Exercises in Commutative Algebra

based on

A Course in Commutative Algebra (G. Kemper)

Marvin Jahn
mail@marvin-jahn.de

August 7, 2020

Contents

9 Mixed Problems

This is a collection of exercises corresponding to the lecture *Algebra II* held by Prof. G. Kemper at the Technical University Munich in the summer semester 2020. It is based on the book *A Course in Commutative Algebra* and all references within this document refer to that book.

Hilbert's Nullstellensatz

Remark 1. (a) It is important to know the difference between being generated as a module, ideal, group or algebra.

(b) We define a R-algebra A as a ring with a homomorphism $\alpha : R \to A$. Another equivalent definition is that A is an additive abelian group, that is both a ring and a R-module. These definitions are equivalent:
If α is given, we define the scalar multiplication for $\lambda \in R, a \in A$ as $\lambda \cdot a \coloneqq \alpha(\lambda) \cdot a$.
If the other definition is given, we define $\alpha : R \to A$ by $\lambda \mapsto \lambda \cdot 1$.

(c) For a K-algebra A, K a field, the corresponding homomorphism is injective and thus it is natural to think of K as being embedded into A.

(d) For a R-algebra A, a R-algebra homomorphism $A \to A$ is also a R-module homomorphism, but not a A-module homomorphism as the example $R = \mathbb{Z}$, $A = \mathbb{Z}[x]$, $\mathbb{Z}[x] \to \mathbb{Z}[x],\ x \mapsto 0$ shows.

(e) Our varieties are called *affine*, because there are also other types of varieties, e.g. *projective* varieties.

(f) It is important to remember that any nonzero polynomial in $K[x]$ only has finitely many roots, but for $K[x, y]$ or larger polynomial rings, this is not true (e.g. $f = x - y \in K[x, y]$ with K an infinite field).

(g) Any finite subset $S \subset K^n$ is an affine variety and for $n = 1$ those are the only affine varieties except for K itself.

(h) It holds for any ideal $I \subset K[x_1, \ldots, x_n]$: $V(I) = V(\sqrt{I})$.

Lemma 2. Let $R \subset S \subset T$ be rings, such that S is finitely generated as an R-algebra and T is finitely generated as an S-algebra. Then T is finitely generated as an R-algebra.

Proof. Write $S = R[s_1, \ldots, s_n]$, $T = S[t_1, \ldots, t_m]$. Let $z \coloneqq s \cdot \prod_{j=1}^{m} t_j^{i_j} \in T$ with $s \in S, i_j \in \mathbb{N}$ and $s = \sum_{h=1}^{k} r_h \prod_{j=1}^{n} s_j^{i'_j}$ with $r_h \in R, i'_j \in \mathbb{N}$. Plugging this into z shows $z \in R[s_1, \ldots, s_n, t_1, \ldots, t_m]$ and because every element in T is a finite sum of elements of the form of z, this shows $T = R[s_1, \ldots, s_n, t_1, \ldots, t_m]$. □

Lemma 3. A K-algebra A with $\dim_K(A) < \infty$ is algebraic over K.

We give two short proofs.

Proof. Let $n \coloneqq \dim_K(A)$. Then any K-linearly independent set has at most n elements. Thus for any $a \in A$, the set $\{1, a, a^2, \ldots, a^n\}$ must be linearly dependent, which gives us a polynomial with coefficients in K and a as a root. □

Proof. By contraposition, assume that A is not algebraic, i.e. there is $a \in A$, which is not algebraic over K. Then the monomorphism (injective homomorphism) of K-algebras (and in particular of K-vector spaces)

$$\phi : K[x] \to A, f \mapsto f(a)$$

shows that

$$\dim_K(A) \geq \dim_K(\mathrm{im}(\phi)) = \dim_K(K[x]) = \infty.$$

□

Lemma 4. Let K be a field. If $S \subset K[x_1, \ldots, x_n]$ is a set of polynomials, then $V(S) = V((S))$. Moreover, if $I = (f_1, \ldots, f_m) \subset K[x_1, \ldots, x_n]$ is a finitely generated ideal, then $V(I) = V(f_1, \ldots, f_m)$, i.e. the vanishing set is determined by the generators.

Proof. Both statements follow directly from the definition, since any element in (S) is a K-linear combination of elements of S and similarly every element in I is a K-linear combination of the f_i. □

1.1 Some K-algebra examples

Find examples of a K-algebra A, such that:

(a) A is an integral domain (ID), but not a field.

(b) A is algebraic over K but not a field.

(c) A is a field but not algebraic over K.

(d) A is an affine K-domain (finitely generated K-algebra, that is an ID), but not algebraic over K.

When we don't specify the corresponding homomorphism, we always mean the natural inclusion.

(a) $A = K[x]$

(b) Three solutions:

(1) $A = 0$: The easiest solution is the zero ring.

(2) $A = K[x]/(x^2)$: This is not an ID ($x \cdot x = 0$) and thus not a field, but it is algebraic over K. This can be seen by taking an element $a + bx$ and finding a polynomial of degree two that has that element as a root.
It also follows directly from 3, since A is a 2-dimensional K vector space.

(3) $A = K^{2\times 2}$: The ring of 2×2 matrices with coefficients in K is clearly not a field, but it is algebraic, since for $M \in A$, its characteristic polynomial $g(x) := \det(x \cdot I_n - M)$ satisfies $g(M) = 0$ by Cayley-Hamilton.

(c) $K(x)$

(d) $K[x]$

1.2 $\mathbb{Q}$ as a $\mathbb{Z}$-algebra

Prove that $\mathbb{Q}$ is not finitely generated as a $\mathbb{Z}$-algebra.

Given finitely many rational numbers $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$, there is a prime number $p \in \mathbb{Z}$, which does not divide any of the q_i. Thus $\frac{1}{p} \notin \mathbb{Q}[\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}]$.

1.3 Properties of the radical operator

Let R be a ring and $I \subset R$ an ideal.

(a) Show that $\sqrt{I}$ is an ideal and that $\sqrt{\sqrt{I}} = \sqrt{I}$.

(b) Show that a prime ideal is radical.

(c) Determine $\sqrt{I}$ for $I = (12) \subset \mathbb{Z}$ and $I = (0) \subset \mathbb{Z}/4\mathbb{Z}$.

(d) Give an example of a proper ideal in $\mathbb{Z}$ that is radical but not prime.

(a) and (b) follow quickly from the definition.
Since $\mathbb{Z}$ is a principal ideal domain (PID), any ideal is generated by one element. In $\mathbb{Z}$, the radical ideals are those, whose generator has no prime factor more than once.
Thus, in (c) we find that $\sqrt{(12)} = (6) \subset \mathbb{Z}$ and $\sqrt{(0)} = (2) \subset \mathbb{Z}/4\mathbb{Z}$.
Using (a) and (c), we know that $(6) \subset \mathbb{Z}$ is a radical ideal, but of course it is not prime, so (d) is done.

1.4 Some (potential) affine varieties

Check if the following subsets of $\mathbb{C}^2$ are affine varieties or not by determining a subset $S \subset \mathbb{C}[x, y]$ such that $X = V(S)$ or proving that such a set cannot exist.

(a) $X = \{(x, y) \in \mathbb{C}^2 : x = y \text{ or } x = -y\}$

(b) $X = \{(x, y) \in \mathbb{C}^2 : x \neq 0 \text{ and } y = x^2\}$

(c) $X = \{(x, y) \in \mathbb{C}^2 : x \neq 0 \text{ and } y = \frac{1}{x} + x^2\}$

(d) $X = \{(x, y) \in \mathbb{C}^2 : x = 0 \text{ and } y \in \{0, 1, 2\}\}$

(e) $X = \{(x, y) \in \mathbb{C}^2 : x = 0 \text{ and } y \in \mathbb{Z}\}$

(a) $S = \{(x + y)(x - y)\}$

(b) This is not an affine variety. We give two proofs:

(1) Since any polynomial f is continuous, the set $f^{-1}(0)$ is closed. As an intersection of closed sets, $V(S)$ must be closed as well, but X is not.

(2) Aiming for contradiction, assume that $X = V(S)$.
Since $X \neq \mathbb{C}^2$, it is $S \neq \emptyset$, so let $f \in S$. It holds $f(x, y) = 0 \ \forall \ (x, y) \in X$. In particular, $f(x, x^2) = 0 \ \forall \ x \in \mathbb{C} \setminus \{0\}$. With the $\mathbb{C}$-algebra homomorphisms

$$\phi : \ \mathbb{C}[x, y] \to \mathbb{C}[x], \ x \mapsto x, \ y \mapsto x^2,$$

$f(x, x^2)$ can be seen as a polynomial in $\mathbb{C}[x]$, namely as its image $\phi(f)$. If $\phi(f)$ were non-zero, it could only have finitely many roots, thus $\phi(f) = 0$. The commutative diagram

$$\begin{array}{ccc} \mathbb{C}[x,y] & \xrightarrow{\quad\phi\quad} & \mathbb{C}[x] \\ & \searrow^{\mathrm{eval}_{(0,0)}} \quad \swarrow_{\mathrm{eval}_0} & \\ & \mathbb{C} & \end{array}$$

shows that

$$f(0,0) = \mathrm{eval}_{(0,0)}(f) = (\mathrm{eval}_0 \circ \phi)(f) = \phi(f)(0) = 0.$$

Since f was generic in S, it follows $(0,0) \in V(S) = X$. Contradiction.

(c) Since

$$y = \frac{1}{x} + x^2, x \neq 0 \iff xy = 1 + x^3,$$

we can choose $S = \{xy - x^3 - 1\}$.

(d) $S = \{x, y(y-1)(y-2)\}$. One can show that since $\mathbb{C}$ is algebraically closed, a single polynomial will not be enough here.

(e) This is not an affine variety. The argument is similar to that of (b). A polynomial with $f \in \mathbb{C}[x, y]$ with $f(0, z) = 0$ for all $z \in \mathbb{Z}$ corresponds to a polynomial $f(0, -) \in \mathbb{C}[y]$, which has infinitely many roots and thus must be the zero polynomial, implying $\{0\} \times \mathbb{C} \subset V(f)$.

1.5 The ring of formal power series

Let K be a field and $R \coloneqq K[\![x]\!]$ the ring of formal power series over K.

(a) Show that R is an integral domain.

(b) Show that the group of units in R is given by

$$R^\times = \left\{ \sum_{i=0}^{\infty} a_i x^i \in R : a_0 \neq 0 \right\}.$$

(c) Show that $(x) \subset R$ is the only maximal ideal.

(d) Show that the *Laurent power series ring*

$$L \coloneqq K((x)) \coloneqq \left\{ \sum_{i=m}^{\infty} a_i x^i : m \in \mathbb{Z}, a_i \in K \right\}$$

is a field and is isomorphic to $\mathrm{Quot}(R)$.

(e) Show that $L = R[x^{-1}]$.

(f) Is R finitely generated as a K-algebra?

(a) Assume $0 = (\sum_{i=0}^{\infty} a_i x^i) \cdot (\sum_{i=0}^{\infty} b_i x^i)$ and $a_i \neq 0$ for some $i \in \mathbb{N}$. Choose $k \in \mathbb{N}$ minimal, such that $a_k \neq 0$. We want to show that $b_i = 0$ for all $i \in \mathbb{N}$. It is

$$0 = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i = \sum_{i=0}^{\infty} \left(\sum_{j=k}^{i} a_j b_{i-j} \right) x^i.$$

We use induction on n.
Base base: Considering the coefficient of x^k, we get $a_k b_0 = 0$, so $b_0 = 0$.
Inductive step ($n-1 \rightsquigarrow n$): Considering the coefficient of x^{n+k}, we get by induction

$$0 = \sum_{j=k}^{n+k} a_j b_{n+k-j} = a_k b_n,$$

showing $b_n = 0$.
Alternatively, one can use contraposition; if $f, g \in R$ are nonzero, then $f \cdot g$ is nonzero by the same calculation as above.

(b) Let $f = \sum_{i=0}^{\infty} a_i x^i \in R$. It holds $f \in R^\times$ if and only if there is $\sum_{i=0}^{\infty} b_i x^i \in R$ with

$$1 = \left(\sum_{i=0}^{\infty} a_i x^i \right) \cdot \left(\sum_{i=0}^{\infty} b_i x^i \right) = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) x^i.$$

Comparing coefficients, this is equivalent to

$$a_0 b_0 = 1 \ \wedge \ \forall\, n \in \mathbb{N}_{>0} : \sum_{j=0}^{n} a_j b_{n-j} = 0.$$

In particular, it follows $a_0 \neq 0$. Moreover, that condition is also sufficient for $f \in R^\times$: Defining recursively

$$b_0 \coloneqq a_0^{-1}, \ \forall\, n \in \mathbb{N}_{>0} : b_n \coloneqq \left(-a_0^{-1}\right) \cdot \sum_{j=1}^{n} a_j b_{n-j}$$

gives $\sum_{i=0}^{\infty} b_i x^i \in R$ with the desired property.

(c) Let $I \subsetneq R$ be a proper ideal and let $a = \sum_{i=0}^{\infty} a_i x^i \in I$. By (b), it is $a_0 = 0$, so

$$a = \sum_{i=1}^{\infty} a_i x^i = x \cdot \sum_{i=0}^{\infty} a_{i+1} x^i \in (x),$$

showing $I \subset (x)$. It is clear that $(x) \neq R$, so (x) is the only maximal ideal of R.

(d) First, we show that L is a field. One possibility to do so is the following:
Let $0 \neq f = \sum_{i=m}^{\infty} a_i x^i \in L$ and $m \in \mathbb{Z}$ minimal with $a_m \neq 0$. Then

$$x^{-m} \cdot f = x^{-m} \cdot \sum_{i=m}^{\infty} a_i x^i = \sum_{i=0}^{\infty} a_{i+m} x^i \in R^\times$$

by (b) and thus there is $g \in R$ with $(\sum_{i=0}^{\infty} a_{i+m} x^i) \cdot g = 1$, implying $f \cdot x^{-m} g = 1$.
Another proof, which is more tedious, goes as follows:

Let $0 \neq \sum_{i=m}^{\infty} a_i x^i \in L$ and choose $m \in \mathbb{Z}$ minimal, such that $a_m \neq 0$. As in (b), we need to construct an inverse; i.e. $\sum_{m'}^{\infty} b_i x^i \in L$, $b_{m'} \neq 0$ with

$$1 = \left(\sum_{i=m}^{\infty} a_i x^i\right) \cdot \left(\sum_{i=m'}^{\infty} b_i x^i\right) = \sum_{i=-\infty}^{\infty} \left(\sum_{j=-\infty}^{\infty} a_j b_{i-j}\right) x^i = \sum_{i=-\infty}^{\infty} \left(\sum_{j=m}^{i-m'} a_j b_{i-j}\right) x^i.$$

Comparing coefficients, this means that

$$\sum_{j=m}^{-m'} a_j b_{-j} = 1 \ \wedge \ \forall\, n \in \mathbb{Z} \setminus \{0\} : \sum_{j=m}^{n-m'} a_j b_{n-j} = 0.$$

In particular, choosing $n = m + m'$ shows $m' = -m$. Thus, the previous expression is equivalent to

$$a_m b_{-m} = 1 \ \wedge \ \forall\, n \in \mathbb{N} \setminus \{0\} : \sum_{j=m}^{n+m} a_j b_{n-j} = 0$$

or equivalently

$$b_{-m} = a_m^{-1} \ \wedge \ \forall\, n \in \mathbb{N} \setminus \{0\} : b_{-m+n} = \left(-a_m^{-1}\right) \cdot \sum_{j=m+1}^{n+m} a_j b_{n-j}.$$

This defines $\sum_{m'}^{\infty} b_i x^i \in L$ with the desired properties and L is thus a field.
Both proofs also shows that any element $0 \neq f = \sum_{i=m}^{\infty} a_i x^i \in L$ is in R, or is a multiplicative inverse of some element of R. This suggests that L is the "smallest" field that contains R and motivates $L \cong \mathrm{Quot}(R)$, which will be proven more formally now. There are again multiple ways to do so:
For one, we can show that L satisfies the universal property of the quotient field $\mathrm{Quot}(R)$: For any field K and any injective ring homomorphism $g : R \hookrightarrow K$, there is a unique ring homomorphism $f : \mathrm{Quot}(R) \to K$, such that the diagram

$$\begin{array}{ccc} R & \longrightarrow & \mathrm{Quot}(R) \\ \downarrow{\scriptstyle g} & \swarrow{\scriptstyle f} & \\ K & & \end{array}$$

commutes.
We see that L indeed satisfies this property, because a ring homomorphism $L \to K$ commuting as in the above diagram is uniquely determined by $g : R \hookrightarrow K$, since any element in L is in R or is a multiplicative inverse of an element in R.
Another proof is to show that the ring homomorphism

$$\phi : \mathrm{Quot}(R) \to L, \ \frac{f}{g} \mapsto f \cdot g^{-1}$$

is an isomorphism.
As a ring homomorphism between fields, ϕ is injective. For $f \in L$, we know that $f \in R$ or $f^{-1} \in R$, so ϕ is surjective.

(e) "$\subset$": Let $f = \sum_{i=m}^{\infty} a_i x^i \in L$. Then

$$f = x^m \cdot \sum_{i=m}^{\infty} a_i x^{i-m} = x^m \cdot \sum_{i=0}^{\infty} a_{i+m} x^i \in R[x^{-1}]$$

so $L \subset R[x^{-1}]$.
Another way to see the same thing:

$$f = \sum_{i=m}^{\infty} a_i x^i = \sum_{i=m}^{-1} \underbrace{a_i}_{\in R} \left(x^{-1}\right)^{-i} + \underbrace{\sum_{i=0}^{\infty} a_i x^i}_{\in R} \in R[x^{-1}].$$

"$\supset$": Let $f = \sum_{i=0}^{<\infty} r_i x^{-i} \in R[x^{-1}], r_i \in R$. For every $i \in \mathbb{N}$, it is $r_i x^{-i} \in L$, so $f \in L$ and $R[x^{-1}] \subset L$.

(f) Arguing by contradiction, suppose that R was finitely generated as a K-algebra. By (e) and 2, this implies that L is finitely generated as a K-algebra. Lemma 1.1(b) shows that L is thus algebraic over K, which is wrong, since $x \in L$. Contradiction. One could also argue further after the application of lemma 1.1(b) and note that R is algebraic as well and thus by application of lemma 1.1(a) conclude that R is a field, which is clearly wrong.

1.6 Maximal spectrum and Rabinowitsch spectrum

(a) Show for any ring R:

$$\mathrm{Spec}_{\mathrm{max}}(R) \subset \mathrm{Spec}_{\mathrm{rab}}(R).$$

(b) Consider the formal power series ring $R \coloneqq K[\![y]\!]$ in the indeterminate y over a field K. Furthermore, let $S \coloneqq R[z]$ be the polynomial ring over R. Show that in S the inclusions

$$\mathrm{Spec}_{\mathrm{max}}(S) \subsetneq \mathrm{Spec}_{\mathrm{rab}}(S) \subsetneq \mathrm{Spec}(S)$$

are strict by considering the ideals $(y)_S$, $(z)_S$.

(a) We give two proofs, the first of constructive nature, the second using the axiom of choice. Consider the surjective R-algebra homomorphism

$$\phi : \ R[x] \to R, \ x \mapsto 0.$$

and let $I \in \mathrm{Spec}_{\mathrm{max}}(R)$ be a maximal ideal. The preimage $\phi^{-1}(I)$ is a maximal ideal in $R[x]$, so $I \in \mathrm{Spec}_{\mathrm{rab}}(R)$ follows from

$$I = \{I + x \cdot R[x]\} \cap R = \phi^{-1}(I) \cap R.$$

Alternatively, one can argue as follows:
For $I \in \mathrm{Spec}_{\max}(R)$ a maximal ideal, there is $\overline{I} \in \mathrm{Spec}_{\max}(R[x])$ with $I \subset \overline{I}$ by Zorn's lemma. It holds $\overline{I} \cap R = i^{-1}(\overline{I}) \in \mathrm{Spec}(R)$, where $i : R \hookrightarrow R[x]$ is the inclusion map. Since also $I \subset \overline{I} \cap R$, we conclude $I = \overline{I} \cap R$ and $I \in \mathrm{Spec}_{\mathrm{rab}}(R)$.

(b) Consider the surjective K-algebra homomorphism

$$\phi : (K[\![y]\!])[z] \to K[z],\ y \mapsto 0$$

with kernel $(y)_S$. The homomorphism theorem shows $S/(y) \cong K[z]$, so $(y) \in \mathrm{Spec}(S)$.
To show $(y)_S \notin \mathrm{Spec}_{\mathrm{rab}}(S)$, let $I \supset (y)_S$ be a maximal ideal in $S[z']$. Then $S[z']/I$ is a field and since $y \in I$, $S[z']/I$ is finitely generated as a K-algebra (namely by $\overline{z}$ and $\overline{z'}$). Lemma 1.1(b) shows that $S[z']/I$ is algebraic over K, so there is a polynomial $f \in K[x] \setminus \{0\}$ with $f(z) \in I$. Since $f(z) \in S \setminus (y)_S$, it follows $I \cap S \supsetneq (y)_S$ and thus $(y)_S \notin \mathrm{Spec}_{\mathrm{rab}}(S)$.
Clearly $(z)_S \notin \mathrm{Spec}_{\max}(S)$, because $S/(z) \cong R = K[\![y]\!]$ is not a field.
It is left show $(z)_S \in \mathrm{Spec}_{\mathrm{rab}}(S)$. A maximal ideal $I \supset (z)_{S[z']}$ in $S[z']$ corresponds to a maximal ideal $I' \subset S[z']/(z)_{S[z']} \cong (K[\![y]\!])[z']$. Quotienting by I' has to yield a field, and y and z' are both lacking inverses, so it is natural to define the algebraic relation $y \cdot z' \coloneqq 1$; i.e. to consider $I' \coloneqq (y \cdot z' - 1)$. Now $(K[\![y]\!])[z']/I' \cong (K[\![y]\!])[y^{-1}]$, which is the ring of formal laurent series and in particular a field.
Therefore, $I' \subset (K[\![y]\!])[z']$ is maximal and so is $I = (I', z) = (y \cdot z' - 1, z) \subset S[z']$. It follows $(z)_S = I \cap S$ and thus $(z)_S \in \mathrm{Spec}_{\mathrm{rab}}(S)$.

1.7 Characterization of Jacobson Rings

Show that a ring R is Jacobson if and only if every prime ideal $P \in \mathrm{Spec}(R)$ is an intersection of maximal ideals.

Since any prime ideal is radical, it is clear that every Jacobson ring has the claimed property.
On the other hand, suppose that every prime ideal $P \in \mathrm{Spec}(R)$ can be written as an intersection of maximal ideals and let $I \subset R$ be an ideal. Since $\sqrt{I}$ is equal to the intersection of all prime ideals containing I and every prime ideal is by assumption equal to an intersection of maximal ideals, $\sqrt{I}$ can be written as an intersection of maximal ideals, which contain I. Consequently,

$$\bigcap_{m \in \mathrm{Spec}_{\max}(R), I \subset m} m \subset \sqrt{I}$$

and the other inclusion is clear.

1.8 Some Jacobson rings

(a) Is $K[\![x]\!]$ Jacobson?

(b) Is $\mathbb{Z}$ Jacobson?

(c) When are local rings (rings with exactly one maximal ideal) Jacobson?

(d) When are principal ideal domains Jacobson?

(a) No, as it is

$$\sqrt{(0)} = (0) \neq (x) = \bigcap_{I \in \mathrm{Spec}_{\max}(K[\![x]\!])} I,$$

since (x) is the only maximal ideal in $K[\![x]\!]$.

(b) Yes. Clearly, it is $\sqrt{(0)} = (0) = \bigcap_{P \in \mathrm{Spec}_{\max}(\mathbb{Z})} P$. Since $\mathbb{Z}$ is a principal ideal domain, it is $\mathrm{Spec}_{\max}(\mathbb{Z}) = \mathrm{Spec}(\mathbb{Z}) \setminus \{(0)\}$ and thus for $I \neq (0)$:

$$\sqrt{I} = \bigcap_{P \in \mathrm{Spec}(\mathbb{Z}), I \subset P} P = \bigcap_{P \in \mathrm{Spec}_{\max}(\mathbb{Z}), I \subset P} P.$$

(c) Since local rings only have one maximal ideal, they are Jacobson, if and only if that maximal ideal is the only prime ideal.

