Primary Decomposition

Notes by Mateusz Michałek
for the lecture on July 03, 2018, in the
IMPRS Ringvorlesung *Introduction to Nonlinear Algebra*

We have seen in several previous lectures that the idea of decomposing a mathematical object into simpler pieces is very important. In this lecture we focus on a vast generalization of the following two well-known, central facts.

1. Every integer $n > 1$ can be uniquely decomposed as a product of powers of prime numbers:
$$n = p_1^{a_1} \cdots p_k^{a_k}.$$
2. (Proposition 5 from Lecture 2) Any variety can be uniquely decomposed as a union of irreducible varieties.

We claim that the central algebraic notion that binds the first - number theoretic - and second - geometric - statement is that of an ideal. Indeed, any integer n can be identified with an ideal $(n) \subset \mathbb{Z}$ of numbers divisible by n. Notice that (n) is a (nonzero) prime ideal if and only if n is a prime number. We can restate fact (1) in terms of intersections of powers of prime ideals as follows:

Every nonzero ideal $I \subset \mathbb{Z}$ has a unique representation as:

$$I = (I_1)^{a_1} \cap \cdots \cap (I_k)^{a_k},$$

where I_i are prime ideals.

Similarly, over an algebraically closed field, we have a correspondence between varieties and radical ideals. We consider the following restatement of (2):

Every radical ideal $I \subset \mathbb{C}[\mathbf{x}]$ has a unique decomposition as an intersection of prime ideals, pairwise not contained in each other:

$$I = p_1 \cap \cdots \cap p_k.$$

From the above examples we see that our aim should be to decompose ideals I in a ring R. Further, decomposition should mean that we present them as an intersection of other ideals. However, we still need to answer the following questions:

1. What kind of ideals should be allowed in the intersection?

2. What restrictions should be put on the ring R?

3. Can we expect the decomposition to be unique?

We start with the first question. Already the number theoretic example shows that we cannot expect to present an ideal as an intersection of prime ideals. Our next guess could be that we should use powers of prime ideals.

Example 1. *Consider the ideal $I = (x^2, y) \subset \mathbb{C}[x, y]$. It is not an intersection of powers of prime ideals. Indeed, suppose $I = \bigcup p_i^{a_i}$. Then each $p_i \supset I$. Hence, each $p_i = (x, y)$ as this is the only prime ideal that contains I. However, I is not a power of (x, y).*

Exercise 3 gives us a hint that the right class of ideals are *primary* ideals. Recall that I is primary if and only if for all a, b if $ab \in I$ and $a \notin I$ then $b^n \in I$ for some n.

Now we pass to the second question: which rings should be consider. Clearly $\mathbb{Z}$ and $\mathbb{C}[\mathbf{x}]$ share a lot of nice properties. It turns out that there is a very large class of rings that will suit us.

Definition 2. *A ring R is called* Noetherian *if every ascending chain of ideals:*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

stabilizes, i.e. there exists k such that $I_k = I_{k+1} = I_{k+2} = \dots$.

Noetherian rings are named after one of the most famous German mathematicians: Emmy Noether. A hint how important they are is given in Exercises 4 and 5.

Before stating our main existence theorem let us introduce a technical definition.

Definition 3. *An ideal I is* irreducible *if and only if whenever $I = J_1 \cap J_2$ for some ideals J_1, J_2 then $I = J_1$ or $I = J_2$.*

Theorem 4. *Let I be an ideal in a Noetherian ring R. Then there exist primary ideals $q_1, \dots, q_k$ such that:*

$$I = q_1 \cap \dots \cap q_k.$$

Proof. First we show that every ideal in R can be presented as a finite intersection of irreducible ideals. For a contradiction, let I_1 be an ideal that cannot be presented in such a way. In particular, it is not irreducible. Thus, $I_1 = J_1 \cap J_2$ and both J_i's are strictly larger than I_1. If both J_i's are finite intersections of irreducible ideals, then so is I_1. Hence, we may assume J_1 cannot be presented in such a way. Let $I_2 := J_1$. We have $I_1 \subsetneq I_2$. We repeat the construction starting with I_2 and get an ideal I_3 with $I_1 \subsetneq I_2 \subsetneq I_3$, where I_3 is not a finite intersection of irreducible ideals. Continuing, we get a chain of strictly ascending ideals, which is not possible in a Noetherian ring.

