M E T U
Department of Mathematics

	Ideals, Varieties and Algorithms Final	
Code : *Math 473* Acad. Year : *2019-2020* Semester : *Fall* Instructor : *Tolga Karayayla* Date : *13.01.2020* Time : *9:30* Duration : *120 minutes*	Last Name : First Name : Student ID : Department : Signature :	6 Questions on 4 Pages SHOW DETAILED WORK!

1	2	3	4	5	6		

NOTE: k is a field in all questions below.

1. (3×7 pts.) a) Show that $f \in \mathbb{C}[x]$ has a multiple root (a root with multiplicity greater than 1, a repeated root) if and only if $\mathrm{Res}(f, f', x) = 0$.

Let r be a root of $f(x) \in \mathbb{C}[x]$ with multiplicity $m \in \mathbb{Z}^+$. $f(x) = (x-r)^m \cdot g(x)$, $g(r) \neq 0$.

$f'(x) = m(x-r)^{m-1} \cdot g(x) + (x-r)^m \cdot g'(x)$. $m > 1 \Rightarrow f'(r) = 0$, $m = 1 \Rightarrow f'(r) \neq 0$. } r is a multiple root iff f and f' both vanish on r.

So, f has a multiple root iff f and f' have a common root.

$(\Leftrightarrow)$ $\Leftrightarrow$ f and f' have a common factor (nonconstant) in $\mathbb{C}[x]$

$\Leftrightarrow \mathrm{Res}(f, f', x) = 0$.

$(\Rightarrow)$ r is a common root $\Rightarrow$ $x-r$ is a common factor

$(\Leftarrow)$: $p(x)$ is a common factor $\Rightarrow$ r is a common root of f and f' where $p(r)=0$

such an r exists since $\mathbb{C}$ is alg. closed.

b) Let $f(x,y) = x^3y + x^2y^2 + x^2 + xy + 2y + 1$ and $g(x,y) = x^2y + 2x + y + 1$ in $k[x,y]$. Write down $\mathrm{Res}(f,g,x)$ and $\mathrm{Res}(f,g,y)$ as determinants (do not expand/calculate the determinants).

$f = y \cdot x^3 + (y^2+1) \cdot x^2 + y \cdot x + (2y+1) \cdot x^0$

$g = y \cdot x^2 + 2 \cdot x + (y+1) \cdot x^0$

$$\mathrm{Res}(f,g,x) = \begin{vmatrix} y & 0 & y & 0 & 0 \\ y^2+1 & y & 2 & y & 0 \\ y & y^2+1 & y+1 & 2 & y \\ 2y+1 & y & 0 & y+1 & 2 \\ 0 & 2y+1 & 0 & 0 & y+1 \end{vmatrix}$$

$f = x^2 \cdot y^2 + (x^3+x+2) \cdot y + (x^2+1) \cdot y^0$

$g = (x^2+1) \cdot y + (2x+1) y^0$

$$\mathrm{Res}(f,g,y) = \begin{vmatrix} x^2 & x^2+1 & 0 \\ x^3+x+2 & 2x+1 & x^2+1 \\ x^2+1 & 0 & 2x+1 \end{vmatrix}$$

c) When two polynomials $p(x,y)$ and $q(x,y) \in k[x,y]$ are given, can you determine whether p and q are relatively prime or not by using resultants without factorizing p and q and without calculating their greatest common divisor? If yes, how and why? If no, why not?

Yes. Compute $\mathrm{Res}(p,q,x)$ and $\mathrm{Res}(p,q,y)$

$\mathrm{Res}(p,q,x) = 0 \Leftrightarrow p(x,y)$ and $q(x,y)$ have a common factor with positive degree in x.

$\mathrm{Res}(p,q,y) = 0 \Leftrightarrow p$ and q have a common factor with positive degree in y in $k[x,y]$.

p and q are relatively prime $\Leftrightarrow$ p and q do not have any nonconstant common factor.

nonconstant polynomials have positive degree in at least one of x and y.

$\Leftrightarrow \mathrm{Res}(p,q,x) \neq 0$ AND $\mathrm{Res}(p,q,y) \neq 0$

not the 0 polynomial.

2. (2 × 7 pts.) a) Let k be an infinite field. Let $f, g \in k[x_1, x_2, ..., x_n]$ ($f \neq 0$ polynomial) satisfy $g(x_1, ..., x_n) = 0$ for all $(x_1, ..., x_n) \in k^n - V(f)$. Show that g is the zero polynomial. (Hint: consider fg).

