Solutions of Some Exercises

1.3. Let $\mathfrak{n} \in \operatorname{Spec}_{\max}(R)$ and consider the homomorphism

$$\varphi\colon R[x] \to R/\mathfrak{n},\ f \mapsto f(0) + \mathfrak{n}.$$

The kernel $\mathfrak{m}$ of φ is a maximal ideal of $R[x]$, and $R \cap \mathfrak{m} = \mathfrak{n}$, so $\mathfrak{n} \in \operatorname{Spec}_{\mathrm{rab}}(R)$.

2.5.

(a) That S generates A means that for every element $f \in A$ there exist finitely many elements $f_1, \ldots, f_m \in S$ and a polynomial $F \in K[T_1, \ldots, T_m]$ in m indeterminates such that $f = F(f_1, \ldots, f_m)$. Let $P_1, P_2 \in K^n$ be points with $f(P_1) \neq f(P_2)$. Then

$$F\left(f_1(P_1), \ldots, f_m(P_1)\right) \neq F\left(f_1(P_2), \ldots, f_n(P_2)\right),$$

so $f_i(P_1) \neq f_i(P_2)$ for at least one i. This yields part (a).

(b) Consider the polynomial ring $B := K[x_1, \ldots, x_n, y_1, \ldots, y_n]$ in $2n$ indeterminates. Polynomials from B define functions $K^n \times K^n \to K$. For $f \in K[x_1, \ldots, x_n]$, define

$$\Delta f := f(x_1, \ldots, x_n) - f(y_1, \ldots, y_n) \in B.$$

So for $P_1, P_2 \in K^n$ we have $\Delta f(P_1, P_2) = f(P_1) - f(P_2)$. Consider the ideal

$$I := (\Delta f \mid f \in A)_B \subseteq B.$$

G. Kemper, *A Course in Commutative Algebra*, Graduate Texts in Mathematics 256, DOI 10.1007/978-3-642-03545-6,

By Hilbert's basis theorem (Corollary 2.13), B is Noetherian, so by Theorem 2.9 there exist $f_1, \ldots, f_m \in A$ such that

$$I = (\Delta f_1, \ldots, \Delta f_m)_B \,.$$

We claim that $S := \{f_1, \ldots, f_m\}$ is A-separating. For showing this, take two points P_1 and P_2 in K^n and assume that there exists $f \in A$ with $f(P_1) \neq f(P_2)$. Since $\Delta f \in I$, there exist $g_1, \ldots, g_m \in B$ with

$$\Delta f = \sum_{i=1}^{m} g_i \Delta f_i,$$

so

$$\sum_{i=1}^{m} g_i(P_1, P_2)\Delta f_i(P_1, P_2) = \Delta f(P_1, P_2) \neq 0.$$

Therefore we must have $\Delta f_i(P_1, P_2) \neq 0$ for some i, so $f_i(P_1) \neq f_i(P_2)$.

(c) $S = \{x, xy\}$ is R-separating.

3.6. Define a partial ordering "$\leq$" on set $\mathcal{M} := \{P \in \operatorname{Spec}(R) \mid P \subseteq Q\}$ by

$$P \leq P' \quad \Longleftrightarrow \quad P' \subseteq P$$

for $P, P' \in \mathcal{M}$. Let $\mathcal{C} \subseteq \mathcal{M}$ be a chain (=totally ordered subset) in $\mathcal{M}$. Set $\mathcal{C}' := \mathcal{C} \cup \{Q\}$ and $P := \bigcap_{P' \in \mathcal{C}'} P'$. Clearly P is an ideal of R, and $P \subseteq Q$. For showing that P is a prime ideal, take $a, b \in R$ with $ab \in P$ but $b \notin P$. There exists $P_0 \in \mathcal{C}'$ with $b \notin P_0$. Let $P' \in \mathcal{C}'$. Since $\mathcal{C}'$ is a chain, we have $P' \subseteq P_0$ or $P_0 \subseteq P'$. In the first case, $b \notin P'$ but $ab \in P'$, so $a \in P'$. In particular, $a \in P_0$. From this, $a \in P'$ follows in the case that $P_0 \subseteq P'$. We have shown that $a \in P$, so $P \in \mathcal{M}$. By the definition of the ordering, P is an upper bound for $\mathcal{C}$. Now Zorn's lemma yields a maximal element of $\mathcal{M}$, which is a minimal prime ideal contained in Q.

If $R \neq \{0\}$, there exists a maximal ideal $\mathfrak{m}$ of R (by Zorn's lemma applied to $\{I \subsetneqq R \mid I \text{ ideal}\}$ with the usual ordering), and by the above, $\mathfrak{m}$ contains a minimal prime ideal.

5.3. As in the proof of Theorem 5.9 and Proposition 5.10, we only have to show that $\operatorname{trdeg}(A) \leq \dim(A)$. By hypothesis, $A \subseteq B$ with B an affine K-algebra. By induction on n, we will show the following, stronger claim:

Claim. If $\operatorname{trdeg}(A) \geq n$, then there exists a chain

$$Q_0 \subseteq Q_1 \subseteq \cdots \subseteq Q_n$$

in $\operatorname{Spec}(B)$ such that with $P_i := A \cap Q_i \in \operatorname{Spec}(A)$ there are strict inclusions $P_{i-1} \subsetneqq P_i$ for $i = 1, \ldots, n$.

The claim is correct for $n = 0$. To prove it for $n > 0$, let $a_1, \ldots, a_n \in A$ be algebraically independent. As in the proof of Theorem 5.9, we see that there exists a minimal prime ideal M_i of B (not A!) such that the a_i are algebraically independent modulo M_i. Replacing B by B/M_i and A by $A/A \cap M_i$, we may assume that B is an affine domain. Set $L := \operatorname{Quot}(K[a_1])$, $A' := L \cdot A$ and $B' := L \cdot B$, which are all contained in $\operatorname{Quot}(B)$. A' has transcendence degree at least $n-1$ over L. By induction, there is a chain

$$Q_0' \subseteq Q_1' \subseteq \cdots \subseteq Q_{n-1}'$$

in $\operatorname{Spec}(B')$ such that with $P_i' := A' \cap Q_i' \in \operatorname{Spec}(A')$ there are strict inclusions $P_{i-1}' \subsetneqq P_i'$ for $i = 1, \ldots, n-1$. Set $Q_i := B \cap Q_i' \in \operatorname{Spec}(B)$ and $P_i := A \cap Q_i = A \cap P_i' \in \operatorname{Spec}(A)$. For $i = 1, \ldots, n-1$, we have $P_{i-1} \subsetneqq P_i$, since $P_{i-1} = P_i$ would imply

$$P_i' \subseteq (L \cdot A) \cap P_i' \subseteq L \cdot P_i = L \cdot P_{i-1} \subseteq L \cdot P_{i-1}' = P_{i-1}' \subsetneq P_i'.$$

As in the proof of Theorem 5.9, we see that A/P_{n-1} is not algebraic over K. Since A/P_{n-1} is contained in B/Q_{n-1}, it follows from Lemma 1.1(b) that A/P_{n-1} is not a field. Choose a maximal ideal $Q_n \subset B$ which contains Q_{n-1}. By Proposition 1.2, $P_n := A \cap Q_n$ is a maximal ideal of A. Clearly $P_{n-1} \subseteq P_n$. Since A/P_{n-1} is not a field, the inclusion is strict. So we have shown the claim, and the result follows.

6.8.

(a) We prove that the negations of both statements are equivalent. First, if $a \in P$, then $U_a \cap P \neq \emptyset$ since $a \in U_a$. If $P + (a)_R = R$, then $1 = b + xa$ with $b \in P$ and $x \in R$, so $b = 1 - xa \in U_a \cap P$. Conversely, if $U_a \cap P \neq \emptyset$, then $a^m(1 + xa) \in P$ with $m \in \mathbb{N}_0$ and $x \in R$. This implies $a \in P$ or $1 + xa \in P$. In the second case we obtain $P + (a)_R = R$.

(b) Assume that $\dim(R) \leq n$, and let $Q_0 \subsetneqq \cdots \subsetneqq Q_k$ be a chain of prime ideals in $U_a^{-1}R$, with $a \in R$. By Theorem 6.5, setting $P_i := \varepsilon^{-1}(Q_i)$ (with $\varepsilon\colon R \to U_a^{-1}R$ the canonical map) yields a chain of length k in $\operatorname{Spec}(R)$, and we have $U_a \cap P_i = \emptyset$. By part (a), this implies that P_i is not a maximal ideal (otherwise, $P_i + (a)_R$ would be R), so we can append a maximal ideal to this chain. Therefore $k + 1 \leq \dim(R) \leq n$, and we conclude $\dim\left(U_a^{-1}R\right) \leq n - 1$.