(d) Just as in (b), we know that $\sqrt{I} = \bigcap_{P \in \mathrm{Spec}_{\max}, I \subset P} P$, for all ideals $I \neq (0)$. So the only potential problem is the zero ideal. This means that principal ideal domains are Jacobson, if and only if $\bigcap_{P \in \mathrm{Spec}_{\max}} P = \{0\}$.

1.9 Maximal ideals of an algebraic field extension

Let $K \subset L$ be an algebraic field extension and $I \subset L[x]$ be a maximal ideal. Prove that $J \coloneqq I \cap K[x]$ is a maximal ideal in $K[x]$.

Consider $K[x] \hookrightarrow L[x] \twoheadrightarrow L[x]/I$. $L[x]/I$ is a field and finitely generated as an L-algebra, so it is algebraic over L by lemma 1.22(b). Since $K \subset L$ is an algebraic field extension, $L[x]/I$ is algebraic over K. Using the monomorphism

$$\phi : K[x]/J \to L[x]/I,\ f + J \mapsto f + I$$

it follows that $K[x]/J$ is also algebraic over K. ϕ also shows that $K[x]/J$ is an integral domain. Alternatively, notice that with $\varphi : K[x] \hookrightarrow L[x]$, it is $J = \varphi^{-1}(I)$. By lemma 1.22(a), $K[x]/J$ is a field.

1.10 A Counterexample to the Nullstellensatz

Consider the polynomial $f(x,y) = x^4 - y^4 \in \mathbb{R}[x,y]$ and the ideal $I = (f) \subset \mathbb{R}[x,y]$. Determine the set $V(I) \subset \mathbb{R}^2$.
Does the second form of the Nullstellensatz hold here, i.e. is $I(V(I)) = \sqrt{I}$?

Since

$$f(x,y) = x^4 - y^4 = (x^2+y^2)(x^2-y^2) = (x^2+y^2)(x-y)(x+y),$$

it is (due to 4)

$$V(I) = V(x^2+y^2) \cup V(x-y) \cup V(x+y) = \{(x,y) \in \mathbb{R}^2 | x = y \text{ or } x = -y\}.$$

Thus

$$I(V(I)) = I(\{(x,y) \in \mathbb{R}^2 | x = y \text{ or } x = -y\}) = (x-y) \cap (x+y) = (x^2-y^2) \subset \mathbb{R}[x,y].$$

It is clear that $f(x,y) = (x^2+y^2)(x-y)(x+y) \subset \mathbb{R}[x,y]$ is a decomposition into irreducible polynomials. Therefore $\sqrt{I} = I$, i.e. I is radical. This shows that $\sqrt{I} = I = (x^4-y^4) \subsetneq (x^2-y^2) = I(V(I))$.

1.11 Colon Ideals

Let R be a ring and $I, J \subset R$ two ideals. We define the *colon ideal* (or *ideal quotient*) via

$$I : J \coloneqq \{a \in R : ab \in I \ \forall \ b \in J\}.$$

Prove the following:

(a) $(I : J) \cdot J \subset I \subset I : J$.

(b) $\sqrt{I} : J = \bigcap_{P \in M} P$, where $M \coloneqq \{P \in \operatorname{Spec}(R) : I \subset P, J \not\subset P\}$.

(c) The geometric content of the ideal quotient is that it gives the ideal of the complement of a subvariety.
More precisely, let K be a field and $X, Y \subset K^n$ be two subsets. If Y is an affine variety, then $I(X) : I(Y) = I(X \setminus Y)$.

(d) Without the assumption of affineness of Y the previous statement is not true, i.e. find a counterexample for that case.

(a) Let $a \in (I : J) \cdot J$ be a generator of that ideal, i.e. we can write $a = b \cdot c$ with $b \in I : J$ and $c \in J$. By definition of $I : J$, it follows $a \in I$, so $(I : J) \cdot J \subset I$.
Now let $a \in I$. Then $b \cdot a \in I$ for any $b \in J$, so $a \in I : J$ and $I \subset I : J$.

(b) "$\subset$": Let $a \in \sqrt{I} : J$ and $P \in M$. By definition, there is $b \in J \setminus P$. Since $ab \in \sqrt{I} \subset P$ and P is prime, it follows $a \in P$.
"$\supset$": Let $a \in \bigcap_{P \in M} P$ and $b \in J$. Additionally, let $Q \in \operatorname{Spec}(R)$ be a prime ideal

with $I \subset Q$. If $J \subset Q$, then $b \in Q$, so $ab \in Q$. If $J \not\subset Q$, then $Q \in M$, so $a \in Q$, thus $ab \in Q$.
Because $\sqrt{I} = \bigcap_{Q \in \mathrm{Spec}(R), I \subset Q} Q$ by Corollary 1.12, it follows $ab \in \sqrt{I}$, i.e. $a \in \sqrt{I} : J$.

(c) "$\subset$": Let $f \in I(X) : I(Y)$ and $p \in X \backslash Y$. By assumption, $f(p) \cdot g(p) = 0 \,\forall\, g \in I(Y)$. Since $p \notin Y$ and Y is an affine variety, there is $g_* \in I(Y)$ with $g_*(p) \neq 0$. Thus $f(p) \cdot g_*(p) = 0$ implies $f(p) = 0$, i.e. $f \in I(X \setminus Y)$.
"$\supset$": Let $f \in I(X \setminus Y)$. By definition, $f(p) = 0 \;\forall\; p \in X \setminus Y$. Thus, for any $g \in I(Y)$ it holds $f(p) \cdot g(p) = 0 \,\forall p \in X$, so $f \in I(X) : I(Y)$.

(d) Let $K = \mathbb{C}$, $n = 1$, $X = \mathbb{C}$ and $Y = \mathbb{Z}$. Then $I(X) = I(Y) = I(X \setminus Y) = \{0\}$. But $I(X) : I(Y) = \mathbb{C}[x]$.

1.12 Affine varieties in non-algebraically closed fields

(a) Let K be a field and $p \in K[x]$ a non-constant polynomial of degree d, which has no zeros in K. Let $f, g \in K[x_1, \ldots, x_n]$ and define $h := p(\frac{f}{g}) \cdot g^d \in K[x_1, \ldots, x_n]$. Prove that $V(f, g) = V(h)$.

(b) Let K be a field which is not algebraically closed and $X \subset K^n$ be a finitely generated affine variety, i.e. $X = V(S)$ with $S \subset K[x_1, \ldots, x_n]$ finite.
Prove that there exists $f \in K[x_1, \ldots, x_n]$ such that $X = V(f)$.
Since $K[x_1, \ldots, x_n]$ is Noetherian (proven later), every affine variety can be given by a finite set of polynomials. Therefore, for non-algebraically closed fields, every affine variety can be given by a single polynomial.

(a) Write $p = \sum_{i=0}^{d} a_i x^i$ with $a_i \in K$. Then $h = \sum_{i=0}^{d} a_i f^i g^{d-i}$.
"$\subset$": Let $x \in V(f, g)$, i.e. $f(x) = g(x) = 0$. Thus $h(x) = 0$.
"$\supset$": Let $x \in V(h)$, i.e. $h(x) = 0$. Since p has no roots in K, it follows $g^d(x) = 0$, i.e. $g(x) = 0$. This means that $0 = h(x) = \sum_{i=0}^{d} a_i f^i(x) g^{d-i}(x) = a_d f^d(x)$ with $a_d \neq 0$, so $f(x) = 0$ as well.

(b) Write $X = V(f_1, \ldots, f_m)$. Since K is not algebraically closed, there is a non-constant polynomial $p \in K[x]$, which has no zeros in K. By (a), there exists $h_1 \in K[x]$ such that $V(f_1, f_2) = h_1$. Repeating this argument inductively, we get

$$V(f_1, \ldots, f_m) = V(h_1, f_2, \ldots, f_m) = V(h_2, f_3, \ldots, f_m) = \ldots = V(h_m).$$

1.13 A generalization of Hilbert's Nullstellensatz

Let K be a field, $\bar{K}$ its algebraic closure and $I \subset K[x_1, \ldots, x_n]$ an ideal. Show that

$$I_{K[x_1,\ldots,x_n]}(V_{\bar{K}^n}(I)) = \sqrt{I}.$$

In this notation, the subscript denotes where the ideal lives or the vanishing takes place.

The proof of this statement is involved, because I is not necessarily an ideal in $\bar{K}[x_1, \ldots, x_n]$.
Set $J \coloneqq (I)_{\bar{K}[x_1,\ldots,x_n]}$. Since $K[x_1, \ldots, x_n] \subset \bar{K}[x_1, \ldots, x_n]$, Hilbert's Nullstellensatz yields

$$I_{K[x_1,\ldots,x_n]}(V_{\bar{K}^n}(I)) = I_{\bar{K}[x_1,\ldots,x_n]}(V_{\bar{K}^n}(I)) \cap K[x_1, \ldots, x_n] = \sqrt{J} \cap K[x_1, \ldots, x_n]$$

So we need to show:

$$\sqrt{J} \cap K[x_1, \ldots, x_n] = \sqrt{I}. \tag{1}$$

We will show the slightly stronger statement

$$J \cap K[x_1, \ldots, x_n] = I, \tag{2}$$

which implies (1). We give two different arguments for the inclusion "$\subset$", the other inclusion "$\supset$" is trivial.

(a) Let $f \in J \cap K[x_1, \ldots, x_n]$. Because $J = (I)_{\bar{K}[x_1,\ldots,x_n]}$, we can write $f = \sum_{i=1}^{<\infty} \bar{k}_i a_i$ with $\bar{k}_i \in \bar{K}[x_1, \ldots, x_n]$, $a_i \in I$. Since $\bar{K}$ is a K-vector space, we can choose a K-basis $B = (b_i)_{i \in I}$ with I an index set and $1 \in B$. Notice that this is also a $K[x_1, \ldots, x_n]$-basis of $\bar{K}[x_1, \ldots, x_n]$, when we view $\bar{K}[x_1, \ldots, x_n]$ as a $K[x_1, \ldots, x_n]$-module. It follows with $a_i \in I, k_i \in \bar{K}[x_1, \ldots, x_n], k_{i,j} \in K[x_1, \ldots, x_n]$:

$$\begin{aligned} 1 \cdot f &= f \\ &= \sum_{i=1}^{<\infty} \bar{k}_i a_i \\ &= \sum_{i=1}^{<\infty} a_i \sum_{j=1}^{<\infty} k_{i,j} b_j \\ &= \sum_{j=1}^{<\infty} b_j \left(\sum_{i=1}^{<\infty} k_{i,j} a_i \right). \end{aligned}$$

Since the b_i form a $K[x_1, \ldots, x_n]$-basis of $\bar{K}[x_1, \ldots, x_n]$ one of the b_j must be 1, so this implies

$$f = \sum_{i=1}^{<\infty} k_{i,j} a_i,$$

which shows that $f \in I$ and thus (2), because I is an ideal in $K[x_1, \ldots, x_n]$.

(b) Let $f \in J \cap K[x_1, \ldots, x_n]$. Then there exist $g_1, \ldots, g_m \in I$ and $h_1, \ldots, h_m \in \bar{K}[x_1, \ldots, x_n]$, such that $f = \sum_{i=1}^{m} g_i h_i$.
For intuition, we first consider the special case $K = \mathbb{R}$, $\bar{K} = \mathbb{C}$: Define $\psi : \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{R}[x_1, \ldots, x_n]$ by taking the real part of each coefficient.
This mapping has the following properties:

- $\psi(f + g) = \psi(f) + \psi(g)$.
- $\forall\, f \in \bar{K}[x_1, \ldots, x_n]$, $g \in K[x_1, \ldots, x_n] : \psi(g \cdot f) = g \cdot \psi(f)$.
  Note that because of the linearity, it is enough to show this property for a monomial $f \in \bar{K}[x_1, \ldots, x_n]$ and for those it is clear.
- $\psi|_{K[x_1,\ldots,x_n]} = \mathrm{id}$.
  This follows from the previous point, since for all $g \in K[x_1, \ldots, x_n]$:
  $\psi(g) = \psi(1 \cdot g) = g \cdot \psi(1) = g$.

The first two properties make ψ a homomorphism of $K[x_1, \ldots, x_n]$-modules. The idea is to write

$$f = \sum_{i=1}^{m} g_i h_i = \sum_{i=1}^{m} g_i \Re(h_i) + i \cdot \sum_{i=1}^{m} g_i \Im(h_i),$$

where the second part vanishes because $f \in K[x_1, \ldots, x_n]$, so $f = \sum_{i=1}^{m} g_i \Re(h_i) \in I$.
Now we generalize the argument. Notice what we did: We extended the $\mathbb{R}$-vector space homomorphism $\Re : \mathbb{C} \to \mathbb{R}, a + ib \mapsto a$ to a homomorphism of $\mathbb{R}[x_1, \ldots, x_n]$-modules. The properties from $\Re$ that we used were:

- $\phi(a + b) = \phi(a) + \phi(b)\ \forall\ a, b \in \bar{K}$.
- $\phi(a \cdot b) = a \cdot \phi(b)\ \forall\ a \in K, b \in \bar{K}$.
- $\phi|_K = \mathrm{id}$.

In other words, we want a homomorphism of K-vector spaces $\phi : \bar{K} \to K$, which satisfies $\phi|_K = \mathrm{id}$. Notice that $\Re$ is nothing but a projection onto the first component when viewing $\mathbb{C}$ as an $\mathbb{R}$-vector space with basis $\{1, i\}$. In the same way, we get our mapping ϕ in the general case:
Since $\{1\}$ is a K-basis of K (viewing K as a vector space over itself), we can extend it to a K-basis B of $\bar{K}$. Since it is enough to define a K-linear map on a K-basis, we get a K-linear map

$$\phi : \bar{K} \to K,\ b \mapsto \begin{cases} 1 & \text{if } b = 1 \\ 0 & \text{otherwise} \end{cases}$$

for $b \in B$. It is clear that this ϕ has the properties we want, so we can extend it to a homomorphism of $K[x_1, \ldots, x_n]$-modules $\psi : \bar{K}[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]$ with $\psi|_{K[x_1,\ldots,x_n]} = \mathrm{id}$.

Similar to the special case, we argue:

$$f = \psi(f) = \sum_{i=1}^{m} \psi(g_i h_i) = \sum_{i=1}^{m} g_i \psi(h_i) \in I.$$

Noetherian and Artinian Rings

Remark 5. (a) There are modules that have no basis, for example, the $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$. This is because $2 \cdot 1 = 0$, so the set $\{1\} \subset \mathbb{Z}/2\mathbb{Z}$ is linearly dependent.

(b) For a field K with algebraic closure $\bar{K}$, let $a \in \bar{K}$, $f \in K[x]$ minimal polynomial of a. Furthermore, let $g \in K[x_1, \ldots, x_n]$ with $g(a, \ldots, a) = 0$.
This does not imply that $f|g$, as the following example shows: For $K = \mathbb{Q}$, $n = 2$, $a = \sqrt{2}$, it is $f = x^2 - 2$, which does not divide $g = x - y$.

(c) We know that:

$$\text{Field} \Rightarrow \text{Euclidean Ring} \Rightarrow \text{PID} \Rightarrow \text{UFD (Factorial Ring)} \Rightarrow \text{ID}$$

It additionally holds that:

- Field $\Rightarrow$ Artinian.
- Artinian $\Rightarrow$ Noetherian.
- Artinian $\Rightarrow$ Jacobson.
- ID $\Rightarrow$ reduced ring.

(d) For a ring R and an ideal $I \subset R$, the quotient ring R/I is reduced if and only if I is a radical ideal.

(e) Any abelian group G (with addition as its operation) can be made a $\mathbb{Z}$-module by defining multiplication as

$$\forall\, z \in \mathbb{Z}, g \in G : z \cdot g \coloneqq \underbrace{g + \cdots + g}_{z \text{ times}}.$$

On the other hand, given a $\mathbb{Z}$-module M, we can simply extract its abelian group. Because of the module axioms, these two operations are inverses to one and another. This means that abelian groups and $\mathbb{Z}$-modules are in 1:1-relation.

(f) A ring R is called *graded*, if it has a direct sum decomposition

$$R = R_0 \oplus R_1 \oplus R_2 \oplus \cdots = \bigoplus_{d \in \mathbb{N}} R_d$$

as an abelian group, such that

$$\forall\, a \in R_i, b \in R_j : ab \in R_{i+j}.$$

An element of R_d is called *homogeneous* of degree d.
Notice that R_0 is a ring and the R_i are R_0-modules. A standard example is $R = K[x_1, \ldots, x_n]$, where R_d is the space of homogeneous polynomials of degree d (i.e. all monomials have degree d).
So for instance in $\mathbb{R}[x, y]$: $2xy, -5x^2 + 6xy \in R_2$.

(g) Another example of a graded ring: Let K be a field and $G \subset GL_n(K)$ be a subgroup of the general linear group. Define a group action of G on K^n as follows:
For $\sigma \in G$, $f \in K[x_1, \dots, x_n]$, $v \in K^n$ set

$$(\sigma.f)(v) \coloneqq f(\sigma^{-1}v).$$

Then the *ring of invariants* is defined as

$$K[x_1, \dots, x_n]^G \coloneqq \{f \in K[x_1, \dots, x_n] : \forall\, \sigma \in G : \sigma(f) = f\}.$$

(h) The image of an affine variety under a morphism of varieties is not necessarily an affine variety. Consider e.g. the projection onto the first component $V(xy-1) \to K^1$. The image is $K^1 \setminus \{0\}$, which is not an affine variety.

Lemma 6. Let X be a set and $f : X \to X$ a function. If there is $n \in \mathbb{N}_{>0}$ such that f^n is bijective, then f is bijective.

Proof. The inverse of f is f^{n-1}:

$$f \circ f^{n-1} = f^n = f^{n-1} \circ f. \qquad \square$$

2.1 A non-Noetherian Ring

Let K be a field and $R = K[x, y]$ be the polynomial ring in two variables. Define the K-subalgebra of R

$$S \coloneqq K + Rx = K[x, xy, xy^2, xy^3, \dots].$$

Show that S is not Noetherian.
Since $K[x, y]$ is Noetherian, this shows that a subring of a Noetherian ring need not be Noetherian.

For $n \in \mathbb{N}$, set $I_n \coloneqq (x, xy, \dots, xy^n) \subset S$. Then $I_n \subsetneq I_{n+1}\ \forall\ n \in \mathbb{N}$, since $xy^{n+1} \notin I_n$. Thus the I_n form an infinite, strictly ascending chain of ideals, so S is not Noetherian.

2.2 An Artinian Module that is not Noetherian

Let p be a prime number and define the $\mathbb{Z}$-module

$$\mathbb{Z}[p^{-1}] \coloneqq \left\{ \frac{a}{p^n} \in \mathbb{Q} : a \in \mathbb{Z}, n \in \mathbb{N} \right\}$$

and $M \coloneqq \mathbb{Z}[p^{-1}]/\mathbb{Z}$.
Prove that M is Artinian but not Noetherian as a $\mathbb{Z}$-module.

For clear notation, we write $\frac{a}{b}$ for the equivalence class $\frac{a}{b} + \mathbb{Z} \in M$ and choose the unique representative in $[0, 1)$ with $\gcd(a, b) = 1$.

Let $0 \neq \frac{a}{p^n} \in M$ be an element. The submodule it generates is $(\frac{a}{p^n}) = \left\{k \cdot \frac{a}{p^n} | k \in \mathbb{Z}\right\}$ and it is clear that any element in that submodule will have a denominator smaller or equal to p^n. Since $\gcd(a, p^n) = 1$, Bezout's identity yields

$$\exists\, x, y \in \mathbb{Z} : xa + yp^n = 1,$$

so $bxa + byp^n = b$ and thus $(bx) \cdot \frac{a}{p^n} = \frac{b}{p^n}$ for any $b \in \mathbb{Z}$. Since this holds for any $a \in \mathbb{Z} \setminus \{0\}$, it shows that

$$\left(\frac{1}{p^n}\right) = \left(\frac{a}{p^n}\right) = \left\{\frac{b}{p^m}\middle| b \in \mathbb{Z}, m \leq n\right\}.$$

Hence, for a submodule $N \subset M$ there are two cases: If $\max\left\{n \in \mathbb{N} : \frac{a}{p^n} \in N\right\} < \infty$, then $N = (\frac{1}{p^n})$ and otherwise $N = M$. In other words, the proper submodules of M are precisely of the form $M_n = (\frac{1}{p^n})$ for $n \in \mathbb{N}$.
Given a strictly decending chain $N_1 \supsetneq N_2 \supsetneq \ldots$ of submodules of M, we know that $N_2 = (\frac{1}{p^n})$ for some $n \in \mathbb{N}$. But since that submodule only contains n different, proper submodules, the chain must terminate. This shows that M is Artinian.
Of course, M is not Noetherian, as the infinite, strictly ascending chain $M_0 \subsetneq M_1 \subsetneq \ldots$ shows.
Alternatively, notice that since $\mathbb{Z}$ is Noetherian, M is Noetherian if and only if $\mathbb{Z}[p^{-1}]$ is Noetherian (proposition 2.4). Moreover, $\mathbb{Z}[p^{-1}]$ is Noetherian as a $\mathbb{Z}$-module if and only if it is finitely generated over $\mathbb{Z}$ (Theorem 2.10), which is not the case.

2.3 Noetherian Graded Rings

For R a graded ring, we define the *irrelevant ideal* as

$$I \coloneqq \bigoplus_{d \in \mathbb{N}_{>0}} R_d.$$

Prove that the following are equivalent:

(a) R is Noetherian.

(b) R_0 is Noetherian and I is finitely generated.

(c) R_0 is Noetherian and R is finitely generated as an R_0-algebra.

(a) "(a) $\Rightarrow$ (b)": The ring homomorphism $\phi : R \to R_0$, which projecs an element of R to its R_0-component, is surjective and has kernel I, so by the isomorphism theorem $R_0 \cong R/I$. Since R is Noetherian, so is R/I (proposition 2.4). By theorem 2.9, I is finitely generated.

(b) "(b) $\Rightarrow$ (c)": Write $I = (f_1, \ldots, f_n)$ with $f_i \in I$. By the direct sum property, we can write $f_i = \sum_{j=1}^{m_j} f_{i,j}$ with $f_{i,j} \in R_j \subset I$. So $I = (f_{i,j} | 1 \leq i \leq n, 1 \leq j \leq m_j)$.
Claim:

$$R = R_0[f_{i,j} | 1 \leq i \leq n, 1 \leq j \leq m_j] =: S.$$

By the direct sum property, it is enough to show that any $g \in R$ homogeneous of degree d is also in S. We use induction on d.
For $d = 0$, $g \in R_0 \subset S$.
Let $d > 0$. Then $g \in I$, so we can write

$$g = \sum_{1 \leq i \leq n, 1 \leq j \leq m_j} h_{i,j} f_{i,j}$$

with $h_{i,j} \in R$. Since g is homogeneous of degree d and the sum is direct, it follows

$$g = \sum_{1 \leq i \leq n, 1 \leq j \leq m_j} (h_{i,j})_{d-j} f_{i,j},$$

where $(h)_i$ denotes the i-th component in the direct sum decomposition of h. By the inductive hypotheses, $(h_{i,j})_{d-j} \in S$, so $g \in S$.

(c) "(c) $\Rightarrow$ (a)": This follows directly from corollary 2.12.

2.4 True or False: Noetherian/Artinian

Are the following statements true or false? Give a proof or a counterexample.

(a) Every Artinian module is finitely generated.

(b) If R is a ring such that $R[x]$ is Noetherian, then R is also Noetherian.

(c) If a ring R is Artinian, then so is $R[x]$.

(d) Every finitely generated module over a ring R is Noetherian.

(e) If R is a ring such that every finitely generated R-module is Noetherian, then R is a Noetherian ring.

