3.2.7. Let $A \subset B$ be integral and $B \smallsetminus A$ be multiplicatively closed in B. Prove that A is integrally closed in B.

3.2.8. Let $A \subset B$ be integral domains and $C = C(A, B)$. Let $f, g \in B[x]$ be monic polynomials such that $f \cdot g \in C[x]$. Prove that $f, g \in C[x]$.

3.2.9. Let $A = \bigoplus_{i=0}^{\infty} A_i$ be a Noetherian graded ring, $d \geq 1$ an integer, and let $A^{(d)} = \bigoplus_{i=0}^{\infty} A_{id}$. Prove that A is integral over $A^{(d)}$.

3.2.10. Prove that a normal local ring is an integral domain.

3.3 Dimension

In this section we shall use chains of prime ideals to define the dimension of a ring. This is one possibility to define the dimension. It is called the *Krull dimension*. We shall show that the dimension of the polynomial ring $K[x_1, \ldots, x_n]$ in the variables $x_1, \ldots, x_n$ over a field K equals n, given by the chain $\langle 0 \rangle \subset \langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \cdots \subset \langle x_1, \ldots, x_n \rangle$.

Definition 3.3.1. Let A be a ring

(1) Let $\mathcal{C}(A)$ denote the set of all *chains of prime ideals* in A, that is,

$$\mathcal{C}(A) := \left\{ \wp = (P_0 \subsetneqq \cdots \subsetneqq P_m \subsetneqq A) \;\middle|\; P_i \text{ prime ideal} \right\}.$$

(2) If $\wp = (P_0 \subsetneqq \cdots \subsetneqq P_m \subsetneqq A) \in \mathcal{C}(A)$ then *length*$(\wp) := m$.
(3) The *dimension* of A is defined as $\dim(A) = \sup\{\text{length}(\wp) \mid \wp \in \mathcal{C}(A)\}$.
(4) For $P \subset A$ a prime ideal, let

$$\mathcal{C}(A, P) = \left\{ \wp = (P_0 \subsetneqq \cdots \subsetneqq P_m) \in \mathcal{C}(A) \;\middle|\; P_m = P \right\}$$

denote the set of prime ideal chains ending in P. We define the *height* of P as $\text{ht}(P) = \sup\{\text{length}(\wp) \mid \wp \in \mathcal{C}(A, P)\}$.
(5) For an arbitrary ideal $I \subset A$, $\text{ht}(I) = \inf\{\text{ht}(P) \mid P \supset I \text{ prime}\}$ is called the *height* of I and $\dim(I) := \dim(A/I)$ is called the *dimension* of I.

Example 3.3.2.

(1) We shall see in Section 3.5 that in the polynomial ring $K[x_1, \ldots, x_n]$ over a field K all maximal chains of prime ideals have the same length n. Here a chain of prime ideals is called *maximal* if it cannot be refined.
(2) Let $A = K[x]_{(x)}[y]$ then $(0) \subset (xy - 1)$ and $(0) \subset (x) \subset (x, y)$ are two maximal chains of different length.
(3) Let $A = K[x, y, z]/\langle xz, yz \rangle$, then $\dim(A) = 2$. Let $P = \langle x, y, z - 1 \rangle$, then $\dim(A_P) = 1$ (cf. Figure 3.5 on page 227).

Corollary 3.3.3. *Let $A \subset B$ be an integral extension, then $Q \mapsto Q \cap A$ defines a surjection $\mathcal{C}(B) \to \mathcal{C}(A)$ preserving the length of chains, in particular,* $\dim(A) = \dim(B)$.

Proof. Using Proposition 3.1.10 we see that the map is surjective. We have to prove that the length is also preserved. Let $Q \subsetneq Q'$ be prime ideals in B, assume $Q \cap A = Q' \cap A = P$.

Now $A_P \subset B_P$ is an integral extension, and A_P is local with maximal ideal PA_P. Moreover, $QB_P \subset Q'B_P$ are prime ideals in B_P, with the property $QB_P \cap A_P = Q'B_P \cap A_P = PA_P$. Because of Lemma 3.1.9 (3), QB_P and $Q'B_P$ are maximal and, therefore, $QB_P = Q'B_P$. This implies $Q = Q'$. $\square$

Definition 3.3.4. Let A be a ring and $I \subset A$ an ideal. A prime ideal P with $I \subset P$ is called *minimal associated prime ideal* of I, if, for any prime ideal $Q \subset A$ with $I \subset Q \subset P$ we have $Q = P$. The set of minimal associated prime ideals of I is denoted by $\operatorname{minAss}(I)$.

Proposition 3.3.5. *Let A be a Noetherian ring and $I \subset A$ be an ideal. Then* $\operatorname{minAss}(I) = \{P_1, \dots, P_n\}$ *is finite and*

$$\sqrt{I} = P_1 \cap \dots \cap P_n \, .$$

In particular, $\sqrt{I}$ is the intersection of all prime ideals containing I.[3]

Proof. Obviously we have $\operatorname{minAss}(I) = \operatorname{minAss}(\sqrt{I})$ and, therefore, we may assume that $I = \sqrt{I}$.

If I is prime, the statement is trivial. Hence, we assume that there exist $a, b \notin I$ with $ab \in I$. We show that $\sqrt{I : \langle a \rangle} = I : \langle a \rangle = I : \langle a^2 \rangle \supsetneq I$. Namely, $f \in \sqrt{I : \langle a \rangle}$ implies $f^\rho \in I : \langle a \rangle$ for a suitable ρ. Therefore, $af^\rho \in I$ and $(af)^\rho \in I$, which implies $af \in \sqrt{I} = I$, that is, $f \in I : \langle a \rangle$. On the other hand, $f \in I : \langle a^2 \rangle$ implies $a^2 f \in I$ and $(af)^2 \in I$, that is, $af \in \sqrt{I} = I$ and, therefore, $f \in I : \langle a \rangle$. Finally, $b \in I : \langle a \rangle$ but $b \notin I$. Now, because of Lemma 3.3.6 below, we obtain $I = (I : \langle a \rangle) \cap \langle I, a \rangle$. In particular, we obtain

$$I = \sqrt{I} = \sqrt{(I : \langle a \rangle)} \cap \sqrt{\langle I, a \rangle} = (I : \langle a \rangle) \cap \sqrt{\langle I, a \rangle} \, .$$

If $I : \langle a \rangle$ or $\sqrt{\langle I, a \rangle}$ are not prime, we can continue with these ideals as we did with I. This process has to stop because A is Noetherian and, finally, we obtain $I = \bigcap_{i=1}^n P_i$ with P_i prime. We may assume that $P_i \not\subset P_j$ for $i \neq j$ by deleting unnecessary primes. In this case we have $\operatorname{minAss}(I) = \{P_1, \dots, P_n\}$. For, if $P \supset I$ is a prime ideal, then $P \supset \bigcap_{i=1}^n P_i$, and, therefore, there exist j such that $P \supset P_j$ by Lemma 1.3.12. This proves the proposition. $\square$

Lemma 3.3.6. (**Splitting tool**) Let A be a ring, $I \subset A$ an ideal, and let $I : \langle a \rangle = I : \langle a^2 \rangle$ for some $a \in A$. Then $I = (I : \langle a \rangle) \cap \langle I, a \rangle$.

