Commutative Algebra: Problems and Solutions

Yankı Lekili

Problem 1. *Let R be a non-zero ring. Suppose that every ideal of R other than R itself is prime. Prove that R is a field.*

Solution. Since $R \neq \{0\}$, the zero ideal (0) is an ideal other than R, hence it is prime by hypothesis. Therefore R is an integral domain: if $xy = 0$ then $xy \in (0)$, so $x \in (0)$ or $y \in (0)$.

Now let $a \in R$ be a non-zero element. We show that a is a unit. Consider the ideal (a^2). There are two cases.

If $(a^2) = R$, then $1 \in (a^2)$, so $1 = ra^2 = (ra)a$ for some $r \in R$, and a is a unit.

If $(a^2) \neq R$, then (a^2) is prime by hypothesis. Since $a \cdot a = a^2 \in (a^2)$, primality gives $a \in (a^2)$, so $a = ra^2$ for some $r \in R$. Hence $a(1 - ra) = 0$. As R is an integral domain and $a \neq 0$, we get $1 - ra = 0$, that is, $ra = 1$, and again a is a unit.

Thus every non-zero element of R is invertible, and $R \neq \{0\}$, so R is a field. □

Problem 2. *Let R be a ring and let $\mathcal{J}(R)$ be its Jacobson radical, that is, the intersection of all maximal ideals of R. Show that $x \in \mathcal{J}(R)$ if and only if $1 - xy$ is a unit of R for all $y \in R$.*

Solution. We use the fact that every proper ideal of R is contained in a maximal ideal; this is where Zorn's lemma enters.

Suppose first that $x \in \mathcal{J}(R)$ and let $y \in R$. If $1 - xy$ were not a unit, then $(1 - xy)$ would be a proper ideal, hence contained in some maximal ideal $\mathfrak{m}$. Since $x \in \mathcal{J}(R) \subset \mathfrak{m}$, we have $xy \in \mathfrak{m}$, and therefore $1 = (1 - xy) + xy \in \mathfrak{m}$, contradicting the fact that $\mathfrak{m}$ is proper. Hence $1 - xy$ is a unit.

Conversely, suppose that $1 - xy$ is a unit for all $y \in R$, and suppose for contradiction that $x \notin \mathcal{J}(R)$. Then there is a maximal ideal $\mathfrak{m}$ with $x \notin \mathfrak{m}$. By maximality, $\mathfrak{m} + (x) = R$, so we can write $1 = m + xy$ with $m \in \mathfrak{m}$ and $y \in R$. But then $1 - xy = m \in \mathfrak{m}$ is a unit, which forces $\mathfrak{m} = R$, a contradiction. Hence $x \in \mathcal{J}(R)$. □

Problem 3. *Let R be a ring. Show that if a prime ideal $\mathfrak{p}$ of R can be written as $\mathfrak{p} = I \cap J$ for ideals I and J, then $\mathfrak{p} = I$ or $\mathfrak{p} = J$.*

Solution. Since $\mathfrak{p} = I \cap J$, we have $\mathfrak{p} \subset I$ and $\mathfrak{p} \subset J$. Suppose for contradiction that neither inclusion is an equality, and choose $a \in I \setminus \mathfrak{p}$ and $b \in J \setminus \mathfrak{p}$. Then $ab \in I$ because $a \in I$, and $ab \in J$ because $b \in J$, so $ab \in I \cap J = \mathfrak{p}$. As $\mathfrak{p}$ is prime, $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, contradicting the choice of a and b. Hence $\mathfrak{p} = I$ or $\mathfrak{p} = J$. □

Problem 4. *Let R be a ring. Recall that a multiplicative set $S \subset R$ is* **saturated** *if whenever $xy \in S$, both x and y are in S. Show that S is a saturated multiplicative set if and only if the complement $R \setminus S$ is a union of prime ideals.*

Solution. Suppose first that $R \setminus S = \bigcup_\lambda \mathfrak{p}_\lambda$ for some family of prime ideals $\mathfrak{p}_\lambda$. Since 1 lies in no proper ideal, $1 \in S$. If $x, y \in S$ and $xy \notin S$, then $xy \in \mathfrak{p}_\lambda$ for some λ, so $x \in \mathfrak{p}_\lambda$ or $y \in \mathfrak{p}_\lambda$ by primality; but $\mathfrak{p}_\lambda \subset R \setminus S$, a contradiction. Hence S is a multiplicative set. It is saturated: if $xy \in S$ and, say, $x \notin S$, then $x \in \mathfrak{p}_\lambda$ for some λ, hence $xy \in \mathfrak{p}_\lambda \subset R \setminus S$, a contradiction.

Conversely, suppose that S is a saturated multiplicative set. We claim that every $x \in R \setminus S$ lies in a prime ideal disjoint from S; since every such prime ideal is contained in $R \setminus S$, this shows that $R \setminus S$ is the union of the prime ideals disjoint from S. So let $x \notin S$. The ideal (x) is disjoint from S: if $rx \in S$ for some $r \in R$, then $x \in S$ by saturation, which is not the case. By Krull's lemma from the lectures (whose proof uses Zorn's lemma), there exists a prime ideal $\mathfrak{p}$ containing (x) and disjoint from S. Thus $x \in \mathfrak{p} \subset R \setminus S$, as claimed. □

Problem 5. *Show that the ring of Gaussian integers $\mathbb{Z}[i]$ is a Euclidean domain with respect to the norm $N(a + bi) = a^2 + b^2$. (Use the fact that the open disks of radius 1 centred at the Gaussian integers cover the whole complex plane.)*

Solution. For $z = a + bi \in \mathbb{Z}[i]$ we have $N(z) = a^2 + b^2 = |z|^2$, where $|z|$ denotes the usual absolute value of the complex number z. In particular N takes values in $\mathbb{N}$, $N(z) = 0$ only for $z = 0$, and $N(zw) = N(z)N(w)$ since $|zw| = |z||w|$. Also, $\mathbb{Z}[i]$ is an integral domain, being a subring of the field $\mathbb{C}$.

Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. We must find $q, r \in \mathbb{Z}[i]$ with $\alpha = q\beta + r$ and $N(r) < N(\beta)$. Consider the complex number $\alpha/\beta = u + vi$ with $u, v \in \mathbb{Q}$. Choose integers m, n with $|u - m| \leq \frac{1}{2}$ and $|v - n| \leq \frac{1}{2}$, and put $q = m + ni \in \mathbb{Z}[i]$. Then

$$\left|\frac{\alpha}{\beta} - q\right|^2 = (u - m)^2 + (v - n)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1.$$

This is the geometric fact in the hint: every complex number lies at distance less than 1 from some Gaussian integer. Now set $r = \alpha - q\beta \in \mathbb{Z}[i]$. Then

$$N(r) = |\alpha - q\beta|^2 = |\beta|^2 \left|\frac{\alpha}{\beta} - q\right|^2 \leq \frac{1}{2} N(\beta) < N(\beta),$$

as required. □

Problem 6. *Let k be an infinite field, and $f \in k[X_1, \ldots, X_n]$. Show that $f = 0$ if and only if $f(x_1, \ldots, x_n) = 0$ for all $(x_1, \ldots, x_n) \in k^n$. Give a counter-example to the statement when $k = \mathbb{F}_2$, the field with two elements.*

Solution. If $f = 0$ then clearly f vanishes at every point of k^n. For the converse we argue by induction on n.

For $n = 1$, a non-zero polynomial $f \in k[X_1]$ of degree d has at most d roots in k. Since k is infinite, a polynomial vanishing at every point of k must therefore be zero.

Now let $n > 1$ and suppose that f vanishes at every point of k^n. Write f as a polynomial in X_n with coefficients in $k[X_1, \ldots, X_{n-1}]$:

$$f = \sum_{j=0}^{d} g_j(X_1, \ldots, X_{n-1}) X_n^j.$$

Fix a point $(x_1, \ldots, x_{n-1}) \in k^{n-1}$. The one-variable polynomial

$$f(x_1, \ldots, x_{n-1}, X_n) = \sum_{j=0}^{d} g_j(x_1, \ldots, x_{n-1}) X_n^j \in k[X_n]$$

vanishes at every $x_n \in k$, so by the case $n = 1$ it is the zero polynomial, that is, $g_j(x_1, \ldots, x_{n-1}) = 0$ for all j. As this holds for every point of k^{n-1}, the induction hypothesis gives $g_j = 0$ for all j, hence $f = 0$.

For $k = \mathbb{F}_2$, the polynomial $f = X_1^2 - X_1 \in \mathbb{F}_2[X_1, \ldots, X_n]$ is non-zero, but $f(x_1, \ldots, x_n) = x_1^2 - x_1 = 0$ for every point of $\mathbb{F}_2^n$, since $0^2 = 0$ and $1^2 = 1$. (More generally, $X_1^q - X_1$ vanishes on $\mathbb{F}_q^n$ for any finite field $\mathbb{F}_q$.) □

Problem 7. *Let $\mathfrak{p} \subset \mathbb{Z}[X]$ be a prime ideal. Show that $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. Thus, $\mathfrak{p} \cap \mathbb{Z} = (p)$ where $p = 0$ or p is a prime number. Suppose now that $\mathfrak{p} \neq (0)$.*

(i) Suppose $\mathfrak{p} \cap \mathbb{Z} = \{0\}$. Show that $\mathfrak{p} = (f)$ where $f \in \mathbb{Z}[X]$ is an irreducible polynomial.

(ii) Suppose $\mathfrak{p} \cap \mathbb{Z} = (p)$ with p a prime number. Show that $\mathfrak{p} = (p, f)$ where $f = 0$ or $f \in \mathbb{Z}[X]$ is a monic polynomial (leading coefficient is one) whose mod p reduction $\overline{f} \in \mathbb{F}_p[X]$ is irreducible.

