MA 312 Commutative Algebra / Jan–April 2020
(BS, Int PhD, and PhD Programmes)

Download from : http://www.math.iisc.ac.in/patil/courses/Current Courses/...

Tel : +91-(0)80-2293 3212 / 09449076304 **E-mails :** patil@math.ac.in

Lectures : Tuesday and Thursday ; 15:30–17:00 **Venue:** MA LH-5 / LH-1

9. Integral Extensions* — Cohen-Seidenberg Theorems*

- **For a ready reference use the R9 Summary of Results listed below**
- **For proofs of Supplementary Results cited see the *Supplements at the end**

R9 Summary of Results

R9.1 Integral extensions In a ring extension $A \subseteq A'$, it is useful to consider elements $x \in A'$ which are zeros of monic polynomials in $A[X]$.

R9.1.1 Integral dependence. Let $\varphi : A \to A'$ be a ring homomorphism (A' is an A-algebra with the structure homomorphism). An element $x \in A'$ is called integral over A with respect to φ if it satisfies so-called integral equation over A, i .e. if there are elements $a_0, \dots, a_{n-1} \in A$ such that $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$. In other words the kernel of the substitution homomorphism $\varepsilon_x : A[X] \to A'$, $X \mapsto x$, contains a monic polynomial over A.

The ring (or, A-algebra) A' is called integral over A, or φ is called integral over A if each $x \in A'$ is integral over A. Further, φ is called finite if the A-algebra A' is finite over A. If $A \subseteq A'$ is a ring extension, then A' is an A-algebra with the structure homomorphism $\iota : A \to A'$ (the natural inclusion) and we say that A' is integral over A if ι is integral over A.

R9.1.2 Example Let $A[X]$ be the polynomial ring in one indeterminate X over a ring $A \neq 0$ and let $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in A[X]$. Further, let Y be another indeterminate. We claim that the substitution homomorphism $\varepsilon_f : A[Y] \to A[X]$, $Y \mapsto f$, is finite and hence integral. For a proof, first note that the equation $X^n + a_{n-1}X^{n-1} + \cdots + a_1X + \big(a_0 - \varepsilon_f(Y)\big) = 0$ is an integral equation for X over $A[Y]$. From this conclude by induction that the $A[Y]$-module $A[X]$ (with the structure homomorphism ε_f) is generated by $1, X, \dots, X^{n-1}$. In other words ε_f is finite. Alternatively, this also follows directly from the following Lemma. Furthermore, it follows that φ is integral which is a non-trivial fact which cannot be derived by a direct *ad hoc* computation.

The following Lemma is the key to handling integral dependence which give a basic characterization on integral dependence in terms of finiteness :

R9.1.3 Lemma *Let $A \to A'$ be a ring homomorphism and let $x \in A'$. Then the following statements are equivalent :*

(i) *x is integral over A.*
(ii) *The subring $A[x] \subseteq A'$ generated by $\varphi(A)$ and x in A' is a finite A-module.*
(iii) *There exists a finite A-module $V \subseteq A'$ such that $1 \in V$ and $xV \subseteq V$.*
(iv) *There exists an $A[x]$-module V such that V is a finite A-module and $\operatorname{Ann}_{A[x]} V = 0$.*

R9.1.4 Remark The proof of the implication (iv)$\Rightarrow$(i) in the above Lemma shows that : *If $xV \subseteq \mathfrak{a}V$ for an ideal $\mathfrak{a} \subseteq A$, then there is an integral equation $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ with $a_j \in \mathfrak{a}^{n-j}$, $j = 0, \dots, n-1$.*

R9.1.5 A nice property of integral extensions $A \subseteq A'$ is that they are compatible with residue-class, localizations, and polynomial rings, i. e. :

(a) If $\mathfrak{a}'$ is an ideal in A', then $A'/\mathfrak{a}'$ is an integral extension of $A/(A \cap \mathfrak{a}')$.

(b) If $S \subseteq A$ is a multiplicatively closed subset in A, then $S^{-1}A'$ is an integral extension of $S^{-1}A$.

(c) The polynomial extension $A[X] \subseteq A'[X]$ is also an integral extension.

R 9.1.6 (Geometric properties of ring extensions) (see Examples R 9.1.8 for motivation) Let $A := K[V]$ and $A' := K[V']$ be K-coordinate rings of affine K-algebraic sets and let $\iota : K[V] \to K[V']$ be the K-algebra homomorphism which corresponds to the morphism $\pi := \iota^* : V' \to V$ on K-spectra, see R 8.1.1 (h). We study the contraction and extension of prime ideals under the ring homomorphism ι — this is equivalent to the study the images and inverse images of irreducible closed subsets under the morphism π.

Note that, if ι is injective, i. e. A is a subring of A', then the contraction of a prime ideal $\mathfrak{p}' \in \operatorname{Spec} A'$ is precisely $A \cap \mathfrak{p}' =: \mathfrak{p} \in \operatorname{Spec} A$ and the extension of a prime ideal $\mathfrak{p} \in \operatorname{Spec} A$ is precisely the ideal $\mathfrak{p}A'$ generated by $\mathfrak{p}$ in A'. Geometrically, the first assertion means that the image of an irreducible closed subset of V' under π is also irreducible in V.

The main geometric question one can ask whether the converse is also true, i. e. every prime ideal $\mathfrak{p} \in \operatorname{Spec} A$ is of the form $\mathfrak{p} = A \cap \mathfrak{p}'$ for some prime ideal $\mathfrak{p}' \in \operatorname{Spec} A'$. Equivalently, for a given irreducible closed subset W of V, whether there are irreducible closed subset W' of V' with the image $\pi(W') = W$.

There are five main geometric results on integral ring extensions in the above spirit which are commonly named maximality, Incomparability, Lying over, Going-up and Going-down their algebraic counterparts – known as Cohen-Seidenberg Theorems — are listed in R 9.1.8 below.

R 9.1.7 Definition Let A be a ring, A' be an A-algebra with structure homomorphism $\varphi : A \to A'$. We say that a prime ideal $\mathfrak{p}' \in \operatorname{Spec} A'$ lies over $\mathfrak{p} \in \operatorname{Spec} A$ if $\mathfrak{p}'$ contracts to $\mathfrak{p}$, i. e. $\varphi^{-1}(\mathfrak{p}') = \mathfrak{p}$ (also denoted by $A \cap \mathfrak{p}' = \mathfrak{p}$).

R 9.1.8 Cohen-Seidenberg Theorems *Let $A \subseteq A'$ be an integral extension of rings.*

(1) (Maximality) *Suppose that $\mathfrak{p}' \in \operatorname{Spec} A'$ lies over $\mathfrak{p} \in \operatorname{Spec} A$. Then $\mathfrak{p}' \in \operatorname{Spm} A'$ if and only if $\mathfrak{p} \in \operatorname{Spm} A$.*

(2) (Incomparability) *Suppose that $\mathfrak{p}', \mathfrak{q}' \in \operatorname{Spec} A'$ with $\mathfrak{p}' \subseteq \mathfrak{q}'$ and both $\mathfrak{p}'$, $\mathfrak{q}'$ lie over $\mathfrak{p}$. Then $\mathfrak{p}' = \mathfrak{q}'$.*

(3) (Lying over) *For a given $\mathfrak{p} \in \operatorname{Spec} A$, there exists a prime ideal $\mathfrak{p}' \in \operatorname{Spec} A'$ lying over $\mathfrak{p}$.* In other words the map $\varphi^* : \operatorname{Spec} A' \to \operatorname{Spec} A$ associated to φ on spectra is surjective. (**Remark :** *More generally, for every ring extension $A \subseteq A'$ and $\mathfrak{p} \in \operatorname{Spec} A$, there exists a prime ideal $\mathfrak{p}' \in \operatorname{Spec} A'$ lying over $\mathfrak{p}$ if and only if $\mathfrak{p}A' \cap A = \mathfrak{p}$.* — **Proof**)

(4) (Going-up) *Suppose that $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec} A$ with $\mathfrak{p} \subseteq \mathfrak{q}$ and that $\mathfrak{p}' \in \operatorname{Spec} A'$ lies over $\mathfrak{p}$. Then there exists $\mathfrak{q}' \in \operatorname{Spec} A'$ such that $\mathfrak{p}' \subseteq \mathfrak{q}'$ and that $\mathfrak{q}'$ lies over $\mathfrak{q}$.*

(**Remark :** Note that the properties maximality, incomparability and going-up hold for arbitrary integral ring homomorphisms $\varphi : A \to A'$. In particular, $\dim A' \le \dim A$ (the *dimension* $\dim A$ of a ring A is the Krull-dimension of A, see Exercise Set 10). Moreover, if φ is injective, then the property lying over holds for φ and hence $\dim A' = \dim A$.

Further, note that, if $\mathfrak{a} \neq 0$ is an ideal in a ring A, then the canonical surjective ring homomorphism $\pi_{\mathfrak{a}} : A \to A/\mathfrak{a}$ is obviously integral, but the Lying over property fails for $\pi_{\mathfrak{a}}$.)

R 9.1.9 Examples (Geometric examples) Let X, Y be indeterminates, $A := \mathbb{C}[X]$, $F = F(X,Y) \in \mathbb{C}[X,Y]$ be a non-constant monic polynomial in Y over A and $A' := A[Y]/\langle F \rangle = A[x,y]$, where x, y are the residue-classes of X, Y modulo $F = Y^2 - X^2$. Note that (see Exercise 8.8 and Exercise 8.21 (d)) $\mathbb{C}$-Spec $A' = \mathrm{V}_{\mathbb{C}}(F) = \{(a,b) \in \mathbb{C}^2 \mid F(a,b) = 0\}$ and $\mathbb{C}$-Spec $A = \mathbb{C}$-Spec $\mathbb{C}[X] = \mathbb{C}$ and the ring extension $\iota : A \to A'$ which corresponds to the morphism $\pi := \iota^* : \mathbb{C}\text{-Spec } A' \to \mathbb{C}\text{-Spec } A$, $(a,b) \mapsto a$ of affine $\mathbb{C}$-algebraic sets on $\mathbb{C}$-spectra.

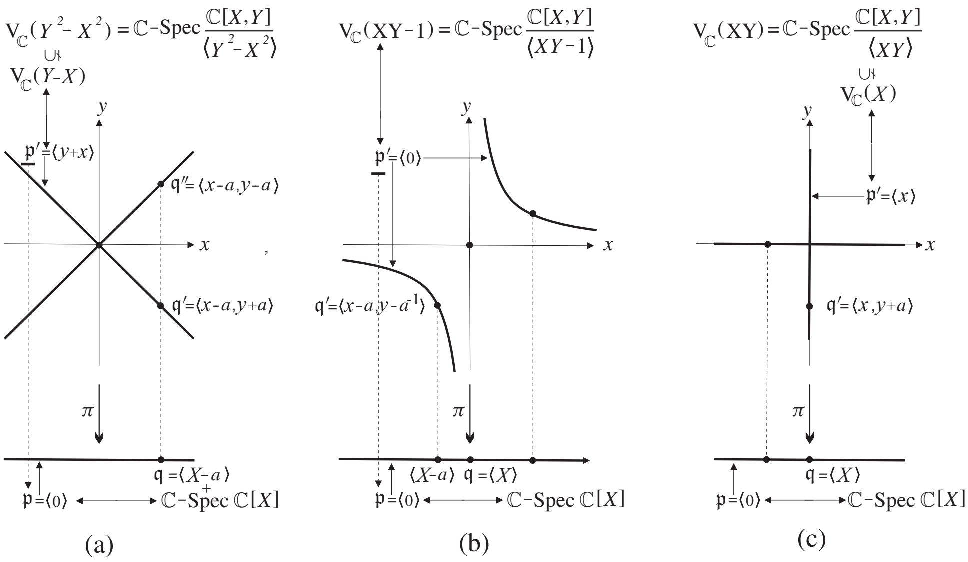
In the following we consider the following three examples (the subtle but important difference between these examples is that in (a) the given polynomial is monic in Y, whereas in (b) and (c) it is not (with the leading term being XY). This has geometric consequences for the inverse images $\pi^{-1}(x)$ for points $x \in \mathbb{C}$, the so-called fibers of π) :

(a) $F = X^2 - Y^2$. In this case $A' = A[y]$ and $y^2 = X^2$ and A' is integral over A. Substituting arbitrary value ($a \in \mathbb{C}$) for X, we always get a (monic) quadratic equation $Y^2 - a^2 = 0$ in Y (over $\mathbb{C}$). Geometrically, this means that in any fiber $\pi^{-1}(a)$ has two points (counted with multiplicities).

(b) $F = XY - 1$. In this case $y \in A'$ does not satisfy a monic polynomial over A (since there are no polynomials $g, h \in A[Y]$ with $g = h(XY-1)$). Substituting arbitrary value ($a \in \mathbb{C}$) for X, we get a linear polynomial $aY - 1 = 0$ in Y over $\mathbb{C}$ for $a \neq 0$, but a constant polynomial -1 for $a = 0$. Geometrically, the consequence is that the fibers $\pi^{-1}(a)$ are singletons for $a \neq 0$ and the fiber $\pi^{-1}(0) = \emptyset$ for $a = 0$.

(c) $F = XY$. This case is similar to the case (b), again A' is not integral over A. Substituting arbitrary value ($a \in \mathbb{C}$) for X, we get (since the $aY = 0$ is linear polynomial in Y over $\mathbb{C}$ for $a \neq 0$ and is the zero polynomial (in Y over $\mathbb{C}$) if $x = 0$) exactly one solution $(a, 0)$ for $a \neq 0$ and infinitely many solutions $(0, b)$, $b \in \mathbb{C}$ for $a = 0$. Geometrically, this means that the fibres $\pi^{-1}(0)$ are singletons if $a \neq 0$ and the fiber $\pi^{-1}(0)$ is infinite, in fact, it is the affine line $\mathrm{V}_{\mathbb{C}}(X)$.