Proof. Let $f \in (I : \langle a \rangle) \cap \langle I, a \rangle$, and let $f = g + xa$ for some $g \in I$. Then $af = ag + xa^2 \in I$ and, therefore, $xa^2 \in I$. That is, $x \in I : \langle a^2 \rangle = I : \langle a \rangle$, which implies $xa \in I$ and, consequently, $f \in I$. $\square$

[3] The latter statement is also true for not necessarily Noetherian rings, see also Exercise 3.3.1.

Example 3.3.7.

(1) Let $I = \langle wx, wy, wz, vx, vy, vz, ux, uy, uz, y^3 - x^2\rangle \subset K[v, w, x, y, z]$. Then $I = \langle x, y, z\rangle \cap \langle u, v, w, x^2 - y^3\rangle$, $\mathrm{minAss}(I) = \{\langle x, y, z\rangle, \langle u, v, w, x^2 - y^3\rangle\}$.
(2) Let $I = \langle x^2, xy\rangle \subset K[x, y]$ then $I = \langle x\rangle \cap \langle x^2, y\rangle$, $\sqrt{I} = \langle x\rangle$ and, hence, $\mathrm{minAss}(I) = \{\langle x\rangle\}$.

The minimal associated primes can be computed (with two different algorithms) using the Singular library `primdec.lib`:

SINGULAR Example 3.3.8 (minimal associated primes).

```
ring A=0,(u,v,w,x,y,z),dp;
ideal I=wx,wy,wz,vx,vy,vz,ux,uy,uz,y3-x2;
LIB"primdec.lib";
minAssGTZ(I);
//-> [1]:                     [2]:
//->    _[1]=z                   _[1]=-y3+x2
//->    _[2]=y                   _[2]=w
//->    _[3]=x                   _[3]=v
//->                             _[4]=u
ring B=0,(x,y,z),dp;
ideal I=zx,zy;
minAssChar(I);
//-> [1]:                     [2]:
//->    _[1]=y                   _[1]=z
//->    _[2]=x
```

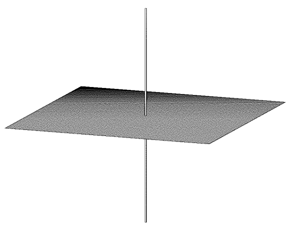

Fig. 3.5. The variety $V(xz, yz)$.

The minimal associated primes of $\langle zx, zy\rangle$ are $\langle z\rangle$ and $\langle x, y\rangle$ which correspond to two components of dimension 2, respectively 1, that is, to the plane, respectively the line, in Figure 3.5.

The following lemma is easy to prove and left as an exercise.

Lemma 3.3.9. *Let A be a ring and $A_{\mathrm{red}} := A/\sqrt{\langle 0\rangle}$ the* reduction *of A, then*

$$\dim(A) = \dim(A_{\mathrm{red}}) = \max_{P\in\mathrm{minAss}(\langle 0\rangle)} \{\dim(A/P)\}\,.$$

Remark 3.3.10. It is possible for a Noetherian integral domain to have infinite dimension: let K be a field and let $A = k[x_1, x_2, \ldots]$ be a polynomial ring in countably many indeterminates. Let $(\nu_j)_{j\geq 1}$ be a strictly increasing sequence of positive integers such that $(\nu_{j+1} - \nu_j)_{j\geq 1}$ is also strictly increasing. Let $P_i := \langle x_{\nu_{i+1}}, \ldots, x_{\nu_i+1}\rangle$ and $S = A \smallsetminus \bigcup_i P_i$. Then $S^{-1}A$ is a Noetherian integral domain (using Exercise 3.3.3). But $\mathrm{ht}(S^{-1}P_i) = \nu_{i+1} - \nu_i$ implies $\dim(S^{-1}A) = \infty$.

Remark 3.3.11. Notice that the ring in the previous remark is not local. We shall see in Chapter 5 that local Noetherian rings have finite dimension. In particular, this implies (using localization) that in a Noetherian ring the height of an ideal is always finite.

Remark 3.3.12. For graded rings, we shall obtain in Chapter 5 another description of the dimension as the degree of the Hilbert polynomial. This will be the basis to compute the dimension due to the fact that for an ideal $I \subset K[x_1, \ldots, x_n]$

$$\dim(K[x_1, \ldots, x_n]/I) = \dim(K[x_1, \ldots, x_n]/L(I))\,,$$

where $L(I)$ is the leading ideal of I (cf. Corollary 5.3.14).

Thus, after a Gröbner basis computation, the computation of the dimension is reduced to a pure combinatorial problem.

SINGULAR Example 3.3.13 (computation of the dimension).
Let I be the ideal of Example 3.3.7 (1). We want to compute the dimension:

```
ring A=0,(u,v,w,x,y,z),dp;
ideal I=wx,wy,wz,vx,vy,vz,ux,uy,uz,y3-x2;
I=std(I);
dim(I);
//-> 3
```

The next lemmas prepare applications of the Noether normalization theorem (see Section 3.4).

Lemma 3.3.14. *Let A be a ring such that for each prime ideal $P \subset A$ there exists a normal Noetherian integral domain $C \subset A$ with $C \subset A/P$ being finite. Then the following holds:*

If $A \subset B$ is a finite ring extension then the map $\mathcal{C}(B) \to \mathcal{C}(A)$ induced by the contraction $P \mapsto P \cap A$ maps maximal chains to maximal chains.

