Using Algebraic Geometry

With 1 Figures

Anakin Dey

Last Edited on 12/16/24 at 14:26

Contents

Preface

At the time of writing this, I am starting my PhD at The Ohio State University. Currently a large part of my interests in algebra are about algorithms as they relate to polynomials and algebraic geometry. I've been doing a bunch of problems from *Ideals, Varieties, and Algorithms* [CLO15]. However, it seems that *Using Algebraic Geometry* [CLO05] moves through the material faster as it assumes you know more algebra. So I've moved onto working through this book as well as trying to comprehend Sturmfel's *Algorithms in Invariant Theory* [Str08].

Chapter 1

Introduction

1.1 Polynomials and Ideals

Solution: [CLO05] Ex. 1.1.1:

(a) We have that $x(x-y^2)+y(xy)=x^2-xy^2+xy^2=x^2$.

(b) It suffices to check for generators. We have that $x+(-1)(y^2)=x-y^2$, $y(x)=xy$, and $y^2=y^2$ showing that $\left\langle x-y^2, xy, y^2 \right\rangle \subseteq \left\langle x, y^2 \right\rangle$. Then $x-y^2+y^2=x$ and $y^2=y^2$ shows the reverse containment and overall the ideals are equal.

(c) We already know from 1. that x^2 lives in $\left\langle x-y^2, xy \right\rangle$. Since $xy=xy$, we overall have that $\left\langle x^2, xy \right\rangle \subseteq \left\langle x-y^2, xy \right\rangle$. It remains to check if $x-y^2 \in \left\langle x^2, xy \right\rangle$. However, notice that every element of $\left\langle x^2, xy \right\rangle$ is divisible by x while $x-y^2$ is clearly not divisible by x. Thus $x-y^2 \notin \left\langle x^2, xy \right\rangle$ and the two ideals are not equal.

□

Solution: [CLO05] Ex. 1.1.2: Let $f, g \in \langle f_1, \ldots, f_s \rangle$. Then $\exists p_1, \ldots, p_s, q_1, \ldots, q_s$ such that $f=\sum_{i=1}^{s} p_i \cdot f_i$ and $g=\sum_{i=1}^{s} q_i \cdot f_i$. Thus $f+g=\sum_{i=1}^{s}(p_i+q_i)\cdot f_i$ which shows that $f+g \in \langle f_1, \ldots, f_s \rangle$. Then let $p \in k[x_1, \ldots, x_n]$. We have that $p \cdot f = p\sum_{i=1}^{s} p_i f_i = \sum_{i=1}^{s}(p \cdot p_i) \cdot f_i$ which shows that $\langle f_1, \ldots, f_s \rangle$ is an ideal. □

Solution: [CLO05] Ex. 1.1.3: We already know that $\langle f_1, \ldots, f_s \rangle$ is an ideal by [CLO05] Ex. 1.1.2. Now suppose that J is an ideal containing $\{f_1, \ldots, f_s\}$. Then, since ideals are closed under addition and scaling, we have that for all $p_1, \ldots, p_s \in k[x_1, \ldots, x_n]$ that $\sum_{i=1}^{s} p_i \cdot f_i \in J$. Thus, $\langle f_1, \ldots, f_s \rangle \subseteq J$. □

Solution: [CLO05] Ex. 1.1.4: We claim that $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$ if and only if $\{g_1, \ldots, g_t\} \subseteq I$ and $\{f_1, \ldots, f_s\} \subseteq J$. The forward implication is immediate. Then by [CLO05] Ex. 1.1.3, if $\{g_1, \ldots, g_t\} \subseteq I$ then $J \subseteq I$. Similarly, $\{f_1, \ldots, f_s\} \subseteq J \implies I \subseteq J$ and overall $I = J$. This fact was used in [CLO05] Ex. 1.1.1 (b). □

Solution: [CLO05] Ex. 1.1.5: It suffices to show that $z-x^3 \in \left\langle y-x^2, z-xy \right\rangle$ and and $z-xy \in \left\langle x-y^2, z-x^3 \right\rangle$. Indeed we have that $(z-xy)+x(y-x^2) = z-x^3$ which also yields that $z-xy = z-x^3 - x(y-x^2)$. $\square$

Solution: [CLO05] Ex. 1.1.6: If $I = \{0\}$ then $I = \langle 0 \rangle$. So suppose $I \neq 0$. Let $d \in I$ be of minimal degree. **⟨⟨ $d = \gcd(I)$ but I need infinite Bezout. ⟩⟩** Then we claim that $\langle d \rangle = I$. Since $d \in I$, we have that $\langle d \rangle \subseteq I$. Now let $f \in I$. By Euclidean division, there exists $q, r \in k[x]$ such that $f = qd + r$ where either $r = 0$ or $0 \leq \deg(r) \leq \deg(d) - 1$. If $r = 0$ then $f \in \langle d \rangle$ and we are done. So suppose $r \neq 0$. Then $f, qd \in I \implies r = f - qd \in I$. Thus, $r \in I$ is of degree strictly less than d, contradicting the minimality of the degree of d. So we must have that $r = 0$ and overall $\langle d \rangle = I$. $\square$

Solution: [CLO05] Ex. 1.1.7:

(a) Suppose $f(x) \in \langle x \rangle$. Then $f(x)^m \in \langle x^n \rangle$ so $f(x) \in \sqrt{\langle x^n \rangle}$ Now suppose that $f(x) \in \sqrt{\langle x^n \rangle}$. Then $\exists k$ such that $f(x)^k \in \langle x^n \rangle$. Thus $f(x)^k$ is a multiple of x^n. This implies that $f(x)^k$ is a multiple of x. Then notice that the unique factorization of $f(x)^k$ into irreducibles is the kth power of the factorization of $f(x)$ into irreducibles. Thus x must be a factor of $f(x)$ and so $f(x) \in \langle x \rangle$. Note, this heavily uses the fact that $k[x]$ is a unique factorization domain for all fields k.

(b) We claim that $\sqrt{\langle p(x) \rangle} = \langle (x-a_1)\cdots(x-a_m) \rangle = I$. Suppose $f(x) \in I$. Let $k = \max e_1, \ldots, e_n$. Then $p(x) \mid f(x)^k$ so $f(x) \in \sqrt{\langle p(x) \rangle}$. Now suppose that $f(x) \in \sqrt{\langle p(x) \rangle}$. Then $\exists k$ such that $f(x)^k \in \langle p(x) \rangle$. Thus $f(x)^k$ is a multiple of each $(x-a_i)$. Then notice that the unique factorization of $f(x)^k$ into irreducibles is the kth power of the factorization of $f(x)$ into irreducibles. Thus $f(x)$ is a multiple of each $(x-a_i)$ and so $f(x) \in I$.

(c) Radical ideals are the ideals I such that $\sqrt{I} = I$. Notice that $\mathbb{C}[x]$ is a principal ideal domain and so any such I must be generated by a single polynomial. Since every polynomial in $\mathbb{C}[x]$ splits into linear factors, (b) immediately implies that the only radical ideals of $\mathbb{C}[x]$ are the ones which are of the form $\langle (x-a_1)\cdots(x-a_m) \rangle$ for $a_1, \ldots, a_m \in \mathbb{C}[x]$.

