Scott [illegible]
20003[illegible]14

MODEL SOLUTIONS #5

21 Jul. 2006

MATH 800 Assignment #5

4.3.6. a) Let I_1, I_2 and J be ideals in $k[x_1,\ldots,x_n]$. Show that $(I_1+I_2)J = I_1J + I_2J$.

Proof: ($\subset$). Let $f \in (I_1+I_2)J$. Then $\exists\, g_i \in I_1+I_2$ and $j_i \in J$ s.t. $f = \sum_{i=1}^{r} g_i j_i$ (for some $r>0$).
But $g_i \in I_1+I_2 \Rightarrow \exists\, h_i \in I_1$ and $l_i \in I_2$ s.t. $g_i = h_i + l_i$. Then
$f = \sum_{i=1}^{r}(h_i+l_i)j_i = \sum_{i=1}^{r}(h_ij_i + l_ij_i) = \sum_{i=1}^{r} h_ij_i + \sum_{i=1}^{r} l_ij_i$.
Now $h_i \in I_1$ and $j_i \in J \Rightarrow \sum_{i=1}^{r} h_ij_i \in I_1J$. ✓ Similarly $\sum_{i=1}^{r} l_ij_i \in I_2J$. ✓
$\Rightarrow f \in I_1J + I_2J$.

5

$\therefore (I_1+I_2)J \subset I_1J + I_2J$.

($\supset$). Let $f \in I_1J + I_2J$. Then $\exists\, f_1 \in I_1J$ and $f_2 \in I_2J$ s.t. $f = f_1 + f_2$. ✓
But then $\exists\, g_i \in I_1$ and $j_i \in J$ s.t. $f_1 = \sum_{i=1}^{r} g_ij_i$ (for some $r>0$). ✓
Now $g_i \in I_1$ and $0 \in I_2 \Rightarrow g_i + 0 = g_i \in I_1 + I_2$, so $f_1 \in (I_1+I_2)J$. ✓
Similarly $f_2 \in (I_1+I_2)J$. ✓
Then, since $(I_1+I_2)J$ is an ideal (and hence closed under $+$),
$f = f_1 + f_2 \in (I_1+I_2)J$. ✓
$\therefore I_1J + I_2J \subset (I_1+I_2)J$, and now equality follows. $\square$

5 4.6.8. [See Maple attachment.]

4.6.9. For an arbitrary field, show that $\sqrt{IJ} = \sqrt{I\cap J}$.

Proof: $f \in \sqrt{IJ} \Rightarrow f^m \in IJ \Rightarrow f^m \in I\cap J \Rightarrow f \in \sqrt{I\cap J}$ (for some $m \geq 1$) ✓ ✓
since $IJ \subset I \cap J$ (see discussion following Proposition 9).
Thus $\sqrt{IJ} \subset \sqrt{I\cap J}$.

3

Let $f \in \sqrt{I\cap J}$. Then $f^m \in I\cap J$ for some $m \geq 1$
$\Rightarrow f^m \in I$ and $f^m \in J$
$\Rightarrow f^m \cdot f^m = f^{2m} \in IJ$
$\Rightarrow f \in \sqrt{IJ}$ ✓
Thus $\sqrt{I\cap J} \subset \sqrt{IJ}$, and equality follows. $\square$

Give an example to show that the product of radical ideals need not be radical.

Let $I = J = \langle x \rangle$. Then I and J are radical, since $\sqrt{\langle x \rangle} = \langle x \rangle$.
However $IJ = \langle x^2 \rangle$ is not radical, since $\sqrt{\langle x^2 \rangle} = \langle x \rangle$. ✓

2

Give an example to show that $\sqrt{IJ}$ can differ from $\sqrt{I}\sqrt{J}$.

Again let $I = J = \langle x \rangle$. Then $\sqrt{IJ} = \sqrt{\langle x^2 \rangle} = \langle x \rangle$ while $\sqrt{I}\sqrt{J} = IJ = \langle x^2 \rangle$. ✓

4.4.1 (a) Find the Zariski closure of the projection of the hyperbola $\mathbb{V}(xy-1) \subset \mathbb{R}^2$ onto the x-axis.

The hyperbola $\mathbb{V}(xy-1) = \{(x, \frac{1}{x}) : x \in \mathbb{R} - \{0\}\}$. $(xy - 1 = 0 \Rightarrow y = \frac{1}{x})$

So the projection onto the x-axis is

2

$S = \{(x, 0) : x \in \mathbb{R} - \{0\}\}$
$\quad = \{(x, 0) : x \in \mathbb{R}\} - \{(0,0)\}$.

Any polynomial $f \in \mathbb{I}(S) \subset \mathbb{R}[x,y]$ must be a multiple of y:
$f = gy + r$ for some $g, r \in \mathbb{R}[x,y]$ with $r = 0$ or no term of r is divisible by y (Division algorithm).

✓
$\Rightarrow r \in \mathbb{R}[x]$.
Then $f \in \mathbb{I}(S) \Rightarrow 0 = f(x,0) = g(x,0)\cdot 0 + r(x) \quad \forall x \in \mathbb{R} - \{0\}$
$\Rightarrow r(x) = 0 \quad \forall x \in \mathbb{R} - \{0\}$
$\Rightarrow r = 0$ since r has infinitely many roots. ✓

$\Rightarrow f = gy$.

Also any polynomial multiple of y is in $\mathbb{I}(S)$, so $\mathbb{I}(S) = \langle y \rangle$.
Thus the Zariski closure of S is
$\bar{S} = \mathbb{V}(\mathbb{I}(S)) = \mathbb{V}(\langle y \rangle) = \{(x,0) : x \in \mathbb{R}\}$.
That is $\bar{S} = S \cup \{(0,0)\}$ is the entire x-axis. ✓

2 4.4.2. [See Maple attachment.]

4.4.3. Let I and J be ideals. Show that if I is a radical ideal, Then $I:J$ is a radical and $I:J = I:\sqrt{J}$.

$\langle x^2\rangle : \langle y^2\rangle = \langle x^2\rangle$
$\langle y\rangle$

$\langle x^4\rangle : \langle x^3\rangle = \langle x^4\rangle : \langle x\rangle$
$\langle x\rangle = \langle x^3\rangle$

Proof: Let $f^m \in I:J$.
Then $f^m \cdot g \in I \ \forall g \in J$
✓ $\Rightarrow (fg)^m = (f^m \cdot g)\cdot g^{m-1} \in I \ \forall g \in J$
✓ $\Rightarrow fg \in I \ \forall g \in J$ (since I is radical)
✓ $\Rightarrow f \in I:J$
$\therefore$ $I:J$ is a radical ideal.