Proof. Let $\langle 0\rangle = Q_0 \subset Q_1 \subset \cdots \subset Q_n$ be a maximal chain of prime ideals in B and consider $\langle 0\rangle = Q_0 \cap A \subset Q_1 \cap A \subset \cdots \subset Q_n \cap A$. We have to prove that this chain is maximal. Assume $Q \subset Q' \subset B$ are two prime ideals and there exists a prime ideal $P \subset A$ such that $Q \cap A \subsetneq P \subsetneq Q' \cap A$. We choose for $Q \cap A$ an integrally closed, Noetherian integral domain A' such that $A' \subset A/(Q \cap A)$ is finite. Note that the ideals $\langle 0\rangle$, $P/(Q\cap A) \cap A'$, $Q'/(Q \cap A) \cap A'$ are pairwise different as $A' \subset A/(Q \cap A)$ is finite (Corollary 3.3.3). Moreover, B/Q is also finite over A', and we can apply the going down theorem to find a prime ideal $\bar{P}' \neq \langle 0\rangle$ in B/Q, $\bar{P}' \subset Q'/Q$ such that $\bar{P}' \cap A' = P \cap A'$. Therefore, $\bar{P}' \subsetneq Q'/Q$. This implies the existence of a prime ideal P', $Q \subsetneq P' \subsetneq Q'$ and proves the lemma, because the case $Q' \cap A \subsetneq P$, can be handled similarly. □

Remark 3.3.15. It is a consequence of the Noether normalization theorem (cf. Section 3.4) that all rings of finite type over a field K have the property required in the assumption of the lemma.

Lemma 3.3.16. *Let A, B satisfy the assumptions of the going down theorem (Theorem 3.2.9). If $Q \subset B$ is a prime ideal then* $\mathrm{ht}(Q) = \mathrm{ht}(Q \cap A)$.

Proof. Due to Corollary 3.3.3, the map $\mathcal{C}(B) \to \mathcal{C}(A)$ induced by $P \mapsto P \cap A$ induces a map $\mathcal{C}(B, Q) \to \mathcal{C}(A, Q \cap A)$, preserving the length of prime ideal chains. To see that this map is surjective, let $Q \cap A = P_s \supsetneq P_{s-1} \supsetneq \cdots \supsetneq P_0$ be a chain of prime ideals in A. Starting with P_{s-1}, and using s times the going down theorem, we obtain a chain $Q = Q_s \supsetneq Q_{s-1} \supsetneq \cdots \supsetneq Q_0$ of prime ideals in B. This proves the lemma. □

Exercises

3.3.1. Let A be a ring and $I \subsetneq A$ a proper ideal. Prove that $\sqrt{I}$ is the intersection of all prime ideals containing I.

(Hint: reduce the statement to the case $I = \langle 0\rangle$ and consider, for $f \in A$ not nilpotent, the set of all ideals not containing any power of f. Show that this set contains a prime ideal by using Zorn's lemma.)

3.3.2. Prove Lemma 3.3.9.

3.3.3. Let A be a ring such that

(1) for each maximal ideal M of A, the localization A_M is Noetherian;
(2) for each $x \neq 0$ in A the set of maximal ideals of A which contain x is finite.

Prove that A is Noetherian.

3.3.4. Check the statement of Example 3.3.2 (2), (3). Moreover, draw the zero–set in $\mathbb{R}^3$ of the ideal

$$I := \langle x \cdot (x^2 + y^2 + z^2 - 1),\ y \cdot (x^2 + y^2 + z^2 - 1)\rangle \subset \mathbb{R}[x, y, z]$$

to see the phenomena occurring in (3).

3.3.5. Use Singular to compute

(1) the minimal associated primes of the ideal

$$I = \langle t-b-d,\ x+y+z+t-a-c-d,\ xz+yz+xt+zt-ac-ad-cd,\\ xzt-acd\rangle \subset \mathbb{Q}[a, b, c, d, t, x, y, z]\,,$$

(2) the intersection of the minimal associated primes, and
(3) the radical of I,

and verify the statement of Proposition 3.3.5.

3.3.6. Let $P \subset K[x_1, \dots, x_s]$ be a homogeneous prime ideal of height r. Prove that there exists a chain $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_r = P$ of homogeneous prime ideals.

3.3.7. Prove that a principal ideal domain has dimension at most 1.

3.3.8. Let A be a Noetherian ring. Prove that $\dim(A[x]) = \dim(A) + 1$.

3.3.9. Let A be a Noetherian ring. Use the previous Exercise 3.3.8 to prove that $\dim(A[x, x^{-1}]) = \dim(A) + 1$.

3.3.10. Let A be a Noetherian ring, and let $P \in \mathrm{minAss}(\langle 0\rangle)$. Prove that $A_P = Q(A)_{PQ(A)}$.

3.3.11. Let K be a field and $A = K[x, y]_{\langle x,y\rangle}/\langle x^2, xy\rangle$. Prove that A is equal to its total ring of fractions, $A = Q(A)$, and $\dim(A) = 1$.

3.3.12. Show that $A := \mathbb{Q}[x, y, z]/\langle xy, xz, yz, (x-y)(x+1), z^3\rangle$ has dimension 0. Compute the $\mathbb{Q}$–vector space dimension of A and compare it to the $\mathbb{Q}$–vector space dimension of the localization of A in $\langle x, y, z\rangle$.

3.3.13. Let K be a field and $A = K[x, y]$. Prove that Lemma 3.3.14 does not hold for $B = K[x, y, z]/\langle xz, z^2 - yz\rangle$.

3.4 Noether Normalization

Let K be a field, $A = K[x_1, \dots, x_n]$ be the polynomial ring and $I \subset A$ an ideal.

Noether normalization is a basic tool in the theory of affine K–algebras, that is, algebras of type A/I. It is the basis for many applications of the theorems of the previous chapters, because it provides us with a polynomial ring $K[x_{s+1}, \dots, x_n] \subset A/I$ such that the extension is finite.

Theorem 3.4.1 (Noether normalization). *Let K be a field, and let $I \subset K[x_1, \ldots, x_n]$ be an ideal. Then there exist an integer $s \leq n$ and an isomorphism*

$$\varphi : K[x_1, \ldots, x_n] \to A := K[y_1, \ldots, y_n],$$

such that:

(1) the canonical map $K[y_{s+1}, \ldots, y_n] \to A/\varphi(I)$, $y_i \mapsto y_i \bmod \varphi(I)$ is injective and finite.
(2) Moreover, φ can be chosen such that, for $j = 1, \ldots, s$, there exist polynomials

$$g_j = y_j^{e_j} + \sum_{k=0}^{e_j-1} \xi_{j,k}(y_{j+1}, \ldots, y_n) \cdot y_j^k \in \varphi(I)$$

satisfying $e_j \geq \deg(\xi_{j,k}) + k$ for $k = 0, \ldots, e_j - 1$.
(3) If I is homogeneous then the g_j can be chosen to be homogeneous, too. If I is a prime ideal, the g_j can be chosen to be irreducible.
(4) If K is perfect and if I is prime, then the morphism φ can be chosen such that, additionally, $Q\big(A/\varphi(I)\big) \supset Q(K[y_{s+1}, \ldots, y_n])$ is a separable field extension and, moreover, if K is infinite then

$$Q\big(A/\varphi(I)\big) = Q(K[y_{s+1}, \ldots, y_n])[y_s]/\langle g_s \rangle .$$

(5) If K is infinite then φ can be chosen to be linear, $\varphi(x_i) = \sum_j m_{ij} y_j$ with $M = (m_{ij}) \in \mathrm{GL}(n, K)$.

