatorname{rad}(\mathfrak{q} : x) = \mathfrak{p}$. Now let $yz \in (\mathfrak{q} : x)$ and suppose $z \notin \mathfrak{p}$. Since $xyz \in \mathfrak{q}$ we have $xy \in \mathfrak{q}$, so $y \in (\mathfrak{q} : x)$.
(3) If $y \in (\mathfrak{q} : x)$ then $xy \in \mathfrak{q}$, so $y \in \mathfrak{q}$. □

Let $\mathfrak{a} \subseteq A$ be an ideal. A *primary decomposition* of $\mathfrak{a}$ is a relation of the form

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i, \quad \mathfrak{q}_i \text{ is } \mathfrak{p}_i\text{-primary for all } i. \tag{$*$}$$

The decomposition $(*)$ is *minimal* if all the $\mathfrak{p}_i$ are distinct and $\mathfrak{q}_i \not\supseteq \bigcup_{j \neq i} \mathfrak{q}_j$ for all i. Every primary decomposition can be turned into a minimal one by collecting or eliminating terms. Thus we will always assume that $(*)$ is minimal when we refer to it.

Theorem 4.7 (Uniqueness 1)**.** Let $\mathfrak{a} \subseteq A$ be an ideal and $(*)$ be a minimal primary decomposition. If $\mathfrak{p} \subseteq A$ is prime, then $\mathfrak{p} = \mathfrak{p}_i$ for some i if and only if $\mathfrak{p} = r(\mathfrak{a} : x)$ for some $x \in A$. In particular, the set $\{\mathfrak{p}_i\}_{i=1}^n$ is independent of the choice of decomposition $(*)$.

Proof. First note that for all $x \in A$,

$$r(\mathfrak{a} : x) = r \bigcap_{j=1}^{n} (\mathfrak{q}_j : x) = r \bigcap_{x \notin \mathfrak{q}_j} (\mathfrak{q}_j : x) = \bigcap_{x \notin \mathfrak{q}_j} r(\mathfrak{q}_j : x).$$

Now for "⇒", let $\mathfrak{p} = \mathfrak{p}_i$. Since $(*)$ is minimal, there exists $x \in \bigcap_{j \neq i} \mathfrak{q}_j \setminus \mathfrak{q}_i$. For this x, we have $r(\mathfrak{a} : x) = r(\mathfrak{q}_i : x) = \mathfrak{p}$.

For "⇐", let $\mathfrak{p} = r(\mathfrak{a} : x)$ for some $x \in A$. Then since $\mathfrak{p} = \bigcap_{x \notin q_j} r(\mathfrak{q}_j : x)$, there exists an i such that $\mathfrak{p} = r(\mathfrak{q}_i : x) = \mathfrak{p}_i$. □

The set $\mathrm{Ass}(\mathfrak{a}) := \{\mathfrak{p}_i\}_{i=1}^n$ is the set of primes *associated* to $\mathfrak{a}$. Inclusion-minimal elements of $\mathrm{Ass}(\mathfrak{a})$ are called *isolated primes* and the other elements *embedded primes*. The terms $\mathfrak{q}_i$ of a primary decomposition $(*)$ are then called *isolated* or *embedded components* according to their radicals $\mathfrak{p}_i$.

Proposition 4.8. Let $\mathfrak{a} \subseteq A$ be an ideal and $(*)$ be a minimal primary decomposition. If $\mathfrak{p} \supseteq \mathfrak{a}$ is prime, then there exists an isolated prime $\mathfrak{p}_i \in \mathrm{Ass}(\mathfrak{a})$ such that $\mathfrak{p} \supseteq \mathfrak{p}_i$.

Proof. We have $\mathfrak{p} \supseteq \bigcap_j \mathfrak{p}_j$, so $\mathfrak{p} \supseteq \mathfrak{p}_i$ for some $\mathfrak{p}_i$, which can be chosen minimal. □

Proposition 4.9. Let $S \subseteq A$ be a multiplicatively closed subset and $\mathfrak{q}$ a $\mathfrak{p}$-primary ideal. Then with respect to $A \to S^{-1}A$:

(1) If $S \cap \mathfrak{p} \neq \emptyset$ then $\mathfrak{q}^e = (1)$.

(2) If $S \cap \mathfrak{p} = \emptyset$ then $\mathfrak{q}^e$ is $\mathfrak{p}^e$-primary and $\mathfrak{q}^{ec} = \mathfrak{q}$.

