8 Elimination of variables

Example 10 We checked several times that $y^2 - x^3 - x^2$ is in the ideal $I \subset k[t, x, y]$ generated by $x - t^2 - 1$ and $y - t^3 - t$. At the time, we were interested in finding any polynomial involving only $x, y$ in $I$. We could have phrased this as

$$y^2 - x^3 - x^2 \in I \cap k[x, y],$$

thinking of $k[x, y] \subset k[x, y, t]$ as a subring. In fact more is true, and we could have worked out that

$$I \cap k[x, y] = (y^2 - x^3 - x^2)$$

as an ideal in $k[x, y]$.

8.1 The image of a polynomial map

We will talk about maps between two affines spaces, so we decide on notation to distinguish source and target: let $k[x_1, \ldots, x_n]$ and $k[y_1, \ldots, y_m]$ be polynomial functions on $A^n_k$ and $A^m_k$ respectively.

A sequence of polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ determines a polynomial map

$$\varphi: A^n_k \rightarrow A^m_k$$

given by $a = (a_1, \ldots, a_n) \mapsto (f_1(a), \ldots, f_m(a))$. We want to compute the image of this map.

As stated, the map $\varphi$ determines a map $\varphi^*: k[y_1, \ldots, y_m] \rightarrow k[x_1, \ldots, x_n]$ of polynomial rings:

$$y_1 \mapsto f_1(x_1, \ldots, x_n), \ldots, y_m \mapsto f_m(x_1, \ldots, x_n).$$

(Of course, by implication $\varphi^*$ is a $k$-algebra homomorphism: to work out the image $\varphi^*(2x_1 + x_2x_3)$, you want to know that it equals $2\varphi^*(x_1) + \varphi^*(x_2)\varphi^*(x_3) = 2f_1 + f_2f_3$, which is the same as saying that $\varphi^*$ respects the $k$-algebra structures.)

Lemma 50 Let $\overline{\text{im}}\varphi$ be the Zariski closure of $\text{im} \varphi = \{\varphi(a) : a \in A^n_k\}$. Then $I(\overline{\text{im}}(\varphi)) = \ker \varphi^*$.

Proof This is trivial once you admit the two main points of definition. First, $I(\overline{\text{im}}\varphi)$ comprises exactly those polynomials that vanish on every image point by the definition of Zariski closure. Second, if $g \in k[y_1, \ldots, y_m]$ then $\varphi^*(g) = g(f_1, \ldots, f_m)$ is the polynomial in $x_1, \ldots, x_n$ made by substituting the $f_j$ in place of the $y_j$. Thus

$$g(\varphi(a)) = g(f_1(a), \ldots, f_m(a)) = (\varphi^*(g))(a)$$

for $g \in k[y_1, \ldots, y_m]$ and $a \in A^n_k$.

If $g \in \ker \varphi^*$, then

$$g(\varphi(a)) = g(f_1(a), \ldots, f_m(a)) = (\varphi^*(g))(a) = 0$$

1
because $\varphi^*(g)$ is the zero polynomial. Conversely, if $g$ vanishes at every point of $\mathrm{im}(\varphi)$, then
\[ 0 = g(\varphi(a)) = g(f_1(a), \ldots, f_m(a)) = (\varphi^*(g))(a). \]
But if $f \in k[x_1, \ldots, x_n]$ evaluates to zero at every $a \in A^n_k$, then $f$ is the zero polynomial because $k$ is an infinite field. Q.E.D.

The algorithm for computing the kernel of a polynomial map is a simple generalisation of the calculation in Example 8.

**Proposition 51** Let $\alpha: k[y_1, \ldots, y_m] \rightarrow k[x_1, \ldots, x_n]$ be a polynomial map defined by $y_i \mapsto f_i(x_1, \ldots, x_n)$ for polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$. Define an ideal
\[ I = (y_1 - f_1, \ldots, y_m - f_m) \]
in the bigger ring $k[y_1, \ldots, y_m, x_1, \ldots, x_n]$. Then $\ker \alpha = I \cap k[y_1, \ldots, y_m]$.