$f\cdot g(x_1,\dots,x_n) = f(x_1,\dots,x_n)\cdot g(x_1,\dots,x_n) = 0$ for all $(x_1,\dots,x_n)\in k^n$

(since $f(x_1,\dots,x_n)\neq 0 \Rightarrow g(x_1,\dots,x_n)=0$ because g vanishes on $k^n - V(f)$)

$f\cdot g$ is 0 function on k^n and k is infinite $\Rightarrow$ $f\cdot g$ is 0 polynomial

$f\cdot g=0$ in $k[x_1,\dots,x_n]$ and $f\neq 0$ in $k[x_1,\dots,x_n]$, thus $g=0$ in $k[x_1,\dots,x_n]$

since $k[x_1,\dots,x_n]$ is an integral domain (no zero divisors)

b) Let k be an infinite field and $W \subset k^n$ ($W \neq k^n$) be an affine variety. Show that if $g \in k[x_1, ..., x_n]$ vanishes on all points of $k^n - W$, then g is the zero polynomial (you can use the fact given in part (a) above even if you did not answer part (a)).

Let $W = V(f_1, f_2, \dots, f_r)$. At least one f_i must be nonzero (otherwise $W = k^n$)

If $f_i \neq 0$, $W = V(f_1,\dots,f_s) \subseteq V(f_i)$

so $k^n - W \supseteq k^n - V(f_i)$

g vanishes on $k^n - W \Rightarrow g$ vanishes on $k^n - V(f_i)$ and by part (a) above

we get $g = 0$ polynomial (since $f_i \neq 0$ polynomial)

3. (13 pts.) For $J = \langle xy, (x-y)x\rangle \subset k[x, y]$, show that $\sqrt{J} = \langle x\rangle$. (Note that k here can be any field, k is not necessarily algebraically closed.)

$(x-y)\cdot x = x^2 - xy \in J$ and $xy \in J \Rightarrow x^2 = (x^2 - xy) + xy \in J$, $x^2 \in J \Rightarrow x \in \sqrt{J} \Rightarrow \langle x\rangle \subseteq \sqrt{J}$

Note that $\sqrt{J} \subseteq I(V(J))$

$\left.\begin{array}{l} xy = 0 \\ (x-y)x = 0 \end{array}\right\} \Rightarrow x = 0 \vee y = 0.$ $\left.\begin{array}{l} x=0 \Rightarrow \text{both equations hold.} \\ y = 0 \Rightarrow x^2 = 0 \Rightarrow x = 0 \end{array}\right\} \Rightarrow V(J) = \{(0,y) \mid y \in k\} = V(x)$

$f(x,y) \in \sqrt{J} \subseteq I(V(J)) \Rightarrow f$ vanishes on all of $V(J) \Rightarrow f(0,y) = 0$ for all $y \in k$.

We can write $f(x,y) = h(x,y)\cdot x + g(y)$ (Do Div. Alg. in lex order with $x > y$)

$f(0,y) = h(0,y)\cdot 0 + g(y) = 0$ for all $y \Rightarrow g(y) = 0$ for all $y \in k$

If k is an infinite field, then g is 0 poly., so $f = h\cdot x \in \langle x\rangle \Rightarrow \sqrt{J} \subseteq \langle x\rangle$

For the complete answer including finite field k case:

$f \in \sqrt{J}$, $f = h\cdot x + g(y)$, $f^m \in J = \langle xy, x^2 - xy\rangle = \langle xy, x^2\rangle$

By binomial expansion:

$f^m = h^m x^m + m h^{m-1} x^{m-1} g + \dots + m h x g^{m-1} + g^m = H_1 xy + H_2 x^2$ $(H_1, H_2 \in k[x,y])$

$x \cdot F(x,y) + g^m = H_1 xy + H_2 x^2$

all terms are divisible by x, so $g^m = (g(y))^m = 0$

non zero $\Rightarrow$ not div. by x.

Thus $f(x,y) = h(x,y)\cdot x \in \langle x\rangle \Rightarrow \sqrt{J} \subseteq \langle x\rangle$

$\sqrt{J} = \langle x\rangle$

4. (2×8 pts.) a) Let $J = \langle x^2 + y^2 - 1, y - 1 \rangle \subset k[x, y]$. Find an $f \in I(V(J))$ such that $f \notin J$.

$\left.\begin{array}{l} x^2+y^2-1=0 \\ y-1=0 \end{array}\right\} \Rightarrow y=1,\ x^2+1-1=0 \Rightarrow x=0 \Rightarrow (x,y)=(0,1) \Rightarrow V(J)=\{(0,1)\}$

$x \in I(V(J)) = I(\{(0,1)\})$ since $x=0$ on $(0,1)$.