Proof. (1) If $s \in S \cap \mathfrak{p}$ then $s^k \in S \cap \mathfrak{q}$ for some k, so $1 \in \mathfrak{q}^e$.

(2) We have $\mathfrak{q}^{ec} = \{x \in A \mid sx \in \mathfrak{q} \text{ for some } s \in S\} = \mathfrak{q}$ since $s \notin \mathfrak{p}$. Furthermore, $r(\mathfrak{q}^e) = r(\mathfrak{q})^e = \mathfrak{p}^e$. If $(a/s)(b/t) \in \mathfrak{q}^e$ then $ab/1 \in \mathfrak{q}^{ec} = \mathfrak{q}$, so $\mathfrak{q}^e$ is $\mathfrak{p}^e$-primary. □

Proposition 4.10. Let $S \subseteq A$ be multiplicatively closed, $\mathfrak{a} \subseteq A$ an ideal, and $(*)$ a minimal primary decomposition. Then with respect to $A \to S^{-1}A$:

$$\mathfrak{a}^e = \bigcap_{S\cap\mathfrak{p}_i=\emptyset} \mathfrak{q}_i^e \quad \text{and} \quad \mathfrak{a}^{ec} = \bigcap_{S\cap\mathfrak{p}_i=\emptyset} \mathfrak{q}_i$$

are both minimal primary decompositions.

Proof. We have $\mathfrak{a}^e = \bigcap_{i=1}^n \mathfrak{q}_i^e = \bigcap_{S\cap\mathfrak{p}_i=\emptyset} \mathfrak{q}_i^e$ and the $\mathfrak{q}_i^e$ in that intersection are $\mathfrak{p}_i^e$-primary. Since $(-)^e$ is order-preserving, this is a minimal primary decomposition of $\mathfrak{a}^e$. Finally, we get $\mathfrak{a}^{ec} = \bigcap_{S\cap\mathfrak{p}_i=\emptyset} \mathfrak{q}_i^{ec} = \bigcap_{S\cup\mathfrak{p}_i=\emptyset} \mathfrak{q}_i$ and this is a minimal primary decomposition. □

A set $\Sigma \subseteq \mathrm{Ass}(\mathfrak{a})$ is *isolated* if for all $\mathfrak{p} \in \Sigma$ and $\mathfrak{p}' \in \mathrm{Ass}(\mathfrak{a})$, $\mathfrak{p}' \subseteq \mathfrak{p}$ implies $\mathfrak{p}' \in \Sigma$.

Lemma 4.11. Let $\Sigma \subseteq \mathrm{Ass}(\mathfrak{a})$ be isolated and $S = A \backslash \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$. Then S is multiplicatively closed and for all $\mathfrak{p}' \in \mathrm{Ass}(\mathfrak{a})$,

(1) If $\mathfrak{p}' \in \Sigma$ then $\mathfrak{p}' \cap S = \emptyset$.

(2) If $\mathfrak{p}' \notin \Sigma$ then $\mathfrak{p}' \cap S \neq \emptyset$.

Proof. If $s, t \notin \mathfrak{p}$ for all $\mathfrak{p} \in \Sigma$ then neither is st. Thus S is multiplicatively closed. Now,

(1) Holds by definition.

(2) If $\mathfrak{p}' \notin \Sigma$ then $\mathfrak{p}' \nsubseteq \mathfrak{p}$ for all $\mathfrak{p} \in \Sigma$ because Σ is isolated, so $\mathfrak{p}' \nsubseteq \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$ by a previous proposition, hence $\mathfrak{p}' \cap S \neq \emptyset$. □

Theorem 4.12 (Uniqueness 2)**.** Let $\mathfrak{a} \subseteq A$ be an ideal, $(*)$ be a minimal primary decomposition and $\Sigma \subseteq \mathrm{Ass}(\mathfrak{a})$ isolated. Then the ideal $\bigcap_{\mathfrak{p}_i\in\Sigma} \mathfrak{q}_i$ is independent of the choice of decomposition $(*)$. In particular, the isolated primary components of $\mathfrak{a}$ depend only on $\mathfrak{a}$, not on $(*)$.

