M E T U
Department of Mathematics

	Ideals, Varieties and Algorithms Midterm 2	

Code : *Math 473* Acad. Year : *2019-2020* Semester : *Fall* Instructor : *Tolga Karayayla*	Last Name : First Name : Student ID : Department : Signature :
Date : *10.12.2019* Time : *17.40* Duration : *120 minutes*	5 Questions on 4 Pages SHOW DETAILED WORK!

1	2	3	4	5		

NOTE: k is a field in all questions below.

1. (3×5 pts.) For a fixed monomial order let G be a Groebner basis for an ideal $I \subset k[x_1, ..., x_n]$, and let $\overline{f}^G$ denote the unique remainder of $f \in k[x_1, ..., x_n]$ on division by elements of G.

a) Show that $\overline{f}^G = \overline{g}^G$ if and only if $f - g \in I$.

$f = f_1 + \overline{f}^G$, $g = g_1 + \overline{g}^G$ where $f_1, f_2 \in I$

$(G = \{h_1, h_2, .., h_s\} \Rightarrow$ By Div. Alg., $f = a_1 h_1 + \cdots + a_s h_s + r$, $\overline{f}^G = r$

$\overline{f}^G = \overline{g}^G \Rightarrow f - g = f_1 + \overline{f}^G - g_1 - \overline{g}^G = f_1 - g_1 \in I$ since $g_1, f_1 \in I$ $\quad a_1 h_1 + \cdots + a_s h_s = f_1)$

$f - g \in I \Rightarrow \overline{f}^G - \overline{g}^G = (f - f_1) - (g - g_1) = (f - g) - f_1 + g_1 \in I. \Rightarrow \overline{\overline{f}^G - \overline{g}^G}^G = 0$

No term of $\overline{f}^G$ and $\overline{g}^G$ is div. by any of $LT(h_1), .., LT(h_s)$ (remainder in Div. Alg.)

so, $\overline{\overline{f}^G - \overline{g}^G}^G = \overline{f}^G - \overline{g}^G$

$0 = \overline{f}^G - \overline{g}^G \Rightarrow \underline{\overline{f}^G = \overline{g}^G}$

b) Conclude that $\overline{f+g}^G = \overline{f}^G + \overline{g}^G$.

since no term of $\overline{f}^G$ and $\overline{g}^G$ is div. by any of $LT(h_1), .., LT(h_s)$, $\overline{\overline{f}^G + \overline{g}^G}^G = \overline{f}^G + \overline{g}^G$

so we want to show $\overline{f+g}^G = \overline{\overline{f}^G + \overline{g}^G}^G$ $(= \overline{f}^G + \overline{g}^G)$

From part a, this is equivalent to show $f + g - (\overline{f}^G + \overline{g}^G) \in I$.

$f = f_1 + \overline{f}^G$, $g = g_1 + \overline{g}^G$ where $f_1, g_1 \in I$ as in part a.

$f + g - (\overline{f}^G + \overline{g}^G) = f_1 + g_1 \in I$ since $f_1, g_1 \in I$, completing the proof.

c) Conclude that $\overline{f \cdot g}^G = \overline{\overline{f}^G \cdot \overline{g}^G}^G$.

From part a, this is equivalent to $f \cdot g - \overline{f}^G \cdot \overline{g}^G \in I$.

$f \cdot g = (f_1 + \overline{f}^G) \cdot (g_1 + \overline{g}^G) = f_1 g_1 + f_1 \overline{g}^G + g_1 \overline{f}^G + \overline{f}^G \cdot \overline{g}^G$

$\Rightarrow f \cdot g - \overline{f}^G \cdot \overline{g}^G = f_1 g_1 + f_1 \overline{g}^G + g_1 \overline{f}^G \in I$ since $f_1, g_1 \in I$. This completes the proof.

2. (20 + 5 + 5 pts.) a) Use Buchberger's Algorithm to compute a Groebner basis of the ideal $I = \langle x^2y^2 + x + 1, xy^3 + y + 1\rangle$ with respect to *lex* order where $x > y > z$.