Conversely, assume $\dim\left(U_a^{-1}R\right) \le n-1$ for all $a \in R$. Let $P_0 \subsetneqq \cdots \subsetneqq P_k$ be a chain in $\operatorname{Spec}(R)$ of length $k > 0$. Choose $a \in P_k \setminus P_{k-1}$. Then $P_{k-1} + (a)_R \neq R$ (both ideals are contained in P_k), so $U_a \cap P_{k-1} = \emptyset$ by part (a). By Theorem 6.5, setting $Q_i := U_a^{-1}P_i$ $(i = 0, \ldots, k-1)$ yields a chain of length $k-1$ in $\operatorname{Spec}\left(U_a^{-1}R\right)$. Therefore $k - 1 \le \dim\left(U_a^{-1}R\right) \le n-1$. We conclude $\dim(R) \le n$ if $n > 0$. If $n = 0$, the above argument shows that there cannot exist a chain of prime ideals in R of positive length, so $\dim(R) \le 0$.

(c) We use induction on n, starting with the case $n = 0$. By part (b), $\dim(R) \le 0$ is equivalent to $U_a^{-1}R = \{0\}$ for all $a \in R$. This condition is equivalent to $0 \in U_a$, which means that there exist $m \in \mathbb{N}_0$ and $x \in R$ with $a^m(1 - xa) = 0$. This is equivalent to $a^m \in (a^{m+1})_R$, which is (6.5) for $n = 0$.

Now assume $n > 0$. By part (b), $\dim(R) \le n$ is equivalent to $\dim\left(U_a^{-1}R\right) \le n-1$ for all $a \in R$. By induction, this is equivalent to the following: For all $a_0, \ldots, a_{n-1} \in R$ and all $u_0, \ldots, u_{n-1} \in U_a$, there exist $m_0, \ldots, m_{n-1} \in \mathbb{N}_0$ such that

$$\prod_{i=0}^{n-1}\left(\frac{a_i}{u_i}\right)^{m_i} \in \left(\frac{a_j}{u_j} \cdot \prod_{i=0}^{j}\left(\frac{a_i}{u_i}\right)^{m_i} \,\middle|\, j = 0, \ldots, n-1\right)_{U_a^{-1}R}.$$

Multiplying generators of an ideal by invertible ring elements does not change the ideal. Since the $\varepsilon(u_i)$ are invertible in $U_a^{-1}R$, it follows that the above condition is independent of the u_i. In particular, the condition is equivalent to

$$\prod_{i=0}^{n-1}\varepsilon(a_i)^{m_i} \in \left(\varepsilon(a_j) \cdot \prod_{i=0}^{j}\varepsilon(a_i)^{m_i} \,\middle|\, j = 0, \ldots, n-1\right)_{U_a^{-1}R}.$$

By the definition of localization, this is equivalent to the existence of $m \in \mathbb{N}_0$ and $x \in R$ with

$$a^m(1 + xa) \cdot \prod_{i=0}^{n-1} a_i^{m_i} \in \left(a_j \cdot \prod_{i=0}^{j} a_i^{m_i} \,\middle|\, j = 0, \ldots, n-1\right)_R.$$

Writing a_n and m_n instead of a and m, we see that this condition is equivalent to (6.5).

7.4.

(a) Let $P \in \operatorname{Spec}(R)$ be a prime ideal containing $I := (x)_R$. For all nonnegative integers i we have $(xy^i)^2 = x \cdot xy^{2i} \in I$, so $xy^i \in P$. Therefore P contains the ideal $(x, xy, xy^2, \ldots)_R$, which is maximal. So

$$P = (x, xy, xy^2, \ldots)_R.$$

(b) The ideal

$$Q := (xy, xy^2, xy^3, \ldots)_R$$

is properly contained in P, and $R/Q \cong K[x]$, so Q is a prime ideal. The chain

$$\{0\} \subsetneqq Q \subsetneqq P$$

shows that $\mathrm{ht}(P) \geq 2$. But $\dim(R) \leq \mathrm{trdeg}(R) = 2$ by Theorem 5.5, so $\mathrm{ht}(P) = 2$.

(c) Let $S_n = K[x, y_1, \ldots, y_{n-1}]$ be a polynomial ring in n indeterminates (countably many for $n = \infty$), and set $R_n := K + S_n \cdot x$. As in (a), we see that $P = S_n \cdot x$ is the unique prime ideal of R_n containing $(x)_{R_n}$. For $0 \leq k < n$, we have prime ideals

$$Q_k := x \cdot (y_1, \ldots, y_k)_{S_n} = R \cap (y_1, \ldots, y_k)_{S_n} \in \mathrm{Spec}(R)$$

forming a strictly ascending chain. Since all Q_k are properly contained in P, we obtain $\mathrm{ht}(P) \geq n$, and equality follows by Theorem 5.5.

7.7. We first show that S is infinite-dimensional. For $i \in \mathbb{N}_0$, we have strictly ascending chains of prime ideals

$$Q_{i,j} = \left(x_{i^2+1}, \ldots, x_{i^2+j}\right)_R \subset R \quad (1 \leq j \leq 2i+1)$$

with $Q_{i,j} \cap U = \emptyset$. By Theorem 6.5, this corresponds to a chain of length $2i$ in $\mathrm{Spec}(S)$. It follows that $\dim(S) = \infty$.

For showing that S is Noetherian, we first remark that R_{P_i} is Noetherian for all $i \in \mathbb{N}_0$. Indeed, with $R_i := K[x_{(i+1)^2+1}, x_{(i+1)^2+2}, x_{(i+1)^2+3}, \ldots] \subseteq R$ we have $R_i \setminus \{0\} \subset R \setminus P_i$, so R_{P_i} is a localization of $\mathrm{Quot}(R_i)[x_1, \ldots, x_{(i+1)^2}]$. Therefore R_{P_i} is Noetherian by Corollaries 2.13 and 6.4. Now let $I \subseteq R$ be a nonzero ideal. Take $f \in I \setminus \{0\}$, and choose $n \in \mathbb{N}_0$ such that all indeterminates x_j occurring in f satisfy $j \leq (n+1)^2$. Since R_{P_i} is Noetherian, there exist $f_1, \ldots, f_m \in I$ such that

$$(I)_{R_{P_i}} = (f_1, \ldots, f_m)_{R_{P_i}} \quad \text{for} \quad 0 \leq i \leq n. \tag{S.7.1}$$

Take $g \in I$ and consider the ideal

$$J := \{h \in R \mid h \cdot g \in (f_1, \ldots, f_m, f)_R\} \subseteq R.$$

Clearly $f \in J$. By (S.7.1), for $0 \le i \le n$ there exists $h_i \in R \setminus P_i$ with $h_i \in J$. By Lemma 7.7, there exists $h \in J \setminus \cup_{i=0}^{n} P_i$. Assume that $J \subseteq \cup_{i \in \mathbb{N}_0} P_i$. Then there exists $i > n$ with $h \in P_i$. With φ_i: $R \to R$ the homomorphism sending $x_{i^2+1}, x_{i^2+2}, \ldots, x_{(i+1)^2}$ to 0 and fixing all other indeterminates, this means $\varphi_i(h) = 0$. The choice of n implies that $\varphi_i(f) = f$. Since $f + h \in J$, there exists $j \in \mathbb{N}_0$ with $f + h \in P_j$, so $\varphi_j(f + h) = 0$. We obtain

$$\varphi_j(h) = \varphi_j\left(f + h - \varphi_i(f + h)\right) = \varphi_j(f + h) - \varphi_i\left(\varphi_j(f + h)\right) = 0, \quad \text{(S.7.2)}$$

so $\varphi_j(f) = \varphi_j(f + h) - \varphi_j(h) = 0$. This implies $j \le n$. Since $h \in P_j$ by (S.7.2), this is a contradiction to the choice of h. We conclude that there exists $u \in J \setminus \cup_{i \in \mathbb{N}_0} P_i$. In other words, $u \in U$ and $ug \in (f_1, \ldots, f_m, f)_R$, so $g \in (f_1, \ldots, f_m, f)_S$. It follows that

$$(I)_S = (f_1, \ldots, f_m, f)_S\,.$$

Since every ideal $I' \subseteq S$ in S can be written as $I' = (I)_S$ with $I = R \cap I' \subseteq R$, we conclude that every ideal in S is finitely generated, so S is Noetherian.