$x \notin \langle x^2+y^2-1, y-1 \rangle$ since: $x = h(x,y)\cdot(x^2+y^2-1) + g(x,y)\cdot(y-1) + x$ (Div. Alg in lexorder)

$S(x^2+y^2-1, y-1) = y(x^2+y^2-1) - x^2(y-1) = x^2+y^3-y = 1.(x^2+y^2-1) + y^3-y^2-y+1$

S-polynomial has 0 remainder on Div. by $(x^2+y^2-1, y-1)$ $= 1(x^2+y^2-1) + (y^2-1)(y-1)+0$

So $\{x^2+y^2-1, y-1\}$ is a Groebner Basis of $J = \langle x^2+y^2-1, y-1\rangle$ by Buchberger's Criterion.

Then $x \notin J$ since remainder of x by a Gr. basis is not 0.

b) If k is $\mathbb{C}$, is J a radical ideal?

$\mathbb{C}$ is algebraically closed, so by Nullstellensatz, $I(V(J)) = \sqrt{J}$

If J is radical, $\sqrt{J} = J$, so $I(V(J)) = J$, contradicting there is $f \in I(V(J)) - J$ in part a.

5. (12 pts.) For the rational parametrization $x = \dfrac{st^2}{1+s^2t^3}$, $y = \dfrac{s+t}{st}$, $z = \dfrac{s^2+t^2}{st+t^4}$ in $\mathbb{R}^3$, how can you find the smallest affine variety in $\mathbb{R}^3$ which contains the image of this parametrization? Explain the process step by step, do not carry out the computations.

1) Let w be a new variable. Let $g = (1+s^2t^3)\cdot st\cdot(st+t^4)$.
Define the ideal $J = \langle (1+s^2t^3)x - st^2,\ sty-(s+t),\ (st+t^4)z-(s^2+t^2),\ 1-w\,g(s,t) \rangle$ in $k[w,s,t,x,y,z]$.

2) Using lexorder with $w>s>t>x>y>z$, find a Groebner basis G of J (Buchberger's Alg.)

3) Let $J_3 = J \cap k[x,y,z]$ be the 3rd elimination ideal of J.
$J_3 = \langle G \cap k[x,y,z] \rangle$

(J_3 is gen. by the elements of the finite set G which are in $k[x,y,z]$)

4) $V(J_3)$ is the smallest affine variety in $\mathbb{R}^3$ that contains the image of the parametrization.

(by rational implicitization Thm since $\mathbb{R}$ is an infinite field).

6. (3×8 pts.) For each problem below, explain its solution method/procedure step by step. Do not prove why this procedure solves the problem, only list what to do in order to solve the problem.

a) When an ideal $I = \langle f_1, f_2, ..., f_s \rangle$ and a polynomial f is given in $k[x_1, ..., x_n]$, how do you determine whether $f \in \sqrt{I}$ or not?

1) Let y be a new variable. Define the ideal $J = \langle f_1, f_2, , f_s, 1-yf \rangle$

2) Then $f \in \sqrt{I} \Leftrightarrow 1 \in J$

3) We can check if $1 \in J$ or not by finding a Groebner Basis of J:
$1 \in J \Leftrightarrow$ Division of 1 by a Gr. Basis of J gives 0 remainder.
$\Leftrightarrow$ Groebner Basis of J contains a nonzero constant.

b) For two ideals $I = \langle f_1, f_2, f_3 \rangle$ and $J = \langle g_1, g_2 \rangle$ in $k[x, y]$, how do you find generators of the ideal $I \cap J$?

1) Define the ideal $P = \langle t \cdot f_1, t \cdot f_2, t \cdot f_3, (1-t) \cdot g_1, (1-t) \cdot g_2 \rangle$ in $k[t, x_1, , x_n]$.

2) $I \cap J = P_1$: the first elimination ideal of P with lex order $t > x_1 > \cdots > x_n$

3) To find P_1, first find a Gr. Basis G of P with lex order $t > x_1 > \cdots > x_n$.
Then let $G_1 = G \cap k[x_1, , x_n]$.
We have $P_1 = \langle G_1 \rangle$

c) For two polynomials $f, g \in k[x_1, x_2, ..., x_n]$, how do you calculate a greatest common divisor of f and g without using factorization of f and g into a product of irreducibles? (Note that $n \geq 2$ here. Even if you did not answer part (b) above, here you can use part (b) directly without explaining how it is solved)

1) $\langle LCM(f, g) \rangle = \langle f \rangle \cap \langle g \rangle$

2) Find generators of $I = \langle f \rangle \cap \langle g \rangle$ using part b algorithm.

3) Find a Gr. Basis of I.

4) Find "THE" reduced gr. basis of I, since $I = \langle LCM(f, g) \rangle$ is principal, reduced gr. basis of I must be a single element set $\{h\}$.
So $I = \langle h \rangle = \langle LCM(f, g) \rangle$.
h is a least common multiple of f and g.

5) Using $f \cdot g = LCM(f, g) \cdot GCD(f, g)$
we get $\frac{f \cdot g}{h}$ is a greatest common divisor of f and g.