21MAB143 Rings and Polynomials: Weeks 10–11

1 Prime and maximal ideals in $K[x_1, \ldots, x_n]$

This week we will explore the connections between irreducible polynomials, prime ideals, and maximal ideals, in the context of multi-variable polynomial rings. We will see that the story is not quite as neat as in the one-variable case, but nevertheless all these objects are closely connected.

At several places in this week's notes we will skip proofs or give sketch proofs as needed so that we can present the main results more clearly. On a first reading, the main thing to focus on is the statements of the main results and how they are illustrated in the examples.

We begin with the following lemma.

Lemma 1.1. *Let $f \in K[x_1, \ldots, x_n]$ be an irreducible polynomial. If $g, h \in K[x_1, \ldots, x_n]$ are any two polynomials such that $f \mid gh$, then $f \mid g$ or $f \mid h$.*

We will not prove this, but we mention that it is closely related to the fact that $K[x_1, \ldots, x_n]$ is a **unique factorisation domain** (UFD). We will come back to this next week. The lemma is an important ingredient in the next result:

Theorem 1.2. *Let $f \in K[x_1, \ldots, x_n]$ be a nonconstant polynomial. Then the ideal $\langle f \rangle$ is prime if and only if f is irreducible in $K[x_1, \ldots, x_n]$.*

Proof. The proof of the implication "$\langle f \rangle$ is prime implies f is irreducible" is essentially identical to the proof of the corresponding implication in Week 9 Theorem 2.2, but for completeness we give it again here. Suppose that f is a nonconstant polynomial in $K[x_1, \ldots, x_n]$ and that the ideal $\langle f \rangle$ is prime. We want to show that f is irreducible in $K[x_1, \ldots, x_n]$. Note that f is nonconstant, so it is not a unit in $K[x_1, \ldots, x_n]$. So suppose that $f = gh$: we must show that either g or h is constant.

Now since $\langle f \rangle$ is prime and $gh = f \in \langle f \rangle$, either g or h must be an element of $\langle f \rangle$. By renaming if necessary, assume $g \in \langle f \rangle$. Then $g = fp$ for some polynomial p. Hence

$$\begin{aligned} f &= gh \\ &= fph \end{aligned}$$

This means that both p and h are nonzero constant polynomials.

For the converse implication, suppose that f is irreducible, and suppose that $gh \in \langle f \rangle$. We want to prove that $g \in \langle f \rangle$ or $h \in \langle f \rangle$. Now $\langle f \rangle$ is exactly the set of all polynomials in $K[x_1, \ldots, x_n]$ that are divisible by f. So $gh \in \langle f \rangle$ means that $f \mid gh$. By Lemma 1.1 this implies that $f \mid g$ or $f \mid h$, in other words $g \in \langle f \rangle$ or $h \in \langle f \rangle$.

□

Example: However, in contrast with the case of one variable, in the ring $K[x_1, \ldots, x_n]$ a prime ideal need **not** be maximal. Let's look at a simple example to see why not.

In $\mathbf{C}[x, y]$ consider a linear polynomial

$$f = ax + by + c$$

where a, b, c are complex numbers with a and b not both zero. If we have $f = gh$ for two polynomials g and h, then since f has degree 1 we see that either g or h must be constant. So f is irreducible in $\mathbf{C}[x, y]$.

Theorem 1.2 therefore tells us that the ideal $\langle ax + by + c \rangle$ is prime. However, it is not maximal, as we will now see.

Suppose that a is nonzero. (If a is zero, then b must be nonzero, and the argument is exactly analogous with the roles of x and y reversed.) Consider the ideal

$$J = \langle ax + by + c, y \rangle$$

Then $\langle ax + by + c \rangle \subseteq J$. I claim that

(a) $\langle ax + by + c \rangle \neq J$;

(b) $J \neq \mathbf{C}[x, y]$.

Together these show that $\langle ax + by + c \rangle$ is not maximal.

To prove (a), observe that if $f \in \langle ax + by + c \rangle$ then $f = (ax + by + c) \cdot p$ for some polynomial p; since $a \neq 0$, this means that f contains at least one term in which the exponent of x is greater than 0. In particular $y \notin \langle ax + by + c \rangle$. On the other hand $y \in J$ by definition, so this shows $\langle ax + by + c \rangle \neq J$.