$\frac{4}{6}$

$(\supseteq)$ $f \in I:\sqrt{J} \Rightarrow fg \in I \ \forall g \in \sqrt{J}$
$\Rightarrow fg \in I \ \forall g \in J$ (since $J \subset \sqrt{J}$) ✓
$\Rightarrow f \in I:J$ ✓

So $I:\sqrt{J} \subset I:J$.

$(\subseteq)$ $f \in I:J \Rightarrow fg \in I \ \forall g \in J$ ~~NOT $\forall$~~
$\Rightarrow fg^m = (fg)\cdot g^{m-1} \in I) \ \forall g \in J \ \forall m \in \mathbb{N}$
You need to use $\Rightarrow fg^m \in I \ \forall g^m \in \sqrt{J}$ X
I is radical somewhere! $\Rightarrow f \in I:\sqrt{J}$

Thus $I:J \subset I:\sqrt{J}$, $\therefore$ $I:J = I:\sqrt{J}$. □

4.4.6. Prove Proposition 10 (for the case $r=2$) and find geometric interpretations.
Let I, J, K be ideals in $k[x_1, \dots, x_n]$.
a) $(I \cap J) : K = (I:K) \cap (J:K)$.

Proof: $f \in (I \cap J):K \Leftrightarrow fg \in I \cap J \ \forall g \in K$
$\Leftrightarrow fg \in I$ and $fg \in J \ \forall g \in K$
$\Leftrightarrow f \in I:K$ and $f \in J:K$
$\Leftrightarrow f \in (I:K) \cap (J:K)$ ✓

$\therefore$ $(I \cap J):K = (I:K) \cap (J:K)$. □

In terms of varieties, we have
$\overline{(U \cup V) - W} = \overline{(U-W) \cup (V-W)}$
$\Rightarrow \overline{(U \cup V) - W} = \overline{(U-W)} \cup \overline{(V-W)}$. ✓

b) $I:(J+K) = (I:J)\cap(I:K)$.

Proof: $f\in I:(J+K) \Leftrightarrow fg\in I\ \forall g\in J+K$
$\Leftrightarrow fh_1+fh_2 = f(h_1+h_2)\in I\ \forall h_1\in J,\ h_2\in K$
$\Leftrightarrow fh_1\in I\ \forall h_1\in J$ and $fh_2\in I\ \forall h_2\in K$
✓ (($\Rightarrow$) by taking $h_2=0$, $h_1=0$; ($\Leftarrow$) since I closed under $+$)
$\Leftrightarrow f\in I:J$ and $f\in I:K$ ✓
$\Leftrightarrow f\in (I:J)\cap(I:K)$ ✓
$\therefore I:(J+K) = (I:J)\cap(I:K)$. □

10

In terms of varieties, we have
$$U-(V\cap W) = (U-V)\cup(U-W) \quad ✓$$
$$\Rightarrow \overline{U-(V\cap W)} = \overline{(U-V)}\cup\overline{(U-W)}$$

c) $(I:J):K = I:JK$ $\quad \{h : hl\in I\ \forall l\in J\} = \{h : hJ\subset I\}$

$JK = \langle fg_j : f\in J, g\in K\rangle$

Proof: $f\in (I:J):K \Leftrightarrow (fg\in I:J)\ \forall g\in K$
✓ $\Leftrightarrow (fgh\in I\ \forall h\in J)\ \forall g\in K$ ✓ ?
✓ $\Leftrightarrow fp\in I\ \forall p\in JK$ ✓
(($\Rightarrow$): $p \overset{\in JK}{=} \sum g_i h_i$, $h_i\in J$, $g_i\in K$, so $fp = \sum (fg_ih_i) \in I$; ?
($\Leftarrow$): if $h\in J$, $g\in K$ then $gh\in JK$, so $fgh\in I$)
$\Leftrightarrow f\in I:JK$ ✓
$\therefore (I:J):K = I:JK$. □

In terms of varieties, we have
$$(U-V)-W = U-(V\cup W) \quad ✓$$
$$\Rightarrow \overline{(U-V)-W} = \overline{U-(V\cup W)}.$$

4.5.2. Show that a prime ideal is radical.

Proof: Let $I \in k[x_1,\dots,x_n]$ be a prime ideal.
TAC suppose I is not radical.
Then $\exists\, f \in k[x_1,\dots,x_n]$ and $m \in \mathbb{N}$ s.t. $f^m \in I$ but $f \notin I$.
Choose m to be the smallest exponent for which $f^m \in I$. ✓

5

Now $f \notin I \Rightarrow$ ~~Clearly~~ $m \geq 2$.
Then $f \cdot f^{m-1} = f^m \in I$, where $f, f^{m-1} \in k[x_1,\dots,x_n]$, but $f \notin I$ and $f^{m-1} \notin I$ (by choice of m). This contradicts that I is prime. ✓
$\therefore$ I must be radical. □

* 4.5.10. Prove that Theorem 11 implies the Weak Nullstellensatz.
[k alg closed & $\emptyset = \mathbb{V}(I) \Rightarrow I = \langle 1 \rangle$]

Proof: Let k be an algebraically closed field, and let $I \subset k[x_1,\dots,x_n]$ be an ideal satisfying $\mathbb{V}(I) = \emptyset$.
TAC suppose I is a proper ideal, i.e. $I \neq k[x_1,\dots,x_n]$.
Claim: $\exists$ a maximal ideal J containing I (perhaps I itself).
If I is maximal then we are done with $J = I$.
Otherwise $\exists$ an ideal I_1 s.t. $I \subsetneq I_1 \subsetneq k[x_1,\dots,x_n]$.