(a) False. Choose M as in 2.2. If M was finitely generated, it would be Noetherian by theorem 2.10, since $\mathbb{Z}$ is Noetherian.

(b) True, since $R \cong R[x]/(x)$ and $R[x]$ being Noetherian implies $R[x]/(x)$ being Noetherian by proposition 2.4.

(c) False, as any field K is Artinian, but $K[x]$ is not: $(x) \supsetneq (x^2) \supsetneq (x^3) \supsetneq \ldots$.

(d) False, because any non-Noetherian ring R is finitely generated over itself $R = (1)$.

(e) True. In particular, R is finitely generated as a module over itself.

2.5 Endomorphisms of Artinean and Noetherian modules

Let R be a ring, M an R-module and $f : M \to M$ a homomorphism of R-modules.

(a) If M is Artinian and f is injective, then f is an isomorphism.

(b) If M is Noetherian and f is surjective, then f is an isomorphism.

(c) Give examples, which show that the assumptions "Artinian" and "Noetherian" in (a) and (b) cannot be omitted.

(a) Consider the descending chain of submodules

$$\mathrm{im}(f) \supset \mathrm{im}(f^2) \supset \mathrm{im}(f^3) \supset \dots.$$

Because M is Artinian, there is $n \in \mathbb{N}_{>0}$, such that $\mathrm{im}(f^n) = \mathrm{im}(f^i)$ for all $i \geq n$. Consider the homomorphism $g \coloneqq f^n, M \to M$, which is injective as a composition of injective functions.
Suppose g was not surjective. Then there is $x \notin \mathrm{im}(g)$ and $g(x) \in \mathrm{im}(g)$, but $g(x) \notin \mathrm{im}(g^2)$, since otherwise there is $y \in M$ with $g(g(y)) = g(x)$ so by injectivity $g(y) = x$. Contradiction, because $\mathrm{im}(g) = \mathrm{im}(g^2)$.
Therefore, g is bijective and 6 yields the claim.

(b) We argue similarly to (a). Consider the ascending chain of submodules

$$\ker(f) \subset \ker(f^2) \subset \ker(f^3) \subset \dots.$$

Because M is Noetherian, there is $n \in \mathbb{N}_{>0}$, such that $\ker(f^n) = \ker(f^i)$ for all $i \geq n$. Consider the homomorphism $g \coloneqq f^n, M \to M$, which is surjective as a composition of surjective functions.
Suppose g was not injective, i.e. there is $0 \neq x \in \ker(g)$. By surjectivity, there is $y \in M$ with $g(y) = x$, so $y \in \ker(g^2)$, but $y \notin \ker(g)$. Contradiction, because $\ker(g) = \ker(g^2)$.
Therefore, g is bijective and 6 yields the claim.

(c) Let R be a nonzero ring and $M = R[x_1, x_2, \dots]$ be the polynomial ring in infinitely many variables. The R-algebra homomorphism

$$M \to M,\ x_1 \mapsto x_2, x_2 \mapsto x_3, x_3 \mapsto x_4,\ \dots$$

is injective, but not surjective and amounts to a R-module homomorphism $M \to M$. Similarly, the R-algebra homomorphism

$$M \to M,\ x_1 \mapsto 0, x_2 \mapsto x_1, x_3 \mapsto x_2,\ \dots$$

is surjective, but not injective and gives rise to a R-module homomorphism $M \to M$.

2.6 More Rings

Find a ring that is...

(a) Artinian, but not a field.

(b) Noetherian, but not Artinian.

(c) Factorial, but not Noetherian.

(d) reduced, but not an integral domain.

(a) Any finite ring that is not a field will work, e.g. $\mathbb{Z}/4\mathbb{Z}$.

(b) $\mathbb{Z}$.

(c) The polynomial ring over a field with infinitely many variables $K[x_1, x_2, \dots]$.

(d) $\mathbb{Z}/6\mathbb{Z}$.

2.7 Idealization

For K a field and V a K-vector space, we define the *idealization* $R = K(+)V$ to be the ring with the set $R = K \times V$, addition $(a, v) + (b, w) = (a + b, v + w)$, multiplication $(a, v) \cdot (b, w) = (ab, aw + bv)$, zero-element $(0, 0)$ and one-element $(1, 0)$. We want to show that this ring is Jacobson, but not Noetherian, if $\dim_K(V) = \infty$. Prove the following:

(a) Let $U \subset V$ be a subspace. Then $\{0\} \times U$ is an ideal of R.

(b) If $\dim_K(V) = \infty$, then R is not Noetherian. (The reverse direction is also true.)

(c) $\{0\} \times V$ is a maximal ideal.

(d) $\{0\} \times V = \sqrt{(0)_R}$.

(e) R is Jacobson.

(a) Follows directly from the definition.

(b) If $\dim_K(V) = \infty$, there exists an infinite, strictly ascending chain of subvector spaces of V

$$U_1 \subsetneq U_2 \subsetneq \dots.$$

With (a), we get an infinite, strictly ascending chain of ideals of R:

$$\{0\} \times U_1 \subsetneq \{0\} \times U_2 \subsetneq \dots.$$

(c) Consider the ring homomorphism $\phi : R \to K, (k, v) \to k$. It is surjective and has kernel $\ker(\phi) = \{0\} \times V$. The isomorphism theorem yields $R/(\{0\} \times V) \cong K$, so

$\{0\} \times V$ is a maximal ideal.
Alternatively, one can also show this in a direct manner: Let $I \supsetneq \{0\} \times V$ be an ideal. Then there is $(c, v) \in I \setminus (\{0\} \times V)$, so $c \neq 0$. Then $(c, 0) = (c, v) - (0, v) \in I$ and thus $1 = (1, 0) = (c^{-1}, 0) \cdot (c, 0) \in I$.

(d) Let $(a, v) \in \{0\} \times V$, i.e. $a = 0$. Then $(a, v) \cdot (a, v) = 0$, so $\{0\} \times V \subset \sqrt{(0)_R}$. Since $(1, 0) \notin \sqrt{(0)_R}$, $\sqrt{(0)_R}$ is a proper ideal, so (c) implies $\{0\} \times V = \sqrt{(0)_R}$. Alternatively, one can deduce $\{0\} \times V \supset \sqrt{(0)_R}$ from the fact that every prime ideal contains the nilradical.

(e) Since $\sqrt{(0)_R} = \bigcap_{P \in \mathrm{Spec}(R)} P$, it follows that $\mathrm{Spec}(R) = \{\{0\} \times V\}$ As a local ring with its only maximal ideal also being the only prime ideal, R is Jacobson:

$$\sqrt{I} = \bigcap_{P \in \mathrm{Spec}(R), I \subset P} P = \bigcap_{m \in \mathrm{Spec}_{\max}(R), I \subset m} m.$$

The Zariski Topology

Remark 7. (a) The closure $\bar{S}$ of a set $S \subset K^n$ with respect to the Zariski topology is by definition the smallest closed subset $T \subset K^n$ with $S \subset T$. So $T = V(I)$ with $I \subset K[x_1, \ldots, x_n]$ a radical ideal.
We have the explict formula $\bar{S} = V(I(S))$, which is proven in 8.

(b) For $X, Y \subset T$ subsets of a topological space T, it holds that

$$\overline{X \cap Y} \subset \overline{X} \cap \overline{Y}.$$

(c) If a topological space X is Noetherian, then any subset equipped with the subset topology is Noetherian.

(d) The image of an affine variety under a morphism of varieties is not necessarily an affine variety. For example, consider

$$f : V_{K^2}(xy - 1) \to K^1, \ (p, q) \mapsto p$$

for K a field. Then $\mathrm{im}(f) = K^1 \setminus \{0\}$, which is not an affine variety if K is infinite.

Lemma 8. Let K be a field and $X \subset K^n$ a set of points. For

$$M \coloneqq \{Y \subset K^n : Y \text{ is an affine variety}, X \subset Y\}$$

it holds $V(I(X)) = \bigcap_{Y \in M} Y$ and the right side is by definition the closure $\overline{X}$ of X with respect to the Zariski topology.

Proof. Since $V(I(X))$ is an affine variety containing X, it is clear that $V(I(X)) \supset \bigcap_{Y \in M} Y$. For the other inclusion, let $Y = V(S) \in M$. Since $X \subset Y$, it follows $S \subset I(X)$ and thus $V(I(X)) \subset V(S) = Y$. □

Lemma 9. Let $X \subset K^n$ be a set and K^n equipped with the Zariski topology. Then $I(X) = I(\overline{X})$.

Proof. It is clear that $I(X) \supset I(\overline{X})$. On the other hand, $I(\overline{X}) = I(V(I(X))) \supset I(X)$.
Alternatively, let $f \in I(X)$ and notice that the set $V(f)$ is closed and contains X, so $\overline{X} \subset V(f)$, implying $I(\overline{X}) \supset I(V(f))$ and thus $f \in I(\overline{X})$. □

3.1 Some properties of affine varieties

Let K be an algebraically closed field and $X, Y \subset K^n$.

(a) Prove that $V(I(X) + I(Y)) = \overline{X} \cap \overline{Y}$, where $I + J \coloneqq \{i + j | i \in I, j \in J\}$ and $\bar{X}$ is the closure of X in K^n.

(b) Give an example where $V(I(X) + I(Y)) \neq \overline{X \cap Y}$.

(c) Prove that $\overline{X} \cap \overline{Y} = \emptyset$, if and only if there is an $f \in K[x_1, \ldots, x_n]$, such that $f(x) = 0$ for all $x \in X$ and $f(y) = 1$ for all $y \in Y$.

(a) Recall that for any ring R and ideals $I, J \subset R$ it holds that $I + J = (I \cup J)_R$. Since a vanishing set is determined by its generators (4), we get:

$$V(I(X) + I(Y)) = V(I(X) \cup I(Y)) = V(I(X)) \cap V(I(Y)) = \overline{X} \cap \overline{Y}.$$

(b) We give two examples:

- Choose $K = \mathbb{C}, n = 1$ and consider $X = \mathbb{N}$, $Y = \mathbb{Z} \setminus \mathbb{N}$. Then $\overline{X} = \overline{Y} = \mathbb{C}$, so $V(I(X) + I(Y)) = \overline{X} \cap \overline{Y} = \mathbb{C}$, but $\overline{X \cap Y} = \emptyset$.
- Choose $K = \mathbb{C}$, $n = 2$ and consider

$$X = \{(x, y) \in \mathbb{C}^2 | x = 0, y \neq 0\} \Rightarrow \overline{X} = \{(x, y) \in \mathbb{C}^2 | x = 0\}$$
$$Y = \{(x, y) \in \mathbb{C}^2 | x \neq 0, y = 0\} \Rightarrow \overline{Y} = \{(x, y) \in \mathbb{C}^2 | y = 0\}.$$

Thus $V(I(X) + I(Y)) = \overline{X} \cap \overline{Y} = \{(0, 0)\}$, but $\overline{X \cap Y} = \emptyset$.

(c) "$\Rightarrow$": By Hilbert's Nullstellensatz (Corollary 1.8)

$$\emptyset = V(I(X) + I(Y)) = \overline{X} \cap \overline{Y} \iff I(X) + I(Y) = (1).$$

Thus there is $f \in I(X)$, $g \in I(Y)$ with $f + g = 1$, so $f(x) = 0$ for all $x \in X$ and $f(y) = 1$ for all $y \in Y$.
"$\Leftarrow$": Since $X \subset V(f)$ and $V(f)$ is closed by definition, it follows $\overline{X} \subset V(f)$. Similarly, $Y \subset V(f - 1)$ implies $\overline{Y} \subset V(f - 1)$. Therefore, the claim follows from $V(f) \cap V(f - 1) = \emptyset$.
An alternative proof goes as follows: Assume there exists $x \in \overline{X} \cap \overline{Y}$. Since $f \in I(X)$, $f(x) = 0$ and because $f - 1 \in I(Y)$, $f(x) - 1 = 0$. Contradiction.

3.2 Dominant morphisms of affine varieties

Let X be an affine variety. An *automorphism* of X is an isomorphism $X \to X$ of affine varieties.

(a) Prove that automorphisms of $\mathbb{C}$ (with the Zariski topology) are precisely the maps $x \mapsto ax + b$ with $a \neq 0$, $b \in \mathbb{C}$.

(b) Give an example of an automorphism of $\mathbb{C}^2$ (with the Zariski topology), which is not of the form $(x, y) \mapsto (ax+by+c, dx+ey+f)$ for some $a, b, c, d, e, f, \in \mathbb{C}$.

(a) $x \mapsto ax + b$ with $a \neq 0$ is an automorphism with inverse $x \mapsto \frac{1}{a}x - \frac{b}{a}$. Now let $f \in \mathbb{C}[x]$ be an automorphism, so there is $g \in \mathbb{C}[x]$ with $g \circ f = \mathrm{id}$. Clearly, $f, g \in \mathbb{C}[x]$ are not constant. Thus it holds that $\deg(g \circ f) = \deg(g) \cdot \deg(f)$.

$$1 = \deg(g \circ f) = \deg(g) \cdot \deg(f) \Rightarrow \deg(f) = 1.$$

(b) For instance

$$\phi : (x, y) \mapsto (x, y - x^2), \ \phi^{-1}(x, y) \mapsto (x, y + x^2).$$

3.3 Graphs as Affine Varieties

Let K be a field, $X \subset K^n$, $Y \subset K^m$ affine varieties and $f : X \to Y$ a morphism of varieties. The *graph* of f is defined as

$$\Gamma_f \coloneqq \{(x, y) \in X \times Y : f(x) = y\} \subset K^{n+m}.$$

(a) Prove that $\Gamma_f \subset K^{n+m}$ is an affine variety.

(b) Prove that $\alpha : X \to \Gamma_f, x \mapsto (x, f(x))$ is an isomorphism of varieties.

(a) Denote the components of f by f_i. It holds

$$\Gamma_f = V(f_1(x_1, \ldots, x_n) - y_1, \ldots, f_m(x_1, \ldots, x_n) - y_m).$$

(b) The inverse is given by $\Gamma_f \to X, (x, y) \mapsto x$.

3.4 Dominant and injective morphisms

For K a field and X, Y affine varieties over K, let $f : X \to Y$ be a morphism and $\phi : K[Y] \to K[X]$ the homomorphism induced by f.
The map f is called *dominant* if $f(X)$ is dense in Y, i.e. $\overline{f(X)} = Y$.

(a) Prove that f is dominant if and only if ϕ is injective.

(b) Prove that f is injective if ϕ is surjective.

(c) Give an example in which f is dominant but not surjective.

(d) Give an example in which f is injective but ϕ is not surjective.

Recall that ϕ is defined by $\phi(g) = g \circ f$, i.e. it simply describes function concatenation.

(a) "$\Rightarrow$": Let $p \in \ker(\phi)$. Then $p \circ f = 0$, thus $p|_{f(X)} = 0$, i.e. $p \in I(f(X))$. By 9 and the assumption, this implies $p \in I(Y)$.
"$\Leftarrow$": We need to prove that $V(I(f(X))) = Y = V(I(Y))$. It suffices to show that $I(f(X)) = I(Y)$. Since $f(X) \subset Y$, we get $I(Y) \subset I(f(X))$.
On the other hand, let $p \in I(f(X))$ with equivalence class $\overline{p} \coloneqq p + I(Y)$. Then $\overline{p}|_{f(X)} = 0$, so $\phi(\overline{p}) = \overline{p} \circ f = 0$ so by injectivity $\overline{p} = 0$, so $p \in I(Y)$.
Alternative proof: By contraposition, suppose f is not dominant and let $y \in Y \setminus \overline{f(X)}$. Since $\overline{f(X)}$ is an affine variety, there is $g \in I(f(X))$, such that $g(y) \neq 0$. Then $\phi(g) = g \circ f = 0$, despite $g \neq 0$ in $K[Y]$, so ϕ is not injective.

(b) Let $K[X] = K[x_1, \ldots, x_n]/I(X)$. By surjectivity, there exist $g_i \in K[Y]$ with $\phi(g_i) = x_i + I(X)$. Let $\xi = (\xi_1, \ldots, \xi_n)$, $\eta = (\eta_1, \ldots, \eta_n) \in X$ with $f(\xi) = f(\eta)$. Then

$$\xi_i = \phi(g_i)(\xi) = g_i(f(\xi)) = g_i(f(\eta)) = \phi(g_i)(\eta) = \eta_i$$

for all $i \in \{1, \ldots, n\}$. Thus f is injective.
Alternative proof: By contraposition, suppose f is not injective, so there are $a, b \in$

X, $a \neq b$ with $f(a) = f(b)$. Choose $i \in \mathbb{N}$, such that $a_i \neq b_i$. Then any $g \in \phi(K[Y])$ satisfies $g(a) = g(b)$, so $x_i + I(X) \notin \phi(K[Y])$ and ϕ is not surjective.

(c) We give two examples:

- Let $X = \mathbb{R} \subset \mathbb{R}^1$, $Y = \mathbb{R}$. Then a morphism $X \to Y$ is just a polynomial in $\mathbb{R}[x]$. $f = x^2$ satisfies $f(X) = \mathbb{R}_{\geq 0}$ and $\overline{f(X)} = \mathbb{R}$.
- Take $X = V(xy - 1) \subset \mathbb{C}^2$ and $Y = \mathbb{C}$ and $f : X \to Y, (x, y) \mapsto x$. Then $f(X) = \mathbb{C} \setminus \{0\}$ and $\overline{f(X)} = \mathbb{C}$.

(d) Again, we give two examples:

- Let $X = \mathbb{R} \subset \mathbb{R}^1$, $Y = \mathbb{R}$ and consider $f = x^3$. Clearly, $x \notin \phi(K[Y])$.
- Choose the same X, Y, f as in the second example of (c). By (a) and (c), ϕ is injective. If it were surjective, then it would be an isomorphism of rings, but

$$K[X] = K[x, y]/(xy - 1) \cong K[x, x^{-1}] \ncong K[x] \cong K[Y],$$

where we applied the homomorphism theorem to the K-algebra isomorphism

$$\chi : K[x, y] \to K[x, x^{-1}], x \mapsto x, y \mapsto x^{-1}.$$

Therefore, f can not be surjective.

3.5 A Basis of the Zariski Topology

Let K be an algebraically closed field. For $f \in K[x_1, \ldots, x_n]$ we define

$$D(f) \coloneqq \{x \in K^n : f(x) \neq 0\}.$$

The set $D(f)$ is called the *distinguished* (or *basic*) open set of K^n associated with f.

(a) Prove that $\{D(f) : f \in K[x_1, \ldots, x_n]\}$ is a basis of the Zariski topology on K^n, i.e. every open set can be written as a union of some of the $D(f)$.

(b) For $f \in K[x_1, \ldots, x_n]$ we define the affine variety

$$X_f \coloneqq \big\{(x_1, \ldots, x_n) \in K^{n+1} : f(x_1, \ldots, x_n) \cdot x_{n+1} = 1\big\}.$$

Prove that the map

$$\pi : X_f \to D(f),\ (x_1, \ldots, x_{n+1}) \mapsto (x_1, \ldots, x_n)$$

is well-defined and bijective.

(c) Prove that π is a homeomorphism with respect to the Zariski topology.

(a) Follows from the definition.

(b) The inverse is given by

$$\pi^{-1} : D(f) \to X_f,\ (x_1, \ldots, x_n) \mapsto \big(x_1, \ldots, x_n, f(x_1, \ldots, x_n)^{-1}\big).$$

(c) π is a morphism of varieties, so it is continuous with respect to the Zariski topology: For $U \subset K^n$, it holds

$$\pi^{-1}(U \cap D(f)) = \pi^{-1}(U) \cap \pi^{-1}(D(f)) = \pi^{-1}(U) \cap X_f,$$

which is closed in X_f.
It is left to show that π^{-1} is continuous. Since the $D(g)$ form a basis of the topology, it is enough to check that their preimages are open. This holds:

$$\begin{aligned}\pi(D(g) \cap X_f) &= \big\{x \in K^n : f(x) \neq 0, g\big(x_1, \ldots, x_n, f(x)^{-1}\big) \neq 0\big\} \\ &= \big\{x \in K^n : f(x) \neq 0, f(x)^{\deg(g)} g\big(x_1, \ldots, x_n, f(x)^{-1}\big) \neq 0\big\} \\ &= D(f) \cap D(h),\end{aligned}$$

where $h \coloneqq f(x_1, \ldots, x_n)^{\deg(g)} g\big(x_1, \ldots, x_n, f(x_1, \ldots, x_n)^{-1}\big) \in K[x_1, \ldots, x_n]$.

3.6 Some morphisms of Varieties

Let $X = V(xy - 1) \subset \mathbb{C}^2$. Consider the mappings

$$\begin{aligned}f_1 &: X \to X,\ (x, y) \mapsto (x^2, y^2) \\ f_2 &: X \to X,\ (x, y) \mapsto (x^{-1}, y^{-1}) \\ f_3 &: X \to X,\ (x, y) \mapsto (\bar{x}, \bar{y})\end{aligned}$$

Are the f_i morphisms or even isomorphisms of varieties?

(a) By definition f_1 is a morphism. But it cannot be an isomorphism, since it is not injective:

$$f_1(1, 1) = 1 = f_1(-1, -1).$$

(b) Any element $(x, y) \in X$ satisfies $xy - 1 = 0$, so $1 = xy$. Therefore

$$f_2 : X \to X,\ (x, y) \mapsto (y, x)$$

and f_2 is a morphism and even an isomorphism, because $f_2 \circ f_2 = \mathrm{id}_X$.

(c) We claim that f_3 is not a morphism. Suppose the opposite, so there exists $g \in \mathbb{C}[x, y]$ with $g(x, y) = \bar{x}\ \forall (x, y) \in X$. As already noted any element $(x, y) \in X$ satisfies $y = x^{-1}$, so $g(x, x^{-1}) = \bar{x}\ \forall x \in \mathbb{C} \setminus \{0\}$. This leads to

$$g(x, x^{-1}) - x = 0\ \forall x \in \mathbb{R} \setminus \{0\}.$$

Let $n \coloneqq \deg_y(g)$ be the degree of g with respect to its y-component. It follows

$$\tilde{g}(x) - x^{n+1} = 0\ \forall x \in \mathbb{R} \setminus \{0\},$$

where $\tilde{g} \in K[x]$ is a polynomial in one variable. This implies $\tilde{g} = x^{n+1}$, so $g = x$. Contradiction.

3.7 A non-morphism on $\mathbb{C}$

Let $X = \mathbb{C}$ and $Y = V(x^2 - y^2) \subset \mathbb{C}^2$. Prove that $X \ncong Y$ (i.e. that there does not exist an isomorphism of varieties between them).

Suppose the opposite, let $f = (f_1, f_2)$ be a surjective morphism from X to Y, $f_1, f_2 \in \mathbb{C}[x]$. Then $f_1^2(x) - f_2^2(x) = 0$ for all $x \in \mathbb{C}$. Thus $f_1(x) = f_2(x)$ or $f_1(x) = -f_2(x)$ for infinitely many $x \in \mathbb{C}$. This implies that $f_1 = f_2$ or $f_1 = -f_2$. In the first case, $(1, -1) \notin \mathrm{im}(f)$, in the second one $(1, 1) \notin \mathrm{im}(f)$. Contradiction.
Alternatively, one can show that the coordinate rings $K[X]$, $K[Y]$ are not isomorphic: $K[X] \cong K[x]$, but $K[Y]$ is not an integral domain, since $((x-y)+I(Y))\cdot((x+y)+I(Y)) = 0 + I(Y)$.

3.8 The Zariski topology on $\mathrm{Spec}(\mathbb{Z})$

Determine the following sets:

(a) $V_{\mathrm{Spec}(\mathbb{Z})}(\{9\})$,

(b) $V_{\mathrm{Spec}(\mathbb{Z})}(\{6, 10\})$,

(c) $I_{\mathbb{Z}}(\{(7), (11)\})$,

(d) $\overline{\{(0)\}}$ (the closure of the zero ideal in $\mathrm{Spec}(\mathbb{Z})$)

(a) $\{(3)\}$

(b) $\{(2)\}$

(c) (77)

(d) Set $X \coloneqq \overline{\{(0)\}}$. Since X is closed, we can write $X = V_{\mathrm{Spec}(\mathbb{Z})}(S)$ for $S \subset \mathbb{Z}$. Since $(0) \in X$, $S \subset (0) = \{0\}$. This implies that $X = \mathrm{Spec}(\mathbb{Z})$.

