M3P23, M4P23, M5P23: COMPUTATIONAL ALGEBRA & GEOMETRY

SOLUTIONS 4

(1) (a) Using lex order, calculated using MAGMA (in 0.010 seconds):

```
x^3 + y^2 + z^2 - 1,
x^2*y^2 + x^2*z^2 - x^2 - y^4 - z^3 + 1,
x^2*z^4 + x^2*z^3 - 2*x^2*z^2 - 1/6*x*z^10 - 2/3*x*z^9 - 1/4*x*z^8 +
    7/6*x*z^7 - 1/12*x*z^6 - x*z^5 + x*z^4 + 1/2*y^10*z^2 + 1/3*y^10*z -
...and an additional 30 lines of output.
```

Using grevlex order, calculated using MAGMA (in 0.000 seconds):

```
y^6 - y^4*z^2 + x^2*z^4 + 2*x*y^2*z^2 + x^2*z^3 + y^2*z^3 + x*z^4 - z^5 -
    2*x^2*z^2 - 2*y^2*z^2 - x*z^3 - z^4 - 2*x*y^2 - 2*x*z^2 + z^3 + y^2 +
    3*z^2 + 2*x - 2,
x*y^4 + y^4 + 2*y^2*z^2 + x*z^3 + z^4 - 2*y^2 - 2*z^2 - x + 1,
x^2*y^2 - y^4 + x^2*z^2 - z^3 - x^2 + 1,
x^3 + y^2 + z^2 - 1
```

It's very obvious that the grevlex basis is preferable.

(b) Using lex order, calculated using MAGMA (in 0.030 seconds):

```
x^3 + y^3 + z^2 - 1,
x^2*y^3 + x^2*z^2 - x^2 - y^4 - z^3 + 1,
x^2*y*z - x^2*y + x^2*z^6 + 2*x^2*z^5 + 3*x^2*z^4 - 3*x^2*z^3 - 3*x^2*z^2 -
    x^2*z + x^2 + 7*x*y^3*z - 7*x*y^3 - 12*x*y^2*z + 12*x*y^2 -
    62093/7776*x*z^20 - 15037/243*x*z^19 - 1974401/7776*x*z^18 -
...and an additional 372 lines of output!!!
```

Using grevlex order, calculated using MAGMA (in 0.000 seconds):

```
y^6 + x*y^4 + 2*y^3*z^2 + x*z^3 + z^4 - 2*y^3 - 2*z^2 - x + 1,
x^2*y^3 - y^4 + x^2*z^2 - z^3 - x^2 + 1,
x^3 + y^3 + z^2 - 1
```

(2) I checked the claim using MAGMA. In each case Gröbner basis is very small.

```
> R<x,y,z,w>:=PolynomialRing(Rationals(),4,"grevlex");
> I:=ideal<R|[x^(n+1)-y*z^(n-1)*w,x*y^(n-1)-z^n,x^n*z-y^n*w]> where n:=3;
> time GroebnerBasis(I);
[
    z^10 - y^9*w,
    x*z^7 - y^7*w,
```

a.m.kasprzyk@imperial.ac.uk
http://magma.maths.usyd.edu.au/∼kasprzyk/.

```
    x^2*z^4 - y^5*w,
    x^4 - y*z^2*w,
    x^3*z - y^3*w,
    x*y^2 - z^3
]
Time: 0.000
> I:=ideal<R|[x^(n+1)-y*z^(n-1)*w,x*y^(n-1)-z^n,x^n*z-y^n*w]> where n:=4;
> time GroebnerBasis(I);
[
    z^17 - y^16*w,
    x*z^13 - y^13*w,
    x^2*z^9 - y^10*w,
    x^3*z^5 - y^7*w,
    x^5 - y*z^3*w,
    x^4*z - y^4*w,
    x*y^3 - z^4
]
Time: 0.000
> I:=ideal<R|[x^(n+1)-y*z^(n-1)*w,x*y^(n-1)-z^n,x^n*z-y^n*w]> where n:=5;
> time GroebnerBasis(I);
[
    z^26 - y^25*w,
    x*z^21 - y^21*w,
    x^2*z^16 - y^17*w,
    x^3*z^11 - y^13*w,
    x^4*z^6 - y^9*w,
    x^6 - y*z^4*w,
    x^5*z - y^5*w,
    x*y^4 - z^5
]
Time: 0.000
```