Definition 3.4.2. Let $I \subset A = K[y_1, \ldots, y_n]$ be an ideal. A finite and injective map $K[y_{s+1}, \ldots, y_n] \to A/I$ is called a *Noether normalization* of A/I. If, moreover, I contains $g_1, \ldots, g_s$ as in Theorem 3.4.1 (2), then it is called a *general Noether normalization.*

Example 3.4.3. $K[x] \subset K[x, y]/\langle x^3 - y^2 \rangle$ is a Noether normalization, but not a general Noether normalization, while $K[y] \subset K[x, y]/\langle x^3 - y^2 \rangle$ is a general Noether normalization.

Proof of Theorem 3.4.1. We prove the theorem for infinite fields, while the proof for finite fields is left as Exercise 3.4.1. The case $I = \langle 0 \rangle$ being trivial, we can suppose $I \neq \langle 0 \rangle$. We proceed by induction on n. Let $n = 1$, and let $I = \langle f \rangle$, f a polynomial of degree d. Then $K[x_1]/I = K + x_1 K + \cdots + x_1^{d-1} K$ is a finite dimensional K–vector space, and the theorem holds with $s = 1$.

Assume now that the theorem is proved for $n - 1 \geq 1$, and let $f \in I$ be a polynomial of degree $d \geq 1$. If I is homogeneous we choose f to be homogeneous. Let $f = \sum_{\nu=0}^{d} f_\nu$ be the decomposition of f into homogeneous parts f_ν of degree ν. To keep notations short in the following construction of the morphism φ, we identify the x_i (resp. the y_j) with their images in $K[y_1, \ldots, y_n]$ (resp. in $K[z_2, \ldots, z_n]$). Let $M_1 = (m_{ij}) \in \mathrm{GL}(n, K)$,

$$M_1 \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} .$$

Then we obtain

$$\begin{aligned} f_d(x_1, \dots, x_n) &= f_d\left(\sum_{j=1}^{n} m_{1j} y_j, \dots, \sum_{j=1}^{n} m_{nj} y_j\right) \\ &= f_d\big(m_{11}, \dots, m_{n1}\big) \cdot y_1^d + \text{ lower terms in } y_1 . \end{aligned}$$

Now the condition for M_1 becomes $f_d(m_{11}, \dots, m_{n1}) \neq 0$, which can be satisfied as K is infinite. Then, obviously, $K[y_2, \dots, y_n] \to A/\langle f \rangle$ is injective and finite by Proposition 3.1.2, since y_1 satisfies an integral relation, and $\widetilde{g}_1 := f(M_1 y)$ has, after normalizing, the property required in (2).

Note that $K[y_2, \dots, y_n]/(I \cap K[y_2, \dots, y_n]) \to A/I$ is injective and still finite (we write I instead of $\varphi(I)$). If $I \cap K[y_2, \dots, y_n] = \langle 0 \rangle$ then there is nothing to show.

Otherwise, let $I_0 := I \cap K[y_2, \dots, y_n]$. By the induction hypothesis there is some matrix $M_0 \in \mathrm{GL}(n-1, K)$ such that, for

$$M_0 \cdot \begin{pmatrix} z_2 \\ \vdots \\ z_n \end{pmatrix} = \begin{pmatrix} y_2 \\ \vdots \\ y_n \end{pmatrix}$$

and some $s \leq n$, the map $K[z_{s+1}, \dots, z_n] \to K[y_2, \dots, y_n]/I_0$ is injective and finite. Moreover, for $j = 2, \dots, s$ there exist polynomials

$$g_j = z_j^{e_j} + \sum_{k=0}^{e_j - 1} \xi_{j,k}(z_{j+1}, \dots, z_n) \cdot z_j^k \in I$$

such that $e_j \geq \deg(\xi_{j,k}) + k$ for $k = 0, \dots, e_j - 1$. Again, the g_j can be chosen to be homogeneous if I is homogeneous.

This implies that $K[z_{s+1}, \dots, z_n] \to A/I$ is injective and finite. The theorem is proved for

$$M = M_1 \cdot \begin{pmatrix} 1 & 0 \dots 0 \\ 0 & \\ \vdots & M_0 \\ 0 & \end{pmatrix}$$

and $g_1 := \widetilde{g}_1\,(y_1, M_0 z)$, $g_2, \dots, g_s \in K[y_1, z_2, \dots, z_n]$.

If I is prime and if a g_j splits into irreducible factors then already one of the factors must be in I. We take this factor which has the desired shape.

The proof of (4) in the case of characteristic zero is left as Exercise 3.4.4. For the general case, we refer to [66, 159]. (5) was already proved in (1). □

Remark 3.4.4. The proof of Theorem 3.4.1 shows that

(1) the theorem holds for M arbitrarily chosen in

- some open dense subset $U \subset \mathrm{GL}(n, K)$, respectively
- some open dense subset U' in the set of all lower triangular matrices with entries 1 on the diagonal;

(2) the theorem holds also for finite fields if the characteristic is large;
(3) for a finite field of small characteristic the theorem also holds, when replacing the linear coordinate change $M \cdot y = x$ by a coordinate change of type $x_i = y_i + h_i(y)$, $\deg(h_i) \geq 2$, see Exercises 3.4.1 and 3.4.2.

The general Noether normalization is necessary in the theory of Hilbert functions, as we shall see in Chapter 5.

Analyzing the proof we obtain the following algorithm to compute a Noether normalization, which is correct and works well for characteristic 0 and large characteristic:

Algorithm 3.4.5 (NoetherNormalization(I)).

Input: $I := \langle f_1, \ldots, f_k \rangle \subset K[x]$, $x = (x_1, \ldots, x_n)$.
Output: A set of variables $\{x_{s+1}, \ldots, x_n\}$ and a map $\varphi : K[x] \to K[x]$ such that $K[x_{s+1}, \ldots, x_n] \subset K[x]/\varphi(I)$ is a Noether normalization.

