

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. $\square$

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 $x \in \mathcal{J}(R)$. $\square$

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 $\mathfrak{p} = J$. $\square$

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. $\square$

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. $\square$

Problem 6. Let k be an infinite field, and $f \in k[X_1, \dots, X_n]$. Show that $f = 0$ if and only if $f(x_1, \dots, x_n) = 0$ for all $(x_1, \dots, x_n) \in k^n$. 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 $k[X_1, \dots, X_{n-1}]$:

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

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

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

vanishes at every $x_n \in k$, so by the case $n = 1$ it is the zero polynomial, that is, $g_j(x_1, \dots, x_{n-1}) = 0$ 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 $f = X_1^2 - X_1 \in \mathbb{F}_2[X_1, \dots, X_n]$ is non-zero, but $f(x_1, \dots, x_n) = x_1^2 - x_1 = 0$ 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 $\mathbb{F}_q$.) $\square$

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 $\mathfrak{p} \neq (0)$.

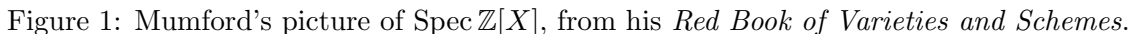
- (i) Suppose $\mathfrak{p} \cap \mathbb{Z} = \{0\}$. Show that $\mathfrak{p} = (f)$ where $f \in \mathbb{Z}[X]$ is an irreducible polynomial.
- (ii) Suppose $\mathfrak{p} \cap \mathbb{Z} = (p)$ with p a prime number. Show that $\mathfrak{p} = (p, f)$ where $f = 0$ or $f \in \mathbb{Z}[X]$ is a monic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

Solution. The inclusion $\iota : \mathbb{Z} \rightarrow \mathbb{Z}[X]$ 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 $g = q'f$.

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

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.

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

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

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

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 $y = scd \in (cd)$. Hence $I = (cd)$ is principal, contradicting the hypothesis. Therefore I is prime. $\square$

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 . $\square$

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 $a + b \notin I \cup J$. $\square$

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 $f = a_0 + a_1X + \dots + a_nX^n \in \mathcal{J}$. 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 $R[X] \rightarrow (R/\mathfrak{p})[X]$. 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, $a_0, a_1, \dots, a_n \in \mathfrak{p}$. 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 . $\square$

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 $f = \sum_{i \geq 0} c_i T^i \in R[[T]]$ write $\text{ord}(f)$ for the smallest i with $c_i \neq 0$, and set $\text{ord}(0) = \infty$.

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

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

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 $J_0 \subset J_1 \subset \dots$ stabilises: there is s with $J_s = J_{s+i}$ for all $i \geq 0$. For each $m \leq s$ write $J_m = (a_{m,1}, \dots, a_{m,r_m})$ 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 $\text{ord}(f - g) \geq s$. If $\text{ord}(f) = m < s$ 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 $\text{ord}(h) \geq s$ 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 $\text{ord}(h_n) \geq s+n$ 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

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

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. $\square$

Problem 13. Let k be a field. For $S \subset k[X_1, \dots, X_n]$ and $U \subset k^n$ let $\mathcal{V}(S) \subset k^n$ and $\mathcal{I}(U) \subset k[X_1, \dots, X_n]$ 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. $\square$