Computer Algebra (2018-2019) Exercises 3
Operations on ideals

Deadline: Monday 25 March, 4.00pm.

This final set of exercises is in two contrasting parts. The first part is the degree exam for April 2016, the aim is to give you timetabled revision and feedback. The second part consists of two example constructions of ideals together with results about them and how they relate to varieties. You are then asked to prove some corresponding results about a third construction and use one of these in a little practical work with Axiom.

Naturally the exam questions have a certain amount of bookwork. In answering these do not just copy out large chunks of the course notes (if you do you will lose credit). Just give a straightforward answer in your own words, keep it simple and direct. I have left the questions intact since the aim is to give you practice in answering genuine exam questions. Note that in the exam you have a choice of two out of three questions. This applies to this exercise. Just as for the exam, if you attempt all three questions I will mark your three attempts and give you credit for the best two. In the actual exam it is a very bad idea to attempt more than two questions due to time constraints. However for the purposes of this exercise you might wish to attempt all three if you have time.

The marking will be carried out as follows: the exam part will be marked as normal (each question out of 25) so that your maximum mark here is 50. This will then be halved to give a score out of 25. (I will also give the mark out of 25 for each question you attempt as part of feedback.) The other part has a maximum score of 25 and each sub-part will be marked out of the indicated sub-total (see below). The two separate marks will then be added together and scaled to be out of 40 (the mark being rounded to the nearest integer). This ensures that the total for the three sets of exercises of the course is out of 100 (recall that the first was out of 20 while the other two are out of 40).

Submission: Submit your handwritten answers, stapled at the top left corner, to all the exercises to the ITO. There is no electronic submission for these exercises.

Good Scholarly Practice: Please remember the University requirement as regards all assessed work for credit. Details and advice about this can be found at:

http://web.inf.ed.ac.uk/infweb/admin/policies/academic-misconduct

and links from there. Note that, in particular, you are required to take reasonable measures to protect your assessed work from unauthorised access. For example, if you put any such work on a public repository then you must set access permissions appropriately (generally permitting access only to yourself, or your group in the case of group practicals).

§1. The April 2016 Exam. Instructions to candidates: *Answer any two questions. All questions carry equal weight.*

1. (a) Consider multivariate polynomials with coefficients from a commutative ring with identity, e.g., $\mathbb{Z}$. With reference to representations of such polynomials, explain briefly the terms *recursive*, *distributive*, *dense* and *sparse*. [*4 marks*]

   (b) Define Vandermonde's determinant for n indeterminates $x_1, x_2, \ldots, x_n$. Explain, briefly, its relevance to the problem of testing polynomial expressions (given as sums of products) for equality to zero. [*6 marks*]

   (c) The following Maple code takes two polynomials f, g with rational coefficients in the indeterminate x where g is not a constant. If $g = f^e$ for some natural number $e > 0$ the code returns e otherwise it returns -1.

```
power?(f:UP(x,FRAC INT),g:UP(x,FRAC INT)):INT==
  m:=totalDegree(f)
  n:=totalDegree(g)
  if m=0 then -1   --assumes g is not constant
  else
    r:=divide(n,m)
    if r.remainder ~= 0 then -1
    else
      e:=r.quotient
      for i in 1..1+n repeat
        if eval(f,x=i)^e ~= eval(g,x=i) then return -1
      e
```

Note that `totalDegree` takes a polynomial (of any type) as argument and returns its total degree, returning 0 for the zero polynomial. The Axiom function `divide(a,b)` takes two integers `a`, `b` and returns a record with two components: a `quotient` part and a `remainder` part. Note that `~=` means $\neq$ in Axiom.