It remains to prove that every irreducible ideal in R is primary. Suppose q is irreducible. By passing to the ring R/q we may assume $q = 0$. Suppose $ab = 0$ and $a \neq 0$. We have to prove that b is nilpotent. Consider the following ascending chain of ideals:

$$\{x : bx = 0\} =: \operatorname{Ann}(b) \subseteq \operatorname{Ann}(b^2) \subseteq \operatorname{Ann}(b^3) \subseteq \dots$$

As the ring is Noetherian, we must have $\mathrm{Ann}(b^n) = \mathrm{Ann}(b^{n+1})$ for some n. We claim that $(a) \cap (b^n) = (0)$. Indeed, suppose $\lambda a = \mu b^n \in (a) \cap (b^n)$ for some $\lambda, \mu \in R/q$. Clearly:

$$0 = \lambda ab = \mu b^{n+1}.$$

Hence, $\mu \in \mathrm{Ann}(b^{n+1}) = \mathrm{Ann}(b^n)$. Thus, $\mu b^n = 0$. As (0) was assumed irreducible and $(a) \supsetneq (0)$ we must have $b^n = 0$, which finishes the proof. □

We now pass to the third question. In fact from now on we will not need to assume that the ring is Noetherian, as long as the ideal is equal to an intersection of a finite number of primary ideals.

First, we make the obvious assumption about the primary decomposition $I = \bigcap_{i=1}^k q_i$, that all q_i's are indeed necessary, i.e. $\bigcap_{j \neq i_0} q_j \not\subset q_{i_0}$ for all $1 \leq i_0 \leq k$. The next two lemmas suggest how to group q_i's according to their radical.

Lemma 5. *The radical of a primary ideal q is the unique smallest prime ideal containing it.*

The (easy) proof is left as Exercise 6 for the reader. A primary ideal q with radical equal to p is called p-primary.

Remark 6. *The converse of Lemma 5 does not hold. Even powers of prime ideals do not have to be primary in general. For example consider the ideal $(x,z)^2$ in the ring $\mathbb{C}[x,y,z]/(xy-z^2)$.*

Lemma 7. *If $q_1, \dots, q_k$ are p-primary ideals, then so is $\bigcap_{i=1}^k q_i$.*

Proof. First we notice that the radical of $I := \bigcap_{i=1}^k q_i$ equals p:

$$a \in \mathrm{rad}(I) \iff \exists_n : a^n \in I \iff \exists_n \forall_{1 \leq i \leq k}\ a^n \in q_i \iff \forall_{1 \leq i \leq k}\ a \in \mathrm{rad}(q_i) = p \iff a \in p.$$

To prove that I is primary assume that $ab \in I$ and $a \notin I$. Then $a \notin q_{i_0}$ for some i_0. As $ab \in q_{i_0}$, which is primary, we have $b \in \mathrm{rad}(q_{i_0}) = p = \mathrm{rad}(I)$, i.e. $b^n \in I$ for some n. □

Lemma 7 shows that given a primary decomposition $I = \bigcap_{i=1}^k q_i$ we should first group together q_i's that have the same radical and replace them by their intersection. Hence, we can always bring any presentation $I = \bigcap_{i=1}^k q_i$ to the following form, which from now on will be called *minimal primary decomposition*

Definition 8. *A* minimal primary decomposition *of I is a presentation: $I = \bigcap_{i=1}^k q_i$, where*

- *all q_i's are primary ideals,*
- *q_i's have pairwise distinct radicals,*
- *$\bigcap_{j \neq i_0} q_j \not\subset q_{i_0}$ for all $1 \leq i_0 \leq k$.*

To sum up, we have proved that:

1. in a Noetherian ring every ideal has a (finite) primary decomposition and

2. (in any ring) if an ideal has a (finite) primary decomposition it can be changed to a minimal one (first applying Lemma 7 and then removing the unnecessary ideals).

The following example shows that minimal primary decomposition may still be not unique.