$f_1 = x^2y^2 + x + 1$, $f_2 = xy^3 + y + 1$, $G_1 = \{f_1, f_2\}$, $S(f_1, f_2) = y(x^2y^2 + x + 1) - x(xy^3 + y + 1) = y - x$

$-x + y = 0 \cdot f_1 + 0 \cdot f_2 + (-x + y) \Rightarrow \overline{-x+y}^{G_1} = \boxed{-x + y = f_3} \Rightarrow G_2 = \{f_1, f_2, f_3\}$

$S(f_1, f_3) = 1 \cdot (x^2y^2 + x + 1) + xy^2(-x + y) = xy^3 + x + 1$

$xy^3 + x + 1 = 0 \cdot f_1 + 1 \cdot f_2 - 1 \cdot f_3 + 0 \Rightarrow \overline{S(f_1, f_3)}^{G_3} = 0.$

$S(f_2, f_3) = 1 \cdot (xy^3 + y + 1) + y^3(-x + y) = y^4 + y + 1 = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + \boxed{y^4 + y + 1 = f_4}$ $\overline{S(f_2, f_3)}^{G_2} = f_4$

$\Rightarrow G_3 = \{f_1, f_2, f_3, f_4)$

$S(f_1, f_4) = y^2(x^2y^2 + x + 1) - x^2(y^4 + y + 1) = -x^2y - x^2 + xy^2 + y^2 = (xy + x + y)(-x + y)$

$= 0f_1 + 0f_2 + (xy + x + y)f_3 + 0f_4 + 0$

$\Rightarrow \overline{S(f_1, f_4)}^{G_3} = 0$

$S(f_2, f_4) = y(xy^3 + y + 1) - x(y^4 + y + 1) = -xy - x + y^2 + y = (-x + y) \cdot (y + 1)$

$= 0f_1 + 0f_2 + (y + 1)f_3 + 0 \cdot f_4 + 0$

$\Rightarrow \overline{S(f_2, f_4)}^{G_3} = 0.$

$S(f_3, f_4) = y^4(-x + y) + x(y^4 + y + 1) = xy + x + y^5 = (-x + y) \cdot (-y - 1) + y^5 + y^2 + y$

$= 0 \cdot f_1 + 0 \cdot f_2 + (-y - 1)f_3 + y \cdot f_4 + 0$

$\Rightarrow \overline{S(f_3, f_4)}^{G_3} = 0.$

We processed all $S(f_i, f_j)$, $1 \leq i < j \leq 4$.

$G_3 = \{f_1, f_2, f_3, f_4)$ is a Gr. Basis of I by Buchberger's Algorithm.

2.b) What is the reduced Groebner basis of I?

$LT(f_3) = -x$, make f_3 monic by replacing it by $\bar{f}_3 = \frac{f_3}{-1} = x - y$.

$\tilde{G} = \{f_1, f_2, \bar{f}_3, f_4\}$ → all are monic.

$LT(\bar{f}_3) = x \mid LT(f_1) = x^2y^2$ and $LT(\bar{f}_3) = x \mid xy^3 = LT(f_2)$

⇒ We can eliminate f_1, f_2 from $\tilde{G}$, to get $\tilde{\tilde{G}} = \{\bar{f}_3, f_4\} = \{x-y, y^4+y+1\}$

$LT(\bar{f}_3) \nmid LT(f_4)$, $LT(f_4) \nmid LT(\bar{f}_3)$ ⇒ $\tilde{\tilde{G}}$ is a minimal Gr. Basis.

No term of f_4 is div. by $x = LT(\bar{f}_3)$
No term of $\bar{f}_3$ is div. by $y^4 = LT(f_4)$ } ⇒ Hence $\tilde{\tilde{G}}$ is the reduced Gr. Basis

c) How many points are there in $V(I) \subset \mathbb{C}^2$?