Solution. The inclusion $\iota : \mathbb{Z} \to \mathbb{Z}[X]$ is a ring homomorphism and $\mathfrak{p} \cap \mathbb{Z} = \iota^{-1}(\mathfrak{p})$. The preimage of a prime ideal under a ring homomorphism is prime (Lecture 2), so $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. The prime ideals of $\mathbb{Z}$ are (0) and (p) for p a prime number, which gives the second claim.

(i) Suppose $\mathfrak{p} \cap \mathbb{Z} = \{0\}$ and $\mathfrak{p} \neq (0)$. Recall that the **content** of a non-zero polynomial in $\mathbb{Z}[X]$ is the greatest common divisor of its coefficients, that a polynomial is **primitive** if its content is 1, and Gauss's lemma: the content of a product is the product of the contents. In particular, if f is primitive and f divides dg in $\mathbb{Z}[X]$ for some non-zero $d \in \mathbb{Z}$, then f divides g: writing $dg = qf$, the content of q equals the content of $qf = dg$, which is divisible by d, so $q = dq'$ with $q' \in \mathbb{Z}[X]$ and $g = q'f$.

Choose a non-zero $f \in \mathfrak{p}$ of smallest possible degree. Writing $f = cf_0$ with $c \in \mathbb{Z}$ the content of f and f_0 primitive, we have $c \notin \mathfrak{p}$ (as $\mathfrak{p} \cap \mathbb{Z} = \{0\}$ and $c \neq 0$), so $f_0 \in \mathfrak{p}$ by primality. Replacing f by f_0, we may assume that f is primitive. We claim that $\mathfrak{p} = (f)$. Let $g \in \mathfrak{p}$. Dividing g by f in $\mathbb{Q}[X]$ and clearing denominators, we find a non-zero $d \in \mathbb{Z}$ and $q, r \in \mathbb{Z}[X]$ with

$$dg = qf + r, \qquad r = 0 \text{ or } \deg r < \deg f.$$

Since $r = dg - qf \in \mathfrak{p}$, the minimality of $\deg f$ forces $r = 0$. Thus f divides dg, and by the consequence of Gauss's lemma above, f divides g in $\mathbb{Z}[X]$. Hence $\mathfrak{p} = (f)$. Finally, f is irreducible: it is non-zero and not a unit, and if $f = gh$ then $g \in \mathfrak{p}$ or $h \in \mathfrak{p}$, say $g = fu$ with $u \in \mathbb{Z}[X]$; then $f = fuh$, so $uh = 1$ and h is a unit.

(ii) Suppose $\mathfrak{p} \cap \mathbb{Z} = (p)$ with p a prime number. Then $(p) \subset \mathfrak{p}$. Let $\pi : \mathbb{Z}[X] \to \mathbb{Z}[X]/(p) \simeq \mathbb{F}_p[X]$ be the reduction mod p, and write $\overline{g} = \pi(g)$. The ideals of $\mathbb{F}_p[X]$ correspond to the ideals of $\mathbb{Z}[X]$ containing (p), and under this correspondence $\mathfrak{p}$ corresponds to $\overline{\mathfrak{p}} = \pi(\mathfrak{p})$, which is a prime ideal since $\mathbb{F}_p[X]/\overline{\mathfrak{p}} \simeq \mathbb{Z}[X]/\mathfrak{p}$ is an integral domain. As $\mathbb{F}_p[X]$ is a PID, $\overline{\mathfrak{p}} = (\overline{f})$ where $\overline{f} = 0$ or $\overline{f}$ is an irreducible polynomial, which we may take to be monic after multiplying by a unit. Let $f \in \mathbb{Z}[X]$ be 0 if $\overline{f} = 0$, and otherwise a monic polynomial lifting $\overline{f}$ (lift each coefficient to an integer, taking the leading coefficient to be 1). Then for $g \in \mathbb{Z}[X]$ we have

$$\begin{aligned} g \in \mathfrak{p} &\iff \overline{g} \in (\overline{f}) \\ &\iff \overline{g} = \overline{h}\,\overline{f} \text{ for some } h \in \mathbb{Z}[X] \\ &\iff g - hf \in (p) \text{ for some } h \in \mathbb{Z}[X] \\ &\iff g \in (p, f), \end{aligned}$$

so $\mathfrak{p} = (p, f)$ as required. □

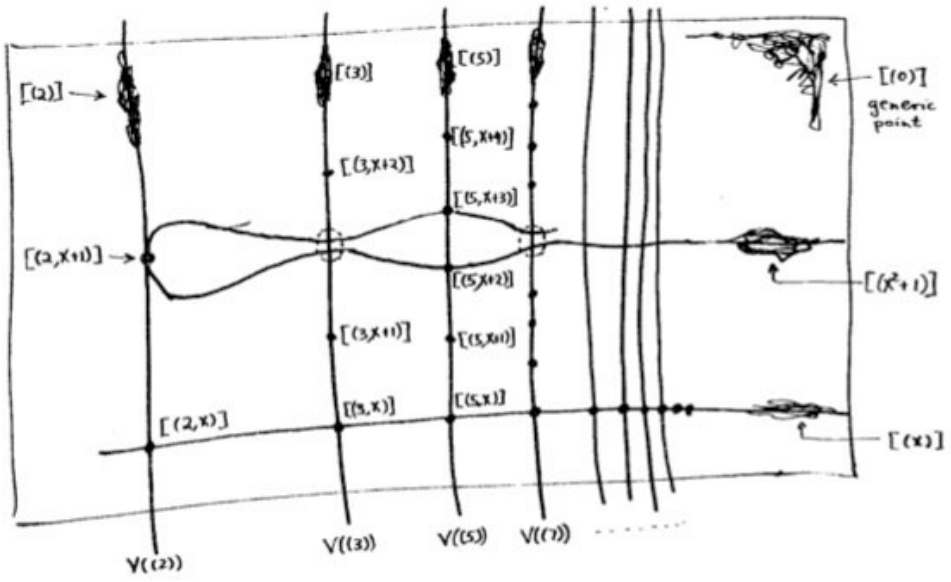

Figure 1: Mumford's picture of $\operatorname{Spec}\mathbb{Z}[X]$, from his *Red Book of Varieties and Schemes*.

Problem 8. *In a ring R, let I be an ideal which is maximal among the non-principal ideals of R, that is, I is not principal and every ideal strictly containing I is principal. Prove that I is prime.*

Solution. First, I is a proper ideal, since $R = (1)$ is principal. Suppose for contradiction that I is not prime, so that there exist $a, b \in R \setminus I$ with $ab \in I$.

The ideal $I + (a)$ strictly contains I because $a \notin I$, so by maximality it is principal: $I + (a) = (c)$ for some $c \in R$. Consider the ideal

$$J \coloneqq (I : c) = \{r \in R : rc \in I\}.$$

We have $I \subset J$, since I is an ideal. Moreover $b \in J$: writing $c = x + ta$ with $x \in I$ and $t \in R$, we get $bc = bx + t(ab) \in I$. As $b \notin I$, the ideal J strictly contains I, so it is principal: $J = (d)$ for some $d \in R$.

We claim that $I = (cd)$. On the one hand, $d \in J$ means $cd \in I$, so $(cd) \subset I$. On the other hand, let $y \in I$. Since $I \subset I + (a) = (c)$, we can write $y = rc$ with $r \in R$; then $rc \in I$ says $r \in J = (d)$, so $r = sd$ for some $s \in R$ and $y = s\,cd \in (cd)$. Hence $I = (cd)$ is principal, contradicting the hypothesis. Therefore I is prime. □

Problem 9. *Show that in a local ring R with maximal ideal $\mathfrak{m}$, the units of R are precisely the elements of $R \setminus \mathfrak{m}$. Conversely, show that a ring R whose non-units form an ideal is a local ring.*

Solution. Let R be a local ring with unique maximal ideal $\mathfrak{m}$. A unit lies in no proper ideal, since an ideal containing a unit contains 1; hence every unit lies in $R \setminus \mathfrak{m}$. Conversely, let $x \in R \setminus \mathfrak{m}$ and suppose that x is not a unit. Then (x) is a proper ideal, so it is contained in some maximal ideal of R (this uses Zorn's lemma, through the proposition of Lecture 2 that every proper ideal lies in a maximal ideal). Since $\mathfrak{m}$ is the only maximal ideal, $x \in (x) \subset \mathfrak{m}$, a contradiction. Thus the units are exactly the elements of $R \setminus \mathfrak{m}$.

Now let R be a ring whose set N of non-units is an ideal. Then N is a proper ideal, as $1 \notin N$. Every proper ideal of R consists of non-units, by the remark above, and is therefore contained in N. It follows that N is a maximal ideal: an ideal strictly containing N is not contained in N, so it is not proper, that is, it equals R. It also follows that N is the only maximal ideal: a maximal ideal is proper, hence contained in N, and then equal to N by maximality. Therefore R is a local ring with maximal ideal N. □

Problem 10. *Give an example of a ring R and ideals I, J of R such that $I \cup J$ is not an ideal. In your example, what is the smallest ideal containing $I \cup J$?*

Solution. Take $R = \mathbb{Z}$, $I = (2)$ and $J = (3)$. Then $2 \in I \cup J$ and $3 \in I \cup J$, but $2 + 3 = 5$ is divisible by neither 2 nor 3, so $5 \notin I \cup J$. Hence $I \cup J$ is not closed under addition and is not an ideal.

The smallest ideal containing $I \cup J$ is $I + J = (2) + (3) = (2, 3)$. Since $1 = 3 - 2 \in (2, 3)$, this is the whole ring $\mathbb{Z}$. More generally, for any ideals I, J of a ring R the smallest ideal containing

$I \cup J$ is $I + J$: it is an ideal containing I and J, and any ideal containing $I \cup J$ is closed under addition, so it contains every sum $a + b$ with $a \in I$, $b \in J$.