3.9 $\mathrm{Spec}(R)$ Noetherian implies R Noetherian?

Prove or disprove: If for a ring R, $\mathrm{Spec}(R)$ is Noetherian, then R is a Noetherian ring.

The statement is false. Consider the ring $R \coloneqq K[x_1, x_2, \dots]/(x_1^2, x_2^2, \dots)$. Since the ideal $I \coloneqq (\overline{x_1}, \overline{x_2}, \dots)$ is not finitely generated, R is not Noetherian. However, I is the unique maximal ideal in R, because every prime ideal has to contain the nilradical elements $\overline{x_i} \in I$ and $R/I \cong K$ is a field. Thus $\mathrm{Spec}(R) = \{I\}$ is a singleton, so in particular Noetherian.

3.10 Jacobson property and the Zariski topology

Prove that a ring R is Jacobson, if and only if for all $Y \subset \mathrm{Spec}(R)$ Zariski-closed, $\mathrm{Spec}_{\max}(R) \cap Y$ is dense in Y.

A ring R is Jacobson if and only if any radical ideal I can be written as

$$\mathcal{I}_R\big(\mathrm{Spec}_{\max}(R) \cap \mathcal{V}_{\mathrm{Spec}(R)}(I)\big) = I.$$

By proposition 3.6, this is equivalent to

$$\overline{\mathrm{Spec}_{\max}(R) \cap \mathcal{V}_{\mathrm{Spec}(R)}(I)} = \mathcal{V}_{\mathrm{Spec}(R)}\big(\mathcal{I}_R\big(\mathrm{Spec}_{\max}(R) \cap \mathcal{V}_{\mathrm{Spec}(R)}(I)\big)\big) = \mathcal{V}_{\mathrm{Spec}(R)}(I).$$

By the same proposition, $\mathcal{V}_{\mathrm{Spec}(R)}$ defines a bijection between the radical ideals of R and the Zariski-closed subsets of $\mathrm{Spec}(R)$, which proves the claim.

3.11 Irreducible components of an affine variety

Determine the decomposition into irreducible components of the affine variety

$$V(x^2 - y^2, z^2 - 1) \cup V(x - y^2, z) \subset \mathbb{C}^3.$$

The affine variety can be rewritten as

$$V(x - y, z - 1) \cup V(x - y, z + 1) \cup V(x + y, z - 1) \cup V(x + y, z + 1) \cup V(x - y^2, z)$$

and we claim that this the desired decomposition into irreducible components. By theorem 3.11, such a decomposition into closed, irreducible subsets with $Z_i \not\subset Z_j$ for $i \neq j$ is unique, so by theorem 3.10, we have to show that the corresponding ideals are prime. The ideal $(x - y, z - 1) \subset \mathbb{C}[x, y, z]$ is prime, because the $\mathbb{C}$-algebra homomorphism

$$\mathbb{C}[x, y, z] \to \mathbb{C}[x],\ x \mapsto x, y \mapsto x, z \mapsto 1$$

is surjective with kernel $(x - y, z - 1)$ and thus induces an isomorphism $\mathbb{C}[x, y, z]/(x - y, z - 1) \cong \mathbb{C}[x]$.
Alternatively, since any morphism of varieties is continuous with respect to the Zariski topology, every isomorphism of varieties is a homeomorphism. Thus we can conclude that $V(x - y, z - 1)$ is irreducible, because an isomorphism of varieties is given by

$$\mathbb{C}^1 \to V(x - y, z - 1),\ x \mapsto (x, x, 1)$$

and $\mathbb{C}^1$ is irreducible. The irreducibility of the other affine varieties follows analogously.

3.12 A homeomorphism

Let K be an algebraically closed field and $X \subset K^n$ an affine variety. Theorem 1.23 establishes a bijection $\phi : X \to \mathrm{Spec}_{\max}(K[X])$. Equip X with the Zariski topology and $\mathrm{Spec}_{\max}(K[X])$ with the subspace topology of the Zariski topology on $\mathrm{Spec}(K[X])$. Prove that ϕ is a homeomorphism.

Proof. Recall that

$$f \in I(\{x\})/I(X) \iff f(x) = 0$$

and thus

$$S \subset I(\{x\})/I(X) \iff x \in V_{K^n}(S). \qquad (*)$$

It is to show that ϕ and ϕ^{-1} are continuous.
To show that ϕ is continuous, we take $U = \mathcal{V}_{\mathrm{Spec}(K[X])}(S) \cap \mathrm{Spec}_{\max}(K[X])$ closed and see that its preimage

$$\begin{aligned}\phi^{-1}(U) &= \big\{x \in X : I(\{x\})/I(X) \in \mathcal{V}_{\mathrm{Spec}(K[X])}(S)\big\} \\ &= \{x \in X : S \subset I(\{x\})/I(X)\} \\ &\overset{(*)}{=} V_{K^n}(S),\end{aligned}$$

is closed as well.
To show that ϕ^{-1} is continuous, let $Y = V_{K^n}(S)$ and note that

$$\begin{aligned}\phi(Y) &= \{I(\{x\})/I(X) : x \in V_{K^n}(S)\} \\ &= \mathcal{V}_{\mathrm{Spec}(K[X])}(S) \cap \mathrm{Spec}_{\max}(K[X]),\end{aligned}$$

where the second equation holds due to $(*)$ and because by surjectivity of ϕ every maximal ideal $J \in \mathrm{Spec}_{\max}(K[X])$ is of the form $J = I(\{x\})/I(X)$. □

3.13 Another homeomorphism and irreducible components

(a) Let R be a ring and $I \subset R$ an ideal. Prove that the bijection between $\mathrm{Spec}(R/I)$ and $\mathcal{V}_{\mathrm{Spec}(R)}(I)$ given in lemma 1.22 is a homeomorphism.

(b) Determine the decomposition of $\mathrm{Spec}(\mathbb{Z}[x]/(2x))$ into irreducible components.

(c) Let R be a ring and $I \subset R$ an ideal with $I \subset \sqrt{(0)}$. Prove that $\mathrm{Spec}(R/I)$ and $\mathrm{Spec}(R)$ are homeomorphic.

(a) Since ψ is an inclusion-preserving bijection, it holds for ideals $S, J \subset R$:

$$S \subset J \iff S/I = \psi^{-1}(S) \subset \psi^{-1}(J) = J/I. \qquad (*)$$

The closed sets in $\mathrm{Spec}(R/I)$ are by bijectivity of ψ of the form $\mathcal{V}_{\mathrm{Spec}(R/I)}(S/I)$ with $S \subset R$ ideal and the closed sets of $\mathcal{V}_{\mathrm{Spec}(R)}(I)$ are of the form $\mathcal{V}_{\mathrm{Spec}(R)}(S)$ with $S \subset R$ ideal and $I \subset S$. Now

$$\begin{aligned}\psi^{-1}(\mathcal{V}_{\mathrm{Spec}(R)}(S)) &= \big\{J/I \in \mathrm{Spec}(R/I) : J \in \mathcal{V}_{\mathrm{Spec}(R)}(S)\big\} \\ &= \{J/I \in \mathrm{Spec}(R/I) : S \subset J\} \\ &\overset{(*)}{=} \{J/I \in \mathrm{Spec}(R/I) : S/I \subset J/I\} \\ &= \mathcal{V}_{\mathrm{Spec}(R/I)}(S/I)\end{aligned}$$

shows that ψ is continuous and applying ψ to both sides shows that ψ^{-1} is continuous.

(b) For R a ring, the irreducible components of $\mathrm{Spec}(R)$ correspond to the minimal prime ideals of R.
In this case, $R = \mathbb{Z}[x]/(2x)$ and a prime ideal in R has to contain 2 or x, since $2x = 0$ in R. Thus (2) and (x) are the minimal prime ideals of R and therefore $\mathcal{V}_{\mathrm{Spec}(R)}((2)/(2x))$ and $\mathcal{V}_{\mathrm{Spec}(R)}((x)/(2x))$ are the irreducible components of $\mathrm{Spec}(R)$.

(c) Since every prime ideal contains $\sqrt{(0)}$, $\mathcal{V}_{\mathrm{Spec}(R)}(I) = \mathrm{Spec}(R)$, so the claim follows from (a).

3.14 Properties of Noetherian and irreducible topological spaces

(a) Give an example of a topological space that is Noetherian but not irreducible and one that is irreducible but not Noetherian.

(b) A topological space X is irreducible if and only if every nonempty open set is dense and $X \neq \emptyset$.

(c) Let X be a topological space and $Y \subset X$ an irreducible subspace (with the subspace topology). Y is irreducible if and only if its closure $\overline{Y}$ is irreducible.
In particular, any maximal irreducible subset is closed.
This gives some intuition about theorem 3.11(c).

(a) The topological space of two elements with the discrete topology is Noetherian but not irreducible. On the other hand, an irreducible space, which is not Noetherian, is given as follows: Take an infinite set X and choose some element $x \in X$, the closed sets of the corresponding topological space shall be $\mathcal{P}(X \setminus \{x\}) \cup \{X\}$.

(b) Suppose $X \neq \emptyset$ is not irreducible, i.e. there are two proper closed sets $A, B \subset X$ with $X = A \cup B$. Then $\neg A$ is open and since $\neg A \subset B$, $\neg A$ is not dense in X.
If on the other hand there is a nonempty open set U, which is not dense, then $X = \neg U \cup \overline{U}$ shows that X is not irreducible.

(c) Suppose Y is irreducible. Since $\overline{Y}$ is closed, the closed (with respect to the subspace topology) sets are precisely the closed subsets of $\overline{Y}$. Suppose $\overline{Y} = A \cup B$ with $A, B \subset \overline{Y}$ closed. Then $Y = (A \cap Y) \cup (B \cap Y)$, so $Y = A \cap Y$ or $Y = B \cap Y$, implying $Y \subset A$ or $Y \subset B$. Since A and B are closed and $\overline{Y}$ is the smallest closed set containing Y, we conclude $\overline{Y} = A$ or $\overline{Y} = B$, so $\overline{Y}$ is irreducible.
Now suppose that $\overline{Y}$ is irreducible and write $Y = (A \cap Y) \cup (B \cap Y)$ with $A, B \subset \overline{Y}$ closed. Then $Y \subset A \cup B$ and $A \cup B$ is closed, so $\overline{Y} \subset A \cup B$. Thus $\overline{Y} = (A \cap \overline{Y}) \cup (B \cap \overline{Y})$ and since $\overline{Y}$ is irreducible, it follows $\overline{Y} = A \cap \overline{Y}$ or $\overline{Y} = B \cap \overline{Y}$. In particular, $Y \subset A$ or $Y \subset B$, which shows $Y = A \cap Y$ or $Y = B \cap Y$ and thus Y is irreducible.

3.15 Morphisms in the spectrum

(a) For the inclusion $\phi : \mathbb{Z} \hookrightarrow \mathbb{Z}[x]$, let ϕ^* denote the corresponding map $\operatorname{Spec}(\mathbb{Z}[x]) \to \mathbb{Z}$. Determine $\phi^*\big((2,x)_{\mathbb{Z}[x]}\big)$.

(b) For the projection $\phi : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/3\mathbb{Z}$, let ϕ^* denote the corresponding map $\operatorname{Spec}(\mathbb{Z}/3\mathbb{Z}) \to \operatorname{Spec}(\mathbb{Z})$. Determine $\phi^*\big((0)_{\mathbb{Z}/3\mathbb{Z}}\big)$.

(a) $\phi^*\big((2,x)_{\mathbb{Z}[x]}\big) = \phi^{-1}\big((2,x)_{\mathbb{Z}[x]}\big) = (2,x)_{\mathbb{Z}[x]} \cap \mathbb{Z} = (2)$.

(b) $\phi^*\big((0)_{\mathbb{Z}/3\mathbb{Z}}\big) = \phi^{-1}\big((0)_{\mathbb{Z}/3\mathbb{Z}}\big) = (3)$.

Krull Dimension

Remark 10. (a) Gauss's lemma is useful for showing that some polynomials are irreducible over a field.
For example, $x - y^2 \in \mathbb{C}[x, y]$ is primitive and can be viewed as a polynomial in $\mathbb{C}[y][x]$. As a polynomial of degree one over a field it is irreducible in $\mathbb{C}(y)[x]$, so Gauss's lemma shows that $x - y^2$ is irreducible in $\mathbb{C}[x, y]$.

(b) An ideal, which is generated by irreducible polynomials, in a multivariable polynomial ring over a field K is not necessarily prime. For example, consider $I \coloneqq (x - y^2, x - z^2) \subset K[x, y, z]$.

(c) For a ring R, it holds (with the usual convention $\sup_\emptyset \coloneqq -1$):

$$\dim(R) = \sup_{P \in \operatorname{Spec}(R)} \dim(R/P).$$

This is used in the proof of lemma 5.6, because it allows restricting to the case of integral domains.

(d) Let K be a field and A be a K-algebra, which is generated by the set S as a K-algebra. If A is an integral domain, then $\operatorname{Quot}(A) \cong K(S)$ by definition of $K(S)$. This is used in the proof of lemma 5.6.

(e) Let R be a ring and A an R-algebra. Then every ideal in A is in particular an R-submodule. This is used in the proof of theorem 5.11.

(f) Let $P \subset R$ be a prime ideal, which is an intersection of finitely many maximal ideals $P = \bigcap_{i=1}^n m_i$. Then P is equal to one of those maximal ideals m_i, because

$$P = \bigcap_{i=1}^{n} m_i \supset \prod_{i=1}^{n} m_i$$

implies $m_i \subset P$ for some $i \in \{1, \dots n\}$.
This is used in the proof of theorem 5.11.

Lemma 11. Let R be a finite-dimensional ring and $I \subset R$ an ideal.
Then $\dim(R/I) = \dim(R)$ if and only if $\operatorname{ht}(I) = 0$ (I contains no prime ideals).
In particular, $\dim(K[x_1, \dots, x_n]/I) = n$ if and only if $I = (0)$.

Proof. If $\operatorname{ht}(I) > 0$, then there is a prime ideal $J \in \operatorname{Spec}(R)$ with $J \subset I$ and thus a chain of prime ideals of length m in R/I gives rise to a chain of prime ideals in R of length $m + 1$. Since $\dim(R/I) \leq \dim(R) < \infty$, this implies $\dim(R/I) < \dim(R)$.
On the other hand, if $\operatorname{ht}(I) = 0$, then there is a order-preserving bijection between $\operatorname{Spec}(R/I)$ and $\operatorname{Spec}(R)$ (in other words, $\operatorname{Spec}(R/I) \cong \operatorname{Spec}(R)$ as partially ordered sets with inclusion $\subset$), so $\dim(R/I) = \dim(R)$. □

4.1 True or False: Krull Dimension

Decide for the following statements whether they are true or false. Give a proof or a counterexample.

(a) If $R \subset S$ is a subring, then $\dim(R) \leq \dim(S)$.

(b) If K is a field, A an affine K-algebra and $B \subset A$ is a subalgebra, then $\dim(B) \leq \dim(A)$.

(c) If I is an ideal in a ring R, then $\dim(R/I) \leq \dim(R)$.

(d) If R is an algebra over a field K with $\dim(R) = 0$, then R is finite dimensional as a K-vector space.

(a) False, since $\mathbb{Z} \subset \mathbb{Q}$, but $\dim(\mathbb{Z}) = 1 > 0 = \dim(\mathbb{Q})$.

(b) True, since by theorem 5.5 and theorem 5.9, it holds

$$\dim(B) \leq \operatorname{trdeg}(B) \leq \operatorname{trdeg}(A) = \dim(A).$$

(c) True, since a chain of prime ideals of length n in R/I gives rise to a chain of prime ideals of the same length in R.

(d) False. Consider $\mathbb{R}$ as a $\mathbb{Q}$-algebra. Because $\mathbb{R}$ is a field, $\dim(\mathbb{R}) = 0$. But $\mathbb{R}$ is not finite dimensional as a $\mathbb{Q}$-vector space, because a finite dimensional vector space over a countable field is countable; but $\mathbb{R}$ is not countable.
Alternatively, consider $R = K[x_1, x_2, \dots]/(x_1^2, x_2^2, \dots)$, which has the unique prime ideal $(\overline{x_1}, \overline{x_2}, \dots)$ and thus has dimension 0. However, R is not finitely generated as a K-vector space.
Another example is $K(x)$, the field of rational functions.

4.2 Noetherian factorial rings of dimension one

Let R be a Noetherian, factorial ring with $\dim(R) = 1$. The goal of this exercise is to prove that R is a principal ideal domain.

(a) First prove that every prime ideal in R is principal.

(b) Now let $a, b \in R \setminus \{0\}$ and $d \coloneqq \gcd(a, b)$. Prove $(a, b) = (d)$.
Hint: Show that $\left(\frac{a}{d}, \frac{b}{d}\right)$ is not contained in any maximal ideal.

(c) Now prove that every ideal in R is principal.

(a) For the zero ideal this holds by definition and because $\dim(R) = 1$, every nonzero prime ideal P satisfies $\operatorname{ht}(P) = 1$, so lemma 5.14 yields the claim.

(b) Since $d|a$, $d|b$, it holds $(a, b) \subset (d)$.
Claim: There is no maximal ideal $m \in \operatorname{Spec}_{\max}(R)$ with $\left(\frac{a}{d}, \frac{b}{d}\right) \subset m$.
If $\frac{a}{d}$ is a unit, then this is clear, so suppose $\frac{a}{d}$ is not a unit. Aiming for contradiction,

suppose such a $m \in \mathrm{Spec}_{\max}(R)$ exists. $\frac{a}{d}$ can be decomposed into irreducible elements $\frac{a}{d} = p_1 \dots p_n$. Since m is a prime ideal, $p_i \in m$ for some $i \in \{1, \dots, n\}$ and thus $(0) \subsetneq (p_i) \subset m$ implies $(p_i) = m$, because $\dim(R) = 1$. In particular, p_i divides both $\frac{a}{d}$ and $\frac{b}{d}$, which is a contradiction.
Using the claim (and the axiom of choice), we conclude that there exist $r, r' \in R$ with $r\frac{a}{d} + r'\frac{b}{d} = 1$, so $ra + r'b = d$ and $(d) \subset (a, b)$.

(c) Let I be an ideal in R. Since R is Noetherian, $I = (a_1, \dots, a_n)$ is finitely generated. Iterating (b), we get

$$I = (a_1, \dots, a_n) = (\gcd(a_1, a_2), a_3, \dots, a_n) = \dots = (\gcd(a_1, \dots, a_n)).$$

4.3 Dimension of a polynomial ring over a PID

Let R be a principal ideal domain, which is not a field. The following steps will show $\dim(R[x]) = 2$.

(a) Prove that $\dim(R[x]) \geq 2$.

(b) Let $P \subset R[x]$ be a prime ideal with $P \cap R = \{0\}$ and $K = \mathrm{Quot}(R)$. Prove that

$$Q = \{f \in K[x] : \exists\, a \in R \setminus \{0\} : af \in P\}$$

is a prime ideal in $K[x]$ and that $Q \cap R[x] = P$.

(c) Let $P_0 \subsetneq P_1 \subsetneq P_2$ be prime ideals in $R[x]$. Prove $P_2 \cap R \neq \{0\}$ and deduce $P_2 \cap R = (p)$ for some prime element $p \in R$.

(d) With the same notation as in the last step, prove that $P_2/(p)$ is a maximal ideal in $R[x]/(p)$.

(e) Conclude that $\dim(R[x]) \leq 2$, proving the claim.

(a) Since R is a principal ideal domain, there is $a \in R$, which is not a unit. Therefore, there is an irreducible element $p|a$. (p) is prime in R and in $R[x]$. Since $R[x]/(p, x) \cong R/p$ and R/p is a field, (p, x) is a maximal ideal in $R[x]$.
We get a chain of prime ideals of length 2:

$$(0) \subset (p) \subset (p, x).$$

Alternatively, one can argue that $R[x]/(x) \cong R$ shows that (x) is not maximal.

(b) Q is a prime ideal in $K[x]$:

- $0 \in Q$.
- Let $a, b \in Q$, i.e. there are $a, b \in R \setminus \{0\}$ with $af \in P$, $bg \in P$. Then $ab \neq 0$ and $ab(f + g) = abf + abg \in P$ shows $f + g \in Q$.
- Let $f \in Q$ with $af \in P$, $a \in R \setminus \{0\}$ and $g \in K[x]$. Let d denote the product of the denominators of the coefficients of g. Then $ad \in R \setminus \{0\}$ and $(ad)gf \in P$, because $dg \in R[x]$, so $gf \in Q$.

- Let $f, g \in K[x]$ with $fg \in Q$, i.e. there is $a \in R \setminus \{0\}$ with $afg \in P$. Let $b, c \in R \setminus \{0\}$ such that $bf \in R[x]$, $cg \in R[x]$. Then $a(bf)(cg) \in P$ implies $bf \in P$ or $cg \in P$, so $f \in Q$ or $g \in Q$.

It is left to show $Q \cap R[x] = P$. Let $f \in Q \cap R[x]$, i.e. there is $a \in R \setminus \{0\}$ with $af \in P$. Since P is prime in $R[x]$ and $P \cap R = \{0\}$, it follows $f \in P$, so $Q \cap R[x] \subset P$.
On the other hand, $1 \cdot p \in P$ for any $p \in P$, so $P \subset Q \cap R[x]$.

(c) By (b), the map

$$\{P \in \operatorname{Spec}(R[x]) : P \cap R = \{0\}\} \to \operatorname{Spec}(K[x]),\ P \mapsto Q_P$$

is inclusion-preserving and injective, because if $Q_P = Q_{P'}$, then

$$P = Q_P \cap R[x] = Q_{P'} \cap R[x] = P'.$$

If it was $P_2 \cap R = \{0\}$, then also $P_0 \cap R = P_1 \cap R = \{0\}$ and thus $Q_{P_0} \subsetneq Q_{P_1} \subsetneq Q_{P_2}$ is a chain of prime ideals of length 2 in $K[x]$, which contradicts $\dim(K[x]) = 1$.
Clearly $P_2 \cap R$ is a prime ideal in R and nonzero by the above. Because R is a principal ideal domain, the second claim follows.

(d) Since $R[x]/(p)_{R[x]} \cong (R/(p))[x]$ and $R/(p)$ is a field, it suffices to show that $P_2/(p)$ is nonzero, because any nonzero prime ideal in a principal ideal domain is maximal. Suppose for contradiction that $P_2/(p) = (0)$, i.e. $P_2 = (p)$. In particular, $p \notin P_1$. Let $f \in P_1 \setminus \{0\}$ and decompose it into irreducible elements $f = p_1 \dots p_n$. Since P_1 is prime, $p_i \in P_1$ for some $i \in \{1, \dots, n\}$. But $P_1 \subset P_2$ shows $p | p_i$, so by irreducibility $p \cdot a = p_i$ with $a \in R[x]$ a unit, implying $p \in P_1$. Contradiction.

(e) By (d), $P_2/(p)$ is maximal in $R[x]/(p)$, so P_2 is maximal in $R[x]$ and $\dim(R[x]) \leq 2$.

4.4 Krull dimensions of rings

Determine the Krull dimension of each of the following rings:
(a) $R = K[\![x]\!]$, the formal power series ring over a field K,

(b) $R = K[x, x^{-1}] = \left\{\sum_{k=-n}^{n} a_k x^k : a_k \in K, n \in \mathbb{N}\right\} \subset K(x)$, the ring of Laurent polynomials over a field K,

(c) $R = \mathbb{Z}/n\mathbb{Z}$, where $n \in \mathbb{N} \setminus \{0, 1\}$.

