Computer Algebra 522

Homework 1

Nutan Nepal

September 22, 2023

1.3.8 Consider the curve defined by $y^2 = cx^2 - x^3$, where c is some constant.

a. Show that a line will meet this curve at either 0,1,2, or 3 points. Illustrate your answer with a picture. Let the equation of the line be either $x = a$ or $y = mx + b$.

b. Show that a non-vertical line through the origin meets the curve at exactly one other point when $m^2 \neq c$. Draw a picture to illustrate this, and see if you can come up with an intuitive explanation as to why this happens.

c. Now draw the vertical line $x = 1$. Given a point $(1, t)$ on this line, draw the line connecting $(1, t)$ to the origin. This will intersect the curve in a point (x, y). Draw a picture to illustrate this, and argue geometrically that this gives a parameterization of the entire curve.

d. Show that the geometric description from part (c) leads to the parameterization

$$x = c - t^2,$$
$$y = t(c - t^2).$$

1.4.8 The ideal $\mathbf{I}(V)$ of a variety has a special property not shared by all ideals. Specifically, we define an ideal I to be *radical* if whenever a power f^m of a polynomial f is in I, then f itself is in I. More succinctly, I is radical when $f \in I$ if and only if $f^m \in I$ for any positive integer m.

a. Prove that $\mathbf{I}(V)$ is always a radical ideal.

If $f \in \mathbf{I}(V)$, then $f^m \in \mathbf{I}(V)$ for all positive integers m since $\mathbf{I}(V)$ is an ideal. If $f^m \in \mathbf{I}(V)$ then $f^m(x) = 0$ for all $x \in V$. So since $k[x]$ is an integral domain, we have $f(x) = 0$ which implies $f \in \mathbf{I}(V)$. Thus, $\mathbf{I}(V)$ is radical.

b. Prove that $\langle x^2, y^2 \rangle$ is not a radical ideal. This implies that $\langle x^2, y^2 \rangle \neq \mathbf{I}(V)$ for any variety $V \subseteq k^2$.

$x^2 \in \langle x^2, y^2 \rangle$ but $x \notin \langle x^2, y^2 \rangle$. So, by (a) $\langle x^2, y^2 \rangle$ is not radical.

1.4.15 In the text, we defined $\mathbf{I}(V)$ for a variety $V \subseteq k^n$. We can generalize this as follows: if $S \subseteq k^n$ is any subset, then we set

$$\mathbf{I}(S) := \{f \in k[x_1, \dots, x_n] | f(a) = 0 \ \forall a \in S\}.$$

a. Prove that $\mathbf{I}(S)$ is an ideal.

> If $f, g \in \mathbf{I}(S) \subset k[x_1, \dots, x_n]$, $(f - g)(a) = 0$ and $(fg)(a) = f(a)g(a) = 0$ for all $a \in S$. So $I(S)$ is a subring of $k[x_1, \dots, x_n]$. Furthermore, for any $h \in k[x_1, \dots, x_n]$ and $f \in \mathbf{I}(S)$, we have $(fh)(a) = f(a)h(a) = 0$ for all $a \in S$. So $fh \in \mathbf{I}(S)$ and $\mathbf{I}(S)$ is an ideal.

b. Let $X = \{(a, a) \in \mathbb{R}^2 | a \neq 1\}$. Determine $\mathbf{I}(X)$.

> If $f \in I(X)$, then $f(a, a) = 0$ for all $a \in \mathbb{R}$ by exercise 1.2.8. Then, f vanishes precisely on the line $y = x$ in $\mathbb{R}^2$. So, $f \in \langle y - x \rangle$. We also have that $\langle y - x \rangle \subset I(X)$ since $y - x$ vanishes at all points of X. Thus $I(X) = \langle y - x \rangle$.

c. Let $\mathbb{Z}^n$ be the points of $\mathbb{C}^n$ with integer coordinates. Determine $\mathbf{I}(\mathbb{Z}^n)$. [Hint: Exercise 1.1.6].

> By 1.1.6, we must have that if f vanishes at every point in $\mathbb{Z}^n$ then $f = 0$. Thus, $I(\mathbb{Z}^n) = 0$.

1.5.3 The fact that every ideal of $k[x]$ is principal is special to the case of polynomials in one variable. In this exercise we will see why. Namely, consider the ideal $I = \langle x, y \rangle \subseteq k[x, y]$. Prove that I is not a principal ideal.

> If I is a principal ideal then it is generated by some element $f \in k[x, y]$. Since $x \in I$, we have $x = fg$ for some $g \in k[x, y]$ and degree(f)+ degree(g) = degree(x). So either f or g must be a constant. f cannot be a constant since $I = \langle f \rangle$ would then be all of $k[x, y]$. If g is a constant, f would be a polynomial entirely on x and so $y = fh$ for $y \in I$ would have no solution. Thus I is not a principal ideal.