In fact, for any ring the union $I \cup J$ is an ideal only when $I \subset J$ or $J \subset I$, in which case $I \cup J$ is the larger of the two. Indeed, if $a \in I \setminus J$ and $b \in J \setminus I$, then $a + b \notin I$ (otherwise $b = (a + b) - a \in I$) and similarly $a + b \notin J$, so $a + b \notin I \cup J$. □

Problem 11. *Let R be a ring. Show that the nilradical and the Jacobson radical of $R[X]$ coincide.*

Solution. Write $\mathcal{N}$ and $\mathcal{J}$ for the nilradical and the Jacobson radical of $R[X]$. Since every maximal ideal is prime, $\mathcal{N}$, the intersection of all prime ideals of $R[X]$, is contained in $\mathcal{J}$, the intersection of all maximal ideals. It remains to show that $\mathcal{J} \subset \mathcal{N}$.

Let $f = a_0 + a_1X + \cdots + a_nX^n \in \mathcal{J}$. By Problem 2 applied with $y = X$, the polynomial $1 - fX$ is a unit of $R[X]$. Let $\mathfrak{p}$ be any prime ideal of R and reduce modulo $\mathfrak{p}$: the image of $1 - fX$ in $(R/\mathfrak{p})[X]$ is a unit, being the image of a unit under the ring homomorphism $R[X] \to (R/\mathfrak{p})[X]$. Now $R/\mathfrak{p}$ is an integral domain, so degrees add under multiplication in $(R/\mathfrak{p})[X]$ and a unit must have degree 0. Hence the image of fX in $(R/\mathfrak{p})[X]$ is 0, that is, $a_0, a_1, \ldots, a_n \in \mathfrak{p}$. As $\mathfrak{p}$ was arbitrary, each a_i lies in the intersection of all prime ideals of R, which is the nilradical $\mathcal{N}(R)$. So each a_i is nilpotent in R, hence each a_iX^i is nilpotent in $R[X]$, and f is a sum of nilpotent elements, hence nilpotent, since the nilradical of $R[X]$ is an ideal. Therefore $f \in \mathcal{N}$.

In fact the argument shows more: $\mathcal{J} = \mathcal{N} = \mathcal{N}(R)[X]$, the polynomials all of whose coefficients are nilpotent in R. □

Problem 12. *Prove that if R is Noetherian, then the power series ring $R[[T]]$ is also Noetherian.*

Solution. We adapt the proof of the Hilbert basis theorem (Theorem 4.1 of the notes), replacing leading coefficients by lowest-order coefficients. For a non-zero $f = \sum_{i \geq 0} c_iT^i \in R[[T]]$ write $\operatorname{ord}(f)$ for the smallest i with $c_i \neq 0$, and set $\operatorname{ord}(0) = \infty$.

Let $I \subset R[[T]]$ be an ideal. For $n \geq 0$ define

$$J_n = \{a \in R : \exists f \in I \text{ of the form } f = aT^n + c_{n+1}T^{n+1} + c_{n+2}T^{n+2} + \ldots\}.$$

As in the proof of Theorem 4.1, J_n is an ideal of R (if $a, a' \in J_n$ come from $f, f' \in I$ and $r \in R$, then $a + a'$ and ra come from $f + f'$ and rf), and $J_n \subset J_{n+1}$ since $f \in I$ implies $Tf \in I$. Since R is Noetherian, the chain $J_0 \subset J_1 \subset \ldots$ stabilises: there is s with $J_s = J_{s+i}$ for all $i \geq 0$. For each $m \leq s$ write $J_m = (a_{m,1}, \ldots, a_{m,r_m})$ and choose $f_{m,j} \in I$ of the form $a_{m,j}T^m + (\text{terms of order} > m)$. Let $I' \subset I$ be the ideal generated by the finitely many $f_{m,j}$. We claim that $I = I'$.

Let $f \in I$. First, we show that there is $g \in I'$ with $\operatorname{ord}(f - g) \geq s$. If $\operatorname{ord}(f) = m < s$ with lowest coefficient a, then $a \in J_m$, so $a = \sum_i b_i a_{m,i}$ with $b_i \in R$, and $f - \sum_i b_i f_{m,i} \in I$ has order $> m$. Repeating this at most s times gives the required g.

So it remains to show that every $h \in I$ with $\operatorname{ord}(h) \geq s$ lies in I'. In the polynomial case the analogous step was an induction on the degree, which terminates. Here the order can only be pushed up indefinitely, so we construct the coefficients of a solution step by step. Put $h_0 = h$. Suppose $h_n \in I$ with $\operatorname{ord}(h_n) \geq s+n$ has been constructed, and let c_n be its coefficient of T^{s+n}. Then $c_n \in J_{s+n} = J_s$, so we can write $c_n = \sum_i b_i^{(n)} a_{s,i}$ with $b_i^{(n)} \in R$, and we set

$$h_{n+1} = h_n - \sum_{i=1}^{r_s} b_i^{(n)} T^n f_{s,i} \in I,$$

which has order $\geq s+n+1$. Now define the power series $g_i = \sum_{n \geq 0} b_i^{(n)} T^n \in R[[T]]$ for $1 \leq i \leq r_s$. For every $N \geq 0$ we have

$$h - \sum_{i=1}^{r_s} g_i f_{s,i} = h_{N+1} - \sum_{i=1}^{r_s} \Big(\sum_{n>N} b_i^{(n)} T^n \Big) f_{s,i},$$

and both terms on the right have order $\geq s+N+1$. Hence every coefficient of $h - \sum_i g_i f_{s,i}$ vanishes, that is, $h = \sum_i g_i f_{s,i} \in I'$. Therefore $f = g + (f-g) \in I'$, and $I = I'$ is finitely generated. □

Problem 13. *Let k be a field. For $S \subset k[X_1, \ldots, X_n]$ and $U \subset k^n$ let $\mathcal{V}(S) \subset k^n$ and $\mathcal{I}(U) \subset k[X_1, \ldots, X_n]$ be as in Lecture 5. Show that $S_1 \subset S_2$ implies $\mathcal{V}(S_2) \subset \mathcal{V}(S_1)$, and $U_1 \subset U_2$ implies $\mathcal{I}(U_2) \subset \mathcal{I}(U_1)$. Use the set $U = \{(0,i) : i \in \mathbb{Z}\} \subset \mathbb{C}^2$ to show that it can happen that $U_1 \subsetneq U_2$ but $\mathcal{I}(U_1) = \mathcal{I}(U_2)$.*

Solution. Let $x \in \mathcal{V}(S_2)$, so $f(x) = 0$ for all $f \in S_2$. In particular $f(x) = 0$ for all $f \in S_1 \subset S_2$, that is, $x \in \mathcal{V}(S_1)$. Similarly, let $f \in \mathcal{I}(U_2)$, so f vanishes at every point of U_2. In particular f vanishes at every point of $U_1 \subset U_2$, that is, $f \in \mathcal{I}(U_1)$.

Now let $U_1 = U = \{(0,i) : i \in \mathbb{Z}\}$ and let $U_2 = \mathcal{V}(X) = \{(0,y) : y \in \mathbb{C}\}$ be the Y-axis in $\mathbb{C}^2$. Then $U_1 \subsetneq U_2$, since for example $(0, \frac{1}{2}) \in U_2 \setminus U_1$. We claim that $\mathcal{I}(U_1) = \mathcal{I}(U_2) = (X)$.

First, X vanishes on U_2, so $(X) \subset \mathcal{I}(U_2)$, and $\mathcal{I}(U_2) \subset \mathcal{I}(U_1)$ by the first part. It remains to show that $\mathcal{I}(U_1) \subset (X)$. Let $f \in \mathcal{I}(U_1)$. Collecting the terms of f that involve X, we can write $f = Xg(X,Y) + h(Y)$ with $g \in \mathbb{C}[X,Y]$ and $h(Y) = f(0,Y) \in \mathbb{C}[Y]$. For every $i \in \mathbb{Z}$ we have $0 = f(0,i) = h(i)$, so the one-variable polynomial h has infinitely many roots and must be 0. Hence $f = Xg \in (X)$, as required.

Note that $\mathcal{V}(\mathcal{I}(U_1)) = \mathcal{V}(X) = U_2$: the Y-axis is the Zariski closure of the set U_1 of integer points on it. □

Problem 14. *Let k be a field and let $R \subset k[X,Y]$ be the set of polynomials $f = \sum a_{ij} X^i Y^j$ with $a_{0j} = 0$ for all $j > 0$, that is, polynomials having no term of the form aY^j with $j > 0$. Show that R is a subring of the Noetherian ring $k[X,Y]$, but that R is not Noetherian.*

Solution. A polynomial $f \in k[X,Y]$ lies in R if and only if $f(0,Y) \in k$, that is, if and only if $f(0,Y) = f(0,0)$. Since $f \mapsto f(0,Y)$ is a ring homomorphism $k[X,Y] \to k[Y]$, we have $(f \pm g)(0,Y) = f(0,Y) \pm g(0,Y)$ and $(fg)(0,Y) = f(0,Y)g(0,Y)$, so R is closed under addition, subtraction and multiplication, and it contains 0 and 1. Hence R is a subring. Note that $R = k + Xk[X,Y]$, and that R is generated as a k-algebra by $X, XY, XY^2, \ldots$, since $X^iY^j = X^{i-1} \cdot XY^j$ for $i > 0$.