(a) By a previous exercise, (x) is the only maximal ideal in R.
Now let $I \subset R$ be a nonempty prime ideal and $f = \sum_{n=0}^{\infty} a_n x^n \in I$ an element of I. If $a_0 \neq 0$, then f is invertible, so $a_0 = 0$ and thus there is $k \in \mathbb{N}_{>0}$, such that $a_k = 0$ and thus

$$f = x^k \cdot \underbrace{\sum_{n=k}^{\infty} a_n x^n}_{\in K[\![x]\!]^\times}.$$

It follows $x \in I$ and by maximality $I = (x)$. Therefore, (0) and (x) are the only prime ideals in $K[\![x]\!]$, implying $\dim(K[\![x]\!]) = 1$.
Alternatively, one can show that $K[\![x]\!]$ is a principal ideal domain, which directly yields the result.

(b) R is an affine K-algebra and is generated by the set $\{x, x^{-1}\}$. Clearly $\{x\}$ is algebraically independent over K, but $\{x, x^{-1}\}$ is not, (consider $yz - 1 \in K[y, z]$). By theorem 5.9 and proposition 5.10, we conclude $\dim(R) = 1$.

(c) Because $(0) \subset (n)$, 11 implies $\dim(\mathbb{Z}/n\mathbb{Z}) < \dim(\mathbb{Z}) = 1$, so $\dim(\mathbb{Z}/n\mathbb{Z}) = 0$.
In particular, we see that $\mathbb{Z}/n\mathbb{Z}$ is an Artinian ring for $n \in \mathbb{N} \setminus \{0\}$ (theorem 2.8).

4.5 Krull dimensions of rings II

Calculate the Krull dimension of the following rings, where K is a field:
(a) $R = K[x, y]/(x^2 + y^2 + 1)$,

(b) $R = K[x, y, z](y - x^2, z^2 - x^3)$,

(a) R is generated as a K-algebra by the set $\{\overline{x}, \overline{y}\}$. Since that set is algebraically dependent and $\{\overline{x}\}$ is algebraically independent, it follows $\dim(R) = 1$ by theorem 5.9 and proposition 5.10.

(b) With the same argument as the previous example, we see that $\dim(R) = 1$.
For example,

$$0 = x^6 - x^6 = y^3 - (z^2)^2 = y^3 - z^4$$

shows that the set $\{y, z\}$ is algebraically dependent over K.

4.6 Von Neumann regular rings

A not necessarily commutative ring R is called *von Neumann regular*, if

$$\forall\, x \in R : \exists\, a \in R : x = xax.$$

So a can be thought of as something like an inverse of x.
For a commutative ring R prove that:
(a) If R is von Neumann regular, then R is reduced and $\dim(R) = 0$.
The converse is also true, but hard.

(b) If R has $\dim(R) = 0$ and is an integral domain, then R is von Neumann regular.

(a) Let $r \in R$ with $r^n = 0$ and n minimal with that property. We show that $n = 1$. If $n > 1$, then $m = \lceil \frac{n}{2} \rceil < n$, so $r^m = r^m a r^m = 0$ yields a contradiction to the minimality of n. Thus $r = 0$ and R is reduced.

Now let $P \subset R$ be a prime ideal. Then R/P is von Neumann regular and an integral domain. For $x \notin P$, we get

$$x + P = ax^2 + P \Rightarrow x(1 + ax) \in P \Rightarrow (1 + ax) \in P \Rightarrow (a + P)(x + P) = 1 + P,$$

so R/P is a field. This means that any prime ideal of R is in fact maximal, so $\dim(R) = 0$.

(b) $R \cong R/(0)$ is a field and thus von Neumann regular.

Localization

Lemma 12. Let M be a module over a ring R and $U \subset R$ a multiplicative submonoid.

(a) If $\operatorname{Ann}(M) \cap U \neq \emptyset$, then $U^{-1}M = 0$.

(b) If M is finitely generated, then $U^{-1}M = 0$ if and only if $\operatorname{Ann}(M) \cap U \neq \emptyset$.

Proof. (a) If $x \in \operatorname{Ann}(M) \cap U$, then $xm = 0$ for any $m \in M$ and thus $\frac{m}{u} = 0$ for any $\frac{m}{u} \in U^{-1}M$.

(b) Choose generators $m_1, \ldots, m_n \in M$ of M as an R-module. Suppose $U^{-1}M = 0$. Then for each m_i, $i \in \{1, \ldots, n\}$ it is $\frac{m_i}{1} = 0$, so there is $u_i \in U$ with $u_i m_i = 0$. It follows $\prod_{i=1}^{n} u_i \in \operatorname{Ann}(M) \cap U$.

□

5.1 Example of a local ring

Let $R := \mathbb{Z}_{(2)}[x]$ and $I := (2x - 1) \subset R$.

(a) Prove that $\mathbb{Z}_{(2)}$ is a principal ideal domain. In particular, $\mathbb{Z}_{(2)}$ is a unique factorization domain.

(b) Show that I is a maximal ideal.

(c) Determine $\operatorname{ht}(I)$.

(d) Does $\dim(R) = \dim(R/I) + \operatorname{ht}(I)$ hold in this case?

(a) An ideal $I \subset \mathbb{Z}_{(2)}$ is of the form $I = J_{(2)}$, where $J \subset \mathbb{Z}$ is an ideal in $\mathbb{Z}$. Since $\mathbb{Z}$ is a principal ideal domain, $J = (p)$ for some $p \in \mathbb{Z}$ and thus $I = \left(\frac{p}{1}\right)$.

(b) Intuitively, the element in $\overline{x} \in R/I$ is precisely the inverse of 2. This motivates the following argument. Viewing $\mathbb{Q}$ as a $\mathbb{Z}_{(2)}$-algebra, we consider the surjective $\mathbb{Z}_{(2)}$-algebra homomorphism

$$R \to \mathbb{Q},\ x \mapsto \frac{1}{2}.$$

The kernel is given by I, so $R/I \cong \mathbb{Q}$ and thus I is maximal.

(c) $\mathbb{Z}_{(2)}$ is Noetherian, because $\mathbb{Z}$ is Noetherian and thus $\mathbb{Z}_{(2)}[x]$ is Noetherian as well. It follows $\operatorname{ht}(I) \leq 1$. The chain $(0) \subsetneq I$ shows that $\operatorname{ht}(I) = 1$.

(d) No. Because $\mathbb{Z}_{(2)}$ is Noetherian, it holds $\dim(R) = 2$, but $\dim(R/I) = 0$ by maximality of I and $\operatorname{ht}(I) = 1$ by (c).

5.2 Reduced rings and localization

Let R be a ring. Prove that the following statements are equivalent:

(a) R is reduced.

(b) R_P is reduced for every prime ideal $P \subset R$.

(c) R_m is reduced for every maximal ideal $m \subset R$.

"(a) $\Rightarrow$ (b)": Let $P \in \operatorname{Spec}(R)$ and $\frac{a}{u} \in R_P$ with $\left(\frac{a}{u}\right)^k = 0$ for some $k \in \mathbb{N}_{>0}$. This means that there is $x \in R \setminus P$ with $xa^k = 0$. Thus $(xa)^k = x^k a^k = 0$ and since R is reduced, it follows $xa = 0$, i.e. $\frac{a}{u} = 0$.
"(b) $\Rightarrow$ (c)": Since every maximal ideal is prime, this is clear.
"(c) $\Rightarrow$ (a)": If R is the zero ring, then there is nothing to show, so suppose $R \neq 0$. By contraposition, suppose R is not reduced, i.e. there is $a \in R \setminus \{0\}$ with $a^k = 0$ for some $k \in \mathbb{N}_{>0}$. Since $R \neq 0$, $\operatorname{Ann}(a) \neq R$ and is thus contained in a maximal ideal $m \in \operatorname{Spec}_{\max}(R)$. Consider $r := \frac{a}{1} \in R_m$ and notice that $r \neq 0$, because $\operatorname{Ann}(a) \subset m$. Since $r^k = \frac{a^k}{1} = 0$, we conclude that R_m not reduced.
One can alternatively formulate the same idea using contradiction instead of contraposition.

5.3 Support of modules

Let R be a ring and M a finitely generated R-module. Prove that

$$\operatorname{supp}(M) = \mathcal{V}_{\operatorname{Spec}(R)}(\operatorname{Ann}(M)).$$

By 12, it holds:

$$\begin{aligned} P \in \operatorname{supp}(M) &\iff M_P \neq 0 \iff \operatorname{Ann}(M) \cap \neg P = \emptyset \\ &\iff \operatorname{Ann}(M) \subset P \iff P \in \mathcal{V}_{\operatorname{Spec}(R)}(\operatorname{Ann}(M)). \end{aligned}$$

5.4 Associated primes

Let R be a Noetherian ring and M a nonzero R-module.
A prime ideal $P \in \operatorname{Spec}(R)$ is called an *associated prime* of M if there exists $m \in M$ such that $P = \operatorname{Ann}(m)$. Notice that not all annihilators of elements of M are prime ideals. Denote with $\operatorname{Ass}(M)$ the set of all associated primes.

(a) Prove that there is $m \in M \setminus \{0\}$ such that $\operatorname{Ann}(m)$ is maximal among all ideals of this form; i.e. there exists no $m' \in M \setminus \{0\}$ with $\operatorname{Ann}(m) \subsetneq \operatorname{Ann}(m')$.

(b) Let m be as in (a). Prove that $\operatorname{Ann}(m)$ is a prime ideal, so in particular $\operatorname{Ass}(M) \neq \emptyset$.

(c) Let $U \subset R$ be a multiplicative submonoid. Prove that

$$\operatorname{Ass}(U^{-1}M) = \{P \in \operatorname{Ass}(M) : P \cap U = \emptyset\}.$$

(d) Let $M = R/I$ for some ideal $I \subset R$ and P a prime ideal which is minimal among those prime ideals which contain I. Prove that $P \in \operatorname{Ass}(M)$.

(e) Let $M = R/I$ for some radical ideal I and $P \in \operatorname{Ass}(M)$. Show that P is a prime ideal which is minimal among those which contain I.
Hint: Use corollary 1.12.
Together with (d), this shows that for a radical ideal I, $\operatorname{Ass}(M)$ is precisely the set of all ideals which are minimal over I.

(a) The set of ideals $X := \{\operatorname{Ann}(m) : m \in M \setminus \{0\}\}$ is nonempty, since M is nonzero. Because R is Noetherian, X has to contain a maximal element.

(b) Let $ab \in \operatorname{Ann}(m)$, i.e. $abm = 0$. If $bm = 0$, then $b \in \operatorname{Ann}(m)$, so suppose $bm \neq 0$. Then $\operatorname{Ann}(m) \subset \operatorname{Ann}(bm)$, so by maximality $\operatorname{Ann}(m) = \operatorname{Ann}(bm)$ and $a \in \operatorname{Ann}(m)$.

(c) "$\subset$": Let $P \in \operatorname{Ass}(U^{-1}M)$, i.e. P is prime and

$$P = \operatorname{Ann}\Big(\frac{m}{u}\Big) = \{r \in R : \exists\, x \in U : rxm = 0\}.$$

Suppose there was $y \in P \cap U$. Then there is $x \in U$ with $yxm = 0$, so $r(yx)m = 0$ for every $r \in R$, implying $P = R$. Contradiction.
It is left to show that $P = \operatorname{Ann}(m')$ for some $m' \in M$. Since R is Noetherian, $P = (a_1, \dots, a_n)$ and because $a_i \in P$, we can choose $x_i \in U$, $i \in \{1, \dots, n\}$ with $a_i x_i m = 0$. Set $m' := (\prod_{i=1}^n x_i) \cdot m$. Clearly, $\operatorname{Ann}(m') \subset \operatorname{Ann}(\frac{m}{u})$. On the other hand, let $r \in \operatorname{Ann}(\frac{m}{u})$. Then $r = \sum_{i=1}^n r_i a_i$ with $r_i \in R$, so by definition of m', $rm' = 0$ and $r \in \operatorname{Ann}(m')$. This shows $P = \operatorname{Ann}(m')$.
"$\supset$": Let $P = \operatorname{Ann}(m) \in \operatorname{Ass}(M)$ with $P \cap U = \emptyset$. If $xrm = 0$ for $x \in U$, $r \in R$, then $xr \in P$, so $r \in P$. This means

$$P = \operatorname{Ann}(m) = \{r \in R : rm = 0\} = \{r \in R : \exists\, x \in U : xrm = 0\} = \operatorname{Ann}\Big(\frac{m}{1}\Big).$$

(d) We need to find a prime ideal ideal $J = \operatorname{Ann}(m)$ with $I \subset J \subset P$. It holds $I \subset \operatorname{Ann}(m)$ for any $m \in M$, so by (c), it is enough to show $\operatorname{Ass}(M_P) \neq \emptyset$. Due to

(b), $\mathrm{Ass}(M_P) = \emptyset$ can only happen if M is the zero module. But since $I \neq R$, M has more than one element, so $M \neq 0$.

(e) Let $P = \mathrm{Ann}(\overline{m})$. It is clear that $I \subset P$ and $m \notin I$. Corollary 1.12 gives the existence of a prime ideal $Q \in \mathrm{Spec}(R)$ with $I \subset Q$ and $m \notin Q$. By corollary 3.14(d), we can assume Q to be minimal over I. Thus it is enough to show $P \subset Q$. To do so, let $r \in P$, i.e. $rm \in I$. Since $I \subset Q$, $m \notin Q$ and Q is prime, this implies $r \in Q$, so $P \subset Q$.

5.5 Examples of localization

Describe the localization $U^{-1}M$ in the following cases, where R is a ring, $U \subset R$ a multiplicative submonoid and M an R-module.

(a) $M = R = \mathbb{Q}[x]$, $U = \left\{x^k : k \in \mathbb{N}\right\}$.

(b) $M = R = \mathbb{Z}$, $U = \{1\} \cup \{12z : z \in \mathbb{Z} \setminus \{0\}\}$.

(c) $R = \mathbb{Z}$, $M = \mathbb{Z}[x]$, $U = \mathbb{Z} \setminus \{0\}$.

(d) $R = \mathbb{Q}[x]$, $M = \mathbb{Q}[x]/(x^2)$, $U = \left\{x^k : k \in \mathbb{N}\right\}$

(e) $R = \mathbb{Q}[x]$, $M = \mathbb{Q}[x]/(x^2)$, $U = \mathbb{Q}[x] \setminus (x)$

(a) Clearly $\mathbb{Q}[x] \subset U^{-1}R \subset \mathbb{Q}(x)$. It holds $U^{-1}R = \mathbb{Q}[x, x^{-1}]$.

(b) It holds $U^{-1}R \cong \mathbb{Q}$ by the ring isomorphism $U^{-1}R \to \mathbb{Q}$, $\frac{a}{b} \mapsto \frac{12a}{12b}$.

(c) It holds $U^{-1}M \cong \mathbb{Q}[x]$ by the module isomorphism

$$U^{-1}M \to \mathbb{Q}[x], \ \frac{a_n x^n + \cdots + a_1 x + a_0}{u} \mapsto \frac{a_n}{u}x^n + \cdots + \frac{a_1}{u}x + \frac{a_0}{u}.$$

(d) Since $x^2 \cdot f = 0$ for any $f \in M$ and $x^2 \in U$, it follows $U^{-1}M = 0$.

(e) It holds $U^{-1}R \cong \mathbb{Q}[x]/(x^2)$, since the elements in U already are "invertible" (multiplying with them is a R-module isomorphism). Equivalently, there is a module isomorphism

$$U^{-1}M \to \mathbb{Q}[x]/(x^2), \ \frac{a_0 + a_1 x}{u} \mapsto \frac{a_0}{u} + \frac{a_1}{u}x.$$

5.6 Localization of a module as base change

Let R be a commutative ring, $U \subset R$ a multiplicative submonoid, and M an R-module. Show

$$U^{-1}M \cong U^{-1}R \otimes_R M.$$

We show that $U^{-1}M$ satisfies the universal property of $U^{-1}R \otimes M$, i.e. there is a bilinear map $\epsilon : U^{-1}R \times M \to U^{-1}M$ such that for any abelian group A and bilinear map

$f : U^{-1}R \times M \to A$, there is a unique group homomorphism $\phi : U^{-1}M \to A$, such that the diagram

$$\begin{array}{ccc} U^{-1}R \times M & \xrightarrow{\epsilon} & U^{-1}M \\ & \searrow^{f} & \downarrow \phi \\ & & A \end{array}$$

commutes.
Define

$$\epsilon : U^{-1}R \times M \to U^{-1}M,\ \left(\frac{r}{u}, m\right) \mapsto \frac{rm}{u} = \frac{r}{u} \cdot \frac{m}{1},$$

which first applies the canonical R-module homomorphism $M \to U^{-1}M$ to the second component and then multiplies the results. Since multiplication in the $U^{-1}R$-module $U^{-1}M$ is in particular R-bilinear, ϵ is R-bilinear.
Let now $f : U^{-1}R \times M \to A$ bilinear be given and we want to construct ϕ. By the commutative diagram, it must in particular hold

$$\phi\left(\frac{m}{u}\right) = f\left(\frac{1}{u}, m\right),$$

which uniquely defines ϕ. This definition is well-defined: If $\frac{m}{u} = \frac{m'}{u'}$, i.e. there is $x \in U$ with $xu'm = xum'$, so by bilinearity of f, it holds

$$\phi\left(\frac{m}{u}\right) = f\left(\frac{xu'}{xu'u}, m\right) = f\left(\frac{1}{xu'u}, xu'm\right) = f\left(\frac{1}{xu'u}, xum'\right) = f\left(\frac{1}{u'}, m'\right) = \phi\left(\frac{m'}{u'}\right).$$

Moreover, ϕ is a group homomorphism: If $\frac{m}{u}, \frac{m'}{u'} \in U^{-1}M$, then the bilinearity of f yields

$$\begin{aligned} \phi\left(\frac{m}{u} + \frac{m'}{u'}\right) &= \phi\left(\frac{u'm + um'}{uu'}\right) = f\left(\frac{1}{uu'}, u'm + um'\right) = f\left(\frac{1}{uu'}, u'm\right) + f\left(\frac{1}{uu'}, um'\right) \\ &= f\left(\frac{1}{u}, m\right) + f\left(\frac{1}{u'}, m'\right) = \phi\left(\frac{m}{u}\right) + \phi\left(\frac{m'}{u'}\right). \end{aligned}$$

It is left to show that the diagram commutes, so let $(\frac{r}{u}, m) \in U^{-1}R \times M$. Then

$$(\phi \circ \epsilon)\left(\frac{r}{u}, m\right) = \phi\left(\frac{rm}{u}\right) = f\left(\frac{1}{u}, rm\right) = f\left(\frac{r}{u}, m\right),$$

so $U^{-1}M$ with ϵ satisfies the universal property of $U^{-1}R \otimes_R M$, and there is a unique isomorphism $U^{-1}M \cong U^{-1}R \otimes_R M$.

5.7 Characterization of local rings and the Jacobson radical

Let R be a ring. Prove the following:

(a) R is local if and only if the set of all non-units $R \setminus R^\times$ is an ideal.
This means that a local ring is precisely a ring R with a maximal ideal m, such that every $r \in R \setminus m$ is invertible.

(b) Let J be the Jacobson radical of R, i.e. the intersection of all maximal ideals of R and let $x \in R$. Then

$$x \in J \iff 1 - xy \in R^\times \ \forall \ y \in R.$$

(a) Suppose R is local. For $r \in R \setminus R^\times$, there is a maximal ideal $m \in \mathrm{Spec}_{\max}(R)$, such that $r \in m$. Since R is local, this means that $R \setminus R^\times \subset m \subset \setminus R^\times$, so the maximal ideal is $m = R \setminus R^\times$.
On the other hand, if $R \setminus R^\times$ is an ideal, every proper ideal is contained in it, so it is the unique maximal ideal of R and thus R is local.

(b) Let $x \in J$ and $y \in R$. Then $1 - xy$ is not contained in any maximal ideal, since otherwise that ideal would contain 1. Thus $1 - xy$ is a unit.
On the other hand, let $m \in \mathrm{Spec}_{\max}(R)$ be a maximal ideal and consider $m \subset (x, m)$. (x, m) is a proper ideal, since $1 = yx + z$ for $y \in R, z \in m$ implies by assumption that m contains a unit. By maximality, it follows $m = (x, m)$, i.e. $x \in m$.

Nakayama's Lemma and the Principal Ideal Theorem

6.1 Nakayama's lemma and system of generators

Let R be a ring, M a finitely generated R-module and $J \subset R$ the Jacobson radical. The module M/JM is a R/J-module. Let $\pi : M \to M/JM$ be the canonical map.

(a) Let $U \subset M$ be a submodule. Prove the following statement:

$$U = M \iff \pi(U) = \pi(M).$$

(b) Let $x_1, \ldots, x_n \in M$. Prove the following statement:

$$M = (x_1, \ldots, x_n)_R \iff \pi(M) = (\pi(x_1), \ldots, \pi(x_n))_{R/J}.$$

(c) Assume R is local with maximal ideal $m = J$ and let $K \coloneqq R/m$ be the residue field of R. Let $x_1, \ldots, x_n$ be a minimal set of generators of M. Prove that $n = \dim_K(M/JM)$; in particular, all minimal sets of generators have the same number of elements.

(d) Give an example of a ring R and a finitely generated R-module M such that not all minimal sets of generators of M have the same number of elements.

(a) Suppose $\pi(U) = \pi(M)$. It is to show that this implies $U = M$. Since

$$J \cdot (M/U) = (JM + U)/U,$$

it is left to show $JM + U = M$, since then Nakayama's lemma yields $M/U = 0$, i.e. $M = U$.
So let $m \in M$. By assumption, there is $u \in U$ with $m - u \in JM$, so $m \in JM + U$ and $M \subset JM + U$.

(b) Since $\pi((x_1, \ldots, x_n)) = (\pi(x_1), \ldots, \pi(x_n))$, the claim follows immediately from (a).

(c) Because the x_i generate M as an R-module, they generate M/JM as a K-vector space, so $\dim_K(M/JM) \leq n$. On the other hand, the dimension of M/JM as a vector space can not be smaller than n, because this would imply that M/JM is generated by a proper subset of $\{\pi(x_1), \ldots, \pi(x_n)\}$, which by (b) contradicts the minimality of the set $\{x_1, \ldots, x_n\}$.

(d) Take $R = \mathbb{Z}$ as a module over itself and notice that $R = (1) = (2, 3)$ and both of the generating sets are minimal, but have a different number of elements.

6.2 Assumptions of the prime avoidance lemma

Show that the assumptions of the prime avoidance lemma can not be weakened by considering the ring $R \coloneqq \mathbb{F}_2[x,y]/(x^2,y^2,xy)$ and finding ideals $J, I_1, I_2, I_3 \subsetneq R$ with $J \subset I_1 \cup I_2 \cup I_3$ but $J \not\subset I_i$ for each i.

Note that $R = \{0, 1, x, y, x+y, x+1, y+1, x+y+1\}$ and consider the ideals

$$I_1 \coloneqq (x)_R = \{0, x\}, \qquad I_2 \coloneqq (y)_R = \{0, y\}, \qquad I_3 \coloneqq (x+y)_R = \{0, x+y\}$$
$$J \coloneqq (x,y)_R = \{0, x, y, x+y\}.$$

Clearly $J \subset \bigcup_{1\leq i\leq 3} I_i$, but $J \not\subset I_i$ for $i \in \{1,2,3\}$.

6.3 Assumptions of the principal ideal theorem

In this exercise, we want to show that the principal ideal theorem only works in Noetherian rings. For this, let $R \coloneqq K[x, xy, xy^2, xy^3, \dots] \subset K[x,y]$, which is a ring that is not Noetherian.

(a) Prove that there is only one prime ideal $P \subset R$ with $(x)_R \subset P$.

(b) Prove that $\operatorname{ht}(P) = 2$.

(a) Let P be a prime ideal containing $(x)_R$. For $n \in \mathbb{N}$, $(xy^n)^2 = x \cdot xy^{2n} \in P$, so $xy^n \in P$ for all $n \in \mathbb{N}$. Since the ideal $P' \coloneqq (x, xy, xy^2, \dots) \subset R$ is maximal ($R/P' \cong K$), it follows that $P = P'$ and thus it is the only prime ideal with $(x)_R \subset P$. Alternatively, the maximality of P' can also be derived from $P' = (x,y)_{K[x,y]} \cap R$ by proposition 1.2.