To illustrate geometric questions (such as in R.9.1.6) we will draw pictures of affine K-algebraic sets and their closed subsets (affine K-algebraic subsets), but label them with their algebraic counterparts (see Exercise Set 8, R 8.1.4). With this considerations the pictures corresponding to the above three examples are drawn as follows :



From the algebraic counter parts and the corresponding geometric consequences, we note the following observations :

(1) In the example (a) : $A' = \mathbb{C}[X,Y]/\langle Y^2 - X^2 \rangle = \mathbb{C}[x,y]$, where x, y are the residue-classes of X, Y modulo $Y^2 - X^2$ and hence $\mathbb{C}$-Spec $A' = \mathrm{V}_{\mathbb{C}}(Y^2 - X^2)$ has two irreducible components, namely, the affine lines (over $\mathbb{C}$) $\mathrm{V}_{\mathbb{C}}\langle Y + X \rangle$ and $\mathrm{V}_{\mathbb{C}}\langle Y - X \rangle$ corresponding to the minimal prime ideals $\mathfrak{p}' := \langle y + x \rangle$ and $\mathfrak{p}'' := \langle y - x \rangle \in \operatorname{Spec} A'$, respectively. The points on the affine line $\mathrm{V}_{\mathbb{C}}\langle Y + X \rangle$ are $(a, -a)$, $a \in \mathbb{C}$ corresponding to the maximal ideals $\langle x - a, y + a \rangle \in \operatorname{Spm} A'$, $a \in \mathbb{C}$ and $\mathfrak{p}' \subsetneq \langle x - a, y + a \rangle$ for every $a \in \mathbb{C}$. Similarly, the points on the affine line $\mathrm{V}_{\mathbb{C}}\langle Y - X \rangle$ are (a, a), $a \in \mathbb{C}$ corresponding to the maximal ideals $\langle x-a, y-a\rangle \in \operatorname{Spm} A'$, $a \in \mathbb{C}$ and $\mathfrak{p}'' \subsetneq \langle x-a, y-a\rangle$ for every $a \in \mathbb{C}$. Further, the irreducible components $\mathrm{V}_{\mathbb{C}}\langle Y+X\rangle$ and $\mathrm{V}_{\mathbb{C}}\langle Y-X\rangle$ intersects exactly at the origin $(0,0)$.

(2) In the example (b): $A' = \mathbb{C}[X,Y]/\langle XY-1\rangle = \mathbb{C}[x,y]$, where x,y are the residue-classes of X,Y modulo $XY-1$ and hence $\mathbb{C}$-Spec $A' = \mathrm{V}_{\mathbb{C}}(XY-1)$ which is irreducible (since $XY-1$ is irreducible in the UFD $\mathbb{C}[X,Y]$) and corresponds to the (unique minimal) zero prime ideal $\mathfrak{p}' := \langle 0\rangle$. The points on $\mathrm{V}_{\mathbb{C}}\langle XY-1\rangle$ are (a, a^{-1}), $a \in \mathbb{C} \smallsetminus \{0\}$ which corresponds to the maximal ideals $\langle x-a, y-a^{-1}\rangle \in \operatorname{Spm} A'$, $a \in \mathbb{C}\smallsetminus\{0\}$ and $\mathfrak{p}' \subsetneq \langle x-a, y-a^{-1}\rangle$ for every $a \in \mathbb{C}\smallsetminus\{0\}$. In particular, the origin $(0,0) \notin \mathbb{C}$-Spec A'.

(3) In the example (c): $A' = \mathbb{C}[X,Y]/\langle XY\rangle = \mathbb{C}[x,y]$, where x,y are the residue-classes of X,Y modulo XY and hence $\mathbb{C}$-Spec A' has two irreducible components, namely, the affine lines (over $\mathbb{C}$) $\mathrm{V}_{\mathbb{C}}(X)$ (y-axis in $\mathbb{C}^2$) and $\mathrm{V}_{\mathbb{C}}(Y)$ (x-axis in $\mathbb{C}^2$) which correspond to the minimal prime ideals $\mathfrak{p}' := \langle x\rangle$ and $\mathfrak{p}'' := \langle y\rangle$, respectively. The points on $\mathrm{V}_{\mathbb{C}}\langle X\rangle$ are $(0,a)$, $a \in \mathbb{C}$ corresponding to the maximal ideals $\langle x, y-a\rangle \in \operatorname{Spm} A'$, $a \in \mathbb{C}$ and $\mathfrak{p}' \subsetneq \langle x, y-a\rangle$ for every $a \in \mathbb{C}$. The points on $\mathrm{V}_{\mathbb{C}}\langle Y\rangle$ are $(a,0)$, $a \in \mathbb{C}$ corresponding to the maximal ideals $\langle x-a, y\rangle \in \operatorname{Spm} A'$, $a \in \mathbb{C}$ and $\mathfrak{p}'' \subsetneq \langle x-a, y\rangle$ for every $a \in \mathbb{C}$.

(4) Note that the affine line $\mathbb{C}$-Spec $\mathbb{C}[X] = \mathrm{V}_{\mathbb{C}}(0) = \mathbb{C}^1$ is irreducible and corresponds to the (unique minimal) zero prime ideal $\mathfrak{p} = \langle 0\rangle \in \operatorname{Spec} A$. The points $a \in \mathbb{C}$ corresponds to the maximal ideals $\langle X-a\rangle$ and $\mathfrak{p} \subsetneq \langle X-a\rangle$ for every $a \in \mathbb{C}$.

(5) In the example (a) the extension $A \subseteq A'$ is integral (since the polynomial $F = Y^2 - X^2$ is monic in Y) and the map π is surjective, since all fibers of π are non-empty. Moreover, since $\mathbb{C}$ is algebraically closed field, the restriction of the lying over property to points in the K-spectrum means that (by the property (1) on maximality in the Theorem R 9.1.8 and HNS 4, see Exercise 6.14 (b)) the morphisms corresponding to integral extensions are always is surjective. Of course, a prime ideal $\mathfrak{q}' \in \operatorname{Spec} A'$ lying over a given prime ideal $\mathfrak{q} \in \operatorname{Spec} A$ is in general not unique — for example, in the picture (a) there are two choices $\mathfrak{q}' = \langle x-a, y+a\rangle$ and $\mathfrak{q}'' = \langle x-a, y-a\rangle$ for lying over $\mathfrak{q} = \langle X-a\rangle$, $a \in \mathbb{C}$, $a \neq 0$. Further, the picture shows that the ring extension $A \subseteq A'$ satisfies the Going-up property.

(6) In contrast, in the example (b) there is no prime ideal in A' lying over the prime ideal $\mathfrak{q} = \langle X\rangle \in K$-Spec A and that the ring extension $A \subseteq A'$ cannot be integral (since the property (2) Lying over does not hold in the Theorem R 9.1.8). Further, the $\mathbb{C}$-algebra $A'' := \mathbb{C}[X,Y]/\mathfrak{a}'$, where $\mathfrak{a}' := \langle XY-1\rangle \cap \langle X,Y\rangle$ is the $\mathbb{C}$-coordinate ring of $V'' := V' \cup \{(0,0)\}$. In this case, it is easy to see from the picture (b) that the ring extension $\mathbb{C}[X] = A \subseteq A''$ satisfies the lying over and incomparability properties, however not the going-up property, since in the picture (b) the maximal ideal $\langle x,y\rangle$ of the origin is the only prime ideal in $\operatorname{Spec} A''$ lying over $\mathfrak{q} = \langle x\rangle$, but it does not contain the given prime ideal $\mathfrak{p}' = \langle 0\rangle \in \operatorname{Spec} A''$ (the only prime ideal) lying over $\mathfrak{p} = \langle 0\rangle \in \operatorname{Spec} A$.

(7) The example (c) is different as the fiber over the prime ideal $\mathfrak{q} = \langle x\rangle$ is the affine line $\mathrm{V}_{\mathbb{C}}(X)$ (and hence one dimensional). Moreover, there are prime ideals $\mathfrak{p}'$ and $\mathfrak{q}' \in \operatorname{Spec} A'$ lying over $\mathfrak{a}$ with $\langle x\rangle = \mathfrak{p}' \subseteq \mathfrak{q}' = \langle x, y+a\rangle$, $a \in \mathbb{C}$, as can be seen in the picture (c) above. Such a situation cannot occur for integral extensions (see the incomparability property (3) in the Theorem R 9.1.8) which essentially means that the fibers of the corresponding maps have to be finite (since finite type integral maps are finite).

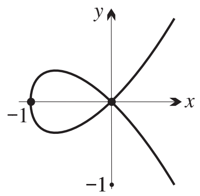
R 9.1.10 (Geometric interpretation of normal domains) Let K be a field and let $K[V]$ be the K-coordinate ring of an irreducible affine K-algebraic set $V \subseteq K^n$. Then $K[V]$ is an integral domain and the elements $\varphi = f/g \in \mathrm{Q}(K[V])$ of the quotient field of $K[V]$ can be interpreted as rational functions on V, i. e. as quotients of polynomial functions that are well-defined except at some isolated points of V (where the denominator g vanishes), i. e. on $V \smallsetminus \mathrm{V}_K(g)$. Therefore, *the normality condition on $K[V]$ is equivalent with the condition that every rational function φ on V which is integral over $K[V]$ is well-defined on V.*

We shall illustrate this geometric observation in the following two examples.

(a) Let $V = \mathbb{C}^1$ be the affine line over $\mathbb{C}$. Then the corresponding $\mathbb{C}$-coordinate ring is $\mathbb{C}[V] = \mathbb{C}[X]$ is the polynomial ring over $\mathbb{C}$. We already know that $\mathbb{C}[X]$ is a normal domain, since it is a UFD. However to see this geometrically : If a rational function $\varphi \in \mathbb{C}(X) = \mathrm{Q}(\mathbb{C}[V])$ on $\mathbb{C}$ is *not* well-defined at a point $a \in \mathbb{C}$, then φ must have a pole at a, i. e. it is of the form $\varphi(X) = f(X)/(X-a)^r$ for some $r \in \mathbb{N}^+$ and $f \in \mathbb{C}(X)$ which is well-defined and $\neq 0$ at a. But then φ can not satisfy a monic polynomial $\varphi^n + c_{n-1}\varphi^{n-1} + \cdots + c_0 = 0$ with $c_0, \ldots, c_{n-1} \in \mathbb{C}[X]$, since otherwise φ^n has a pole of order nr at a which cannot be cancelled by lower order pole of the other terms $c_{n-1}\varphi^{n-1} + \cdots + c_0$.

(b) Let $V := \mathrm{V}_{\mathbb{R}}(Y^2 - X^2 - X^3) \subseteq \mathbb{R}\text{-Spec}\, \mathbb{R}[X,Y]$ and $A := \mathbb{R}[V] = \mathbb{R}[X,Y]/\langle Y^2 - X^2 - X^3\rangle = \mathbb{R}[x,y]$, where x and y are the residue-classes modulo $\langle Y^2 - X^2 - X^3\rangle$, respectively. Then $y^2 = x^2 + x^3$.

$\mathrm{V}_{\mathbb{R}}(Y^2 - X^2(X+1))$



Strophoid — Parabola nodata

In this case A is not normal, since the rational function $\varphi = y/x \in \mathrm{Q}(A) \smallsetminus A$ satisfies the monic equation $\varphi^2 - x - 1 = (y^2/x^2) - x - 1 = \big((x^2 + x^3)/x^2\big) - x - 1 = 0$. See also Exercise 9.19 (d). (**Remark :** The reason for $\mathbb{R}[V]$ not being normal is that the origin is a "singular point" of V. See also Exercise 9.20.)

R9.1.11 Theorem (Going-down) *Let $A \subseteq A'$ be an integral extension of integral domains and suppose that A is normal. Suppose that $\mathfrak{p}$, $\mathfrak{q} \in \operatorname{Spec} A$ with $\mathfrak{p} \subseteq \mathfrak{q}$ and that $\mathfrak{q}' \in \operatorname{Spec} A'$ lies over $\mathfrak{q}$. Then there exists $\mathfrak{p}' \in \operatorname{Spec} A'$ such that $\mathfrak{p}' \subseteq \mathfrak{q}'$ and that $\mathfrak{p}'$ lies over $\mathfrak{p}$.*

For a proof of Going-down Theorem, use the following lemma (for $\mathfrak{p}'$ take any minimal prime ideal over $\mathfrak{p}A'$ contained in $\mathfrak{q}'$) :

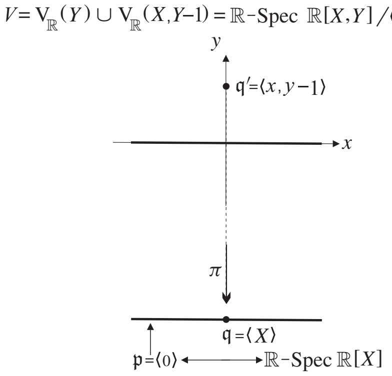
R9.1.12 Lemma *Let $A \subseteq A'$ be an integral extension of integral domains and suppose that A is normal. If $\mathfrak{p} \in \operatorname{Spec} A$ and if $\mathfrak{p}' \in \operatorname{Spec} A'$ is minimal over $\mathfrak{p}A'$, then $\mathfrak{p}' \cap A = \mathfrak{p}$.*

Proof. $\mathfrak{p}' A'_{\mathfrak{p}'}$ is nilpotent modulo $\mathfrak{p} A'_{\mathfrak{p}'}$. Therefore, for $x \in \mathfrak{p}' \cap A$, there exist $n \in \mathbb{N}^*$ and $y \in A' \smallsetminus \mathfrak{p}'$ such that $z := yx^n \in \mathfrak{p}A'$. Let $F = X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in A[X]$ be the minimal polynomial of y (see Exercise 9.23). Then $G := X^m + a_{m-1}x^n X^{m-1} + \cdots + a_0 x^{mn}$ is the minimal polynomial of z. All its coefficients $a_{m-1}x^n, \ldots, a_0 x^{mn}$ belong to $\mathfrak{p}$. This follows from $z \in \mathfrak{p}A'$ and the facts that, by the Remark on Page 1, there exists an integral equation $H(z) = z^d + b_{d-1}z^{d-1} + \cdots + b_0 = 0$ with $b_0, \ldots, b_{d-1} \in \mathfrak{p}$ and that G divides the polynomial $H = X^d + b_{d-1}X^{d-1} + \cdots + b_0$. Now, if $x \notin \mathfrak{p}$, then $a_{m-1}, \ldots, a_0 \in \mathfrak{p}$ and $y^m \in \mathfrak{p}A' \subseteq \mathfrak{q}$, i. e., $y \in \mathfrak{q}$, a contradiction. •

R9.1.13 Examples (Where Going-down fails) In contrast to Going-up (see R9.1.8 (3)) property the Going-down property does not hold for general integral extensions. The integral ring extension $K[X] \hookrightarrow K[X,Y]/\langle Y^2 - X^2\rangle$, K is a field, satisfies also the Going-down property, see R 9.1.9 (9). Consider the following two examples :

(a) Let K be a field and $V := \mathrm{V}_K(Y) \cup \mathrm{V}_K(X\,,\,Y-1) \subseteq K^2$ be affine K-algebraic set with two disjoint irreducible components $\mathrm{V}_K(Y) =$ the x-axis and $\mathrm{V}(X\,,\,Y-1) = \{(0,1)\}$ in K^2 corresponding to the prime ideal $\mathfrak{p} := \langle Y\rangle \in \operatorname{Spec} K[X,Y]$ and the maximal ideal $\mathfrak{q}' := \mathfrak{m}_{(0,1)} = \langle X\,,\,Y-1\rangle \in K\text{-Spec}\, K[X,Y]$, respectively. The the projection morphism $\pi = \iota^* : V \to K^1$, $(a,b) \mapsto a$, of K-algebraic sets corresponds to the K-algebra homomorphism $\iota : A := K[K^1] = K[X] \hookrightarrow K[X,Y]/\langle Y\rangle \cap \langle X\,,\,Y-1\rangle = K[V] =: A'$ which is injective and integral (since $y(y-1) = 0$ in A', where y denote the residue-class of Y in A') and the maximal ideal $\mathfrak{q}'$ is the only maximal ideal lying over the maximal ideal $\mathfrak{q} := \langle X\rangle \in K\text{-Spec}\, A$.