To see that R is not Noetherian, consider the ideals

$$I_N = (X, XY, XY^2, \ldots, XY^N) \subset R, \qquad N \geq 0.$$

Clearly $I_0 \subset I_1 \subset I_2 \subset \ldots$, and we claim that each inclusion is strict, so that R does not satisfy the ascending chain condition. Suppose that $XY^{N+1} \in I_N$, say

$$XY^{N+1} = \sum_{j=0}^{N} g_j \, XY^j$$

with $g_j \in R$. Cancelling X, which is allowed since $k[X,Y]$ is an integral domain, gives $Y^{N+1} = \sum_{j=0}^{N} g_j Y^j$, and setting $X = 0$ gives

$$Y^{N+1} = \sum_{j=0}^{N} g_j(0,Y)\, Y^j = \sum_{j=0}^{N} g_j(0,0)\, Y^j,$$

which is impossible since the right hand side has degree at most N. Hence $XY^{N+1} \notin I_N$.

Thus a subring of a Noetherian ring need not be Noetherian. Note that the union $\bigcup_N I_N = Xk[X,Y]$ is the kernel of the homomorphism $R \to k$, $f \mapsto f(0,0)$, so it is a maximal ideal of R which is not finitely generated. □

Problem 15. *Let $I = (f_1, f_2) \subset k[X,Y]$ with $f_1 = X^3 - 2XY$ and $f_2 = X^2Y - 2Y^2 + X$, and use the graded lexicographic order $\leq_{grlex}$ with $X > Y$. Show that $(LT(f_1), LT(f_2))$ is strictly contained in $\mathfrak{in}(I)$, that is, $(LT(f_1), LT(f_2)) \subsetneq \mathfrak{in}(I)$.*

Solution. With respect to $\leq_{grlex}$ we have $LT(f_1) = X^3$ and $LT(f_2) = X^2Y$, the terms of highest degree. Since $f_1, f_2 \in I$, we have $(X^3, X^2Y) \subset \mathfrak{in}(I)$. On the other hand,

$$Xf_2 - Yf_1 = (X^3Y - 2XY^2 + X^2) - (X^3Y - 2XY^2) = X^2$$

lies in I, so $X^2 = LT(X^2) \in \mathfrak{in}(I)$. But $X^2 \notin (X^3, X^2Y)$: by Lemma 4.4 of the notes, a polynomial lies in a monomial ideal if and only if each of its terms is divisible by one of the generating monomials, and X^2 is divisible by neither X^3 nor X^2Y. Hence $(LT(f_1), LT(f_2)) \subsetneq \mathfrak{in}(I)$; in other words, $\{f_1, f_2\}$ is not a Gröbner basis of I.

In fact, since $X^2 \in I$ we also get $XY = \frac{1}{2}(X \cdot X^2 - f_1) \in I$ and $Y^2 - \frac{1}{2}X = \frac{1}{2}(Y \cdot X^2 - f_2) \in I$, and conversely $f_1 = X \cdot X^2 - 2 \cdot XY$ and $f_2 = Y \cdot X^2 - 2(Y^2 - \frac{1}{2}X)$, so

$$I = (X^2,\ XY,\ Y^2 - \tfrac{1}{2}X).$$

The S-polynomials of these three generators are 0, $\frac{1}{2}X^3$ and $\frac{1}{2}X^2$, each of which has remainder 0 on division by X^2, so by Buchberger's criterion this is a Gröbner basis of I. Hence $\mathfrak{in}(I) = (X^2, XY, Y^2)$, $C(I) = \{1, X, Y\}$, and $\dim_k k[X,Y]/I = 3$ by Theorem 4.8. □

Problem 16. *Let $f = X^2Y + XY^2 + Y^2$, $f_1 = XY - 1$ and $f_2 = Y^2 - 1$ in $k[X,Y]$. Using the lexicographic order with $X > Y$, divide f by f_1, f_2 and then by f_2, f_1.*

Solution. The leading terms are $LT(f) = X^2Y$, $LT(f_1) = XY$ and $LT(f_2) = Y^2$. We follow the proof of Proposition 4.6: at each step we look at the leading term of the current polynomial, subtract a multiple of the first divisor in the list whose leading term divides it, and if there is no such divisor we move the leading term to the remainder.

Division by f_1, f_2. Since $XY \mid X^2Y$, we subtract Xf_1:

$$f - Xf_1 = XY^2 + X + Y^2.$$

The leading term XY^2 is again divisible by XY, so we subtract Yf_1:

$$XY^2 + X + Y^2 - Yf_1 = X + Y^2 + Y.$$

The leading term X is divisible by neither XY nor Y^2, so X goes to the remainder, leaving $Y^2 + Y$. Its leading term is divisible by Y^2, and $Y^2 + Y - f_2 = Y + 1$, neither of whose terms is divisible by XY or Y^2. Altogether

$$f = (X + Y)f_1 + f_2 + (X + Y + 1),$$

with remainder $r = X + Y + 1$.

Division by f_2, f_1. Now $Y^2 \nmid X^2Y$ but $XY \mid X^2Y$, so the first step is the same: $f - Xf_1 = XY^2 + X + Y^2$. This time f_2 is the first divisor whose leading term divides XY^2, so we subtract Xf_2:

$$XY^2 + X + Y^2 - Xf_2 = 2X + Y^2.$$

The term $2X$ goes to the remainder, and $Y^2 - f_2 = 1$ goes to the remainder as well. Altogether

$$f = (X + 1)f_2 + Xf_1 + (2X + 1),$$

with remainder $r = 2X + 1$.

The two remainders are different, so the remainder depends on the order in which the divisors are listed. By Theorem 4.8 this cannot happen for a Gröbner basis, and indeed $\{f_1, f_2\}$ is not a Gröbner basis of $I = (f_1, f_2)$: the difference of the two remainders, $(X + Y + 1) - (2X + 1) = Y - X = Xf_2 - Yf_1$, lies in I, but its leading term $-X$ is divisible by neither XY nor Y^2. □

Problem 17. *Let $I \subset k[X,Y,Z]$ be the ideal generated by $Y - X^2$ and $Z - X^3$. (a) Determine a Gröbner basis of I for the lexicographic order with $X < Y < Z$. (b) Determine a Gröbner basis of I for the lexicographic order with $X > Y > Z$.*

Solution. (a) For the lexicographic order with $Z > Y > X$, the generators $g_1 = Y - X^2$ and $g_2 = Z - X^3$ have leading terms Y and Z. By Buchberger's criterion (Theorem 4.11) it suffices to check that $S(g_1, g_2)$ has remainder 0 on division by g_1, g_2. We have

$$S(g_1, g_2) = Zg_1 - Yg_2 = X^3Y - X^2Z,$$

whose leading term is $-X^2Z$, since $Z > Y$. Subtracting $-X^2g_2$ gives $X^3Y - X^5$, and subtracting X^3g_1 gives 0. Hence $\{Y - X^2, Z - X^3\}$ is a Gröbner basis of I, and it is reduced.

(b) For the lexicographic order with $X > Y > Z$ we write the generators as $g_1 = X^2 - Y$ and $g_2 = X^3 - Z$, with leading terms X^2 and X^3, and run Buchberger's algorithm. First, $S(g_1, g_2) = Xg_1 - g_2 = -XY + Z$ is its own remainder on division by g_1, g_2, so we add $g_3 = XY - Z$ to the generators. Since $g_2 = Xg_1 + g_3$, we may discard g_2. Next,

$$S(g_1, g_3) = Yg_1 - Xg_3 = XZ - Y^2$$

is its own remainder on division by g_1, g_3, so we add $g_4 = XZ - Y^2$. Now $S(g_1, g_4) = Zg_1 - Xg_4 = XY^2 - YZ = Yg_3$ has remainder 0, but

$$S(g_3, g_4) = Zg_3 - Yg_4 = Y^3 - Z^2$$

is its own remainder on division by g_1, g_3, g_4, so we add $g_5 = Y^3 - Z^2$. Finally, division with remainder gives

$$\begin{aligned} S(g_1, g_5) &= X^2Z^2 - Y^4 = Z^2g_1 - Yg_5, \\ S(g_3, g_5) &= XZ^2 - Y^2Z = Zg_4, \\ S(g_4, g_5) &= XZ^3 - Y^5 = Z^2g_4 - Y^2g_5, \end{aligned}$$

all with remainder 0, and $S(g_1, g_3) = g_4$ and $S(g_3, g_4) = g_5$ now have remainder 0 as well. By Buchberger's criterion,

$$G = \{X^2 - Y,\ XY - Z,\ XZ - Y^2,\ Y^3 - Z^2\}$$

is a Gröbner basis of I for the lexicographic order with $X > Y > Z$; it is in fact the reduced Gröbner basis. The ideal I is the ideal of the twisted cubic curve $t \mapsto (t, t^2, t^3)$; compare with the example in Lecture 8, where the same four polynomials form a Gröbner basis for the graded lexicographic order. Note that $G \cap k[Y, Z] = \{Y^3 - Z^2\}$, which by Problem 21 generates $I \cap k[Y, Z]$: the projection $(t, t^2, t^3) \mapsto (t^2, t^3)$ of the twisted cubic to the (Y, Z)-plane lies on the cuspidal cubic $Y^3 = Z^2$. □

Problem 18. *For the lexicographic order with $X > Y > Z > W$, determine a Gröbner basis of the ideal*

$$(3X - 6Y - 2Z,\ 2X - 4Y + 4W,\ X - 2Y - Z - W) \subset \mathbb{Q}[X, Y, Z, W].$$

Compare the result with the reduced row echelon form (Gaussian elimination) of the system of linear equations

$$\begin{aligned} 3X - 6Y - 2Z &= 0 \\ 2X - 4Y + 4W &= 0 \\ X - 2Y - Z - W &= 0. \end{aligned}$$

Solution. Write $h_1 = 3X - 6Y - 2Z$, $h_2 = 2X - 4Y + 4W$, $h_3 = X - 2Y - Z - W$ and $I = (h_1, h_2, h_3)$. All three leading terms are multiples of X, so the S-polynomials are

$$\begin{aligned} S(h_1, h_3) &= h_1 - 3h_3 = Z + 3W, \\ S(h_2, h_3) &= h_2 - 2h_3 = 2Z + 6W, \\ S(h_1, h_2) &= \tfrac{1}{3}h_1 - \tfrac{1}{2}h_2 = -\tfrac{2}{3}Z - 2W. \end{aligned}$$

None of these is divisible by X, so by Buchberger's criterion $\{h_1, h_2, h_3\}$ is not a Gröbner basis, and we add $g_2 = Z + 3W$ to the generators. Since $h_1 = 3h_3 + g_2$ and $h_2 = 2h_3 + 2g_2$, we have $I = (h_3, g_2)$, and replacing h_3 by $h_3 + g_2$ we get $I = (g_1, g_2)$ with

$$g_1 = X - 2Y + 2W, \qquad g_2 = Z + 3W.$$

It remains to check that $S(g_1, g_2) = Zg_1 - Xg_2 = -3XW - 2YZ + 2ZW$ has remainder 0 on division by g_1, g_2. Its leading term $-3XW$ is divisible by X, and $S(g_1, g_2) + 3Wg_1 = -2YZ - 6YW + 2ZW + 6W^2$. Continuing, $-2YZ - 6YW + 2ZW + 6W^2 + 2Yg_2 = 2ZW + 6W^2 = 2Wg_2$, so the remainder is 0. Hence $\{X - 2Y + 2W,\ Z + 3W\}$ is a Gröbner basis of I, and it is reduced.