i. What single line would you add to the start of the code that checks if g is not a constant and signals an error if it is? [*2 marks*]

ii. Including the type information as shown makes the function header rather obscure. Give an alternative way to declare the type information so that the header is left as `power?(f,g)==` and the body is left unchanged. [*2 marks*]

iii. A user wants to amend the code so that it takes a third polynomial h and tests if $g(h(x))$ is a power of $f(x)$. He does this by amending the code with `k:=eval(g,x=h)`, where `k` is a new local variable. He replaces all other occurrences of `g` in the code with `k`. While this is correct, it is potentially inefficient, e.g., it creates structures that are bigger than necessary. Explain an alternative simple approach that avoids the situation and explain why this is so for your approach. [*4 marks*]

iv. Suppose that $f \neq 0$ (to avoid special cases) and let $m = \deg f$, $n = \deg g$. Show that $g = f^e$ for some $e > 0$ if and only if

- $n = em$.
- $g(a_i) = f(a_i)^e$, for $1 \leq i \leq n+1$, where the a_i can be chosen to be any $n+1$ distinct numbers.

Use this to deduce that `power?` is correct.
[**Note:** You may assume without proof the fact that a non-zero polynomial of degree d with coefficients from an integral domain has at most d roots.] [*7 marks*]

2. In this question we consider non-zero polynomials in one indeterminate x with rational coefficients. Throughout "root" means a root from the real numbers.

(a) Explain briefly what it means to say that a polynomial f is *square free*. Give a method for finding the square free part, denoted by $\mathrm{sqfp}(f)$, of f and state the relationship between the roots of f and the roots of $\mathrm{sqfp}(f)$. [*4 marks*]

(b) Define the *Sturm sequence* of a square free polynomial f and state how we know when it stops. How would you use the sequence to

i. Find how many roots f has in the interval (a, b), assuming that $f(a) \neq 0$ and $g(b) \neq 0$.

ii. Find exactly how many roots f has. [*7 marks*]

(c) Suppose that we want to find the common roots of f and g both square free.

i. Prove that the roots we wish to find are precisely the roots of $f^2 + g^2$. Is $f^2 + g^2$ guaranteed to be square free? Justify your answer with a proof or counterexample as appropriate. [*4 marks*]

ii. The approach of the preceding part has the disadvantage that it always creates a polynomial of higher degree than that of f and g. Give a method for producing a single polynomial with precisely the common roots of f and g such that the single polynomial has degree no higher than that of f and of g and is always square free. Prove that your method is correct. *[6 marks]*

(d) Suppose we have infinitely many polynomials $f_1, f_2, \ldots$ and let I be the ideal of $\mathbb{Q}[x]$ that they generate, i.e., $I = (f_1, f_2, \ldots)$. Prove that there is a single polynomial h such that $I = (h)$. How do the roots of h relate to the roots of $f_1, f_2, \ldots$? Justify your answer. *[4 marks]*

3. This question is concerned with Gröbner bases of ideals of polynomials with coefficients from a field k.

(a) Define what is meant by an *admissible order* $<$ on power products. Prove that if u, v are power products and $u \mid v$ then $u \le v$. *[4 marks]*

(b) Explain what is meant by a lexicographic order on power products.
Suppose we have such a lexicographic order with $x_1 > x_2 > \cdots > x_n$ and p is a non-zero polynomial whose leading power product is of the form x_i^e where $1 \le i \le n$. What can we say about the other power products (if any) that occur in p? *[4 marks]*

(c) Let $u_1, u_2, \ldots, u_r$ and $x_1, x_2, \ldots, x_n$ be distinct indeterminates over k and $g_1, g_2, \ldots, g_n \in k[u_1, u_2, \ldots, u_r]$. Let

$$I = (x_1 - g_1, \ldots, x_n - g_n)$$

be the ideal of $k[x_1, \ldots, x_n, u_1, \ldots, u_r]$ generated by the polynomials $x_1 - g_1, x_2 - g_2, \ldots, x_n - g_n$ and set

$$J = I \cap k[x_1, x_2, \ldots, x_n].$$

i. Prove that J is an ideal of $k[x_1, x_2, \ldots, x_n]$. *[3 marks]*

ii. Let G be a Gröbner basis of I with respect to a lexicographic order in which every u_i is greater than every x_j. Is it correct to say that $H = G \cap k[x_1, x_2, \ldots, x_n]$ is a Gröbner basis for J? Justify your answer. *[6 marks]*

iii. Assume now that k is infinite and $g_1, g_2, \ldots, g_n \in k[u_1, u_2, \ldots, u_r]$. The polynomials define the subset S of k^n given by

$$S = \{\, (g_1(a_1, \ldots, a_r), \ldots, g_n(a_1, \ldots, a_r)) \mid a_1, \ldots, a_r \in k \,\}.$$