- perform a random lower triangular linear coordinate change
$$\varphi(x) = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ * & & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} ;$$
- compute a reduced standard basis $\{f_1, \ldots, f_r\}$ of $\varphi(I)$ with respect to the lexicographical ordering with $x_1 > \cdots > x_n$, and order the f_i such that $\mathrm{LM}(f_r) > \cdots > \mathrm{LM}(f_1)$;
- choose s maximal such that $\{f_1, \ldots, f_r\} \cap K[x_{s+1}, \ldots, x_n] = \emptyset$;
- for each $i = 1, \ldots, s$, test whether $\{f_1, \ldots, f_r\}$ contains polynomials with leading monomial $x_i^{\rho_i}$ for some ρ_i;
- if the test is true for all i then return φ and $x_{s+1}, \ldots, x_n$ (note that in this case $K[x_{s+1}, \ldots, x_n] \subset K[x_1, \ldots, x_n]/\varphi(I)$ is finite);
- return NoetherNormalization(I).

Let us try an example:

SINGULAR Example 3.4.6 (Noether normalization).

```
LIB"random.lib";
ring R=0,(x,y,z),lp;
ideal I=xy,xz;
dim(std(I));
//-> 2
ideal M=ideal(sparsetriag(3,3,0,100)
                  *transpose(maxideal(1)));
```

```
M;
//-> M[1]=x   M[2]=65x+y   M[3]=85x+82y+z

map phi=R,M;
ideal J=phi(I);   //the random coordinate change
J;
//-> J[1]=65x2+xy   J[2]=85x2+82xy+xz

//dim(I)=2 implies R/J <--Q[y,z] is a Noether normalization
```

The algorithm in the SINGULAR programming language can be found in Section 3.7 at the end of this chapter.

Exercises

3.4.1. (*Noether normalization over finite fields*).
Let K be a finite field, and let $f \in K[x_1, \ldots, x_n] \setminus K$. Prove that there exist $y_2, \ldots, y_n \in K[x_1, \ldots, x_n]$ such that $K[y_2, \ldots, y_n] \subset K[x_1, \ldots, x_n]/\langle f \rangle$ is finite. For any sufficiently large e one can choose $y_i = x_i - x_1^{e^i}$.

If f is homogeneous then $y_2, \ldots, y_n$ can be chosen to be homogeneous.

3.4.2. Use Exercise 3.4.1 to prove the Noether normalization theorem 3.4.1 in the case of a finite field, replacing the linear coordinate change $M \cdot y = x$ by a coordinate change of the form $x_i = y_i + h_i(y_1, \ldots, y_{i-1})$, $i = 1, \ldots, n$, $h_1 = 0$.

3.4.3. Write a SINGULAR procedure to compute a Noether normalization over finite fields.

3.4.4. With the notations and assumptions of Theorem 3.4.1 prove that if I is a prime ideal and the characteristic of K is zero, then g_s can be chosen such that $Q(A/I) = Q(K[y_{s+1}, \ldots, y_n])[y_s]/\langle g_s \rangle$.

3.4.5. Compute a general Noether normalization for the ideal

$$I = \langle x^3 + xy - z,\ y^3 - t + z,\ x^2y + xy^2 - u \rangle \subset \mathbb{Q}[x, y, z, t, u].$$

Prove that I is a prime ideal. Check this using SINGULAR. Check whether your Noether normalization has the properties of Exercise 3.4.4.

3.4.6. (*Noether normalization for local rings*).
Let K be a field. Then $f \in K[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle}$ is called a *Weierstraß polynomial* of degree s with respect to x_n if $f = x_n^s + a_{s-1}x_n^{s-1} + \cdots + a_0$, with $a_i \in \langle x_1, \ldots, x_{n-1} \rangle \cdot K[x_1, \ldots, x_{n-1}]_{\langle x_1, \ldots, x_{n-1} \rangle}$. Prove that

$$K[x_1, \ldots, x_{n-1}]_{\langle x_1, \ldots, x_{n-1} \rangle} \subset K[x_1, \ldots, x_n]_{\langle x_1, \ldots, x_n \rangle}/\langle g \rangle$$

is finite and injective for $g \in K[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$ if and only if $u \cdot g$ is a Weierstraß polynomial of degree ≥ 1 with respect to x_n for a suitable unit u.

(Hint: prove that the extension above is finite if and only if the localization $S^{-1}K[x_1, \ldots, x_n]/\langle g\rangle$ w.r.t. $S := \{g \in K[x_1, \ldots, x_{n-1}] \mid g(0) \neq 0\}$ is a local ring.)

3.4.7. Let $f = x^4 + y^4 + x^3 + y^3 + x^2 + y^2 + x + y \in K[x, y]$. Prove that there exists no linear automorphism $\varphi : K[x, y]_{\langle x,y\rangle} \to K[x, y]_{\langle x,y\rangle}$ such that $\varphi(f)$ is a product of a unit and a Weierstraß polynomial (cf. Exercise 3.4.6). This proves that, in general, Noether normalization as in Theorem 3.4.1 does not hold for localizations of polynomial rings.

(Hint: use the fact that the polynomial ring is a unique factorization domain and that f is irreducible to prove that $\varphi(f) = ug$, u a unit, g a Weierstraß polynomial, implies that $\varphi(f)$ is already a Weierstraß polynomial.)

3.4.8. Formulate and prove Theorem 3.4.1 for ideals generated by homogeneous polynomials in $K[x_1, \ldots, x_n]_{\langle x_1,\ldots,x_n\rangle}$.

3.5 Applications

In this section we shall use the Noether normalization to develop the dimension theory for the polynomial ring $K[x_1, \ldots, x_n]$ and, more generally, affine algebras $K[x_1, \ldots, x_n]/I$. We shall prove Hilbert's Nullstellensatz and give an algorithm to compute the dimension of an affine algebra. Finally, we prove that the normalization of an affine algebra R, being an integral domain, is finite over R and, therefore, again an affine algebra.