The coefficient matrix of the linear system and its reduced row echelon form are

$$\begin{pmatrix} 3 & -6 & -2 & 0 \\ 2 & -4 & 0 & 4 \\ 1 & -2 & -1 & -1 \end{pmatrix} \quad \rightsquigarrow \quad \begin{pmatrix} 1 & -2 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

and the non-zero rows of the latter are exactly the coefficient vectors of g_1 and g_2. This is not a coincidence: for linear forms, the steps of Buchberger's algorithm are row operations. The S-polynomial of two linear forms with the same leading variable is a linear combination of the two in which that variable has been eliminated, and reducing a linear form by linear forms with other leading variables is back substitution. In general, the non-zero rows of the reduced row echelon form of a system of linear forms give the reduced Gröbner basis of the ideal they generate, for the lexicographic order in which the variables are ordered as the columns. □

Problem 19. *Suppose that $V \subset k^n$ is a linear subspace, that is,*

$$V = \mathcal{V}\Big(\Big\{ f_j = \sum_{i=1}^{n} a_{ij} X_i : 1 \le j \le m \Big\}\Big)$$

for some $a_{ij} \in k$. Show that $\dim_k V = \deg HP_I(t)$, where $I = (f_1, f_2, \ldots, f_m)$.

Solution. Let A be the $m \times n$ matrix whose j-th row is the coefficient vector $(a_{1j}, \ldots, a_{nj})$ of f_j. Then $V = \{x \in k^n : Ax = 0\}$ is the kernel of A, so $\dim_k V = n - r$ by the rank–nullity theorem, where $r = \operatorname{rank}(A)$.

Row operations on A replace $f_1, \ldots, f_m$ by linear forms which span the same k-subspace of $k[X_1, \ldots, X_n]$, and hence generate the same ideal I. Bringing A into reduced row echelon form, we therefore get $I = (g_1, \ldots, g_r)$ with

$$g_i = X_{p_i} + \sum_{l \in F} b_{il} X_l, \qquad 1 \le i \le r,$$

where $p_1 < \ldots < p_r$ are the pivot columns and $F \subset \{1, \ldots, n\}$ is the set of the remaining $n - r$ indices.

Let $\phi : k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]$ be the k-algebra homomorphism with $\phi(X_{p_i}) = g_i$ for $1 \leq i \leq r$ and $\phi(X_l) = X_l$ for $l \in F$. It is an automorphism: its inverse is the k-algebra homomorphism ψ with $\psi(X_{p_i}) = X_{p_i} - \sum_{l \in F} b_{il} X_l$ and $\psi(X_l) = X_l$ for $l \in F$, as one checks on the variables. Both ϕ and ψ send each variable to a polynomial of degree ≤ 1, so both map $k[X_1, \ldots, X_n]_{\leq s}$ into itself, and being mutually inverse they restrict to bijections of $k[X_1, \ldots, X_n]_{\leq s}$. Let $J = (X_{p_1}, \ldots, X_{p_r})$. Since ϕ is an automorphism sending the generators of J to the generators of I, we have $\phi(J) = I$, and then $\phi(J_{\leq s}) \subset I_{\leq s}$ and $\psi(I_{\leq s}) \subset J_{\leq s}$, so $\phi(J_{\leq s}) = I_{\leq s}$. Hence ϕ induces a k-linear isomorphism

$$k[X_1, \ldots, X_n]_{\leq s} / J_{\leq s} \xrightarrow{\sim} k[X_1, \ldots, X_n]_{\leq s} / I_{\leq s},$$

and $HF_I(s) = HF_J(s)$ for all s.

Now J is a monomial ideal, so by Lemma 4.4 a polynomial lies in J if and only if each of its terms is divisible by one of $X_{p_1}, \ldots, X_{p_r}$. Hence $J_{\leq s}$ is spanned by the monomials of degree $\leq s$ which involve a pivot variable, and $k[X_1, \ldots, X_n]_{\leq s} / J_{\leq s}$ has a basis given by the classes of the monomials of degree $\leq s$ in the $n - r$ variables X_l, $l \in F$. As in Example (b) of Lecture 8, there are $\binom{n-r+s}{n-r}$ of these, so

$$HF_I(s) = HF_J(s) = \binom{s+n-r}{n-r} = \frac{(s+1)(s+2)\cdots(s+n-r)}{(n-r)!},$$

which is a polynomial in s of degree $n - r$. Therefore $HP_I(t) = \binom{t+n-r}{n-r}$ and $\deg HP_I(t) = n - r = \dim_k V$.

Geometrically, ϕ corresponds to a linear change of coordinates on k^n in which V becomes the coordinate subspace $\{X_{p_1} = \ldots = X_{p_r} = 0\}$. The argument used that ϕ preserves degrees. An automorphism of $k[X_1, \ldots, X_n]$ which does not, such as $X_1 \mapsto X_1 + X_2^2$, $X_2 \mapsto X_2$, can change the Hilbert function: it sends (X_1), whose Hilbert function is $s+1$, to $(X_1 + X_2^2)$, whose Hilbert function is $2s + 1$. Alternatively, one can show that $g_1, \ldots, g_r$ form a Gröbner basis of I for the graded lexicographic order (compare Problem 18), so that $\mathfrak{in}(I) = J$, and deduce $HF_I = HF_J$ from Macaulay's lemma. □

Problem 20. *Let $I = (X^2 + Y + Z - 1,\ X + Y^2 + Z - 1,\ X + Y + Z^2 - 1)$ be the ideal in $\mathbb{C}[X, Y, Z]$. Find a Gröbner basis of I with respect to the lexicographic order with $X > Y > Z$, and use it to determine $\mathcal{V}(I)$ explicitly.*

Solution. Write $f_1 = X^2 + Y + Z - 1$, $f_2 = X + Y^2 + Z - 1$ and $f_3 = X + Y + Z^2 - 1$, with leading terms X^2, X and X, and run Buchberger's algorithm. First, $S(f_2, f_3) = f_2 - f_3$ is its own remainder on division by f_1, f_2, f_3, so we add

$$g_2 = Y^2 - Y - Z^2 + Z$$

to the generators. Next, reducing $S(f_1, f_3) = f_1 - Xf_3 = -XY - XZ^2 + X + Y + Z - 1$ modulo f_2, f_3, g_2 gives the remainder

$$g_3 = 2YZ^2 + Z^4 - Z^2,$$

and reducing $S(g_2, g_3) = Z^2 g_2 - \frac{1}{2} Y g_3$ modulo g_3 gives $\frac{1}{4} g_4$, where

$$g_4 = Z^6 - 4Z^4 + 4Z^3 - Z^2.$$

Since $f_2 = f_3 + g_2$ and $f_1 = Xf_3 + S(f_1, f_3)$, the ideal I is generated by $g_1 = f_3$, g_2, g_3 and g_4. One checks that all remaining S-polynomials of g_1, g_2, g_3, g_4 have remainder 0; this is tedious by hand and best left to a computer, for example

```
R = QQ[x,y,z, MonomialOrder => Lex];
I = ideal (x^2+y+z-1, x+y^2+z-1, x+y+z^2-1);
gens gb I
```

in Macaulay2. Hence

$$G = \{X + Y + Z^2 - 1,\ Y^2 - Y - Z^2 + Z,\ 2YZ^2 + Z^4 - Z^2,\ Z^6 - 4Z^4 + 4Z^3 - Z^2\}$$

is a Gröbner basis of I for the lexicographic order with $X > Y > Z$.

The point of the lexicographic order is that G is triangular: g_4 involves only Z, g_2 and g_3 involve only Y and Z, and g_1 is linear in X. Since

$$g_4 = Z^2(Z-1)^2(Z^2 + 2Z - 1), \qquad g_2 = (Y - Z)(Y + Z - 1), \qquad g_3 = Z^2(2Y + Z^2 - 1),$$

every point of $\mathcal{V}(I)$ has $Z \in \{0, 1, -1 + \sqrt{2}, -1 - \sqrt{2}\}$, and for each such Z we find Y from $g_2 = g_3 = 0$ and then $X = 1 - Y - Z^2$ from $g_1 = 0$. Since G generates I, the points obtained lie in $\mathcal{V}(I)$.