5

Either I_1 is maximal, or $\exists$ an ideal I_2 s.t. $I_1 \subsetneq I_2 \subsetneq k[x_1,\dots,x_n]$.
Continuing, we must eventually terminate with a maximal ideal I_k, otherwise we would have an infinite proper ascending chain of ideals $I \subsetneq I_1 \subsetneq I_2 \subsetneq \dots$, which is impossible. OK ✓
By Theorem 11, $J = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ for some $a_1,\dots,a_n \in k$. ✓
So $\mathbb{V}(J) = \{(a_1,\dots,a_n) \in k^n\}$. ✓
But then $I \subset J \subset k[x_1,\dots,x_n] \Rightarrow \mathbb{V}(I) \supset \mathbb{V}(J) \supset \mathbb{V}(k[x_1,\dots,x_n])$
$\Rightarrow \emptyset \supset \{(a_1,\dots,a_n)\} \supset \emptyset$.
This is a contradiction. So I cannot be a proper ideal. ✓
$\therefore$ $I = k[x_1,\dots,x_n]$. □

4.6.2. Show that an irredundant intersection of at least two prime ideals is never prime.

Proof: Let $I \subset k[x_1, \ldots, x_n]$ be an ideal and let $I = P_1 \cap \ldots \cap P_r$ be an irredundant intersection with $r \geq 2$.

$\boxed{\frac{2}{4}}$

Then $\forall P_i$, $1 \leq i \leq r$, $\exists$ an irreducible $f_i \in P_i$ s.t. $f_i \notin P_j$ for some j.

Let $f = f_1 \cdots f_r$. Then $f \in P_i$ $\forall 1 \leq i \leq r$ since P_i is an ideal. ✓

So $f = f_1 \cdots f_r \in I$. ✓

Needs a proof.

But $\forall 1 \leq i \leq r$, $f_i \notin I$ since $\exists$ some j s.t. $f_i \notin P_j$.

$\therefore$ I must not be prime. □

3/5 4.6.4. [See Maple attachment.]

5/6 4.6.7. [See Maple attachment.]

TAC Suppose I is prime.

$f = f_1 f_2 \cdots f_r \in I$ and I is prime $\Rightarrow f_1 \in I$ or $f_2 \cdots f_r \in I$

But $f_1 \notin I \Rightarrow f_2 \cdots f_r \in I$.

Repeating this we obtain $f_{r-1} \in I$ or $f_r \in I$.

But neither are, ~~[illegible]~~ a contradiction.

Additional Exercise 1: Rewrite the proof that $I+J$ is the smallest ideal containing I and J using proof by contradiction.

Proof: TAC suppose there exists an ideal H that contains I and J but does not contain $I+J$, ~~$I+J \not\subset H$.~~ $I+J \supsetneq H \supset I, J$ -1

Then $\exists\, f \in I+J$ s.t. $f \notin H$.

But $f \in I+J \Rightarrow \exists\, g \in I$ and $h \in J$ s.t. $f = g+h$.

Then $I, J \subset H \Rightarrow g, h \in H$

$\Rightarrow f = g+h \in H$ (since H is an ideal), contradicting our choice of f. ✓

$\therefore$ every ideal H containing I and J also contains $I+J$ (so $I+J$ is the "smallest" ideal containing I and J). □

$\boxed{2/3}$

3 Additional Exercise 2: [See Maple attachment.]

Additional Exercise 3: Let $f, g \in GF(p)[x_1, \dots, x_n]$ where $GF(p)$ is the finite field on p elements. Let $S = \mathbb{V}(f) - \mathbb{V}(g)$. Is S an affine variety?

2

$S \subset GF(p)^n$, where $|GF(p)^n| = p^n$, so S is a finite set, ✓

$S = \{s_1, s_2, \dots, s_r\}$ for some $r \le p^n$.

Now for each $s_i = (a_1, \dots, a_n)$ we can construct an ideal I_i s.t. $\mathbb{V}(I_i) = \{s_i\}$, namely

$I_i = \langle x_1 - a_1, \dots, x_n - a_n \rangle$. ✓

Then let $J = \bigcap_{i=1}^{r} I_i$. It follows from Proposition 9 from §4.3 that J is an ideal in $GF(p)[x_1, \dots, x_n]$. ✓

It then follows from Theorem 15 from §4.3 that

$\mathbb{V}(J) = \bigcup_{i=1}^{r} \mathbb{V}(I_i) = \{s_1, \dots, s_r\} = S$. ✓

So we have shown (constructively) that S must be an affine variety.

(The key is that $|S|$ must be finite. This need not hold in an infinite field.)

Additional Exercise 4: Which of the following ideals are prime and which are maximal?

i) $I = \langle x^3+1 \rangle \subset \mathbb{R}[x]$.

$x^3+1 = (x+1)(x^2-x+1)$. $x^3+1 \in I$ but $x+1 \notin I$, so I is not prime. ✓
Then by Proposition 10 of §4.5, I is not maximal. ✓

ii) $I = \langle x^4+1 \rangle \subset \mathbb{R}[x]$.

x^4+1 is irreducible over $\mathbb{R}$. So any polynomial $(x^4+1)\cdot h \in I$ contains x^4+1 as an irreducible factor, and any factorization $(x^4+1)h = fg$ must have $x^4+1 | f$ or $x^4+1 | g$. So either $f \in I$ or $g \in I$. Therefore I is prime. ✓
$1 \notin I$, so $I \neq \mathbb{R}[x]$. Let J be an ideal s.t. $I \subsetneq J$.
Then $\exists f \in J$ s.t. $f \notin I$, i.e. $x^4+1 \nmid f$. But then f and x^4+1 are relatively prime, since x^4+1 is irreducible. That is,
$GCD(x^4+1, f) = 1$.
Then $\exists A, B \in \mathbb{R}[x]$ s.t. $A(x^4+1)+Bf = 1$, so $1 \in J$. Thus $J = \mathbb{R}[x]$.
Therefore I is maximal. ✓

5

iii) $I = \langle x^2+1 \rangle \subset \mathbb{R}[x,y]$.

x^2+1 is irreducible over $\mathbb{R}$. So it follows that I is prime. ✓
Let $J = \langle x^2+1, y \rangle$. Then $I \subset J$ but $I \neq J$. Also $1 \notin J$ (notice that $\{x^2+1, y\}$ is a GB) so $J \neq \mathbb{R}[x,y]$.
Therefore I is not maximal. ✓

iv) $I = \langle x^2+1, y^2+1 \rangle \subset \mathbb{R}[x,y]$.