Proof. Let $S = A \backslash \bigcup_{\mathfrak{p}_i\in\Sigma} \mathfrak{p}_i$. By Theorem 4.7, S does not depend on $(*)$, and thus neither does $\mathfrak{a}^{ec}$ (w.r.t. $A \to S^{-1}A$). But $\mathfrak{a}^{ec} = \bigcap_{\mathfrak{p}_i\in\Sigma} \mathfrak{q}_i$ by Proposition 4.10 and Lemma 4.11. Finally, $\{p_i\}$ is an isolated set if and only if $\mathfrak{q}_i$ is an isolated component. □

Noetherian rings

A ring A is *Noetherian* if for all sequences $(\mathfrak{a}_i)_{i\in\mathbb{N}}$ of ideals $\mathfrak{a}_i \subseteq A$ with

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq A,$$

there exists $n \in \mathbb{N}$ such that $\mathfrak{a}_n = \mathfrak{a}_m$ for all $m \geq n$. We say that in Noetherian rings, *all ascending chains are stationary.*

Proposition 4.13. Let A be a ring. The following are equivalent:

(1) A Noetherian.
(2) Every set of ideals in A has a $\subseteq$-maximal element.
(3) Every ideal in A is finitely generated.

Proof. (1) $\Rightarrow$ (2): If a set of ideals does not have a maximal element, then we can inductively construct a non-stationary ascending chain.

(2) $\Rightarrow$ (3): Let $\mathfrak{a}$ be an ideal and consider the set of ideals of the form $\sum_{i=1}^{n}(a_i)$ for some $n \in \mathbb{N}$ and $a_i \in \mathfrak{a}$. A maximal element of this set must equal $\mathfrak{a}$.

(3) $\Rightarrow$ (1): Given an ascending chain $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$, the union $\mathfrak{a} := \bigcup_{i\in\mathbb{N}} \mathfrak{a}_i$ is an ideal. But then there must be an $\mathfrak{a}_n$ that contains all the generators of $\mathfrak{a}$. □

Example 4.14. Principal ideal domains are Noetherian. In particular the ring $\mathbb{Z}$ is Noetherian, as well as every field K.

Proposition 4.15. Let A be a ring, $\mathfrak{a} \subseteq A$ an ideal. If A is Noetherian, then so is $A/\mathfrak{a}$.

Proof. Ascending chains in $A/\mathfrak{a}$ correspond to ascending chains in A containing $\mathfrak{a}$. □

Proposition 4.16. Let A be Noetherian and let $N \subseteq M$ be A-modules. If M is finitely generated then so is N.

Proof. Let $M = \sum_{i=1}^{n} Ax_i$ for some $x_i \in M$. Use induction on n. If $n = 1$ then $M \simeq A/\mathrm{ann}(x_1)$ and the submodules of M correspond to the ideals of $A/\mathrm{ann}(x_1)$. If $n > 1$, let $N'' := N/(N \cap Ax_n)$. This is a submodule of M/Ax_n, which is generated by $n-1$ elements. Thus N'' is finitely generated. Similarly, $N' := N \cap Ax_n$ is a submodule of Ax_n, thus finitely generated. Since $N = N' + p^{-1}(N'')$ and $p : N \to N''$ is surjective, N is also finitely generated. □

Remark. The final part of the above proof can be adapted to show the following: if N' and N'' are finitely generated modules over any ring A and $0 \to N' \to N \to N'' \to 0$ is an exact sequence, then N is finitely generated.

Proposition 4.17. If A is Noetherian and $S \subseteq A$ multiplicative then $S^{-1}A$ is Noetherian.

Proof. If $\mathfrak{b} \subseteq S^{-1}A$ is an ideal then $\mathfrak{b}^c$ is finitely generated, hence so is $\mathfrak{b}^{ce} = \mathfrak{b}$. □

Theorem 4.18 (Hilbert's Basis Theorem)**.** If A is Noetherian, then so is $A[t]$.

Proof. Let $\mathfrak{a} \subseteq A[t]$ be an ideal. For $n \in \mathbb{N}$, we define recursively elements $f_n \in \mathfrak{a}$, ideals $\mathfrak{a}_n := \sum_{i=1}^{n}(f_i)$ and numbers $d_n := \deg(f_n)$, as follows. First let $f_1 := 0$. Then if $n > 1$, let f_n be any element of minimal degree in $\mathfrak{a} \setminus \mathfrak{a}_{n-1}$. If at some point $\mathfrak{a} = \mathfrak{a}_n$ then $\mathfrak{a}$ is finitely generated and we are done. If not, we want to find a contradiction.

Note that $d_{i-1} \leq d_i$ for all $i > 1$, since $f_i \in \mathfrak{a} \setminus \mathfrak{a}_{n-2}$.