To prove (b), recall that every polynomial in the ideal $J = \langle ax + by + c, y \rangle$ has the form

$$f \cdot (ax + by + c) + g \cdot y$$

for some polynomials f, $g \in \mathbf{C}[x, y]$. If $J = \mathbf{C}[x, y]$ then we could choose f and g such that

$$f \cdot (ax + by + c) + g \cdot y = 1$$

Evaluating the polynomial on the left-hand side at the point $(-\frac{c}{a}, 0) \in \mathbf{C}^2$ we get 0, while evaluating the constant polynomial 1 at that point we get 1. This is a contradiction, and therefore $J \neq \mathbf{C}[x, y]$ as required.

In fact, in the case when $K = \mathbf{C}$, the complex numbers, we can give a complete description of maximal ideals in $\mathbf{C}[x_1, \ldots, x_n]$, as follows.

Theorem 1.3. *An ideal* $I \subseteq \mathbf{C}[x_1, \ldots, x_n]$ *is maximal if and only if it can be written in the form*

$$I = \langle x_1 - z_1, \ldots, x_n - z_n \rangle$$

for some complex numbers $z_1, \ldots, z_n$.

This is part of the theorem known as "Hilbert's Nullstellensatz" which is a basic result in algebraic geometry. You will learn more about this if you take the Part C Algebraic Geometry module. The full proof uses a result known as "Zariski's Lemma" which we won't go into here, but we can give a fairly complete sketch proof as follows.

Sketch of proof. First let us prove that an ideal I of the form above is indeed maximal. To see this, recall from Week 9 Theorem 2.5 that it is enough to show that the quotient ring $\mathbf{C}[x_1, \ldots, x_n]/I$ is a field. Consider the evaluation homomorphism

$$\begin{aligned} \mathrm{ev} \colon \mathbf{C}[x_1, \ldots, x_n] &\to \mathbf{C} \\ p &\mapsto p(z_1, \ldots, z_n) \end{aligned}$$

If $f \in \mathbf{C}[x_1, \ldots, x_n]$ is any polynomial, we can write it in the form

$$f = a_0 + \sum_{i=1}^{n} f_i(x_i - z_i)$$

for some $a_0 \in \mathbf{C}$ and some polynomials f_i. So $\mathrm{ev}(f) = 0$ if and only if $a_0 = 0$, in other words if and only if $f \in I$. This shows that the kernel of the homomorphism ev is exactly the ideal I. Moreover ev is clearly surjective, and so the Ring Homomorphism Theorem shows that

$$\mathbf{C}[x_1, \ldots, x_n]/I \cong \mathbf{C}$$

Since $\mathbf{C}$ is a field, this shows I is maximal as claimed.

To prove the converse, suppose that $I \subseteq \mathbf{C}[x_1, \ldots, x_n]$ is a maximal ideal. Then by Week 9 Theorem 2.5 the quotient ring $\mathbf{C}[x_1, \ldots, x_n]/I$ is a field K. A result known as "Zariski's Lemma" shows that in fact K must be isomorphic to $\mathbf{C}$. So we consider the quotient map

$$q \colon \mathbf{C}[x_1, \ldots, x_n] \to \mathbf{C}[x_1, \ldots, x_n]/I \cong \mathbf{C}$$

Recall that $\mathrm{Ker}(q) = I$.

Now for each i let $z_i = q(x_i)$. Then $q(x_i - z_i) = z_i - z_i = 0$, so the kernel of q contains each of the polynomials $x_i - z_i$. Hence

$$\langle x_1 - z_1, \ldots, x_n - z_n \rangle \subseteq \mathrm{Ker}(q) = I$$

But we saw in the first part of the proof that the ideal on the left-hand side is maximal, so in fact we must have $I = \langle x_1 - z_1, \ldots, x_n - z_n \rangle$. □

Warning: Notice that Theorem 1.2 is true for polynomials over any field K, whereas Theorem 1.3 is stated **only** for the complex numbers. Theorem 1.3 is not true for polynomials over $\mathbf{R}$ or $\mathbf{Q}$: for example, we already saw that $\left\langle x^2+1\right\rangle \subseteq \mathbf{R}[x]$ is maximal, but it is not of the form stated in the theorem.

Warning: A given ideal in K[x] can be generated by many different sets of polynomials. So it is possible that an ideal $I = \langle f_1, \dots, f_k\rangle$ is maximal even if the polynomials f_i don't have the form written in the statement of Theorem 1.3. For example, the ideal

$$I = \left\langle x - y^2, y\right\rangle \subseteq \mathbf{C}[x, y]$$

is maximal, even though $x - y^2$ is not a linear polynomial. The theorem says that if I is maximal, then **there exists** a set of generators of I that have the stated form. In this example, you can check that

$$\begin{aligned} I &= \left\langle x - y^2, y\right\rangle \\ &= \langle x, y\rangle \end{aligned}$$

and the second set of generators are of the form stated in the theorem.