Therefore the Going-down fails if we choose a chain $\mathfrak{p}=\langle 0\rangle \subsetneq \mathfrak{q}$ in $\operatorname{Spec} A$ and $\mathfrak{q}'\in\operatorname{Spec} A'$, since there is no prime ideal $\mathfrak{p}'\in\operatorname{Spec} A'$ with $\mathfrak{p}'\subsetneq\mathfrak{q}'$ and which lies over $\mathfrak{p}$, see the picture below. In order to avoid such situation, one need to assume that A' is an integral domain.



(a)

(b) Let K be a field of characteristic $\neq 2$, $K[X,Y,Z]$, $K[T,Z]$ polynomial algebras over K, and let $\varepsilon : K[X,Y,Z]\to K[T,Z]$ be the K-algebra (substitution) homomorphism defined by $\varepsilon(X)=T^2-1$, $\varepsilon(Y)=T(T^2-1)$, and $\varepsilon(Z)=Z$, and $A:=\operatorname{Img}\varepsilon = K[(T^2-1),T(T^2-1),Z]\subseteq A':=K[T,Z]$. Note that the quotient field of A is $\mathrm{Q}(A)=\mathrm{Q}(A')=K(T,Z)$ (since $T^{-1}=\varepsilon(X)/\varepsilon(Y)\in\mathrm{Q}(A)$ and the K-algebra A' is integral over A (since $T^2\in A$ and $Z\in A$, A' is generated by integral elements T and Z). Moreover, A' is the normalization of $A \xleftarrow{\sim} \big(K[X,Y]/\langle Y^2-X^2(X+1)\rangle\big)[Z]=K[V][Z]$, where $K[V]$ is the K-coordinate ring of the affine plane curve (over K) $V:=\mathrm{V}_K(Y^2-X^2(X+1))\subseteq K^2$. Moreover, the K-algebra A is the affine K-coordinate ring $K[V\times K^1]$ of the affine surface (over K) $V\times K^1\subseteq K^3$ and the injective integral K-algebra homomorphism $\iota : A\to A'$ corresponds to the morphism

$$\pi=\iota^* : K\text{-Spec }A' = K^2 \longrightarrow V\times K^1,\ (t,z)\longmapsto (t^2-1\,,\,t^3-t\,,\,z),$$

of affine K-algebraic sets, see R 8.1.1 (h). In fact, this is a 2-dimensional version (base change) of the situation of Example 9.19 (d) (see also R 9.1.10 (b)). Although both affine K-algebraic sets are irreducible, the singular locus of the base space $V\times K^1$ makes the Going-down property fails :

(b.1) Note that $\mathfrak{p}:=\langle (T^2-1)-(Z^2-1), T(T^2-1)-Z(Z^2-1)\rangle\in\operatorname{Spec}A$, since $A/\mathfrak{p}\xrightarrow{\sim} K[T,Z]/\langle T-Z\rangle$ and $\mathfrak{p}':=\langle T-Z\rangle\in\operatorname{Spec}A'$ is the *only* prime ideal in A' which lies over $\mathfrak{p}$ (proof ?), i. e. $\mathfrak{p}=A\cap\mathfrak{p}'$. Moreover, $\mathfrak{p}'\notin\operatorname{Spm}A'$, since $\mathfrak{p}\notin\operatorname{Spm}A$. Furthermore, $\mathfrak{p}A'\subseteq\mathfrak{q}':=\langle T-1, Z+1\rangle\in K\text{-Spec }A'$ and hence $\mathfrak{p}\subsetneq\mathfrak{q}\in\operatorname{Spm}A$, and $\mathfrak{p}'\not\subseteq\mathfrak{q}'$ (since the characteristic of K is $\neq 2$).

(b.2) With the prime ideals $\mathfrak{p}\in\operatorname{Spec}A$ and $\mathfrak{q}'\in\operatorname{Spec}A'$ as defined in (b.1), it follows that for the choice of the chain $\mathfrak{p}\subsetneq\mathfrak{q}:=\mathfrak{q}'\cap A$ and $\mathfrak{q}'\in K\text{-Spec }A'$, there is *no* prime ideal $\operatorname{Spec}A'$ which lies over $\mathfrak{p}$ and is contained in $\mathfrak{q}'$.

(b.3) Geometric interpretation (for the failure of Going-down for $\iota : A\to A'$) : With the notations as in (b.1), the prime ideal $\mathfrak{p}'\in\operatorname{Spec}A'\smallsetminus\operatorname{Spm}A'$ corresponds to the irreducible affine plane curve — the diagonal

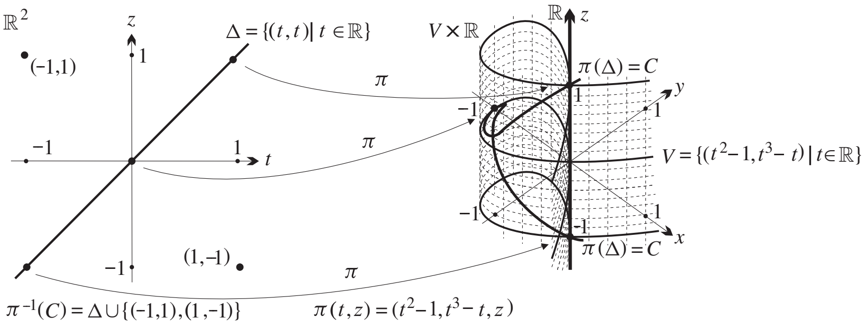
$$\mathrm{V}_K(T-Z)=\Delta:=\Delta_{K^2}:=\{(t,t)\mid t\in K\}\subseteq K^2$$

and the prime ideal $\mathfrak{p}\in\operatorname{Spec}A$ corresponds to the irreducible affine space curve (on the affine surface $V\times K^1$) — the image

$$C:=\pi(\Delta)=\{(t^2-1\,,\,t^3-t\,,\,t)\in K^3\mid t\in K\}\subseteq V\times K^1.$$

However, the inverse image $\pi^{-1}(C)=\Delta\cup\{(1,-1),(-1,1)\}$, where the point $(1,-1)$ corresponds to the maximal ideal $\mathfrak{q}'\in K\text{-Spec }A'$, and the additional points $(1,-1)$, $(-1,1)$ do not lie in any irreducible affine K-algebraic subset $C'\subseteq K^2$ with $\pi(C')=C$ (prove!). Therefore the Going-down fails for $\iota : A \to A'$. The source of the additional points $(1,-1)$ and $(-1,1)$ can be explained as follows:

(b.4) The affine curve C on $V \times K^1$ passes twice through the singular locus of $V \times K^1$ — the affine line $\{(0,0)\} \times K^1 \subseteq V \times K^1$. Since every point of this singular locus has two preimages in K^2, the two points of C on the singular locus have four preimages in K^2. The two of these preimages lie in the diagonal Δ_{K^2}, and the other two points are the additional points $(1,-1)$ and $(-1,1)$.



9.1 **(a)** Let $\varphi_i : A \to A_i$, $i = 1, \ldots, n$ be finite (resp. integral) ring homomorphisms. Then the ring homomorphism $A \to \prod_{i=1}^n A_i$, , $a \mapsto (\varphi_i(a))_{i \in \{1,\ldots,n\}}$ is also finite (resp. integral).

(b) Let $A_i \subseteq A'_i$ be ring extensions, $x_i \in A'_i$, $1 \leq i \leq n$, and $x = (x_1, \ldots, x_n) \in \prod_{i=1}^n A'_i$. Then x is integral over $\prod_{i=1}^n A_i$ if and only x_i is integral over A_i for all $i = 1, \ldots, n$. Further, $\prod_{i=1}^n A_i$ is integrally closed in $\prod_{i=1}^n A'_i$ if and only if A_i is integrally closed in A'_i for all $i = 1, \ldots, n$,

9.2 Let $A \subseteq B$ be a ring extension.

(a) Let $r_1, \ldots, r_n$ be positive integers and $X_1, \ldots, X_n$ be indeterminates. If B is integral over A, then $B[X_1, \ldots, X_n]$ is integral over $A[X_1^{r_1}, \ldots, X_n^{r_n}]$.

(b) Let $f = f(X) \in A[X]$ be a monic polynomial of positive degree. If B is integral over A, then $B[X]$ is integral over $A[f]$.

9.3 Let $A \subseteq B$ be an extension of rings and let $x \in B^\times$. Show that

(a) x is integral over A if and only if $x \in A[x^{-1}]$. (**Hint:** Note that (multiplying by x^{-n+1} and conversely by x^{n-1}) $x^n + a_1x^{n-1} + \cdots + a_n = 0$, for some $a_1, \ldots, a_n \in A$, $n \geq 1$, if and only if $x = -a_1 - a_2x - \cdots - a_nx^{-n+1} \in A[x^{-1}]$.)

(b) $A[x] \cap A[x^{-1}]$ is integral over A.

(**Hint:** If $y = a_0 + \cdots + a_nx^n = b_0 + \cdots + b_mx^{-m}$ where $m, n \in \mathbb{N}^+$, $a_0, \ldots, a_n, b_0, \ldots, b_m \in A$. The A- submodule of B generated by $1, x, \ldots, x^{m+n+1}$ is a faithful $A[y]$-module.)

(c) If B is integral over A, then $B^\times \cap A = A^\times$ and $x^{-1} \in A[x]$ for all $x \in B^\times$.

9.4 Let $A \subseteq B$ be a ring extension. If $B \smallsetminus A$ is multiplicatively closed in B, then A is integrally closed in B. (**Hint:** Let $x \in B \smallsetminus A$. If x integral over A with an integral equation $x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ over A with minimal $n \in \mathbb{N}$. Then $n > 1$, since $x \notin A$. Further, $y := x^{n-1} + a_1x^{n-2} + \cdots + a_{n-1} \notin A$, otherwise $x^{n-1} + a_1x^{n-2} + \cdots + (a_{n-1} - y) = 0$ will be an integral equation of degree $n-1$, a contradiction to the minimality of n. But $xy = -a_n \in A$. Therefore $B \smallsetminus A$ is not closed under multiplication. a contradiction.)

9.5 **(a)** In the matrix ring $\mathrm{M}_2(\mathbb{Q})$ give two elements which are integral over $\mathbb{Z}$, but neither their sum nor their product are integral over $\mathbb{Z}$. (**Hint :** Consider the unipotent matrices $\mathfrak{E}_2+\mathfrak{N}$, where $\mathfrak{E}_2$ is the identity matrix and $\mathfrak{N}$ is a nilpotent matrix.)

(b) Let K be a field and let $A := K[Y^kX^{k+1} \mid k\in\mathbb{N}]$ be the K-subalgebra of the polynomial algebra $K[X,Y]$ generated by monomials Y^kX^{k+1}, $k\in\mathbb{N}$. Show that $A[XY]$ is contained in a finitely generated A-module, but XY is not integral over A. (Note that A is not noetherian!)

9.6 Let $A := \mathbb{Z}[X]/\langle 2X-1\rangle$ be the residue class $\mathbb{Z}$-algebra of the polynomial algebra $\mathbb{Z}[X]$ by the ideal generated by $2X-1$ and let $\varphi : \mathbb{Z}\hookrightarrow\mathbb{Z}[X]\xrightarrow{\pi} A$ be the canonical ring homomorphism.

(a) Is A a finite algebra over $\mathbb{Z}$? Is A integral over $\mathbb{Z}$?

(b) Describe the fibres of the map $\operatorname{Spec}\varphi : \operatorname{Spec}A \longrightarrow \operatorname{Spec}\mathbb{Z}$.

9.7 We say that an integral domain A with quotient field K is a valuation ring of K if for every $x\in K$, $x\neq 0$ if either $x\in A$ or $x^{-1}\in A$. Show that every valuation ring A is a normal domain.

9.8 Let $A\subseteq B$ be an integral extension of rings. Show that :

(a) Let $\mathfrak{m}\in\operatorname{Spm}A$ be a maximal ideal in A and let $S_\mathfrak{m} := A\smallsetminus\mathfrak{m}$. Then the natural map $B/\mathfrak{m}B\to S_\mathfrak{m}^{-1}(B/\mathfrak{m}B)$ is an isomorphism. (**Hint :** Show that the image of each $s\in S_\mathfrak{m}$ in $B/\mathfrak{m}B$ does not belong to $\mathfrak{M}$ for every $\mathfrak{M}\in\operatorname{Spm}B/\mathfrak{m}B$ and hence is a unit in $B/\mathfrak{m}B$.)

(b) $\mathfrak{m}_A=\mathfrak{m}_B\cap A$, where $\mathfrak{m}_A$ and $\mathfrak{m}_B$ denote the Jacobson-radical of A and B, respectively.

9.9 Let $\varphi : A\to B$ be an *injective* integral homomorphism of integral domains and let $\psi : B\to C$ be a ring homomorphism. Show that ψ is injective if and only if $\psi\varphi$ is injective.

9.10 Let A be an integral domain and $\mathfrak{p}$ be a *non-maximal prime* ideal in A. Show that $A_\mathfrak{p}$ can not be integral over A.

9.11 Let $\varphi : A\to B$ be a ring homomorphism and let $\varphi^* : \operatorname{Spec}B\longrightarrow\operatorname{Spec}A$ be the map associated to φ on spectra.

(a) If φ is integral over A, then the map φ^* is closed. See also Exercise 9.32 (b).

(b) The following conditions are equivalent :
(i) B is integral over A.
(ii) For every $y\in B$, the element $1/y$ is a unit in $\varphi(A)[1/y]\subseteq B[1/y] := B_y$.
(iii) The map $\operatorname{Spec}B[X]\to\operatorname{Spec}A[X]$ is closed.