$\square$

Solution: [CLO05] Ex. 1.1.8:

(a) Let $\mathfrak{p}$ be a prime ideal in $k[\overline{x}]$. Clearly $\mathfrak{p} \subseteq \sqrt{\mathfrak{p}}$ always. Let $f(\overline{x}) \in \sqrt{\mathfrak{p}}$. Then $f(\overline{x})^m \in \mathfrak{p}$ for some $m \in \mathbb{Z}_{\geq 1}$. We prove the reverse inclusion by induction on m. If $m = 1$ then $f(\overline{x}) = f(\overline{x})^1 \in \mathfrak{p}$. Now let $m > 1$ and suppose the claim holds for all $k \leq m$. Then suppose $f(\overline{x})^{m+1} \in \mathfrak{p}$. Then $f(\overline{x}) \cdot f(\overline{x})^m \in \mathfrak{p}/$ Either $f(\overline{x}) \in \mathfrak{p}$ or $f(\overline{x})^m \in \mathfrak{p}$ which by induction implies that $f(\overline{x}) \in \mathfrak{p}$. Thus, $f(\overline{x})^m \in \mathfrak{p} \implies f(\overline{x}) \in \mathfrak{p}$ for all $m \in \mathbb{Z}_{\geq 1}$ and so $\sqrt{\mathfrak{p}} \subseteq \mathfrak{p}$. Thus, all prime ideals are radical.

(b) Notice that for all fields k that $k[x]$ is a principal ideal domain. Thus, all the prime ideals are the ones generated by a single irreducible polynomial. Also, in $k[x]$ we have that (0) is a prime ideal as well as $k[x]$ is an integral domain. In $\mathbb{C}[x]$, these are the ideals generated by $x - z$ for some $z \in \mathbb{C}$. In $\mathbb{R}[x]$, the primes are the ideals generated by $x - r$ for some $r \in \mathbb{R}$ or $x^2 + r$ for some positive $r \in R$. **⟨⟨ What would be a general condition for $\mathbb{Q}[x]$? ⟩⟩**

□

Solution: [CLO05] Ex. 1.1.9:

(a) First, observe that $\langle x_1, \ldots, x_n \rangle$ is the ideal consisting exactly of polynomials which have no constant term. Let I be an ideal in $k[x_1, \ldots, x_n]$ such that $\langle x_1, \ldots, x_n \rangle \subsetneq I$. Thus there exists $f(x_1, \ldots, x_n) \in I \setminus \langle x_1, \ldots, x_n \rangle$. We have by our observation that f has a nonzero constant term z. Then note that the non-constant terms of f form a polynomial $g(x_1, \ldots, x_n)$ in $\langle x_1, \ldots, x_n \rangle$. Thus, we have that $z = f(x) - g(x) \in I$. Since I contains a nonzero constant term, we must have that $I = k[x_1, \ldots, x_n]$.

(b) Recall that an ideal I is maximal if and only if R/I is a field. Let $I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Consider the evaluation map $\mathrm{ev}_{\overline{a}} \colon k[x_1, \ldots, x_n] \to k$ sending $f(x_1, \ldots, x_n) \mapsto f(a_1, \ldots, a_n)$. Clearly this map is surjective. Then since for all i we have that $x_i \equiv a_i \pmod{I}$, we have that $f(x_1, \ldots, x_n) \equiv f(a_1, \ldots, a_n) \pmod{I}$ for all $f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$. Thus, $\mathrm{ev}_{\overline{a}}(f) = f(a_1, \ldots, a_n) = 0$ if and only if $f(x_1, \ldots, x_n) \in I$. Thus, $\ker(\mathrm{ev}_{\overline{a}}) = I$ and $k[x_1, \ldots, x_n]/I$ is a field, meaning $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is maximal.

(c) Since $\mathbb{R}[x]$ is a principal ideal domain, any ideal I strictly containing $\left\langle x^2 + 1 \right\rangle$ is of the form $\langle g(x) \rangle$ for some $g(x) \mid x^2 + 1$. However, since $x^2 + 1$ is irreducible in $\mathbb{R}[x]$, we have that $g(x)$ is either $z(x^2 + 1)$ for some nonzero $z \in \mathbb{C}$ or $g(x) = z$ for some nonzero $z \in \mathbb{C}$, meaning $\langle g(x) \rangle = \left\langle x^2 + 1 \right\rangle$ or or $\langle g(x) \rangle = \mathbb{R}[x]$. Thus, $\left\langle x^2 + 1 \right\rangle$ is maximal. However, in $\mathbb{C}[x]$, we have that $x^2 + 1 = (x + i)(x - i)$ and so $\left\langle x^2 + 1 \right\rangle \subsetneq \langle x - i \rangle \subsetneq \mathbb{C}[x]$.

□

Solution: [CLO05] Ex. 1.1.10:

(a) Since $x^2 + y^2 - (x^2 - z^3) = y^2 + z^3$ is an element of I which does not depend on x, $y^2 + z^3$ is in I_1.

(b) For all $\ell \geq 1$, we have that $0 \in I_\ell$. Then, if $f(x_{\ell+1}, \ldots, x_n), g(x_{\ell+1}, \ldots, x_n)$ are two polynomials in I who do not depend on the first ℓ variables, then so is $f + g$. Finally, let $r(x_\ell + 1, \ldots, x_n) \in k[x_{\ell+1}, \ldots, x_n]$. Then $r \cdot f \in I_\ell$ since $r \cdot f \in I$ and still does not depend on any of the first ℓ variables.

$\square$

Solution: [CLO05] Ex. 1.1.11:

(a) **⟨⟨ meh ⟩⟩**

(b) **⟨⟨ meh ⟩⟩**

(c) We claim that $I + J = \langle f_1, \ldots, f_s, g_1, \ldots, g_t \rangle$. Clearly $I, J \subseteq \langle f_1, \ldots, f_s, g_1, \ldots, g_t \rangle$ and thus so is $I \cup J$. By (b), this shows that $I + J \subseteq \langle f_1, \ldots, f_s, g_1, \ldots, g_t \rangle$. Then, since $f_i = f_i + 0$ and $g_j = 0 + g_j$ for all i, j, we have the reverse inclusion and thus the two ideals are equal.

$\square$

Solution: [CLO05] Ex. 1.1.12:

(a) **⟨⟨ meh ⟩⟩**

(b) Suppose that $h(\overline{x}) \in IJ$. Note that IJ is generated by the products $f(\overline{x}) \cdot g(\overline{x})$ for $f(\overline{x}) \in I$, and $g(\overline{x}) \in J$. Then $h(\overline{x})$ consists of sums of terms of the form $r(\overline{x}) \cdot f(\overline{x}) \cdot g(\overline{x})$ for $r(\overline{x}) \in k[\overline{x}]$, $f(\overline{x}) \in I$, and $g(\overline{x}) \in J$. Thus, each term is in both I and J and overall so is $h(\overline{x})$.

To see an example where $IJ \subsetneq I \cap J$, consider $I = \left\langle x^2 y \right\rangle$ and $J = \left\langle x y^2 \right\rangle$ in $k[x, y]$. Then $I \cap J = \left\langle x^2 y^2 \right\rangle$ and $IJ = \left\langle x^3 y^3 \right\rangle$. Thus $IJ \subsetneq I \cap J$ as $I \cap J$ contains $x^2 y^2$ and IJ does not contain $x^2 y^2$.