Example 9. *The following are two minimal primary decompositions:*

$$(x^2, xy) = (x) \cap (x, y)^2 = (x) \cap (x^2, y) \subset \mathbb{C}[x, y].$$

It turns out that, while q_i's in the decomposition are not unique, their radicals are. Recall the notation:

$$I : a := \{b \in R : ab \in I\}.$$

Theorem 10. *For any ideal I in a ring R, the set of radicals* $\mathrm{rad}(q_i)$ *does not depend on the choice of a minimal primary decomposition:*

$$I = \bigcap_{i=1}^{k} q_i.$$

These radicals are precisely the prime ideals of the form $\mathrm{rad}(I : a)$ *for some $a \in R$. Further, if R is Noetherian, then these are also (exactly) prime ideals of the form $I : a$ for $a \in R$.*

Proof. Fix a minimal primary decomposition $I = \bigcap_{i=1}^{k} q_i$. We start by proving that $\mathrm{rad}(q_i)$ are exactly the prime ideals of the form $\mathrm{rad}(I : a)$.

Claim: $\mathrm{rad}(I : a) = \bigcap_{a \notin q_j} \mathrm{rad}(q_j)$

Proof of the claim. We have the following:

$$x \in \mathrm{rad}(I : a) \Leftrightarrow \exists_n : ax^n \in \bigcap_{i=1}^{k} q_i \Leftrightarrow \exists_n \forall_{1 \leq i \leq k}\ ax^n \in q_i \Leftrightarrow x \in \bigcap_{i=1}^{k} \mathrm{rad}(q_i : a),$$

i.e. $\mathrm{rad}(I : a) = \bigcap_{i=1}^{k} \mathrm{rad}(q_i : a)$. Our next aim is to understand the ideals $\mathrm{rad}(q_i : a)$. Clearly, if $a \in q_i$, then $\mathrm{rad}(q_i : a)$ is the whole ring, thus may be removed from the intersection:

$$\bigcap_{i=1}^{k} \mathrm{rad}(q_i : a) = \bigcap_{a \notin q_j} \mathrm{rad}(q_j : a).$$

To finish the proof of the claim we have to show that if $a \notin q_i$ then $\mathrm{rad}(q_i : a) = \mathrm{rad}(q_i)$. Suppose $b \in \mathrm{rad}(q_i : a)$, i.e. $b^n a \in q_i$. As q_i is primary and $a \notin q_i$, then $(b^n)^m \in q_i$, i.e. $b \in \mathrm{rad}(q_i)$. Hence, $\mathrm{rad}(q_i : a) \subset \mathrm{rad}(q_i)$ and the other inclusion is obvious. $\square$

The claim tells us that every ideal $\mathrm{rad}(I : a)$ equals the intersection of (some) prime ideals $\mathrm{rad}(q_j)$. By Exercise 8, we see that if $\mathrm{rad}(I : a)$ is prime it has to be in fact equal to one of the $\mathrm{rad}(q_j)$. Conversely, if we consider any $\mathrm{rad}(q_{i_0})$, as the primary decomposition is minimal, there exists $a \in \bigcap_{j \neq i_0} q_j \setminus q_{i_0}$. The claim shows that $\mathrm{rad}(I : a) = \mathrm{rad}(q_{i_0})$.

It remains to prove the last statement of the theorem. Clearly, if $I : a$ is prime, then it is equal to its radical. Thus, we have to consider a prime ideal $\mathrm{rad}(I : a)$ and show it equals $I : a'$ for some $a' \in I$. From the first part we already know that $\mathrm{rad}(I : a) = \mathrm{rad}(q_{i_0})$ for some i_0. By Exercise 9 there exists n such that $\mathrm{rad}(q_{i_0})^n \subset q_{i_0}$. Hence, there exists n such that $(\bigcap_{j \neq i_0} q_j) \cdot (\mathrm{rad}(q_{i_0}))^n \subseteq I$ and we fix the smallest possible n with this property. Then we may pick

$$a' \in \left((\bigcap_{j \neq i_0} q_j) \cdot (\mathrm{rad}(q_i))^{n-1} \right) \setminus I.$$

(Here we notice that if $n = 1$ then $\mathrm{rad}(q_i))^{n-1}$ should be considered as the whole ring.) By definition $a' \cdot \mathrm{rad}(q_i) \subseteq I$, thus $\mathrm{rad}(q_i) \subseteq I : a'$. However, $a' \in (\bigcap_{j \neq i_0} q_j) \setminus I$, thus $a' \notin q_{i_0}$. From the first part, we have a sequence of inclusions:

$$\mathrm{rad}(q_i) \subseteq I : a' \subseteq \mathrm{rad}(I : a') = \mathrm{rad}(q_i),$$

which thus must be in fact equalities. □

The uniquely determined radicals of q_i's are in fact so important that they deserve a separate definition.