(**Hint :** For a proof of (iii) $\Rightarrow$ (ii) consider the following commutative diagrams :

$$\begin{tikzcd}
A[X] \arrow[r, "{\varphi[X]}"] \arrow[d, "\varepsilon_{A,1/y}"'] & B[X] \arrow[d, "\varepsilon_{B,1/y}"] \\
\varphi(A)[X]/\langle yX-1\rangle=\varphi(A)[1/y] \arrow[r, "\varphi'"] & B[1/y]=B[X]/\langle yX-1\rangle
\end{tikzcd}$$

$$\begin{tikzcd}
\operatorname{Spec}B[X] \arrow[r, "{\varphi[X]^*}"] & \operatorname{Spec}A[X] \\
\operatorname{Spec}B[1/y] \arrow[u, "\varepsilon^*_{1/y}"] \arrow[r, "\varphi'^*"] & \operatorname{Spec}\varphi(A)[1/y]\,, \arrow[u, "\varepsilon^*_{A,1/y}"']
\end{tikzcd}$$

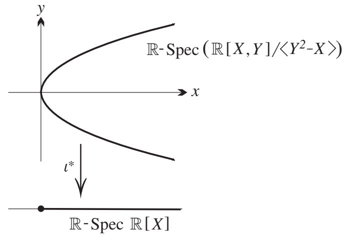
where $\varepsilon_{A\,,\,1/y} : A[X] \to \varphi(A)[1/y]$, $F \mapsto \varphi(A)(F)(1/y)$ (resp. $\varepsilon_{B\,,\,1/y} : B[X] \to B[1/y]$, $G \mapsto G(1/y)$) is the substitution A-algebra (resp. B-algebra homomorphism) and $\varphi' : A' := \varphi(A)[1/y] \to B[1/y] = B_y$, is the canonical ring homomorphism induced by φ. Note that, since $\varepsilon_{A\,,\,1/y}$, $\varepsilon_{B\,,\,1/y}$ are surjective and φ' is injective. Therefore the maps $\varepsilon^*_{A\,,\,1/y}$, $\varepsilon^*_{B\,,\,1/y}$ are homeomorphism onto the closed subsets, see Exercise 8.25 (a) and hence, since φ' is injective, φ'^* is surjective see Exercise 8.25 (b). This proves that $\{\mathfrak{p}' \in \operatorname{Spec} \varphi(A)[1/y] \mid 1/y \in \mathfrak{p}'\} = \varphi'^*\big(\{\mathfrak{q} \in \operatorname{Spec} B_y \mid 1/y \in \mathfrak{q}\}\big) = \varphi'^*(\emptyset) = \emptyset$, since $y \in B$, and hence $1/y$ is a unit in $\varphi(A)[1/y]$.

Remark : It follows from this Exercise that : *Integral morphisms of affine schemes is even an universally closed map.*)

9.12 **(a)** Let K be an algebraically closed field and let $\varphi : A \to B$ be an integral K-algebra homomorphism of K-algebras of finite type. Then $\varphi^*(K\text{-Spec}\, B) = \mathrm{V}_K(\operatorname{Ker}\varphi)$. (**Hint :** It is enough to prove the inclusion $\mathrm{V}_K(\operatorname{Ker}\varphi) \subseteq \varphi^*(K\text{-Spec}\, B)$. To prove this, replacing A by $A/\operatorname{Ker}\varphi$, we may assume that φ is injective. Then, since φ is injective and integral, for every $\xi \in K\text{-Spec}\, A$ the maximal ideal $\mathfrak{m}_\xi$, there exists a maximal ideal $\mathfrak{n} \in \operatorname{Spm} B$ lying over $\mathfrak{m}_\xi$, i. e. $\mathfrak{m}_\xi = \varphi^*(\mathfrak{n})$. Now by Hilbert's Nullstellensatz (HNS 3) (see R8.1.3 (b)) $\mathfrak{n} \in K\text{-Spec}\, B$.)

(b) Let K be an algebraically closed field. Let $\varphi : A \to B$ be an integral K-algebra homomorphism of K-algebras of finite type. Then the map $\varphi^* : K\text{-Spec}\, B \to K\text{-Spec}\, A$ associated to φ on K-spectra is closed. (**Hint :** Use part (a).)

(c) If K is not algebraically closed, then give an example to show that the assertion in (b) is not true. (**Hint :** For example, for the natural inclusion $\iota : \mathbb{R}[X] \to \mathbb{R}[X,Y]/\langle Y^2 - X\rangle$, the image $\iota^*(\,\mathbb{R}\text{-Spec}\, \mathbb{R}[X,Y]/\langle Y^2 - X\rangle\,) = \{a \in \mathbb{R} \mid a \geq 0\}$ is not closed in the $\mathbb{R}$-Zariski topology of $\mathbb{R}$-Spec $\mathbb{R}[X]$.



.)

9.13 Let $A \subseteq A'$ be an integral extension of rings and let $\mathfrak{p} \in \operatorname{Spec} A$. Suppose that there is *only one prime* ideal $\mathfrak{p}' \in \operatorname{Spec} A'$ lying over $\mathfrak{p}$. Show that :

(a) $\mathfrak{p}' A'_{\mathfrak{p}}$ is the only maximal ideal of $A'_{\mathfrak{p}}$, i. e. the ring $A'_{\mathfrak{p}}$ is local.

(b) $A'_{\mathfrak{p}'} = A'_{\mathfrak{p}}$. (**Hint :** Check that the pair $(A'_{\mathfrak{p}}, \iota_{\mathfrak{p}} : A' \to A'_{\mathfrak{p}})$ satisfies the universal property of $(A'_{\mathfrak{p}'}, \iota_{\mathfrak{p}'} : A' \to A'_{\mathfrak{p}'})$. For this, let $\psi : A' \to B$ be a ring homomorphism with $\psi(A' \smallsetminus \mathfrak{p}') \subseteq B^\times$. Then, since $A'_{\mathfrak{p}}$ is a local ring with the unique maximal ideal $\mathfrak{p}' A'_{\mathfrak{p}}$ by the part (a), $A'_{\mathfrak{p}} \smallsetminus \mathfrak{p}' A'_{\mathfrak{p}} = (A'_{\mathfrak{p}})^\times$ and hence $\iota_{\mathfrak{p}}(A' \smallsetminus \mathfrak{p}')(A'_{\mathfrak{p}})^\times$ too. Now, since $(A \smallsetminus \mathfrak{p}) \subseteq (A' \smallsetminus \mathfrak{p}')$, $\psi(A \smallsetminus \mathfrak{p}) \subseteq \psi(A' \smallsetminus \mathfrak{p}') \subseteq B^\times$, it follows that ψ factors uniquely through $A'_{\mathfrak{p}}$, i. e. there exists a unique ring homomorphism $\psi_{\mathfrak{p}} : A'_{\mathfrak{p}} \dashrightarrow B$ such that the diagram

$$\begin{tikzcd} A' \arrow[r, "\iota_{\mathfrak{p}}"] \arrow[d, "\psi"'] & A'_{\mathfrak{p}} \arrow[dl, dashed, "\psi_{\mathfrak{p}}"] \\ B & \end{tikzcd}$$

is commutative, i. e. $\psi = \psi_{\mathfrak{p}}\, \iota_{\mathfrak{p}}$.)

(c) $A'_{\mathfrak{p}'}$ is integral over $A_{\mathfrak{p}}$. (**Remark :** Moreover, the converse of (c) holds i. e. if $\mathfrak{p}' \in \operatorname{Spec} A'$ and $\mathfrak{p}' \cap A = \mathfrak{p}$, and if $A'_{\mathfrak{p}'}$ is integral over $A_{\mathfrak{p}}$, then $\mathfrak{p}'$ is the only prime ideal in A' lying over $\mathfrak{p}$. Proof is similar to that of Exercise 9.14 (a).)

9.14 **(a)** Let $A \subseteq A'$ be an integral extension of *integral domains*, $\mathfrak{p} \in \operatorname{Spec} A$ and let $\mathfrak{p}'$, $\mathfrak{q}' \in \operatorname{Spec} A'$ be two distinct prime ideals in A' lying over $\mathfrak{p}$. Show that $A'_{\mathfrak{p}'}$ is not integral over $A_{\mathfrak{p}}$.

(b) Let K be a field, X an indeterminate, $A' := K[X]$, $Y := X^2$, and $A := K[Y]$. Further, let $\mathfrak{p} := \langle Y-1\rangle$ and $\mathfrak{p}' := \langle X-1\rangle$ be the ideals in A and A' generated by $Y-1$ and $X-1$, respectively. Then $A \subseteq A'$ is integral extension of integral domains. Is $A'_{\mathfrak{p}'}$ integral over $A_{\mathfrak{p}}$?

(c) Let $A' := \mathbb{R}[X]$, $A := \mathbb{R}[X^2-1]$, $\mathfrak{p}' := \langle X-1\rangle \in \operatorname{Spec} A'$, and $\mathfrak{p} := \mathfrak{p}' \cap A$. Then A' is integral over A, but the localization $A'_{\mathfrak{p}'}$ is not integral extension of $A_{\mathfrak{p}}$. Is this a counter example for R 9.1.5 (b)? (**Hint :** Consider the element $1/(X+1) \in A'_{\mathfrak{p}'}$.)

9.15 Let $A \subseteq B$ be a ring extension. Suppose that B is noetherian and for each minimal prime ideal $\mathfrak{q} \in \operatorname{Min} \operatorname{Spec} B$, the ring extension $A/\mathfrak{q} \cap A \subseteq B/\mathfrak{q}$ is integral. Show that B is integral over A. (**Hint :** Note that since B is noetherian the set $\operatorname{Min}(\operatorname{Spec} B, \subseteq)$ is finite. For $x \in B$, consider the subset $S := \{F(x) \mid F \in A[X] \text{ is monic}\}$ and show that S is multiplicatively closed in B and that $0 \in S$.)

9.16 Let A be an integral domain with the quotient field K.

(a) Let $L\,|\,K$ be a finite field extension of K and let $\overline{A}_L$ be the integral closure of A in L. Then the field L is the quotient field of $\overline{A}_L$. (**Hint :** In fact, every element $x \in L$ can be expressed as a fraction b/a with $b \in \overline{A}_L$ and $a \in A$, $a \neq 0$.)

(b) Let $A \subseteq B$ be integral domains with quotient fields K and L respectively. Suppose that B is an A-algebra of finite type and $L\,|\,K$ is a finite (field) extension. Then show that there exists $f \in A$ such that B_f is a finite A_f-module. (**Hint :** Suppose that $B = A[x_1, \ldots, x_n]$ with $x_i \in B$, $i = 1, \ldots, n$. Use the part (a) to write $x_i = b_i/a_i$, $b_i \in B$ integral over A, $a_i \in A$, $a_i \neq 0$, $i = 1, \ldots, n$. Then for $f := \prod_{i=1}^n a_i$, prove that $A_f \subseteq B_f = A_f[x_1, \ldots, x_n]$ is an integral extension.)

9.17 Let $A \subseteq A'$ be an integral extension of rings and let $\rho : A \to \Omega$ be a ring homomorphism from A into an algebraically closed field Ω. Then ρ extends to a ring homomorphism $\rho' : A' \to \Omega$. (**Hint : Algebraic field extension case :** Suppose that $A'|A$ is an algebraic field extension $K\,|\,k$. By Zorn's Lemma to the set $\mathcal{S} := \{(E, \eta) \mid L$ is a subfield with $k \subseteq E \subseteq K$ and $\eta_{|K} = \rho\}$ with the order defined by $(E, \eta) \leq (E', \eta')$ if $E \subseteq E'$ and $\eta'_{|E} = \eta$, there exists a maximal extension $\eta_0 : E_0 \to \Omega$. To prove $E_0 = K$, consider $x \in K$ and the substitution homomorphism $\varepsilon_x : E[X] \to E[x] \subseteq K$, $X \mapsto x$; since x is algebraic over E, its kernel $\operatorname{Ker} \varepsilon_x = \langle \mu_{x,E}\rangle \neq 0$ is the principal ideal generated by the minimal polynomial $\mu := \mu_{x,E}$ of x over E. Further, since Ω is algebraically closed, the polynomial $\eta_0(\mu) \in \Omega[X]$ has a zero $y \in \Omega$. Note that the kernel of the substitution homomorphism $\varepsilon_y : E[X] \to E[y] \subseteq \Omega$ is $\langle \mu\rangle$ and hence ε induce a homomorphism $\eta' : E' := E[y] \to \Omega$ which extends η_0. In particular, $(E_0, \eta_0) \leq (E', \eta')$ and hence $x \in E_0$ by the maximality of (E_0, η_0). This proves that $E_0 = K$ and $\eta_0 : K \to \Omega$ is the desired extension of ρ.

General case : Since $\mathfrak{p} := \operatorname{Ker} \rho \in \operatorname{Spec} A$, $\rho(s) \neq 0$ in the field Ω and so $\rho(s) \in \Omega^{\times}$ for every $s \in A \smallsetminus \mathfrak{p}$. Therefore there exists a homomorphism $\xi : A_{\mathfrak{p}} \to \Omega$ with $\mathfrak{p}A_{\mathfrak{p}} \subseteq \operatorname{Ker} \xi$. Put $\kappa(\mathfrak{p}) := A_p/\mathfrak{p}A_{\mathfrak{p}}$. Then $\kappa(\mathfrak{p})$ is a field and ξ factors through a homomorphism $\xi : \kappa(\mathfrak{p}) \to \Omega$. Moreover, $A_{\mathfrak{p}} \to A'_{\mathfrak{p}}$ is injective and $A'_{\mathfrak{p}}$ is integral over $A_{\mathfrak{p}}$. Therefore (by R 9.1.8 (1) and (3)) there exists a maximal ideal $\mathfrak{M}' \in \operatorname{Spm} A'_{\mathfrak{p}}$ lying over $\mathfrak{p}A_{\mathfrak{p}}$. Finally, $K := A'_{\mathfrak{p}}/\mathfrak{M}'$ is a field which is an (integral=) algebraic extension of $\kappa(\mathfrak{p})$ and hence ξ' extends to a homomorphism $\eta : K \to \Omega$ by the algebraic field extension case. Now, the composition $\rho' : A' \to A'_{\mathfrak{p}} \xrightarrow{\pi_{\mathfrak{M}'}} K \xrightarrow{\eta} \Omega$ is the desired extension of ρ.)

9.18 (N o r m a l i z a t i o n) Let A be a ring and let $Q := \mathrm{Q}(A)$ be its total quotient ring. Then the integral closure $\overline{A}$ of A in Q is called the n o r m a l i z a t i o n of A. An integral domain A is called n o r m a l if $\overline{A} = A$. The normalization of an integral domain A is the smallest subring of its quotient field $\mathrm{Q}(A) = K$ which is normal and contains A.

For example : *Every factorial domain A is normal. In particular, polynomial rings over* $\mathbb{Z}$ *or a K are normal.* For the *proof* note that if $x = a/b \in \mathrm{Q}(A)$ with $\gcd(a,b) = 1$ and x is a zero of a polynomial $a_nX^n + \cdots + a_0 \in A[X]$ then a divides a_0 and b divides a_n. More generally, $bX - a$ is a generator of the kernel of the subsitution homomorphism $\varepsilon : A[X] \to \mathrm{Q}(A), X \mapsto a/b$.