8.7. Set $K := \operatorname{Quot}(R)$. For showing that $\widetilde{R[x]} \subseteq \widetilde{R}[x]$, let $f \in \operatorname{Quot}\left(R[x]\right) = K(x)$ be integral over $R[x]$, so

$$f^m = \sum_{i=1}^{m-1} g_i f^i \quad \text{with} \quad g_i \in R[x]. \quad \text{(S.8.1)}$$

Then f is integral over $K[x]$, so $f \in K[x]$ by Example 8.9(1). Therefore there exists $u \in R \setminus \{0\}$ with $uf^k \in R[x]$ for all $0 \le k < m$. In order to reduce to the case that R is Noetherian, we may substitute R by the subring generated by the coefficients of all uf^k $(0 \le k < m)$ and of all g_i from (S.8.1). By (S.8.1), $uf^k \in R[x]$ holds for all $k \ge 0$. If $a_n \in K$ is the highest coefficient of f, this implies $ua_n^k \in R$ for all k, so $R[a_n] \subseteq u^{-1}R$. By Theorem 2.10 (and using that R is Noetherian), this implies that $R[a_n]$ is finitely generated as an R-module, so $a_n \in \widetilde{R}$ by Lemma 8.3. This implies that $\widehat{f} := f - a_n x^n$ is integral over $R[x]$, so by induction on n we obtain $\widehat{f} \in \widetilde{R}[x]$. This completes the proof of $\widetilde{R[x]} \subseteq \widetilde{R}[x]$.

Conversely, let $f \in \widetilde{R}[x]$. Then all coefficients of f are integral over R and therefore also over $R[x]$, so f itself is integral over $R[x]$. This implies $f \in \widetilde{R[x]}$. The equivalence $R[x]$ normal $\Longleftrightarrow$ R normal is now clear.

8.11. Clearly $c_i - c_i(x) \in \mathfrak{m}$ for all i, so

$$I := (c_1 - c_1(x), \dots, c_n - c_n(x))_A \subseteq \mathfrak{m}.$$

By Corollary 8.24, $\operatorname{ht}(\mathfrak{m}) = \dim(A) = n$. So all we need to show is that $\mathfrak{m}_\mathfrak{m} \subseteq \sqrt{I_\mathfrak{m}}$.

A is integral over $K[c_1, \dots, c_n]$, so for every $a \in A$ there exist polynomials $g_1, \dots, g_m \in K[x_1, \dots, x_n]$ such that

$$a^m + g_1(c_1, \dots, c_n)\, a^{m-1} + \dots + g_{m-1}(c_1, \dots, c_n)\, a + g_m(c_1, \dots, c_n) = 0.$$

Computing modulo I and setting $\gamma_i := c_i(x) \in K$, this yields

$$a^m + g_1(\gamma_1, \dots, \gamma_n)\, a^{m-1} + \dots + g_{m-1}(\gamma_1, \dots, \gamma_n)\, a + g_m(\gamma_1, \dots, \gamma_n) \in I,$$

so A/I is algebraic. By Theorem 5.11, it follows that it is Artinian. The ideals $(\mathfrak{m}/I)^k \subseteq A/I$ form a descending chain, so there exists $k \in \mathbb{N}$ with $(\mathfrak{m}/I)^k = (\mathfrak{m}/I)^{k+1}$. Localizing at $\mathfrak{m}$, we obtain $M := (\mathfrak{m}_\mathfrak{m}/I_\mathfrak{m})^k = (\mathfrak{m}_\mathfrak{m}/I_\mathfrak{m})^{k+1}$. So M is a finitely generated $R_\mathfrak{m}$-module satisfying $\mathfrak{m}_\mathfrak{m} M = M$. Nakayama's lemma (Theorem 7.3) yields $M = \{0\}$, so $\mathfrak{m}_\mathfrak{m}^k \subseteq I_\mathfrak{m}$. This implies $\mathfrak{m}_\mathfrak{m} \subseteq \sqrt{I_\mathfrak{m}}$.

9.2.

(a) It is clear from the definition that $\mathcal{C}$ is closed under addition. From this, the result follows for $\alpha_i \in \mathbb{N}_{>0}$. Take $\mathbf{c} \in \mathbb{Z}^n$ such that $k\mathbf{c} = \mathbf{e} - \mathbf{f}$ with $k \in \mathbb{N}_{>0}$ and $\mathbf{e}, \mathbf{f} \in \mathbb{N}_0^n$ such that $\mathbf{f} < \mathbf{e}$. There exists $\mathbf{x} \in \mathbb{N}_0^n$ with $\mathbf{x} \equiv -\mathbf{e} \mod k$ (componentwise congruence), so also $\mathbf{x} \equiv -\mathbf{f} \mod k$ since $\mathbf{f} \equiv \mathbf{e} \mod k$. Set $\mathbf{e}' := (\mathbf{e}+\mathbf{x})/k$ and $\mathbf{f}' := (\mathbf{f}+\mathbf{x})/k$. Then $\mathbf{e}', \mathbf{f}' \in \mathbb{N}_0^n$, $\mathbf{e}' - \mathbf{f}' = \mathbf{c}$, and $k\mathbf{f}' < k\mathbf{e}'$ (where we used (3) from Definition 9.1(a)). If $\mathbf{e}' \le \mathbf{f}'$, then also $k\mathbf{e}' \le k\mathbf{f}'$ by induction on k (using (3) from Definition 9.1(a) again), a contradiction. By (1) from Definition 9.1(a), we conclude $\mathbf{f}' < \mathbf{e}'$ and so $\mathbf{c} \in \mathcal{C}$.
Since we already have the result for $\alpha_i \in \mathbb{N}_{>0}$, it follows for $\alpha_i \in \mathbb{Q}_{>0}$ from the above.
Now assume $\alpha_i \in \mathbb{R}_{>0}$ and $\mathbf{c}_i \in \mathcal{C}$ such that $\mathbf{c} := \sum_{i=1}^m \alpha_i \mathbf{c}_i \in \mathbb{Z}^n$. We will see that the α_i can be modified in such a way to make them rational. The set
$$L := \left\{ (\beta_1, \dots, \beta_m) \in \mathbb{R}^m \mid \sum_{i=1}^m \beta_i \mathbf{c}_i = \mathbf{c} \right\} \subseteq \mathbb{R}^m$$
is the solution set of an inhomogeneous system of linear equations with coefficients in $\mathbb{Q}$, so L is theimage of a map $\varphi\colon \mathbb{R}^l \to \mathbb{R}^m,\ (\gamma_1, \dots, \gamma_l) \mapsto$

$v_0 + \sum_{j=1}^{l} \gamma_j v_j$ with $v_0, \ldots, v_l \in \mathbb{Q}^m$. By hypothesis $(\alpha_1, \ldots, \alpha_m) \in \operatorname{im}(\varphi) \cap \mathbb{R}^m_{>0}$, so the preimage $U := \varphi^{-1}(\mathbb{R}^m_{>0}) \subseteq \mathbb{R}^l$ is nonempty. Since φ is continuous, U is open. It follows that there is a point $(\gamma_1, \ldots, \gamma_l) \in U \cap \mathbb{Q}^l$. So $(\alpha'_1, \ldots, \alpha'_m) := \varphi(\gamma_1, \ldots, \gamma_l) \in \mathbb{Q}^m \cap L \cap \mathbb{R}^m_{>0} = \mathbb{Q}^m_{>0} \cap L$, and therefore $\sum_{i=1}^m \alpha'_i \mathbf{c}_i = \mathbf{c}$. By what we have shown already, it follows that $\mathbf{c} \in \mathcal{C}$.

(b) It follows from (2) in Definition 9.1(a) that the standard basis vectors $\mathbf{e}_j \in \mathbb{R}^n$ lie in $\mathcal{C}$, so we may include them into the given list of $\mathbf{c}_i$. By definition, $\mathbf{0} \notin \mathcal{C}$, and so $\mathbf{0} \notin \mathcal{H}$ by part (a). (Notice that if some α_i are zero, this means that we are just considering fewer vectors $\mathbf{c}_i$.)
$\mathcal{H}$ is the image of the compact set

$$\mathcal{D} := \left\{(\alpha_1, \ldots, \alpha_m) \in \mathbb{R}^m_{\geq 0} \mid \alpha_1 + \cdots + \alpha_m = 1\right\}$$

under the map $\psi \colon \mathbb{R}^m \to \mathbb{R}^n$, $(\alpha_1, \ldots, \alpha_m) \mapsto \sum_{i=1}^m \alpha_i \mathbf{c}_i$. Also consider the map $\delta \colon \mathcal{D} \to \mathbb{R}_{\geq 0}$, $x \mapsto \langle \psi(x), \psi(x) \rangle$, where $\langle \cdot, \cdot \rangle$ denotes the Euclidean scalar product. With $d := \inf(\operatorname{im}(\delta))$, there exists a $\mathcal{D}$-valued sequence (x_k) such that $\delta(x_k)$ converges to d. By the Bolzano–Weierstrass theorem we may substitute (x_k) by a convergent subsequence. With $x = \lim_{k\to\infty} x_k \in \mathcal{D}$, the continuity of δ implies $\delta(x) = \lim_{k\to\infty} \delta(x_k) = d$. Setting, $\mathbf{w}' := \psi(x) \in \mathcal{H}$, we get $d = \langle \mathbf{w}', \mathbf{w}' \rangle$. Since $0 \notin \mathcal{H}$, this implies $d > 0$. We claim that $\langle \mathbf{w}', \mathbf{c} \rangle \geq d$ for all $\mathbf{c} \in \mathcal{H}$. Indeed, for all $\alpha \in \mathbb{R}$ with $0 \leq \alpha \leq 1$ we have $\mathbf{w}' + \alpha(\mathbf{c} - \mathbf{w}') \in \mathcal{H}$, so the definition of d implies

$$d \leq \langle \mathbf{w}' + \alpha(\mathbf{c} - \mathbf{w}'), \mathbf{w}' + \alpha(\mathbf{c} - \mathbf{w}') \rangle = d + 2\left(\langle \mathbf{w}', \mathbf{c} \rangle - d\right)\alpha + \langle \mathbf{c} - \mathbf{w}', \mathbf{c} - \mathbf{w}' \rangle \alpha^2.$$