$I = \langle \tilde{\tilde{G}} \rangle = \langle x-y, y^4+y+1 \rangle$

$V(I) = V(y^4+y+1, x-y)$ ⇒ $x - y = 0$
$y^4 + y + 1 = 0$ ⇒ At most 4 sol. in $\mathbb{C}$
4 sol counted with multiplicity

$(y^4+y+1)' = 4y^3+1$
$f = y^4+y+1$ has a repeated root ⇔ f and f' have a common root.

$f' = 0 \Rightarrow 4y^3+1 = 0 \Rightarrow y^3 = -\frac{1}{4}$

$y^3 = -\frac{1}{4} \Rightarrow y^4+y+1 = -\frac{1}{4}y + y + 1 = \frac{3y}{4} + 1 \neq 0$ since $y \neq -\frac{4}{3}$

f and f' do not have a common root, so f has 4 distinct roots $y \in \mathbb{C}$,
$(x, y) = (y, y) \in \mathbb{C}^2$ has 4 distinct values. $(x = y)$

$V(I)$ has 4 points.

3. (15 + 5 pts.) a) Is $\{x^3z + xy, xy^4 - xz\}$ a Groebner basis of the ideal $I = \langle x^3z + xy, xy^4 - xz \rangle$ with respect to *grlex* order where $x > y > z$?

$f_1 = x^3z + xy$, $f_2 = xy^4 - xz$, $S(f_1, f_2) = y^4 \cdot (x^3z + xy) - x^2z(xy^4 - xz) = x^3z^2 + xy^5$
$(LT = xy^5)$

$$
\begin{array}{l|l}
 & a_1 : z \qquad a_2 : y \\
x^3z + xy & xy^5 + x^3z^2 \\
xy^4 - xz & \underline{-\; xy^5 - xyz} \\
 & x^3z^2 + xyz \\
 & \underline{-\; x^3z + xyz} \\
 & 0
\end{array}
$$

⇒ $S(f_1, f_2) = z f_1 + y f_2 + 0$

$G = \{f_1, f_2\}$ ⇒ $\overline{S(f_1, f_2)}^G = 0$

Therefore, by Buchberger's Criterion
$G = \{f_1, f_2\}$ is a Groebner Basis of $I = \langle f_1, f_2 \rangle$

b) Is $x^2y^3z^2 + xy^4z$ in I?

Since $G = \{f_1, f_2\}$ is a Gr. Basis of $I = \langle f_1, f_2 \rangle$,

$f \in I \Leftrightarrow \bar{f}^G = 0$.

$$
\begin{array}{l|l l}
 & a_1 = \qquad a_2 = z & r \\
x^3z + xy & x^2y^3z^2 + xy^4z \quad \longrightarrow & x^2y^3z^2 \\
xy^4 - xz & xy^4z & \\
 & \underline{xy^4z - xz^2} & \\
 & xz^2 \quad \longrightarrow & x^2y^3z^2 + xz^2
\end{array}
$$

$\bar{f}^G = r = x^2y^3z^2 + xz^2 \neq 0 \in k[x, y, z]$.

Then, $f \notin I$

4. (6 + 4 + 10 pts.) Let $x = st$, $y = s^2$, $z = t^2$ be a parametrization. A Groebner basis for the ideal $I = \langle x - st, y - s^2, z - t^2 \rangle \subset \mathbb{C}[s,t,x,y,z]$ for *lex* order with $s > t > x > y > z$ is given as $G = \{st - x, s^2 - y, t^2 - z, x^2 - yz, sx - ty, sz - tx\}$.

a) Write down generators of the elimination ideals I_1 and I_2.

$I_1 = \langle G \cap k[t,x,y,z] \rangle = \langle t^2 - z, x^2 - yz \rangle$

$I_2 = \langle G \cap k[x,y,z] \rangle = \langle x^2 - yz \rangle$

b) What is the smallest affine variety in $\mathbb{C}^3$ containing the image of this parametrization.

