Exercises 3

Deadline: Monday 23 March, 4.00pm.

This final set of exercises is in two contrasting parts. The first part is the degree exam for April 2013, 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 Maple.

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 real exam it is a very bad idea to attempt more than two questions due to time constraints. However for the purposes of this exercise I would encourage you 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 adjusted to be out of 40. This ensures that the total for the three sets 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.

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

http://www.ed.ac.uk/schools-departments/academic-services/students/undergraduate/discipline/academic-misconduct

and at:


§1. The April 2013 Exam. Instructions to candidates: Answer any two questions. All questions carry equal weight.

1. (a) Maple represents integers in a base \( B \) where \( B \) is chosen as large as possible subject to a certain condition. Describe the condition and explain its significance. [3 marks]

(b) Describe briefly the way in which Maple represents rational numbers so that they are in canonical form.

Suppose \( a/b \) and \( c/d \) are rational numbers in canonical form. The obvious way to obtain the canonical form of their product is by

\[
\frac{ac}{\gcd(ac, bd)} \quad \frac{bd}{\gcd(ac, bd)}
\]

Explain the main disadvantage of this method and show how to avoid it. [6 marks]
(c) Consider the following Maple code:

```
# f, g, p ...... polynomials in x with rational coefficients
# where p is irreducible.
# x ............ a name.
# Output:
# View the arguments as specifying f(a)/g(a) for any root a
# of p. If g(a) = 0 then an error is signalled. Otherwise we
# return a polynomial r in the indeterminate x such that
# f(a)/g(a) = r(a) and r is either 0 or has degree strictly less
# than that of p.
# Assumptions:
# The three polynomials are given in expanded form, and
# p is irreducible.
adiv:=proc(f,g,p,x)
  local u,v;
  if rem(g,p,x) = 0 then error "attempt to divide by 0"
  else
    gcdex(g,p,x,u,v);
    rem(u*f,p,x)
  end if
end proc:
```

The call `gcdex(g,p,x,u,v)` returns `gcd(g,p)` (as a monic polynomial) and assigns polynomial values to `u`, `v` so that 

\[ ug + vp = \text{gcd}(g,p) \]

Thus if \( g(a) \neq 0 \) the code finds a polynomial \( u \) such that \( ug \equiv 1 \pmod{p} \). Hence \( u \) is the inverse of \( g \) in \( \mathbb{Q}[x] / (p) \), the field obtained by carrying out arithmetic on polynomials from \( \mathbb{Q}[x] \) but with all results taken modulo \( p \). Thus \( u \) is the inverse of \( g \) in this field and \( f/g = uf \).

(i. What simple change to the procedure header would ensure a check by Maple that the parameter \( x \) is indeed a name when \texttt{adiv} is called? [2 marks]

(ii. The code checks that \( g(a) \neq 0 \) by testing that \( p \) does not divide \( g \). Justify this by proving that \( g(a) = 0 \) if and only if \( p \) divides \( g \) in \( \mathbb{Q}[x] \). (You may assume without proof the fact that two polynomials have a common root in \( \mathbb{C} \) if and only if they have a non-constant common factor in \( \mathbb{Q}[x] \).) [5 marks]

(iii. The efficiency of the code can be improved by observing that the test \( \text{rem}(g,p,x) = 0 \) could be replaced by a suitable test on the result of \( \text{gcdex}(g,p,x,u,v) \) (which is not used at all in the version of the code shown). State the test and justify it briefly. [3 marks]

(iv. Assume that \( g(a) \neq 0 \) and let \( r \) be the result returned by \texttt{adiv}(f,g,p,x). Is \( r(a) \) a canonical form for \( f(a)/g(a) \)? Justify your answer. [6 marks]

2. Throughout \( x, y \) are indeterminates over \( \mathbb{C} \) (and hence over any subfield, e.g., \( \mathbb{Q} \)). Let \( p, q \in \mathbb{Q}[x] \) and assume that at least one of them is non-zero.

(a) Define what is meant by a greatest common divisor, \texttt{gcd}(p,q), of \( p, q \) and explain how to make it unique. [2 marks]

(b) Put

\[
\begin{align*}
p &= a_m x^n + a_{m-1} x^{n-1} + \cdots + a_0, \\
q &= b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0,
\end{align*}
\]

and assume that neither polynomial is 0.

(i. Define the resultant, \texttt{Res}(p,q), of \( p \) and \( q \). [2 marks]
3. This question is concerned with Gröbner bases of ideals of polynomials in the indeterminates $X = \{x_1, x_2, \ldots, x_n\}$ with coefficients from a field $k$.

(a) Define what is meant by an admissible order on power products. [2 marks]

(b) Prove that for an admissible order $<$ and power products $u, v$ if $u \mid v$ then $u \leq v$. [3 marks]

(c) Let $I$ be a non-zero ideal of $k[X]$ and $G$ a finite subset of $k[X]$.

i. State a condition for $G$ to be a Gröbner basis for $I$ that does not assume $G$ to be a basis for $I$. [2 marks]

ii. Prove that if $G$ is a Gröbner basis for $I$ then it is a basis for $I$, i.e., it generates $I$. [3 marks]

(d) Let $U = \{u_1, u_2, \ldots, u_r\}$ be a Gröbner basis for $I$ and suppose that we have $g_1, g_2, \ldots, g_n \in k[U]$. These 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 $f_1, f_2, \ldots, f_m \in k[X]$ such that $S \subseteq V(f_1, f_2, \ldots, f_m)$ and this is the smallest variety that contains $S$, i.e., we have $V(f_1, f_2, \ldots, f_m) \subseteq W$ whenever $W$ is a variety such that $S \subseteq W$.