$\square$

1.2 Gröbner Bases

Solution: ⟨⟨ [CLO05] Ex. 1.3.11 ⟩⟩ :

□

1.3 Affine Varieties

Solution: **⟨⟨ [CLO05] Ex. 1.4.9 ⟩⟩** :

$\square$

Chapter 2

Solving Polynomial Equations

2.1 Solving Polynomial Systems by Elimination

Solution: ⟨⟨ **[CLO05] Ex. 2.1.1** ⟩⟩ :

□

Solution: ⟨⟨ **[CLO05] Ex. 2.1.2** ⟩⟩ :

□

Solution: [CLO05] Ex. 2.1.3: We may freely rewrite the polynomial as $p(z) = z^n - a_{n-1}z^{n-1} - \cdots - a_0$ We have that $0 = \overline{z}^n - a_{n-1}\overline{z}^{n-1} - \cdots - a_0$ and so $\overline{z}^n = a_{n-1}\overline{z}^{n-1} + \cdots + a_0$. Suppose now that $|\overline{z}| \geq 1$. Then

$$|\overline{z}|^n = \left|a_{n-1}\overline{z}^{n-1} + \cdots + a_0\right| \leq |a_{n-1}||z|^{n-1} + \cdots + a_0 \leq |a_{n-1}|\overline{z}^{n-1} + \cdots |a_0|\overline{z}^{n-1}.$$

Thus, $|\overline{z}| \leq |a_{n-1}| + \cdots + |a_0|$. However, we assumed that $|\overline{z}| \geq 1$. This may not be the case. Thus, $|\overline{z}| \leq B := \max\{1, |a_{n-1}| + \cdots + |a_0|\}$. □

Solution: ⟨⟨ **[CLO05] Ex. 2.1.4** ⟩⟩ : Numerically find all roots of $2z^6 + 2z^5 - z^4 - z^3 - 2z^2 - 2z - 2$. □

Solution: [CLO05] Ex. 2.1.5: We apply Buchberger's Criterion. Let $f(x,y)=x^2+2x+3+y^5-y$ and $g(x,y)=y^6-y^2+2y$. Then we have that

$$S(f,g)=\frac{x^2y^6}{x^2}\cdot(x^2+2x+3+y^5-y)-\frac{x^2y^6}{y^6}\cdot(y^6-y^2+2y)=y^6\cdot(x^2+2x+3+y^5-y)-x^2\cdot(y^6-y^2+2y).$$

This shows that $\overline{S(f,g)}^G=0$ which yields that G is a Gröbner basis. $\square$

Solution: ⟨⟨ **[CLO05] Ex. 2.1.6** ⟩⟩ : $\square$

Solution: ⟨⟨ **[CLO05] Ex. 2.1.7** ⟩⟩ : $\square$

Solution: [CLO05] Ex. 2.1.8:

(a) Let $\bar{z}$ be a simple root of $p(z)$, so $p(z) = 0$ but $p'(z) \neq 0$. Then $N_p(\bar{z}) = \bar{z} - \frac{p(\bar{z})}{p'(\bar{z})} = \bar{z}$ meaning $\bar{z}$ is a fixed point of $N_p(z)$.

(b) Suppose that $\bar{z}$ is a multiple root of $p(z)$ with multiplicity $m \geq 2$. Then we may express $p(z) = \tilde{(p)}(z)(z-\bar{z})^m$ such that $\tilde{p}(\bar{z}) \neq 0$. Thus, we have that

$$\begin{aligned} N_p(z) &:= z - \frac{p(z)}{p'(z)} \\ &= z - \frac{\tilde{p}(z)(z-\bar{z})^m}{\tilde{p}'(z)(z-\bar{z})^m + m\tilde{p}(z)(z-\bar{z})^{m-1}} = z - \frac{\tilde{p}(z)(z-\bar{z})}{\tilde{p}'(z)(z-\bar{z}) + m\tilde{p}(z)} \end{aligned}$$

Note that $m\tilde{p}(\bar{z}) \neq 0$. Thus, we have that

$$\left|N_p(\bar{z})\right| = \left|\bar{z} - \frac{\tilde{p}(\bar{z})(\bar{z}-\bar{z})}{\tilde{p}'(\bar{z})(\bar{z}-\bar{z}) + m\tilde{p}(\bar{z})}\right| = |\bar{z}| \leq \mathrm{LC}(p) \cdot B$$

where B is the value from [CLO05] Ex. 2.1.3 and $\mathrm{LC}(p)$ is the leading coefficient of $p(z)$.

(c) Suppose now that $\bar{z}$ is a simple root of $p(\bar{z})$. Then we may express $p(z) = \tilde{p}(z)(z-\bar{z})$ such that $\tilde{p}(\bar{z}) \neq 0$. We have that

$$p'(z) = \tilde{p}'(z)(z-\bar{z}) + \tilde{p}(z)$$

and evaluation of $p'(z)$ at $\bar{z}$ is nonzero.

(d) Let $\bar{z}$ be a root of multiplicity m. Following (b), we write $p(z) = \tilde{p}(z)(z-\bar{z})^m$ such that $\tilde{p}(\bar{z}) \neq 0$. Then we have, by differentiating the expression for $N_p(z)$ from (b), that

$$N_p'(z) = 1 - \frac{(\tilde{p}'(z)(z-\bar{z}) + \tilde{p}(z))(\tilde{p}'(z)(z-\bar{z}) + m\tilde{p}(z)) - (\tilde{p}(z)(z-\tilde{z}))(\tilde{p}''(z)(z-\bar{z}) + \tilde{p}'(z) + m\tilde{p}'(z))}{(\tilde{p}'(z)(z-\bar{z}) + m\tilde{p}(z))^2}.$$

Evaluation at $z = \bar{z}$ yields that $\lim_{z \to \bar{z}} N_p'(z) = 1 - \frac{1}{m}$.

(e) Let $\bar{z}$ be a root of multiplicity m. Following (b), we write $p(z) = \tilde{p}(z)(z-\bar{z})^m$ such that $\tilde{p}(\bar{z}) \neq 0$. Then

$$p'(z) = \tilde{p}'(z-\bar{z})^m + m\tilde{p}(z)(z-\bar{z})^{m-1} = (z-\bar{z})^{m-1}(\tilde{p}'(z)(z-\bar{z}) + m\tilde{p}(z)).$$

Notice that $\tilde{p}'(\bar{z})(\bar{z}-\bar{z}) + m\tilde{p}(\bar{z}) = m\tilde{p}(\bar{z}) \neq 0$. Thus, a root of multiplicity $m \geq 1$ of $p(z)$ is a root of multiplicity $m-1$ of $p'(z)$. This implies that if we have roots $\bar{z}_1, \ldots, \bar{z}_k$ with multiplicities $m_1, \ldots, m_k \geq 1$, then $\gcd(p(z), p'(z)) = (z-\bar{z}_1)^{m_1} \cdots (z-\bar{z}_k)^{m_k}$. Thus, the polynomial $p_{\text{red}}(z) = \frac{p(z)}{\gcd(p(z),p'(z))}$ has the same roots of $p(z)$ but all with multiplicity 1 which is the best case for Newton's method.

$\square$

Solution: [CLO05] Ex. 2.1.9:

(a) Let $p(z) = z^2 + 1$. We have that

$$N_p(z) = z - \frac{z^2+1}{2z} = \frac{2z^2 - z^2 + 1}{2z} = \frac{z^2+1}{2z} = \frac{x^2 + 2ixy - y^2 + 1}{2x + 2iy}.$$

If z is real then $y = 0$ and so $N_p(x) = \frac{x^2+1}{2x}$ which is always real. Thus, Newton's method will never reach the imaginary roots of $z^2 + 1$. However, if we begin with a guess with nonzero imaginary part, then the guess does converge as expected.