By polynomial implicitization Thm, since $\mathbb{C}$ is infinite field, answer is $V(I_2)$
$= V(x^2 - yz)$

c) Show that the image of the parametrization equals the variety in part (b) in $\mathbb{C}^3$, but if the parametrization is considered from $\mathbb{R}^2$ to $\mathbb{R}^3$, then the image of the parametrization is not equal to this variety in $\mathbb{R}^3$.

Let $(x,y,z) \in V(I_2) = V(x^2 - yz) \subseteq \mathbb{C}^3$ be a partial solution.

By Extension Thm ($\mathbb{C}$ is alg. closed), $(x,y,z) \notin V(1, x^2 - yz)$ $(=\emptyset)$ $\Rightarrow$ it extends to $V(I_1) \subseteq \mathbb{C}^4$

(1 = coef. of t^2 in $t^2 - z \in I_1$, $x^2 - yz$: coef. of t^0 in $x^2 - yz \in I_1$) so (satisfied) $(t,x,y,z) \in$

similarly, by Ext. Thm $(t,x,y,z) \in V(I_1)$ extends to $(s,t,x,y,z) \in V(I)$

since $(t,x,y,z) \notin V(1, \ldots) = \emptyset$

If we work over $\mathbb{R}$, we can't use Ext. Thm ($\mathbb{R}$ is not alg. closed) 1: coef. of s^2 in $s^2 - y \in V(I)$

To show $V(x^2 - yz) \subseteq \mathbb{R}^3$ is not equal to image of param, we'll show that some $(x,y,z) \in V(x^2 - yz) = V(I_2)$ does not extend to $(s,t,x,y,z) \in V(I) \subseteq \mathbb{R}^5$

(For some $(x,y,z) \in V(x^2 - yz)$ $(\subseteq \mathbb{R}^3)$, there is no $(s,t) \in \mathbb{R}^2$ such that $(s,t,x,y,z) \in V(I)$)

Let $x^2 - yz = 0$

$\left.\begin{array}{l} t^2 - z = 0 \\ s^2 - y = 0 \end{array}\right\} \Rightarrow \begin{array}{l} t^2 = z \\ s^2 = y \end{array}$, $s,t \in \mathbb{R} \Rightarrow y \geq 0, z \geq 0$ in $\mathbb{R}$.

But in $V(x^2 - yz)$, there are points with $y < 0$ or $z < 0$. Infinitely many such $(x,y,z) \in V(I_2) \subseteq \mathbb{R}^2$ do not extend.

For example (r^2, r, r) for any $r \neq 0$, $r \in \mathbb{R}$.

5. (15 pts.) Let $I = \langle f_1, f_2, \ldots, f_r \rangle \subset k[x_1, x_2, \ldots, x_n]$ be a given ideal. How can you determine whether I is a principal ideal or not? Describe an algorithm for this problem. DO NOT write down a code for the algorithm, only describe the process step by step in words. Explain why this algorithm gives the result.

I is principal ideal $\Leftrightarrow I = \langle h \rangle$ for some $h \in k[x_1, \ldots, x_n]$

Let $J = \langle h \rangle$, $I = \langle f_1, f_2, \ldots, f_r \rangle$

$I = J \Leftrightarrow$ Their reduced Groebner Bases are the same.

For $J = \langle h \rangle$, since there is one generator, Buchberger's Alg. gives a Groebner Basis of J as $G = \{h\}$, reduced Gr. Basis of J is $\{\frac{1}{c} \cdot h\}$ where $c = LC(h)$.

Thus, $I = J = \langle h \rangle$ for some $h \Leftrightarrow$ Reduced Gr Basis of I is of the form $\{\frac{1}{c} h\}$

So,

Step 1: Find a Gr. Basis of I by Buchberger's Alg.

Step 2: From this Gr. Basis of I, we can find the reduced Gr. Basis of I

Step 3. If reduced Gr. Basis of I has only one element, then I is principal.
If reduced Gr. Basis has more than one element, then I is not principal.