- $Z = 0$: $g_3 = 0$ holds automatically, $g_2 = 0$ gives $Y \in \{0, 1\}$, and $X = 1 - Y$. This gives the points $(1, 0, 0)$ and $(0, 1, 0)$.
- $Z = 1$: $g_3 = 0$ gives $Y = 0$, which also satisfies $g_2 = 0$, and $X = 0$. This gives the point $(0, 0, 1)$.
- $Z = \zeta$ with $\zeta^2 + 2\zeta - 1 = 0$: $g_3 = 0$ gives $Y = \frac{1}{2}(1 - \zeta^2) = \zeta$, which also satisfies $g_2 = 0$, and $X = 1 - \zeta - \zeta^2 = \zeta$. This gives the points (ζ, ζ, ζ) with $\zeta = -1 \pm \sqrt{2}$.

Hence $\mathcal{V}(I)$ consists of the five points

$$(1,0,0), \quad (0,1,0), \quad (0,0,1), \quad (-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}), \quad (-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2}).$$

It is instructive to compare $|\mathcal{V}(I)| = 5$ with $\dim_{\mathbb{C}} \mathbb{C}[X, Y, Z]/I$. From G we read off $\mathfrak{in}(I) = (X, Y^2, YZ^2, Z^6)$ for the lexicographic order, so $C(I)$ consists of the 8 monomials

$$1,\ Y,\ Z,\ YZ,\ Z^2,\ Z^3,\ Z^4,\ Z^5,$$

and $\dim_{\mathbb{C}} \mathbb{C}[X,Y,Z]/I = 8$ by Theorem 4.8. Since this number does not depend on the monomial order, we can use it to find the initial ideal for the graded lexicographic order without further computation. The leading terms of f_1, f_2, f_3 are now X^2, Y^2, Z^2, and the complement of (X^2, Y^2, Z^2) consists of the 8 monomials

$$1,\ X,\ Y,\ Z,\ XY,\ XZ,\ YZ,\ XYZ.$$

As $(X^2, Y^2, Z^2) \subset \mathfrak{in}_{grlex}(I)$ and a strictly larger monomial ideal would have a strictly smaller complement, we get $\mathfrak{in}_{grlex}(I) = (X^2, Y^2, Z^2)$, so $\{f_1, f_2, f_3\}$ is a Gröbner basis for $\leq_{grlex}$. Macaulay's lemma (Lecture 8) now gives the Hilbert function: $HF_I(0) = 1$, $HF_I(1) = 4$, $HF_I(2) = 7$ and $HF_I(s) = 8$ for $s \geq 3$, so $HP_I(t) = 8$. Counting instead the elements of degree $\leq s$ in the lexicographic complement would give $1, 3, 5, 6, 7, 8, 8, \ldots$, which is wrong: Macaulay's lemma needs a graded order.

Finally, here is why $5 \neq 8$. The polynomial $h = XY - YZ = Y(X - Z)$ vanishes at all five points of $\mathcal{V}(I)$, and

$$h^2 = (X - Z)\big((X - Z)f_2 + f_3 - f_1\big) \in I,$$

but $h \notin I$: no term of h is divisible by X^2, Y^2 or Z^2, so h is its own remainder on division by the Gröbner basis $\{f_1, f_2, f_3\}$, and by Theorem 4.8 the remainder of an element of I is 0. Thus I is not a radical ideal, and $\mathcal{I}(\mathcal{V}(I)) \neq I$. One can show, using the Nullstellensatz (Lecture 9), that if J is a radical ideal with $\mathcal{V}(J)$ finite then $|\mathcal{V}(J)| = \dim_{\mathbb{C}} \mathbb{C}[X_1, \ldots, X_n]/J$. Indeed, Macaulay2 tells us that

```
I == radical I
gens gb radical I
```

return `false` and the Gröbner basis

$$\sqrt{I} = (Z^4 + Z^3 - 3Z^2 + Z,\ 2YZ + Z^3 - Z,\ Y^2 - Y - Z^2 + Z,\ X + Y + Z^2 - 1),$$

with initial ideal (X, Y^2, YZ, Z^4) and $C(\sqrt{I}) = \{1, Y, Z, Z^2, Z^3\}$, so that $\dim_{\mathbb{C}} \mathbb{C}[X,Y,Z]/\sqrt{I} = 5 = |\mathcal{V}(I)|$. □

Problem 21. *Let $I \subset k[X_1, \ldots, X_n]$ be a non-zero ideal and G a Gröbner basis of I with respect to the lexicographic order with $X_1 > X_2 > \ldots > X_n$. Show that $G \cap k[X_{l+1}, \ldots, X_n]$ generates the ideal $I \cap k[X_{l+1}, \ldots, X_n]$ of $k[X_{l+1}, \ldots, X_n]$ for all $0 \leq l \leq n$.*

Solution. Fix l and write $G_l = G \cap k[X_{l+1}, \ldots, X_n]$ and $I_l = I \cap k[X_{l+1}, \ldots, X_n]$. The intersection I_l of the ideal I with the subring $k[X_{l+1}, \ldots, X_n]$ is an ideal of that subring, and $G_l \subset I_l$, so the ideal (G_l) generated by G_l in $k[X_{l+1}, \ldots, X_n]$ is contained in I_l.

The key observation is that a non-zero $g \in k[X_1, \ldots, X_n]$ whose leading monomial lies in $k[X_{l+1}, \ldots, X_n]$ lies in $k[X_{l+1}, \ldots, X_n]$ itself. Indeed, let X^α be a monomial in which some X_i with $i \leq l$ occurs, and let $X^\beta \in k[X_{l+1}, \ldots, X_n]$, so that $\beta_1 = \ldots = \beta_l = 0$. Then the first non-zero entry of $\alpha - \beta$ occurs at an index $\leq l$ and is positive, so $X^\alpha >_{lex} X^\beta$. Hence a term of g involving one of $X_1, \ldots, X_l$ would be larger than $LM(g)$, which is impossible.

Now let $f \in I_l$ be non-zero. We show that $f \in (G_l)$ by induction on $LM(f)$, which is legitimate by Lemma 4.5. Since G is a Gröbner basis, $LT(f) \in \mathfrak{in}(I) = (LT(g) : g \in G)$, so by Lemma 4.4 there is $g \in G$ with $LM(g) \mid LM(f)$. As $LM(f) \in k[X_{l+1}, \ldots, X_n]$, so is its divisor $LM(g)$, hence $g \in G_l$ by the key observation. Put

$$f' = f - \frac{LT(f)}{LT(g)}\, g.$$

Then $f' \in I$ and $f' \in k[X_{l+1}, \ldots, X_n]$, so $f' \in I_l$, and either $f' = 0$ or $LM(f') < LM(f)$. By induction $f' \in (G_l)$, and therefore $f = f' + \frac{LT(f)}{LT(g)} g \in (G_l)$. This proves $I_l = (G_l)$.

In fact the argument shows more: for every non-zero $f \in I_l$ there is $g \in G_l$ with $LM(g) \mid LM(f)$, so G_l is a Gröbner basis of I_l for the lexicographic order on $k[X_{l+1}, \ldots, X_n]$. This is what makes the lexicographic order useful for solving systems of polynomial equations: in Problem 20, the element $g_4 \in G \cap \mathbb{C}[Z]$ generates $I \cap \mathbb{C}[Z]$, and the elements of $G \cap \mathbb{C}[Y, Z]$ generate $I \cap \mathbb{C}[Y, Z]$, which is why we could solve for Z first, then for Y and finally for X. □

Problem 22. *Let k be an algebraically closed field, $I \subset k[X_1, \ldots, X_n]$ an ideal and G a Gröbner basis of I with respect to some monomial order. Let $V = \mathcal{V}(I) \subset k^n$ be the affine variety defined by I. Show that the following are equivalent:*

(i) V is a finite set;

(ii) for every $j \in \{1, \ldots, n\}$ there exists $g_j \in G$ such that $LM(g_j) = X_j^{m_j}$ for some $m_j \geq 0$.

Under these conditions, show that $|V| \leq \prod_{j=1}^n m_j$.

Solution. Recall from Theorem 4.8 that the standard monomials of I, that is, the monomials $X^\alpha \notin \mathfrak{in}(I) = (LM(g) : g \in G)$, form a basis of $k[X_1, \ldots, X_n]/I$ over k.

Suppose that (ii) holds. If X^α is a monomial with $\alpha_j \geq m_j$ for some j, then $LM(g_j) = X_j^{m_j}$ divides X^α, so $X^\alpha \in \mathfrak{in}(I)$. Hence every standard monomial X^α satisfies $\alpha_j < m_j$ for all j, there are at most $\prod_j m_j$ of them, and

$$\dim_k k[X_1, \ldots, X_n]/I \leq \prod_{j=1}^n m_j.$$

Now let $x_1, \ldots, x_r$ be distinct points of V. The evaluation map $k[X_1, \ldots, X_n] \to k^r$, $f \mapsto (f(x_1), \ldots, f(x_r))$, is a ring homomorphism which vanishes on I, since $x_i \in \mathcal{V}(I)$, and it is surjective: its kernel is the intersection of the r distinct maximal ideals $\mathcal{I}(\{x_i\})$, and the quotient by this intersection is k^r (see the solution of Problem 23). It therefore induces a surjective k-linear map $k[X_1, \ldots, X_n]/I \to k^r$, so that $r \leq \dim_k k[X_1, \ldots, X_n]/I \leq \prod_j m_j$. Thus V is finite and $|V| \leq \prod_j m_j$. This proves (ii) ⇒ (i) together with the bound, and does not use that k is algebraically closed.

Conversely, suppose that V is finite. If $V = \emptyset$, then $I = k[X_1, \ldots, X_n]$ by the weak Nullstellensatz (Theorem 4.29), so $1 \in \mathfrak{in}(I)$ and G contains a non-zero constant g, with $LM(g) = 1 = X_j^0$

for every j. Otherwise, fix j and let $a_1, \ldots, a_r$ be the distinct values taken by the j-th coordinate on V. The polynomial $p = \prod_{i=1}^{r}(X_j - a_i) \in k[X_j]$ vanishes on V, so $p \in \mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$ by the Nullstellensatz (Lecture 13), say $p^N \in I$. Then $LM(p^N) = X_j^{rN} \in \mathfrak{in}(I)$, so by Lemma 4.4 there is $g_j \in G$ whose leading monomial divides X_j^{rN}, that is, $LM(g_j) = X_j^{m_j}$ with $0 \leq m_j \leq rN$.