Finally we mention (without proof) one more connection between prime and maximal ideals in $K[x_1, \dots, x_n]$. Although not every prime ideal is maximal, as we have seen, it is still the case that every prime ideal is an **intersection** of maximal ideals. This is usually known as the **Jacobson property**:

Theorem 1.4 (Jacobson property of polynomial rings). *Let* $I \subseteq K[x_1, \dots, x_n]$ *be a prime ideal. Then*

$$I = \bigcap \{J \mid I \subseteq J,\ J \textit{ maximal}\}$$

That is, I *is equal to the intersection of all maximal ideals containing* I.

1.1 Example

In the polynomial ring $\mathbf{C}[x, y]$ consider the polynomials

$$\begin{aligned} f &= y - x^2 \\ g &= x - y^2 \end{aligned}$$

Note that both f and g are irreducible polynomials in $\mathbf{C}[x, y]$, so the ideals $\langle f\rangle$ and $\langle g\rangle$ are prime.

However, the ideal $I = \langle f, g\rangle$ is **not** prime. To see this, we need to find polynomials p and q (say) such that $pq \in I$ but $p \notin I$ and $q \notin I$. To find these p and q, note that I contains the polynomial

$$\begin{aligned} y \cdot f + g &= y(y - x^2) + (x - y^2) \\ &= x - x^2 y \\ &= x(1 - xy) \end{aligned}$$

Claim: neither x nor $1 - xy$ is in I. (So these are the polynomials p and q we need!)

To prove the claim, we use the fact that every element of I can be written in the form

$$af + bg$$

for some polynomials a, $b \in \mathbf{C}[x, y]$. Now we argue as follows:

- If $x \in I$, then there exists a, b such that

  $$x = af + bg.$$

  The trick is to notice that $f(1, 1) = g(1, 1) = 0$, whereas $x(1, 1) = 1$. So it is not possible to write x in the form $x = af + bg$.

- If $1 - xy$ in I, then again there exist a, b such that

  $$1 - xy = af + bg.$$

  In this case we note that $f(0, 0) = g(0, 0) = 0$, whereas $(1 - xy)(0, 0) = 1$. So again this is impossible.

So we conclude that $x \notin I$ and $1 - xy \notin I$ but

$$x(1 - xy) \in I.$$

This shows I is not prime.

Addendum: Let $h = (x - 1)(y + 1)$. This polynomial is reducible, so $\langle h \rangle$ is not prime. But on Problem Sheet 10 you will show that

$$\langle f, g, h \rangle = \langle x - 1, y - 1 \rangle .$$

This ideal is maximal, hence prime.

This example shows again that sets of generators for maximal ideals are not unique: here the 3 polynomials f, g, h, each of degree 2, generate the same (maximal) ideal as the 2 linear polynomials $x - 1$ and $y - 1$.

2 Algebraic sets corresponding to prime and maximal ideals

In Week 5 we defined the algebraic set $V(I)$ corresponding to an ideal $I \subseteq K[x_1, \ldots, x_n]$ as follows:

$$V(I) = \{(a_1 \ldots, a_n) \in K^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}$$

In this section, we will explore some connections between properties of the ideal I and the structure of the set $V(I)$. We stick to the case $K = \mathbf{C}$ for the rest of this section.

We start with maximal ideals. Here the corresponding algebraic sets are as simple as possible: they are single points.

Proposition 2.1. *Let $I \subset \mathbf{C}[x_1, \ldots, x_n]$ be a maximal ideal. Then*

$$V(I) = \{(z_1, \ldots, z_n)\},$$

a single point in $\mathbf{C}^n$.

Proof. This follows from Theorem 1.3. That theorem says that I is maximal if and only if it has the form

$$I = \langle x_1 - z_1, \ldots, x_n - z_n \rangle$$

for some complex numbers $z_1, \ldots, z_n$, and for this ideal it is clear that the only point of $V(I)$ is $(z_1, \ldots, z_n)$. □

To explore algebraic sets defined by prime ideals, we need some prepatory results.