The *implicitization problem* is to find $f_1, f_2, \ldots, f_m \in k[x_1, x_2, \ldots, x_n]$ such that $S \subseteq \mathbf{V}(f_1, f_2, \ldots, f_m)$ and this is the smallest variety that contains S, i.e., $\mathbf{V}(f_1, f_2, \ldots, f_m) \subseteq W$ whenever W is a variety such that $S \subseteq W$. Using the notation above, it can be shown that we can take for $f_1, f_2, \ldots, f_m$ any set of generators of J].
Describe an algorithm for finding $f_1, f_2, \ldots, f_m$ (you are not required to prove its correctness).
Let $r = 1$, $n = 2$ and $g_1 = u_1 - 1$, $g_2 = u_1 + 1$ with $k = \mathbb{Q}$. Use your algorithm to show that $f_1 = x_1 - x_2 + 2$ solves the implicitazation problem in this case.
[**Note:** In the example part you may assume the following fact: if G is a set of polynomials and h_1, h_2 are polynomials whose leading power products are coprime then $\mathrm{spol}(h_1, h_2) \to_G^* 0$.] *[8 marks]*

§2. Operations on Ideals: the Algebra–Geometry Dictionary. Let k be a field and $X = \{\, x_1, x_2, \ldots, x_n \,\}$ a set of indeterminates over k. We have seen how to associate special subsets (i.e., varieties) of k^n with ideals of $k[X]$ and vice versa. It is reasonable to ask such questions as: let V_1, V_2 be varieties, are $V_1 \cap V_2$ and $V_1 \cup V_2$ also varieties? Naturally the answers to such questions are related to an understanding of operations on ideals. We discuss the two cases cited in detail as preparation for the exercises.

Throughout we let I, J be ideals of $k[X]$.

Definition 2.1 *The sum of I and J is given by*

$$I + J = \{f + g \mid f \in I, g \in J\}.$$

Lemma 2.1 *$I + J$ is an ideal and $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$.*

Proof $I + J$ is not empty since it contains 0. Now suppose that $h \in I + J$ and $p \in k[X]$. Then $h = f + g$ for some $f \in I$ and $g \in J$. Thus $ph = pf + pg \in I + J$ since $pf \in I$ and $pg \in J$ (as they are both ideals). Finally if $h_1, h_2 \in I + J$ then $h_1 = f_1 + g_1$ and $h_2 = f_2 + g_2$ for some $f_1, f_2 \in I$ and $g_1, g_2 \in J$. Thus $h_1 - h_2 = (f_1 - f_2) + (g_1 - g_2) \in I + J$ again because I and J are ideals and are thus closed under subtraction. This proves that $I + J$ is an ideal.

To prove that $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$ let $a \in \mathbf{V}(I + J)$. Then $a \in \mathbf{V}(I)$ since $I \subseteq I + J$ and similarly $a \in \mathbf{V}(J)$. Thus $a \in \mathbf{V}(I) \cap \mathbf{V}(J)$. For the reverse inclusion suppose that $a \in \mathbf{V}(I) \cap \mathbf{V}(J)$. This means that $f(a) = 0$ for all $f \in I$ and $g(a) = 0$ for all $g \in J$. It follows that $(f + g)(a) = 0$ for all $f \in I$ and $g \in J$, i.e., $h(a) = 0$ for all $h \in I + J$ and thus $a \in \mathbf{V}(I + J)$ as required. □

Definition 2.2 *The product of I and J is given by*

$$IJ = (\{fg \mid f \in I, g \in J\}).$$

Note that in this defintion we cannot just define the product as the set of all fg with $f \in I$ and $g \in J$ because this is (in general) not closed under sums. The correct definition takes all finite sums of such products, i.e.,

$$IJ = \{f_1 g_1 + f_2 g_2 + \cdots + f_m g_m \mid f_i \in I, g_i \in J, \text{ for } m \geq 1 \text{ and } 1 \leq i \leq m\}.$$

It is worth noting here that we have $IJ \subseteq I$ and $IJ \subseteq J$ (can you see why?). We will return to this below.