(b) Because R is a K-subalgebra of a finitely generated K-algebra,

$$\dim(R) \leq \dim(K[x,y]) = 2$$

and thus $\operatorname{ht}(P) \leq 2$. On the other hand, the ideal $P' \coloneqq (xy, xy^2, xy^3, \dots)_R$ is prime, because $R/P' \cong K[x]$ is an integral domain (alternatively, since $P' = (y)_{K[x,y]} \cap R$). Therefore, the chain of prime ideals

$$\{0\} \subsetneq P' \subsetneq P,$$

has length 2 and we conclude $\operatorname{ht}(P) = 2$.

6.4 Noetherian (local) rings

(a) Let R be a Noetherian local ring with maximal ideal m and

$$\mathcal{M} \coloneqq \{P \in \operatorname{Spec}(R) : \operatorname{ht}(P) \leq 1\}.$$

Prove that $\bigcup_{P\in\mathcal{M}} P = m$.

(b) Let R be a Noetherian ring (not necessarily local) with $\dim(R) \geq 2$. Prove that $\operatorname{Spec}(R)$ is an infinite set.

(a) Since any prime ideal is contained in a maximal ideal and the only maximal ideal in R is m, $\bigcup_{P\in\mathcal{M}} P \subset m$ is clear. On the other hand, let $x \in m$. Then (x) is a proper ideal and by corollary 3.14, there are minimal prime ideals over (x). Pick one of them and call it Q. By the principal ideal theorem, $\operatorname{ht}(Q) \leq 1$, so $x \in Q \subset \bigcup_{P\in\mathcal{M}} P$ and $m \subset \bigcup_{P\in\mathcal{M}} P$.

(b) Let Q be a prime ideal with $\operatorname{ht}(Q) \geq 2$ and consider the localization R_Q, which is a Noetherian local ring with maximal ideal Q_Q. By (a), $\bigcup_{P\in\mathcal{M}} P = Q_Q$. If $\mathcal{M}$ was finite, then the prime avoidance lemma would imply $Q_Q \subset P$ for some $P \in \mathcal{M}$, which contradicts $\operatorname{ht}(Q) = \operatorname{ht}(Q_Q) \geq 2$. Therefore, $\mathcal{M}$ and thus $\operatorname{Spec}(R_Q)$ are infinite sets, so in particular $\operatorname{Spec}(R)$ is an infinite set, as well.

6.5 Examples of systems of parameters

Let $x = (0, \ldots, 0) \in \mathbb{C}^n$. Find a system of parameters for the local ring $\mathbb{C}[X]_x$ in each of the following cases:

(a) $X = \{(\xi_1, \xi_2) \in \mathbb{C}^2 : \xi_1\xi_2 = 0\}$,

(b) $X = \{(\xi_1, \xi_2, \xi_3) \in \mathbb{C}^3 : \xi_1^2 + \xi_2^2 - \xi_3^2 = 0\}$,

(c) $X = \{(\xi_1, \xi_2) \in \mathbb{C}^2 : \xi_2^2 + \xi_1(\xi_1^2 + 1) = 0\}$.

By corollary 7.9, the number of elements in a system of parameters is given by the Krull dimension of $\mathbb{C}[X]_x$. Also note that the maximal ideal m in $\mathbb{C}[X]_x$ is given by $m = \left(\frac{\overline{x_1}}{1}, \ldots, \frac{\overline{x_n}}{1}\right)$.

(a) It is $\mathbb{C}[X]_x = \left(\mathbb{C}[x_1, x_2]/(x_1 \cdot x_2)\right)_x$. Since prime ideals in $\mathbb{C}[X]_x$ correspond to prime ideals $P \in \mathbb{C}[x_1, x_2]$ with $(x_1 \cdot x_2) \subset P \subset (x_1, x_2)$, the chain of prime ideals $(x_1) \subsetneq (x_1, x_2)$ shows that $\dim(\mathbb{C}[X]_x) = 1$. Guessing yields $m = \sqrt{(\overline{x_1} + \overline{x_2})}$, so a system of parameters is given by $\overline{x_1} + \overline{x_2}$.

(b) Note that

$$(x_1^2 + x_2^2 - x_3^2) \subsetneq (x_1, x_2 - x_3) \subsetneq (x_1, x_2, x_3)$$

is a chain of prime ideals, so $\dim(\mathbb{C}[X]_x) = 2$. It holds $m = \sqrt{(\overline{x_1}, \overline{x_2})}$.

(c) Since

$$\left(x_2^2 + x_1(x_1^2 + 1)\right) \subsetneq (x_1, x_2)$$

is a chain of prime ideals, it holds $\dim(\mathbb{C}[X]_x) = 1$. We guess $m = \sqrt{(\overline{x_1})}$.

6.6 Chains in a Noetherian ring

Let R be a Noetherian ring and

$$P_0 \supset P_1 \supset P_2 \supset \dots$$

a chain of prime ideals. Prove that the chain stabilizes; i.e. there exists $n \in \mathbb{N}$, such that $P_n = P_i$ for all $i \geq n$.

(a) Because R is Noetherian, $P_0 = (a_1, \dots, a_n)$ is finitely generated. By the principal ideal theorem, $\mathrm{ht}(P_0) \leq n$.

Integral Extensions

Remark 13. (a) Let $K \subset S$ be a ring extension with K a field. An element $\alpha \in S$ is integral over K if and only if it is algebraic over K.

(b) If $R \subset S$ is a ring extension and R is not a field, then the notion of a minimal polynomial does not necessarily exist. This is because for $\alpha \in S$, the kernel of the R-algebra homomorphism $R[x] \to S,\ x \mapsto s$ is not necessarily a principal ideal. See example 8.2(3).

(c) For an integral ring extension $R \subset S$ and $P \in \operatorname{Spec}(R)$, there is $Q \in \operatorname{Spec}(S)$ with $Q \cap R = P$. This is an often used consequence of theorem 8.12.

(d) Let $R \subset S$ be a ring extension and $Q \in \operatorname{Spec}(S)$, $P \in \operatorname{Spec}(R)$. Does $Q \subset (P)_S$ imply $R \cap Q \subset P$?
No, consider e.g. $\mathbb{Z} \subset \mathbb{Z}_{(2)}$ and $Q = (2)_{(2)}$, $P = (3)$.

(e) It is obvious that e.g. $K[x, xy, xy^2, \dots]/(xy, xy^2, \dots) \cong K[x]$, but sometimes one has to be careful. For example, consider $S \coloneqq K[x, y] = K[x, x - y, x^2 - y]$ and $I = (x - y, x^2 - y)$. Then $S/I \ncong K[x]$, because $x^2 - x = (x^2 - y) - (x - y)$. Instead, $S/I \cong K[x]/(x^2 - x)$.

Lemma 14. Let G be a group and $g \in G$. Then multiplication by g, i.e. the map $G \to G,\ x \mapsto g \cdot x$, is a bijection.

Proof. The inverse is given by $G \to G, x \mapsto g^{-1} \cdot x$. □

Lemma 15. Let $R \subset S$ be an integral ring extension and $Q, Q' \in \operatorname{Spec}(S)$ with $Q \subset Q'$ and $Q \cap R = Q' \cap R$. Then $Q = Q'$.

Proof. This follows directly from theorem 8.12(b) by taking $P = Q \cap R$, $I = (0)$. □

Lemma 16. Let A be an affine K-variety with $A \cong K[x_1, \dots, x_n]/I$, $I \neq (0)$, where $I = (p)$ is a principal ideal. Then for the Hilbert function h_I, it holds $h_I(d) = \binom{d+n}{n}$ for $d < \deg(p)$ and $h_I(d) = \binom{d+n}{n} - \binom{d-\deg p+n}{n}$ otherwise.

Proof. Consider the K-vector space $I_{\leq d} \coloneqq I \cap K[x_1, \dots, x_n]_{\leq d}$. By the second isomorphism theorem, there is an isomorphism of K-vector spaces

$$A_{\leq d} = (K[x_1, \dots, x_n]_{\leq d} + I)/I \cong K[x_1, \dots, x_n]_{\leq d}/I_{\leq d},$$

so

$$\dim_K(A_{\leq d}) = \dim_K(K[x_1, \dots, x_n]_{\leq d}) - \dim_K(I_{\leq d}).$$

It holds $\dim_K(K[x_1, \dots, x_n]_{\leq d}) = \binom{d+n}{n}$ and $\dim_K(I_{\leq d}) = 0$ for $d < \deg(p)$. Additionally, for $d \geq \deg(p)$, the isomorphism of K-vector spaces

$$I_{\leq d} \to K[x_1, \dots, x_n]_{\leq d-\deg(p)},\ f \cdot p \mapsto f$$

shows that $\dim_K(I_{\leq d}) = \dim(K[x_1, \dots, x_n]_{\leq d-\deg(p)}) = \binom{d-\deg p+n}{n}$. It follows for $d \geq \deg(p)$:

$$\dim_K(A_{\leq d}) = \binom{d+n}{n} - \binom{d-\deg p+n}{n}.$$

□

7.1 Rings of invariants of finite groups

Let $R \subset S$ be rings. Then S becomes an R-algebra via the inclusion $R \hookrightarrow S$. Let $\mathrm{Aut}_R(S)$ denote the group of R-algebra automorphisms of S. For a finite subgroup $G \subset \mathrm{Aut}_R(S)$, the *ring of invariants* is

$$S^G := \{a \in S : \forall\, \sigma \in G : \sigma(a) = a\}.$$

This is again an R-algebra. Prove the following:

(a) S is integral over S^G.

(b) If S is finitely generated as an R-algebra, then there is a finitely generated subalgebra $A \subset S^G$, such that S is integral over A.

(c) If S is finitely generated as an R-algebra and R is Noetherian, then S^G is finitely generated as an R-algebra.

(a) For $a \in S$, define

$$f := \prod_{\sigma \in G} (x - \sigma(a)) \in S[x].$$

This is a monic polynomial with $f(a) = 0$. For $\tau \in G$, applying τ to the coefficients of f yields $\prod_{\sigma \in G}(x - (\tau \circ \sigma)(a))$, which equals f by 14, so the coefficients of f are in S^G.

(b) Write $S = R[a_1, \ldots, a_n]$. By (a), each of the a_i is integral over S^G. Let A be the R-algebra generated by the coefficients of the integral equations of the a_i. By definition, A finitely generated and by theorem 8.4, S is integral over A, because the generators are integral over A.

(c) Let $A \subset S^G$ as in (b). Since S is finitely generated as an R-algebra, it is also finitely generated as an A-algebra, so by theorem 8.4, S is finitely generated as an A-module. A is Noetherian as a finitely generated R-algebra (corollary 2.12), so theorem 2.10 implies that $S^G \subset S$ is a finitely generated A-submodule. Now the claim follows from 2.

7.2 Rings of invariants are normal

Let R be a normal ring and $G \subset \mathrm{Aut}(R)$ a group automorphism of R. Show that the ring of invariants R^G is normal, too.

Let $\frac{r}{s} \in \mathrm{Quot}\,(R^G)$ integral over R^G, i.e. there exist $a_i \in R^G$ such that

$$\left(\frac{r}{s}\right)^n + a_1\left(\frac{r}{s}\right)^{n-1} + \cdots + a_{n-1}\frac{r}{s} + a_n = 0.$$

Consider the inclusion $\phi : \mathrm{Quot}(R^G) \to \mathrm{Quot}(R)$, $\frac{a}{b} \mapsto \frac{a}{b}$, which is a ring homomorphism with $\phi(R^G) \subset R$. Applying ϕ to the integral equation of $\frac{r}{s}$, we receive an integral

equation for $\phi(\frac{r}{s}) \in \mathrm{Quot}(R)$, so $\phi(\frac{r}{s}) \in R$, since R is normal. Therefore, s is invertible in R. Because $\sigma(s) = s \; \forall \sigma \in G$, it follows $\sigma(s^{-1}) = s^{-1} \; \forall \sigma \in G$, so $s^{-1} \in R^G$ and therefore $\frac{r}{s} \in R^G$.

7.3 A normality criterion

Let R be a ring and assume there exists an element $0 \neq a \in R$, such that

(i) a is not a zero divisor,

(ii) the ideal (a) is a radical ideal,

(iii) the localizaiton R_a is a normal domain.

Prove that R is a normal integral domain.

We first show that R is an integral domain. Let $x, y \in R$ with $x \cdot y = 0$. Thus $\frac{x}{1} \cdot \frac{y}{1} = \frac{xy}{1} = 0$ and because R_a is an integral domain, this implies $a^k \cdot x = 0$ or $a^k \cdot y = 0$ for some $k \in \mathbb{N}_{>0}$. We conclude that $x = 0$ or $y = 0$, because a (and thus a^k for any $k \in \mathbb{N}_{>0}$) is not a zero divisor.
It is left to show that R is normal. First notice $\mathrm{Quot}(R_a) = \mathrm{Quot}(R)$, because a is not a zero-divisor. Let $r \in \mathrm{Quot}(R)$ be integral over R. In particular, r is integral over R_a, which is normal, so $r = \frac{p}{a^k}$ with $p \in R, k \in \mathbb{N}$. If $k = 0$, then $r = p \in R$, so suppose $k > 0$. The integral equation yields the existence of $b_i \in R$, $n \in \mathbb{N}_{>0}$, such that

$$\frac{p^n}{a^{kn}} + b_1 \frac{p^{n-1}}{a^{k(n-1)}} + \cdots + b_{n-1} \frac{p}{a^k} + b_n = 0$$

and multiplying with a^{kn} yields

$$p^n + \underbrace{b_1 a^k p^{n-1} + \cdots + b_{n-1} a^{k(n-1)} p + b_n a^{kn}}_{\in (a)} = 0.$$

Therefore, $p^n \in (a)$ and (a) is radical, implying $p \in (a)$. This means that there exists $p' \in R$ with $p = p'a$, so $r = \frac{p'}{a^{k-1}}$. Applying the previous argument iteratively (first to $r = \frac{p'}{a^{k-1}}$) shows $r = \frac{p^*}{a^0} = p^* \in R$.

7.4 Normalization of polynomials rings

Let R be a Noetherian integral domain. The goal of this exercise is to prove that $\tilde{R}[x] = \tilde{R[x]}$. Proceed in the following steps:

(a) Show $\tilde{R}[x] \subset \tilde{R[x]}$.

(b) For $f \in \tilde{R[x]}$, show that there is $u \in R \setminus \{0\}$, such that $uf^k \in R[x]$ for all $k \in \mathbb{N}$.

(c) Using (b), prove $\tilde{R[x]} \subset \tilde{R}[x]$.

(a) For $a \in \tilde{R}$ with integral equation $f \in R[x]$, f is also an integral equation in $(R[y])[x]$ (with y-degree 0), so $\tilde{R} \subset R\tilde{[}x]$. By definition, $x \in R\tilde{[}x]$ and because $\tilde{R}[x]$ is an $\tilde{R}$-algebra generated by x, this implies $\tilde{R}[x] \subset R\tilde{[}x]$.

(b) With $K \coloneqq \mathrm{Quot}(R)$, it holds $R\tilde{[}x] \subset K\tilde{[}x] = K[x]$. Thus, for every $k \in \mathbb{N}$, there is $u_k \in R \setminus \{0\}$ with $u_k f^k \in R[x]$. Consider the finitely generated $R[x]$-algebra $(R[x])[f]$. Because f is integral over $R[x]$, $(R[x])[f]$ is finitely generated as an $R[x]$-module by lemma 8.3. These generators can be written as polynomials with coefficients in $R[x]$ and "variable" f. Let n denote the highest power of f occuring in these polynomials. Then every element in $(R[x])[f]$ is an $R[x]$-linear combination of $\{1, f, f^2, \ldots, f^n\}$. Since $f^k \in (R[x])[f]$ for every $k \in \mathbb{N}$, $u \coloneqq \prod_{i=1}^{n} u_i$ satsifies the desired property.

(c) Let $f \in R\tilde{[}x]$ and $u \in R \setminus \{0\}$ as in (b). Write $f = \sum_{i=0}^{n} a_i x^i$ with $a_i \in K$. Because the coefficient of x^{nk} in f^k is a_n^k, it holds $u a_n^k \in R$ for every $k \in \mathbb{N}$, so a_n is almost integral over R. Because R is Noetherian, lemma 8.11 implies that a_n is integral over R, i.e. $a_n \in \tilde{R}$. In particular, $a_n x^n \in \tilde{R}[x] \subset R\tilde{[}x]$, so considering $f' \coloneqq \sum_{i=0}^{n-1} a_i x^i \in R\tilde{[}x]$ and applying the argument iteratively yields the claim.

7.5 Integral extension of a Jacobson ring

Let $R \subset S$ be an integral ring extension and R a Jacobson ring. Prove that this implies that S is also Jacobson.
Hint: Use that a ring is Jacobson if and only if every prime ideal is an intersection of maximal ideals.

Let $I \in \mathrm{Spec}(S)$. Then $J \coloneqq R \cap I \in \mathrm{Spec}(R)$ and because R is a Jacobson ring, it holds

$$J = \bigcap_{m \in \mathrm{Spec}_{\max}(R), J \subset m} m.$$

Applying theorem 8.12 with $P = m$, $I = I$, it follows the existence of $Q_m \in \mathrm{Spec}(S)$ with $R \cap Q_m = m$ and $I \subset Q_m$.
We claim that Q_m is maximal. Suppose $Q_m \subset Q$ with $Q \in \mathrm{Spec}(S)$. Then $R \cap Q \supset R \cap Q_m = m$ and because $R \cap Q \in \mathrm{Spec}(R)$, it follows $R \cap Q = m$ by maximality of m. Additionally, $I \subset Q_m \subset Q$, so 8.12(b) implies $Q_m = Q$, so Q_m is maximal.
It follows with $Q \coloneqq \bigcap_{m \in \mathrm{Spec}_{\max}(R), J \subset m} Q_m$

$$R \cap Q = \bigcap_{m \in \mathrm{Spec}_{\max}(R), J \subset m} (R \cap Q_m) = \bigcap_{m \in \mathrm{Spec}_{\max}(R), J \subset m} m = J = R \cap I.$$

Clearly,

$$I \subset \bigcap_{n \in \mathrm{Spec}_{\max}(S), I \subset n} n \subset Q,$$

so it is left to show $Q \subset I$.
If Q was prime, then we could conclude by 15. Therefore, we want to find a prime ideal containing Q, and then apply the claim. Theorem 8.12 yields for $P = J$, $I = Q$ the

existence of $Q' \in \mathrm{Spec}(S)$, such that $R \cap Q' = J$ and $Q \subset Q'$. Now I and Q' are prime ideals in S with $R \cap Q' = J = R \cap I$ and $I \subset Q \subset Q'$, so 15 implies $I = Q'$ and we conclude $I = Q$.

7.6 Examples of Noether normalization

For a given field K and K-algebra R, find algebraically independent elements $a_1, \ldots, a_n \in R$, such that R is integral over $K[a_1, \ldots, a_n]$.

(a) $K = \mathbb{R}$, $R = \mathbb{R}[x, y]/(x^2 + y^2 - 1)$,

(b) $K = \mathbb{F}_2$, $R = \mathbb{F}_2[w, x, wy + y^2, wz + xy, xz + z^2] \subset \mathbb{F}_2[w, x, y, z]$.

By theorem 8.19, $n \in \mathbb{N}$ is the Krull dimension of R.

(a) Clearly $\dim(R) \leq 1$. Since x^2+y^2-1 is prime and $x^2+y^2-1 = x^2+(y-1)(y+1)$, it follows $(x^2 + y^2 - 1) \subsetneq (x, y - 1)$ and $(x, y - 1)$ is maximal, so $\dim(R) = 1$.
Consider $a_1 = x$. It is algebraically independent and integral over K, since $x^2 + y^2 - 1 = 0$.

(b) Since $y^2 + wy = 0$ and $z^2 + zx = 0$, $\mathbb{F}_2[w, x, y, z]$ is integral over R, implying $\dim(R) = \dim(\mathbb{F}_2[w, x, y, z]) = 4$.
Let $a_1 = w$, $a_2 = x$, $a_3 = wy + y^2$ and $a_4 = xz + z^2$. Let $f \in \mathbb{F}_2[a, b, c, d]$ be a polynomial in four indeterminants, such that $f(a_1, a_2, a_3, a_4) = 0$. Comparing y-degrees, it follows that $f \in \mathbb{F}_2[a, b, d]$, but a_1, a_2, a_4 are algebraically independent, so f is zero and all the a_i are algebraically independent. They are also integral over $\mathbb{F}_2[a_1, a_2, a_3, a_4]$, because

$$(wz + xy)^2 + a_1 a_2 (wz + xy) + (a_1^2 a_4 + a_2^2 a_3) = 0.$$

7.7 Where going down fails

Going down holds for a ring extension $R \subset S$ if for every $P \in \mathrm{Spec}(R)$ and every $Q' \in \mathrm{Spec}(S)$ with $P \subset Q'$, there exists $Q \in \mathrm{Spec}(S)$ with $Q \subset Q'$ and $R \cap Q = P$. In this exercise, we find an example of an integral extension of rings in which going down fails.
Let K be a field of characterstic $\neq 2$, $S = K[x, y]$ the polynomial ring in two indeterminants, and

$$R = K[a, b, y] \subset S \quad \text{with} \quad a = x^2 - 1 \quad \text{and} \quad b = xa.$$

(a) Prove that S is the normalization of R.

(b) Show that

$$P \coloneqq (a - (y^2 - 1), b - y(y^2 - 1))_R \subset R$$

is a prime ideal and that P is contained in the prime ideal

$$Q' \coloneqq (x - 1, y + 1)_S \in \mathrm{Spec}(S).$$

(c) Show that the unique ideal $Q \in \mathrm{Spec}(S)$ with $R \cap Q = P$ is $Q \coloneqq (x - y)_S$ and conclude that going down fails for the inclusion $R \hookrightarrow S$.

(a) S is integral over R, because x is integral over R by

$$x^2 - 1 - a = 0.$$

As a factorial ring, S is normal and $\mathrm{Quot}(R) \subset \mathrm{Quot}(S)$, so $\tilde{R} = S$.
Alternatively, notice that $R' \coloneqq K[a, b]$ is Noetherian and an integral domain. By exercise 7, it is left to show that $K[x]$ is the normalization of R'. Since $R' \subset K[x]$, it is clear that $\tilde{R'} \subset K[x] = \tilde{K[x]}$. Also $a \neq 0$, so $x = b \cdot a^{-1}$ and therefore $K[x] \subset \tilde{R'}$.

(b) Consider the inclusion map $\phi : R \to S$ and the K-algebra homomorphism

$$\phi' : S \to K[x],\ x \mapsto x,\ y \mapsto x.$$

Then $\psi \coloneqq \phi' \circ \phi : R \to K[x]$ is a surjective homomorphism with kernel P. It follows that $R/P \cong K[x]$, so P is prime.
Clearly, $x^2 - 1 \in Q'$ and $y^2 - 1 \in Q'$, so $a - (y^2 - 1) \in Q'$.
Moreover,

$$x^3 - x = (x^2 - 1)(x - 1) + (x^2 - 1) \in Q',$$
$$y^3 - y = (y^2 - 1)(y + 1) - (y^2 - 1) \in Q',$$

so $b - y(y^2 - 1) \in Q'$ and we conclude $P \subset Q'$.

(c) We first prove uniqueness. Let $Q \in \mathrm{Spec}(S)$ with $R \cap Q = P$. By theorem 8.12, it is enough to show that every such Q has to contain $(x - y)_S$. Since $x^2 - y^2 \in Q$, it follows $x - y \in Q$ or $x + y \in Q$. Assume for contradiction that $x + y \in Q$. Because $(x^3 - x) - (y^3 - y) \in Q$, subtracting $x^2(x + y) \in Q$ and adding $y^2(x + y) \in Q$ yields

$$-x^2y + y^2x - x + y = -x(xy - 1) + y(yx + 1) = -(xy + 1)(x - y) \in Q.$$

By assumption and because Q is prime, it follows $(xy+1) \in Q$. Because Q is prime, $K[x,y]/Q$ is an integral domain. Additionally, $K[x,y]/Q$ is algebraic over K, because $x = -y \bmod Q$ and $xy+1 \in Q$. Lemma 1.1(a) implies that $K[x,y]/Q$ is a field, so Q is maximal. But by proposition 1.2, this means that $R \cap Q = P$ is also maximal, which it is not. Contradiction.
It is left to show that $Q = (x-y)_S$ satisfies $R \cap Q = P$. With the same notation as in (b), this follows from $\ker(\phi') = Q$ and

$$R \cap Q = \phi^{-1}(\ker(\phi')) = \ker(\psi) = P.$$

This shows that going down fails for the inclusion $R \hookrightarrow S$: For P and Q' as in (b), there is no $Q \in \operatorname{Spec}(S)$ with $Q \subset Q'$ and $R \cap Q = P$, because the only candidate is $Q \coloneqq (x-y)_S$ by (c), but clearly Q is not a subset of Q'.