$(x^2+1)-(y^2+1) = x^2-y^2 = (x+y)(x-y) \in I$, but $x+y \notin I$ (notice that $\{x^2+1, y^2+1\}$ is a GB). So I is not prime. ✓
Then by Proposition 10 of §4.5, I is not maximal. ✓

v) $I = \langle x^2+1, y^2 \rangle \subset \mathbb{R}[x,y]$.

$y^2 = y \cdot y \in I$ but $y \notin I$ (notice that $\{x^2+1, y^2\}$ is a GB), so I is not prime.
Then by Proposition 10 of §4.5, I is not maximal.

Additional Exercise 5:

i) Identify which ideals in $\mathbb{C}[x]$ are maximal.

Since $\mathbb{C}$ is algebraically closed, by Theorem 11 of §4.5 the maximal ideals are
$$\langle x-a \rangle \quad \forall a \in \mathbb{C}.$$

ii) Identify which ideals in $\mathbb{R}[x]$ are maximal.

The ideals in $\mathbb{R}[x]$ are $\langle f \rangle$ $\forall f \in \mathbb{R}[x]$.
If f is reducible then $f = gh$ where $g \neq f$ and $h \neq f$, so $\langle f \rangle \subsetneq \langle g \rangle \subsetneq \langle 1 \rangle$.
2 If f is irreducible then $\forall g \notin \langle f \rangle$ $\langle f, g \rangle = \langle GCD(f,g) \rangle = \langle 1 \rangle$.
So the maximal ideals in $\mathbb{R}[x]$ are
$\langle f \rangle$ s.t. f is irreducible over $\mathbb{R}$.
(eg. $f = x-a$, x^2+a^2, x^4+a^2, etc.)

5 Additional Exercise 6
5 Additional Exercise 7
6/7 Bonus Exercise:
[See Maple attachment.]

MATH 800 Assignment 5
(due July 24, 2006, 9:30)

```
> restart;
```

4.3.8

We enter f and g.

```
> f :=
x^4+x^3*y+x^3*z^2-x^2*y^2+x^2*y*z^2-x*y^3-x*y^2*z^2-y^3*z^2;
g := x^4+2*x^3*z^2-x^2*y^2+x^2*z^4-2*x*y^2*z^2-y^2*z^4;
```

$$f := x^4+x^3y+x^3z^2-x^2y^2+x^2yz^2-xy^3-xy^2z^2-y^3z^2$$
$$g := x^4+2x^3z^2-x^2y^2+x^2z^4-2xy^2z^2-y^2z^4$$

a)

We compute a GB for $\langle f\rangle \cap \langle g\rangle = I \cap k[x,y,z]$, where $I = \langle tf, (1-t)g\rangle \in k[t,x,y,z]$.

```
> Gt := Groebner[Basis]( [t*f, (1-t)*g], lexdeg( [t], [x,y,z] )
  ):
  G1 := remove( has, Gt, t );
```

$$G1 := [2z^2x^3y+z^4x^2y-2z^2xy^3+x^3z^4+2x^4z^2-x^3y^2+x^5-2x^2y^2z^2-xy^2z^4+yx^4 -x^2y^3-z^4y^3]$$

To compute a GB for $\sqrt{\langle f\rangle\langle g\rangle}$, we first note that $\langle f\rangle\langle g\rangle = \langle fg\rangle$ is a principal ideal. Then (if we are working over a field containing the rational numbers) $\sqrt{\langle f\rangle\langle g\rangle} = \langle (fg)_{red}\rangle$ (Proposition 12 of section 4.2).

```
> fg := expand(f*g);
  dfg := map2( diff, fg, [x,y,z] ):
  fg_red := simplify( fg / gcd( fg, gcd( dfg[1], gcd( dfg[2],
  dfg[3] ) ) ) );
```

3

$$fg := -6x^5y^2z^2+x^8-6x^4y^2z^4+3x^6yz^2+3x^5yz^4-6x^4y^3z^2-6x^3y^3z^4-2x^3z^6y^2 +3x^3y^4z^2+3x^2y^4z^4+x^4yz^6-2x^2y^3z^6+3x^2y^5z^2+3xy^5z^4+xy^4z^6+3x^7z^2 -2x^6y^2+3x^6z^4+x^7y-2x^5y^3+x^5z^6+x^4y^4+x^3y^5+y^5z^6$$

$$fg\_red := x^3+z^2x^2-xy^2-y^2z^2$$

As a verification, we factor fg and $(fg)_{red}$.

```
> factor(fg);
  factor(fg_red);
```

$$(x+z^2)^3(x-y)^2(x+y)^3$$
$$(x+z^2)(x-y)(x+y)$$

We see that $(fg)_{red}$ is in fact the reduction of fg. Also, by Proposition 9 of section 4.2, we have $\sqrt{\langle f\rangle\langle g\rangle} = \langle (fg)_{red}\rangle$ over any field, since $x+z^2, x-y, x+y$ are all irreducible factors over any field.

b)

Since (from part (a)) $\langle f\rangle \cap \langle g\rangle$ is a principal ideal, Proposition 13 tells us that its generator is LCM(f, g) Then from Proposition 14 we get $\mathrm{GCD}(f,g)=\dfrac{fg}{\mathrm{LCM}(f,g)}$. We compute $h=\mathrm{GCD}(f,g)$ in this fashion.

```
> h := simplify( f*g/G1[1] );
  evalb( h = gcd(f,g) );
```

$$h := x^3 + z^2 x^2 - x y^2 - y^2 z^2$$

true

c)

We enter p and q.

```
> p := x^2+x*y+x*z+y*z;
  q := x^2-x*y-x*z+y*z;
```

$$p := x^2 + x y + x z + y z$$

$$q := x^2 - x y - x z + y z$$

We compute a GB for $I \cap J = (t\,I + (1-t)\,J) \cap k[x,y,z]$, where $I=\langle f, g\rangle$, $J=\langle p, q\rangle$.

```
> Gt := Groebner[Basis]( [t*f, t*g, (1-t)*p, (1-t)*q], lexdeg(
  [t], [x,y,z] ) ):
  G2 := remove( has, Gt, t );
```

$$G2 := [x^4 + x^3 y + x^3 z^2 - x^2 y^2 + x^2 y z^2 - x y^3 - x y^2 z^2 - y^3 z^2,$$
$$x^2 z^4 - y^2 z^4 - 2 x^2 y z^2 + 2 y^3 z^2 - x^4 - 2 x^3 y + x^2 y^2 + 2 x y^3]$$