For $i \in \mathbb{N}$, write $f_i = a_i t^{d_i}$ + (lower terms) and let $\bar{\mathfrak{a}} := \sum_{i\in\mathbb{N}}(a_i) \subseteq A$. Then there exists $n \in \mathbb{N}$ such that $\bar{\mathfrak{a}} = \sum_{i=1}^{n}(a_i)$. In particular, there exist $u_i \in A$ such that $a_{n+1} = \sum_{i=1}^{n} u_i a_i$. Let $g := \sum_{i=1}^{n} u_i f_i t^{d_{n+1}-d_i}$. Then $g \in \mathfrak{a}_n$ and $f_{n+1} \in \mathfrak{a} \setminus \mathfrak{a}_n$, so $f_{n+1} - g \in \mathfrak{a} \setminus \mathfrak{a}_n$. But

$$g = (\sum_{i=1}^{n} u_i a_i)t^{d_{n+1}} + (\text{lower terms}) = a_{n+1}t^{d_{n+1}} + (\text{lower terms}),$$

so $\deg(f_{n+1} - g) < d_{n+1} = \deg(f_{n+1})$, contradiction. □

Corollary 4.19. If A is Noetherian then so is $A[t_1, \ldots, t_n]$. In particular, if K is a field then $K[t_1, \ldots, t_n]$ is Noetherian, thus every finitely-generated K-algebra is Noetherian, as well as every finitely generated $\mathbb{Z}$-algebra. □

Primary decompositions in Noetherian rings

An ideal $\mathfrak{a} \subseteq A$ is *irreducible* if for all ideals $\mathfrak{b}, \mathfrak{c} \subseteq A$, if $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ then $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{a} = \mathfrak{c}$.

Lemma 4.20. If A is Noetherian, then every ideal $\mathfrak{a} \subseteq A$ is the intersection of finitely many irreducible ideals.

Proof. Suppose not. Then the set Σ of ideals that aren't such an intersection has a maximal element $\mathfrak{a}$. In particular $\mathfrak{a}$ is reducible, so there exist $\mathfrak{b} \supsetneq \mathfrak{a}$ and $\mathfrak{c} \supsetneq \mathfrak{a}$ such that $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$. But then $\mathfrak{b}, \mathfrak{c} \notin \Sigma$, so $\mathfrak{a} \notin \Sigma$, contradiction. □

Lemma 4.21. Let A be a Noetherian ring and $\mathfrak{q} \subsetneq A$ irreducible. Then $\mathfrak{q}$ is primary.

Proof. Since $\mathfrak{q}$ is irreducible, (0) is irreducible in $A/\mathfrak{q}$. Now let $x, y \in A/\mathfrak{q}$ with $xy = 0$, $x \neq 0$. We show that y is nilpotent. The ascending chain

$$(0) \subseteq \operatorname{ann}(y) \subseteq \operatorname{ann}(y^2) \subseteq \cdots$$

is stationary, so $\operatorname{ann}(y^n) = \operatorname{ann}(y^{n+1})$ for some n. If $z \in (y^n)$ then $z = gy^n$ for some $g \in A/\mathfrak{q}$. If additionally $z \in (x)$ then $gy^{n+1} = yz = 0$, thus $gy^n = 0$ because $g \in \operatorname{ann}(y^n)$. Hence we have $(0) = (x) \cap (y^n)$. Since $(x) \neq (0)$, we must have $(y^n) = (0)$. □

From these lemmas we immediately deduce the following theorem:

Theorem 4.22 (Noether)**.** Every ideal in a Noetherian ring has a primary decomposition.

Hilbert's Nullstellensatz

Lemma 4.23 (Artin–Tate)**.** Let $A \subseteq B \subseteq C$ be rings, where A is Noetherian, C is finitely generated as an A-algebra, and C is finitely generated as a B-module. Then B is finitely generated as an A-algebra.