Applying this with α small yields $\langle \mathbf{w}', \mathbf{c} \rangle \geq d$, so in particular $\langle \mathbf{w}', \mathbf{c}_i \rangle > 0$ for all i. So the preimage of $\mathbb{R}^m_{>0}$ under the map $\mathbb{R}^n \to \mathbb{R}^m$, $\mathbf{w} \to (\langle \mathbf{w}, \mathbf{c}_1 \rangle, \ldots, \langle \mathbf{w}, \mathbf{c}_m \rangle)$ is nonempty. Since the map is continuous, the preimage is open, and it follows that it contains points in $\mathbb{Q}^n$. So there exists $\mathbf{w} \in \mathbb{Q}^n$ with $\langle \mathbf{w}, \mathbf{c}_i \rangle > 0$ for all i. Multiplying $\mathbf{w}$ by a common denominator of the components, we may assume $\mathbf{w} \in \mathbb{Z}^n$. Since the standard basis vectors $\mathbf{e}_j$ are contained among the $\mathbf{c}_i$, it follows that $\mathbf{w} \in \mathbb{N}^n_{>0}$.

(c) Let $G = \{g_1, \ldots, g_r\}$. For $1 \leq i < j \leq r$ set $g_{i,j} := \operatorname{spol}(g_i, g_j)$. By Buchberger's criterion (Theorem 9.12), we have $g_{i,j} = \sum_{k=1}^r g_{i,j,k} \cdot g_k$ with $g_{i,j,k} \in K[x_1, \ldots, x_n]$ such that $\operatorname{LM}(g_{i,j,k} \cdot g_k) \leq \operatorname{LM}(g_{i,j})$. Let $M \subset K[x_1, \ldots, x_n]$ be the set of all g_i, $g_{i,j}$, and $g_{i,j,k}$. For a monomial $t = x_1^{e_1} \cdots x_n^{e_n}$, write $\mathbf{e}(t) := (e_1, \ldots, e_n)$. Observe that for $g \in K[x_1, \ldots, x_n]$ and $t \in \operatorname{Mon}(g)$ with $t \neq \operatorname{LM}(g)$, we have $\mathbf{e}(\operatorname{LM}(g)) - \mathbf{e}(t) \in \mathcal{C}$. Form the finite set

$$D := \Big\{\mathbf{e}\left(\operatorname{LM}(g)\right) - \mathbf{e}(t) \mid g \in M \text{ and } \operatorname{LM}(g) \neq t \in \operatorname{Mon}(g)\Big\} \subset \mathcal{C}.$$

By part (b) there exists $\mathbf{w} \in \mathbb{N}_{>0}^n$ such that $\langle \mathbf{w}, \mathbf{c} \rangle > 0$ for all $\mathbf{c} \in D$. By the definition of "$\leq_{\mathbf{w}}$" it follows that $\mathrm{LM}_{\leq_{\mathbf{w}}}(g) = \mathrm{LM}_{\leq}(g)$ for all $g \in M$. Here the subscripts indicate the monomial ordering that is used. This implies

$$\mathrm{spol}_{\leq_{\mathbf{w}}}(g_i, g_j) = \mathrm{spol}_{\leq}(g_i, g_j) = g_{i,j} = \sum_{k=1}^{r} g_{i,j,k} \cdot g_k$$

and $\mathrm{LM}_{\leq_{\mathbf{w}}}(g_{i,j,k} \cdot g_k) = \mathrm{LM}_{\leq}(g_{i,j,k} \cdot g_k) \leq \mathrm{LM}_{\leq}(g_{i,j}) = \mathrm{LM}_{\leq_{\mathbf{w}}}(g_{i,j})$. Applying Buchberger's criterion (Theorem 9.12) again yields that G is a Gröbner basis with respect to "$\leq_{\mathbf{w}}$". Moreover, we obtain

$$L_{\leq_{\mathbf{w}}}(I) = (\mathrm{LM}_{\leq_{\mathbf{w}}}(g_1), \ldots, \mathrm{LM}_{\leq_{\mathbf{w}}}(g_r)) = (\mathrm{LM}_{\leq}(g_1), \ldots, \mathrm{LM}_{\leq}(g_r)) = L_{\leq}(I).$$

10.3. By substituting R by its image in A, we may assume that $R \subseteq A$ is a subring. $\mathrm{Quot}(A)$ is finitely generated as a field extension of $\mathrm{Quot}(R)$, so the same is true for $\mathrm{Quot}(B)$. It follows that there exists a subalgebra $C \subseteq B$ such that $\mathrm{Quot}(C) = \mathrm{Quot}(B)$, and C is finitely generated. Since A is finitely generated as a C-algebra, Corollary 10.2 applies and yields an $a \in C \setminus \{0\}$ such that A_a is free as a module over C_a, and there exists a basis $\mathcal{M}$ with $1 \in \mathcal{M}$. We claim that $B_a = C_a$. The inclusion $C_a \subseteq B_a$ is clear. Conversely, for every $x \in B_a$ we have

$$x = \sum_{b \in \mathcal{M}} c_b \cdot b$$

with $c_b \in C_a$, and only finitely many c_b are nonzero. Since $\mathrm{Quot}(B) = \mathrm{Quot}(C)$, there exists $y \in C \setminus \{0\}$ such that $yx \in C$, so

$$yx \cdot 1 = \sum_{b \in \mathcal{M}} y c_b \cdot b.$$

The linear independence of $\mathcal{M}$ yields $c_b = 0$ for $b \neq 1$, so $x = c_1 \cdot 1 \in C_a$. We have shown that $B_a = C_a$. This completes the proof, since C_a is clearly finitely generated.

10.7. According to the hypothesis, we have $Y = \bigcup_{i=1}^m L_i$ with $L_i \subseteq X$ locally closed. Being a subset of a Noetherian space, the closure $\overline{Y}$ is Noetherian, too, so Theorem 3.11 yields

$$\overline{Y} = \bigcup_{j=1}^{n} Z_j$$

with Z_j the irreducible components, which are closed in X. Pick a Z_j and let Z_j^* be the union of all other components. Since

$$Z_j = Z_j \cap \overline{Y} = \bigcup_{i=1}^{m} \left(Z_j \cap \overline{L_i}\right),$$

there exists i with $Z_j \subseteq \overline{L_i}$. L_i is not a subset of Z_j^*, since otherwise $Z_j \subseteq Z_j^*$, so Z_j would be contained in a component other than itself. Write $L_i = C_i \cap U_i$ with C_i closed and U_i open, and form $U_j' := U_i \setminus Z_j^*$, which is also open. Then $L_i \not\subseteq Z_j^*$ and $L_i \subseteq \overline{Y} = Z_j \cup Z_j^*$ imply $U_j' \cap Z_j \neq \emptyset$. We have $Z_j = \overline{(U_j' \cap Z_j)} \cup \left(Z_j \setminus U_j'\right)$. With the irreducibility of Z_j, this yields

$$Z_j = \overline{U_j' \cap Z_j}.$$

Moreover,

$$U_j' \cap Z_j \subseteq U_i \cap Z_j \subseteq U_i \cap \overline{L_i} = L_i \subseteq Y.$$

Form the open set $U' := \bigcup_{j=1}^{n} U_j'$. Then

$$U := U' \cap \overline{Y} = \bigcup_{j=1}^{n} \left(U_j' \cap (Z_j \cup Z_j^*)\right) = \bigcup_{j=1}^{n} \left(U_j' \cap Z_j\right) \subseteq Y,$$

and

$$\overline{U} = \bigcup_{j=1}^{n} \overline{U_j' \cap Z_j} = \bigcup_{j=1}^{n} Z_j = \overline{Y}.$$

So U is a subset of Y that is open and dense in $\overline{Y}$.