9.19 (a) (Monoid algebras and their normalization) Let M be a numerical monoid, i. e., M is a submonoid of $\mathbb{N} = (\mathbb{N},+)$ such that $\mathbb{N} \setminus M$ is finite. Let $A = K[M] := \{\sum_{m\in M} a_mT^m \in K[T]\} \subseteq K[T]$ be the monoid algebra of M over a field K. Then the polynomial algebra $K[T]$ is finite over $K[M]$, indeed, $\mathrm{Dim}_K K[T]/K[M] = \mathrm{card}\,(\mathbb{N}\smallsetminus M)$, and so $K[T]$ is integral over $K[M]$. Since T belongs to the quotient field of $K[M]$ and $K[T]$ is normal, $K[T]$ is the normalization of $K[M]$. The K-algebra $K[M]$ is called the coordinate algebra of the monomial curve over K defined by M. (See the Exercise 9.20.)

(b) *Let K be a field and let A be a normal K-subalgebra of $K[T]$, $A \neq K$. Then A is a polynomial algebra $K[f]$ for some $f \in A$.* (Note that f is necessarily a non-constant polynomial in A of least degree.)

As a consequence we get : *Let A be a K-subalgebra of $K[T]$, $A \neq K$. Then the normalization $\overline{A}$ of A is a polynomial algebra $K[f]$ for some non-constant polynomial $f \in K[T]$.* (Note that every K-subalgebra of $K[T]$ is a K-algebra of finite type.)

(**Hint :** For a proof, let $\mu_T = X^n + f_{n-1}X^{n-1} + \cdots + f_0 \in \mathrm{Q}(A)[X]$ be the minimal polynomial of T over $\mathrm{Q}(A)$. By the Exercise 9.23, the coefficients $f_0,\ldots,f_{n-1} \in A$. But every non-constant coefficient f of μ_T generates the field $\mathrm{Q}(A)$ over K (see the proof of Lüroth's theorem in the Supplement S 9.1.4). Then $K[f] \subseteq A \subseteq \mathrm{Q}(A) = K(f)$ and $K[f] = A$, since $K[T]$ and hence A is integral over $K[f]$ and $K[f]$ is normal.)

(c) In general a K-algebra A of finite type is called rational if it is an integral domain and if the quotient field $\mathrm{Q}(A)$ of A is K-isomorphic to a rational function field $K(T_1,\ldots,T_m)$ in m variables $T_1,\ldots,T_m$. The integer m is nothing but the transcendence degree of the field extension $K \subseteq \mathrm{Q}(A)$. By Lüroth's theorem (Supplement S 9.1.4), any K-subalgebra A of $K(T)$, $A \neq K$, of finite type is rational with $m = 1$.

(d) Consider the K-algebra (substitution) homomorphism $\varepsilon : K[X,Y] \to K[T]$ defined by $x := \varepsilon(X) = T^2 - 1$ and $y := \varepsilon(Y) = T(T^2-1)$ and the K-subalgebra $A := \mathrm{Img}\,\varepsilon$ of $K[T]$. Then *the polynomial algebra $K[T]$ is the normalization of $A \xleftarrow{\sim} K[X,Y]/\big(Y^2 - X^2(X+1)\big)$*.

(**Hint :** Obviously, if $f \in K[X,Y]$ with $f \neq 0$ and if $\deg_Y f \leq 1$, i. e. $f = f_0 + f_1Y$, $f_0, f_1 \in K[X]$, then $f \notin \mathrm{Ker}\,\varepsilon$, since $\varepsilon(f) = f(\varepsilon(X),\varepsilon(Y)) = f_0(T^2-1) + f_1(T^2-1)T(T^2-1) \neq 0$. Therefore $\mathrm{Ker}\,\varepsilon$ is the principal ideal generated by $Y^2 - X^2 - X^3$. Note that $T = y/x \in \mathrm{Q}(A)$ the quotient field of A and that A is a normal domain, see details in R 9.1.10 (b).)

9.20 (Affine monomial curves) Let K be an infinite field and let $m_1,\ldots,m_n$ be positive integers with $\gcd(m_1,\ldots,m_n) = 1$. Let $\gamma : K \to K^n$ be the curve defined by $t \mapsto (t^{m_1},\ldots,t^{m_n})$.

(a) Show that γ is injective and the image Img *gamma* is an affine K-algebraic set. This is called the affine monomial curve defined (over K) by the sequence $m_1,\ldots,m_n$. The defining ideal $\mathrm{I}_K(\mathrm{Img}\,\gamma)$ is the kernel $\mathrm{Ker}\,\varepsilon$ of the K-algebra (substitution) homomorphism $\varepsilon : K[X_1,\ldots,X_n] \to K[T]$ defined by $X_i \mapsto T^{m_i}$, $i = 1,\ldots,n$, and so the coordinate K-algebra of $\mathrm{Img}\,\gamma$ is $A_\gamma := K[X_1,\ldots,X_n]/\mathrm{Ker}\,\varepsilon \xrightarrow{\sim} K[T^{m_1},\ldots,T^{m_n}] = K[M] \subseteq K[T]$, where $M = \mathbb{N}m_1 + \cdots + \mathbb{N}m_n$ is the numerical monoid generated by the elements $m_1,\ldots,m_n$.

(b) The quotient field of A_γ is the rational function field $K(T)$. (This means, by definition, *affine monomial curves are rational curves*.) $K[T]$ is the normalization of A_γ, i. e. $K[T]$ is the integral closure of A_γ in $K(T)$. Again by definition, *the affine line* $K = K$-Spec $K[T]$ *is the normalization of the curve* $\operatorname{Img}\gamma$ (and $\gamma : K \to \operatorname{Im}\gamma$ is the normalization map).

(c) There exists a K-algebra isomorphism $A_\gamma \simeq K[T]$ if and only if $m_i = 1$ for some i. In this case find a (minimal) set of generators for the ideal $\mathrm{I}_K(\operatorname{Img}\gamma)$.

(d) If $n = 2$ then the ideal $\mathrm{I}_K(\operatorname{Img}\gamma)$ is generated by $X_1^{m_2} - X_2^{m_1}$.

(e) Let $n = 3$ and $m_1 := 2m, m_2 := 2m+1, m_3 := 2m+2$, $m \in \mathbb{N}^*$. Then the ideal $\mathrm{I}_K(\operatorname{Img}\gamma)$ is generated by two binomials. (**Hint:** $X_2^2 - X_1X_3$ and $X_3^m - X_1^{m+1}$ generate $\mathrm{I}_K(\operatorname{Img}\gamma)$.)

(f) Let $n = 3$ and $m_1 := 2m+1, m_2 := 2m+2, m_3 := 2m+3$, $m \in \mathbb{N}^*$. Then the ideal $\mathrm{I}_K(\operatorname{Img}\gamma)$ is generated by three binomials and can not be generated by two polynomials. (**Hint:** $X_2^2 - X_1X_3$, $X_1^{m+2} - X_2X_3^m$ and $X_3^{m+1} - X_1^{m+1}X_2$ generate $\mathrm{I}_K(\operatorname{Img}\gamma)$. — **Remark:** If $\operatorname{Ker}\varepsilon$ is generated by $n-1$ polynomials then we say that the curve $\operatorname{Img}\gamma$ is an (ideal-theoretic) complete intersection. In this case $\mathrm{I}_K(\operatorname{Img}\gamma)$ is generated by $n-1$ binomials. If there exist $n-1$ polynomials $F_1, \ldots, F_{n-1} \in K[X_1, \ldots, X_n]$ such that $\mathfrak{a} = \sqrt{(F_1, \ldots, F_{n-1})}$, then we say that the curve $\operatorname{Img}\gamma$ is a set-theoretic complete intersection. In 1970 J. Herzog has proved that the ideal $\mathrm{I}_K(\operatorname{Img}\gamma)$ of an affine monomial space curve ($n = 3$) is always generated by three binomials and using the explicit form of these generators, he proved that affine monomial space curves are set-theoretic complete intersections. (In the Example (f) try to find two polynomials F and G such that $\mathrm{I}_K(\operatorname{Img}\gamma) = \sqrt{(F, G)}$.) For general n this is still an open question.)

9.21 Let A be an integral domain with quotient field K.

(a) (Localization and Normalization commute) Let $S \subseteq A \setminus \{0\}$ be a multiplicatively closed subset. Then the localization of the normalization $S^{-1}\overline{A}$ is equal to the normalization of the localization $\overline{S^{-1}A}$.

(b) (Normality a local property) The following statements are equivalent:
(i) A is normal. (ii) $A_\mathfrak{p}$ is normal for every prime ideal $\mathfrak{p} \in \operatorname{Spec} A$. (iii) $A_\mathfrak{m}$ is normal for every maximal $\mathfrak{m} \in \operatorname{Spm} A$. (**Remark:** An arbitrary ring A is said to be normal if $A_\mathfrak{p}$ is a normal domain for every $\mathfrak{p} \in \operatorname{Spec} A$. If A is an integral domain, then this definition is equivalent to the earlier one by part (a). Furthermore, for a ring A with finitely many minimal primes ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \operatorname{Spec} A$ (for example, if A is noetherian) and the total quotient ring $\mathrm{Q}(A)$, the following statements are equivalent: (i) A is normal. (ii) A is reduced and integrally closed in $\mathrm{Q}(A)$. (iii) A is a finite product of normal domains $A_1, \ldots, A_r$. Moreover, in this case, there exists a permutation $\sigma \in \mathfrak{S}_r$ such that $A_i \xrightarrow{\sim} A/\mathfrak{p}_{\sigma(i)}$ for every $i = 1, \ldots, r$.)

9.22 Let $A \subseteq A'$ be an extension of rings, $A[X]$ be the polynomial ring in one indeterminate X over A and let $f \in A[X]$ be a monic polynomial. Then:

(a) There exists a ring extension A'' of A such that f splits into linear factors in $A''[X]$, i. e. $f(X) = \prod_{i=1}^{d} (X - x_i)$ with $x_1, \ldots, x_d \in A''$. Moreover, A'' is a free A-module of rank $d!$, where $d := \deg f$.

(b) Suppose that $f = gh$ with $g, h \in A'[X]$ and g is monic. Then h is monic and the coefficients of g and h are integral over A.

9.23 Let A be an integral domain with quotient field K, $\overline{A}$ the integral closure of A in K, $L\,|\,K$ be a field extension and let $x \in L$. Show that the following statements are equivalent:
(i) x is integral over A. (ii) x is algebraic over K and the minimal polynomial (of x over K) $\mu_{x,K} \in \overline{A}[X]$.

In particular, if A is normal and if $x \in L$ is integral over A, then $\mu_{x,K} \in A[X]$ and $\mu_{x,K}(x) = 0$ is an integral equation of x over A. Furthermore, if the field extension $L\,|\,K$ is finite, then the above equivalent statements (i) and (ii) are further equivalent to the statement:

(iii) $\chi_{x,L|K} \in \overline{A}[X]$, where $\chi_{x,L|K}$ denote the characteristic polynomial of the K-linear map $\lambda_x : L \to L$, $y \mapsto xy$. For a proof note that $\mathrm{V}(\chi_{x,L|K}) = \mathrm{V}(\mu_{x,K})$.

9.24 Let A be a reduced ring with finitely many minimal prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ (for example, if A is noetherian) and let $\mathrm{S}_0 = A \smallsetminus \bigcup_{i=1}^r \mathfrak{p}_i$ (the set of all non-zerodivisors in A, see Exercise 8.8). Then there is a canonical isomorphism $\mathrm{Q}(A) = \mathrm{S}_0^{-1}A \xrightarrow{\sim} \prod_{i=1}^r \mathrm{Q}(A/\mathfrak{p}_i)$. Let $\overline{A}$ be the integral closure of A in its total quotient ring $\mathrm{Q}(A)$. Show that there is a canonical isomorphism: $\overline{A} \xrightarrow{\sim} \prod_{i=1}^r \overline{A}_i$, where $\overline{A}_i$ is the integral closure of $A/\mathfrak{p}_i$ in its total quotien ring $\mathrm{Q}(A/\mathfrak{p}_i)$, $i = 1, \ldots, r$. (**Hint:** If $e \in A$ is an idempotent element in any ring, then $e^2 - e = 0$ is an integral equation for e over any subring of A.)

9.25 (Conductor) Let $A \subseteq B$ be a ring extension and let $\mathfrak{c}_{B|A} := \{c \in A \mid cB \subseteq A\} = \mathrm{Ann}_A(B/A)$ is the so-called conductor of B over A. The conductor of A is the ideal $\mathfrak{c}_A = \mathfrak{c}_{\overline{A}|A}$, where A is the integral closure of A in its total quotient ring $\mathrm{Q}(A)$. Show that:

(a) $\mathfrak{c}_{B|A}$ is the largest ideal in A which is also an ideal in B. If $\mathfrak{c}_{B|A}$ contains a non-zerodivisor in A, then $B \subseteq Aa^{-1}$ can be embedded in the total quotient ring $\mathrm{Q}(A)$ of A. Furthermore, if A is noetherian, then B is finite over A.

(b) If $\mathfrak{p} \in \operatorname{Spec} A \smallsetminus \mathrm{V}(\mathfrak{c}_{B|A})$, then $A_\mathfrak{p} = B_\mathfrak{p}$. Moreover, if B is finite over A, then the converse holds, i. e. if $A_\mathfrak{p} = B_\mathfrak{p}$, then $\mathfrak{p} \in \operatorname{Spec} A \smallsetminus \mathrm{V}(\mathfrak{c}_{B|A})$.

(c) Suppose that A is an integral domain with quotient field K, $B = \overline{A}$ is the integral closure of A in K and B is finite over A (all these assumptions are satisfied if A is a k-algebra of finite type over an arbitrary field). Then $\mathfrak{c}_{B|A} \neq 0$ and for $\mathfrak{p} \in \operatorname{Spec} A$, $A_\mathfrak{p}$ is integrally closed if and only if $\mathfrak{p} \notin \mathrm{V}(\mathfrak{c}_{B|A})$. In particular, the subset $\{\mathfrak{p} \in \operatorname{Spec} A \mid A_\mathfrak{p} \text{ is integrally closed}\}$ if open and dense in $\operatorname{Spec} A$.