Lemma 2.2. *(i) For ideals I and J in $\mathbf{C}[x_1, \ldots, x_n]$, if $I \subseteq J$ then $V(J) \subseteq V(I)$.*

(ii) For an ideal I and a maximal ideal $J = \langle x_1 - z_1, \ldots, x_n - z_n \rangle$, we have $I \subseteq J$ if and only if the point $(z_1, \ldots, z_n)$ is in the set $V(I)$.

Proof. (i): Suppose $I \subseteq J$. Let $p \in V(J)$. Then $f(p) = 0$ for all $f \in J$. In particular $f(p) = 0$ for all $f \in I$. So $p \in V(I)$. This shows $V(J) \subseteq V(I)$.

(ii): Now suppose $J = \langle x_1 - z_1, \ldots, x_n - z_n \rangle$ is a maximal ideal. Then $V(J) = \{(z_1, \ldots, z_n)\}$. By Part (i), if $I \subseteq J$ then $(z_1, \ldots, z_n) \in V(I)$. Conversely, if I is not contained in J, choose an element $f \in I \setminus J$. The ideal J consists of all polynomials which are zero at $(z_1, \ldots, z_n)$, so this means $f(z_1, \ldots, z_n) \neq 0$. Therefore $(z_1, \ldots, z_n) \notin V(I)$. □

Now we can try to describe the algebraic sets corresponding to prime ideals. For this we need the following definition.

Definition 2.3. *Let $V(I)$ be the algebraic set in K^n defined by an ideal $I \subseteq K[x_1, \dots, x_n]$. We say $V(I)$ is* **irreducible** *if it cannot be written in the form*

$$V(I) = V(I_1) \cup V(I_2)$$

where I_1, I_2 are ideals in $K[x_1, \dots, x_n]$ such that neither of the sets $V(I_1)$ nor $V(I_2)$ is contained in the other.

Roughly speaking, the definition says that $V(I)$ is irreducible if it can't be "broken up" into two smaller algebraic subsets.

Our main result is then the following.

Theorem 2.4. *If the ideal $I \subset \mathbf{C}[x_1, \dots, x_n]$ is prime, then the algebraic set $V(I)$ is irreducible.*

Proof of Theorem 2.4. Suppose I is prime and suppose $V(I) = V(I_1) \cup V(I_2)$ for some ideals I_1 and I_2. We want to show that one of these algebraic sets must be contained in the other. Let us suppose not and obtain a contradiction.

So suppose neither $V(I_1)$ nor $V(I_2)$ is contained in the other. Then there are points $p \in V(I_1) \setminus V(I_2)$ and $q \in V(I_2) \setminus V(I_1)$. Therefore there are polynomials $f \in I_1$ and $g \in I_2$ such that $f(q) \neq 0$ and $g(p) \neq 0$. So neither f nor g belongs to I (because polynomials in I are zero at every point of $V(I)$, in particular at both p and q).

On the other hand, since $f(x) = 0$ for every point $x \in V(I_1)$ and $g(x) = 0$ for every point $x \in V(I_2)$, the polynomial fg is zero at every point of $V(I_1) \cup V(I_2) = V(I)$. In other words, $(fg)(z_1, \dots, z_n) = 0$ for all points $(z_1, \dots, z_n) \in V(I)$. Equivalently, we can say

$$fg \in \langle x_1 - z_1, \dots, x_n - z_n \rangle$$

for every $(z_1, \dots, z_n) \in V(I)$. But by Lemma 2.2, these are exactly the maximal ideals that contains I. Since fg belongs to each of them, it belongs to their intersection, which by Theorem 1.4 is exactly I. So we get $fg \in I$, contradicting the facts that $f \notin I$ and $g \notin I$ and I is prime. □

Corollary 2.5. *If $f \in K[x_1, \dots, x_n]$ is irreducible, then the algebraic set $V(\langle f \rangle)$ is irreducible.*

Proof. By Theorem 1.2 if f is irreducible, then the ideal $\langle f \rangle$ is prime. By Theorem 2.4 this implies that the algebraic set $V(\langle f \rangle)$ is irreducible. □

Remark: A bit disappointingly, the converse of Theorem 2.4 is not quite true: if $V(I)$ is irreducible it is not necessarily the case that I is prime. (Problem Sheet 10 will ask you to give an example). The correct statement, which is a bit more complicated, is part of "Hilbert's Nullstellensatz" as mentioned previously.

2.1 Example

Let's return to the example from Section 1.1. Here we had the polynomials

$$\begin{aligned} f &= y - x^2 \\ g &= x - y^2 \end{aligned}$$

and we proved that the ideal $I = \langle f, g \rangle$ is not prime. Using Theorem 2.4 we can now give an alternative explanation of this fact, by showing that the algebraic set $V(I)$ is not irreducible.