A word about the bigger ring $k[y_1, \ldots, y_m, x_1, \ldots, x_n]$. This contains $k[x_1, \ldots, x_n]$ and $k[y_1, \ldots, y_m]$ by the natural injections (implicit in the notation). But we also use the projection
\[ \bar{\alpha}: k[y_1, \ldots, y_m, x_1, \ldots, x_n] \rightarrow k[x_1, \ldots, x_n] \]
\[ y_i \mapsto f_i \]
\[ x_i \mapsto x_i \]
which covers $\alpha$. It is useful to observe now that if $g = g(x)$ is a polynomial in the bigger ring that does not involve the $y_i$ variables, then $\bar{\alpha}(g) = 0$ only if $g$ is already the zero polynomial.

**Proof** If $f \in I$ then it has the form $f = \sum p_i(y_i - f_i)$, so certainly it maps to zero under $\bar{\alpha}$ (that is, under $y_i \mapsto f_i$).

Give the big ring $k[y_1, \ldots, y_m, x_1, \ldots, x_n]$ the lex monomial order with every $y_i$ bigger than every $x_j$. (In fact, with this order, the given generators of $I$ form a Gröbner basis, although we do not use this fact.) Regard $f \in \ker \alpha$ as lying in $k[y_1, \ldots, y_m]$ inside the bigger ring. Then dividing by the given generators of $I$ gives
\[ f = \sum p_i(y_i - f_i) + r \]
where $r = r(x_1, \ldots, x_n)$ does not involve the $y_i$ variables since they are the leading terms of the polynomials $y_i - f_i$. Applying $\bar{\alpha}$ to the displayed equation for $f$ shows that $\bar{\alpha}(r) = 0$, so $r = 0$ by the comments before the proof and $f \in I$ as required. Q.E.D.

To complete the image calculation, we need to be able to intersect an ideal with a subring. This calculation is known as elimination of variables.
8.2 Elimination of variables

**Definition 52** Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. The $i$th elimination ideal $I_i$ of $I$ is the intersection

$$I_i = I \cap k[x_{i+1}, \ldots, x_n].$$

More generally, if $S \subset R$ is any subring and $I \subset R$ an ideal, then $I \cap S$ is an ideal of $S$ called the elimination ideal of $I$ with respect to $S$.

It is only by tradition (and lexicographical prejudice) that we eliminate the first variables: in applications we will choose which variables to eliminate carefully. You should check, Exercise 8.3, that $I_i$ and $I \cap S$ really are ideals as claimed.

**Theorem 53** Let $I \subset k[x_1, \ldots, x_n]$ be an ideal and $k \in \{1, \ldots, n\}$. Let $G$ be a Gröbner basis for $I$ for the lex order $> \cdot \cdot \cdot > x_n$. Then $G \cap k[x_{i+1}, \ldots, x_n]$ is a Gröbner basis for $I_i$ (for the induced lex monomial order).

**Proof** Let $G_i = G \cap k[x_{i+1}, \ldots, x_n]$. Certainly $G_i \subset I_i$. We show that it is a Gröbner basis for $I_i$, and so in particular it generates $I_i$.

If $f \in I_i$, then, regarding $f$ as an element of $I$ there is some $g \in G$ for which $LT(g)$ divides $LT(f)$. Since actually $f \in I_i$, we know that $LT(f) \in k[x_{i+1}, \ldots, x_n]$ and so the same is true of $LT(g)$. But in the given lex order, this means that every term of $g$ is also in $k[x_{i+1}, \ldots, x_n]$. This says that $g \in G_i$, which was what we had to prove. Q.E.D.

**Example 10 (continued)** Let $I = (x-t^2-1, y-t^3-t) \subset k[t, x, y]$. You compute that

$$t^2 - x + 1, \quad tx - y, \quad ty - x^2 + x, \quad x^3 - x^2 - y^2$$

is a Gröbner basis of $I$ with respect to lex order $t > x > y$. The theorem implies that $x^3 - x^2 - y^2$ generates the first elimination ideal.

**Algorithms**

Putting all these results together gives the computation of the (Zariski closure of the) image of a polynomial map between affine spaces.

**Algorithm 1 (Elimination algorithm)**

```plaintext```
input $I \subset k[x_1, \ldots, x_n], k \in \{1, \ldots, n\}$.
output Gröbner basis for $I \cap k[x_{k+1}, \ldots, x_n]$.

$G :=$ Gröbner basis for $I$ with respect to lex order with $x_1 > \cdots > x_n$;

Return those elements of $G$ lying in $k[x_{k+1}, \ldots, x_n]$.
```

Putting the elimination algorithm together with Proposition 51, we get an algorithm for computing the kernel of an algebra map between polynomial rings.