(b) **⟨⟨ Just basic arithmetic not worth doing. ⟩⟩**

□

Solution: [CLO05] Ex. 2.1.10: Let $\bar{z}$ be a root of $p(z)$. Then $-\bar{z}^n = a_{n-1}\bar{z}^{n-1} + \cdots + a_0$ and so

$$\begin{aligned}
|\bar{z}|^n &= \left|a_{n-1}\bar{z}^{n-1} + \cdots + a_0\right| \\
&\le \max_i \{|a_i|\} \cdot \left|\bar{z}^{n-1} + \cdots + 1\right| \\
&\le \max_i \{|a_i|\} \cdot \left(|\bar{z}|^{n-1} + \cdots + 1\right) \\
&= \max_i \{|a_i|\} \cdot \frac{|\bar{z}|^n + 1}{|\bar{z}| - 1} \le \max_i \{|a_i|\} \cdot \frac{|\bar{z}|^n}{|\bar{z}| - 1}.
\end{aligned}$$

Thus, $|\bar{z}|^n \le \max_i \{|a_i|\} \cdot \frac{|z|^n}{|z|-1}$ which implies that $|z| - 1 \le \max_i \{|a_i|\}$. Thus, $|z| \le 1 + \max_i \{|a_i|\}$. □

2.2 Finite Dimensional Algebras

Solution: ⟨⟨ **[CLO05] Ex. 2.2.1** ⟩⟩ : □

Solution: [CLO05] Ex. 2.2.2: It is clear that $\langle p_i(x_i)\rangle \subseteq I \cap k[x_i]$. Now suppose that $f(x_i) \in I \cap k[x_i]$. Then $\deg(f(x_i))$ must be $\geq m_i$. If not, then by the minimality of m_i we would arrive at a contradiction. Now by the division algorithm, write $f(x_i) = q(x_i)p_i(x_i) + r(x_i)$ where $\deg(r_{x_i}) < m_i$. Then $r(x_i) = f(x_i) - q(x_i)p(x_i) \in I$ and so $r(x_i)$ must be 0 since if not, we would arrive at a contradiction of the minimality of m_i.

This gives us an algorithm to compute $p_i(x_i)$. Let I be a zero dimensional ideal and G a Gröbner basis for I. Then we know there exists m_i such that $\{1, [x_i], \ldots, [x^{m_i}]\}$ is linearly dependent in $k[\overline{x}]/I$. In fact, we may use the Finiteness Theorem to set m_i to the smallest integer such that $x_i^{m_i} = \textsc{lt}(g)$ for some $g \in G$. Since $k[x_1, \ldots, x_n]/I$ is a vector space, we can check linear independence in the usual way. See `code/ch2/2_2_2.sage` for a SageMath implementation of this. □

Solution: [CLO05] Ex. 2.2.3: Let $0 \neq f(x) \in \sqrt{\langle p(x)\rangle}$. Then there exists $m \geq 1$ such that $f^m \in \langle p(x)\rangle$ and so $p(x) \mid f(x)^m$. In particular, each linear factor $(x - \overline{z})$ of $p(x)$ divides $f(x)^n$ and so divides $f(x)$ as $(x - \overline{z})$ is irreducible. Thus, $p_{\text{red}}(x) \mid f(x)$ and so $f(x) \in \langle p_{\text{red}}(x)\rangle$. Conversely, suppose $f(x) \in \langle p_{\text{red}}(x)\rangle$ so that $\langle p_{\text{red}}\rangle \mid f(x)$. Label the roots of $p(x)$ as $\overline{z}_1, \ldots, \overline{z}_r$, each $\overline{z}_i \in \overline{k}$. Then for each i, $(x - \overline{z}_i) \mid f(x)$ Let m_i be the multiplicity of z_i in $p(x)$ and $m = \max\{m_1, \ldots, m_r\}$. Then $p(x) \mid f(x)^m$ and so $f(x) \in \sqrt{\langle p(x)\rangle}$ □

Solution: [CLO05] Ex. 2.2.4: We use the algorithm from [CLO05] Ex. 2.2.2 implemented in `code/ch2/2_2_2sage`. See `code/ch2/2_2_2sage` for the code in action. □

Solution: ⟨⟨ **[CLO05] Ex. 2.2.5** ⟩⟩ : Then $\sqrt{I} = I + \langle x(x-1), y(y-2)\rangle$. Since $I \subseteq \sqrt{I}$, we see that $\dim \mathbb{C}[x,y]/I \geq \dim \mathbb{C}[x,y]/\sqrt{I}$. A quick SageMath computation confirms this: $\dim \mathbb{C}[x,y]/I = 9$ and $\dim \mathbb{C}[x,y]/\sqrt{I} = 2$. See `code/ch2/2_2_5.sage` for the code in action. Then, since $I \subseteq \sqrt{I}$ we have that $V(\sqrt{I}) \subseteq V(I)$. Notice that

$$\begin{aligned} y^4x + 3x^3 - y^4 - 3x^2 &= y^4(x-1) + 3x^2(x-1) = (y^4+3x^2)(x-1) \\ x^2y - 2x^2 &= x^2(y-2) \\ 2y^4x - x^3 - 2y^4 + x^2 &= 2y^4(x-1) - x^2(x-1) = (2y^4 - x^2)(x-1). \end{aligned}$$

Thus, $(1,2)$ and $(0,0)$ are the only two points in $V(I)$. Since it is evident that $V(\sqrt{I})$ contains these two points, we see in this case that $V(\sqrt{I}) = V(I)$. □

Solution: [CLO05] Ex. 2.2.6: A grevlex Gröbner basis for I is $\{y^4 - 16y^2, x^3 - x^2, -2x^2\}$. Thus, by the Finiteness Theorem, we know that the for monomials $x^a y^b$ in $\mathbb{C}[x,y]/I$ we must have that $0 \leq a \leq 1$ and $0 \leq b \leq 3$. See `code/ch2/2_2_6.sage` for the code in action to compute the table. □

Solution: [CLO05] Ex. 2.2.7: We implement the algorithm described in ⟨⟨ **[CLO05] Ex. 1.3.11** ⟩⟩ . See `/code/ch2/2_2_7.sage` for the code in action. □

Solution: [CLO05] Ex. 2.2.8:

(a) See `code/ch2/2_2_8.sage` for the code in action.

(b) Since each of the I_j are maximal ideals and $I_j \subseteq \sqrt{I_j}$, we must have that $I = \sqrt{I_j}$. Thus $I(V(I_j)) = I_j$ and we must have that $I_j = \sqrt{I_j}$. Since each I_j is radical and $I = \bigcap_{j=1}^{5} I_j$, we have by [CLO05] Ex. 2.2.7 that I is radical.

□

Solution: [CLO05] Ex. 2.2.9:

(a) Let $f(\overline{x}) \in I + \langle p \rangle$ and let $1 \le j \le d$. Then $f(\overline{x}) = g(\overline{x}) + h(\overline{x})p(x_1)$ for some $g(\overline{x}) \in I$ and $h(\overline{x}) \in k[\overline{x}]$. We have that $(x_1 - a_j) \mid p(x_1)$ and so $h(\overline{x})p(x_1) \in \left\langle x_1 - a_j \right\rangle$. Thus, $f(\overline{x}) = g(\overline{x}) + h(\overline{x})p(x_1) \in I + \left\langle x_1 - a_j \right\rangle$. As j was arbitrary, we have that $f(\overline{x}) \in \bigcap_j (I + \left\langle x_1 - a_j \right\rangle)$.