Theorem 3.5.1. *Let K be a field and $A = K[x]$, $x = \{x_1, \ldots, x_n\}$. Then*

(1) $\dim(A) = n$*, moreover, all maximal chains in $\mathcal{C}(A)$ have length n.*
(2) If $f \in A$, $\deg(f) \geq 1$*, then* $\dim\big(A/\langle f\rangle\big) = n - 1$ *(Krull's principal ideal theorem).*
(3) If $P \subset A$ is a prime ideal then $ht(P)$ $+ \dim(A/P) = \dim(A) = n$.
(4) If $P \subset A$ is a prime ideal then $\dim(A/P) = \mathrm{trdeg}_K\, Q(A/P)$*, the transcendence degree of the field extension $K \subset Q(A/P)$. Moreover, all maximal chains in $\mathcal{C}(A/P)$ have the length* $\dim(A/P)$.
(5) If $M \subset A$ is a maximal ideal, then $A/M \supset K$ is finite (Hilbert's Nullstellensatz)[4].
(6) Let $I \subset A$ be an ideal and $u \subset x$ be a subset such that $I \cap K[u] = 0$, then $\dim(A/I) \geq \#u$*. Furthermore, there exists some $u \subset x$ with $I \cap K[u] = 0$ and* $\dim(A/I) = \#u$.[5]

[4] This is a weak form of Hilbert's Nullstellensatz. For K algebraically closed we obtain $A/M = K$, hence, the maximal ideals are of type $\langle x_1 - a_1, \ldots, x_n - a_n\rangle$.
[5] Note that u is allowed to be empty, that is, $\#u = 0$.

(7) *Let $I \subsetneq A$ be an ideal, and let S be a standard basis of I with respect to any global ordering $>$ on* $\mathrm{Mon}(x_1, \dots, x_n)$. *Then* $\dim(I) = 0$ *if and only if $L(I)$ contains suitable powers of each variable x_i, $i = 1, \dots, n$. This is the case if and only if S contains, for each variable x_i, an element whose leading monomial is $x_i^{a_i}$ for some a_i.*

Proof. We use induction on n, the case $n = 0$ being trivial. To prove (1), let $\langle 0 \rangle = P_0 \subsetneq \cdots \subsetneq P_m \subsetneq A$ be a maximal chain in $C(A)$. Choose an irreducible $f \in P_1$ and coordinates $y_1, \dots, y_{n-1}$ (Theorem 3.4.1 and Exercise 3.4.2) such that $K[x_1, \dots, x_n]/\langle f \rangle \supset K[y_1, \dots, y_{n-1}]$ is finite. Then, clearly, the chain

$$\langle 0 \rangle = P_1/\langle f \rangle \subsetneq P_1/\langle f \rangle \subsetneq \cdots \subsetneq P_m/\langle f \rangle$$

is maximal, too. Using Lemma 3.3.14 and the Noether normalization theorem, this chain induces a maximal chain in $K[y_1, \dots, y_{n-1}]$ which, due to the induction hypothesis, has length $n - 1$.

(3), (2) are immediate consequences of (1), respectively its proof. To prove (4), we may assume, again, that $A/P \supset K[y_1, \dots, y_s]$ is finite. Then Corollary 3.3.3 implies $\dim(A/P) = \dim(K[y_1, \dots, y_s])$, which equals s due to (1). On the other hand, $\mathrm{trdeg}_K\, Q(A/P) = \mathrm{trdeg}_K\, Q(K[y_1, \dots, y_s]) = s$.

Moreover, each maximal chain $\bar{P}_m \supsetneq \cdots \supsetneq \bar{P}_0 = \langle 0 \rangle$ of primes in A/P lifts to a maximal chain $P_m \supsetneq \cdots \supsetneq P_0 = P \supsetneq \cdots \supsetneq \langle 0 \rangle$ of prime ideals in A.

(5) is a consequence of Theorem 3.4.1 and the fact that M is maximal: if $K[y_1, \dots, y_s] \subset A/M$ is finite, then, because A/M is a field and by Lemma 3.1.9, $K[y_1, \dots, y_s]$ is also a field, hence, $s = 0$.

(6) Let $u \subset x$ be a subset such that $I \cap K[u] = \langle 0 \rangle$. In particular, we have $\sqrt{I} \cap K[u] = \langle 0 \rangle$, hence, $\bigcap_{P \in \mathrm{minAss}(I)} (P \cap K[u]) = \langle 0 \rangle$ (Proposition 3.3.5). This implies $P \cap K[u] = \langle 0 \rangle$ for some $P \in \mathrm{minAss}(I)$ (Lemma 1.3.12) and, therefore, $K(u) \subset Q(K[x]/P)$. We obtain

$$\dim(K[x]/I) \geq \dim(K[x]/P) = \mathrm{trdeg}_K\, Q(K[x]/P) \geq \#u\,.$$

Now let $P \in \mathrm{minAss}(I)$ with $d = \dim(K[x]/I) = \dim(K[x]/P)$. Then, due to (4), we may choose $x_{i_1}, \dots, x_{i_d}$ being algebraically independent modulo P. Then $P \cap K[u] = \langle 0 \rangle$ for $u := \{x_{i_1}, \dots, x_{i_d}\}$ and, therefore, $I \cap K[u] = \langle 0 \rangle$.

(7) We use (6) to see that $I \cap K[x_i] \neq \langle 0 \rangle$ for all i because I is zero–dimensional. Let $f \in I \cap K[x_i]$, $f \neq 0$, then $\mathrm{LM}(f) = x_i^{a_i}$ for a suitable $a_i > 0$ (f is not constant and $>$ is a well–ordering). By definition of a standard basis there exist $g \in S$ and $\mathrm{LM}(g) \mid \mathrm{LM}(f)$. This proves the "only if"–direction.

For the "if"–direction, we show that under our assumption on S, $K[x]/I$ is, indeed, a finite dimensional K–vector space. Let $p \in K[x]$ be any polynomial, and consider $\mathrm{NF}(p \mid S)$, the reduced normal form of p with respect to S. Then, clearly $\mathrm{NF}(p \mid S) = \sum_\beta c_\beta x^\beta$, where $c_\beta \neq 0$ implies $\beta_i < a_i$ for all i. In particular, the images of the monomials x^β with $\beta_i < a_i$ for all i generate $K[x]/I$ as K–vector space. □

Theorem 3.5.2 (Hilbert's Nullstellensatz). *Assume that $K = \overline{K}$ is an algebraically closed field. Let $I \subset K[x] = K[x_1, \ldots, x_n]$ be an ideal, and let*

$$V(I) = \big\{x \in K^n \;\big|\; f(x) = 0 \textit{ for all } f \in I\big\}\,.$$

If, for some $g \in K[x]$, $g(x) = 0$ for all $x \in V(I)$ then $g \in \sqrt{I}$.

Proof. We consider the ideal $J := IK[x,t] + \langle 1 - tg\rangle$ in the polynomial ring $K[x,t] = K[x_1, \ldots, x_n, t]$.

