M3P23, M4P23, M5P23: COMPUTATIONAL ALGEBRA & GEOMETRY

EXAM SOLUTIONS

(1) (a) Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. Fix a monomial order. We say that a Gröbner basis G for I is *reduced* if $\mathrm{LC}(g) = 1$ and no monomial of g is contained in $(\mathrm{LT}(G \setminus \{g\}))$, for all $g \in G$.
The reduced Gröbner basis of I is unique, hence two ideals I_1 and I_2 are identical if and only if their reduced Gröbner bases agree.

(b) Buchberger's Criterion states that a finite generating set $G = \{g_1, \ldots, g_m\}$ for an ideal $I \subset k[x_1, \ldots, x_n]$ is a Gröbner basis if and only if $\overline{S(g_i, g_j)}^G = 0$ for all $i \neq j$.
Using grlex order we have S-polynomials:

$$\begin{aligned} S(x^2 + 2xy, xy) &= 2xy^2, \\ S(x^2 + 2xy, y^2 - x/2) &= 2xy^3 + x^3/2, \\ S(xy, y^2 - x/2) &= x^2/2. \end{aligned}$$

In each case, upon division by G we obtain remainder zero.

(c) G is not reduced since $xy \in (xy)$. We have that

$$\overline{x^2 + 2xy}^{xy, y^2 - x/2} = x^2,$$

so we can transform G to $G' = \{x^2, xy, y^2 - x/2\}$. This is also a Gröbner basis, and we see that it is reduced.

(2) (a) (i) Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis for I with respect to the given monomial order. The Division Algorithm gives us

$$f = a_1 g_1 + \ldots + a_m g_m + r,$$

where no term of r is divisible by any $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m)$. Suppose that there exists some $h \in \mathrm{LT}(I)$ such that a term of r is divisible by h. Since G is a Gröbner basis for I, we have that $(\mathrm{LT}(I)) = (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m))$. Hence $\mathrm{LT}(g_i) \mid h$ for some i, which is a contradiction. Finally, setting $g = a_1 g_1 + \ldots + a_m g_m$ we notice that $g \in I$ (since I is an ideal).

(ii) Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis for I with respect to the given monomial order, and suppose that $f = g + r = g' + r'$. Then $r - r' = g' - g \in I$, so if $r \neq r'$ we have that $\mathrm{LT}(r - r') \in (\mathrm{LT}(I)) = (\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m))$. Hence $\mathrm{LT}(r - r')$ is divisible by $\mathrm{LT}(g_i)$ for some i. But this is impossible, since no term of either r or r' is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m)$. We conclude that $r - r' = 0$ and so $r = r'$.

a.m.kasprzyk@imperial.ac.uk

http://magma.maths.usyd.edu.au/~kasprzyk/.

(b) Since our choice of Gröbner basis G in the proof of (ii) was arbitrary, the result follows immediately.

(c) Using lex order we calculate the remainder of x^3 upon division by G in two different ways:

$$\overline{x^3}^{-x^2+y,-x^3+z} = xy, \qquad \text{and} \qquad \overline{x^3}^{-x^3+z,-x^2+y} = z.$$

Since the remainders do not agree, the order in which we list the elements of G matters. Hence by (b) we conclude that G is not a Gröbner basis with respect to lex order.

(3) (a) An ideal $I \subset k[x_1, \ldots, x_n]$ is said to be *radical* if for each $f \in k[x_1, \ldots, g_n]$, if $f^m \in I$ for some positive power $m > 0$ then $f \in I$.

Given an ideal $I \subset k[x_1, \ldots, x_n]$ we define

$$\sqrt{I} := \{f \in k[x_1, \ldots, x_n] \mid f^m \in I \text{ for some } m > 0\}.$$

We will prove that $\sqrt{I}$ is an ideal. First, suppose that $f \in \sqrt{I}$ and $g \in k[x_1, \ldots, x_n]$. Then there exists some $m > 0$ such that $f^m \in I$. Since I is an ideal, we see that $g^m f^m \in I$, and hence $gf \in \sqrt{I}$. Now suppose that $f_1, f_2 \in \sqrt{I}$. Then there exists some $m_1, m_2 > 0$ such that $f_1^{m_1}, f_2^{m_2} \in I$. Let $m := \max\{m_1, m_2\}$ and consider the binomial expansion

$$(f_1 + f_2)^{2m} = f_1^{2m} + \binom{2m}{1} f_1^{2m-1} f_2 + \ldots + \binom{2m}{i} f_1^{2m-i} f_2^i + \ldots + f_2^{2m}.$$

For each term of the expansion, either $2m - i \geq m$ or $i \geq m$. In the first case we can write the term in the form $hf_1^{m_1}$, where $h = \binom{2m}{i} f_1^{2m-i-m_1} f_2^i \in k[x_1, \ldots, x_n]$. In the second case we can write the term in the form $h' f_2^{m_2}$, where $h' = \binom{2m}{i} f_1^{2m-i} f_2^{i-m_2} \in k[x_1, \ldots, x_n]$. Since I is an ideal, we conclude that $(f_1 + f_2)^{2m} \in I$, and hence that $f_1 + f_2 \in \sqrt{I}$.