(b) Let $f(\overline{x}) \in p_j \cdot (I + \left\langle x_1 - a_j \right\rangle)$. Then $f(\overline{x}) = p_j(x_1) \cdot (g(\overline{x}) + h(\overline{x})(x_1 - a_j))$ for some $g(\overline{x}) \in I$ and $h(\overline{x}) \in k[\overline{x}]$. We have that $p_j(x_1)g(\overline{x}) \in I$ and $p_j(x_1)h(\overline{x})(x_1 - a_j) = h(\overline{x})p(x_1) \in \langle p \rangle$. Thus, $f(\overline{(x)}) = p_j(x_1)g(\overline{x}) + h(\overline{x})p(x_1) \in I + \langle p \rangle$.

(c) Let $d = \gcd(p_1, \ldots, p_d)$. Then as $d \mid p_1$ and $d \mid p_2$, we have that $d \mid \prod_{j \neq 1,2}(x_1 - a_j)$. Continuing on inductively, we have that for all $c \le d$ that $d \mid \prod_{j \notin [c]}(x_1 - a_j)$. In particular, this means that $d \mid \prod_{j \notin [d]}(x_1 - a_j) = 1$. Thus, d itself is a unit in $k[\overline{x}]$ and p_i and p_j are coprime. By Bezout's Lemma, there exists polynomials $h_1, \ldots, h_d \in k[\overline{x}]$ such that $1 = \sum_{j=1}^d h_j(\overline{x})p_j(x_1)$.

(d) Now let $h(\overline{x}) \in \bigcap_{j=1}^d (I + \left\langle x_1 - a_j \right\rangle)$. As all the p_j are coprime, we have that there exist polynomials $h_1, \ldots, h_d \in k[\overline{x}]$ such that $1 = \sum_{j=1}^d h_j(\overline{x})p_j(x_1)$. Thus, $h = \sum_{j=1}^d h_j(\overline{x})p_j(x_1)h(\overline{x})$. Then for all $1 \le j \le d$, we have that as $p_j(x_1)h(\overline{x}) \in p_j \cdot (I + \left\langle x_1 - a_j \right\rangle) \subseteq I + \langle p \rangle$. Thus, each summand of $\sum_{j=1}^d h_j(\overline{x})p_j(x_1)h(\overline{x})$ is in $I + \langle p \rangle$ and so overall $h \in I + \langle p \rangle$.

$\square$

Solution: [CLO05] Ex. 2.2.10:

(a) Let $\overline{f}^G = \sum_{j=1}^d c_j(f)x^{\alpha(j)}$ and $\overline{g}^G = \sum_{j=1}^d c_j(g)x^{\alpha(j)}$. Then by combining like terms, we have that $\overline{f}^G + \overline{g}^G = \sum_{j=1}^d (c_j(f) + c_j(g))x^{\alpha(j)}$. On the other hand, we have that $\overline{f+g}^G = \sum_{j=1}^d c_j(f+g)x^{\alpha(j)}$. Since $\overline{f}^G + \overline{g}^G = \overline{f+g}^G$ and each of the $x^{\alpha(j)}$ are linearly independent, we may equate coefficients and conclude that $c_j(f) + c_j(g) = c_j(f+g)$. For $\lambda \in k$, $\overline{\lambda f}^G = \sum_{j=1}^d c_j(\lambda f)x^{\alpha(j)}$. Now notice that $\overline{\lambda f}^G = \lambda \overline{f}^G$ as we are working over a field. Thus, we have by equating coefficients that $c_j(\lambda f) = \lambda c_j(f)$. Thus, c_j is a linear function $A \to k$.

(b) Let $\alpha_j \in A^*$ be the linear map $\alpha_j(f) = c_j(f)$. Notice that for all $1 \le i, j \le d$ we have that $\alpha_j(x^{\alpha(i)}) = c_j(x^{\alpha(i)}) = \delta_{i,j}$. Suppose there exists $\lambda_1, \ldots, \lambda_d \in k$ such that $\lambda_1\alpha_1 + \cdots + \lambda_d\alpha_d = 0$. Then for all $1 \le i \le d$ we have that

$$0 = \left(\sum_{j=1}^d \lambda_j \alpha_j\right)(x^{\alpha(i)}) = \sum_{j=1}^d \lambda_j \alpha_j(x^{\alpha(i)}) = \lambda_i$$

and so for all $1 \le i \le d$, $\lambda_i = 0$ meaning that $\{\alpha_1, \ldots, \alpha_d\}$ is linearly independent. Since we know that $d = \dim A = \dim A^*$, we have that $\{\alpha_1, \ldots, \alpha_d\}$ is a basis for A^*.

(c) This was proven in **(b)**.

$\square$

Solution: [CLO05] Ex. 2.2.11:

(a) We want a linear polynomial $\ell(\overline{x}) = \ell_1 x_1 + \cdots + \ell_n x_n$ takes distinct values at each of the $p_i \in \mathbb{C}^n$. Consider the space of all such $(\ell_1, \ldots, \ell_n)$. This itself is a $\mathbb{C}$ vector space, call it L. Let $L_{i,j}$ be the subspace of L corresponding to polynomials $\ell(\overline{x})$ such that $\ell(p_i) = \ell(p_j)$. There are finitely many such $L_{i,j}$. We know that vector spaces over an infinite field cannot be expressed as the finite union of proper subspaces. Thus, $L \neq \bigcup_{1 \leq i \neq j \leq m} L_{i,j}$. This means there exists $(\ell_1, \ldots, \ell_n) \in L \setminus \bigcup_{1 \leq i \neq j \leq m} L_{i,j}$ such that $\ell(\overline{x}) = \ell_1 x_1 + \cdots + \ell_n x_n$ takes distinct values at each of the p_i.

⟨⟨ Can we do this constructively? ⟩⟩

(b) Let $\ell(\overline{x})$ be our constructed polynomial from **(a)**. For $1 \leq i \leq m$, we define $g_i \in \mathbb{C}[x_1, \ldots, x_n]$ as

$$g_i(\overline{x}) = \frac{\prod_{1 \leq i \neq j \leq m} \ell(\overline{x}) - \ell(\overline{p_j})}{\prod_{1 \leq i \neq j \leq m} \ell(p_i) - \ell(\overline{p_j})}.$$

Then clearly $g_i(p_j) = \delta_{ij}$ as desired.

□

Solution: [CLO05] Ex. 2.2.12:

(a) Clearly the map is linear. We now show it is well defined. Let $[f] = [g] \in \mathbb{C}[\overline{x}]/I$ meaning that $f - g \in I$. Thus, we have that

$$\varphi([f]) - \varphi([g]) = \varphi([f - g]) = 0 \implies \varphi([f]) = \varphi([g])$$

as desired.

(b) Let $[f], [g] \in \mathbb{C}[\overline{x}]/I$. Then we have

$$\begin{aligned} \varphi([f] \cdot [g]) &= \varphi([f \cdot g]) \\ &= ((f \cdot g)(p_1), \ldots, (f \cdot g)(p_m)) \\ &= (f(p_1) \cdot g(p_1), \ldots, f(p_m) \cdot g(p_m)) \\ &= (f(p_1), \ldots, f(p_m)) \cdot (g(p_1), \ldots, g(p_m)) = \varphi([f]) \cdot \varphi([g]). \end{aligned}$$

Thus, φ is a homomorphism of rings. In fact, it is a homomorphism of $\mathbb{C}$-algebras as $(\lambda \cdot f)(x) := \lambda \cdot f(\overline{x})$ for all $\lambda \in \mathbb{C}$ and $f \in \mathbb{C}[\overline{x}]$ and this descends to $\mathbb{C}[\overline{x}]/I$.