10.9. Since X is a union of finitely many locally closed sets, it suffices to prove the result for the case that X itself is locally closed. So $X = \mathcal{V}_{\mathrm{Spec}(S)}(I) \setminus \mathcal{V}_{\mathrm{Spec}(S)}(J)$ with $I, J \subseteq S$ ideals. If $J = (a_1, \ldots, a_n)_S$, then X is the union of all $\mathcal{V}_{\mathrm{Spec}(S)}(I) \setminus \mathcal{V}_{\mathrm{Spec}(S)}(a_i)$. So we may assume

$$X := \mathcal{V}_{\mathrm{Spec}(S)}(I) \setminus \mathcal{V}_{\mathrm{Spec}(S)}(a) = \{Q \in \mathrm{Spec}(S) \mid I \subseteq Q \text{ and } a \notin Q\}$$

with $a \in S$. With ψ: $S \to S_a/I_a$ the canonical map, Lemma 1.22 and Theorem 6.5 yield $X = \psi^* \left(\mathrm{Spec}(S_a/I_a)\right)$. So

$$\varphi^*(X) = (\psi \circ \varphi)^* \left(\mathrm{Spec}(S_a/I_a)\right).$$

Observe that S_a is generated as an R-algebra by $\frac{1}{a}$ and the images of the generators of S, so S_a/I_a is finitely generated as an R-algebra, too. Applying Corollary 10.8 to $\psi \circ \varphi\colon R \to S_a/I_a$ shows that $\varphi^*(X)$ is constructible.

11.7. In order to avoid introducing a lot of additional notation, it is useful to choose and fix the weight vector $\mathbf{w} = (w_1, \dots, w_n) \in \mathbb{N}_{>0}^n$ throughout, and from now on write deg for $\deg_{\mathbf{w}}$. Everything in Definition 11.1 carries over to the weighted situation. (Notice that $\dim_K(A_{\leq d}) < \infty$ since all w_i are positive.) The formulas in Proposition 11.4 need to be modified as follows:

$$H_I(t) = \frac{1 - t^{\deg(f)}}{\prod_{i=0}^n (1 - t^{w_i})} \quad \text{if} \quad f \neq 0, \quad H_I(t) = \frac{1}{\prod_{i=0}^n (1 - t^{w_i})} \quad \text{if} \quad f = 0,$$

where we set $w_0 := 1$. The induction step in the proof works by using the direct sum decomposition

$$K[x_1, \dots, x_n]_{\leq d} = \bigoplus_{\substack{i,j \in \mathbb{N}_0, \\ i + w_n j = d}} K[x_1, \dots, x_{n-1}]_{\leq i} \cdot x_n^j,$$

which implies

$$H_n(t) = H_{n-1}(t) \cdot \Big(\sum_{j=0}^{\infty} t^{w_n j}\Big) = H_{n-1}(t) \cdot \frac{1}{1 - t^{w_n}} = \frac{1}{\prod_{i=0}^n (1 - t^{w_i})}.$$

The definition of a *weighted degree ordering* is straightforward, and Theorem 11.6 and its proof carry over word by word to the weighted situation. Ditto for the concept of homogeneity and Lemma 11.7. In Algorithm 11.8, the proof of Theorem 11.9, and Corollary 11.10, every occurrence of the denominator $(1 - t)^{n+1}$ should be replaced by $\prod_{i=0}^n (1 - t^{w_i})$. Obtaining an analogue of the Hilbert polynomial is a bit less straightforward. Write $w := \operatorname{lcm}\{w_1, \dots, w_n\}$. Since $\frac{1}{1-t^{w_i}} = \frac{1+t^{w_i}+t^{2w_i}+\cdots t^{w-w_i}}{1-t^w}$, the formula from the first part of Corollary 11.10 can be rewritten as

$$H_I(t) = \frac{a_0 + a_1 t + \cdots + a_k t^k}{(1 - t^w)^{n+1}}.$$

Since

$$\frac{1}{(1 - t^w)^{n+1}} = \sum_{d=0}^{\infty} \binom{d+n}{n} t^{wd} = \sum_{\substack{d \in \mathbb{N}_0, \\ d \equiv 0 \bmod w}} \binom{d/w + n}{n} t^d$$

we get

$$H_I(t) = \sum_{d=0}^{\infty} \sum_{\substack{0 \le i \le \min\{k,d\},\\ i \equiv d \bmod w}} a_i \binom{(d-i)/w + n}{n} t^d.$$

So if we define

$$p_{I,j} := \sum_{\substack{0 \le i \le k,\\ i \equiv j \bmod w}} a_i \binom{(x-i)/w + n}{n} \in \mathbb{Q}[x] \quad (j = 0, \dots, w-1),$$

we get $h_I(d) = p_{I,j}(d)$ for $d \ge k$ with $d \equiv j \mod w$. So instead of one Hilbert polynomial we obtain w polynomials to choose from according to the congruence class modulo w. We could substitute the degree of the Hilbert polynomial by the maximal degree of the $p_{I,j}$. Equivalently (and more conveniently), we define $\deg(h_I)$ to be the minimal k such that the Hilbert function is bounded above by a polynomial of degree k. With this, we get an analogue of Lemma 11.12, where $K[y_1, \dots, y_m]$ may be equipped with another weighted degree. The proof remains unchanged. Now consider the proof of Theorem 11.13. By the freedom of the choice of the weight vector in Lemma 11.12, we may equip $K[y_1, \dots, y_m, z_1, \dots, z_r]$ with the "standard" weight vector $(1, 1, \dots, 1)$. Therefore the proof of $\deg(p_J) = m$ remains valid, and we obtain the generalized form $\deg(h_I) = \dim(A)$ of Theorem 11.13. So Corollary 11.14 follows for "$\le$" a weighted degree ordering.

Finally, let "$\le$" be an arbitrary monomial ordering and $I \subseteq K[x_1, \dots, x_n]$ an ideal. By Exercise 9.2(c) there exists a weight vector $\mathbf{w} \in \mathbb{N}_{>0}^n$ such that $L_\le(I) = L_{\le_\mathbf{w}}(I)$. Clearly "$\le_\mathbf{w}$" is a weighted degree ordering, so with the generalized version of Corollary 11.14 we get

$$\dim\left(K[x_1, \dots, x_n]/I\right) = \dim\left(K[x_1, \dots, x_n]/L_\le(I)\right).$$

12.1. We keep Definition 11.1 except for the definition of the Hilbert series, which we omit. We omit Example 11.2 and Remark 11.3(a). The other parts of Remark 11.3 are optional. Remark 11.5 is replaced by the following

Lemma. *For the zero ideal* $\{0\} \subset K[x_1, \dots, x_n]$ *the formula*

$$h_{\{0\}}(d) = \binom{d+n}{n}$$

holds.

Proof. Since the Hilbert function of the zero ideal depends on the number n of indeterminates, we will write it in this proof as $h_n(d)$. We proceed by induction on n. For $n = 0$, $h_0(d) = 1$, so the formula is correct. For $n > 0$, we use the direct sum decomposition (11.1) on page 153, which implies

$$h_n(d) = \sum_{i=0}^{d} h_{n-1}(i) = \sum_{i=0}^{d} \binom{i+n-1}{n-1},$$

where induction was used for the second equality. We now show by induction on d that the latter sum equals $\binom{d+n}{n}$. This is correct for $d = 0$. For $d > 0$, we obtain

$$h_n(d) = \sum_{i=0}^{d} \binom{i+n-1}{n-1} = \binom{d+n-1}{n} + \binom{d+n-1}{n-1} = \binom{d+n}{n},$$

using a well-known identity of binomial coefficients in the last step. $\square$

The Lemma implies that the Hilbert function of an ideal $I \subseteq K[x_1, \ldots, x_n]$ is bounded above by a polynomial. So we can define $\delta(I) \in \mathbb{N}_0 \cup \{-1\}$ to be the smallest integer δ such that h_I can be bounded above by a polynomial in $\mathbb{Q}[x]$ of degree δ. We skip the rest of Section 11.1. We modify the assertion of Lemma 11.12 to $\delta(I) = \delta(J)$. The proof works for the modified assertion with a slight change of last two sentences. The assertion of Theorem 11.13 becomes $\delta(I) = \dim(A)$. In the proof of Theorem 11.13, we replace $\deg(p_I)$ and $\deg(p_J)$ by $\delta(I)$ and $\delta(J)$, and use the above Lemma instead of Remark 11.5. Otherwise, the proof needs no modification. We skip everything else from Section 11.2. So only the following material is required from Part III: The shortened Definition 11.1, the above Lemma, the definition of $\delta(I)$, and the modified versions of Lemma 11.12 and Theorem 11.13.

