Computational Algebra

0. An intersection

Let us consider two ideals in the ring of polynomials with rational coefficients, for example:

$$I_1 := (x_2, x_3) \subseteq \mathbb{Q}[x_0, x_1, x_2, x_3]$$

$$I_2 := (x_1, x_3 - x_0) \subseteq \mathbb{Q}[x_0, x_1, x_2, x_3]$$

Suppose we were asked (or, we asked ourselves), to compute the intersection $I := I_1 \cap I_2$. First of all, what does "to compute" mean in this context? This question may have different answers, depending on the goal we want to achieve and the tools we have at our disposal. For us "to compute" will mean "to produce a system of generators". In fact, once we know a system of generators of an ideal, we may in principle produce each and every element of the ideal, right? This is somehow true (if we had at our disposal infinite time or infinite computing power), and it would for example allow us to answer questions of the kind: "does this specific polynomial belong to that ideal?". We will see, during the course, that these aspects are actually quite subtle. But one step at a time, let us go back to our intersection.

One possible technique to exhibit a system of generators for

$$(x_2, x_3) \cap (x_1, x_3 - x_0)$$

is to start from a set of candidates and prove that they are enough to generate the whole ideal. How do we construct such candidates? We start from the general observation that

$$I_1 \cdot I_2 \subseteq I_1 \cap I_2$$

and that a set of generators for the product of two ideals is given by the set of all possible products of the generators of the ideals:

$$I_1 \cdot I_2 = (x_1x_2, x_1x_3, x_2x_3 - x_0x_2, x_3^2 - x_3x_0)$$

Immediately to our mind should come the thought: there is a situation when the product and the intersection of two ideals are equal, namely when the two ideals are comaximal:

Prop: let R be a commutative unitary ring, let $I_1, I_2 \subseteq R$ be ideals;
if $I_1 + I_2 = R$, then $I_1 \cdot I_2 = I_1 \cap I_2$

Unfortunately, this is not the case in our situation, because

$$1 \notin I_1 + I_2$$

simply for degree reasons (any polynomial in $I_1 + I_2$ must have degree at least one). However, it could still be the case that equality

holds also in our case. To prove that, we may try to use a technique that works very well for univariate polynomials, namely the one of division. Recall, in fact, that if we are given an ideal $J \subseteq \mathbb{Q}[x]$, then $J = (h)$ where h is any polynomial of smallest degree in J. The proof of this fact relies on the properties of division: if $f \in J$, then we can always write $f = q \cdot h + r$ with r of degree smaller than the degree of h; however, since $r = f - q \cdot h$, it follows that $r \in J$, and the minimality of the degree of h forces $r = 0$, thus showing that f is a multiple of h.

Can we apply the same technique here? First of all, since we are dealing with multivariate polynomials, we have to be aware that division does not always work. It does, however, when we can write a multivariate polynomial as a univariate one whose power of maximal degree has a constant term. In fact, we have the following fact.

Prop: let R be a commutative unitary ring, let $h \in R[x]$; then if the coefficient of the maximal power of x in h is invertible in R, then division by h can be performed as in the standard algorithm for polynomials with coefficients in a field.

By inspecting our candidates, we notice that one of them meets

the requirement, namely $x^3 - x_0 x_3$, which can be thought as a polynomial in x_3 with coefficients in $\mathbb{Q}[x_0, x_1, x_2]$.

So let us try to attack our problem.

Claim: the ideal $I := I_1 \cap I_2$ is generated by

$$x_1 x_2 \,,\; x_1 x_3 \,,\; x_2 x_3 - x_0 x_2 \,,\; x_3^2 - x_3 x_0$$

We hence pick $f \in I$, and we divide it by $x_3^2 - x_3 x_0$:

$$f = f_2 \cdot (x_3^2 - x_0 x_3) + f_1 x_3 + f_0 \qquad (*)$$

where $f_i \in \mathbb{Q}[x_0, x_1, x_2]$. Our goal is to make the other generator candidates "emerge" in the equality $(*)$. To do so, we should use the information we have about f, namely that it belongs to $I_1 \cap I_2$:

$$f = g_1 \cdot x_2 + g_2 \cdot x_3$$

$$f = h_1 \cdot x_1 + h_2 \,(x_3 - x_0)$$

with $g_i, h_i \in \mathbb{Q}[x_0, x_1, x_2, x_3]$. Hence

$$f_2 (x_3^2 - x_0 x_3) + f_1 x_3 + f_0 = g_1 x_2 + g_2 x_3$$

$$\Longrightarrow \quad x_3 \left((x_3 - x_0) f_2 + f_1 - g_2 \right) = -f_0 + g_1 x_2$$

Therefore x_3 must divide $-f_0 + g_1 x_2$. If we write

$$g_1 = x_3 \cdot \tilde{g}_1 + \hat{g}_1 \quad \text{with } \hat{g}_1 \in \mathbb{Q}[x_0, x_1, x_2]$$

then x_3 must divide $-f_0 + \tilde{g}_1 x_2$, but in the latter there is no x_3, therefore $-f_0 + \tilde{g}_1 x_2$, namely, f_0 is a multiple of x_2, $f_0 = \tilde{f}_0 x_2$.