(c) We have that φ is surjective and that $I \subseteq \ker(\varphi)$ as in the proof of [CLO05, Theorem 2.10]. So we want to show that $\ker(\varphi) \subseteq I$ if and only if $I = \sqrt{I}$ which holds exactly as in the proof of [CLO05, Theorem 2.10].

□

2.3 Gröbner Basis Conversion

Solution: [CLO05] Ex. 2.3.2: Recall that *lex* ordering compares the exponents of x_1, and then in the case of equality compares the exponents of x_2, and continues on in this manner. As such $\overline{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \geq x_1^a$ if and only if $alpha_1 \geq a_1$ which is equivalent to saying that $x_1^{a_1} \mid x_1^{\alpha_1} \mid \overline{x}^\alpha$ □

Solution: [CLO05] Ex. 2.3.3:

(a) Suppose for some $1 \leq i \leq k$ we have that $\mathrm{LT}(g_i) \mid x_1^{a_1+1}$. This would imply that $\mathrm{LT}(g_i)$ is a power of x_1. However, we assumed that we were in the situation of the Next Monomial procedure, meaning that the algorithm has not terminated which in turn implies that we have not added any polynomials to G_{lex} such that their leading term is a power of x_1. Thus, no such $\mathrm{LT}(g_i)$ divides $x_1^{a_1+1}$.

(b) Clearly we have that

$$\overline{x}^\beta = x_1^{a_1} \cdots x_{k-1}^{a_{k-1}} x_k^{a_k+1} > x_1^{a_1} \cdots x_{k-1}^{a_{k-1}} x_k^{a_k} = \overline{x}^\alpha.$$

To show that $\overline{x}^\beta$ is the smallest monomial greater than $\overline{x}^\alpha$ where no $\mathrm{LT}(g_i)$ divides $\overline{x}^\beta$, we want to show that $k+1 \leq j, \ell \leq n$ and monomial $\overline{x}^\gamma$ of the form

$$\overline{x}^\gamma = x_1^{a_1} \cdots x_k^{a_k} x_{k+1}^{c_{k+1}} \cdots x_j^{c_j},\ c_{k+1} \geq a_{k+1}, \ldots, c_{\ell-1} \geq a_{\ell-1}, c_\ell > a_\ell, c_{\ell+1} \geq 0, \ldots, c_j \geq 0. \tag{2.1}$$

sharing the same properties as $\overline{x}^\beta$. First, we indeed see that $\overline{x}^\beta > \overline{x}^\gamma$ as $a_k + 1 > a_k$ and $x^\gamma > x^\alpha$ by the assumption on ℓ. We also see that any x^γ such that $x^\beta > x^\gamma > x^\alpha$ must satisfy Equation (2.1). Suppose towards contradiction that none of the $\mathrm{LT}(g_i)$ divide $\overline{x}^\gamma$. Then we have that

$$\overline{x}^\beta > x_1^{a_1} \cdots x_k^{a_k} x_{k+1}^{c_{k+1}} \cdots x_j^{c_j} \geq x_1^{a_1} \cdots x_k^{a_k} x_{k+1}^{c_{k+1}} \cdots x_\ell^{c_\ell} \geq x_1^{a_1} \cdots x_k^{a_k} x_{k+1}^{c_{k+1}} \cdots x_\ell^{a_\ell+1} > \overline{x}^\alpha.$$

Since No $\mathrm{LT}(g_i)$ divides $\overline{x}^\gamma$, we have that no $\mathrm{LT}(g_i)$ divides $x_1^{a_1} \cdots x_k^{a_k} x_{k+1}^{c_{k+1}} \cdots x_\ell^{a_\ell+1}$. As $\ell > k$, this contradicts the maximality of k. Thus, we cannot have that none of the $\mathrm{LT}(g_i)$ divide $\overline{x}^\gamma$.

□

Solution: [CLO05] Ex. 2.3.4: We want to show that B_{lex} is a monomial basis for $k[x_1, \ldots, x_n]/I$. A monomial basis is the set of all monomials that are not in $\langle \mathrm{LT}(g) \mid g \in G_{lex} \rangle$, i.e. the non-leading monomials. However, in the proof of the correctness of the FGLM algorithm, we note that because we are stepping through monomials in $k[\overline{x}]$ in increasing *lex* order, all non-leading monomials of each $g \in G_{lex}$ must have been included in B_{lex} already. Thus, B_{lex} is our desired monomial basis. □

Solution: [CLO05] Ex. 2.3.7: Since polynomials are added to G_{lex} with coefficient 1 in the Main Loop (a.), we have that G_{lex} is a monic Gröbner basis. Then, as monomials are considered in increasing order and we consider them only once per iteration of the Main Loop, we automatically have that G_{lex} is a *minimal lex* Gröbner basis meaning that for all distinct $p \in G_{lex}$, we have that $\textsc{lt}(p) \notin \langle \textsc{lt}(G_{lex} \setminus \{p\}) \rangle$. Recall that a *reduced lex* Gröbner basis G is one such that for all distinct $p, q \in G$ that no monomial appearing in p is a multiple of $\textsc{lt}(q)$. Suppose there was such distinct $p, q \in G$ and let $\overline{x}^\alpha$ be the monomial in p such that $\textsc{lt}(q) \mid x^\alpha$. Then in particular, this implies that $\textsc{lt}(q) \leq_{lex} \overline{x}^\alpha$. Suppose that $\textsc{lt}(q) = \overline{x}^\alpha$. Then if $\overline{x}^\alpha$ is not a leading term of some $p \in G_{lex}$, then when p was added to G_{lex} we must have that $x^\alpha = \textsc{lt}(q) \in B_{lex}$, contradicting that $q \in G_{lex}$. If $\overline{x}^\alpha$ is a leading term of some $p \in G_{lex}$, then $p = q$ contradicting distinctness. Now suppose that $\textsc{lt}(q) <_{lex} \overline{x}^\alpha$. Then $\textsc{lt}(q) < \textsc{lt}(p)$. When $\textsc{lt}(p)$ was added to G_{lex}, $\overline{x}^\alpha = \textsc{lt}(q)$ was a monomial in B_{lex} but $\textsc{lt}(q)$ cannot be an element of B_{lex}, a contradiction. **⟨⟨ There should be an easier cleaner solution. ⟩⟩** □

Solution: [CLO05] Ex. 2.3.8: See `code/ch2/2_3_8.sage` for the code in action. □

2.4 Solving Equations via Eigenvalues and Eigenvectors

Solution: [CLO05] Ex. 2.4.2: If $f(t)$ and $g(t)$ are in I_M so that $f(M) = g(M) = 0$, then we have that $(f+g)(M) = f(M)+g(M) = 0$ so $(f+g)(t) \in I_M$. Then if $p(t) \in k[t]$, we have that $(p \cdot f)(M) = p(M) \cdot f(M) = 0$. Thus, I_M is an ideal in $k[t]$. $\square$

2.5 Real Root Location and Isolation

Chapter 3

Resultants

3.1 The Resultant of Two Polynomials

Solution: [CLO05] Ex. 3.1.1: Swapping two adjacent columns in a matrix multiplies the determinant by -1. Since the matrix for $\mathrm{Res}(g, f)$ is formed by moving each of the l columns of $\mathrm{Res}(f, g)$ corresponding to g a total of m columns each, we have that the determinants must differ by a factor of $(-1)^{l\cdot m}$. $\square$

Solution: [CLO05] Ex. 3.1.3:

(a) Let $f(x) = a_0(x-\xi_1)\cdots(x-\xi_l)$ and $g(x) = b_0(x-\eta_1)\cdots(x-\eta_m)$. To see the first equality, we have that

$$a_0^m b_0^l \prod_{i=1}^{l}\prod_{j=1}^{m}(\xi_i - \eta_j) = a_0^m \prod_{i=1}^{l} b_0(\xi_i - \eta_1)\cdots(\xi_i - \eta_m) = a_0^m \prod_{i=1}^{k} g(\xi_i).$$

The equality $a_0^m b_0^l \prod_{i=1}^{l}\prod_{j=1}^{m}(\xi_i - \eta_j) = (-1)^{lm} b_0^l \prod_{j=1}^{m} f(\eta_j)$ follows the same logic using the fact that $(\xi_i - \eta_j) = -(\eta_j - \xi_i)$ and there are lm many such pairs.