Lemma 2.2 *IJ is an ideal and $\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$.*

Proof IJ is not empty since it contains 0. Suppose that $h \in IJ$ and $p \in k[X]$. Then $h = f_1 g_1 + f_2 g_2 + \cdots + f_m g_m$ for some $f_1, f_2, \ldots, f_m \in I$ and $g_1, g_2, \ldots, g_m \in J$. Thus $ph = (pf_1)g_1 + (pf_2)g_2 + \cdots + (pf_m)g_m \in IJ$ since I is an ideal and thus closed under multiplication by elements of $k[X]$. Finally if $h_1, h_2 \in IJ$ then $h_1 = f_{11}g_{11} + f_{12}g_{12} + \cdots + f_{1r}g_{1r}$ and $h_2 = f_{21}g_{21} + f_{22}g_{22} + \cdots + f_{2s}g_{2s}$ for some $f_{ij} \in I$ and $g_{ij} \in J$. Thus

$$\begin{aligned} h_1 - h_2 &= f_{11}g_{11} + f_{12}g_{12} + \cdots + f_{1r}g_{1r} + (-f_{21})g_{21} + (-f_{22})g_{22} + \cdots + (-f_{2s})g_{2s} \\ &\in IJ, \end{aligned}$$

since I is closed under negation.

To prove that $\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$ let $a \in \mathbf{V}(IJ)$. Then $f(a)g(a) = 0$ for all $f \in I$ and $g \in J$. If $f(a) = 0$ for all $f \in I$ then $a \in \mathbf{V}(I)$. Otherwise there is some $f \in I$ such that $f(a) \neq 0$ in which case $g(a) = 0$ for all $g \in J$ (since $f(a), g(a) \in k$, a field) and so $a \in \mathbf{V}(J)$. Thus $a \in \mathbf{V}(I) \cup \mathbf{V}(J)$. For the reverse inclusion let $a \in \mathbf{V}(I) \cup \mathbf{V}(J)$ and suppose w.l.o.g. that $a \in \mathbf{V}(I)$. Then $f(a) = 0$ for all $f \in I$ and it follows that $h(a) = 0$ for all $h \in IJ$ (since h is a finite sum of products of members of I and J). It follows that $a \in \mathbf{V}(IJ)$. □

An obvious and important question to ask in connection with these constructions is how to find a basis for the constructed ideal given bases for I and J. This turns out to be easy for these cases.

Lemma 2.3 *Let $f_1, f_2, \ldots, f_r$ be a basis for I and $g_1, g_2, \ldots, g_s$ a basis for J. Then*

1. *$f_1, f_2, \ldots, f_r, g_1, g_2, \ldots, g_s$ is a basis for $I + J$.*
2. *$f_i g_j$ for $1 \leq i \leq r$ and $1 \leq j \leq s$ is a basis for IJ.*

Proof For the basis of $I+J$ let $H=(f_1,\dots,f_r,g_1,\dots,g_s)$. Cleary H contains both I and J as subsets and thus $I+J\subseteq H$ since H is closed under addition. The reverse inclusion is obvious since the generators of H are contained in $I+J$.

For the basis of IJ it is clear that the ideal $H=(f_ig_j, 1\le i\le r, 1\le j\le s)$ is contained in IJ. For the reverse inclusion it suffices to show that any product fg with $f\in I$ and $g\in J$ is in H. We have $f=\sum_{i=1}^r p_if_i$ and $g=\sum_{j=1}^s q_jg_j$ for some polynomials p_i, q_j. Thus $fg=\sum_{i=1}^r\sum_{j=1}^s p_iq_jf_ig_j$ and this is in H as required. □

The two examples given above are relatively straightforward and the question of finding bases is easily settled. We now move to look at a rather more intricate case.