We make no change to Section 12.1, except using the above Lemma instead of Remark 11.5 in the proof of Lemma 12.4. In Section 12.2, we modify the assertion of Proposition 12.5 to: $\dim(\mathrm{gr}(R))$ *is the least degree of a polynomial providing an upper bound for* $\mathrm{length}\left(R/\mathfrak{m}^{d+1}\right)$. This follows from (12.5) and the modified Theorem 11.13. We omit the definition of the Hilbert–Samuel polynomial. The modified version of Proposition 12.5 and Lemma 12.4 yield (12.7). The next modification is to the proof of Lemma 12.7. We start with: "In order to use Proposition 12.5, we compare the Hilbert–Samuel functions $h_{R/Ra}$ and h_R." We replace the last sentence of the proof by: "From this, the lemma follows by Proposition 12.5." Finally, we delete the last sentence from Theorem 12.8. The proof of the theorem remains unchanged. Observe that the Hilbert–Samuel polynomial is not used anywhere outside Chapter 12 in the book.

12.5. The elements $c_i := \frac{x_i+I}{1} \in A_{\mathfrak{m}} =: R$ generate the maximal ideal $\mathfrak{m}_{\mathfrak{m}}$ of R. By Exercise 12.4 we have $R/\mathfrak{m}_{\mathfrak{m}} \cong A/\mathfrak{m} \cong K$. By the discussion before Proposition 12.5, $\mathrm{gr}(R)$ is generated as a K-algebra by the elements $a_i := c_i t + (\mathfrak{m}_{\mathfrak{m}})_{R^*}$, and the a_i are homogeneous of degree 1. Let J be the kernel of the map $K[x_1, \ldots, x_n] \to \mathrm{gr}(R)$, $x_i \mapsto a_i$. We are done if we can show that $J = I_{\mathrm{in}}$.

To prove that I_{in} is contained in J, take $f \in I \setminus \{0\}$ and write $\widehat{f} := f_{\mathrm{in}} - f$. So $f_{\mathrm{in}} \equiv \widehat{f} \mod I$, and every monomial in $\widehat{f}$ has degree larger than $\deg(f_{\mathrm{in}}) =: d$. Therefore

$$f_{\mathrm{in}}(c_1 t, \ldots, c_n t) = f_{\mathrm{in}}(c_1, \ldots, c_n) t^d = \widehat{f}(c_1, \ldots, c_n) t^d \in \mathfrak{m}_{\mathfrak{m}}^{d+1} t^d \subseteq (\mathfrak{m}_{\mathfrak{m}})_{R^*},$$

where the last inclusion follows from the definition of R^*. We conclude $f_{\mathrm{in}} \in J$, so $I_{\mathrm{in}} \subseteq J$.

For proving the reverse inclusion, take $f \in J$. Since J is a homogeneous ideal, we may assume that f is homogeneous of some degree d, and $f \neq 0$. We have $0 = f(a_1, \ldots, a_n) = f(c_1, \ldots, c_n) t^d + (\mathfrak{m}_{\mathfrak{m}})_{R^*}$, so $f(c_1, \ldots, c_n) \in \mathfrak{m}_{\mathfrak{m}}^{d+1}$ by the definition of R^*. This means that there exists $a \in A \setminus \mathfrak{m}$ such that $a \cdot (f + I) \in \mathfrak{m}^{d+1}$. We may write $a = h + I$ with $h \in K[x_1, \ldots, x_n]$, so $hf + I \in \mathfrak{m}^{d+1}$. This means that there exists $g \in \mathfrak{n}^{d+1}$ with $hf - g \in I$. From $a \notin \mathfrak{m}$ we conclude $h \notin \mathfrak{n}$, so $h(0) \neq 0$ and $(hf)_{\mathrm{in}} = h(0) \cdot f$. The condition $g \in \mathfrak{n}^{d+1}$ means that every monomial of g has degree $> d$, so by the above

$$(hf - g)_{\mathrm{in}} = h(0) \cdot f.$$

We conclude that $h(0) \cdot f \in I_{\mathrm{in}}$, so also $f \in I_{\mathrm{in}}$. This completes the proof.

13.6.

(a) Since the polynomial $x_2^2 - x_1^2(x_1 + 1) \in K[x_1, x_2]$ is irreducible, $K[X]$ is an integral domain. Therefore the same holds for its localization R.

(b) By Exercise 13.5(d) there exists $f = \sum_{i=0}^{\infty} a_i x_1^i \in K[[x_1]]$ with $f^2 = x_1 + 1$. For $k \in \mathbb{N}_0$, form the polynomials

$$A_k := x_2 - x_1 \sum_{i=0}^{k} a_i x_1^i \quad \text{and} \quad B_k := x_2 + x_1 \sum_{i=0}^{k} a_i x_1^i \in K[x_1, x_2].$$

Clearly (A_k) and (B_k) are Cauchy sequences with respect to the Krull topology given bythe filtration $I_n := \mathfrak{n}^n$ with $\mathfrak{n} := (x_1, x_2)$, and the product sequence $(A_k \cdot B_k)$ converges to $x_2^2 - x_1^2(x_1+1)$. Also observe that none of the A_k or B_k lie in $\mathfrak{n}^2$. Applying the canonical map $K[x_1, x_2] \to R$ to the A_k and B_k yields Cauchy sequences in R whose product converges to 0, and no element of these sequences lies in $\mathfrak{m}^2$, the square of the maximal ideal of R. The sequences have limits, A and B, in the completion $\widehat{R}$. A and B must be nonzero, since the A_k and B_k lie outside $\mathfrak{m}^2$. Since the limit of the product sequence is 0, it follows with Exercise 13.4(c) that $A \cdot B = 0$. So $\widehat{R}$ has zero divisors.

14.11. Since $R := K[X]$ is a Dedekind domain and $\bar{l} \neq 0$, $(\bar{l})$ is a finite product of maximal ideals. A maximal ideal $\mathfrak{m} \in \operatorname{Spec}_{\max}(R)$ occurs in this product if and only if $\bar{l} \in \mathfrak{m}$, i.e., if and only if $\mathfrak{m}$ corresponds to a point in the intersection $L \cap X$. So the $\mathfrak{m}_i$ are precisely the maximal ideals occurring in the product. The difficulty lies in the fact that some $\mathfrak{m}_i$ may coincide, so we have to get the multiplicities right. If ξ_i has multiplicity n_i as a zero of f, we need to show that $(\bar{l}) \in \mathfrak{m}_i^{n_i}$, but $(\bar{l}) \notin \mathfrak{m}_i^{n_i+1}$. Fix an i. By a change of coordinates, we may assume that

$$P_i = (0,0),\ L = \{(\xi, 0) \mid \xi \in K\},\ \xi_i = 0, \text{ and } l = x_2.$$

Then $g = x_2 \cdot h + f(x_1)$ with $h \in K[x_1, x_2]$ and $f \in K[t]$ as defined in the exercise. By definition, n_i is the maximal k such that x_1^k divides $f(x_1)$. With $\mathfrak{n} := (x_1, x_2) \in \operatorname{Spec}_{\max}(K[x_1, x_2])$ (so $\mathfrak{m}_i = \mathfrak{n}/(g)$), we need to show that n_i is the maximal k with

$$x_2 + (g) \in (\mathfrak{n}/(g))^k. \tag{S.14.1}$$

The condition (S.14.1) is equivalent to the existence of $u \in K[x_1, x_2]$ such that all monomials in $x_2 - ug$ have degree $\geq k$. First consider the case that $h(0,0) = 0$. Since X is nonsingular, it follows by the Jacobian criterion (Theorem 13.10) that $f'(0) \neq 0$, so $n_i = 1$. In this case, x_2 occurs as a monomial in $x_2 - ug = x_2(1 - uh) - uf(x_1)$ for every $u \in K[x_1, x_2]$, so the maximal k satisfying (S.14.1) is $1 = n_i$.

Now consider the case $h(0,0) \neq 0$. Then h is invertible as an element of the formal power series ring $K[[x_1, x_2]]$ (see Exercise 1.2(b)). In particular, there exists $u \in K[x_1, x_2]$ such that all monomials in $uh - 1$ have degree $\geq n_i$, so the same is true for $x_2 - ug = x_2(1 - uh) - uf(x_1)$. On the other hand, for every $u \in K[x_1, x_2]$, $x_2 - ug$ has monomials of degree $\leq n_i$, since x_2 occurs if $u(0,0) = 0$, and otherwise $x_1^{n_i}$ occurs. Therefore in this case the maximal k satisfying (S.14.1) is n_i again. This finishes the proof.

14.12.