**Algorithm 2 (Kernel of $k$-algebra homomorphism)** Let $R = k[x_1, \ldots, x_n]$ and $S = k[y_1, \ldots, y_m]$. 3
Section 8.1 together with the kernel calculation above computes the image of a map \( \varphi : \mathbb{A}^n_k \to \mathbb{A}^m_k \) defined by polynomials (in the precise sense of finding a basis for \( I(\varphi(\mathbb{A}^n_k)) \)).

Algorithm 3 (Image of polynomial map)

\begin{itemize}
\item \textbf{input} \( f_1, \ldots, f_m \in k[x_1, \ldots, x_n] \) giving a map \( \varphi : \mathbb{A}^n_k \to \mathbb{A}^m_k \).
\item \textbf{output} Gröbner basis for \( I(\varphi(\mathbb{A}^n_k)) \subset k[y_1, \ldots, y_m] \).
\item \textbf{start} \( I_\varphi := (y_1 - f_1, \ldots, y_m - f_m) \subset k[x_1, \ldots, x_n, y_1, \ldots, y_m] \);
\item \textbf{start} \( G := \text{Gröbner basis for } I_\varphi \cap k[y_1, \ldots, y_m] \) (Algorithm 1);
\end{itemize}

8.3 Intersection and union of algebraic sets

It is easy to see that unions and intersections of algebraic sets are also defined by polynomial equations. We will compare these set-theoretic operations with the suite of arithmetic operations on ideals. The algebra adds precision to the geometry, which becomes most clear when discussing primary decomposition. The machinery at the heart of everything is a combination of Gröbner basis and the use of **tag variables**, auxiliary variables such as Lagrange multipliers that must be eliminated at the end of a calculation.

Example 11 It is easy to compute \( V(xy, xz) \) as subsets of \( \mathbb{A}^3_k \): simply solve \( xy = xz = 0 \) to get \( (x = 0) \cup (y = z = 0) \) to get the union of the \( x \)-axis and the \( yz \)-plane. In terms of ideals, this expresses the fact that

\[(xy, xz) = (x) \cap (y, z) \subset k[x, y, z].\]

Thinking in terms of the usual algebra–geometry dictionary, this example has a union in geometry corresponding to an intersection in algebra. In fact, this works in general.

The first two arithmetic operations for ideals, addition and multiplication, are trivial. If \( I = (f_1, \ldots, f_r) \) and \( J = (g_1, \ldots, g_s) \) are ideals of \( R \), then

\[ I + J = \{ f + g : f \in I, g \in G \} = (f_1, \ldots, f_r, g_1, \ldots, g_s) \]

and

\[ I \cdot J = \{ fg : f \in I, g \in G \} = (\{ f_i g_j : i = 1, \ldots, r, j = 1, \ldots, s \}) \].

These two constructions are easy in algebra, and easy to interpret in geometry.

Lemma 54 \( V(I + J) = V(I) \cap V(J) \) and \( V(I \cdot J) = V(I) \cup V(J) \).
Proof This is easy. Q.E.D.

There are several more complicated operations in algebra which have geometric interpretations. The first of these is another way of computing the union of two algebraic sets: it is easy to check that

$$V(I) \cup V(J) = V(I \cap J).$$

Intersection of ideals can be computed using a lovely trick. Let $I, J$ be as above. Add a tag variable $t$ to the polynomial ring and eliminate $t$ from the ideal

$$N = (tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s) \subset k[x_1, \ldots, x_n, t] = R[t].$$

Lemma 55 With the notation of (1) above, $I \cap J$ is the elimination ideal $N \cap R$.

This is often written in shorthand as $I \cap J = (tI + (1-t)J) \cap R$.

Proof If $f \in I \cap J$ then $f = tf + (1-t)f \in N$. Conversely, if $f \in N$ then

$$f = f_I + f_J \quad \text{where} \quad f_I = f_I(x, t) \in tI \quad \text{and} \quad f_J = f_J(x, t) \in (1-t)J. \quad (2)$$

Notice that the left-hand side of (2) does not involve $t$ at all, whereas, at first sight, the right-hand side does. So we can set $t$ to any value and (2) will remain an equality that determines $f$. In particular, when $t = 0$,

$$f = f_I(x, 0) + f_J(x, 0) = f_J(x, 0) \in J \quad \text{since} \quad f_I \in tI,$$

while when $t = 1$

$$f = f_I(x, 1) + f_J(x, 1) = f_I(x, 1) \in I \quad \text{since} \quad f_J \in (t-1)J.$$

So $f \in I \cap J$ as required. Q.E.D.