§2.1. Intersection of Ideals. Since ideals are (special kinds of) sets we can take their intersection.

Exercise 2.1 *Prove that $I\cap J$ is an ideal.* [*5 marks*]

Note that we always have $IJ\subseteq I\cap J$ because $IJ\subseteq I$ and $IJ\subseteq J$ as observed above. However equality need not hold as can be seen by taking $I=J=(x)$ in $k[x]$: we have $IJ=(x^2)$ but $I\cap J=(x)$ and $(x^2)\subset(x)$ since $x^2\in(x)$ but $x\notin(x^2)$ [why?].

[*5 marks*]

Exercise 2.2 *Prove that* $\mathbf{V}(I\cap J)=\mathbf{V}(I)\cup\mathbf{V}(J)$.

Thus $\mathbf{V}(IJ)$ and $\mathbf{V}(I\cap J)$ are the same. We will see that finding a basis for $I\cap J$ from bases of I and J is quite hard. So why bother with this harder concept? The simple example given above (with $I=J=(x)$) provides a clue. Although IJ and $I\cap J$ have the same common zeros as sets the latter gives more refined information. In our simple example the variety is just $\{0\}$ but IJ has this as a repeated root whereas $I\cap J$ captures it as a simple root. Recall that if k is algebraically closed, Hilbet's Nullstellensatz tells us that $f\in\mathbf{I}\mathbf{V}(I)$ if and only if $f^s\in I$ for some $s\ge1$. The *radical* of I, denoted by $\sqrt{I}$, is defined to be all $f\in k[X]$ such that $f^s\in I$ for some $s\ge1$; this is an ideal (the proof is not hard). The Nullstellensatz can now be restated as $\sqrt{I}=\mathbf{I}\mathbf{V}(I)$. It is thus reasonable to look for constructions that behave well in terms of taking radicals. $I\cap J$ is very well behaved in this regard whereas IJ is not (we always have $\sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J}$ but we need not have $\sqrt{IJ}=\sqrt{I}\sqrt{J}$ as the simple example shows).

We now discuss the question of finding a basis for $I\cap J$. Let t be a new indeterminate over k. We will be considering elements of $k[t]$, $k[X]$ and of $k[X,t]$. In order to keep things clear we will use the argument based notation $u(t)$, $g(X)$ and $h(X,t)$ for the three types of elements (note that $h(X,t)$ need not involve t or even members of X, the notation just indicates the possible indeterminates that it might involve). For $u(t)\in k[t]$ we will use $u(t)I$ to denote the ideal of $k[X,t]$ generated by $\{u(t)h\mid h\in I\}$ (remember that I is an ideal of $k[X]$). The following result is fairly straightforward to prove, we omit the proof just to save a little space.

Lemma 2.4 *Suppose that I is generated by $f_1(X),f_2(X),\dots,f_r(X)$ as an ideal of $k[X]$.*

1. *The ideal $u(t)I$ of $k[X,t]$ is generated by $u(t)f_1(X),u(t)f_2(X),\dots,u(t)f_r(X)$.*
2. *If $h(X,t)\in u(t)I$ and $a\in k$ then $h(X,a)\in I$.*

The two simple observations of the preceding lemma are very helpful in the following.

Exercise 2.3 *Prove that $I\cap J=(tI+(1-t)J)\cap k[X]$. (Hint: Use the preceding Lemma as part of your proof.)* [*10 marks*]

Having established the main result we can dispense with the clumsy argument based notation for elements. Suppose that I is generated by $f_1,f_2,\dots,f_r$ and J by $g_1,g_2,\dots,g_s$ (as ideals of $k[X]$). Then the ideal $tI+(1-t)J$ of $k[X,t]$ is generated by $tf_1,\dots,tf_r,(1-t)g_1,\dots,(1-t)g_s$, this follows from Lemma 2.4 and Lemma 2.3. We are now ready to produce an algorithm for finding a basis for $I\cap J$.