7.8 Examples of Hilbert functions

For a field K and each of the following ideals I in a polynomial ring over K, determine the Hilbert function h_I.

(a) $I = (y^2 - x(x^2+1)) \subset K[x,y]$,

(b) $I = (x^2 - yz) \subset K[x,y,z]$,

(c) $I = (x^4, x^2y^2, y^4) \subset K[x,y]$.

One solution for (a) and (b) is to apply 16 and calculate the result. The following presents an alternative solution by explicitly determining the basis of $A_{\leq d}$.

(a) Clearly

$$B_d \coloneqq \left\{1, y, \dots y^d, x, xy, \dots, xy^{d-1}, x^2, x^2y, \dots, x^2y^{d-2}\right\}$$

is a linearly independent subset of $A_{\leq d}$.
Moreover, $x^3 = y^2 - x$ in $K[x,y]/I$ and iteratively $x^{i+3} = x^iy^2 - x^{i+1}$, so B_d is in fact a basis of $A_{\leq d}$. Therefore, h_I is given by

$$h_I : \mathbb{N} \to \mathbb{N},\ 0 \mapsto 1,\ 1 \mapsto 3,\ 2 \leq d \mapsto |B_d| = 3d.$$

(b) Similarly to (a), a basis of $A_{\leq d}$ is given by

$$B_d \coloneqq \left\{y^iz^j : i+j \leq d\right\} \cup \left\{xy^iz^j : i+j \leq d-1\right\}.$$

The monomials without x account for $\frac{(d+1)(d+2)}{2}$ elements and the monomials with x for $\frac{d(d+1)}{2}$ element, so $h_I(d) = |B_d| = (d+1)^2$.

(c) Notice that $\dim(K[x,y]/I) = 0$, because every prime ideal in $K[x,y]/I$ has to contain (x,y), which is already maximal. This implies that the polynomial to be determined has to be constant.
Moreover, $A_{\leq d} = A_4$ for $d \geq 4$, because a monomial of degree 5 or higher has

to be dividable by x^4, y^4 or x^2y^2. Using this, we derive the following bases and corresponding values of the Hilbert function:

$$\begin{aligned} 0 &: \{1\} && h_I(0) = 1 \\ 1 &: \{1, x, y\} && h_I(1) = 3 \\ 2 &: \{1, x, x^2, y, y^2, xy\} && h_I(2) = 6 \\ 3 &: \{1, x, x^2, x^3, y, y^2, y^3, xy, x^2y, xy^2\} && h_I(3) = 10 \\ \geq 4 &: \{1, x, x^2, x^3, y, y^2, y^3, xy, x^2y, xy^2, x^3y, xy^3\} && h_I(d \geq 4) = 12 \end{aligned}$$

7.9 Integral over $\mathbb{Z}$?

Decide for each of the following complex numbers whether it is integral over $\mathbb{Z}$ or not:

$$\text{(a)} \ \frac{1}{2+\sqrt{3}}, \quad \text{(b)} \ \frac{1-\sqrt{5}}{4}, \quad \text{(c)} \ \frac{3+2\sqrt{6}}{1-\sqrt{6}}.$$

(a) Since $\frac{1}{2+\sqrt{3}} = \frac{2-\sqrt{3}}{4-3} = 2-\sqrt{3}$ and $(2-\sqrt{3})^2 = 7-4\sqrt{3}$, an integral equation for $\frac{1}{2+\sqrt{3}}$ is given by $x^2 - 4x + 1 \in \mathbb{Z}[x]$.

(b) Suppose for contradiction that $\frac{1+\sqrt{5}}{2}$ was integral over $\mathbb{Z}$, i.e. there are $a_i \in \mathbb{Z}$, such that

$$\left(\frac{1-\sqrt{5}}{4}\right)^n + a_1\left(\frac{1-\sqrt{5}}{4}\right)^{n-1} + \cdots + a_{n-1}\frac{1-\sqrt{5}}{4} + a_n = 0,$$

so

$$\left(1-\sqrt{5}\right)^n + 4a_1\left(1-\sqrt{5}\right)^{n-1} + \cdots + 4^{n-1}a_{n-1}(1-\sqrt{5}) + 4^n a_n = 0.$$

Notice that the terms of $\left(1-\sqrt{5}\right)^n$ lying in $\mathbb{Z}$ are even in $1+5\mathbb{Z}$. Because 1 and $\sqrt{5}$ are $\mathbb{Z}$-linearly independent, all the terms in the previous equation, which lie in $\mathbb{Z}$, are divisible by 2, except for 1. But 2 divides 0, so this is a contradiction.
Alternatively, recall that $\frac{1+\sqrt{5}}{2}$ is integral over $\mathbb{Z}$. If $\frac{1-\sqrt{5}}{4}$ was integral over $\mathbb{Z}$, then $\frac{1-\sqrt{5}}{4} \cdot \frac{1+\sqrt{5}}{2} = \frac{-4}{8} = -\frac{1}{2}$ was integral over $\mathbb{Z}$ as well. But $\mathbb{Z}$ is normal, so $-\frac{1}{2} \in \mathbb{Q}$ can not be integral over $\mathbb{Z}$.

(c) Because

$$\frac{3+2\sqrt{6}}{1-\sqrt{6}} = \frac{(3+2\sqrt{6})(1+\sqrt{6})}{-5} = -\sqrt{6} - 3,$$

it is integral over $\mathbb{Z}$, because $\sqrt{6}$ and 3 are integral over $\mathbb{Z}$.

7.10 Unit groups of integral ring extensions

Let $R \subset S$ be an integral ring extension. Prove for the unit group $R^\times$ that $R^\times = S^\times \cap R$.

It is clear that $R^\times \subset S^\times \cap R$. On the other hand, let $r \in S^\times \cap R$, so there is $s \in S$ with $r \cdot s = 1$. Because S is integral over R, there are $a_i \in R$ and $n \in \mathbb{N}_{>0}$, such that

$$s^n + a_1 s^{n-1} + \cdots + a_{n-1} s + a_n = 0$$

and multiplying by r^{n-1} yields

$$s + a_1 + \cdots + a_{n-1} r^{n-2} + a_n r^{n-1} = 0,$$

so $s \in R$.

7.11 Example of an integral closure

Determine the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{11})$.

We claim that the integral closure R is $S \coloneqq \mathbb{Z}[\sqrt{11}]$. Because $\sqrt{11}$ is integral over $\mathbb{Z}$, S is integral over $\mathbb{Z}$, implying $S \subset R$. Since S is factorial, it is normal and $\mathrm{Quot}(S) = \mathbb{Q}(\sqrt{11})$, so $S = R$.

7.12 Right or Wrong?

Decide whether each of the following statements is true or false.

(a) Let K be a finite field and let X be a set. Then the ring $S \coloneqq \{f : X \to K : f \text{ is a function}\}$ with pointwise operations is an integral extension of K, which is embedded into S as the ring of constant functions.

(b) If $R \subset S$ is an integral ring extension, then for every $P \in \mathrm{Spec}(R)$ the set $\{Q \in \mathrm{Spec}(S) : R \cap Q = P\}$ is finite.

(a) True. Denote $K = \{k_1, \ldots, k_n\}$. For $f \in S$, an integral equation is given by $\prod_{i=1}^n (x - k_i) \in S[x]$. Alternatively, notice that $f^{|K|} - f = 0$.

(b) False. For a finite field K and an infinite set X, consider $S \coloneqq \{f : X \to K : f \text{ is a function}\}$ as in (a). For $x \in X$, the maximal ideal $I_x \coloneqq \{f \in S : f(x) = 0\}$ satisfies $K \cap I_x = (0)$, so $P = (0) \in \mathrm{Spec}(K)$ provides a counterexample.

Dimension Theory

Remark 17. (a) Let $I \subset K[x_1, \ldots, x_n]$ be an ideal and $A = K[x_1, \ldots, x_n]/I$. For each $f \in I \setminus \{0\}$, the **initial form** f_{in} of f is defined to be the nonzero homogeneous component of f of least degree. The **initial form ideal** is defined as

$$I_{\text{in}} \coloneqq (f_{\text{in}} : f \in I \setminus \{0\}) \subset K[x_1, \ldots, x_n]$$

and the affine variety $V(I_{\text{in}})$ is called the **tangent cone** of $V(I)$.

(b) The $(\cdot)_{\text{in}}$ operator does not behave well with respect to addition. More precisely, the function

$$(\cdot)_{\text{in}} : I \to I, \ f \mapsto f_{\text{in}}$$

is generally not a group homomorphism (defining $0_{\text{in}} \coloneqq 0$). For example, consider $I = K[x] \subset K[x]$ and notice $((x + x^2) + (-x))_{\text{in}} = (x^2)_{\text{in}} = x^2$, but $(x + x^2)_{\text{in}} + (-x)_{\text{in}} = x - x = 0$.
Moreover, it also generally does not hold that $I_{\text{in}} = ((f_1)_{\text{in}}, \ldots, (f_n)_{\text{in}})$ for $I = (f_1, \ldots, f_n)$ finitely generated. An example is given by $I \coloneqq (x + y^2, x) \subset K[x, y]$, because $y^2 \in I_{\text{in}}$, but $((x + y^2)_{\text{in}}, (x)_{\text{in}}) = (x)$.

(c) Let R be a ring with an ideal $I \subset R[x]$. It generally does not hold

$$R[x]/I \cong (R/(R \cap I))[x].$$

For example, consider $R = \mathbb{C}$ and $I = (x - 1)$. Then $R[x]/I \cong \mathbb{C}$ and $(R/(R \cap I))[x] \cong \mathbb{C}[x]$.

Lemma 18. Let $m \subset R$ be a maximal ideal of a ring R. For any $u \in R \setminus m$, there exists $r \in R$, such that $ru + 1 \in m$. Moreover, there exists $r' \in R$, such that $r'u - 1 \in m$.

Proof. Since $m \subsetneq (m, u)$, the maximality of m yields the existence of $a \in m$, $r \in R$, such that $a + ru = 1$, so $(-r)u + 1 \in m$, proving the first claim. The second follows from the first by multiplying with -1. □

Lemma 19. Consider the ideal $I \coloneqq K[x_1, \ldots, x_n] \subset K[x_1, \ldots, x_n]$ with initial ideal I_{in}. The function

$$(\cdot)_{\text{in}} : K[x_1, \ldots, x_n]^\times \to K[x_1, \ldots, x_n]^\times, \ f \mapsto f_{\text{in}}$$

is a group homomorphism. In particular, for any multiplicative subgroup $M \subset K[x_1, \ldots, x_n]$ (e.g. the unit group of a subring or an ideal), a group homomorphism is given by

$$(\cdot)_{\text{in}} : M \to K[x_1, \ldots, x_n]^\times, \ f \mapsto f_{\text{in}}.$$

Proof. For two monomials $f, g \in K[x_1, \ldots, x_n] \setminus \{0\}$, it holds $\deg(f) \cdot \deg(g) = \deg(f + g)$, so for arbitrary $f, g \in K[x_1, \ldots, x_n] \setminus \{0\}$, the nonzero homogeneous component of $f \cdot g$ of least degree is precisely $f_{\text{in}} \cdot g_{\text{in}}$. □

Lemma 20. Let $I \subset K[x_1, \ldots, x_n]$ be an ideal with initial ideal I_{in}. If $I = (f)$ is a principal ideal, then $I_{\text{in}} = (f_{\text{in}})$.

Proof. Let $g \in I \setminus \{0\}$, so $g = f \cdot h$ for some $h \in K[x_1, \ldots, x_n] \setminus \{0\}$. By 19, $g_{\text{in}} = f_{\text{in}} \cdot h_{\text{in}}$, so $g_{\text{in}} \in (f_{\text{in}})$. By definition of I_{in}, this implies $I_{\text{in}} \subset (f_{\text{in}})$.
On the other hand, it is clear that $f_{\text{in}} \in I_{\text{in}}$, so $(f_{\text{in}}) \subset I_{\text{in}}$. □

Lemma 21. Let R be a ring with $I \subset R$ an ideal. Then $(I)_{R[x]} \cap R = I$.

Proof. Clearly, $I \subset (I)_{R[x]} \cap R$.
On the other hand, let $f = \sum_{i=1}^{n} g_i a_i \in (I)_{R[x]} \cap R$ with $g_i = \sum_{j=0}^{m_i} r_{i,j} x^j \in R[x]$ and $a_i \in I$. It follows

$$f = \sum_{i=1}^{n} \left(\sum_{j=0}^{m_i} r_{i,j} x^j \right) a_i = \sum_{i=1}^{n} r_{i,0} a_i + x \cdot h$$

for some $h \in R[x]$. Because $f \in R$, it follows $f = \sum_{i=1}^{n} r_{i,0} a_i \in I$. □

8.1 Noetherian integral domain of Krull-dimension 1

Let R be a Noetherian integral domain with $\dim(R) = 1$. Prove that the map

$$\phi : \text{Quot}(R)^\times \to \mathbb{Z},\ \frac{p}{q} \mapsto \text{length}(R/(p)) - \text{length}(R/(q))$$

is a homomorphism of group. Proceed as follows:

(a) Prove first that $d(a) \coloneqq \text{length}(R/(a)) < \infty$ for every $a \in R \setminus \{0\}$.

(b) Next, prove that $d(ab) = d(a) + d(b)$ for every $a, b \in R \setminus \{0\}$.

(c) Finally, prove that ϕ is a well-defined group homomorphism.

(a) Notice that it does not matter for the length whether one views $R/(a)$ as a module over itself or as an R-module, since the submodules coincide in both cases.
Every nonzero prime ideal in R is maximal, because R is an integral domain and $\dim(R) = 1$. In particular, $\dim(R/(a)) = 0$ for $a \in R \setminus \{0\}$ and because R is Noetherian, so is $R/(a)$. By theorem 2.8, $R/(a)$ is Artinian, thus theorem 12.3(b) shows that $R/(a)$ has finite length.

(b) Consider the surjective homomorphism

$$\phi : R/(ab) \to R/(b),\ x + (ab) \mapsto x + (b)$$

with kernel $(b)/(ab)$. It follows $R/(ab) \big/ (b)/(ab) \cong R/(b)$ by the homomorphism theorem and theorem 12.3(c) shows that $d(ab) = \text{length}((b)/(ab)) + d(b)$. The R-module homomorphism

$$R \to R/(ab),\ r \mapsto rb + (ab)$$

consisting of first multiplying by b and then the projection onto $R/(ab)$ has image $(b)+(ab)$ and kernel (a), implying $R/(a) \cong (b)/(ab)$ and thus showing the assertion.

(c) We first show that ϕ is well defined, so let $\frac{p}{q} = \frac{p'}{q'} \in \mathrm{Quot}(R)^\times$, i.e. $pq' = p'q$. By (b), this implies $d(p) + d(q') = d(p') + d(q)$. It follows

$$\phi\left(\frac{p}{q}\right) = d(p) - d(q) = d(p') - d(q') = \phi\left(\frac{p'}{q'}\right).$$

By (a), the image of ϕ lies in $\mathbb{Z}$, so ϕ is well-defined.
To show that ϕ is a group homomorphism, we take $\frac{p}{q}, \frac{p'}{q'} \in \mathrm{Quot}(R)^\times$ and calculate using (b):

$$\phi\left(\frac{p}{q} \cdot \frac{p'}{q'}\right) = d(pp') - d(qq') = d(p) + d(p') - d(q) - d(q') = \phi\left(\frac{p}{q}\right) + \phi\left(\frac{p'}{q'}\right).$$

8.2 Length and exact sequences

Let R be a ring and

$$\{0\} \xrightarrow{\phi_0} M_1 \xrightarrow{\phi_1} M_2 \xrightarrow{\phi_2} \cdots \xrightarrow{\phi_{n-2}} M_{n-1} \xrightarrow{\phi_{n-1}} M_n \xrightarrow{\phi_n} \{0\}$$

an exact sequence of R-modules. Assume that $\mathrm{length}(M_i) < \infty$ for all $i \in \{1, \ldots, n\}$. Prove that

$$\sum_{i=1}^{n} (-1)^i \,\mathrm{length}(M_i) = 0.$$

We use induction on the length of the exact sequence n.
Base case: For $n = 1$, it holds $M_1 = 0$, since $\phi_0 = \phi_{n-1}$ has to be surjective. Since $M_1 = 0$, the assertion is clear.
Inductive step: Since ϕ_{n-1} is surjective, it holds

$$M_n \cong M_{n-1}/\ker(\phi_{n-1}) = M_{n-1}/\mathrm{im}(\phi_{n-2}),$$

which implies

$$\mathrm{length}(M_{n-1}) = \mathrm{length}(M_n) + \mathrm{length}(\mathrm{im}(\phi_{n-2})). \qquad (*)$$

Now let $n \geq 2$ and assume that the claim holds for $n - 1$. Consider the exact sequence of length $n - 1$

$$\{0\} \xrightarrow{\phi_0} M_1 \xrightarrow{\phi_1} M_2 \xrightarrow{\phi_2} \cdots \xrightarrow{\phi_{n-2}} \mathrm{im}(\phi_{n-2}) \xrightarrow{0} \{0\}.$$

By the inductive hypothesis and $(*)$, it follows

$$0 = \sum_{i=1}^{n-2} (-1)^i \,\mathrm{length}(M_i) + (-1)^{n-1} \,\mathrm{length}(\mathrm{im}(\phi_{n-2})) = \sum_{i=1}^{n} (-1)^i \,\mathrm{length}(M_i).$$

8.3 Easier computation of the Hilbert–Samuel function

Let $m \subset R$ be a maximal ideal of a ring R and consider the localization R_m with maximal ideal m_m. Show that for every $i \in \mathbb{N}$, there is an isomorphism

$$m_m^i/m_m^{i+1} \cong m^i/m^{i+1}$$

of R-modules. With $K \coloneqq R/m \cong R_m/m_m$, show that the isomorphism is K-linear, so $\dim_K(m_m^i/m_m^{i+1}) = \dim_K(m^i/m^{i+1})$.

First notice that $(m^i)_m = (m_m)^i$, i.e. the order does not matter.
For $i \in \mathbb{N}$, consider the R-module homomorphism

$$\phi : m^i \xrightarrow{\epsilon} m_m^i \twoheadrightarrow m_m^i/m_m^{i+1},$$

where $\epsilon : m^i \to m_m^i, a \mapsto \frac{a}{1}$ is the canonical map. We claim that the kernel of ϕ is m^{i+1}. It is clear that $m^{i+1} \subset \ker(\phi)$. For the other direction, let $x \in \ker(\phi)$, i.e. $\frac{x}{1} \in m_m^{i+1}$. This means that there exist $p \in m^{i+1}$, $u \in R \setminus m$, such that $\frac{x}{1} = \frac{p}{u}$, so for some $u' \in R \setminus m$, it holds $u'ux = u'p$. By 18, there exists $r \in R$ and $a \in m$, such that $ru'u - 1 = a$, so

$$x = x \cdot 1 = x \cdot (ru'u - a) = ru'p - xa \in m^{i+1}.$$

Moreover, ϕ is surjective: Let $y \coloneqq \frac{\prod_{j=1}^i a_j}{u} + m_m^{i+1} \in m_m^i/m_m^{i+1}$ with $a_j \in m$, $u \in R \setminus m$. Since every element in m_m^i/m_m^{i+1} is a finite sum of elements of the form of y, it is enough to show that there is $x \in m^i$, such that $\phi(x) = y$. By definition, $\phi(x) = y$ is equivalent to

$$\frac{ux - \prod_{j=1}^i a_j}{u} = \frac{x}{1} - \frac{\prod_{i=1}^i a_i}{u} \in m_m^{i+1}.$$

Try $x = z \cdot \prod_{j=1}^i a_j \in m^i$ with $z \in R$. Then we need to find $z \in R$, such that $uz - 1 \in m$. The existence of such a z is guaranteed by 18, so ϕ is indeed surjective.
By the homomorphism theorem, there is an isomorphism of R-modules $m^i/m^{i+1} \cong m_m^i/m_m^{i+1}$.
That the isomorphism is R/m-linear can either be checked directly or can be seen in a more general setting: Consider the full subcategory $\mathcal{C}$ of the category of R-modules, consisting only of those R-modules M, which satisfy $m \subset \mathrm{Ann}(M)$. Denote the category of R/m-vector spaces as $\mathcal{D}$. Then there is a functor $F : \mathcal{C} \to \mathcal{D}$, which maps an R-module with $m \subset \mathrm{Ann}(M)$ to the R/m vector space with the same underlying abelian group and scalar multiplication given by $k \cdot x \coloneqq r \cdot x$ for $k = r + m \in R/m$, $r \in R$, $x \in M$. An R-module homomorphism $f : M \to N$ becomes R/m-linear, since for $k = r + m \in R/m$, $r \in R$, $x \in M$, it holds

$$f(k \cdot x) = f(r \cdot x) = rf(x) = kf(x).$$

This declares the action of F on morphisms and at the same time proves the claim.

8.4 Associated graded ring and tangent cone

Let $I \subset K[x_1, \ldots, x_n]$ be an ideal and $A = K[x_1, \ldots, x_n]/I$ with initial form ideal I_{in}. Assume that $I \subset (x_1, \ldots, x_n) =: n$ and set $m := n/I$, which is a maximal ideal in A. It can be shown that there is an isomorphism

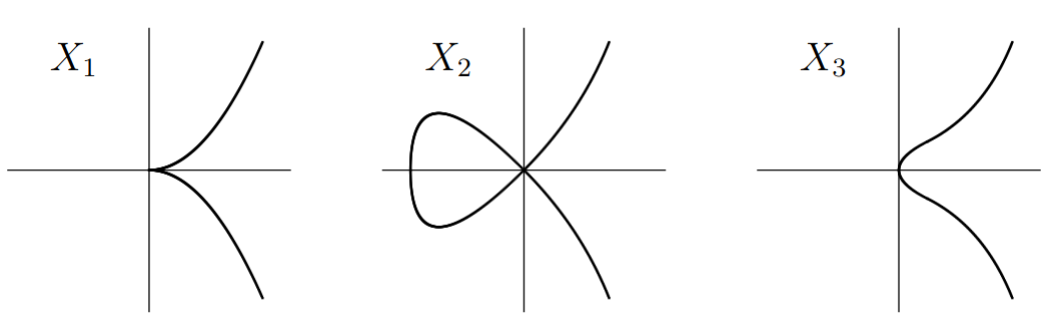
$$K[x_1, \ldots, x_n]/I_{\text{in}} \cong \text{gr}(A_m),$$

which sends homogeneous elements to homogeneous elements of the same degree. You may use this result without a proof.
Determine the associated graded ring of the localization $R_i := \mathbb{C}[X_i]_{(0,0)}$ of the coordinate ring at the origin for the following affine varieties $X_i \subset \mathbb{C}^2$:

(a) $X_1 = V(x_1^3 - x_2^2)$,

(b) $X_2 = V(x_2^2 - x_1^2(x_1 + 1))$,

(c) $X_3 = V(x_2^2 - x_1(x_1^2 + 1))$.



For an affine variety $X \subset \mathbb{C}^2$, denote the corresponding ideal with $I := I(X)$ and set $A := \mathbb{C}[X] = \mathbb{C}[x, y]/I$. With $m = I(\{0, 0\})/I = (x + I, y + I) \subset A$ and $R := A_m = \mathbb{C}[X]_{(0,0)}$, the hint shows that $\mathbb{C}[x, y]/I_{\text{in}} \cong \text{gr}(R)$, so in order to calculate $\text{gr}(R)$, it is enough to determine I_{in}. If $I = (f)$ is principal, it holds $I_{\text{in}} = (f_{\text{in}})$ by 20.
This will be used in the following.