Algebraic closedness cannot be dropped in (i) $\Rightarrow$ (ii): for $I = (X^2 + Y^2 + 1) \subset \mathbb{R}[X, Y]$ we have $\mathcal{V}(I) = \emptyset$, but the Gröbner basis $\{X^2 + Y^2 + 1\}$ contains no element whose leading monomial is a power of Y (for $\leq_{lex}$ or $\leq_{grlex}$ with $X > Y$). □

Problem 23. *Let $V \subset k^n$ be a finite set (so that V is an affine variety, being a finite union of points) and let $I = \mathcal{I}(V)$. Show that the Hilbert polynomial $HP_I(t)$ is constant, equal to $|V|$.*

Solution. Let $x = (a_1, \ldots, a_n) \in k^n$. Then $\mathcal{I}(\{x\})$ is the maximal ideal $\mathfrak{m}_x = (X_1 - a_1, \ldots, X_n - a_n)$. Indeed, each $X_i - a_i$ vanishes at x. Conversely, if $f \in k[X_1, \ldots, X_n]$, then applying division with remainder we can write $f = g_1(X_1 - a_1) + \ldots + g_n(X_n - a_n) + r$ with $r \in k$, and if $f(x) = 0$ it follows that $r = 0$ (compare the proof of Theorem 4.29). We deduce that $\mathcal{I}(V) = \bigcap_{x \in V} \mathfrak{m}_x$. Distinct maximal ideals are coprime, so by the Sunzi remainder theorem (Theorem 2.3)

$$k[X_1, \ldots, X_n]/\mathcal{I}(V) \simeq \prod_{x \in V} k[X_1, \ldots, X_n]/\mathfrak{m}_x = \prod_{x \in V} k,$$

the isomorphism being induced by $f \mapsto (f(x))_{x \in V}$. In particular $\dim_k k[X_1, \ldots, X_n]/I = |V|$.

Now $HF_I(s) = \dim_k k[X_1, \ldots, X_n]_{\leq s}/I_{\leq s}$ is the dimension of the image of $k[X_1, \ldots, X_n]_{\leq s}$ in $k[X_1, \ldots, X_n]/I$, since the kernel of $k[X_1, \ldots, X_n]_{\leq s} \to k[X_1, \ldots, X_n]/I$ is $I_{\leq s}$. Thus $HF_I(s) \leq |V|$, with equality as soon as the polynomials of degree $\leq s$ map onto $\prod_{x \in V} k$. This happens for $s \geq |V| - 1$. To see this, write $V = \{x_1, \ldots, x_m\}$ with $x_i = (x_i^{(1)}, \ldots, x_i^{(n)})$. For each pair $i \neq j$ choose l_{ij} with $x_i^{(l_{ij})} \neq x_j^{(l_{ij})}$, which exists since $x_i \neq x_j$, and put

$$f_i = \prod_{\substack{j=1 \\ j \neq i}}^{m} \frac{X_{l_{ij}} - x_j^{(l_{ij})}}{x_i^{(l_{ij})} - x_j^{(l_{ij})}}.$$

Then $\deg f_i = m - 1$, $f_i(x_i) = 1$ and $f_i(x_j) = 0$ for $j \neq i$, so $f_1, \ldots, f_m$ map to the standard basis of k^m. Hence $HF_I(s) = |V|$ for all $s \geq |V| - 1$, and $HP_I(t) = |V|$. □

Problem 24. *Compute the Hilbert polynomials of the following ideals:*

(i) $(X^3Y, XY^2) \subset k[X, Y]$,

(ii) $(X^3YZ^5, XY^3Z^2) \subset k[X, Y, Z]$.

Solution. Both ideals are monomial ideals, so $HF_I(s)$ is the number of monomials of degree $\leq s$ not in I (Theorem 4.8 and Lemma 4.4; see Lecture 8), and we count these as in the proof of Theorem 4.16.

(i) A monomial X^aY^b lies outside $I = (X^3Y, XY^2)$ if and only if it is divisible by neither X^3Y nor XY^2, that is, if and only if $b = 0$, or $a = 0$, or $b = 1$ and $a \leq 2$. So the standard monomials are X^a ($a \geq 0$), Y^b ($b \geq 1$), XY and X^2Y: two rays and two isolated points in the staircase diagram. For $s \geq 3$ there are $(s+1) + s + 2 = 2s + 3$ of them of degree $\leq s$, hence

$$HP_I(t) = 2t + 3,$$

and $HF_I(s) = HP_I(s)$ for $s \geq 3$, while $HF_I(0), HF_I(1), HF_I(2) = 1, 3, 6$.

(ii) A monomial $X^aY^bZ^c$ lies outside $I = (X^3YZ^5, XY^3Z^2)$ if and only if $(a, b, c) \not\geq (3, 1, 5)$ and $(a, b, c) \not\geq (1, 3, 2)$ componentwise. This holds whenever $a = 0$, $b = 0$ or $c \leq 1$; if $a, b \geq 1$ and $c \geq 2$ it holds if and only if $b \leq 2$ and ($a \leq 2$ or $c \leq 4$). So the set of exponents of standard monomials is the disjoint union of the four planes

$$\{a = 0\}, \quad \{b = 0,\ a \geq 1\}, \quad \{c = 0,\ a, b \geq 1\}, \quad \{c = 1,\ a, b \geq 1\},$$

the four lines $\{a, b \in \{1, 2\},\ c \geq 2\}$ and the six lines $\{a \geq 3,\ b \in \{1, 2\},\ c \in \{2, 3, 4\}\}$. The number of points with $a+b+c \leq s$ on these pieces is $\binom{s+2}{2}$, $\binom{s+1}{2}$, $\binom{s}{2}$, $\binom{s-1}{2}$ for the four planes, $s - a - b - 1$ for the line with given $a, b \in \{1, 2\}$, and $s - b - c - 2$ for the line with given b, c. Summing, for $s \geq 8$,

$$HF_I(s) = \binom{s+2}{2} + \binom{s+1}{2} + \binom{s}{2} + \binom{s-1}{2} + (4s - 16) + (6s - 39) = 2s^2 + 10s - 53,$$

hence $HP_I(t) = 2t^2 + 10t - 53$. In accordance with Theorem 4.16 the degree is 2, the dimension of the planes, and each of the four planes contributes $s^2/2 + O(s)$ points, which explains the leading coefficient 2. □

Problem 25. *Let $A \subset B$ be commutative rings. Show that B is finitely generated as an A-module if and only if B is finitely generated as an A-algebra and integral over A.*

Solution. Suppose that $B = Ab_1 + \ldots + Ab_n$. Then $B = A[b_1, \ldots, b_n]$, since the subring $A[b_1, \ldots, b_n]$ of B generated by A and $b_1, \ldots, b_n$ contains $Ab_1 + \ldots + Ab_n = B$; so B is a finitely generated A-algebra. Moreover, for $b \in B$ the subring $C = B$ satisfies $A[b] \subset C$ and is finitely generated as an A-module, so b is integral over A by Lemma 4.21 (iii ⇒ i).

Conversely, suppose that $B = A[b_1, \ldots, b_n]$ is integral over A. Each b_i is integral over A, hence over the larger ring $A[b_1, \ldots, b_{i-1}]$, and Corollary 4.23 (a) shows that B is a finitely generated A-module. Explicitly, if b_i satisfies a monic equation of degree d_i over A, then B is generated as an A-module by the monomials $b_1^{e_1} \cdots b_n^{e_n}$ with $0 \leq e_i < d_i$. □

Problem 26. *Find the normalisation of $\mathbb{Z}[\sqrt{d}]$ for a square-free integer $d \neq 1$.*

Solution. We first note that the field of fractions of $\mathbb{Z}[\sqrt{d}]$ is $K = \mathbb{Q}(\sqrt{d})$. This follows from the observation that $\mathbb{Q}(\sqrt{d})$ is the smallest field containing $\mathbb{Z}[\sqrt{d}]$; alternatively, for $x, y, z, w \in \mathbb{Z}$ with $(z, w) \neq (0, 0)$ one can write

$$\frac{x + y\sqrt{d}}{z + w\sqrt{d}} = \frac{(x + y\sqrt{d})(z - w\sqrt{d})}{z^2 - dw^2} = \frac{xz - ywd}{z^2 - dw^2} + \frac{yz - xw}{z^2 - dw^2}\sqrt{d},$$

where $z^2 - dw^2 \neq 0$ because d is not a square.

Next, we observe that any element of K that is integral over $\mathbb{Z}[\sqrt{d}]$ is in fact integral over $\mathbb{Z}$. This holds because $\mathbb{Z}[\sqrt{d}]$ is an integral extension of $\mathbb{Z}$, as $\sqrt{d}$ is a root of the monic polynomial $X^2 - d$ with integer coefficients, and integrality is transitive (Corollary 4.23 (c)). Therefore the normalisation of $\mathbb{Z}[\sqrt{d}]$ coincides with the ring of algebraic integers $\mathcal{O}_K$, that is, the integral closure of $\mathbb{Z}$ in $K = \mathbb{Q}(\sqrt{d})$.