9.26 (Conductor of Monoid Algebra) Let $m_1, \ldots, m_n$ be positive integers with $\gcd(m_1, \ldots, m_n) = 1$ and let M be the submonoid of $\mathbb{N} = (\mathbb{N}, +)$ generated by $m_1, \ldots, m_n$. For a field K, the normalization of the affine monomial curve $X := \operatorname{Spec} A$, where $A := K[T^{m_1}, \ldots, T^{m_n}] = k[M] = \oplus_{m \in M} KT^m$, is the affine line $\mathbb{A}_K^1 = \operatorname{Spec} K[T]$, (see the Exercise 9.19). The conductor $\mathfrak{c}_A = \mathrm{Ann}_{K[M]} K[T]/K[M]$ is the ideal $T^f k[T]$, where f is the least non-negative integer with $f + \mathbb{N} \subseteq M$. This integer $f = f_M$ is also called the conductor of M and $g = g_M := f - 1 \notin M$ is called the Frobenius number of M. The (vector space) dimension $\mathrm{Dim}_K K[T]/K[M] = \mathrm{Card}(\mathbb{N} \smallsetminus M)$ is the number of gaps and is called the degree of singularity $\delta = \delta_A = \delta_M$ of A (or of M). If $m \in M$, $0 \le m < f$, then $f - 1 - m = g - m \notin M$ and hence $2\delta_M \ge f_M$. If $M \neq \mathbb{N}$, then the origin $0 \in X$ is the only non-normal (= singular) point of the curve X. For the simplest case $n = 2$, one has $f_M = (m_1 - 1)(m_2 - 1)$ and $\delta_M = f_M/2 = (m_1 - 1)(m_2 - 1)/2$ which was first proved by Sylvester. (**Hint:** If $m_1 < m_2$, then show that $\delta_M = \delta_{M'} + \binom{m_1}{2}$ where $M' = \mathbb{N}m_1 + \mathbb{N}(m_2 - m_1)$. — In general, if $f_M = 2\delta_M$, then the monoid M is called symmetric or Gorenstein. This is the case if and only if the local ring $A_{\mathfrak{m}_0}$, $\mathfrak{m}_0 = AT^{m_1} + \cdots + AT^{m_n}$, in the origin $0 \in X$ is *Gorenstein.*)

9.27 Let K be a field of characteristic $\neq 2$ and let ${}^2K^\times := \{x^2 \mid x \in K^\times\}$be the group of non-zero squares Then the residue-class group $K^\times/{}^2K^\times$ is called the quadratic residue-class group of K. (Every element of $K^\times/^2K^\times$ has the self inverse and hence $K^\times/^2K^\times$ is a vector space over $\mathbb{F}_2$.)

(a) Let $D \in K^\times \smallsetminus {}^2K^\times$, $K[\sqrt{D}] := K[X]/(X^2 - D)$, $\sqrt{D} := x =$ the residue class of X. Show that $K[\sqrt{D}]$ is a quadratic field extension of K and the map $K[\sqrt{D}] \longmapsto D \cdot {}^2K^\times$ induces a bijective map on the set $\{[L] \mid L|K \text{ is quadratic field extension of } K\}$ of K-algebra isomorphism classes of the quadratic field extensions of K onto the set of non-trivial elements of $K^\times/^2K^\times$.

(b) Let K be the quotient field of the factorial domain A and let $\mathbb{P}(A)$ be a complete representative system for the associative classes of the prime elements of A. Show that:

$$K^\times/^2K^\times \xrightarrow{\sim} \left(A^\times/^2A^\times\mathbb{Q}\right) \times \mathbb{F}_2^{(\mathbb{P}(A))}.$$

(c) For the following fields K give a (canonical) representative system for the isomorphism classes of the quadratic field extensions of K:

(i) K is a finite field of characteristic $\neq 2$. (ii) $K = \mathbb{R}$ or $K = \mathbb{C}$. (iii) $K = \mathbb{Q}$.

(iv) $K = k(X)$ (resp. $K = k((X))$) the rational function field (resp. the field of formal Laurent series) in one variable over a field k of $\operatorname{Char} k \neq 2$.

(v) $K = \mathbb{Q}_p$ the field of p-adic numbers.

9.28 (Quadratic extensions of polynomials rings) Let K be a field, $K[X_1,\ldots,X_n]$ the polynomial ring in n indeterminates $X_1,\ldots,X_n]$ over K of characteristic $\neq 2$ and let $f \in K[X_1,\ldots,X_n]$ be a polynomial which is *not a square* in $K[X_1,\ldots,X_n]$. Show that $A := K[X_1,\ldots,X_n,Y]/\langle f\rangle$ (with Y a further indeterminate) is normal if and only if f is *square-free* in $K[X_1,\ldots,X_n]$.

9.29 Let K be the quotient field of the factorial domain A with $2 \in A^\times$ and let $\mathbb{P}(A)$ be a complete representative system for the associative classes of the prime elements of A. Further, let $D = \varepsilon\pi_1^{\nu_1}\cdots\pi_r^{\nu_r} \in A$ with $\varepsilon \in A^\times$ and $\pi_1,\ldots,\pi_r \in \mathbb{P}(A)$ are pairwise distinct, $\nu_1,\ldots,\nu_r \geq 1$, be a non-square element in A and $L := K[\sqrt{D}] = K[X]/\langle X^2 - D\rangle$. Then L is a quadratic extension of K.

(a) An element $y = a + b\sqrt{D} \in L$, $a, b \in K$, is integral over A if and only if $a \in A$ and b is fo the form $b'/\pi_1^{\mu_1}\cdots\pi_r^{\mu_r}$ with $b' \in A$ and $\mu_1 \leq \nu_1/2,\ldots,\mu_r \leq \nu_r/2$.

(b) $A[\sqrt{D}] = A[X]/\langle X^2 - D\rangle$ is normal if and only if $\nu_1 = \cdots = \nu_r = 1$ (i. e. D is square-free). (**Remark:** The assertion (a) and (b) are also true if A is noetherian and normal with $2 \in A^\times$.)

9.30 Let A be a normal domain with quotient field K.

(a) The polynomial ring $A[X]$ in one indeterminate X over A is also normal.

(b) Suppose that A is *noetherian* and $L|K$ is a finite separable field extension. Then the integral closure $\overline{A}_L$ of A in L is a *finite* A-algebra. In particular, if A is noetherian, then $\overline{A}_L$ is a finite A-module. (**Hint:** Since $L|K$ is finite separable, the trace form $\operatorname{Tr}_{L|K} : L \times L \to K$, $(x,y) \mapsto \operatorname{Tr}(xy)$ is a non-degenerate bilinear form. Use this to show that there is a K-basis $y_1,\ldots,y_d$ of L such that $\overline{A}_L \subseteq Ay_1 + \cdots + Ay_d$.)

9.31 Let A be a *normal* domain.

(a) Let X be an indeterminate over A and let $A[X] \subseteq B$ be an integral extension. For every $\mathfrak{m} \in \operatorname{Spm} B$, show that there exists $\mathfrak{q} \in \operatorname{Spec} B$ with $\mathfrak{q} \subsetneq \mathfrak{m}$ and $\mathfrak{q} \cap A = \mathfrak{m} \cap A$.

(b) Let B be an A-algebra the structure homomorphism $\varphi : A \to B$. Suppose that B is a cyclic A-algebra generated by $x \in B$, i. e. $B = A[x]$, B an integral domain and φ is integral over A. Show that B is a free A-module of finite rank.

9.32 Let $X_1, \ldots, X_{n-1}, X_n$ be indeterminates, $A := \mathbb{C}[X_1, \ldots, X_{n-1}]$, $F := F(X_n) \in A[X_n]$ be a *monic* polynomial over A and let $\varphi : A \to A[X_n]/\langle F \rangle =: B$ be the canonical ring homomorphism. Further, let $a := (a_1, \ldots, a_n) \in \mathbb{C}^n$, $\mathfrak{M}_a := \langle X_1 - a_1, \ldots, X_n - a_n \rangle \in \operatorname{Spm} A[X_n]$ with $F(a_1, \ldots, a_n) = 0$ and let $\overline{\mathfrak{M}}_a \in \operatorname{Spm} B$ denote the image of $\mathfrak{M}_a$ in B. Show that $\mathfrak{m} := \overline{\mathfrak{M}}_a \cap A \in \operatorname{Spm} A$ is a maximal ideal in A and that the canonical ring homomorphism $\mathbb{C} = A/\mathfrak{m} \longrightarrow B_{\overline{\mathfrak{M}}_a}/\mathfrak{m} B_{\overline{\mathfrak{M}}_a}$ is an isomorphism if and only if $\partial F/\partial X_n(a_1, \ldots, a_n) \neq 0$.

9.33 Let $\varphi : A \to A'$ be a ring homomorphism and let $\varphi^* : \operatorname{Spec} A' \longrightarrow \operatorname{Spec} A$ be the map associated to φ on spectra.

(a) Consider the following three statements :

(i) $\varphi^* : \operatorname{Spec} A' \to \operatorname{Spec} A$ is a closed map, i. e. it maps closed sets to closed sets.

(ii) The map φ has the Going-up property, i. e. for prime ideals $\mathfrak{p}' \in \operatorname{Spec} A'$ and $\mathfrak{p} \in \operatorname{Spec} A$ with $\varphi^{-1}(\mathfrak{q}') \subseteq \mathfrak{p}$, there exists a prime $\mathfrak{p}' \in \operatorname{Spec} A'$ with $\varphi^{-1}(\mathfrak{p}') = \mathfrak{p}$ and $\mathfrak{q}' \subseteq \mathfrak{p}'$.

(iii) For a prime ideal $\mathfrak{q}' \in \operatorname{Spec} A'$ with $\mathfrak{q} := \varphi^{-1}(\mathfrak{q}') \in \operatorname{Spec} A$ and $\overline{\varphi} : A/\mathfrak{q} \to A'/\mathfrak{q}'$ is the natural ring homomorphism induced by φ, the map $\overline{\varphi}^* : (\operatorname{Spec} A'/\mathfrak{q}') \longrightarrow \operatorname{Spec}(A/\mathfrak{q})$ associated to $\overline{\varphi}$ is surjective.

Prove that (i) $\Rightarrow$ (ii) $\Longleftrightarrow$ (iii). See also the part (b) below.

(**Hint :** Note that (ii) $\Longleftrightarrow \varphi^*(\mathrm{V}(\mathfrak{q}')) = \mathrm{V}\left(\varphi^{-1}(\mathfrak{q}')\right) \Longleftrightarrow$ (iii), since the residue-class map $\pi_{\mathfrak{a}}$: $A \to A/\mathfrak{q}$ induces induces a homeomorphism $\pi_{\mathfrak{q}}^* : \operatorname{Spec}(A/\mathfrak{q}) \xrightarrow{\sim} \mathrm{V}(\mathfrak{q}) \hookrightarrow \operatorname{Spec} A$. Further, since $\overline{\varphi^*(\mathrm{V}(\mathfrak{q}'))} = \mathrm{V}\left(\varphi^{-1}(\mathfrak{q}')\right)$ by the Exercise 8.22 (a.2), the implication (iii) $\Rightarrow$ (i) is immediate.)

(b) Suppose that $\operatorname{Spec} A'$ is a noetherian space. Prove that $\varphi^* : \operatorname{Spec} A' \to \operatorname{Spec} A$ is a closed map if and only if φ has the Going-up property.

9.34 Let $\varphi : A \to A'$ be a ring homomorphism and let $\varphi^* : \operatorname{Spec} A' \longrightarrow \operatorname{Spec} A$ be the map associated to φ on spectra.

(a) Consider the following three statements :

(i) $\varphi^* : \operatorname{Spec} A' \to \operatorname{Spec} A$ is an open map, i. e. it maps open sets to open sets.

(ii) The map φ has the Going-down property, i. e. for prime ideals $\mathfrak{q}' \in \operatorname{Spec} A'$ and $\mathfrak{p} \in \operatorname{Spec} A$ with $\mathfrak{p} \subseteq \varphi^{-1}(\mathfrak{q}')$, there exists a prime $\mathfrak{p}' \in \operatorname{Spec} A'$ with $\varphi^{-1}(\mathfrak{p}') = \mathfrak{p}$ and $\mathfrak{p}' \subseteq \mathfrak{q}'$.

(iii) For a prime ideal $\mathfrak{q}' \in \operatorname{Spec} A'$ with $\mathfrak{q} := \varphi^{-1}(\mathfrak{q}') \in \operatorname{Spec} A$ and the natural ring homomorphism $\varphi_{\mathfrak{q}} : A_{\mathfrak{q}} \to A'_{\mathfrak{q}'}$ induced by φ, the map $\varphi_{\mathfrak{q}}^* : \operatorname{Spec}(A'_{\mathfrak{q}'}) \to \operatorname{Spec}(A_{\mathfrak{q}})$ is surjective.
Prove that (i) $\Rightarrow$ (ii) $\Longleftrightarrow$ (iii). See also the part (b) below.

(**Hint :** Identify (via $\operatorname{Spec}(\varphi_{S_{\mathfrak{q}}}^*) : \operatorname{Spec}\left(S_{\mathfrak{q}}^{-1}A\right) \to \operatorname{Spec} A$, where $S_{\mathfrak{q}} := A \setminus \mathfrak{q}$ and $\varphi_{S_{\mathfrak{q}}} : A \to S_{\mathfrak{q}}^{-1}A$ is the natural map) $\operatorname{Spec}(A_{\mathfrak{q}})$ with the subspace $\{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \subseteq \mathfrak{q}\}$ of $\operatorname{Spec} A$; similarly, identify $\operatorname{Spec}(A'_{\mathfrak{q}'})$ with the subspace $\{\mathfrak{p}' \in \operatorname{Spec} A' \mid \mathfrak{p}' \subseteq \mathfrak{q}'\}$ of $\operatorname{Spec} A'$. Then $\varphi^*(\operatorname{Spec}(A'_{\mathfrak{q}'})) \subseteq \operatorname{Spec}(A_{\mathfrak{q}})$. (ii$'$) $\varphi^*(\operatorname{Spec}(A'_{\mathfrak{q}'})) = \operatorname{Spec}(A_{\mathfrak{q}})$ if and only if (ii) holds. Further, since φ^* induces $\varphi_{\mathfrak{q}}^*$ where $\varphi_{\mathfrak{q}} : A_{\mathfrak{q}} \to A'_{\mathfrak{q}'}$ is the ring homomorphism induced by φ, the equality $\varphi^*(\operatorname{Spec}(A'_{\mathfrak{q}'})) = \operatorname{Spec}(A_{\mathfrak{q}})$ holds if and only if (iii) holds. This proves the equivalence of (ii) and (iii). Further, since (i) implies the inclusion $\operatorname{Spec} A_{\mathfrak{q}} \subseteq \varphi^*(\operatorname{Spec}(A'_{\mathfrak{q}'}))$ and hence the equality $\varphi^*(\operatorname{Spec}(A'_{\mathfrak{q}'})) = \operatorname{Spec}(A_{\mathfrak{q}})$. This proves that the statement (i) implies (ii) and hence also (iii).)

(b) Suppose that A is a noetherian ring and φ is finite type over A, i. e. A' is an A-algebra of finite type (and hence A' is also noetherian by HBT). Prove that $\varphi^* : \operatorname{Spec} A' \to \operatorname{Spec} A$ is an open map if and only if φ has the Going-down property. (**Remark :** Proof need the concept of *constructible sets* in a topological space.)