Choose a lexicographic order with t greater than $x_1, x_2, \dots, x_n$ (these can be ordered in any way). Compute a Gröbner basis G for $tI + (1-t)I$ using this order. The elements of G that do not involve t are a basis (actually a Gröbner basis) for $I \cap J$. To see this let H be the elements of G chosen as described (i.e., $H = G \cap k[X]$), it follows from the exercise that $H \subseteq I \cap J$. Since G is a Gröbner basis for $tI + (1-t)J$ and $I \cap J \subseteq tI + (1-t)J$ it follows that every element $f \in I \cap J$ reduces to 0 w.r.t. G. Of course the power products of any such f are all free of t. On the other hand if we consider an element of G that involves t then its leading power product will also involve t (because the order is lexicographic and t is the largest indeterminate). Thus no such element can ever be used in reducing f to 0, i.e., f reduces to 0 w.r.t. H. Thus H is a Gröbner basis for $I \cap J$ and it is a simple exercise (which you are advised to do) to see that a Gröbner basis for an ideal is a basis for it (i.e., it generates the ideal).

As a simple example consider $I = (x^3y)$ and $J = (xy^2)$; it is easy to see that $I \cap J = (x^3y^2)$. We verify this by following the algorithm using Axiom's function `groebner` with $y <_L x <_L t$. The basis we obtain is $[\, tx^3y, txy^2 - xy^2, x^3y^2 \,]$ and so $H = [\, x^3y^2 \,]$ as expected.

Note that in Axiom we tell the function `groebner` which order to use by giving the polynomials the appropriate type. In our case this is

```
DistributedMultivariatePolynomial([t,x,y],Integer)
```

which, mercifully, can be abbreviated to `DMP([t,x,y],INT)`. You can declare the (same) type of several variables in one go, e.g., `(f1,f2,g1,g2):DMP([t,x,y],INT)`. The procedure `groebner` takes a list of polynomials as its argument so the type of this must be `List(DMP([t,y,x],INT))`. You can ensure this type in various ways but do check the type before calling the procedure, probably the safest thing is to assign the list to a variable and look at the type that Axiom returns (for a single variable `B` you can just use `B:`⟨*type*⟩`:=`⟨*value*⟩).

Exercise 2.4 *We use polynomials with coefficients from $\mathbb{Q}$ throughout.*

1. *Let $I = (x^2 + y^2 - 1, xy)$ and $J = (y - x, xy - 1)$. Find a basis for $I \cap J$. Note that $\mathbf{V}(I)$ consists of four points and $\mathbf{V}(J)$ consists of two points (use the Axiom function* `solve`*). Find these points and check that the variety of your computed basis is the union of the points (this does not prove that the basis is correct but it does provide a reasonable check). For your answer just write down the basis.*

2. *Let $I = (x)$, $J_1 = (x^2, y)$ and $J_2 = (x^2, xy, y^2)$. Find $I \cap J_1$ and show that this is the same as $I \cap J_2$. Since the three ideals are all generated by power products you should be able to see easily that the generators for the interestion belong to all the ideals (why?). For your answer just write down the common basis of the two intersections.* [*5 marks*]

Notes. If you have computed a basis `G` with the extra indeterminate `t` you can pick out the polynomials that do not involve `t` with the simple function

```
freeOf(t,L)==
  R:=[]
  for f in L repeat if not member?(t,variables(f)) then R:=cons(f,R)
  R
```

You could try other examples, especially ones for which you can describe the varieties easily. An obvious source is to take linear polynomials with finitely many solutions (one set to generate I and another to generate J). Naturally the algorithm works in general but things get complicated: even here you can do some checking, e.g., the generators for $I \cap J$ should be in I and in J and this can be checked using Gröbner bases for I and J. In Axiom you can do this using the procedure `normalForm`, if G is the Gröbner basis then the normal form of f is obtained by `normalForm(f,G)`.

Kyriakos Kalorkoti, March 2019