If $J = K[x,t]$ then there exist $g_1, \ldots, g_s \in I$ and $h, h_1, \ldots, h_s \in K[x,t]$ such that $1 = \sum_{i=1}^{s} g_i h_i + h(1 - tg)$. Setting $t := \frac{1}{g} \in K[x]_g$, this implies

$$1 = \sum_{i=1}^{s} g_i \cdot h_i \left(x, \frac{1}{g}\right) \in K[x]_g\,.$$

Clearing denominators, we obtain $g^\rho = \sum_i g_i h_i'$ for some $\rho > 0$, $h_i' \in K[x]$, and, therefore, $g \in \sqrt{I}$.

Now assume that $J \subsetneq K[x,t]$. We choose a maximal ideal $M \subset K[x,t]$ such that $J \subset M$. Using Theorem 3.5.1 (5) we know (since K is algebraically closed) that $K[x,t]/M \cong K$, and, hence, $M = \langle x_1 - a_1, \ldots, x_n - a_n, t - a\rangle$, for some $a_i, a \in K$. Now $J \subset M$ implies $(a_1, \ldots, a_n, a) \in V\big(J\big)$.

If $(a_1, \ldots, a_n) \in V(I)$ then $g(a_1, \ldots, a_n) = 0$. Hence, $1 - tg \in J$ does not vanish at $(a_1, \ldots, a_n)$, contradicting the assumption $(a_1, \ldots, a_n, a) \in V\big(J\big)$. If $(a_1, \ldots, a_n) \notin V\big(I\big)$ then there is some $h \in I$ such that $h(a_1, \ldots, a_n) \neq 0$, in particular (as h does not depend on t) $h(a_1, \ldots, a_n, a) \neq 0$ and, therefore, $(a_1, \ldots, a_n, a) \notin V(J)$, again contradicting our assumption. □

Definition 3.5.3. Let $I \subset K[x_1, \ldots, x_n]$ be an ideal. Then a subset

$$u \subset x = \{x_1, \ldots, x_n\}$$

is called an *independent set* (with respect to I) if $I \cap K[u] = 0$. An independent set $u \subset x$ (with respect to I) is called *maximal* if $\dim(K[x]/I) = \#u$.

Example 3.5.4. Let $I = \langle xz, yz\rangle \subset K[x,y,z]$, then $\{x,y\} \subset \{x,y,z\}$ is a maximal independent set. Notice that $\{z\} \subset \{x,y,z\}$ is independent and non–extendable (that is, cannot be enlarged) but it is not a maximal independent set.

Note that all maximal (resp. all non–extendable) independent sets of the leading ideal $L(I)$ are computed by the SINGULAR commands `indepSet(std(I))` (respectively by `indepSet(std(I),1)`). Thus, using these commands, we obtain independent sets of I but maybe not all. Exercises 3.5.1 and 3.5.2 show how to compute independent sets.

SINGULAR Example 3.5.5 (independent set).

```
ring R=0,(x,y,z),dp;
ideal I=yz,xz;
indepSet(std(I));
//-> 1,1,0
```

This means, $\{x, y\}$ is a maximal independent set for I.

```
indepSet(std(I),1);
//-> [1]:        [2]:
        1,1,0      0,0,1
```

This means, the only independent sets which cannot be enlarged are $\{x, y\}$ and $\{z\}$.

The geometrical meaning of $u \subset x$ being an independent set for I is that the projection of $V(I)$ to the affine space of the variables in u is surjective, since $V(I \cap K[u]) = V(\langle 0 \rangle)$ is the whole affine space.

```
ring A  = 0,(x,y,t),dp;
ideal I = y2-x3-3t2x2;
indepSet(std(I),1);
//-> [1]:          [2]:
       1,1,0         0,1,1
```

Hence, $\{x, y\}$ and $\{y, t\}$ are the only non–extendable independent sets for the leading ideal $L(I) = \langle t^2x^2 \rangle$. However, the ideal I itself has, additionally, $\{x, t\}$ as a non–extendable independent set. The difference is seen in the pictures in Figure 3.6, which are generated by the following SINGULAR session:

```
LIB"surf.lib";
plot(lead(I),"clip=cube;");
plot(I,"rot_x=1.4; rot_y=3.0; rot_z=1.44;"); //see Fig. 3.6
```

The first surface is $V\big(L(I)\big)$ and the second $V(I)$. The projection of $V\big(L(I)\big)$ to the $\{x, t\}$–plane is not dominant, but the projection of $V(I)$ is.

Next we want to compute the dimension of monomial ideals.

Definition 3.5.6. Let $I = \langle m_1, \dots, m_s \rangle \subset K[x] = K[x_1, \dots, x_n]$ be a monomial ideal (with $m_i \in \mathrm{Mon}(x_1, \dots, x_n)$ for $i = 1, \dots, s$). Then we define an integer $d(I, K[x])$ by the recursive formula: $d(\langle 0 \rangle, K[x]) := n$ and

$$d(I, K[x]) := \max \left\{ d\big(I\big|_{x_i=0}, K[x \smallsetminus x_i]\big) \;\middle|\; x_i \text{ divides } m_1 \right\} ,$$

where $x \smallsetminus x_i = (x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$.

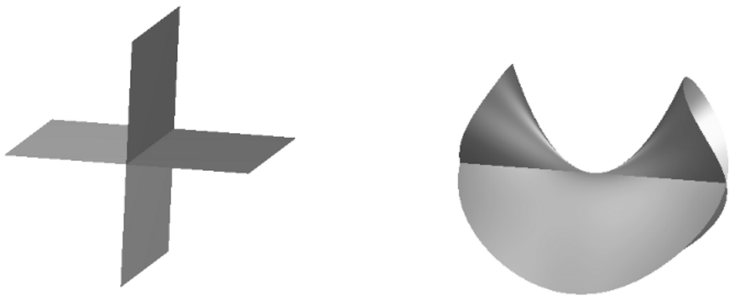

Fig. 3.6. The zero–sets of t^2x^2, respectively $y^2 - x^3 - 3t^2x^2$.