(a) We have $L = K(\overline{x}_1, \overline{x}_2)$ with $\overline{x}_2^2 - \overline{x}_1^3 - a\overline{x}_1 - b = 0$, and $R = K[\overline{x}_1, \overline{x}_2]$. Let $\mathcal{O}$ be a place of L with maximal ideal $\mathfrak{p}$, and let ν: $L \to \mathbb{Z}$ be the corresponding discrete valuation. If ν were trivial on $K(\overline{x}_1)$, then $K(\overline{x}_1)$ would be contained in $\mathcal{O}$, so $\mathcal{O} = L$ since L is integral over $K(\overline{x}_1)$ and $\mathcal{O}$ is integrally closed in L. This contradiction shows that ν is nontrivial on $K(\overline{x}_1)$. Consider two cases.
(1) $\nu(\overline{x}_1) \geq 0$. Then by the results of Exercise 14.2, $K[\overline{x}_1] \subseteq \mathcal{O}$, and there exists $\xi_1 \in K$ such that $\overline{x}_1 - \xi_1 \in \mathfrak{p}$. We have $\overline{x}_2^2 \in \mathcal{O}$, so $\overline{x}_2 \in \mathcal{O}$ and hence $R \subseteq \mathcal{O}$. Choose $\xi_2 \in K$ with $\xi_2^2 = \xi_1^3 + a\xi_1 + b$. Then

$$(\overline{x}_2 - \xi_2)(\overline{x}_2 + \xi_2) = \overline{x}_1^3 + a\overline{x}_1 + b - \left(\xi_1^3 + a\xi_1 + b\right) \in \mathfrak{p},$$

so $\overline{x}_2 - \xi_2 \in \mathfrak{p}$ or $\overline{x}_2 + \xi_2 \in \mathfrak{p}$. By changing our choice of ξ_2, we may assume the first possibility. With $P := (\xi_1, \xi_2) \in E$, we get $\mathfrak{m}_P = (\overline{x}_1 - \xi_1, \overline{x}_2 - \xi_2)_R \subseteq \mathfrak{p}$, so $R \cap \mathfrak{p} = \mathfrak{m}_P$. This implies $R \setminus \mathfrak{m}_P \subseteq \mathcal{O} \setminus \mathfrak{p} = \mathcal{O}^\times$, so $R_P := R_{\mathfrak{m}_P} \subseteq \mathcal{O}$. But R_P is a place of L since E is nonsingular by Exercise 13.10. Therefore if R_P were strictly contained in $\mathcal{O}$, $\mathcal{O}$ would be equal to L. This contradiction shows that $\mathcal{O} = R_P$.
(2) $\nu(\overline{x}_1) < 0$. Then $\overline{y}_1 := 1/\overline{x}_1 \in \mathfrak{p}$. With $\overline{y}_2 := \overline{x}_1/\overline{x}_2$ we have the relation

$$\overline{y}_2^2 \cdot \left(1 + a\overline{y}_1^2 + b\overline{y}_1^3\right) = \overline{y}_1,$$

so $\overline{y}_2 \in \mathfrak{p}$. Therefore $S := K[\overline{y}_1, \overline{y}_2] \subseteq \mathcal{O}$, and $\mathfrak{m} := (\overline{y}_1, \overline{y}_2)_S \subseteq \mathfrak{p}$. Using the Jacobian criterion (Theorem 13.10), we conclude from the above relation that $S_{\mathfrak{m}}$ is regular. By the same argument as above, we obtain $\mathcal{O} = S_{\mathfrak{m}}$. So there exists exactly one place for which $\nu(\overline{x}_1) < 0$. We write this place as $\mathcal{O}_\infty$, and its maximal ideal as $\mathfrak{p}_\infty$.
We now show that $R \cap \mathfrak{p}_\infty = \{0\}$. It follows from the equation defining E that we have a K-automorphism φ of L mapping $\overline{x}_1$ to itself and $\overline{x}_2$ to $-\overline{x}_2$. If $f \in R$, then clearly $f \cdot \varphi(f) \in K[\overline{x}_1]$. Moreover, φ maps $\mathfrak{p}_\infty$ to itself, so if $f \in R \cap \mathfrak{p}_\infty$ we obtain

$$f \cdot \varphi(f) \in K[\overline{x}_1] \cap \mathfrak{p}_\infty = K[1/\overline{y}_1] \cap \mathfrak{p}_\infty = \{0\},$$

so $f = 0$.

(b) Let φ: $L \to L$ be as above. By the assumption on a and b, the polynomial $x_1^3 + ax_1 + b$ has three pairwise distinct zeros $\alpha_1, \alpha_2, \alpha_3 \in K$. With $P_i := (0, \alpha_i) \in E$, φ fixes the places $\mathcal{O}_{P_i}$. Looking at the results from (a), we see that φ also fixes $\mathcal{O}_\infty$.
Now we consider $K(x)$ and claim that for every K-automorphism ψ: $K(x) \to K(x)$ thereexist $\alpha, \beta, \gamma, \delta \in K$ with

$$\psi(x) = \frac{\alpha x + \beta}{\gamma x + \delta}.$$

(Notice that this gives an automorphism only if $\alpha\delta - \beta\gamma \neq 0$, but we do not need this here.) Indeed, if we write $\psi(x) = g/h$ with $g, h \in K[x]$ coprime, then $K(x) = K(g/h)$. We have $g(x) - \frac{g}{h} \cdot h(x) = 0$. With a new indeterminate t, the polynomial $g(x) - th(x) \in K[t, x]$ is irreducible, so it is also irreducible in $K(t)[x]$. Since g/h is transcendental over K, it follows that $g(x) - \frac{g}{h} \cdot h(x) = 0$ is a minimal equation for x over $K(g/h)$. So its degree must be one, and we get $g = \alpha x + \beta$ and $h = \gamma x + \delta$ as claimed. If $\psi = \mathrm{id}$, then ψ fixes infinitely many places. Which places are fixed if $\psi \neq \mathrm{id}$? The places of $K(x)$ are determined in Exercise 14.2. A place corresponding to a point $\xi \in K$ is fixed if and only if $\frac{\alpha\xi+\beta}{\gamma\xi+\delta} = \xi$, so at most two such places are fixed. In addition, the place corresponding to the point at infinity may be fixed, giving at most three fixed places. This concludes the proof of (b).

(c) If $(f)_R = \mathfrak{m}_P$, then $f \in R$, so $f \notin \mathfrak{p}_\infty$ by (a). On the other hand, if $(f)_R = \mathfrak{m}_P \cdot \mathfrak{m}_Q^{-1}$ and $f \in \mathfrak{p}_\infty$, then by interchanging P and Q and substituting f by f^{-1}, we also get $f \notin \mathfrak{p}_\infty$. (In fact, the latter case turns out to be impossible by the theory of divisors of projective curves.) So in both cases, $f \in \mathfrak{p}_P \setminus \mathfrak{p}_P^2$, and f does not lie in the maximal ideal of any place $\mathcal{O} \neq \mathcal{O}_P$ of L.

Since $f \notin K$, f is transcendental over K, so L is a finite field extension of $K(f)$. We are done if we can show that the degree $d := [L : K(f)]$ is one. Let A be the integral closure of $K[f]$ in L. By Lemma 8.27, A is finitely generated as a module over $K[f]$. Since A is torsion-free, the structure theorem for finitely generated modules over a principal ideal domain (see Lang [33, Chapter XV, Theorem 2.2]) tells us that A is free. Clearly A contains a basis of L over $K(f)$, and on the other hand no more than d elements of A can be linearly independent. So A is a free $K[f]$-module of rank d. This implies that $A/(f)_A$ has dimension d as a vector space over $K[f]/(f)_{K[f]} = K$.

From $f \in \mathfrak{p}_P$ it follows that $K[f] \subseteq \mathcal{O}_P$, so also $A \subseteq \mathcal{O}_P$ since $\mathcal{O}_P$ is integrally closed in L. Since $\mathcal{O}_P = R_P$, there is a map

$$\psi\colon A \to K,\ a \mapsto a(P),$$

which is clearly K-linear and surjective. We claim that $\ker(\psi) = (f)_A$. If we can prove this, then $A/(f)_A \cong K$, so $d = 1$, and we are done. Since $f \in \mathfrak{p}_P$, f lies in $\ker(\psi)$. Conversely, take $a \in \ker(\psi)$ and consider the quotient $b := a/f \in L$. We need to show that $b \in A$. This is true if $b \in A_\mathfrak{m}$ for every $\mathfrak{m} \in \mathrm{Spec}_{\max}(A)$, since then the ideal $\{c \in A \mid c \cdot b \in A\} \subseteq A$ is not contained in any maximal ideal. (One could also use Exercise 8.3 for this conclusion.)

So let $\mathfrak{m} \in \operatorname{Spec}_{\max}(A)$. Since A is a normal Noetherian domain of dimension 1, $A_\mathfrak{m}$ is a DVR. We also have $K \subseteq A_\mathfrak{m} \subseteq L$ and $L = \operatorname{Quot}(A_\mathfrak{m})$. Therefore $A_\mathfrak{m}$ is a place of L. If $A_\mathfrak{m} \neq \mathcal{O}_P$, then f does not lie in the maximal ideal of $A_\mathfrak{m}$, so $1/f \in A_\mathfrak{m}$. Since also $a \in A \subseteq A_\mathfrak{m}$, we get $b \in A_\mathfrak{m}$. On the other hand, if $A_\mathfrak{m} = \mathcal{O}_P$, then b lies in $A_\mathfrak{m}$ since $a \in \mathfrak{p}_P$ and $f \notin \mathfrak{p}_P^2$. So $b \in A_\mathfrak{m}$ for every $\mathfrak{m} \in \operatorname{Spec}_{\max}(A)$, and the proof is complete.