Let $I$ be the ideal of $k[X, U]$ generated by the polynomials $x_1 - g_1, x_2 - g_2, \ldots, x_n - g_n$ and set $J = I \cap k[X]$.

i. Prove that $J$ is an ideal of $k[X]$. [3 marks]

ii. Explain briefly why we know that there are finitely many polynomials $f_1, f_2, \ldots, f_m \in k[X]$ that generate $J$. [2 marks]
iii. It is claimed that there are polynomials \( h_{ij} \in k[X, U] \), for \( 1 \leq i \leq m \) and \( 1 \leq j \leq n \) such that
\[
 f_i = h_{i1}(x_1 - g_1) + h_{i2}(x_2 - g_2) + \ldots + h_{in}(x_n - g_n).
\]

Explain why this claim is correct. \([2 \text{ marks}]\)

iv. Prove that \( S \subseteq V(f_1, f_2, \ldots, f_m) \). \([3 \text{ marks}]\)

v. In fact the preceding part can be extended to show that \( V(f_1, f_2, \ldots, f_m) \subseteq W \) whenever \( W \) is a variety such that \( S \subseteq W \).

Describe an algorithm for solving the implicitization problem (you are not required to prove its correctness). \([5 \text{ marks}]\)

§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 \( V(I + J) = V(I) \cap V(J) \).

**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 \( V(I + J) = V(I) \cap V(J) \) let \( x \in V(I + J) \). Then \( x \in V(I) \) since \( I \subseteq I + J \) and similarly \( x \in V(J) \). Thus \( x \in V(I) \cap V(J) \). For the reverse inclusion suppose that \( x \in V(I) \cap V(J) \). This means that \( f(x) = 0 \) for all \( f \in I \) and \( g(x) = 0 \) for all \( g \in J \). It follows that \( (f + g)(x) = 0 \) for all \( f \in I \) and \( g \in J \), i.e., \( h(x) = 0 \) for all \( h \in I + J \) and thus \( x \in V(I + J) \) as required. \( \square \)

**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 definition 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 \( V(IJ) = V(I) \cup V(J) \).

**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
\[
 h_1 - h_2 = f_{11} g_{11} + f_{12} g_{12} + \cdots + f_{1r} g_{1r} + (-f_{21}) g_{21} + (-f_{22}) g_{22} + \cdots + (-f_{2s}) g_{2s} \in IJ,
\]
since $I$ is closed under negation.

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

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 $H = (f_1, \ldots, f_r, g_1, \ldots, g_s)$. Clearly $H$ 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 $H = (f_i g_j, 1 \leq i \leq r, 1 \leq j \leq s)$ 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 $f = \sum_{i=1}^r p_i f_i$ and $g = \sum_{j=1}^s q_j g_j$ for some polynomials $p_i, q_j$. Thus $fg = \sum_{i=1}^r \sum_{j=1}^s p_i q_j f_i g_j$ 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 $I \cap J = (x)$.

**Exercise 2.2** Prove that $V(I \cap J) = V(I) \cup V(J)$. [5 marks]

Thus $V(IJ)$ and $V(I \cap J)$ 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, Hilbert’s Nullstellensatz tells us that $f \in V(I)$ if and only if $f^s \in I$ for some $s \geq 1$. 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 $s \geq 1$; this is an ideal (the proof is not hard). The Nullstellensatz can now be restated as $\sqrt{I} = V(I)$. 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 $\sqrt{IJ} = \sqrt{\sqrt{I} \cap \sqrt{J}}$ 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 possibility that it might and of course $g(X)$ tells us that $g$ does not involve $t$). 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 $f_1(X), f_2(X), \ldots, f_r(X)$ as an ideal of $k[X]$.  

1. The ideal $u(t)I$ of $k[X,t]$ is generated by $u(t)f_1(X), u(t)f_2(X), \ldots, u(t)f_r(X)$. 

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 $I \cap J = (tI + (1-t)J) \cap k[X]$. [10 marks]

Having established the main result we can dispense with the clumsy argument based notation for elements. Suppose that $I$ is generated by $f_1, f_2, \ldots, f_r$ and $J$ by $g_1, g_2, \ldots, g_s$ (as ideals of $k[X]$). Then the ideal $tI + (1-t)J$ of $k[X,t]$ is generated by $tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s$, 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 $x_1, x_2, \ldots, x_n$ (these can be ordered in any way). Compute a Gröbner basis $G$ for $tI + (1-t)J$ 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 the procedure Basis in Maple’s Groebner package with $x <_L y <_L t$. The basis we obtain is $G = \{x^3y^2, tx^3y, -xy^2 + xy^2t\}$ and so $H = \{x^3y^2\}$ as expected.

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 $V(I)$ consists of four points and $V(J)$ consists of two points. 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 intersection belong to all the ideals (why?). For your answer just write down the common basis of the two intersections. [5 marks]

Notes. Use ?Groebner,Basis. 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 single line

```maple
map(proc(f) if member(t,indets(f)) then NULL else f end if end proc,G).
```

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 $J$. 

Kyriakos Kalorkoti, March 2015