Proof. Let $x_1, \dots, x_m, y_1, \dots, y_n \in C$ such that $C = A[x_1, \dots, x_m] = By_1 + \dots + By_n$. Then for every x_i and every product pair $y_j y_k$ there are equations of the form

$$\begin{aligned} x_i &= \sum_{j=1}^{n} b_{ij} y_j, \quad b_{ij} \in B, \\ y_j y_k &= \sum_{\ell=1}^{n} b_{jk\ell} y_\ell, \quad b_{jk\ell} \in B. \end{aligned}$$

Let $B' := A[b_{ij}, b_{jk\ell}]_{i,j,k,\ell}$. Then $B'y_1 + \dots + B'y_n$ contains all x_i, all products $x_i x_{i'}$, and all other monomials in the x_i. Thus $C = B'y_1 + \dots + B'y_n$, so C is a finitely-generated B'-module. Now B' is Noetherian (it is a finitely-generated A-algebra) and $B' \subseteq B$, thus the B'-submodule $B \subseteq C$ is a finitely-generated B'-module. Then B is finitely generated as an A-algebra: if, say, $B = B'y'_1 + \dots + B'y'_r$ then $B = A[b_{ij}, b_{jk\ell}, y'_\alpha]_{i,j,k,\ell,\alpha}$. □

Lemma 4.24. Let K be a field and E the function field $K(t_1, \dots, t_r)$ for some $r \geq 1$. Then E is *not* a finitely-generated K-algebra.

Proof. Exercise. □

Lemma 4.25 (Zariski)**.** Let $K \subseteq L$ be fields, where L is a finitely-generated K-algebra. Then L is a finitely-generated K-vector space.

Proof. By "basic field theory" (see supp. material), there exists a field E such that

- $K \subseteq E \subseteq L$,
- E is isomorphic to the function field $K(t_1, \dots, t_r)$ for some $r \geq 0$, and
- L is a finite-dimensional E-vector space.

Then since K is Noetherian and L finitely generated as a K-algebra and as an E-module, E is a finitely-generated K-algebra. But this can only happen when $r = 0$. □

Corollary 4.26. Let A be a finitely-generated K-algebra and $\mathfrak{m} \subseteq A$ a maximal ideal. Then $A/\mathfrak{m}$ is a finitely-generated K-vector space. In particular, if K is algebraically closed then $A/\mathfrak{m} \simeq K$.

Proof. We have $K \subseteq A/\mathfrak{m}$ and $A/\mathfrak{m}$ is a finitely-generated K-algebra and a field, so it is finitely-generated as a K-vector space. In particular, if $\alpha \in A/\mathfrak{m}$ then there exists $n \in \mathbb{N}$ such that the elements $1, \alpha, \dots, \alpha^n$ are linearly dependent over K. If K is algebraically closed, this implies $\alpha \in K$, thus $A/\mathfrak{m} = K$ in this case. □

Theorem 4.27 (Hilbert's Nullstellensatz). Let $A := k[t_1, \dots, t_n]$, where k is an algebraically closed field, and $\mathfrak{a} \subseteq A$ an ideal. Let $V(\mathfrak{a}) := \{x \in k^n \mid g(x) = 0 \text{ for all } g \in \mathfrak{a}\}$ and

$$I(V(\mathfrak{a})) := \{f \in A \mid f(x) = 0 \text{ for all } x \in V(\mathfrak{a})\}.$$

Then $I(V(\mathfrak{a})) = \operatorname{rad}(\mathfrak{a})$.

Proof. If $f^n \in \mathfrak{a}$ and $x \in V(\mathfrak{a})$, then $f(x)^n = 0$, thus $f(x) = 0$. So $\operatorname{rad}(\mathfrak{a}) \subseteq I(V(\mathfrak{a}))$.

Now let $B := A/\mathfrak{a}$. Suppose $f \notin \operatorname{rad}(\mathfrak{a})$ and let $\overline{f}$ be the image of f in B. Then $B_{\overline{f}} \neq 0$, so there exists a maximal ideal $\mathfrak{m} \subset B_{\overline{f}}$. Also, $B_{\overline{f}} \simeq B[t]/(1 - t\overline{f})$ is a finitely generated k-algebra, thus so is $B_{\overline{f}}/\mathfrak{m}$. Since k is algebraically closed we have $B_{\overline{f}}/\mathfrak{m} \simeq k$ and a ring homomorphism

$$\varphi : A \to B \to B_{\overline{f}} \to B_{\overline{f}}/\mathfrak{m} \xrightarrow{\sim} k.$$

Let $x := (\varphi(t_1), \dots, \varphi(t_n)) \in k^n$. For all $g \in A$ we have $g(x) = \varphi(g)$. In particular, if $g \in \mathfrak{a}$ then $g(x) = 0$ since g becomes 0 in B, thus $x \in V(\mathfrak{a})$. But $f(x) \neq 0$ since f becomes a unit in $B_{\overline{f}}$. Hence, $f \notin I(V(\mathfrak{a}))$, which concludes the proof. □

On this happy note, we conclude our introduction to commutative algebra.