Definition 11. *For an ideal I the* associated primes *are the radicals of the primary ideals appearing in a minimal primary decomposition. Equivalently, these are the prime ideals of the form* $\mathrm{rad}(I : a)$ *for some element a of the ring, or in case the ring is Noetherian, prime ideals of the form $I : a$.*

Before passing further let us discuss the geometry behind the associated primes. Notice that if $I = \bigcap_{i=1}^k q_i$ is a minimal primary decomposition then $\mathrm{rad}(I) = \bigcap_{i=1}^k \mathrm{rad}(q_i)$. Thus one is tempted to say that the associated primes correspond to components of the irreducible decomposition of the variety $V(I)$. This is not quite true; although q_i's are incomparable, their radicals may still be!

Example 12. *We continue Example 9 and consider the ideal $I = (x^2, xy) \subset \mathbb{C}[x, y]$. We have* $\mathrm{rad}(I) = (x)$*, i.e. the associated variety is irreducible - a line in a plane. However, the minimal primary decomposition:*

$$(x^2, xy) = (x) \cap (x^2, y)$$

tells us that there are two associated primes. The expected one (x) and the unexpected one: (x, y) - a point on the line. Thus, the associated primes remember more information than just the variety associated to the ideal; there is a 'hidden' - embedded - point on that line distinguished by the ideal I. Although we do not see the point, let us try to persuade you that it is important.

Consider a situation in which you make a measurement y, but independently you get a (very small, unknown) error x. Think about your observations as pairs of numbers (x, y). We want to understand which points in the plain we may get. A priori the observation y is arbitrary, but the error is very small. In algebraic setting, we could say that x is meaningful, *but x^2 is so small that in fact $x^2 = 0$. Hence, we work modulo the ideal (x^2). So far this ideal defines a (double) line which tells us that we can get arbitrary y and 'almost zero' value of x.*

The story does not end here: we just got new equipment that allows us to get rid of the error - but only when $y \neq 0$. In other words if we get a nonzero observation then $x = 0$, but if we get a zero observation $y = 0$ we still do not know the error. Hence, our new equipment gives us a new restriction $xy = 0$. Now we indeed consider $I = (x^2, xy)$. From the description of the situation we know which kind of points we can get: arbitrary nonzero y and zero error x or zero y and some extremely small x. Primary decomposition tells us about this! The embedded point (x, y) is precisely the point where the 'strange extremely small' error is allowed! This point, which geometrically is only $(0, 0)$ remembers that in fact the first coordinate could be 'infinitesimally small' and we could say that the point has a 'direction'.

Although the previous example may sound science-fiction, the formal algebraic replacement of purely geometric varieties (corresponding to radical ideals) by arbitrary ideals allowed a tremendous advance of XX-th century algebraic geometry. We are now ready to work with 'functions' that are nonzero, but their square is zero, using basic, well-understood algebra. Such an algebraic breakthrough could only be compared to introduction of complex numbers in XVII-th and XVIII-th century, where basically in the same way, instead of answering a question: does there exists a square root of -1?, one introduces a formal algebraic object (field of complex numbers) and shows how to work with it in an efficient way.

Still, at each step we should not forget the 'classical' geometry we started from. Clearly the line from Example 12 is of different type than the point and these two should be distinguished.

Definition 13. *For an ideal I let* $\mathrm{Ass}(I)$ *be the set of associated primes. The minimal (with respect to inclusion) elements of* $\mathrm{Ass}(I)$ *are called the* minimal (or isolated) primes. *The associated primes that are not minimal are called* embedded.

First we note that an embedded prime p (for an ideal I) must contain a minimal prime p'. We recall from Lecture 2, that this means that the variety of p' contains that of p. Hence, geometrically we do not see the variety represented by p - it is *embedded* in the variety represented by p'. Further the minimal primes correspond exactly to irreducible components of the variety associated to I, i.e. are the irredundant terms in the decomposition:

$$\mathrm{rad}(I) = \bigcap_{i=1}^{k} \mathrm{rad}(q_i).$$

The lemma below gives one more explanation for the name for minimal primes.