Let $\alpha = u + v\sqrt{d} \in \mathcal{O}_K$ with $u, v \in \mathbb{Q}$, and let $\bar{\alpha} = u - v\sqrt{d}$. Applying the automorphism $\sqrt{d} \mapsto -\sqrt{d}$ of K to an equation of integral dependence for α shows that $\bar{\alpha} \in \mathcal{O}_K$ too. Hence $2u = \alpha + \bar{\alpha}$ and $u^2 - dv^2 = \alpha\bar{\alpha}$ are rational numbers which are integral over $\mathbb{Z}$, so they are integers because $\mathbb{Z}$ is normal (Lecture 10). It follows that $d(2v)^2 = (2u)^2 - 4(u^2 - dv^2) \in \mathbb{Z}$; writing $2v = p/q$ in lowest terms, q^2 divides dp^2 and hence d, so $q = 1$ as d is square-free. Thus $m = 2u$ and $n = 2v$ are integers with

$$m^2 \equiv dn^2 \pmod 4.$$

Recall that a square is congruent to 0 or 1 modulo 4, and note that $d \not\equiv 0 \pmod 4$ since d is square-free.

If $d \equiv 2$ or $3 \pmod 4$: if n were odd we would get $m^2 \equiv d \pmod 4$, which is impossible, so n is even, and then $m^2 \equiv 0 \pmod 4$ forces m to be even. Hence $u, v \in \mathbb{Z}$, and we conclude that $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$: the ring $\mathbb{Z}[\sqrt{d}]$ is normal.

If $d \equiv 1 \pmod 4$: then $m^2 \equiv n^2 \pmod 4$, so $m \equiv n \pmod 2$ and $u - v = (m-n)/2 \in \mathbb{Z}$. Hence

$$\alpha = (u - v) + n \cdot \frac{1 + \sqrt{d}}{2} \in \mathbb{Z} + \mathbb{Z}\,\frac{1 + \sqrt{d}}{2} = \mathbb{Z}\Big[\frac{1 + \sqrt{d}}{2}\Big].$$

Conversely, $\frac{1+\sqrt{d}}{2}$ is a root of $X^2 - X + \frac{1-d}{4} \in \mathbb{Z}[X]$, so it lies in $\mathcal{O}_K$. We conclude that $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, which is strictly larger than $\mathbb{Z}[\sqrt{d}]$. For instance, $\mathbb{Z}[\sqrt{5}]$ is not normal, and for $d = -3$ we recover the example $\mathbb{Z}[\sqrt{-3}] \subsetneq \mathbb{Z}[\omega]$ of Lecture 9. □

Problem 27. *Show that* 1 *lies in the ideal* $I = (X^2 + Y^2 - Z,\ (X^2 + Y^2 - Y)X,\ Y^5 - Y^4Z + Z^2Y^3,\ XYZ - 1)$ *of* $\mathbb{C}[X, Y, Z]$.

Solution. Write $f_1 = X^2 + Y^2 - Z$, $f_2 = (X^2 + Y^2 - Y)X$, $f_3 = Y^5 - Y^4Z + Z^2Y^3$ and $f_4 = XYZ - 1$. By the weak Nullstellensatz (Theorem 4.29) it suffices to show that $\mathcal{V}(I) = \emptyset$, that is, that the system $f_1 = f_2 = f_3 = f_4 = 0$ has no solution in $\mathbb{C}^3$. Suppose that (x, y, z) were a solution. From $f_4 = 0$ we get $x, y, z \neq 0$. From $f_1 = 0$ we get $z = x^2 + y^2$, and then $f_2 = (z - y)x = 0$ with $x \neq 0$ gives $z = y$. Substituting into $f_3 = 0$ gives $y^5 - y^5 + y^5 = y^5 = 0$, contradicting $y \neq 0$.

The argument can be turned into an explicit proof, valid over any field, by working modulo I instead of at a point. Write $\equiv$ for congruence modulo I. Then $X(Z - Y) = f_2 - Xf_1 \in I$ and $XYZ \equiv 1$, so

$$Z - Y \equiv XYZ\,(Z - Y) = YZ \cdot X(Z - Y) \equiv 0.$$

Hence $Z \equiv Y$, and therefore $0 \equiv f_3 \equiv Y^5 - Y^5 + Y^5 = Y^5$. Finally

$$1 \equiv (XYZ)^5 = (XZ)^5\, Y^5 \equiv 0,$$

that is, $1 \in I$. (Macaulay2 agrees: `gens gb I` returns the 1×1 matrix (1).) □

Problem 28. *Let* $M = \begin{pmatrix} X & Y \\ Z & W \end{pmatrix}$ *be a* 2*-by-*2 *matrix with entries* X, Y, Z, W*. Solving* $M^2 = 0$ *amounts to four polynomial equations; let*

$$I = (X^2 + YZ,\ XY + YW,\ XZ + WZ,\ W^2 + YZ) \subset k[X, Y, Z, W]$$

be the ideal they generate. Is I *a radical ideal? Show that* $\sqrt{I} = (X + W, XW - YZ)$*.*

Solution. Let us first give a proof under the assumption that $k = \overline{k}$ is algebraically closed. Recall that the characteristic polynomial of a 2-by-2 matrix M is

$$\chi_M(t) = t^2 - (\operatorname{tr} M)\, t + \det M.$$

If M is a matrix with entries in k such that $M^2 = 0$, then every eigenvalue λ of M satisfies $\lambda^2 = 0$, so $\chi_M(t) = t^2$ as k is algebraically closed; hence $\operatorname{tr} M = X + W$ and $\det M = XW - YZ$ vanish at every point of $\mathcal{V}(I)$. It follows from the Nullstellensatz, $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$ (Lecture 13), that

$$J \coloneqq (X + W, XW - YZ) \subset \sqrt{I}.$$

Conversely, to prove that $\sqrt{I} \subset J$ it suffices to show that $I \subset J$ and that J is prime, for then $\sqrt{I} \subset \sqrt{J} = J$. It is easy to see that $I \subset J$, because

$$\begin{aligned} X^2 + YZ &= (X + W)X - (XW - YZ), & XY + YW &= (X + W)Y, \\ XZ + WZ &= (X + W)Z, & W^2 + YZ &= (X + W)W - (XW - YZ). \end{aligned}$$

(Alternatively, observe that if $\operatorname{tr} M = 0 = \det M$, then $\chi_M(M) = 0$ gives $M^2 = 0$ by the Cayley–Hamilton theorem; hence $I \subset \sqrt{J}$ by the Nullstellensatz, which implies $I \subset J$ once we know that J is prime.)

It remains to show that $J = (X + W, XW - YZ)$ is prime, that is, that $k[X, Y, Z, W]/J$ is an integral domain. Consider the surjective homomorphism $\phi : k[X, Y, Z, W] \to k[X, Y, Z]/(X^2 + YZ)$ sending X, Y, Z to their classes and W to $-\overline{X}$. It sends $X + W$ to 0 and $XW - YZ$ to $-(\overline{X}^2 + \overline{Y}\,\overline{Z}) = 0$, so $J \subset \ker \phi$. Conversely, dividing by $W + X$ as a polynomial in W, any $f \in k[X, Y, Z, W]$ can be written as $f = (X + W)q + r$ with $r \in k[X, Y, Z]$; if $\phi(f) = 0$ then $r \in (X^2 + YZ)\, k[X, Y, Z] \subset J$, since $X^2 + YZ = X(X + W) - (XW - YZ) \in J$, so $f \in J$. Thus

$$k[X, Y, Z, W]/(X + W, XW - YZ) \simeq k[X, Y, Z]/(X^2 + YZ),$$

and it suffices to see that $(X^2 + YZ) \subset k[X, Y, Z]$ is prime. This holds because $k[X, Y, Z]$ is a UFD and $X^2 + YZ$ is irreducible: it has degree 1 in Y, and its coefficients Z and X^2 have no common factor in $k[X, Z]$, so it cannot be written as a product of two non-units.

We now give a proof that works for any field k. The only place where we used that k is algebraically closed was to show that $X + W$ and $XW - YZ$ lie in $\sqrt{I}$. This can be verified directly:

$$(X+W)^3 = (X+3W)(X^2+YZ) + (W+3X)(W^2+YZ) - 4Z(XY+YW),$$
$$(XW-YZ)^2 = (X^2+YZ)(W^2+YZ) - XZ(XY+YW) - YW(XZ+WZ).$$

(Alternatively, once $X + W \in \sqrt{I}$ is known from the first equation, $XW - YZ = (X+W)W - (W^2 + YZ)$ shows that it too lies in $\sqrt{I}$.)

Finally, I is not radical: $X+W \in \sqrt{I}$, but $X+W \notin I$, since the generators of I are homogeneous of degree 2, so every element of I lies in $(X, Y, Z, W)^2$, and a polynomial of degree 1 does not. □

Problem 29. *Let $f : R \to S$ be a homomorphism of k-algebras between finitely generated k-algebras R and S. Show that $f^{-1}(\mathfrak{m})$ is a maximal ideal of R for every maximal ideal $\mathfrak{m}$ of S.*

Solution. Because S is a finitely generated k-algebra, its quotient $S/\mathfrak{m}$ by a maximal ideal $\mathfrak{m}$ is a field which is finitely generated as a k-algebra, hence a finite field extension of k by Zariski's lemma (Lemma 4.30). The image of R in $S/\mathfrak{m}$ under the composite $R \to S \to S/\mathfrak{m}$ is a subring of a field containing k, hence an integral domain, and it is integral over k by Lemma 4.21 (iii), being contained in the finitely generated k-module $S/\mathfrak{m}$. Therefore it is a field by Corollary 4.23 (d). But the kernel of $R \to S/\mathfrak{m}$ is $f^{-1}(\mathfrak{m})$, so this image is isomorphic to $R/f^{-1}(\mathfrak{m})$, which we have just shown to be a field. Hence $f^{-1}(\mathfrak{m})$ is a maximal ideal.

Note that the preimage of a maximal ideal under a ring homomorphism is always a prime ideal, but need not be maximal in general: for the inclusion $\mathbb{Z} \to \mathbb{Q}$, the preimage of the maximal ideal (0) of $\mathbb{Q}$ is $(0) \subset \mathbb{Z}$. □