So in (*) we can write

$$f = f_2 (x_3^2 - x_0 x_3) + \tilde{f}_1 x_3 + \tilde{\tilde{f}}_0 x_2$$

Some structure seems to start to emerge, but the path from here to writing f as a combination of x_1x_2, x_1x_3, $x_2x_3 - x_0x_2$, and $x_3^2 - x_0x_3$ is not clear yet, and the journey looks definitevely tedious.

When it is not so clear how to attack a problem, it may be of help to <u>change the problem</u> itself, and see if we have better luck.

In our case we may try to <u>simplify the situation</u> by noticing that the following homomorphism of rings:

$$\varphi : \mathbb{Q}[x_0, x_1, x_2, x_3] \longrightarrow \mathbb{Q}[x_0, x_1, x_2, x_3]$$

$$\begin{aligned} x_0 &\longmapsto x_3 - x_0 \\ x_1 &\longmapsto x_1 \\ x_2 &\longmapsto x_2 \\ x_3 &\longmapsto x_3 \end{aligned}$$

is actually an automorphism of $\mathbb{Q}[x_0, x_1, x_2, x_3]$ (<u>check this!</u>).

Therefore understanding the intersection of I_1 and I_2 is the same task as understanding the intersection of

$$J_1 := \varphi(I_1) \quad \text{and} \quad J_2 := \varphi(I_2)$$

The reason why this may help us is that

$$J_1 = I_1 \quad \text{but} \quad J_2 = (x_0, x_1)$$

We reduced our problem to an intersection of two ideals generated by <u>monomials</u>. The hope is that the richer structure of these objects will turn out to be useful. We notice that also their product is generated by monomials:

$$J_1 \cdot J_2 = (x_0x_2, x_0x_3, x_1x_2, x_1x_3)$$

The key observation here is that, if we denote $K := J_1 \cdot J_2$, then

$$K = \underbrace{(K, x_2)}_{= (x_2, x_0x_3, x_1x_3)} \cap \underbrace{(K, x_0)}_{= (x_0, x_1x_2, x_2x_3)} \qquad (\Delta)$$

In fact:

"$\subseteq$" this inclusion is clear by construction

"$\supseteq$" let $f \in (K, x_2) \cap (K, x_0)$, then

$$f = \lambda_1 x_2 + \mu_1 x_0x_3 + \nu_1 x_1x_3$$

$$= \lambda_2 x_0 + \mu_2 x_1x_2 + \nu_2 x_1x_3$$

the inclusion would be proved once we were able to show that λ_1 is divisible by x_0 or by x_1; notice that

$$\lambda_1 x_2 = -\mu_1 x_0x_3 + \lambda_2 x_0 + \mu_2 x_1x_2 + (\nu_2 - \nu_1) x_1x_3 \qquad (\square)$$

it is now sufficient to look at equality $(\square)$ in the quo=

tient $\dfrac{\mathbb{Q}[x_0,x_1,x_2,x_3]}{(x_0)} \cong \mathbb{Q}[x_1,x_2,x_3]$: in fact, if λ_1 is divisible by x_0, there is nothing to prove; if it is not, then the class of $\lambda_1 x_2$ is nonzero in $\mathbb{Q}[x_1,x_2,x_3]$ and, because of $(\square)$, it is a multiple of x_1; thus, we can always write $\lambda_1 = \tilde{\lambda}_1 x_0 + \hat{\lambda}_1 x_1$, which shows that the polynomial f belongs to K.

It follows that the equality (Δ) is correct. By repeating the same argument we get

$$K = \big((x_2, x_0, x_1x_3) \cap (x_2, x_3)\big) \cap \big((x_0, x_1) \cap (x_0, x_2, x_1x_3)\big)$$

$$= (x_2, x_3) \cap (x_0, x_1) \cap \underbrace{(x_0, x_2, x_1x_3)}$$

$$= (x_0, x_2, x_1) \cap (x_0, x_2, x_3)$$

$$= (x_2, x_3) \cap (x_0, x_1)$$

So we proved that $J_1 \cdot J_2 = J_1 \cap J_2$, namely we can provide an explicit set of generators for $J_1 \cap J_2$, hence for $I_1 \cap I_2$.

All of this seems, however, pretty ad hoc: what happens if we cannot perform the "change of variables" φ? and how do we deal with the case of ideals when the product is strictly contained in the intersection?

Finally: is it so difficult to compute with polynomial ideals?