9.35 Let $\varphi : A \to A'$ be a *flat* homomorphism of rings. Then φ has the going-down property. Moreover, if A is noetherian and the A-algebra A' is of finite type A, then $\varphi^* : \operatorname{Spec} A' \to \operatorname{Spec} A$ is an open map. (**Hint :** Use Exercise 9.33 (a) to prove the equivalent statement (iii). To prove this, let $\mathfrak{q}' \in \operatorname{Spec} A'$ and $\mathfrak{q} := \varphi^{-1}(\mathfrak{q}') \in \operatorname{Spec} A$. Note that $\varphi_{\mathfrak{q}} : A_{\mathfrak{q}} \to A'_{\mathfrak{q}}$ is flat (base change) and $A'_{\mathfrak{q}'}$ is a localization of $A'_{\mathfrak{q}}$, hence flat over $A'_{\mathfrak{q}}$. Therefore, the composite ring homomorphism $A_{\mathfrak{q}} \xrightarrow{\varphi_{\mathfrak{q}}} A'_{\mathfrak{q}} \to A'_{\mathfrak{q}'}$ is flat and a local homomorphism. Now, use Exercise 8.31 to conclude that $\varphi^*_{\mathfrak{q}} : \operatorname{Spec}(A'_{\mathfrak{q}'}) \to \operatorname{Spec}(A_{\mathfrak{q}})$ is surjective. The later statement is immediate from Exercise 9.33 (b).)

9.36 (Rings of invariants of finite groups — Emmy Noether (1882-1935)) Let B be an A-algebra over a ring A and let $G \subseteq \operatorname{Aut}_{A\text{-alg}} B$ be a finite group of A-algebra automorphisms of B. The subset $B^G := \{x \in B \mid \sigma(x) = x \text{ for all } \sigma \in G\} \subseteq B$ is a subring of B and is called the ring of invariants of G, it is even an A-subalgebra of B.

(a) Every $x \in B$ is integral over B^G, i. e. B is integral over B^G and so $\dim B^G = \dim B$.

(b) If B is an A-algebra of finite type, then there exists an A-subalgebra A' $(\subseteq B^G)$ of finite type over A and that B is integral over A'.

(c) If A is noetherian and if B is an A-algebra of finite type, then B^G is also an A-algebra of finite type. In particular, B^G is noetherian.

(d) Let $S \subseteq B$ be a multiplicatively closed subset in B such that $\sigma(S) \subseteq S$ for every $\sigma \in G$ and let $S^G = S \cap B^G$. Then the action of G on B extends to an action on $S^{-1}B$ and that $(S^G)^{-1}B^G \xrightarrow{\sim} (S^{-1}A)^G$.

(For the proof indicated below see the article :
[Emmy Noether , Der Endlichkeitsatz der Invarianten endlicher linearer Gruppen der Charakteristik p, Nachr. Ges. Wiss. Gottingen (1926), 28-35])

(— **Hint : (a) :** Let G act on the polynomial ring $B[X]$ coefficient-wise. Then for every $x \in B$, the polynomial $f_x := \prod_{\sigma \in G}(X - \sigma(x)) \in B[X]$ is G-invariant and hence its coefficients belong to B^G which provides an integral equation for x.

(b) : Assume that $B = A[x_1, \ldots, x_n]$ and let A' be the A-subalgebra of B^G generated by all coefficients of the polynomials $f_{x_1}, \ldots, f_{x_n}$. Then A' is of finite type over A and B is integral over A' (since $B = A[x_1, \ldots, x_n] = A'[x_1, \ldots, x_n]$ and each x_i is integral over A and hence over A' with integral equation f_{x_i}, $i = 1, \ldots, n$).

(c) : Note that by (b) there exists a finite type A-subalgebra $A' \subseteq B^G$ such that B is integral over A'. Further, since B is finite type over A, it is also finite type over A' and hence (by Corollary on Page 1) B is a finite A'-module. Now, since A' is noetherian by HBT, B is a noetherian A'-module and hence the A'-submodule B^G of B is also finite A'-module. Therefore B^G is an A-algebra of finite type. For, if $A' = A[y_1, \ldots y_m]$ and $B^G = A'z_1 + \cdots + A'z_r$, then $B^G = A[y_1, \ldots, y_m, z_1, \ldots, z_r]$.)

9.37 Let A be a ring.

(a) Let B an A-algebra, G be a group acting on the A-algebra B (by A-algebra automorphisms) and let $\overline{A}$ be the integral closure of A in B. Then G acts canonically on the

A-algebra $\overline{A}$. (**Hint :** Let $x \in \overline{A}$ with integral equation $x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ with $a_1, \ldots, a_n \in A$ and let $\sigma \in G$. Applying σ, we get $0 = \sigma(0) = \sigma(x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n) = \sigma(x)^n + a_1\sigma(x)^{n-1} + \cdots + a_{n-1}\sigma(x) + a_n$ is an integral equation for $\sigma(x)$ over A and hence $\sigma(x) \in \overline{A}$. Therefore $\sigma(\overline{A}) \subseteq \overline{A}$. Similarly, $\sigma^{-1}(\overline{A}) \subseteq \overline{A}$ and so $A \subseteq \sigma(\overline{A})$. Therefore $\sigma(\overline{A}) = A$.)

(b) Suppose that A is a *normal* domain with quotient field K, $L\,|\,K$ be a *Galois extension* with Galois group $G = \mathrm{Aut}_{K\text{-alg}}\, L$ and let $\overline{A}_L$ be the integral closure of A in L. Prove that $A = \overline{A}_L^{\,G}$. (**Hint :** Note that be definition of Galois extension $K = L^G$. Futher, G acts canonically on $\overline{A}_L$ by part (a) and hence $\overline{A}_L^{\,G}$ is an A-algebra and $A \subseteq \overline{A}_L^{\,G}$. Conversely, $\overline{A}_L^{\,G} \subseteq L^G = K$, since $L\,|\,K$ is a Galois extension and hence $\overline{A}_L^{\,G} \subseteq \overline{A}_L \cap K = A$, since A is normal.)

9.38 Let $A \subseteq B$ be integral domains with quotient fields K and L, respectively. Suppose that A is integrally closed and $L\,|\,K$ is a finite Galois extension with Galois group $G := \mathrm{Gal}(L\,|\,K)$. Prove that : **(a)** $\sigma(B) \subseteq B$ for every $\sigma \in G$. **(b)** $B^G = A$.

9.39 Let B be a ring, $G \subseteq \mathrm{Aut}_{\mathrm{Rings}}\, B$ be a finite group of ring automorphisms of B and let $\mathfrak{p} \in \mathrm{Spec}\, B^G$. Further, let $\mathcal{P}(\mathfrak{p}) := \{\mathfrak{P} \in \mathrm{Spec}\, B \mid \mathfrak{P} \cap B^G = \mathfrak{p}\}$. Then :

(a) G acts transitively on $\mathcal{P}(\mathfrak{p})$. **(b)** $\mathcal{P}(\mathfrak{p})$ is non-empty and finite.

(**Hint : (a) :** For $\mathfrak{P} \in \mathcal{P}(\mathfrak{p})$ and $\sigma \in G$, $\sigma(\mathfrak{P}) \in \mathrm{Spec}\, B$, since σ is a ring automorphism of B. Moreover, $\sigma(\mathfrak{P}) \cap B^G = \mathfrak{P} \cap B^G = \mathfrak{p}$, since σ leaves B^G fixed. Therefore $\sigma(\mathfrak{P}) \in \mathcal{P}(\mathfrak{p})$.
For transitivity of the action of G on $\mathcal{P}(\mathfrak{p})$, let $\mathfrak{P}$, $\mathfrak{P}' \in \mathcal{P}(\mathfrak{p})$. To find $\sigma \in G$ with $\sigma(\mathfrak{P}) = \mathfrak{P}'$. For $x \in \mathfrak{P}'$, put $y := \prod_{\sigma \in G} \sigma(x)$. Then $y \in B^G \cap \mathfrak{P}' = \mathfrak{p} \subseteq \mathfrak{P}$ and so there exists $\sigma \in G$ with $\sigma(x) \in \mathfrak{P}$, i.e. $x \in \sigma^{-1}(\mathfrak{P})$. This proves that $\mathfrak{P}' \subseteq \bigcup_{\sigma \in G} \sigma(\mathfrak{P})$. Therefore by Exercise 1.9 (b) $\mathfrak{P}' \subseteq \sigma(\mathfrak{P})$ for some $\sigma \in G$. But, since B is integral over B^G (see Exercise 9.35 (b)) with $A = \mathbb{Z}$), by Theorem (2) Incomparibility on Page 1, $\mathfrak{P}' = \sigma(\mathfrak{P})$.

(b) : Since B is integral over B^G, $\mathcal{P}(\mathfrak{p}) \neq \emptyset$. Now, since G acts transitively on $\mathcal{P}(\mathfrak{p})$ by (a) and G is finite, it follows that $\mathcal{P}(\mathfrak{p})$ is finite.)

9.40 Let $f = f(X) \in \mathbb{Z}[X]$ be a monic polynomial of positive degree and let $B := \mathbb{Z}[X]/\langle f \rangle$. For a prime number $p \in \mathbb{P}$, show that the number of prime ideals in B lying over the prime ideal $p\mathbb{Z}$ is equal to the number of distinct monic irreducible factors of $\overline{f}$ in $(\mathbb{Z}/\mathbb{Z}p)[X]$. (**Hint :** Note that the splitting field of $\overline{f}$ over $\mathbb{Z}/\mathbb{Z}p$ is a finite Galois extension of $\mathbb{Z}/\mathbb{Z}p$. With this use Exercise 37 and Exercise 38 to prove the assertion.)

9.41 Let B be an A-algebra over a ring A with the structure homomorphism $\varphi : A \to B$ and let $\mathfrak{P} \in \mathrm{Spec}\, B$. We say that $\mathfrak{P}$ is i s o l a t e d o v e r $\mathfrak{P} \cap A =: \mathfrak{p} \in \mathrm{Spec}\, A$ if $\mathfrak{P}$ is maximal and minimal (with respect to the natural inclusion $\subseteq$) in the fibre $(\varphi^*)^{-1}(\mathfrak{p}) = \{\mathfrak{P}' \in \mathrm{Spec}\, B \mid \mathfrak{P}' \cap A = \mathfrak{p}\}$ of the map $\varphi^* : \mathrm{Spec}\, B \to \mathrm{Spec}\, A$ associated to φ on spectra over $\mathfrak{p}$, i.e. $\{\mathfrak{P}\}$ is open in the fibre $(\varphi^*)^{-1}(\mathfrak{p})$.

(a) Let $A \subseteq B$ be an integral extension of rings. Then every $\mathfrak{P} \in \mathrm{Spec}\, B$ isolated over $\mathfrak{p} := \mathfrak{P} \cap A$. (**Hint :** Remember the Incomparability (2) in Theorem on Page 1.)

(b) Let $A[X]$ be the polynomial ring in the indeterminate X over an integral domain A. Then every prime ideal $\mathfrak{P} \in \mathrm{Spec}\, A[X]$ cannot be isolated over $\mathfrak{p} = \mathfrak{P} \cap A$. (**Hint :** Let $\iota : A \to A[X]$ be the natural inclusion. Then both $\mathfrak{p}A[X]$, $\langle \mathfrak{p}, X \rangle \in \mathrm{Spec}\, A[X]$ with $\mathfrak{p}A[X] \subsetneq \langle \mathfrak{p}, X \rangle$ and belong to $(\iota^*)^{-1}(\mathfrak{p})$.)

(c) Let B be an integral domain, $x \in B$ and $A \subseteq B$ a subring of B such that x is transcendental (not algebraic) over A and that $A[x] \subseteq B$ is integral. Then every $\mathfrak{P} \in \mathrm{Spec}\, B$ is not isolated over $\mathfrak{P}\cap A =: \mathfrak{p}\in \operatorname{Spec} A$. (**Hint :** Consider the two cases :

Case 1: *A is a normal domain* : Then by assumptions $A[x]=A[X]$ is the polynomial ring and hence also a normal domain, see Exercise 9.29 (a). Let $\mathfrak{P}\in\operatorname{Spec} B$ and $\mathfrak{p}_1 = \mathfrak{P}\cap A[X]\in\operatorname{Spec} A[X]$. Then $\mathfrak{p}_1\cap = \mathfrak{P}\cap A=\mathfrak{p}$ and $\mathfrak{P}_1$ cannot be isolated over $\mathfrak{p}$ by part (b). Now, applying Going-up or Going-down to the integral extension $A[X]\subseteq B$, conclude that $\mathfrak{P}$ is not isolated over $\mathfrak{p}$.

Case 2: *A is not integrally closed* : In this case, let A' and B' be integral closures of A and B. Then clearly x is also transcendental over A' and B' is integral over $A'[x]=A[X]$ is the polynomial ring. Now, since B' is integral over B, we can choose $\mathfrak{P}'\in\operatorname{Spec} B'$ with $\mathfrak{P}=\mathfrak{P}'\cap B$ and $\mathfrak{P}'$ is not isolated over $\mathfrak{P}'\cap A'$ by Case 1. From this conclude that $\mathfrak{P}\in\operatorname{Spec} B$ is not isolated over $\mathfrak{P}\cap A=\mathfrak{p}$.)

9.42 Let A be a *normal* domain with quotient field K, $L\,|\,K$ a finite field extension and let $\overline{A}_L$ be the integral closure of A in L. Show that if $\mathfrak{p}\in\operatorname{Spec} A$ is any prime ideal, then the set $\mathcal{P}(\mathfrak{p}) := \{\mathfrak{P}\in\operatorname{Spec}\overline{A} \mid \mathfrak{P}\cap A=\mathfrak{p}\}$ is finite. in other words the map $\varphi^*:\operatorname{Spec} A_L\to\operatorname{Spec} A$ associated to φ on spectra has finite fibers. (**Hint :** Put $\overline{A}:=\overline{A}_L$. Consider the three cases :

Case 1 : $L\,|\,K$ is separable : There exists a finite Galois extension $L'\,|\,K$ (with Galois group $\operatorname{Gal}(L'|K)$) such that $L\subseteq L'$. Let A' be the integral closure of A in L'. Then $A'^G=A$ by Exercise 9.36 (b) and hence by Exercise 9.38 (b) there are only finitely many prime ideals $\mathfrak{P}'\in\operatorname{Spec} A'$ lie over $\mathfrak{p}$. Since A' is integral over $\overline{A}$, for each $\mathfrak{P}\in\mathcal{P}(\mathfrak{p})$ there is some $\mathfrak{P}'$ lies over $\mathfrak{P}$ (by Theorem (3) Lying over, on Page 1). This proves that the set $\mathcal{P}(\mathfrak{p})$ is finite.