1.5.11 In this exercise we will study the one-variable case of the *consistency problem* from section 1.2. Given $f_1, \dots, f_s \in k[x]$, this asks if there is an algorithm to decide whether $\mathbf{V}(f_1, \dots, f_s)$ is nonempty. we will see that the answer is yes when $k = \mathbb{C}$.

a. Let $f \in \mathbb{C}[x]$ be a nonzero polynomial. Then use Theorem 7 of section 1.1 to show that $\mathbf{V}(f) = \emptyset$ if and only if f is constant.

> By theorem 7, every non-constant polynomial in $\mathbb{C}[x]$ has a root. Thus for the forward direction, we see that if f is not constant then it has a root, say, a. Hence $a \in V(f) \neq \emptyset$. Now, if $f \neq 0$ is a constant polynomial $f = c$, then $c = 0$ is always false. So

$V(f) = \emptyset$.

b. If $f_1, \ldots, f_s \in \mathbb{C}[x]$ Prove $\mathbf{V}(f_1, \ldots, f_s) = \emptyset$ if and only if $\gcd(f_1, \ldots, f_s) = 1$.

Since $\mathbb{C}[x]$ is a principal ideal domain, we have $\langle f_1, \ldots, f_s \rangle = \langle f \rangle$ for some f. By proposition 4 in 1.4, we have $V(f_1, \ldots, f_s) = V(f)$. Thus using (a) on $V(f)$ we have, $V(f) = \emptyset$ iff f is a constant polynomial. If $gcd = f = 1$, then $V(f_1, \ldots, f_s)$ is clearly empty. If $V(f_1, \ldots, f_s)$ is empty, then f is a constant polynomial k and we have

$$\alpha_1 f_1 + \cdots + \alpha_s f_s = k$$

for some polynomials α_i. Dividing by k, we see that $\sum_{i=1}^{s} \beta_i f_i = 1$ which implies that the gcd of the polynomials is 1.

c. Describe in words an algorithm for determining whether or not $\mathbf{V}(f_1, \ldots, f_s)$ is nonempty.

We calculate the gcd of the $f_1, \ldots, f_s$. If the gcd is not constant, then the set $V(f_1, \ldots, f_s)$ is not empty.

1.5.12 This exercise will study the one-variable case of the *Nullstellensatz* problem from section 1.4 which asks for the relation between $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ and $\langle f_1, \ldots, f_s \rangle$ when $f_1, \ldots, f_s \in \mathbb{C}[x]$. By using gcd's, we can reduce to the case of a single generator. So, in this problem, we will explicitly determine $\mathbf{I}(\mathbf{V}(f))$ when $f \in \mathbb{C}[x]$ is a nonconstant polynomial. Since we are working over the complex numbers, we know by Exercise 1.5.1 that f factors completely, i.e.,

$$f = c(x - a_1)^{r_1} \cdots (x - a_l)^{r_l},$$

where $a_1, \ldots, a_l \in \mathbb{C}$ are distinct and $c \in \mathbb{C} \backslash \{0\}$. Define the polynomial

$$f_{\text{red}} = c(x - a_1) \cdots (x - a_l).$$

The polynomials f and f_{red} have the same roots, but their multiplicities may differ. In particular, all roots of f_{red} have multiplicity one. We call f_{red} the *reduced* or *square-free* part of f. The latter name recognizes that f_{red} is the square-free factor of f of largest degree.

a. Show that $\mathbf{V}(f) = \{a_1, \ldots, a_l\}$.

Clearly for each $a_i \in \{a_1, \ldots, a_l\}$, we have $f(a_i) = 0$ and so $\{a_i\}_1^n \subset V(f)$. Since $\mathbb{C}[x]$ is an integral domain, we have $f = 0 \implies (x - a_i) = 0$ for some a_i and so $V(f) \subset \{a_i\}_1^n$.

b. Show that $\mathbf{I}(\mathbf{V}(f)) = \langle f_{red} \rangle$.

If $g \in I(V(f))$, then $g(a_i) = 0$ for all i. So, all $(x - a_i)$ divides g and hence, f_{red} also divides $g \implies g \in \langle f_{red} \rangle$. So $I(V(f)) \subset \langle f_{red} \rangle$. Similarly, if $h \in \langle f_{red} \rangle$, $f_{red} \mid h \implies h = k \cdot f_{red}$ for some polynomial k. So $h(a_i) = 0$ for all i and hence $\langle f_{red} \rangle \subset I(V(f))$.

2.2.11 Let $>$ be a monomial order on $k[x_1, \ldots, x_n]$.

a. Let $f \in k[x_1, \ldots, x_n]$ and let m be a monomial. Show that $\mathrm{LT}(m \cdot f) = m \cdot \mathrm{LT}(f)$.

Since $\mathrm{LM}(m \cdot f) = m \cdot \mathrm{LM}(f)$, we have $\mathrm{LT}(m \cdot f) = \mathrm{LC}(m \cdot f) \cdot \mathrm{LM}(m \cdot f) = \mathrm{LC}(f) \cdot m \cdot \mathrm{LM}(f) = m \cdot \mathrm{LT}(f)$.

b. Let $f, g \in k[x_1, \ldots, x_n]$. Is $\mathrm{LT}(f \cdot g)$ necessarily the same as $\mathrm{LT}(f) \cdot \mathrm{LT}(g)$?