Exercise 7. For this exercise, let $A := K[x, y, z]$ and let $\mathfrak{a}$ denote the ideal $(yz, xz^2) \subseteq A$.

(1) Show that the ideals (z) and (y, x) are prime and that $V(\mathfrak{a}) = V(z) \cup V(y, x)$.

(2) Show that the ideal (y, z^2) is primary and find its radical.

(3) Show that $\mathfrak{a} = (z) \cap (y, x) \cap (y, z^2)$.

(4) Show that the relation in (3) is a minimal primary decomposition of $\mathfrak{a}$.

(5) Determine the set $\operatorname{Ass}(\mathfrak{a})$ of prime ideals associated to $\mathfrak{a}$, together with its partial order $\subseteq$. Indicate which associated primes are isolated and which are embedded.

Exercise 8. In this exercise, K denotes an arbitrary field. Recall that the *variety* of an arbitrary subset $E \subseteq K[t_1, \dots, t_n]$ is

$$V(E) := \{x \in K^n \mid f(x) = 0 \text{ for all } f \in E\}.$$

(1) Find an ideal $\mathfrak{a} \subseteq K[x, y, z]$ such that $\operatorname{Ass}(\mathfrak{a})$ consists of three distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ with $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \mathfrak{p}_3$.

(2) Let $E \subseteq K[t_1, \dots, t_n]$ be any subset. Show that there exist $f_1, \dots, f_k \in K[t_1, \dots, t_n]$ such that $V(E) = V(\{f_1, \dots, f_k\})$.

(3) Let K be algebraically closed and let $\mathfrak{a} \subseteq K[t_1, \dots, t_n]$ be an ideal. Show that $V(\mathfrak{a}) = \emptyset$ implies $\mathfrak{a} = (1)$. Deduce that every maximal ideal $\mathfrak{m} \subseteq K[t_1, \dots, t_n]$ is of the form $\mathfrak{m}_x$ for some $x \in K^n$. (Or, if you prefer, prove the second statement and deduce the first from the second).

(4) Find an ideal $\mathfrak{a} \subseteq \mathbb{R}[t]$ such that $V(\mathfrak{a}) = \emptyset$ but $\mathfrak{a} \neq (1)$. Compute $V(\mathfrak{a}^e)$, where the extension is taken with respect to the inclusion $\mathbb{R}[t] \to \mathbb{C}[t]$.

(5) Let $r \geq 1$, $E := K(t_1, \dots, t_r)$, and $\alpha_1, \dots, \alpha_m \in E$. Show that there exists $\alpha \in E$ such that $\alpha \notin K[\alpha_1, \dots, \alpha_m]$. Deduce that E is not a finitely-generated K-algebra.

Supplementary Material

Homomorphisms from a polynomial ring

Let A be a ring, $P = A[t_1, \ldots, t_n]$ the polynomial ring in n variables over A. We have

- A ring homomorphism $u : A \to P$ (the obvious inclusion)
- A choice of n elements of P (the t_i)

with the following property:

> For all rings R, ring homomorphisms $v : A \to R$, and all choices of n elements $r_1, \ldots, r_n$ of R, there exists a *unique* ring homomorphism $f : P \to R$ such that $f \circ u = v$ and $f(t_i) = r_i$ for all i.

This is called the 'universal property' of the polynomial ring in n variables over A, for the following reason. If any other ring P' with a ring homomorphism $u' : A \to P$ and a choice of n elements $t'_i \in P'$ satisfies the property above (with P', u' and t'_i instead of P, u, and t_i), then there exists a *unique* ring *isomorphism* $h : P \xrightarrow{\sim} P'$ such that $h \circ u = u'$ and $h(t_i) = t'_i$ for all i.

In other words, the above property characterizes the polynomial ring P up to unique isomorphism. The reason for this uniqueness is purely formal: given such a P', use the property of P to get a homomorphism $P \to P'$ and the property of P' to get a homomorphism $P' \to P$. From the *uniqueness* clause of the property of P, the composition $P \to P' \to P$ must be the identity. From the uniqueness clause of the property of P', the composition $P' \to P \to P'$ must be the identity. Thus the homomorphisms we found are mutually inverse, so isomorphisms.

As an example of how to use the universal property, let k be a field and suppose we want to define a ring homomorphism from $k[t_1, \ldots, t_n]$ to some ring R. Then for this we just need to specify n elements of R and a ring homomorphism $k \to R$. In most cases, it will be clear what this homomorphism should be. For instance, if $R = k$ then take the identity, and if $R = A_x$ from the exercises, we could map $\lambda \in k$ to $\lambda/1$.