It's worth noting that $z^{n^2+1} - y^{n^2}w$ is the first term in each case. (In fact this is true for all n.) Redoing the calculation when $n = 3$ using lex order, we get:

```
> R<x,y,z,w>:=PolynomialRing(Rationals(),4,"lex");
> I:=ideal<R|[x^(n+1)-y*z^(n-1)*w,x*y^(n-1)-z^n,x^n*z-y^n*w]> where n:=3;
> time GroebnerBasis(I);
[
    x^4 - y*z^2*w,
    x^3*z - y^3*w,
    x^2*z^4 - y^5*w,
```

```
    x*y^2 - z^3,
    x*z^7 - y^7*w,
    y^9*w - z^10
]
Time: 0.000
```

In this case the claim no-longer holds.

(3) (a) First we calculate $I \cap k[y]$ via the technique of calculating a Gröbner basis for I using lex order with $x < y$. We use MAGMA to calculate the Gröbner basis:

```
> R<x,y>:=PolynomialRing(Rationals(),2,"lex");
> I:=ideal<R|[x^2+2*y^2-3,x^2+x*y+y^2-3]>;
> GroebnerBasis(I);
[
    x^2 + 2*y^2 - 3,
    x*y - y^2,
    y^3 - y
]
```

Hence:

$$I \cap k[y] = (y^3 - y).$$

In order to calculate $I \cap k[x]$ we need to exchange the order of x and y – i.e. we calculate lex order using $y < x$:

```
> R<y,x>:=PolynomialRing(Rationals(),2,"lex");
> I:=ideal<R|[x^2+2*y^2-3,x^2+x*y+y^2-3]>;
> GroebnerBasis(I);
[
    y + 1/2*x^3 - 3/2*x,
    x^4 - 4*x^2 + 3
]
```

Hence:

$$I \cap k[x] = (x^4 - 4x^2 + 3).$$

(b) We should try to minimise our work by using the simpler of the two bases we found in part (a). To my mind that looks like the case when $y < x$, so I'll use that. I see immediately that:

$$(x^2 - 1)(x^2 - 3) = 0 \qquad \Rightarrow \qquad x = \pm 1 \text{ or } x = \pm\sqrt{3}.$$

Substituting into $y = \frac{1}{2}x(3 - x^2)$ gives four solutions:

$$(-1, -1), (1, 1), (\pm\sqrt{3}, 0).$$

(c) Clearly only the first two solutions are contained in $\mathbb{Q}^2$.

(d) Set $k = \mathbb{Q}[\sqrt{3}]$. Notice that this really is a field, since $1/\sqrt{3} = \sqrt{3}/3 \in \mathbb{Q}[\sqrt{3}]$.

(4) Taking a hint from the previous question, I computed two lex Gröbner bases: one with $x < y$ and one with $y < x$. The second one looks better to me, so I used that. The resulting Gröbner basis is:

$$G = \left\{ y + \frac{3}{4}x^3 - \frac{3}{2}x, x^4 - \frac{8}{3}x^2 + \frac{4}{3} \right\}.$$

Solving for x I get:

$$(x^2 - 2)(3x^2 - 2) = 0 \qquad \Rightarrow \qquad x = \pm\sqrt{2} \text{ or } x = \pm\sqrt{2/3}.$$

Substituting into $y = \frac{3}{4}x(2 - x^2)$ gives the four solutions:

$$(\pm\sqrt{2}, 0), (\sqrt{2/3}, \sqrt{2/3}), (-\sqrt{2/3}, -\sqrt{2/3}).$$

(5) The standard lex-ordered Gröber basis is:

$$G = \left\{ x + 2z^3 - 3z, y^2 - z^2 - 1, z^4 - \frac{3}{2}z^2 + \frac{1}{2} \right\}.$$