Lemma 14. *A prime ideal is a minimal prime associated to I if and only if it is a minimal element (with respect to inclusion) among the primes that contain I.*

Proof. It is enough to prove that every prime ideal p containing I contains also a prime associated to I. Then p must also contain a minimal associated prime and hence, if p is minimal with respect to inclusion it must be equal to it.

Thus, let us consider $p \supseteq I$ and a minimal primary decomposition $I = \bigcap_{i=1}^k q_i$. Then

$$p \supseteq I = \bigcap_{i=1}^{k} q_i.$$

By Exercise 8 we have $p \supseteq q_{i_0}$ for some some i_0. Hence, $p = \mathrm{rad}(p) \supset \mathrm{rad}(q_{i_0})$. □

The geometry that lead us to distinguish among embedded and minimal associated primes shows us an idea how to get additional uniqueness properties about the primary decomposition. Indeed, in Example 9 it is the ideal corresponding to the embedded component that changes, while the minimal prime remains the same.

Theorem 15. *Let $I = \bigcap_{i=1}^k q_i$ be a minimal primary decomposition of I. The primary ideals q_i corresponding to minimal primes (associated to I) are uniquely determined.*

Proof. Let q_{i_0} be such that $\mathrm{rad}(q_{i_0})$ is a minimal prime. We claim that:

$$q_{i_0} = \{a : \exists_{b \notin \mathrm{rad}(q_{i_0})} : ab \in I\}.$$

As we already proved the right hand side does not depend on the decomposition, thus indeed it is enough to prove the claim. We show both inclusions.

First we pick $a \in q_{i_0}$. For every $j \neq i_0$ we must have $q_j \not\subset \mathrm{rad}\, q_{i_0}$, as otherwise we would have $\mathrm{rad}(q_j) \subset \mathrm{rad}\, q_{i_0}$ contradicting the fact that $\mathrm{rad}\, q_{i_0}$ is minimal. Hence, there exist $b_j \in q_j \setminus \mathrm{rad}(q_{i_0})$. We define $b := \prod_{j \neq i_0} b_j$. As $\mathrm{rad}(q_{i_0})$ is prime we have $b \notin \mathrm{rad}\, q_{i_0}$. However, $ab \in q_j$ for $j \neq i_0$, as $b \in q_j$ and $ab \in q_{i_0}$, as $a \in q_{i_0}$. Hence, $ab \in I = \bigcap_{i=1}^k q_i$ and $a \in \{a : \exists_{b \notin \mathrm{rad}\, q_{i_0}} : ab \in I\}$.

Now we pick a and $b \notin \mathrm{rad}(q_{i_0})$ such that $ab \in I$. In particular, $ab \in q_{i_0}$. If $a \notin q_{i_0}$ we get a contradiction to the fact that q_{i_0} is primary, which proves the second inclusion. □

The Joy of Primary Decomposition

What follows is the additional material presented by Bernd on Tuesday, July 3, at 11:30am. Every polynomial with real or complex coefficients can be interpreted as a linear differential operator with constant coefficients. This operator is obtained by simply replacing x_i by the differential operator $\frac{\partial}{\partial x_i}$. Every ideal I in $\mathbb{R}[x_1, x_2, \ldots, x_n]$ can thus we interpreted as a system of linear partial differential equations (PDE) with constant coefficients. Suppose we are interested in the solutions to these PDE within some nice class of functions, like polynomial functions, real analytic functions $\mathbb{R}^n \to \mathbb{R}$, or complex holomorphic functions $\mathbb{C}^n \to \mathbb{C}$. Then the set of solutions to our PDE is a linear space over $\mathbb{R}$ or $\mathbb{C}$. We are interested in computing a basis for that solutions space. This computation rests on the primary decomposition of the ideal I. Both minimal primes and embedded primes will play a role, and all primary components will contribute to our basis for the solution space.