Scott Cowan
200034814
scottc@sfu.ca

>

MATH 800 Assignment 5
(due July 24, 2006, 9:30)

```
> restart;
```

4.4.2

We enter f and g.

```
> f := (x+y)^2*(x-y)*(x+z^2);
  g := (x+z^2)^3*(x-y)*(z+y);
```

$$f := (x+y)^2 (x-y)(x+z^2)$$

$$g := (x+z^2)^3 (x-y)(z+y)$$

To compute a basis for $\langle f\rangle : \langle g\rangle$ we first compute a GB for $\langle f\rangle \cap \langle g\rangle$. $= LCM(f, g)$

```
> Gt := Groebner[Basis]( [t*f, (1-t)*g], lexdeg( [t], [x,y,z] )
  ):
  G := remove( has, Gt, t );
```

$$G := [-x^4 y^3 - x^3 y^4 + z^6 x^3 y + 3 x^4 z^4 y + x^6 y + x^5 y^2 + x^3 z^7 + 3 x^4 z^5 + x^6 z + 3 x^5 z^3 - y^3 z^7 + x^5 y z - 3 z^4 y^3 x^2 - z^6 y^3 x - 3 z^4 y^4 x - z^6 y^4 - 3 x^3 y^2 z^3 - x y^2 z^7 - 3 x^3 y^3 z^2 - 3 x^2 y^2 z^5 - x^4 y^2 z - 3 y^3 x^2 z^3 - 3 y^4 x^2 z^2 - 3 y^3 x z^5 - y^3 x^3 z + x^2 z^6 y^2 + 3 x^4 y z^3 + x^2 z^7 y + 3 x^5 z^2 y + 3 x^4 y^2 z^2 + 3 x^3 z^5 y + 3 x^3 z^4 y^2]$$

2

Now by Theorem 11, a basis for $\langle f\rangle : \langle g\rangle$ is found by dividing the basis for $\langle f\rangle \cap \langle g\rangle$ by g. $= \frac{LCM(f,g)}{g}$

```
> B := [simplify( G[1]/g )];
```

$$B := [x^2 + 2 x y + y^2]$$ ✓

Since the basis contains a single polynomial, it is a GB for the principal ideal $\langle f\rangle : \langle g\rangle$.

```
> factor(B[1]);
```

$$(x+y)^2$$ ✓

This makes sense: from the factorizations of f and g we can see that, given any $h \in k[x, y, z]$, $h g$ is divisible by f (hence is in $\langle f\rangle$) iff h is a multiple of $(x+y)^2$.

Scott Cowan
200034814
scottc@sfu.ca

```
>
```

MATH 800 Assignment 5
(due July 24, 2006, 9:30)

```
> restart;
```

4.6.4

a)

We enter the generators for I.

```
> F := [x*z-y^2, x^3-y*z];
```

$$F := [x z - y^2, x^3 - y z]$$

We compute a basis for $I : \langle x^2 y - z^2 \rangle$.

```
> g := x^2*y-z^2;
  Gt := Groebner[Basis]( [op(map( `*`, F, t )), (1-t)*g],
  lexdeg( [t], [x,y,z] ) ):
  G := normal(map( `/`, remove( has, Gt, t ), g ) );
```

Use [seq(t*f, f=F)]

2

$$g := x^2 y - z^2$$

$$G := [y, x]$$

✓

Therefore $I : \langle x^2 y - z^2 \rangle = \langle x, y \rangle$.

b)

0/2

By Proposition 9 of section 4.5, $I : \langle x^2 y - z^2 \rangle = \langle x, y \rangle$ is a maximal ideal. Therefore by Proposition 10 of section 4.5, this is also a prime ideal.

X

$I \subset k[x,y,z]$

X

c)

Now we compute a basis for $\langle x, y \rangle \cap \langle x z - y^2, x^3 - y z, z^2 - x^2 y \rangle$.

```
> Gt := Groebner[Basis]( [op(map( `*`, G, t )), op(map( `*`, F,
  1-t )), (1-t)*(-g)], lexdeg( [t], [x,y,z] ) ):
  GG := remove( has, Gt, t );
  Groebner[Basis]( F, tdeg(x,y,z) );
```

1

$$GG := [-x z + y^2, x^3 - y z]$$

$$[-x z + y^2, x^3 - y z]$$

✓

We see that this intersection equals I.

4.6.7

a)

```
> interface( imaginaryunit = _i ):
  with(PolynomialIdeals):
Warning, the assigned name <,> now has a global binding

Warning, the protected name subset has been redefined and unprotected
```

We enter the ideal I.

```
> I := <x*z-y^2, z^3-x^5>;
```

$$I := \langle x\,z - y^2, z^3 - x^5 \rangle$$

We compute a GB for I and factor it.

```
> G := Groebner[Basis]( I, plex(x,y,z) );
  factor(G);
```

$$G := [y^{10} - z^8, x\,z - y^2, y^8\,x - z^7, y^6\,x^2 - z^6, y^4\,x^3 - z^5, x^4\,y^2 - z^4, -z^3 + x^5]$$

$$[(y^5 - z^4)\,(y^5 + z^4), x\,z - y^2, y^8\,x - z^7, (y^3\,x - z^3)\,(y^3\,x + z^3), y^4\,x^3 - z^5, (x^2\,y - z^2)\,(x^2\,y + z^2), -z^3 + x^5]$$