References

In the square brackets at the end of each reference we give the pages where the reference is cited.

1. William W. Adams, Phillippe Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics **3**, American Mathematical Society, Providence, 1994 [117].
2. Michael F. Atiyah, Ian Grant Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, 1969 [174].
3. Thomas Becker, Volker Weispfenning, *Gröbner Bases*, Springer, Berlin, 1993 [117, 118, 161].
4. David J. Benson, *Polynomial Invariants of Finite Groups*, Lond. Math. Soc. Lect. Note Ser. **190**, Cambridge University Press, Cambridge, 1993 [vii].
5. Wieb Bosma, John J. Cannon, Catherine Playoust, *The Magma algebra system I: The user language*, J. Symb. Comput. **24** (1997), 235–265 [127, 213].
6. Nicolas Bourbaki, *General Topology. Chapters 1–4*, Springer, Berlin, 1998 [2, 33].
7. Nicolas Bourbaki, *Algebra II, Chapters 4–7*, Elements of Mathematics, Springer, Berlin, 2003 [148].
8. Winfried Bruns, Jürgen Herzog, *Cohen-Macaulay Rings*, Cambridge University Press, Cambridge, 1993 [194].
9. Antonio Capani, Gianfranco Niesi, Lorenzo Robbiano, *CoCoA: A system for doing computations in commutative algebra*, available via anonymous ftp from `cocoa.dima.unige.it`, 2000 [126].
10. Luther Claborn, *Every abelian group is a class group*, Pacific J. Math. **18** (1966), 219–222 [210].
11. Thierry Coquand, Henri Lombardi, *A short proof for the Krull dimension of a polynomial ring*, Am. Math. Mon. **112** (2005), 826–829 [72].
12. David Cox, John Little, Donal O'Shea, *Ideals, Varieties, and Algorithms*, Springer, New York, 1992 [4, 117].
13. David Cox, John Little, Donal O'Shea, *Using Algebraic Geometry*, Springer, New York, 1998 [117].
14. Steven D. Cutkosky, *Resolution of Singularities*, vol. 63 of *Graduate Studies in Mathematics*, American Mathematical Society, Providence, 2004 [201].
15. Wolfram Decker, Christoph Lossen, *Computing in Algebraic Geometry. A quick start using SINGULAR*, vol. 16 of *Algorithms and Computation in Mathematics*, Springer, Berlin, 2006 [117].
16. Harm Derksen, Gregor Kemper, *Computing invariants of algebraic group actions in arbitrary characteristic*, Adv. Math. **217** (2008), 2089–2129 [118].

17. David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer, New York, 1995 [4, 15, 89, 117, 118, 160, 162, 171, 173–175, 184, 185, 194, 195, 199].
18. David Gale, *Subalgebras of an algebra with a single generator are finitely generated*, Proc. Am. Math. Soc. **8** (1957), 929–930.
19. Joachim von zur Gathen, Jürgen Gerhard, *Modern Computer Algebra*, Cambridge University Press, Cambridge, 1999 [127].
20. Robert Gilmer, *Multiplicative Ideal Theory*, Marcel Dekker, New York, 1972 [88, 213].
21. Daniel R. Grayson, Michael E. Stillman, *Macaulay 2, a software system for research in algebraic geometry*, available at `http://www.math.uiuc.edu/Macaulay2`, 1996 [126].
22. Gert-Martin Greuel, Gerhard Pfister, *A* **Singular** *Introduction to Commutative Algebra*, Springer, Berlin, 2002 [117, 160, 178].
23. Gert-Martin Greuel, Gerhard Pfister, Hannes Schönemann, *Singular version 1.2 user manual*, Reports On Computer Algebra **21**, Centre for Computer Algebra, University of Kaiserslautern, 1998, available at `http://www.mathematik.uni-kl.de/~zca/Singular` [127].
24. Paul R. Halmos, *Naive Set Theory*, Springer, New York, 1974 [11].
25. Joe Harris, *Algebraic Geometry. A First Course*, Springer, New York, 1992 [4].
26. Robin Hartshorne, *Algebraic Geometry*, Springer, New York, 1977 [4, 38, 205].
27. David Hilbert, *Über die vollen Invariantensysteme*, Math. Ann. **42** (1893), 313–370 [23].
28. Harry C. Hutchins, *Examples of commutative rings*, Polygonal Publishing House, Passaic, N.J., 1981 [107, 213].
29. Theo de Jong, *An algorithm for computing the integral closure*, J. Symb. Comput. **26** (1998), 273–277 [118].
30. Gregor Kemper, *The calculation of radical ideals in positive characteristic*, J. Symb. Comput. **34** (2002), 229–238 [118].
31. Martin Kreuzer, Lorenzo Robbiano, *Computational Commutative Algebra 1*, Springer, Berlin, 2000 [117].
32. Martin Kreuzer, Lorenzo Robbiano, *Computational Commutative Algebra 2*, Springer, Berlin, 2005 [117].
33. Serge Lang, *Algebra*, second edn., Addison-Wesley, Redwood City, 1984 [2, 9, 90, 101–103, 110, 171, 186–188, 199, 209, 216, 233].
34. Max D. Larsen, Paul J. McCarthy, *Multiplicative Theory of Ideals*, Academic, New York, 1971 [207].
35. Saunders Mac Lane, *Modular fields. I. Separating transcendence bases*, Duke Math. J. **5** (1939), 372–393 [186].
36. Ryutaroh Matsumoto, *Computing the radical of an ideal in positive characteristic*, J. Symb. Comput. **32** (2001), 263–271 [118].
37. Hideyuki Matsumura, *Commutative Algebra*, Mathematics Lecture Note Series **56**, Benjamin, Reading, 1980 [4, 107, 182, 184, 193].
38. Hideyuki Matsumura, *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics **8**, Cambridge University Press, Cambridge, 1986 [171, 174].
39. Ferdinando Mora, *An algorithm to compute the equations of tangent cones*, in: *Computer algebra (Marseille, 1982)*, Lecture Notes in Comput. Sci. **144**, pp. 158–165, Springer, Berlin 1982 [178].
40. Masayoshi Nagata, *On the closedness of singular loci*, Inst. Hautes Études Sci. Publ. Math. **1959** (1959), 29–36 [193].
41. Masayoshi Nagata, *Local Rings*, Wiley, New York, 1962 [89, 107, 110].
42. Jürgen Neukirch, *Algebraic Number Theory*, vol. 322 of *Grundlehren der Mathematischen Wissenschaften*, Springer, Berlin, 1999 [210].
43. Emmy Noether, *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p*, Nachr. Ges. Wiss. Göttingen (1926), 28–35 [111].

44. Vladimir L. Popov, Ernest B. Vinberg, *Invariant theory*, in: N.N. Parshin, I.R. Shafarevich, eds., *Algebraic Geometry IV*, Encyclopaedia of Mathematical Sciences **55**, Springer, Berlin, 1994 [145, 147].
45. J.L. Rabinowitsch, *Zum Hilbertschen Nullstellensatz*, Math. Ann. **102** (1930), 520–520 [12].
46. Igor R. Shafarevich, *Basic Algebraic Geometry*, Springer, Berlin, New York, 1974 [213].
47. Karen E. Smith, Lauri Kahanpää, Pekka Kekäläinen, William Traves, *An Invitation to Algebraic Geometry*, Springer, New York, 2000 [4].
48. Tonny A. Springer, *Invariant Theory*, Lecture Notes in Math. **585**, Springer, Berlin, 1977 [145].
49. Tonny A. Springer, *Aktionen reduktiver Gruppen auf Varietäten*, in: Hanspeter Kraft, Peter Slodowy, Tonny A. Springer, eds., *Algebraische Transformationsgruppen und Invariantentheorie, DMV Seminar* **13**, Birkhäuser, Basel 1987 [147].
50. Bernd Sturmfels, *Algorithms in Invariant Theory*, Springer, Wien, New York, 1993 [vii, 145].
51. Wolmer V. Vasconcelos, *Computational Methods in Commutative Algebra and Algebraic Geometry*, Algorithms and Computation in Mathematics **2**, Springer, Berlin, 1998 [117, 118].
52. Lawrence C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Discrete Mathematics and Its Applications, Chapman & Hall, Boca Raton, 2003 [212].

Notation

Index

Please note that a boldface page number indicates the page on which the word or phrase is defined.