Example 3.5.7. Let $I = \langle xz, yz\rangle \subset K[x,y,z]$ then

$$d(I, K[x,y,z]) = \max\Big\{\underbrace{d(\langle yz\rangle, K[y,z])}_{=1}, \underbrace{d(\langle 0\rangle, K[x,y])}_{=2}\Big\} = 2.$$

Proposition 3.5.8. *Let $I = \langle m_1, \dots, m_s\rangle \subset K[x]$ be a monomial ideal, then*

$$\dim(K[x]/I) = d(I, K[x]) .$$

Proof. Let $P \supset I$ be a prime ideal, then for all i one factor of m_i has to be in P. In particular, for every $P \in \operatorname{minAss}(I)$ there exists some ρ, such that $x_\rho \in P$ divides m_1. In particular, we have $I|_{x_\rho=0} \subset P|_{x_\rho=0} \subset K[x \smallsetminus x_\rho]$. Using the induction hypothesis we may assume that

$$\begin{aligned} d\Big(I\big|_{x_\rho=0}, K[x \smallsetminus x_\rho]\Big) &= \dim\Big(K[x \smallsetminus x_\rho]/\big(I\big|_{x_\rho=0}\big)\Big) \\ &\geq \dim\Big(K[x \smallsetminus x_\rho]/\big(P\big|_{x_\rho=0}\big)\Big) = \dim\big(K[x]/P\big) . \end{aligned}$$

This implies that $d(I, K[x]) \geq \max_{P \in \operatorname{minAss}(I)} \dim(K[x]/P) = \dim(K[x]/I)$. Let us assume that $d(I, K[x]) > \dim(K[x]/I)$. Then there would exist some i such that x_i divides m_1 and

$$\dim\big(K[x]/I\big) < d\Big(I\big|_{x_i=0}, K[x \smallsetminus x_i]\Big) = \dim\Big(K[x \smallsetminus x_i]/\big(I\big|_{x_i=0}\big)\Big) ,$$

the latter equality being implied by the induction hypothesis. But

$$\dim\Big(K[x \smallsetminus x_i]/\big(I\big|_{x_i=0}\big)\Big) = \dim\big(K[x]/\langle I, x_i\rangle\big) \leq \dim\big(K[x]/I\big) ,$$

whence a contradiction. $\square$

SINGULAR Example 3.5.9 (computation of $d(I, K[x])$).
We give a procedure to compute the function $d(I, K[x])$ of Definition 3.5.6:

```
proc d(ideal I)
{
   int n=nvars(basering);
   int j,b,a;
   I=simplify(I,2);  //cancels zeros in the generators of I
   if(size(I)==0) {return(n);}  //size counts generators
                                //not equal to 0
   for(j=1;j<=n;j++)
   {
     if(I[1]/var(j)!=0)
     {
        a=d(subst(I,var(j),0))-1;
        //we need -1 here because we stay in the basering
        if(a>b) {b=a;}
     }
   }
   return(b);
}
```

Let us test the procedure:

```
ring R=0,(x,y,z),dp;
ideal I=yz,xz;

d(I);
//-> 2
dim(std(I));
//-> 2
```

We shall prove later that for any ideal $I \subset K[x]$,

$$\dim(K[x]/I) = \dim\big(K[x]/L(I)\big)\,.$$

Hence, $\dim(K[x]/I) = d\big(L(I), K[x]\big)$ is very easy to compute once we know generators for $L(I)$, which are the leading terms of a standard basis of I.

Now we prove the finiteness of the normalization.

Theorem 3.5.10 (E. Noether). *Let $P \subset K[x_1, \ldots, x_n]$ be a prime ideal, and let $A = K[x_1, \ldots, x_n]/P$, then the normalization $\overline{A} \supset A$ is a finite A–module.*

Remark 3.5.11. In general, that is, for an arbitrary Noetherian integral domain, Theorem 3.5.10 is incorrect, as discovered by Nagata [183, Ex. 5, p. 207]. The polynomial ring $K[x_1, \ldots, x_n]$ and, more generally, each affine algebra $R = K[x_1, \ldots, x_n]/I$ satisfy the following stronger[6] condition: for each

[6] Strictly speaking, this is only a stronger condition if K has characteristic $p > 0$.

prime ideal $P \subset R$ and for each finite extension field L of $Q(R/P)$, the integral closure of R/P in L is a finite R/P–module. A Noetherian ring with this property is called *universally Japanese* (in honour of Nagata).

To prove Theorem 3.5.10 we need an additional lemma. We shall give a proof for the case that K is a perfect field (for example, $\mathrm{char}(K) = 0$, or K is finite, or K is algebraically closed, cf. Exercise 1.1.6). For a proof in the general case, see [66, Corollary 13.15].

Lemma 3.5.12. *Let A be a normal Noetherian integral domain, $L \supset Q(A)$ a finite separable field extension and B the integral closure of A in L. Let $\alpha \in B$ be a primitive element of the field extension, F the minimal polynomial of α and Δ the discriminant of F.*[7] *Then $B \subset \frac{1}{\Delta}A[\alpha]$. In particular, B is a finite A–module.*

Proof of Theorem 3.5.10. We use the Noether normalization theorem and choose $y_1, \dots, y_s$ such that $K[y_1, \dots, y_s] \hookrightarrow K[x_1, \dots, x_n]/P$ is finite. We obtain a commutative diagram

$$\begin{tikzcd}
 & K[x_1,\dots,x_n]/P \arrow[dl, hook] \arrow[dd, hook] & K[y_1,\dots,y_s] \arrow[l, hook', "\text{finite}"'] \arrow[dd, hook] \\
\overline{A} \arrow[dr, hook] & & \\
 & Q(K[x_1,\dots,x_n]/P) & Q(K[y_1,\dots,y_s]) \arrow[l, hook', "\text{finite}"'] .
\end{tikzcd}$$

Notice that $\overline{A}$ is also the integral closure of $K[y_1, \dots, y_s]$ in the quotient field $Q(K[x_1, \dots, x_n]/P)$, which is a finite separable extension of $Q(K[y_1, \dots, y_s])$. Since $K[y_1, \dots, y_s]$ is a normal Noetherian integral domain, we obtain the assumption of Lemma 3.5.12, which proves the theorem. $\square$

Proof of Lemma 3.5.12. Let L_0 be the splitting field of F, and let $\alpha = \alpha_1$, $\alpha_2, \dots, \alpha_n \in L_0$ be the roots of F. Further, let B_0 be the integral closure of A in L_0. Then $\alpha_1, \dots, \alpha_n \in B_0$ (since F is monic), and we have the following diagram

$$\begin{array}{ccccc}
A & \subset & B & \subset & B_0 \\
\cap & & \cap & & \cap \\
Q(A) & \subset & L & \subset & L_0,
\end{array}$$

where $L_0 \supset Q(A)$ is Galois. We consider the matrix

[7] The *discriminant* of a univariate polynomial $F \in K[x]$ is defined to be the resultant of F and its derivative F'. If $\alpha_1, \dots, \alpha_n$ are the roots of F in the algebraic closure $\overline{K}$ of K then the discriminant equals $\prod_{i \neq j}(\alpha_i - \alpha_j)$, see, e.g., [162].