Let $(a_1, a_2) \in \mathbf{C}^2$ be a point in the algebraic set $V(I)$. Then we have

$$\begin{aligned} f(a_1, a_2) &= 0 \\ g(a_1, a_2) &= 0 \end{aligned}$$

which gives

$$\begin{aligned} a_2 - a_1^2 &= 0 \\ a_1 - a_2^2 &= 0. \end{aligned}$$

Putting these two together we get $a_1 = a_1^4$, so the possibilities are:

$$\begin{aligned} a_1 &= 0, a_2 = 0 \\ a_1 &= 1, a_2 = 1 \\ a_1 &= \omega, a_2 = \omega^2 \\ a_1 &= \omega^2, a_2 = \omega^4 = \omega \end{aligned}$$

(Here $\omega = \exp(2\pi i/3)$, a cube root of 1.)

Note that each of these pairs (a_1, a_2) satisfies $f(a_1, a_2) = g(a_1, a_2) = 0$. So $V(I)$ consists of 4 points:

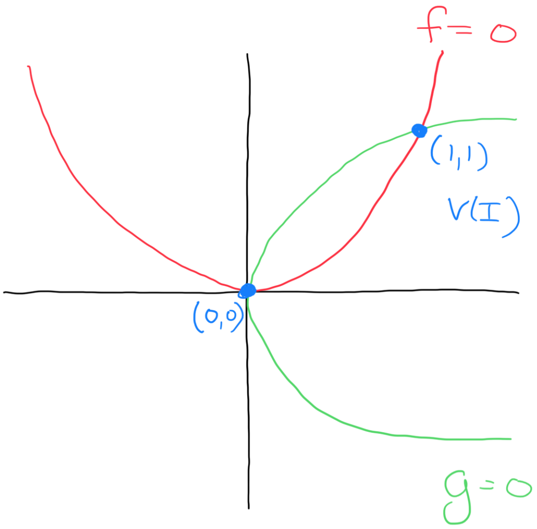
$$V(I) = \left\{(0,0), (1,1), (\omega, \omega^2), (\omega^2, \omega)\right\}$$

Note that each of the 4 points is itself an algebraic set:

$$\begin{aligned} \{(0,0)\} &= V(I_1) \quad \text{where } I_1 = \langle x, y \rangle \\ \{(1,1)\} &= V(I_2) \quad \text{where } I_2 = \langle x-1, y-1 \rangle \\ \left\{(\omega, \omega^2)\right\} &= V(I_3) \quad \text{where } I_3 = \left\langle x-\omega, y-\omega^2 \right\rangle \\ \left\{(\omega^2, \omega)\right\} &= V(I_4) \quad \text{where } I_4 = \left\langle x-\omega^2, y-\omega \right\rangle \end{aligned}$$

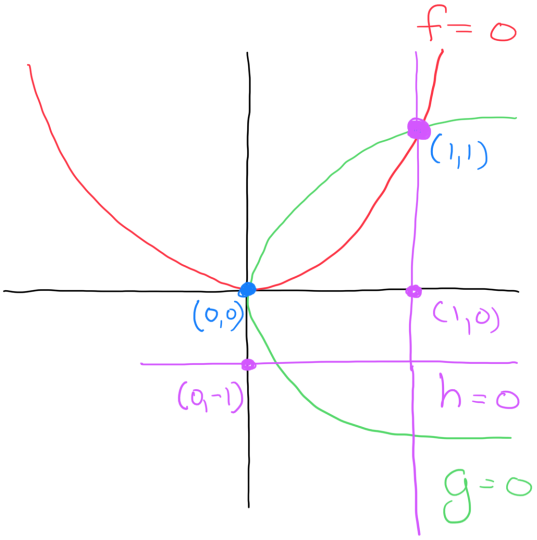
So $V(I) = V(I_1) \cup V(I_2) \cup V(I_3) \cup V(I_4)$.None of the sets $V(I_k)$ is contained in any other one, so this shows that $V(I)$ is not irreducible, and hence I is not prime.

Let's look at the picture of these sets to get another view of what is going on. The algebraic set $V(I)$ is the intersection of the curves $f = 0$ and $g = 0$. The picture below shows two of its irreducible components, the points $V(I_1) = \{(0,0)\}$ and $V(I_2) = \{(1,1)\}$. (The other two points have non-real coordinates, so are not visible in this picture.)