(a) It holds $I = (x_1^3 - x_2^2)$, so $I_{\text{in}} = (x_2^2)$ and $\text{gr}(R_1) \cong \mathbb{C}[x_1, x_2]/(x_2^2)$.

(b) It holds $I = (x_2^2 - x_1^2 + x_1^3)$, so $I_{\text{in}} = (x_1^2 - x_2^2)$ and $\text{gr}(R_2) \cong \mathbb{C}[x_1, x_2]/(x_1^2 - x_2^2)$.

(c) It holds $I = (x_2^2 - x_1^3 - x_1)$, so $I_{\text{in}} = (x_1)$ and $\text{gr}(R_2) \cong \mathbb{C}[x_1, x_2]/(x_1) \cong \mathbb{C}[x]$.

8.5 Hypotheses of Krull's intersection theorem

Let $C^0(\mathbb{R},\mathbb{R})$ be the ring of all continuous (with respect to the Euclidean topology) functions $\mathbb{R}\to\mathbb{R}$ and consider the ideal

$$I \coloneqq \left\{ f \in C^0(\mathbb{R},\mathbb{R}) :\ \exists\, U \subset \mathbb{R} \text{ open} : 0 \in U, f|_U = 0 \right\}$$

with $R \coloneqq C^0(\mathbb{R},\mathbb{R})/I$.

(a) Prove that R is a local ring with maximal ideal

$$\mathfrak{m} \coloneqq \left\{ f + I : f \in C^0(\mathbb{R},\mathbb{R}), f(0) = 0 \right\}.$$

Hint: Recall that a ring S is local with maximal ideal $\mathfrak{n}$ if and only if every $x \in S \setminus \mathfrak{n}$ is invertible.

(b) Prove that there exists a nonzero element in R which lies in $\mathfrak{m}^n$ for every $n \in \mathbb{N}$.

(c) Is R Noetherian?

The equivalence classes in R of two functions $f, g \in C^0(\mathbb{R},\mathbb{R})$ are the same if and only if $f - g \in I$; i.e. if there is an open neighborhood around 0, such that f and g agree on it.

(a) We show that every $f \in R$ is invertible. Let $f + I \in R \setminus \mathfrak{m}$, i.e. $f(0) \neq 0$. Since f is continuous, there exists $\epsilon > 0$ such that $f(x) > 0$ for all $x \in [-\epsilon, \epsilon]$. The function

$$g : \mathbb{R} \to \mathbb{R},\ x \mapsto \begin{cases} f(-\epsilon) & x \leq -\epsilon \\ f(x) & x \in (-\epsilon, \epsilon) \\ f(\epsilon) & x \geq \epsilon \end{cases}$$

is continuous and satisfies $(f-g)|_{(-\epsilon,\epsilon)} = 0$, so $f - g \in I$ and $f + I = g + I$. Since $g(x) \neq 0$ for all $x \in \mathbb{R}$, g is invertible and thus the same holds for f.

(b) Clearly, $0 \neq |x| \in \mathfrak{m}$. Since $\sqrt[n]{|x|} \in \mathfrak{m}$ for all $n \in \mathbb{N}$, it follows $|x| \in \mathfrak{m}^n$ for every $n \in \mathbb{N}$.

(c) If R was Noetherian, then Krull's intersection Theorem would imply

$$\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n = \{0\},$$

which contradicts (b), so R is not Noetherian.

8.6 Polynomial ring over a regular ring

(a) Let R be a ring, $P \in \operatorname{Spec}(R)$ and $Q \coloneqq (P)_{R[x]}$. Prove that Q is a prime ideal with $\operatorname{ht}(P) \leq \operatorname{ht}(Q)$.

(b) Let R be a regular local ring with maximal ideal $\mathfrak{m}$ and let $P \subset R[x]$ be a prime ideal with $\mathfrak{m} \subset P$. Prove that the localization $R[x]_P$ is a regular local ring, as well.

(c) Let S be a Noetherian regular ring. Show that $S[x]$ is also regular.

(d) Prove that $\mathbb{Z}[x_1, \ldots, x_n]$ is regular for every $n \in \mathbb{N}$. So in particular, $\mathbb{Z}$ is regular.

(a) Consider the R-algebra homomorphism

$$\phi : R[x] \to (R/P)[x],\ x \mapsto x,$$

(it takes the coefficients of a polynomial mod P). It is surjective and has kernel Q, so $R[x]/Q \cong (R/P)[x]$ and we conclude that Q is prime.
Moreover, a chain of prime ideals in R of length n

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_{n-1} \subsetneq P_n = P$$

gives rise to a chain of prime ideals in $R[x]$ of the same length

$$(P_0)_{R[x]} \subsetneq (P_1)_{R[x]} \subsetneq \cdots \subsetneq (P_{n-1})_{R[x]} \subsetneq (P_n)_{R[x]} = (P)_{R[x]}$$

and the inclusions are strict by 21, thus $\operatorname{ht}(P) \leq \operatorname{ht}(Q)$.

(b) Let $n \coloneqq \operatorname{ht}(\mathfrak{m}) \in \mathbb{N}$ and $k \coloneqq \operatorname{ht}(P) \in \mathbb{N}$. We have to show that $P_P \subset R[x]_P$ can be generated by k elements and it is enough to prove the same statement for $P \subset R[x]$.
Because any regular ring is by definition Noetherian, corollary 7.13 implies that $\dim(R[x]) = \dim(R) + 1 = n + 1$. In particular, $k \leq \dim(R[x]) = n + 1$. By (a), $I \coloneqq (\mathfrak{m})_{R[x]} \subset R[x]$ is a prime ideal with $\operatorname{ht}(I) \geq n$. Since R is regular, $\mathfrak{m}$ is generated by n elements, and so is I. By corollary 7.6, this implies $\operatorname{ht}(I) \leq n$, so $\operatorname{ht}(I) = n$.
If $k = n$, then $P = I$ and P is generated by k elements. Therefore, we may assume $k = n + 1$. With the same isomorphism as in (a), we see $R[x]/I \cong (R/\mathfrak{m})[x]$. Since P/I is an ideal in $R[x]/I$ and $(R/\mathfrak{m})[x]$ is a principal ideal domain, P/I is generated by a single (irreducible) polynomial, so P is generated by $n + 1$ elements.

(c) Let $P \in \operatorname{Spec}(S[x])$, $I \coloneqq S \cap P \in \operatorname{Spec}(S)$ and $U \coloneqq S \setminus I$, which is a multiplicative submonoid of S and of $S[x]$. By proposition 6.3(g), it holds $S[x]_P \cong (S_I[x])_{U^{-1}P}$. Because S_I is local with maximal ideal I_I and $I_I \subset U^{-1}P$, (b) shows that $(S_I[x])_{U^{-1}P}$ is a regular local ring, so the same holds for $S[x]_P$.

(d) Let $P \in \operatorname{Spec}(\mathbb{Z})$. If $I = (0)$, then $\mathbb{Z}_P \cong \mathbb{Q}$, which is normal. Otherwise, $I = (p)$ for some $p \in \mathbb{Z}$ and $\operatorname{ht}(P) = 1$, $P_P = \left(\frac{p}{1}\right)$, showing that $\mathbb{Z}$ is regular.
By (c), $\mathbb{Z}[x]$ is regular and by iterating, the same follows for $\mathbb{Z}[x_1, \ldots, x_n]$.

8.7 Example of a singular locus

Determine the singular locus of the following affine varieties in $\mathbb{C}^2$.
(a) $\{(x, y) \in \mathbb{C}^2 : x^3 = y^2\}$.

(b) $\{(x, y) \in \mathbb{C}^2 : y^2 = x^2(x + 1)\}$.

We will use the Jacobian Criterion (theorem 13.10) and the notation from the lecture notes.

(a) We have $f = x^3 - y^2 \in \mathbb{C}[x, y]$ and $I = (f)$, which is prime, because f is irreducible. Thus $Q = I$ and $\mathrm{ht}(Q) = 1$ since $\{0\} \subsetneq Q \subsetneq (x, y)$ and $\dim(\mathbb{C}[x, y]) = 2$.
For $(a, b) \in \mathbb{C}^2$ with $f(a, b) = 0$, consider the maximal ideal $P = (x - a, y - b) \supset I$. Then

$$J_f = (3x^2 \quad -2y) \equiv (3a^2 \quad -2b) \mod P,$$

so $\mathrm{rank}(J_f \mod P) < \mathrm{ht}(Q)$ if and only if $(a, b) = (0, 0)$. Therefore, the singular locus is $\{(0, 0)\}$.

(b) Analogously to (a), let $f = x^2(x + 1) - y^2 \in \mathbb{C}[x, y]$ and $I = (f)$, which again is prime, so $Q = I$ with $\mathrm{ht}(Q) = 1$.
For $(a, b) \in \mathbb{C}^2$ with $f(a, b) = 0$, consider $P \coloneqq (x - a, y - b) \supset I$.
We calculate

$$J_f = \Big(x(3x + 2) \quad -2y\Big) \equiv \Big(a(3a + 2) \quad -2b\Big) \mod P,$$

so $\mathrm{rank}(J_f \mod P) < \mathrm{ht}(Q) = 1$ if and only if $(a, b) \in \{(0, 0), (-\frac{2}{3}, 0)\}$.
Since $f(-\frac{2}{3}, 0) \neq 0$, the singular locus amounts to $\{(0, 0)\}$.

8.8 Elliptic curves

Let K be an algebraically closed field of characterstic $\neq 2$ and take $a, b \in K$. Show that the cubic curve $E \subset K^2$ given by the equation

$$x_2^2 = x_1^3 + ax_1 + b$$

is nonsingular if and only if $4a^2 + 27b^2 \neq 0$.
The above equation is called *Weierstrass normal form* of a cubic curve. If E is nonsingular, then it is called an *elliptic curve*.

The polynomial $x_1^3 + ax_1 + b + x_2^2 \in K[x_1, x_2]$ is irreducible for every $a, b \in K$, so $K[E] = K[x_1, x_2]/(x_1^3 + ax_1 + b + x_2^2)$.
Let $f(x_1) = x_1^3 + ax_1 + b \in K[x_1]$ be a polynomial. By the Jacobian criterion, a point $(x, y) \in E$ is singular, if and only if $f'(x) = 0$ and $y = 0$. Thus E is singular if and only if there is $x \in K$ with $f(x) = f'(x) = 0$, which is equivalent to x being a double root of f. This, in turn, is equivalent to the discriminant being 0, which precisely amounts to the given equation.

8.9 Example of an associated graded ring

Find a well-known ring which is isomorphic to $\mathrm{gr}(\mathbb{Z}_{(p)})$.

$\mathbb{Z}_{(p)}$ is a Noetherian, local ring with maximal ideal $m \coloneqq (p)_{(p)}$.
One way to determine an isomorphic ring to $\mathrm{gr}(\mathbb{Z}_{(p)})$ is to look at its graded components. The d-th graded component $\mathrm{gr}(\mathbb{Z}_{(p)})_d$ is isomorphic as a group to m^d/m^{d+1}. By a previous exercise, $m^d/m^{d+1} \cong (p)^d/(p)^{d+1}$ as groups. Since the surjective group homomorphism

$$\mathbb{Z} \to (p)^d \twoheadrightarrow (p)^d/(p)^{d+1}, a \mapsto ap^d + (p)^{d+1}$$

has kernel (p), it follows $\mathrm{gr}(\mathbb{Z}_{(p)})_d \cong \mathbb{Z}/(p)$ as groups.
Alternatively, work with the group homomorphism

$$\mathbb{Z} \to m^d \twoheadrightarrow m^d/m^{d+1},\ a \mapsto \frac{p^d a}{1} \mapsto \frac{p^d a}{1} + m^{d+1}$$

and for bijectivity argue similarly to the proof of that exercise.
Therefore, $\mathrm{gr}(\mathbb{Z}_{(p)}) \cong \bigoplus_{d=0}^{\infty} \mathbb{Z}/(p)$ as groups (not as rings). Notice that $\bigoplus_{d=0}^{\infty} \mathbb{Z}/(p)$ is as a group isomorphic to $\mathbb{F}_p[x]$. The multiplication of $\mathrm{gr}(\mathbb{Z}_{(p)})$ is given for homogeneous elements $a + (m) \in \mathrm{gr}(\mathbb{Z}_{(p)})_i$, $b + (m) \in \mathrm{gr}(\mathbb{Z}_{(p)})_j$ by $a \cdot b \coloneqq ab + (m) \in \mathrm{gr}(\mathbb{Z}_{(p)})_{i+j}$ and this uniquely determines the ring structure of $\mathrm{gr}(\mathbb{Z}_{(p)})$. But the multiplication of homogeneous elements in $\mathbb{F}_p[x]$ works in the same way, suggesting $\mathrm{gr}(\mathbb{Z}_{(p)}) \cong \mathbb{F}_p[x]$ as rings.
More precisely, the group isomorphism $\mathbb{F}_p[x] \to \mathrm{gr}(\mathbb{Z}_{(p)})$, which maps a homogeneous element $ax^d \in \mathbb{F}_p x^d$ of degree d to $ap^d t^d \in m^d t^d + (m)$ is multiplicative on the homogeneous elements, so it is a ring isomorphism, showing $\mathrm{gr}(\mathbb{Z}_{(p)}) \cong \mathbb{F}_p[x]$.
In particular, we showed $\mathbb{Z}_{(p)}/(p)_{(p)} \cong \mathbb{F}_p$ as rings.
Alternatively, notice that $\mathbb{Z}_{(p)}[mt] = \mathbb{Z}_{(p)}[pt]$, so $\mathrm{gr}(\mathbb{Z}_{(p)}) = \mathbb{Z}_{(p)}[pt]/(m)_{\mathbb{Z}_{(p)}[pt]}$.
Intuitively, $pt + (m)_{\mathbb{Z}_{(p)}[pt]}$ acts as an inderminant; it is not transcendental over $\mathbb{Z}_{(p)}$, but when embedding $\mathbb{F}_p$ into $\mathrm{gr}(\mathbb{Z}_{(p)})$ via the ring homomorphism $a \mapsto a + (m)_{\mathbb{Z}_{(p)}[pt]}$ (it even holds $\mathrm{gr}(\mathbb{Z}_{(p)})_0 \cong \mathbb{F}_p$, see previous proof), it is clear that $pt + (m)_{\mathbb{Z}_{(p)}[pt]}$ is transcendental over $\mathbb{F}_p$. Therefore, an injective $\mathbb{F}_p$-algebra homomorphism is given by

$$\phi : \mathbb{F}_p[x] \to \mathrm{gr}(\mathbb{Z}_{(p)}),\ x \mapsto pt + (m)_{\mathbb{Z}_{(p)}[pt]}.$$

To show that ϕ is surjective, let $\frac{a}{b}p^d t^d + (m)_{\mathbb{Z}_{(p)}[pt]} \in \mathrm{gr}(\mathbb{Z}_{(p)})_d$ homogeneous with $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus (p)$, $d \in \mathbb{N}$. Let $a' = a \mod p \in \mathbb{F}_p$, $b' = b \mod p \in \mathbb{F}_p \setminus \{0\}$. Then

$$\phi\Big(a' \cdot b'^{-1} \cdot x^d\Big) = \frac{a'}{b'}p^d t^d + (m)_{\mathbb{Z}_{(p)}[pt]} = \frac{a}{b}p^d t^d + (m)_{\mathbb{Z}_{(p)}[pt]},$$

because $ab' - a'b \in (p)$ and thus $\big(\frac{a}{b} - \frac{a'}{b'}\big)p^d t^d = \frac{ab'-a'b}{bb'}p^d t^d \in (m)_{\mathbb{Z}_{(p)}[pt]}$.
An alternative, similar to the previous proof, is to consider the surjective ring homomorphism

$$\psi : \mathbb{Z}_{(p)}[pt] \to \mathbb{F}_p[x],\ \sum_{k=0}^{n} a_k (pt)^k \mapsto \sum_{k=0}^{n} \overline{a}_k x^k,$$

which has kernel $\ker(\psi) = (p)_{\mathbb{Z}_{(p)}[pt]}$, because $f = \sum_{k=0}^{n} a_k (pt)^k \in \ker(\psi)$ satisfies $p | a_k$ for all $k \in \{0, \ldots, n\}$, so $p | f$. Therefore, ψ induces an isomorphism $\mathrm{gr}(\mathbb{Z}_{(p)}) \cong \mathbb{F}_p[x]$.

Mixed Problems

9.1 Rings and Fields

(a) Let $A \subset B$ be integral domains and suppose that B is integral over A. Show that A is a field if and only if B is a field.

(b) Let R be a Noetherian local ring. Show that $m/m^2 = 0$ if and only if R is a field.

(c) Let R be a Noetherian ring. Show that $\sqrt{(0)}^n = (0)$ for some $n \in \mathbb{N}_{>0}$.

(d) Find a counterexample for the previous statement if R is not Noetherian.

(e) Find a ring R in which there is an element $r \in R$, which is a zero divisor, but not contained in any minimal prime ideal.

(f) For a ring R and any $n \in \mathbb{N}_{>0}$, a prime ideal $P \subset R$ satisfies

$$\sqrt{P^n} = P.$$

(a) Since B is integral over A, it holds $\dim(A) = \dim(B)$. Because for an integral domain R, it holds

$$R \text{ is a field} \iff (0) \text{ is the unique prime ideal} \iff \dim(R) = 0,$$

the claim is clear.

(b) One direction is obvious, the other follows from Nakayama's Lemma.

(c) This follows from lemma 2.6 ($I = \sqrt{(0)}$, $J = (0)$), since I is finitely generated, because R is Noetherian.
Alternatively, a direct argument, which is very similar to the proof of lemma 2.6 can be given: Since R is Noetherian, $\sqrt{(0)} = (a_1, \dots, a_n)$ is finitely generated. With $k \coloneqq \max(k_i : i \in \{1, \dots, n\})$, $n \coloneqq (n-1) \cdot k + 1$ has the desired property.

(d) A counterexample is given by $K[x_1, x_2, x_3, \dots]/(x_1, x_2^2, x_3^3)$.

(e) For a field K, consider $R = K[x, y]/(x^2, xy)$. The unique minimal prime ideal in R is $(\overline{x})$, but $\overline{y} \notin (\overline{x})$.

(f) Let $x \in \sqrt{P^n}$, i.e. there is $k \in \mathbb{N}$ such that x^k can be written as a finite sum of elements of the form $\prod_{i=1}^n p_i$ with $p_i \in P$. Thus $x^k \in P$ and since P is prime we conclude $x \in P$.
On the other hand, let $x \in P$. Then $x^n \in P^n$, so $x \in \sqrt{P^n}$.

9.2 More dimensions

Compute the dimension of the following rings R:

(a) $\mathbb{C}[\![x,y]\!]/(y^2)$,

(b) $K[x,y]/(x^2-y^3)$,

(c) $\prod_{i=1}^{n} K$,

(d) $\mathbb{Z}[i]$,

(e) $\mathbb{Q}[u,v,w]/(w^2-vw+u)$.

The lemma 11 is very useful, especially in integral domains. It will be used without further notice. Furthermore, in (a), (b) and (e), one can alternatively use theorem 5.13.

(a) Every prime ideal in the ring has to contain y, so (y) is a minimal prime ideal, but not maximal. It follows $\dim(R) = 1$.

(b) Since (x^2-y^3) is prime, but not maximal, it follows $\dim(R) = 1$.

(c) R is generated as a K-algebra by elements of the form $(0,\ldots,0,1,0,\ldots,0)$. Since any such element is algebraic over K (it is a root of x^2-x), it follows $\dim(R) = 0$. Alternative solution: Let P be a prime ideal in R. Since for $I \coloneqq 0 \times K \times \ldots \times K$, $J \coloneqq K \times 0 \times \ldots \times 0$, it holds $I \cdot J \subset P$, it follows $I \subset P$ or $J \subset P$. There are two cases:

- If $I \subset P$, then P/I is a prime ideal in $R/I \cong \prod_{i=1}^{n-1} K$.
- If $J \subset P$, then $R/J \cong K$ and thus $P = J$.

It follows inductively that any prime ideal is of the form $0 \times \ldots \times 0 \times K \times 0 \times \ldots \times 0$ and thus all prime ideals are maximal, implying $\dim(R) = 0$.

(d) Because $i \in \mathbb{C}$ is integral over $\mathbb{Z}$, $\dim(R) = \dim(\mathbb{Z}) = 1$.

(e) It is clear that $\dim(R) \leq 2$. Since $w^2 - vw + u$ is prime (Gauss's lemma in $\mathbb{Q}(v,w)$), the chain $(w^2-vw+u) \subsetneq (w,u) \subsetneq (u,v,w)$ shows that $\dim(R) = 2$.

9.3 Some Computations

(a) Compute the length of $\mathbb{Z}/24\mathbb{Z}$.

(b) Find $\sqrt{I}$ for $I = (xy^3, x(x-y)) \subset \mathbb{C}[x,y]$.

(c) Compute the dimension of $X \coloneqq V(x^2+y^2)$ in $\mathbb{C}^2$.

(d) Compute the nilradical of $\mathbb{Z}/4\mathbb{Z}$.

(a) The submodules of $\mathbb{Z}/24\mathbb{Z}$ are precisely the ideals, which correspond to those ideals in $\mathbb{Z}$, which contain 24. Since $24 = 2^3 \cdot 3$, it follows $\text{length}(\mathbb{Z}/24\mathbb{Z}) = 4$.

(b) Since $V(I) = \{(0,k) : k \in \mathbb{C}\}$, Hilbert's Nullstellensatz yields $\sqrt{I} = I(V(I)) = (x)$.

(c) The minimal prime ideals over $f := x^2 + y^2 = x^2 - (iy)^2$ are $(x+iy)$ and $(x-iy)$. Since $\dim(\mathbb{C}[x,y]) = 2$ and $(f) \neq (0)$, $\dim(K[X]) \leq 1$. Because $(x+iy)$ is contained in the maximal ideal (x,y), it follows $\dim(K[X]) = 1$.

(d) The unit group of $\mathbb{Z}/4\mathbb{Z}$ is $\{1,3\}$; and the other elements are nilpotent, so $\sqrt{(0)} = \{0,2\}$.

9.4 Singular Locus

Compute the singular locus of $V(y^2 - x^3)$ in $\mathbb{C}^2$ and prove that its normalization is isomorphic to a polynomial ring in one variable.

By the Jacobian criterion, the singular locus consists of those points $(x,y) \in \mathbb{C}^2$ with $(-3x^2, 2y) = (0,0)$, i.e. the only singular point is $(0,0)$.
The localizations at all nonzero points is regular, so in particular normal and it follows $\tilde{K[X]} \subset K[X]_{(x,y)}$ for $(x,y) \in \mathbb{C}^2 \setminus \{(0,0)\}$. This inspires considering $z := \frac{\overline{y}}{\overline{x}} \in \mathrm{Quot}(K[X])$ and dividing $\overline{y}^2 - \overline{x}^3 = 0$ by $\overline{x}^2$ reveals that $z^2 - \overline{x} = 0$, so $K[z]$ is integral over $K[X]$.
It is left to show that z is transcendental over K, because this implies that $K[z]$ is isomorphic to a polynomial ring, so it is factorial and thus normal, which shows that $K[z]$ is the normalization of $K[X]$. If z was algebraic, then the same would hold for $z^2 = \overline{x}$, but $\overline{x}$ is not algebraic over K:
This can be seen by noting that a polynomial with coefficients in K and $\overline{x}$ as a root needs to be a multiple of $y^2 - x^3$, thus has to be 0 by comparison of y-degrees.
Alternatively, consider the K-algebra homomorphism

$$K[x,y] \to K[x],\ x \mapsto x^2,\ y \mapsto x^3,$$

which has kernel $(y^2 - x^3)$, so $K[X]$ is isomorphic to a subring of $K[x]$. The image of $\overline{x}$ under that isomorphism is x^2, which is transcendental over K.