We shall explain this for the ideal $I = \langle x^3 - yz, y^3 - xz, z^3 - xy\rangle$, seen in Exercise 8 of the first lecture (April 10) of the Ringvorlesung. The corresponding system of PDE equals

$$\frac{\partial^3 f}{\partial x^3} = \frac{\partial^2 f}{\partial y \partial z} \qquad \text{and} \qquad \frac{\partial^3 f}{\partial y^3} = \frac{\partial^2 f}{\partial x \partial z} \qquad \text{and} \qquad \frac{\partial^3 f}{\partial z^3} = \frac{\partial^2 f}{\partial x \partial y}. \tag{1}$$

We seek all holomorphic functions $f : \mathbb{C}^3 \to \mathbb{C}$ that satisfy these equations, and among these, we seek all real analytic solutions $f : \mathbb{R}^3 \to \mathbb{R}$, and especially all polynomial solutions.

The Bézout number of our ideal I is $27 = 3 \times 3 \times 3$, which comes from the degrees of the three generators of I. The number 27 is also the dimension of the space of holomorphic solutions f to (1). A basis of that solution space is given by the following 27 functions:

$$\begin{gathered} 1\,,\, x\,,\, y\,,\, z\,,\, x^2\,,\, y^2\,,\, z^2\,,\, x^3+6yz\,,\, y^3+6xz\,,\, z^3+6xy\,,\, x^4+y^4+z^4+24xyz\,, \\ \exp(x-y-z)\,,\;\; \exp(x+y+z)\,,\;\; \exp(-x-y+z)\,,\;\; \exp(-x+y-z)\,, \\ \exp(x-iy+iz)\,, \exp(x+iy-iz)\,, \exp(-x-iy-iz)\,, \exp(-x+iy+iz)\,, \\ \exp(ix-y+iz)\,, \exp(ix+y-iz)\,, \exp(ix-iy+z)\,, \exp(ix+iy-z)\,, \\ \exp(-ix-y-iz)\,, \exp(-ix+y+iz)\,, \exp(-ix-iy-z)\,, \exp(-ix+iy+z). \end{gathered} \tag{2}$$

The space of polynomial solution has dimension 11 and is spanned by the first row. The space of real analytic solutions has dimension 15 and is spanned by the first two rows. All other basis functions are exponentials of linear forms that have $i = \sqrt{-1}$ among its coefficients.

This basis of solutions in (2) was derived from the primary decomposition of our ideal:

$$I \quad = \quad Q \;\cap \bigcap_{\substack{a+b+c \,\equiv\, 0 \\ \bmod 4}} \big\langle\, x - i^a,\, y - i^b,\, z - i^c \,\big\rangle \qquad \text{in } \mathbb{C}[x,y,z].$$

The 16 ideals in the intersection on the right hand side are maximal and hence prime. They correspond to the 16 exponential solutions in (2). The ideal Q is primary to the maximal ideal $\sqrt{Q} = \langle x,y,z\rangle$. Since all associated primes are minimal, this primary ideal is unique:

$$Q \;=\; \big\langle\, x^2y, x^2z, xy^2, xz^2, y^2z, yz^2, x^3-yz, y^3-xz, z^3-xy \,\big\rangle.$$

This ideal has length 11, and it contributes the 11 polynomial solutions to our PDE.

We next consider an ideal that has an embedded component. Let $n = 4$ and consider

$$J \;=\; \langle\, xw,\, xz + yw,\, yz\rangle.$$

The ideal J as three associated primes. The primes $\langle x,y\rangle$ and $\langle z,w\rangle$ are minimal primes, and the maximal ideal $\langle x,y,z,w\rangle$ is an embedded prime. A primary decomposition is given by

$$J \;=\; \langle x,y\rangle \;\cap\; \langle z,w\rangle \;\cap\; (J + \langle x,y,z,w\rangle^3).$$

The third primary component is embedded. It is not unique. We can replace the third power of the maximal ideal by any higher power and get the same intersection.

The radical of the ideal J is the intersection of the two minimal primes:

$$\sqrt{J} \;=\; \langle x,y\rangle \,\cap\, \langle z,w\rangle \;=\; \langle xw, xz, yw, yz\rangle.$$

We now interpret the generators of J as a system of linear PDE with constant coefficients:

$$\frac{\partial^2 f}{\partial x \partial w} \;=\; \frac{\partial^2 f}{\partial x \partial z} + \frac{\partial^2 f}{\partial y \partial w} \;=\; \frac{\partial^2 f}{\partial y \partial z} \;=\; 0.$$

The linear space of solutions is infinite-dimensional. It is spanned by all functions of the form $g(y,z)$ and $h(x,y)$, together with the one special function $xz - yw$. The former correspond to the two minimal primes, whereas the latter arises from the embedded primary component.