Finally, we can also consider how the polynomial $h = (x-1)(y+1)$ from Section 1.1 fits into the picture. We saw that the ideal $J = \langle f, g, h \rangle$ is maximal, so by Proposition 2.1 the corresponding algebraic set $V(J)$ should just consist of a single point.

The set $V(J)$ can be obtained as the set of common zeroes of the polynomials f, g, and h. The zero set of h is the union of the lines $\{a_1 = 1\}$ and $\{a_2 = -1\}$, shown in purple in the picture below. We see that indeed it only contains one of the two blue points from the previous picture, namely the point $(1, 1)$.



2.2 Another Example

This example is taken from the 20MAB143 Sample Exam available on Learn.

Problem: *Show that in the ring* $\mathbf{C}[x, y]$ *the ideal*

$$I = \langle x + 2, 5y + xy - 3\rangle$$

is maximal, and find the algebraic set $V(I)$*.*

By Theorem 1.3 we know that maximal ideals in $\mathbf{C}[x, y]$ have the form $\langle x - z_1, y - z_2\rangle$ for some complex numbers a and b. So to prove that I is maximal, we should show that I can be written in this form for some z_1 and z_2.

Suppose that we have a polynomial $f \in I$. Since I is generated by $x + 2$ and $5y + xy - 3$, this means by defintion that f can be written in the form

$$f = a(x + 2) + b(5y + xy - 3)$$

for some polynomials a and b. But we can rewrite this in the following way: if we write x as $(x + 2) - 2$ we get

$$\begin{aligned} f &= a(x + 2) + b(5y + ((x + 2) - 2)y - 3) \qquad (*)\\ &= (a + by)(x + 2) + b(3y - 3) \\ &= (a + by)(x + 2) + 3b(y - 1) \end{aligned}$$

which is an element of the maximal ideal $\langle x + 2, y - 1\rangle$. This shows that

$$I \subseteq \langle x + 2, y - 1\rangle \, .$$

Since the right-hand side is a maximal ideal, if I is maximal it must equal the right-hand side.

To prove this, we need to prove the reverse inclusion $\langle x + 2, y - 1\rangle \subseteq I$. Then we will have that each of the ideals I and $\langle x + 2, y - 1\rangle$ is contained in the other, hence they must be equal.

So let's prove the inclusion $\langle x + 2, y - 1\rangle \subseteq I$. By definition of I, we know that $x + 2 \in I$, so it is enough to show $y - 1 \in I$. That is, we have to find polynomials α and β such that

$$y - 1 = \alpha(x + 2) + \beta(5y + xy - 3).$$

To do this, let's go back to the equations $(*)$ and put $f = 5y + xy - 3$. Then in the first line, clearly we have $a = 0$ and $b = 1$. Inserting these values in the last line, we get the equation

$$5y + xy - 3 = y(x + 2) + 3(y - 1)$$

which we can rearrange to give

$$y - 1 = -\frac{y}{3}(x + 2) + \frac{1}{3}\left(5y + xy - 3\right).$$

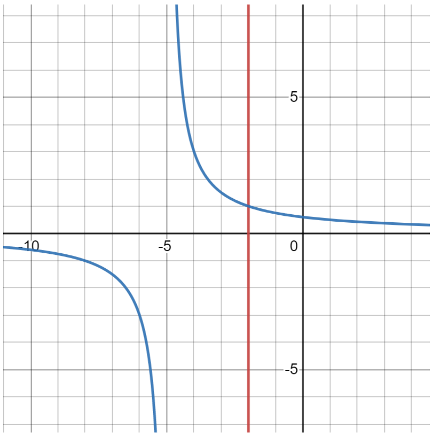
So the required polynomials are $\alpha = -\frac{y}{3}$ and $\beta = \frac{1}{3}$. We have shown that $y - 1 \in I$, and therefore

$$I = \langle x + 2, y - 1 \rangle .$$

As explained in the proof of Proposition 2.1, the associated algebraic set consists of a single point:

$$V(I) = \{(-2, 1)\} .$$

Finally let's look at the picture:



Here the red vertical line is the zero set of the generator $x + 2$, and the blue hyperbola is the zero set of the generator $5y + xy - 3$, and we see that indeed these curves have only 1 intersection point at $(-2, 1)$. (Since the hyperbola has a vertical asymptote $x = -5$, we can be sure that there is no other intersection point somewhere beyond the edge of the picture.)