We will use the factorization of the first polynomial in the GB in computing the decompositions V(I) and I.

```
> f1,f2 := op( factor(G[1]) );
```

$$f1, f2 := y^5 - z^4, y^5 + z^4$$

We compute the quotients $J = I : \langle f_2 \rangle$ and $K = I : \langle f_1 \rangle$.

```
> J := Quotient( I, <f2> );
  K := Quotient( I, <f1> );
```

$$J := \langle -x\,z + y^2, x^2\,y - z^2, -z\,y + x^3 \rangle$$

$$K := \langle -x\,z + y^2, z\,y + x^3, x^2\,y + z^2 \rangle$$

We also compute lexicographic GBs for J and K.

```
> G1 := Groebner[Basis]( J, plex(x,y,z) );
  G2 := Groebner[Basis]( K, plex(x,y,z) );
```

$$G1 := [y^5 - z^4, x\,z - y^2, y^3\,x - z^3, x^2\,y - z^2, -z\,y + x^3]$$

$$G2 := [y^5 + z^4, x\,z - y^2, y^3\,x + z^3, x^2\,y + z^2, z\,y + x^3]$$

Now we have $I = J \cap K$. ✓

```
> Intersect( J, K );
  evalb( Groebner[Basis]( %, plex(x,y,z) ) = G );
```

$$\langle -x\,z + y^2, -z^3 + x^5, -x\,z^2 + z\,y^2, -x^3\,z + y^2\,x^2 \rangle$$

$$true$$

This also means that $\mathrm{V}(I) = \mathrm{V}(J) \cup \mathrm{V}(K)$. If V($J$) and V($K$) are irreducible varieties then we have found a decomposition of V(I) into irreducible varieties. We will show that V(J) and V(K) are irreducible by giving parametrizations for them.

```
> Gt := Groebner[Basis]( [x-t^3, y-t^4, z-t^5], plex(t,x,y,z)
  );
  remove( has, Gt, t );
  evalb( % = G1 );
```

$$Gt := [y^5 - z^4, x\,z - y^2, y^3\,x - z^3, x^2\,y - z^2, -z\,y + x^3, -x^2 + t\,z, -z + t\,y, -y + t\,x, -x + t^3]$$

$$[y^5 - z^4, x\,z - y^2, y^3\,x - z^3, x^2\,y - z^2, -z\,y + x^3]$$ ✓

$$true$$

This shows that $[x, y, z] = [t^3, t^4, t^5]$ is a polynomial parametrization of V(J), in that V(J) is the smallest affine variety containing $\{[t^3, t^4, t^5], t \in R\}$. Also, since the leading coefficient of the last polynomial in Gt, $t^3 - x$, is a constant, by the Extension Theorem every partial solution for $[x, y, z] \in C^3$ extends to a solution for $[t, x, y, z] \in C^4$. We can also see from the other polynomials in Gt that are linear in t that if we have a partial solution $[x, y, z] \in R^3$ then t must also be real, so that the partial solution extends to $[t, x, y, z] \in R^4$. Therefore V(J) is exactly the set $\{[t^3, t^4, t^5], t \in R\}$, and since V($J$) has a polynomial parametrization it is an irreducible variety.

```
> Gt := Groebner[Basis]( [x-t^3, y+t^4, z-t^5], plex(t,x,y,z)
  );
  remove( has, Gt, t );
  evalb( % = G2 );
```

$$Gt := [y^5 + z^4, x z - y^2, y^3 x + z^3, x^2 y + z^2, z y + x^3, -x^2 + t z, z + t y, y + t x, -x + t^3]$$

$$[y^5 + z^4, x z - y^2, y^3 x + z^3, x^2 y + z^2, z y + x^3]$$

true ✓

Similarly $[x, y, z] = [t^3, -t^4, t^5]$ is a polynomial parametrization of V(K), and so V(K) is an irreducible variety.

Therefore the decomposition V(I) = V(J) $\cup$ V(K) is a decomposition into irreducible varieties.

5/6

b)

We have already done most of the work to express I as an intersection of prime ideals. We have shown that $I = J \cap K$. We need to argue that J and K are prime.

```
> IsPrime(J), IsPrime(K);
```

true, true

Use the fact that J and K have polynomial parametriz
⇒ They are prime
Prop 5 of 4.5 and Prop 3.

So we have a decomposition of I into prime ideals. By Exercise 1, this implies that I is a radical ideal.

Finally, we check that $J = I : K$ and $K = I : J$.

```
> J = Quotient( I, K );
  K = Quotient( I, J );
```

$$\langle -x z + y^2, x^2 y - z^2, -z y + x^3 \rangle = \langle -x z + y^2, x^2 y - z^2, -z y + x^3 \rangle$$ ✓

$$\langle -x z + y^2, z y + x^3, x^2 y + z^2 \rangle = \langle -x z + y^2, z y + x^3, x^2 y + z^2 \rangle$$

Scott Cowan
200034814
scottc@sfu.ca

```
>
```

MATH 800 Assignment 5
(due July 24, 2006, 9:30)

```
> restart;
  interface( imaginaryunit = _i ):
  with(PolynomialIdeals):
Warning, the assigned name <,> now has a global binding

Warning, the protected name subset has been redefined and unprotected
```

Additional Exercise 2

We enter $f \in Q[x, y]$ and compute its derivatives $f_x = \frac{\partial}{\partial x} f$ and $f_y = \frac{\partial}{\partial y} f$. The goal here is to compute the GCD of these 3 polynomials.

```
> f :=
  x^5+3*x^4*y+3*x^3*y^2-2*x^4*y^2+x^2*y^3-6*x^3*y^3-6*x^2*y^4+x^3
  *y^4-2*x*y^5+3*x^2*y^5+3*x*y^6+y^7;
  fx := diff(f,x);
  fy := diff(f,y);
```

$$f := x^5 + 3x^4 y + 3x^3 y^2 - 2x^4 y^2 + x^2 y^3 - 6x^3 y^3 - 6x^2 y^4 + x^3 y^4 - 2xy^5 + 3x^2 y^5 + 3xy^6 + y^7$$

$$fx := 5x^4 + 12x^3 y + 9x^2 y^2 - 8x^3 y^2 + 2xy^3 - 18x^2 y^3 - 12xy^4 + 3x^2 y^4 - 2y^5 + 6xy^5 + 3y^6$$

$$fy := 3x^4 + 6x^3 y - 4x^4 y + 3x^2 y^2 - 18x^3 y^2 - 24x^2 y^3 + 4x^3 y^3 - 10xy^4 + 15x^2 y^4 + 18xy^5 + 7y^6$$