For each term $c_i m_i$ of g, we have $\mathrm{LT}(c_i m_i \cdot f) = c_i m_i \cdot \mathrm{LT}(f)$. If $c_i m_i$ is the leading term of g then $c_i m_i \cdot \mathrm{LT}(f)$ appears exactly once in the sum $\sum_i c_i m_i \cdot f$ and so does not cancel out or add up with any other terms. Furthermore, $\mathrm{LT}(g) \cdot \mathrm{LT}(f)$ has the maximal multidegree. Thus, $\mathrm{LT}(fg) = \mathrm{LT}(f)\mathrm{LT}(g)$.

c. If $f_i, g_i \in k[x_1, \ldots, x_n]$, $1 \le i \le s$, is $\mathrm{LM}(\sum_{i=1}^s f_i g_i)$ necessarily equal to $\mathrm{LM}(f_i) \cdot \mathrm{LM}(g_i)$ for some i?

No. For $f_1 = f_2 = x_1$, $g_1 = x_1$ and $g_2 = -x_1$, we have $f_1 g_1 + f_2 g_2 = 0$. But none of $f_i g_i$ have the leading terms equal to 0.

2.3.11 In this exercise, we will characterize completely the expression

$$f = q_1 f_1 + \cdots + q_s f_s + r$$

that is produced by the division algorithm (among all the possible expressions for f of this form). Let $\mathrm{LM}(f_i) = x^{\alpha(i)}$ and define

$$\begin{aligned}
\Delta_1 &= \alpha(1) + \mathbb{Z}^n_{\ge 0}, \\
\Delta_2 &= (\alpha(2) + \mathbb{Z}^n_{\ge 0}) \backslash \Delta_1, \\
&\vdots \\
\Delta_s &= (\alpha(s) + \mathbb{Z}^n_{\ge 0}) \backslash \left(\bigcup_{i=1}^{s-1} \Delta_i \right), \\
\overline{\Delta} &= \mathbb{Z}^n_{\ge 0} \backslash \left(\bigcup_{i=1}^{s} \Delta_i \right)
\end{aligned}$$

a. Show that $\beta \in \Delta_i$ iff $x^{\alpha(i)}$ divides x^β and no $x^{\alpha(j)}$ with $j < i$ divides x^β.

If $\beta \in \Delta_i$, then $\beta = \alpha(i) + \delta$ for some $\delta \in \mathbb{Z}^n_{\geq 0}$ and $\beta \neq \alpha(j) + \delta'$ for $j < 1$ and some $\delta' \in \mathbb{Z}^n_{\geq 0}$. So, $x^{\alpha(i)}$ divides x^β and no $x^{\alpha(j)}$ with $j < i$ divides x^β.

Similarly, if $x^{\alpha(i)}$ divides x^β and no $x^{\alpha(j)}$ with $j < i$ divides x^β, then $\beta = \alpha(i) + \delta$ for some $\delta \in \mathbb{Z}^n_{\geq 0}$ and $\beta \neq \alpha(j) + \delta'$ for $j < 1$ and some $\delta' \in \mathbb{Z}^n_{\geq 0}$. In other words,

$$\beta \in (\alpha(i) + \mathbb{Z}^n_{\geq 0}) \backslash \left(\bigcup_{j=1}^{i-1} \Delta_j \right) = \Delta_i.$$

b. Show that $\gamma \in \overline{\Delta}$ iff no $x^{\alpha(i)}$ divides x^γ.

$\gamma \in \overline{\Delta}$ iff $\gamma \notin \Delta_i$ for all $i \leq s$. Thus by (a), $\gamma \in \overline{\Delta}$ iff no $x^{\alpha(i)}$ divides x^γ.

c. Show that in the expression $f = q_1 f_1 + \cdots + q_s f_s + r$ computed by the division algorithm, for every i, every monomial x^β in q_i satisfies $\beta + \alpha(i) \in \Delta_i$, and every monomial x^γ in r satisfies $\gamma \in \overline{\Delta}$.

d. Show that there is exactly one expression $f = q_1 f_1 + \cdots + q_s f_s + r$ satisfying the properties given in part (c).

Programming Exercise 1

```
R.<x> = PolynomialRing(CC)
def gcduni(g,f):
    f1=g; f2=f
    q, r = g.quo_rem(f)
    if (q==0):
        f1 = f; f2 = g
    h=f1; s=f2

    while s!= 0:
        q, r = h.quo_rem(s)
        h = s
        s = r
return h
```

Programming Exercise 2

```
S.<x,y> = PolynomialRing(CC,2,'xy',order='degrevlex')
def multidiv(f, listf):
    listofqs = []
    p=f
    for fs in listf:
        q, r = p.quo_rem(fs)
        listofqs.append(q)
        p=r
return (listofqs, p)
```