Case 2 : $L\,|\,K$ is purely separable :
In this case $\operatorname{Char} K=p>0$ and $\mathcal{P}(\mathfrak{p})=\{\mathfrak{P}:=\sqrt{\mathfrak{p}\overline{A}}\}$ is singleton, where $\mathfrak{P} :\overset{(*)}{=} \{x\in\overline{A}\mid x^{p^n}\in\mathfrak{p}$ for some $n\in\mathbb{N}\}$. Let $\mathfrak{P}\in\mathcal{P}(\mathfrak{p})$. To prove the equality (*), let $x\in\mathfrak{P}$. First note that $x^q\in K$, where $q:=p^n$ for some $n\in\mathbb{N}^+$ (since $L\,|\,K$ is purely inseparable). But, since $x^q\in\mathfrak{P}\subsetneq\overline{A}$, x^q is integral over A and A is normal, $x^q\in\mathfrak{P}\cap A=\mathfrak{p}$. Conversely, for $x\in\overline{A}$ with $x^r\in\mathfrak{p}$ for some $r\in\mathbb{N}^+$, then $x^r\in\mathfrak{P}$ and hence $x\in\mathfrak{P}$, since $\mathfrak{P}$ is a prime ideal. This proves the equality (*).

Case 3 : General case $L\,|\,K$ be arbitrary finite field extension : There is an intermediate field K' with $K\subseteq K'\subseteq L$ such that $K'\,|\,K$ is separable and $L\,|\,K'$ is pure inseparable (see for example, Proposition 6.6 on Page 250 of the Book[1]). Let A' be the integral closure of A in K'. Then by the Case 1, there are only finitely many prime ideals $\mathfrak{P}'\in\operatorname{Spec} A'$ lying over $\mathfrak{p}$. Moreover A' is normal and $\overline{A}$ is also the integral closure of A' in L. For, first $\overline{A}$ is integral over A, so over A'. Second, if $x\in L$ is integral A', then x is integral over A and hence $x\in\overline{A}$ as desired. Therefore, by the Case 2 only one prime ideal $\mathfrak{P}\in\operatorname{Spec}\overline{A}$ lies over each $\mathfrak{P}'$ over A. This proves the assertion.)

9.43 Let B be an A-algebra of finite type over a ring A with the structure homomorphism $\varphi:A\to B$, $\mathfrak{q}\in\operatorname{Spec} B$ and $\mathfrak{p}:=\varphi^*(\mathfrak{q})=\varphi^{-1}(\mathfrak{q})$. Show that the following statements are equivalent :

(i) $\mathfrak{q}$ is isolated in the fibre $(\varphi^*)^{-1}(\mathfrak{p})$ of $\varphi^*:\operatorname{Spec} B\to\operatorname{Spec} A$ over $\mathfrak{p}$.
(ii) $\kappa(\mathfrak{q}) := B_{\mathfrak{q}}/\mathfrak{q}B_{\mathfrak{q}}$ is a finite $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}=\kappa(\mathfrak{p})$-algebra.

(**Hint :** Use the Exercise 8.29 and the following commutative diagrams :

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d] & B \arrow[d] \\ \kappa(\mathfrak{p}) \arrow[r] & \kappa(\mathfrak{q}) \end{tikzcd} \qquad \begin{tikzcd} \operatorname{Spec} B \arrow[r, "\varphi^*"] & \operatorname{Spec} A \\ \operatorname{Spec}\kappa(\mathfrak{q}) \arrow[r] \arrow[u] & \operatorname{Spec}\kappa(\mathfrak{p}) \arrow[u] \end{tikzcd}$$.)

— Remark : We say that B is q u a s i - f i n i t e over A at $\mathfrak{q}\in\operatorname{Spec} B$ if any one of the above equivalent conditions hold. with this definition we state the following very important theorem :

Zariski's Main Theorem (ZMT)[2] *Let B be an A-algebra of finite type over a ring A with the*

[1] Lang, S., Algebra, Graduate Texts in Mathematics **211**, Springer-Verlag, 2002.

[2] Proved by Oscar Zariski (1899-1986) in 1943. In algebraic geometry it is a statement about the structure of birational morphisms which states roughly that there is only one branch at any normal point of a variety. It is the

structure homomorphism $\varphi : A \to B$ and $\overline{A}$ be the integral closure of $\varphi(A)$ in B and let $\mathfrak{q} \in \operatorname{Spec} B$. If B is quasi-finite over A at $\mathfrak{q}$, then there exists $f \in \overline{A}$, $f \notin \mathfrak{q}$ such that $\overline{A}_f = B_f$.

For a proof see the following article by Peskine :
[Peskine, C. : *Le théorème principal de Zariski*, Bull. Sc. Maths. **90** 1966, pp 119-127.]

9.44 Let K be a field.

(a) Let $A := K[X,Y]$, $A' := K[X,Y,Z]/\langle Z^2 - XZ - 1\rangle$ and $\mathfrak{p} := \langle X\rangle \in \operatorname{Spec} A$. Find a prime ideal $\mathfrak{p}' \in \operatorname{Spec} A'$ with $\mathfrak{p}A' \subseteq \mathfrak{p}'$ such that $\mathfrak{p} = A \cap \mathfrak{p}'$.

(b) Test the going-down theorem in the following cases :

(1) $A := K[Y,Z]$, $A' := K[X,Y,Z]/\langle X,Y\rangle \cap \langle X+Z\rangle\langle Z^2 - XY\rangle$, $\mathfrak{p} := \langle 0\rangle \subseteq \mathfrak{q} := A \cap \mathfrak{q}'$ in $\operatorname{Spec} A$ and $\mathfrak{q}' := \langle X,Y\rangle \in \operatorname{Spec} A'$.

(2) $A := \mathbb{Q}[X,Y]$, $A' := \mathbb{Q}[X,Y,Z]\langle Z^2 - XY\rangle$, $\mathfrak{p} := \langle Y^2 - X^3\rangle \subseteq \mathfrak{q} := \langle X,Y\rangle$ in $\operatorname{Spec} A$ and $\mathfrak{q}' := \langle X,Y,Z\rangle \in \operatorname{Spec} A'$.

---

special case of Zariski's connectedness theorem when the two varieties are birational. Zariski's main theorem can be stated in several ways which at first sight seem to be quite different, but are in fact deeply related.

S9 Supplements*

S9.1 In this supplement, we prove the Lüroth's Theorem which was used in Exercise 9.18.

Recall that a field extension $L|K$ is said to be purely transcendental of it is generated over K by a set of algebraically independent elements over K. In this supplement we study purely transcendental field extensions of transcendence degree one. Such extension is of the form $K(t)\,|\,K$, where t transcendental over a field K.

Let $y\in K(t)$, $y\neq 0$. Then we can write $y=p(t)/q(t)$ with $0\neq p(t), 0\neq q(t)\in K[t]$ and $\gcd(p(t),q(t))=1$, and define the degree of y by $\deg y = \text{Max}\,(\deg p(t), \deg q(t))$. It is clear that this definition is independent of the representation $p(t)/q(t)$ of y as above and that $\deg y=0$ if and only if $y\in K^\times$.

First we first prove the following lemma:

S9.1.1 Lemma. Let $y\in K(t)$, $y\notin K$. Then y is transcendental over K and the field extension $K(t)\,|\,K(y)$ is algebraic and $[K(t):K(y)]=\deg y$.

Proof. Let $y=P(t)/q(t)$ with $p(t),\ q(t)\in K[t]\smallsetminus\{0\}$, $\gcd(p(t),q(t)0=1$, and $n=\deg y=\text{Max}\,(\deg p(t),\deg q(t))$. Write $p(t)=p_0+p_1t+\cdots+p_nt^n$ and $q(t)=q_0+q_1t+\cdots+q_nt^n$ with $p_0,\ldots,p_n\,;q_0,\ldots,q_n\in K$ and $p_n\neq 0$ or $q_n\neq 0$. Let X be indeterminate and $f(X):=p(X)-y\cdot q(X)=(p_0-yq_0)+(p_1-yq_1)X+\cdots+(p_n-yq_n)X^n\in K[y][X]$ and $f(t)=0$. Therefore, since $y\notin K$, we have $n\geq 1$ and $p_n-yq_n\neq 0$, and hence $f(X)\neq 0$ and that $\deg f(X)=n$. Therefore t is algebraic over $K[y]$ and so y is transcendental over K. This shows that $K[y,X]$ is the polynomial ring in two variables y and X over K and in this ring $f(X)=p(X)-yq(X)$ is a polynomial of y-degree 1. Further, $\gcd(p(X),q(X))=1$ in $K[X]$. Therefore $f(X)$ is irreducible in $K[y,X]=K[y][X]$. Now, since $\deg f(X)>0$, $f(X)$ is irreducible in $K(y)[X]$ by the following Theorem [3] and hence $f(X)=\mu_{t\,,K(y)}$ is the minimal polynomial of t over $K(y)$. Therefore $[K(t):K(y)]=\deg f(X)=n=\deg y$. •

S9.1.2 Corollary. $K(t)=K(y)$ *if and only if* $\deg y=1$.

S9.1.3 Corollary. *The group of K-automorphisms of the field $K(t)$ is isomorphic to the projective linear group* $\mathrm{PGL}_2(K)$.

Proof. Note that for $\varphi=f/g\in K(X)\smallsetminus K$ with $\gcd(f,g)=1$, the map $K(X)\to K(X)$, $F/G\mapsto F(\varphi)/G(\varphi)$ is a K-algebra homomorphism. Moreover, it is a K-algebra automorphism if and only if $\deg\varphi=\text{Max}\,(\deg f,\deg g)=1$. This shows that every $\sigma\in\mathrm{Aut}_{K\text{-alg}}K(X)$ is the substitution homomorphism with $\sigma(X)=(aX+b)/(cX+d)$ with $a,b,c,d\in K$, $cX+d\neq 0$, at least one of a and c is non-zero and $\gcd(aX+b,cX+d)=1$, or, equivalently, $ad-bc\neq 0$. The map (it is easy to verify that it is well defined)

$$\mathrm{Aut}_{K\text{-alg}}K(X)\to\mathrm{PGL}_2(K):=\mathrm{GL}_2(K)/K^\times\,,\quad \sigma\mapsto \text{the image of } \begin{pmatrix} a & b\\ c & d\end{pmatrix} \text{ in } \mathrm{PGL}_2(K)$$

is a canonical isomorphism of groups, where σ is defined by $\sigma(X)=(aX+b)/(cX+d)$.

(**Remark:** The group $\mathrm{PGL}_n(K)$ is the well-known group of projective collineations of the projective space $\mathrm{P}_K(K^n)$ over k. It is called the Projective linear group over K and often occurs in Projective Geometry, Complex Analysis and Riemann Surfaces.) •

S9.1.4 Lüroth's Theorem. *Let $K(t)\,|\,K$ be a purely transcendental field extension over K of transcendence degree one. Then every intermediate subfield $K\subsetneq L\subseteq K(t)$ is purely transcendental field extension over K of transcendence degree one.*

Proof. We have to show that $L=K(y)$ for some transcendental element $y\in K(t)$. Note that $K(t)\,|\,L$ is algebraic by Lemma S9.1.1. Let $g:=\mu_{t\,,L}=X^m+g_1X^{m-1}+\cdots+g_m\in L[X]$ be the minimal monic

[3] **Theorem.** *Let A be a UFD with quotient field K and let $f(X)\in A[X]$ be an irreducible polynomial of* $\deg f(X)>0$. *Then $f(X)$ is irreducible in $K[X]$.*

polynomial of t over L. Then $[K(t):L]=m$ and since t is not algebraic over K, $g_j \notin K$ for some j with $1\leq j\leq m$.

S 9.1.4.1 We claim that $L=K(g_j)$ for every j with $1\leq j\leq m$ and $g_j\notin K$.

Put $y:=g_j$ Then y is transcendental over K and by Lemma S9.1.1 $[K(t):K(y)]=\deg y:=n$. Since $K\subseteq K(y)\subseteq L$, to prove $L=K(y)$, it is enough to prove that $m=n$. Write $g_i=a_i(t)/a_0(t)$ with $a_i(t)\in K[t]$, $i=0,\ldots,m$, $a_0(t)\neq 0$ and $\gcd(a_0(t),a_1(t),\ldots,a_m(t))=1$, and let

$$G(t,X):=a_0(t)g(X)=a_0X^m+a_1(t)X^{m-1}+\cdots+a_m(t)\in K[t][X].$$

Then $G(t,X)$ is a primitive polynomial (over the UFD) $K[t]$. Write $y=p(t)/q(t)$ with $0\neq p(t)$, $0\neq q(t)\in K[t]$ and $\gcd(p(t),q(t))=1$, and let

$$F(t,X)=q(t)p(X)-p(t)q(X)\in K[t,X].$$

Then, since $(F(t,X)/q(t))(t)=0$, $g(X)=\mu_{t,L}(X)$ divides the polynomial $F(t,X)/q(t)$ in $L[X]$ and hence $g(X)$ divides $F(t,X)$ in $K(t)[X]$. Now, since $a_0(t)g(X)=G(t,X)$ is primitive over $K[t]$, $G(t,X)$ divides $F(t,X)$ in $K(t)[X]$ by *Gauss Lemma* [4] and hence

S 9.1.4.a $F(t,X)=G(t,X)H$ with $H\in K[t][X]$ and $\deg_t F(t,X)\geq \deg_t G(t,X)$.

On the other hand, since $a_j(t)/a_0(t)=g_j=y=p(t)/q(t)$ and $\gcd(p(t),q(t))=1$, we have $a_j(t)=b(t)p(t)$ and $a_0(t)=b(t)q(t)$ for some $b(t)\in K[t]$. This gives

S 9.1.4.b $\deg_t G(t,X)\geq \operatorname{Max}\big(\deg a_j(t),\deg a_0(t)\big)\geq \operatorname{Max}\,(\deg p(t),\deg q(t))\geq \deg_t F(t,X)$.

Combining S 9.1.4.b and S 9.1.4.a, we get

$$\deg_t G(t,X)=\deg_t F(t,X)=\operatorname{Max}\,(\deg p(t),\deg q(t))=\deg y=n.$$

Therefore $\deg_t H=0$, i.e. $H\in K[X]$ and so $F(t,X)=G(t,X)$ is primitive over $K[t]$ and so $G(t,X)=F(t,X)$. Now, since $F(X,t)=-F(t,X)$, we get $\deg_X F(t,X)=n$ and that $F(t,X)$ is primitive over $K[X]$. This implies that $\deg_X H=0$, and so we get $n=\deg_X F(t,X)=\deg_X G(t,X)=m$. This completes the proof of S9.1.4. •

---

[4] **Gauss Lemma.** *Let A be a UFD with quotient field K and let $f,g\in A[X]$ be non-zero polynomials. Then*:
(1) *If f and g are primitive, then so is fg.*
(2) $\operatorname{Cont}(fg)=\operatorname{Cont}(f)\operatorname{Cont}(g)$ (up to multiplication by a unit)
(3) *If f is primitive and if f divides g in $K[X]$, then f divides g in $A[X]$.*
(4) *If f is primitive, then the following four conditions are equivalent*:
 (i) *f is irreducible in $K[X]$*; (ii) *f is irreducible in $A[X]$*; (iii) *f is prime in $K[X]$*; (iv) *f is prime in $A[X]$*.