3

Letting $I = \langle f \rangle$, $J = \langle f_x \rangle$, $K = \langle f_y \rangle$, we first compute a GB for $J \cap K = (tJ + (1-t)K) \cap Q[x, y]$. Since J, K are principal ideals, their intersection is principal too and we will get a single polynomial in the GB. By Proposition 13 of section 4.3 this polynomial is LCM(f_x,f_y).

```
> Gt := Groebner[Basis]( [t*fx, (1-t)*fy], lexdeg( [t], [x,y] )
  ):
  G1 := remove( has, Gt, t );
```

$$G1 := [-32x^4 y^3 + 20x^5 y - 15x^5 - 14y^7 - 6x^2 y^3 - 137x^3 y^4 - 36x^4 y - 27x^3 y^2 + 107x^4 y^2 + 174x^3 y^3 + 107x^2 y^4 + 20xy^5 - 192x^2 y^5 - 101xy^6 + 21y^8 + 12x^3 y^5 + 45x^2 y^6 + 54xy^7]$$

Now from Proposition 14 of section 4.3, we get $\mathrm{GCD}(f_x, f_y) = \frac{f_x f_y}{\mathrm{LCM}(f_x, f_y)}$. We compute $h = \mathrm{GCD}(f_x, f_y)$ this way.

```
> h := simplify( fx*fy/G1[1] );
```

$$h := -x^3 + x^2 y^2 - 2x^2 y + 2xy^3 - xy^2 + y^4$$ ✓

Now we repeat. To compute GCD(f, h) we first compute a GB for $I \cap L =$

$(t\,I+(1-t)\,L) \cap Q[x,y]$ where $L=\langle h\rangle$. This ideal is also principal so the GB will contain a single polynomial, LCM(f, h). From this we compute $g = \mathrm{GCD}(f, h)$.

```
> Gt := Groebner[Basis]( [t*f, (1-t)*h], lexdeg( [t], [x,y] ) ):
  G2 := remove( has, Gt, t );
  g := simplify( f*h/G2[1] );
```

$G2 :=$

$$[x^5+3\,x^4\,y+3\,x^3\,y^2-2\,x^4\,y^2+x^2\,y^3-6\,x^3\,y^3-6\,x^2\,y^4+x^3\,y^4-2\,x\,y^5+3\,x^2\,y^5+3\,x\,y^6+y^7]$$

$$g := -x^3+x^2\,y^2-2\,x^2\,y+2\,x\,y^3-x\,y^2+y^4$$

This gives $g = \mathrm{GCD}(f, f_x, f_y)$ as desired. We check that it agrees with the gcd computed directly (up to an arbitrary constant factor).

```
> evalb( sign(g)*primpart(g) = gcd( f, gcd( fx, fy ) ) );
```

$$true$$

Additional Exercise 6

We enter the ideal I corresponding to the variety we will decompose.

```
> I := <y*x-x^3, z-x^3>;
```

$$I := \langle y\,x-x^3, z-x^3\rangle$$

We check whether it is radical or prime.

```
> IsRadical(I), IsPrime(I);
```

$$true, false$$

We compute a GB for I.

```
> G := Groebner[Basis]( I, plex(z,y,x) );
  factor(G);
```

$$G := [y\,x-x^3, z-x^3]$$

$$[-x\,(x^2-y), z-x^3]$$

4/5

Under the chosen variable ordering, the GB is simply the given generators for I. The first polynomial factors, so we compute its factors.

```
> f1,f2 := x,y-x^2;
```

$$f1, f2 := x, y-x^2$$

We compute the quotients $J = I : \langle f_1\rangle$ and $K = I : \langle f_2\rangle$.

```
> J := Quotient( I, <f1> );
  K := Quotient( I, <f2> );
```

$$J := \langle -z+y\,x, x^2-y, -x\,z+y^2\rangle$$

$$K := \langle -z, -x\rangle$$

We check if J and K are prime.

```
> IsPrime(J), IsPrime(K);
  G1 := Groebner[Basis]( J, plex(z,y,x) );
  G2 := Groebner[Basis]( K, plex(z,y,x) );
```

$$true, true$$

$$G1 := [y - x^2, z - x^3]$$
$$G2 := [x, z]$$

They are. We can also see that J is prime because it is the ideal of the twisted cubic in C^3 - a variety that is irreducible because it has a polynomial parametrization $[x, y, z] = [t, t^2, t^3]$, and K is prime because it is maximal. X No, $\langle x, z \rangle$ is NOT maximal in $k[x,y,z]$.

We also check that $J = I : K$ and $K = I : J$.

-1

```
> Quotient( I, K );
  Quotient( I, J );
```

$$\langle y - x^2, z - y\,x, x\,z - y^2 \rangle$$
$$\langle x, z \rangle$$

Therefore the prime decomposition is $I = J \cap K = \langle y - x^2, z - x^3 \rangle \cap \langle x, z \rangle$.
Since $J = \mathrm{I}(U)$ and $K = \mathrm{I}(V)$ where U is the twisted cubic and V is the y-axis, we have $W = V(I) = U \cup V$ as the irreducible decomposition of W.

Additional Exercise 7

We enter the ideal I that we will decompose.

```
> I := <x^2-y, y^4-y*z^2, x*y^3-x*z^2>;
```

$$I := \langle x^2 - y, y^4 - y\,z^2, x\,y^3 - x\,z^2 \rangle$$

We check whether it is radical or prime.

```
> IsRadical(I), IsPrime(I);
```

true, *false*

We compute a GB for I.

```
> G := Groebner[Basis]( I, plex(z,y,x) );
  factor(G);
```

$$G := [y - x^2, x\,z^2 - x^7]$$
$$[y - x^2, -x\,(-z + x^3)\,(z + x^3)]$$

5

The second polynomial in the GB, g_2, factors into 3 irreducible factors.

```
> f1,f2,f3 := x,z-x^3,z+x^3;
```

$$f1, f2, f3 := x, z - x^3, z + x^3$$

We compute the ideal quotients of I by $\langle \frac{g_2}{f_1} \rangle$, $\langle \frac{g_2}{f_2} \rangle$ and $\langle \frac{g_2}{f_3} \rangle$.

```
> P1 := Quotient( I, <quo( G[2], f1, x )> );
  P2 := Quotient( I, <quo( G[2], f2, x )> );
  P3 := Quotient( I, <quo( G[2], f3, x )> );
```

$$P1 := \langle -y, -x \rangle$$
$$P2 := \langle x^2 - y, y^3 - z^2, x\,y - z, x\,z - y^2 \rangle$$
$$P3 := \langle y - x^2, -x\,z - y^2, -y^3 + z^2, -x\,y - z \rangle$$