It is now time to prove the universal property for $P = A[t_1, \ldots, t_n]$.

Proof. For an index tuple $I = (i_1, \ldots, i_n)$ where $i_j \in \mathbb{Z}_{\geq 0}$, and a choice of n elements $r_1, \ldots, r_n$ in an arbitrary ring R, we write r^I for the product $r_1^{i_1} \cdots r_n^{i_n}$. Thus every element of P can be written as a sum $\sum_I u(a_I)t^I$, where I ranges over all possible index tuples, $a_I \in A$, and all but a finite number of the $u(a_I)$ are zero. Now let $v : A \to R$ and $r_1, \ldots, r_n$. If a ring homomorphism $f : P \to R$ is supposed to satisfy $f \circ u = v$ and $f(t_i) = r_i$, then setting for all $p = \sum_I u(a_I)t^I \in P$

$$f(p) = \sum_I f(u(a_I))f(t^I) = \sum_I v(a_I)r^I$$

is our only choice. We see that by our definition, $f \circ u = v$ and $f(t_i) = r_i$. It remains to show that f is a homomorphism, but this I will leave to the reader. It follows from the fact that addition and multiplication of elements of R of the form $\sum_I b_I r^I$, where $b_I \in R$, mirrors precisely the addition and multiplication defined in the polynomial ring. □

On that last point, it may be good to recall the addition and multiplication in the polynomial ring: we have

$$\sum_I a_I t^I + \sum_I b_I t^I = \sum_I (a_I + b_I) t^I,$$
$$\Big(\sum_I a_I t^I\Big)\Big(\sum_I b_I t^I\Big) = \sum_I \Big(\sum_{J+K=I} a_J b_K\Big) t^I,$$

where the addition of index tuples is defined componentwise:

$$(j_1, \dots, j_n) + (k_1, \dots, k_n) = (j_1 + k_1, \dots, j_n + k_n).$$

"Basic field theory."

This section is to explain one step of the proof of Zariski's Lemma 4.25. Field theory studies *field extensions*, which are inclusions of the form $K \subseteq L$, where K and L are fields. Such a field extension is often written L/K and L is said to be a field *over* K.

Given an extension L/K, an element $\alpha \in L$ is *algebraic* if there exists a polynomial $f \in K[t]$ such that $f(\alpha) = 0$.

If $\Sigma \subseteq L$ is any set of elements, then $K(\Sigma)$ denotes the smallest subfield of L that contains Σ. This is well-defined since the intersection of two subfields is again a field. In particular, if $\alpha_1, \dots, \alpha_n \in L$ then $K(\alpha_1, \dots, \alpha_n)$ is the smallest subfield containing all the α_i. Note already that $K(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) = K(\alpha_1, \dots, \alpha_n)$.

The field extension L/K is said to be

- *algebraic* if all elements $\alpha \in L$ are algebraic,
- *finitely-generated* if there exist $\alpha_1, \dots, \alpha_n \in L$ such that $L = K(\alpha_1, \dots, \alpha_n)$,
- *finite* if L is a finite-dimensional K-vector space.

Note that the extension L/K being finitely-generated is a very different condition from the field L being a finitely-generated K-algebra. The former says that every element of L can be written as a *rational expression* in the α_i with coefficient in K. The latter, that every element can be expressed as a *polynomial* in the α_i.

Being finite is a transitive condition: if $K \subseteq E \subseteq L$ are fields, E/K is finite, and L/E is finite, then L/K is finite. Indeed, if (x_i) is a K-basis of E and (y_j) is an E-basis of L, then $(x_i y_j)$ is a K-basis of L.

The first important fact about field extensions is the following: *Let L/K be a field extension. The following are equivalent:*

(1) L/K is finite.
(2) L/K is finitely-generated and algebraic.
(3) $L = K(\alpha_1, \dots, \alpha_n)$ and the $\alpha_i \in L$ are algebraic.

Proof. (1) ⇒ (2): Let L/K be finite. Then it is finitely generated. Now let $\alpha \in L$. Then there exists $n \in \mathbb{N}$ such that the $1, \alpha, \dots, \alpha^n$ are linearly dependent over K. This gives a polynomial $f \in K[t]$ of degree n such that $f(\alpha) = 0$. Thus α is algebraic.