(b) Notice that $I = (x^2 + y^2 + 2xy, x^2 + y^2 - 2xy) = \big((x + y)^2, (x - y)^2\big)$. In particular we see that $x + y, x - y \in \sqrt{I}$, and hence $x, y \in \sqrt{I}$. Since $1 \notin I$, we conclude that $\sqrt{I} = (x, y)$.

(c) Let $I = \big(x^2 - 1, y(x + 2)\big) \subset \mathbb{C}[x, y]$. We see that $\mathbb{V}(I) = \mathbb{V}(x^2 - 1) \cap \mathbb{V}(y(x + 2)) \subset \mathbb{C}^2$. Now $\mathbb{V}(x^2 - 1) = \mathbb{V}(x + 1) \cup \mathbb{V}(x - 1)$ is given by the union of the two lines $x = \pm 1$. $\mathbb{V}(y(x + 2)) = \mathbb{V}(y) \cup \mathbb{V}(x + 2)$ is the union of the lines $y = 0$ and $x = -2$. Hence $\mathbb{V}(I) = \{(\pm 1, 0)\}$. The Nullstellensatz tells us that

$$\sqrt{I} = \mathbb{I}(\mathbb{V}(I)) = \mathbb{I}(\{(\pm 1, 0)\}) = (x^2 - 1, y).$$

(4) (a) Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. We say that I is *prime* if whenever $f, g \in k[x_1, \ldots, x_n]$ are such that $fg \in I$, then either $f \in I$ or $g \in I$. We say that I is *maximal* if $I \neq k[x_1, \ldots, x_n]$ and for any ideal $J \supseteq I$, either $J = I$ or $J = k[x_1, \ldots, x_n]$.

Let $I \neq k[x_1, \ldots, x_n]$ be an ideal. We will prove the contrapositive: if I is not prime then I is not maximal. For suppose there exist polynomials $f, g \in k[x_1, \ldots, x_n]$ with

$fg \in I$, $f, g \notin I$, and consider the ideal $(f) + I$. Clearly $I \subset (f) + I$. Furthermore, since $f \notin I$ we see that $I \neq (f) + I$. If $(f) + I = k[x_1, \dots, x_n]$ then $1 \in (f) + I$, hence $1 = cf + h$ for some $c \in k[x_1, \dots, x_n]$ and $h \in I$. Multiplying through by g gives

$$g = cfg + hg.$$

But $fg \in I$ by assumption, and $hg \in I$ by construction. Hence $g \in I$; a contradiction. Hence $(f) + I \neq k[x_1, \dots, x_n]$ and so I is not maximal.

(b) First we consider $(x^2 + 1) \subset \mathbb{C}[x]$. Since $x^2 + 1 = (x - i)(x + i)$, we see that $(x^2 + 1)$ is not prime, and hence cannot be maximal.

Now we consider $(x^2 + 1) \subset \mathbb{R}[x]$. Suppose that $J \subset \mathbb{R}[x]$ is an ideal containing $(x^2 + 1)$. Since $\mathbb{R}[x]$ is a principal ideal domain, we can write $J = (f)$ for some $f \in \mathbb{R}[x]$. Since $x^2 + 1 \in (f)$, we have that $f \mid x^2 + 1$. But $x^2 + 1$ is irreducible, hence, up to multiplication by a non-zero constant, $f = 1$ or $f = x^2 + 1$. Since in the first case we have that $J = \mathbb{R}[x]$, and in the second case that $J = (x^2 + 1)$, we conclude that $(x^2 + 1)$ is maximal.

(c) Let $I \subset \mathbb{R}[x_1, \dots, x_n]$ be maximal, and suppose that $\mathbb{V}(I) \neq \emptyset$. Then there exists some point $(a_1, \dots, a_n) \in \mathbb{V}(I) \subset \mathbb{R}^n$. In particular, $I \subset (x_1 - a_1, \dots, x_n - a_n)$. Clearly $(x_1 - a_1, \dots, x_n - a_n) \neq \mathbb{R}[x_1, \dots, x_n]$, so by maximality of I we have that $I = (x_1 - a_1, \dots, x_n - a_n)$. Hence $\mathbb{V}(I) = \mathbb{V}(x_1 - a_1, \dots, x_n - a_n) = \{(a_1, \dots, a_n)\}$.