(b) Let $f_1(x) = a_1(x-\xi_1)\cdots(x-\xi_{l_1})$, $f_2(x) = a_2(x-\xi_{l_1+1})\cdots(x-\xi_{l_2})$, and $g(x) = b_0(x-\eta_1)\cdots(x-\eta_m)$. Then $f_1(x)f_2(x) = a_1a_2(x-\xi_1)\cdots(x-\xi_{l_1})(x-\xi_{l_1+1})\cdots(x-\xi_{l_2})$. Thus, we have that

$$\begin{aligned}
\mathrm{Res}(f_1f_2, g) &= a_1^m a_2^m b_0^{l_1+l_2} \prod_{i=1}^{l_1+l_2}\prod_{j=1}^{m}(\xi_i - \eta_j) \\
&= a_1^m a_2^m b_0^{l_1+l_2} \left(\prod_{i=1}^{l_1}\prod_{j=1}^{m}(\xi_i - \eta_j)\right)\left(\prod_{i=l_1+1}^{l_2}\prod_{j=1}^{m}(\xi_i - \eta_j)\right) \\
&= \left(a_1^m b_0^{l_1} \prod_{i=1}^{l_1}\prod_{j=1}^{m}(\xi_i - \eta_j)\right)\left(a_2^m b_0^{l_2} \prod_{i=l_1+1}^{l_2}\prod_{j=1}^{m}(\xi_i - \eta_j)\right) = \mathrm{Res}(f_1, g)\cdot\mathrm{Res}(f_2, g).
\end{aligned}$$

$\square$

Solution: [CLO05] Ex. 3.1.4: The result is seen by looking at the definition of $\text{Res}(F,G)$ for homogeneous $F,G \in k[x,y]$ We see that $a_0 = 1$, the coefficient of x^l, lies on the first m entries of the main diagonal and that $b_m = 1$, the coefficient of y^m, lies on the last l entries of the main diagonal. All other entries of the matrix are 0 and so the resulting matrix is just the $(l+m)\times(l+m)$ identity matrix which has determinant 1. □

Solution: [CLO05] Ex. 3.1.7: **⟨⟨ This is clear to see if you write out the matrix but awful to type out formally... ⟩⟩** □

Solution: [CLO05] Ex. 3.1.8:

(a) Since $m = \deg(g) = 0$, there are no columns with the coefficients of f. Thus, $\text{Syl}(f,g)$ is a $l \times l$ matrix just consisting of b_0 along the main diagonal and so $\text{Res}(f,g) = b_0^l$.

□

Chapter 4

Computation in Local Rings

4.1 Local Rings

Solution: [CLO05] Ex. 4.1.6: Let R be the set of all elements x of F such that $v(x) \geq 0$, along with 0.

(a) We claim that the unique maximal ideal in R is $M := \{ x \in \mathbb{R} \mid v(x) > 0 \}$. To show this, we will show that every element in $R \setminus M$, the nonzero elements x such that $v(x) = 0$, is a unit in R. As such, let $0 \neq x \in R \setminus M$. Then $0 \neq x \in F$ implies that $0 \neq x^{-1} \in F$. We claim that $x^{-1} \in R \setminus M$. Indeed, we have that

$$v(1) + v(x^{-1}) = v(1 \cdot x^{-1}) = v(x^{-1}) = v(x) + v(x^{-1}) = v(xx^{-1}) = v(1)$$

and so $v(x^{-1}) = 0$ as well showing that $x^{-1} \in R \setminus M$. Thus, R is a local ring.

(b) The check that v is a discrete valuation is straightforward **⟨⟨ and omitted for now ⟩⟩** . The maximal ideal is given by

$$M = \{ x \in k(x) \mid v(x) = 0 \} = \left\{ \frac{n}{d} \in k(x) \;\middle|\; f \text{ does not divide } n, d \right\}.$$

(c) The check that v is a discrete valuation is straightforward **⟨⟨ and omitted for now ⟩⟩** . The maximal ideal is given by

$$M = \{ x \in \mathbb{Q} \mid v(x) = 0 \} = \left\{ \frac{n}{d} \in \mathbb{Q} \;\middle|\; p \text{ does not divide } n, d \right\}.$$

□

Solution: [CLO05] Ex. 4.1.7:

(a) Let $c_0(x) = 1$. Treating $a_{i,1}$ as an indeterminate, we have that

$$\begin{aligned} f(x, a_i + a_{i,1}x) &\equiv \sum_{j=0}^{n} c_{n-j}(x)(a_i + a_{i,1}x)^j \\ &\equiv \sum_{j=0}^{n} c_{n-j}(x) \sum_{\ell=0}^{j} \binom{k}{j} (a_{i,1}x)^\ell a_i^{j-\ell} \\ &\equiv \sum_{j=0}^{n} c_{n-j}(x)(a_i^j + j a_{i,1} x a_i^{j-1}) \\ &\equiv f(x, a_i) + (a_{i,1}x) \frac{\partial f}{\partial y}(x, a_i) \equiv f(0, a_i) + \left(C + \frac{\partial f}{\partial y}(0, a_i) a_{i,1} \right) x \pmod{x^2} \end{aligned}$$

where C is some polynomial expression in the coefficients of f and a_i, and in particular doesn't depend on $a_{i,1}$ or x. Such C exists as all terms with $\deg_x \geq 2$ go to $0 \pmod{x^2}$ and we can factor out the remaining x. Then as $f(0, a_i) = 0$, we want $a_{i,1}$ such that $\left(C + \frac{\partial f}{\partial y}(0, a_i)a_{i,1}\right)x \equiv 0 \pmod{x^2}$. This is equivalent to saying that $C + \frac{\partial f}{\partial y}(0, a_i)a_{i,1} = 0$ in k. Then as a_i is a *simple* root, we know that $\frac{\partial f}{\partial y}(0, a_i) \neq 0$ and so we can solve for $a_{i,1}$.

(b) Let $c_0(x) = 1$ and $\ell \geq 1$. As $f(x, y_i^{(\ell)}(x)) \equiv 0 \pmod{x^{\ell+1}}$, let C be a constant which is a polynomial in the coefficients of f and coefficients of $y_i^{(\ell)}$ such that $f(x, y_i^{(\ell)}(x)) \equiv Cx^{\ell+1} \pmod{x^{\ell+2}}$. Treating $a_{i,\ell+1}$ as an indeterminate, we have by similar arguments to above that

$$\begin{aligned} f(x, y_i^{(\ell+1)}(x)) &\equiv f(x, y_i^{(\ell)}) + (a_{i,\ell+1}x^{\ell+1}) \frac{\partial f}{\partial y}(x, y_i^{(\ell)}(x)) \\ &\equiv f(x, y_i^{(\ell)}) + (a_{i,\ell+1}x^{\ell+1}) \frac{\partial f}{\partial y}(0, a_i) \equiv \left(D + a_{i,\ell+1} \frac{\partial f}{\partial y}(0, a_i) \right) x^{\ell+1} \pmod{x^{\ell+2}}. \end{aligned}$$

This **⟨⟨ implies ⟩⟩** that $D + a_{i,\ell+1}\frac{\partial f}{\partial y}(0, a_i) = 0$ in k. Again, as a_i is a simple root, we know that $\frac{\partial f}{\partial y}(0, a_i) \neq 0$ and so we can solve for $a_{1,\ell+1}$.