Whenever one encounters a system of polynomial equations with special structure, and one is curious about the variety of solutions, it pays to explore the primary decomposition. This decomposition often reveals interesting structures, and it tells us how to break up the solutions into meaningful pieces. As an illustration consider the following question. *Let A, B, C be 2×2-matrices. How is it possible that the triple product ABC is the zero matrix?*

We approach this problem as follows. We set $n = 12$ and we consider the polynomial ring $\mathbb{R}[a_{ij}, b_{ij}, c_{ij}]$ whose variables are the 12 entries of the matrices A, B, C. Let K be the ideal of $\mathbb{R}[a_{ij}, b_{ij}, c_{ij}]$ that is generated by the four entries of the matrix product ABC.

A computation reveals that K is a radical ideal, and that K is the intersection of six prime ideals. Three of them are ideals generated by the entries of A or B or C respectively. The next two minimal primes are generated respectively by the 2×2 minors of the matrices

$$\begin{pmatrix} a_{11} & a_{21} & -b_{21} & -b_{22} \\ a_{12} & a_{22} & b_{11} & b_{12} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} b_{11} & b_{21} & -c_{21} & -c_{22} \\ b_{12} & b_{22} & c_{11} & c_{12} \end{pmatrix}.$$

Finally, the last associated prime of K is the ideal $K + \langle \det(A), \det(B)\rangle$. One checks with a computer algebra system that our ideal K is the intersection of these six prime ideals.

Geometrically, we have studied the variety $V(K)$ which is defined by four cubic equations and which lives in $\mathbb{C}^{12}$. It is the union of six irreducible components. Three of them are linear spaces of dimension 8. The other three irreducible components have dimension 9 and they are not linear spaces. Their degrees are $4, 4$ and 8 respectively. In terms of the original linear algebra question, the six irreducible components correspond to the following six cases:

$$\begin{gathered} \mathrm{rank}(A) = 0 \quad \text{or} \quad \mathrm{rank}(B) = 0 \quad \text{or} \quad \mathrm{rank}(C) = 0 \quad \text{or} \\ \mathrm{rank}(A) = \mathrm{rank}(B) = 1 \quad \text{or} \quad \mathrm{rank}(B) = \mathrm{rank}(C) = 1 \quad \text{or} \quad \mathrm{rank}(A) = \mathrm{rank}(C) = 1. \end{gathered}$$

As always, taking a fresh look at linear algebra offers a point of entry to nonlinear algebra.

Exercises

1. Consider the ring $\mathbb{C}[x,y]/(x^2, xy, y^2)$. Is (0) an irreducible ideal? Is it primary?

2. a) Prove that intersection of prime ideals is radical.

   b)* Prove the opposite implication. Hint: Apply Kuratowski-Zorn lemma.

3. Prove that an ideal $I \subsetneq \mathbb{Z}$ is a power of a prime ideal if and only if it is primary.

4. Prove that a ring is Noetherian if and only if every ideal is finitely generated.

5. a) Prove that if R is Noetherian, then so is R/I for any ideal I.

   b) Prove Hilbert Basis Theorem: If R is Noetherian, then so is $R[x]$.

6. Prove Lemma 5

7. Check that Example 9 provides two distinct minimal primary decompositions.

8. a) Prove that a prime ideal p cannot be equal to an intersection of (finitely many, more than one, incomparable) ideals.

   b) More generally prove that if a prime ideal contains an intersection of finitely many ideals, then it contains one of them.

9. Prove that in a Noetherian ring every ideal contains a power of its radical. Give a counterexample in case of a non-Noetherian ring.

References

[1] M.F. Atiyah and I.G. Macdonald: *Introduction to Commutative Algebra.*

[2] D. Cox, J. Little and D. O'Shea: *Ideals, Varieties, and Algorithms.* An introduction to computational algebraic geometry and commutative algebra, Third edition, Undergraduate Texts in Mathematics, Springer, New York, 2007.