(2) ⇒ (3): Clear.

(3) $\Rightarrow$ (1): Let $L = K(\alpha_1, \dots, \alpha_n)$ with the $\alpha_i \in L$ algebraic. We proceed by induction on n. If $n = 1$ and $L = K(\alpha)$, let $\varphi \coloneqq K[t] \to L$ be the ring homomorphism defined by $t \mapsto \alpha$. Then $K[t]/\ker(\varphi) \simeq K[\alpha] \subseteq L$ is an integral domain, so $\ker(\varphi)$ is prime. Since α is algebraic, $\ker(\varphi)$ is nonzero. Since $K[t]$ is a principal ideal domain, $\ker(\varphi)$ is maximal. Thus $K[\alpha]$ is a field containing α, so $L = K[\alpha]$, and hence L is a finite-dimensional K-vector space, again since $\ker(\varphi) \neq 0$.

Now let $n > 1$ and $E \coloneqq K(\alpha_1, \dots, \alpha_{n-1})$ Then $K \subseteq E \subseteq L$. By the induction assumption, E/K is finite and by the $n = 1$ case, L/E is finite. Thus L/K is finite. □

Now we can prove a statement that we need for Zariski's lemma: *If L/K is a finitely-generated field extension, then there exists a field $K \subseteq E \subseteq L$ such that E is isomorphic to the function field $K(t_1, \dots, t_r)$ for some $r \geq 0$ and L/E is finite.*

Proof. Write $L = K(\alpha_1, \dots, \alpha_n)$. We construct E step by step:

(1) Start with $E \coloneqq K$.
(2) For $i = 1, \dots, n$: if α_i is not algebraic over E, then replace E by $E(\alpha_i)$.
(3) Rename the α_i so that $E = K(\alpha_1, \dots, \alpha_r)$.

At the end of this algorithm, we have $L = E(\alpha_{r+1}, \dots, \alpha_r)$ where $\alpha_{r+1}, \dots, \alpha_n \notin E$, and by our construction the $\alpha_{r+1}, \dots, \alpha_n$ are algebraic over E. Thus L is algebraic over E.

Moreover, $E \simeq K(t_1, \dots, t_r)$, which we show by proving that $K[\alpha_1, \dots, \alpha_r] \simeq K[t_1, \dots, t_r]$. We have a surjective homomorphism $\varphi : K[t_1, \dots, t_r] \to K[\alpha_1, \dots, \alpha_r]$, and if f is a nonzero element of $\ker(\varphi)$, then f contains some variable t_i. Among these possible t_i, we can choose one such that α_i was added last in the algorithm, say for instance $i = r$. But then f shows that α_r is algebraic over $K(\alpha_1, \dots, \alpha_{r-1})$, contradiction. □

Zariski's lemma's assumption is that L is even finitely generated as a K-algebra, so in particular L/K is a finitely generated as a field extension. Again, the former condition is much stronger: by Zariski's lemma itself, it implies for instance that we can take $E = K$ in the former statement.

References

Reported here is the bibliographic data for the course textbook, as well as the articles where this course's major results first appeared. I give the references for Noether's theory of ideal decompositions, Hilbert's Basis Theorem and Nullstellensatz, and Artin–Tate's and Zariski's lemmas. Also included is a classic text by Artin on modern field theory.

[1] Emil Artin. *Galois Theory.* University of Notre Dame, 1942.

[2] Emil Artin and John T. Tate. A note on finite ring extensions. *Journal of the Mathematical Society of Japan* **3**, 74–77 (1951). https://doi.org/10.2969/jmsj/00310074

[3] Michael F. Atiyah and Ian G. Macdonald. *Introduction to Commutative Algebra.* Addison-Wesley, 1969.

[4] David Hilbert. Ueber die Theorie der algebraischen Formen. *Mathematische Annalen* **36**, 473–534 (1890). https://doi.org/10.1007/BF01208503

[5] David Hilbert. Ueber die vollen Invariantensysteme. *Mathematische Annalen* **42**, 313–373 (1893). https://doi.org/10.1007/BF01444162

[6] Emmy Noether. Idealtheorie in Ringbereichen. *Mathematische Annalen* **83**, 24–66 (1921). https://doi.org/10.1007/BF01464225

[7] Oscar Zariski. A new proof of Hilbert's Nullstellensatz. *Bulletin of the American Mathematical Society* **53**, 362–368 (1947). https://doi.org/10.1090/s0002-9904-1947-08801-7