This corresponding Gröbner bases for the elimination ideals are:

$$\begin{aligned} G \cap k[y, z] &= \left\{ y^2 - z^2 - 1, z^4 - \frac{3}{2}z^2 + \frac{1}{2} \right\}, \\ G \cap k[z] &= \left\{ z^4 - \frac{3}{2}z^2 + \frac{1}{2} \right\}. \end{aligned}$$

Solving for z we obtain:

$$2\left(z^2 - 1\right)\left(z^2 - \frac{1}{2}\right) = 0 \qquad \Rightarrow \qquad z = \pm 1 \text{ or } z = \pm\frac{1}{\sqrt{2}}.$$

Since we're only interested in rational solutions, we restrict to the cases $z = \pm 1$. Substituting into $y^2 = z^2 + 1$ gives $y^2 = 2$ in both cases, hence there are no rational solutions.

(6) (a) We calculate the lex Gröbner basis for $I = (x^{10} - x^5 y + 1, x^2 - xz + 1) \subset \mathbb{C}[x, y, z]$:

$$G = \{x^2 - xz + 1, y - z^5 + 5z^3 - 5z\}.$$

Hence we obtain bases for I_1 and I_2 given by, respectively,

$$\begin{aligned} G \cap \mathbb{C}[y, z] &= \{y - z^5 + 5z^3 - 5z\} \\ G \cap \mathbb{C}[z] &= \emptyset \end{aligned}$$

That $I_2 = (0)$ is immediate.

(b) Since $I_2 = (0)$, we have that $\mathbb{V}(I_2) = \mathbb{C}$. The generator of I_1 can be written in the form

$$1 \cdot y^1 + (-z^5 + 5z^3 - 5z),$$

hence the Elimination Theorem tells us to consider when solutions $a \in \mathbb{V}(I_2) = \mathbb{C}$ are contained in $\mathbb{V}(1) = \emptyset$. Since this is never so, we conclude that every partial solution in $\mathbb{V}(I_2)$ extends to a solution $\left(a^5 - 5a^3 + 5a, a\right) \in \mathbb{V}(I_1) \subset \mathbb{C}^2$.

The generators of I can be written in the form:

$$1 \cdot x^2 + (-zx + 1),$$
$$(y - z^5 + 5z^3 - 5z) \cdot x^0.$$

Hence we consider $\mathbb{V}(1, y-z^5+5z^3-5z) = \emptyset$. So, again by the Elimination Theorem, we see that every partial solution $(a^5 - 5a^3 + 5a, a) \in \mathbb{V}(I_1)$ extends to a solution in $\mathbb{V}(I)$. Hence we conclude that each partial solution in $\mathbb{V}(I_2)$ extends to a solution in $\mathbb{V}(I)$, as desired.

(c) Let $(a^5 - 5a^3 + 5a, a) \in \mathbb{V}(I_1)$, $a \in \mathbb{R}$. Then x satisfies $x^2 - ax + 1 = 0$. This has real solutions if and only if $a^2 - 4 \geq 0$. In other words, a partial solution $(y, z) \in \mathbb{V}(I_1) \subset \mathbb{R}^2$ extends to solutions $\mathbb{V}(I) \subset \mathbb{R}^3$ if and only if $z \geq 2$ or $z \leq -2$. This doesn't contradict the Extension Theorem, since $\mathbb{R}$ is not algebraically closed.

(d) We've basically already done the work (and the real part is sketched below):

$$\mathbb{V}(I) = \left\{ \left(\frac{1}{2}(a \pm \sqrt{a^2 - 4}), a^5 - 5a^3 + 5a, a \right) \,\middle|\, a \in \mathbb{C} \right\} \subset \mathbb{C}^3.$$