Example 11 (continued) Let $I = (xy, xz)$ and $J = (y)$ in $x, y, z$ space $\mathbb{A}^3$. So $V(I)$ is the union of the $y, z$ plane and the $x$-axis, while $V(J)$ is the $x, z$ plane. Certainly $V(I) \cup V(J)$ is the union of two planes and both $I \cdot J$ and $I \cap J$ will be ideals that define it. But they are different ideals:

$$I \cdot J = (xy^2, xyz) \quad \text{while} \quad I \cap J = (xy)$$

since you can compute a lex Gröbner basis for $N$ with $t > x > y > z$ to be $(txz, ty - y, xy)$. One might regard the intersection as the better ideal representing the union of planes: indeed, it is clearly radical (and it is an easy exercise to see that, in general, the intersection of primary ideals is itself primary). On the other hand, when we look at primary decomposition we will see that

$$I \cdot J = (x) \cap (y) \cap (y, z)$$

so this ideal has remembered all the ingredients that went into the union. So, although we have two ways of computing $X \cup Y$, the two methods achieve different results, and which method you use depends upon what you want to know. ☻
Aside: Principal ideals and LCM times GCD The ring $R$ is not a Euclidean domain so given $f, g \in R$ there is no Euclidean algorithm for computing an expression $uf + vf = \gcd(f, g)$. Nevertheless, the GCD exists.

**Definition 56** Let $R = k[x_1, \ldots, x_n]$ and $f, g \in G$.

A polynomial $h \in R$ is a greatest common divisor (GCD) of $f, g$ if and only if $h$ divides both $f$ and $g$, and if $h_1 \in R$ also divides both $f, g$ then $h_1$ divides $h$.

A polynomial $h \in R$ is a least common multiple (LCM) of $f, g$ if and only if both $f$ and $g$ divide $h$, and if both $f, g$ divide $h_1 \in R$ then $h$ divides $h_1$.

**Lemma 57** Let $f, g \in R$.

1. LCM$(f, g)$ and GCD$(f, g)$ are well defined up to non-zero scalar multiple.
2. The ideal $(f) \cap (g)$ is principal and a generator is a LCM$(f, g)$.
3. The polynomial $(fg \div \text{LCM}(f, g)) \in R$ is a GCD$(f, g)$.

We use the notation GCD$(f, g)$ to denote any GCD and LCM$(f, g)$ to denote any LCM, keeping the ambiguity of (1) in mind. This is epitomised by the common abbreviation of (3) as LCM$(f, g)$ GCD$(f, g) = fg$, although we could be pedantic and acknowledge that this doesn’t make any sense.

**Proof** This is an algebra exercise. Q.E.D.

It is clear from the definition or the lemma that GCD$(x, y) = 1$ in the ring $k[x, y]$. Furthermore, there do not exist polynomials $u, v \in R$ such that $ux + vy = 1$.

**Exercises**

**Q.1.** Let $I = (x_1x_2 - x_3^2, x_1^2 - x_2x_3)$. Compute the first elimination ideal $I_1$.

**Q.2.** Let $\alpha : k[y_1, y_2, y_3] \to k[x_1, x_2]$ be the polynomial map defined by

$$\alpha(y_1) = x_1^3x_2, \quad \alpha(y_2) = x_1^2, \quad \alpha(y_3) = x_1x_2^2.$$

Show that ker$(\alpha) = (y_1^4 - y_2^5y_3^2) \subset k[y_1, y_2, y_3]$.

**Q.3.** Using the algorithms above, compute the radical ideal defining the Zariski closure of the image of the polynomial map $\varphi : \mathbb{R} \to \mathbb{R}^2$ defined by $\varphi^*(x) = t^3$ and $\varphi^*(y) = t^4$.

Why is $\overline{\text{im}(\varphi)} = \text{im}(\varphi)$ in this case?

**Q.4.** Being careful to say which ring you are working in, show that the elimination ideals $I_i$ and $I \cap N$ really are ideals.

**Q.5.** Show using the definition or Lemma 57 that GCD$(x, y) = 1$ in the ring $k[x, y]$. Show that there do not exist polynomials $u, v \in R$ such that $ux + vy = 1$. 6