We compute lexicographic GBs for these ideal quotients P_1, P_2 and P_3.

```
> G1 := Groebner[Basis]( P1, plex(z,y,x) );
  G2 := Groebner[Basis]( P2, plex(z,y,x) );
  G3 := Groebner[Basis]( P3, plex(z,y,x) );
```

$$G1 := [x, y]$$

$$G2 := [y - x^2, z - x^3]$$

$$G3 := [y - x^2, z + x^3]$$

We can see that all 3 are prime ideals. P_1 is prime because it is maximal. P_2 is prime because it is the ideal of the twisted cubic, and P_3 is prime because it is the ideal of the "negative" twisted cubic. We can also verify these with Maple.

```
> IsPrime(P1), IsPrime(P2), IsPrime(P3);
```

true, true, true

We check that I is the intersection of P_1, P_2 and P_3.

```
> Intersect( P1, P2, P3 );
  I;
```

$$\langle x^2 - y, y^4 - y z^2, x y^3 - x z^2 \rangle$$

$$\langle x^2 - y, y^4 - y z^2, x y^3 - x z^2 \rangle$$

generating

It remains to show that this is a minimal (irredundant) decomposition. That is, we need to show that no P_i is contained in another P_j. We will do this by choosing polynomials $g_i \in P_i$ and showing that each g_i is not in the other P_j (by showing that g_i does not reduce to 0 modulo P_j).

```
> Groebner[Reduce]( G1[2], G2, plex(z,y,x) );
  Groebner[Reduce]( G1[2], G3, plex(z,y,x) );
  Groebner[Reduce]( G2[2], G1, plex(z,y,x) );
  Groebner[Reduce]( G2[2], G3, plex(z,y,x) );
  Groebner[Reduce]( G3[2], G1, plex(z,y,x) );
  Groebner[Reduce]( G3[2], G2, plex(z,y,x) );
```

Use NormalForm.

$$x^2$$

$$x^2$$

$$z$$

$$-x^3$$

$$z$$

$$x^3$$

Note, that is sufficient but Not necessary.
E.g.
$\langle x, y \rangle = P_1$
$\langle x, z \rangle = P_2$
are both prime
and $P_1 \not\subseteq P_2$
and $P_2 \not\subseteq P_1$
but $x \in P_1$ and P_2.

Therefore We have a minimal decomposition for I.

Bonus Exercise

We enter the ideal I.

```
> I := <(z^2-2)*(z^2-3),
  y^5+y^3*z+y^3-3*y^4*z-3*y^2*z^2-3*y^2*z+3*y^3*z^2+3*y*z^3+3*y*z
  ^2-z^3*y^2-z^3+6-5*z^2>;
```

$I := \langle y^5 + y^3 z + y^3 - 3y^4 z - 3y^2 z^2 - 3y^2 z + 3y^3 z^2 + 3yz^3 + 3yz^2 - z^3 y^2 - z^3 + 6 - 5z^2,$
$(z^2-2)(z^2-3)\rangle$

To compute $\sqrt{I}$, we first compute a GB for I (w.r.t. lexicographic order) and try to factor this GB.

```
> G := Groebner[Basis]( I, plex(y,z) );
  factor(G);
```

$$G := [z^4 - 5z^2 + 6,$$
$$y^5 + y^3 z + y^3 - 3y^4 z - 3y^2 z^2 - 3y^2 z + 3y^3 z^2 + 3yz^3 + 3yz^2 - z^3 y^2 - z^3 + 6 - 5z^2]$$
$$[(z^2-2)(z^2-3),$$
$$y^5 + y^3 z + y^3 - 3y^4 z - 3y^2 z^2 - 3y^2 z + 3y^3 z^2 + 3yz^3 + 3yz^2 - z^3 y^2 - z^3 + 6 - 5z^2]$$

It turns out that the original generating set is a (factored) GB for I. Since it does not factor further over Q, we must introduce an algebraic extension. The first polynomial in the GB gives two choices of irreducible polynomial from which to construct the extension. We choose the first, $z^2 - 2$.

```
> alias( alpha=RootOf( z^2-2 ) );
```

$$\alpha$$

Now we try to factor the second polynomial in the GB over $Q(\alpha)$.

```
> g := subs( z=alpha, G[2] );
  factor(g);
```

$$g :=$$
$$y^5 + y^3\alpha + y^3 - 3y^4\alpha - 3y^2\alpha^2 - 3y^2\alpha + 3y^3\alpha^2 + 3y\alpha^3 + 3y\alpha^2 - \alpha^3 y^2 - \alpha^3 + 6 - 5\alpha^2$$
$$(y^2 + 1 + \alpha)(y - \alpha)^3$$

We compute the square-free part of this polynomial g, $g_{red} = \dfrac{g}{\mathrm{GCD}\left(g, \dfrac{\partial}{\partial y} g\right)}$.

6/7

```
> g_red := simplify( g/gcd( g, diff(g,y) ) );
  factor(g_red);
```

$$g\_red := y^3 - y^2\alpha + y + y\alpha - 2 - \alpha$$
$$(y^2 + 1 + \alpha)(y - \alpha)$$

g_{red} is exactly what we expect it to be, given the factorization of g.

Now replacing α with z we should have $\sqrt{I} = \langle (z^2-2)(z^2-3), g_{red}\rangle$. We verify this with Maple.

```
> J := <G[1], subs( alpha=z, g_red )>;
  IsRadical(J);
  Groebner[Basis]( Radical(I), plex(y,z) );
```

$$J := \langle z^4 - 5z^2 + 6, y^3 - y^2 z + y + zy - 2 - z\rangle$$
$$true$$
$$G = [z^4 - 5z^2 + 6, y^3 - y^2 z + zy + y - z^2 - z]$$

Notice that if we had taken the correct combination of the polynomials in the GB for I we would

-1 You need to check G_2 is square-free mod z^2-3 too (unless you have an oracle (Maple) to tell you $\langle G \rangle$ is already radical) have seen that g (with z instead of α) is in I. Then we would have deduced that g_{red} is in $\sqrt{I}$ without having to use field extensions.

```
> factor( G[2]-G[1] );
```

$$(y^2 + 1 + z)\,(y - z)^3$$

Scott Cowan
200034814
scottc@sfu.ca

```
>
```