(c) The prior two parts lay out an inductive argument for the claim.

□

Solution: [CLO05] Ex. 4.1.11: Note that $M = \langle x_1, \ldots, x_n \rangle$ is a prime,in fact maximal, ideal in $k[x_1, \ldots, x_n]$. Thus, every ideal $I_M \trianglelefteq R$ is of the form $I_M = \left\{ \frac{a}{s} \,\middle|\, a \in I, s \notin M \right\}$ for some ideal $I \trianglelefteq k[x_1, \ldots, x_n]$. We know that I is generated by polynomials $\{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n]$. Then, every element of the form $\frac{1}{s}$ for $s \notin M$ is an element of R_P. These two facts yields that $\{f_1, \ldots, f_s\}$ generates I_M in R. □

4.2 Multiplicities and Milnor Numbers

Solution: [CLO05] Ex. 4.2.1:

(a) Recall that the maximal ideal of $k[x_1, \dots, x_n]_{\langle x_1 - a_1, \dots, x_n - a_n \rangle}$ is the set $\left\{ \frac{f}{g} \,\middle|\, f, g \in k[x_1, \dots, x_n], g(\overline{a}) \neq 0, f(\overline{a}) = 0 \right\}$. Thus, as $1 + 0 = 1 \neq 0$, we know that $1 + x$ is not in the maximal ideal $\mathfrak{m}$ of R and so must be a unit.

(b) This follows immediately from part **a.** where $1 + x$ is a unit in R and the fact that $x^2 + x^3 = x^2(1 + x)$.

(c) Note that for all $h \in \langle x, y \rangle \subseteq R$, $1 + h(0,0) \neq 0$ and so $\frac{1}{1+h} \in R$. Then, $\langle x, y \rangle \subseteq k[x, y]$ is the set of all polynomials with constant term 0. Since we know that elements $f = \frac{g}{b} \in R$, where $g, b \in k[x, y]$, are such that $b(0,0) \neq 0$, we know there is a non-zero constant term. Via rescaling, we may assume that b has constant term 1 and so $b = 1 + h$ for some $h \in \langle x, y \rangle \subseteq k[x, y]$. To see uniqueness, suppose $\frac{g'}{1+h'} = f = \frac{g}{1+h}$ so that there exists $s \in k[x, y] \setminus \langle x, y \rangle$ such that

$$0 = s(g'(1 + h) - g(1 + h')) = s(g' - g + g'h - gh').$$

We know that $s \neq 0$ and so $g'(1 + h) = g(1 + h')$. Thus, $\frac{g}{1+h} = \frac{g'}{1+h'}$ in $k[x, y]$. The constant term being 1 in each denominator immediately implies uniqueness.

(d) Let $f \in R$ and g, h as in **(c)** such that $f = \frac{g}{1+h}$. Note that $g(1 - h + h^2) \in R$ by the inclusion $k[x, y] \hookrightarrow R$. We want to show that $f - g(1 - h + h^2) \in \left\langle x^2, y^2 \right\rangle \subseteq R$. To see this, first we compute the following:

$$f - g(1 - h + h^2) = \frac{g}{1 + h} - g(1 - h + h^2) = \frac{-h^3}{1 + h}.$$

As $h \in \langle x, y \rangle$, we have that $h = ax + by$ for some $a, b \in R$. Then, h^3 is such that every term has degree at least 2 in x or y and so $\frac{-h^3}{1+h} \in \left\langle x^2, y^2 \right\rangle$ as desired.

(e) Since we are working in $R/\left\langle x^2, y^2 R \right\rangle$, in g and h we may ignore terms in f, g which have degree at least 2 in either x or y. Writing $g = g_1 + g_x x + g_y y + g_{xy} xy$ where $g_1 g_x, g_y$, and $g_{xy} \in k$, and similarly $h = h_x x + h_y y + h_{xy} xy$, and expanding $[f] = [g(1 - h + h^2)]$ yields the desired constants. Uniqueness follows from the uniqueness of f, g.

□

Solution: [CLO05] Ex. 4.2.3:

(a) Using SageMath, we find the following four solutions:

$$(-3.464102, -1.732051)$$
$$(3.464102, 1.732051)$$
$$(-1.732051, 1.732051)$$
$$(1.732051, -1.732051)$$

(b) In Figure 4.1, we see that two points of intersection "bounce" which we know geometrically indicates these points have multiplicity > 1.

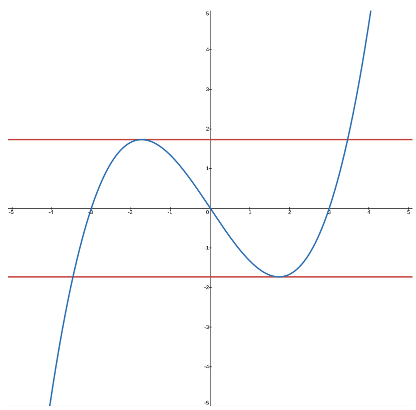

Figure 4.1: Real Plot of $y^2 - 3 = 0, 6y - x^3 + 9x = 0$.

(c) Using SageMath, we see that a monomial basis of $k[x, y]/I$ is given by $\{1, x, y, x^2, xy, x^2y\}$. Using this basis, m_x has the following matrix

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 18 \\ 1 & 0 & 0 & 9 & 0 & 0 \\ 0 & 0 & 0 & 6 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 9 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

which has characteristic polynomial

$$u^6 - 18u^4 + 81u^2 - 108 = (u^2 - 12)(u^2 - 3)^2.$$

(d) Further factoring of the characteristic polynomial over k into linear parts yields that

$$u^6 - 18u^4 + 81u^2 - 108 = (u^2 - 12)(u^2 - 3)^2 = (u - 2\sqrt{3})(u + 2\sqrt{3})(u - \sqrt{3})^2(u + \sqrt{3})^2.$$

Applying [CLO05, §4.2, Proposition 2.7] yields that the points with x-coordinate $\pm\sqrt{3}$ each have multiplicity 2, as expected from Figure 4.1, and the other points with x-coordinate $\pm 2\sqrt{3}$ each have multiplicity 2.

(e) **⟨⟨ TODO: Return once you have learned more about resultants. ⟩⟩**

□

Solution: [CLO05] Ex. 4.2.6: To show that $k[\overline{x}]_M / Ik[\overline{x}]_M$ is a local ring, it suffices to show that $(k[\overline{x}]/Ik[\overline{x}])_M \simeq k[\overline{x}]_M / Ik[\overline{x}]_M$. Consider the following morphism:

$$\begin{aligned} \phi : k[\overline{x}]_M / Ik[\overline{x}]_M &\to (k[\overline{x}]/Ik[\overline{x}])_M \\ \frac{f}{g} + Ik[\overline{x}]_M &\mapsto \frac{f+I}{g+I}. \end{aligned}$$

It is immediate that ϕ is well defined and surjective. To see that ϕ is injective, suppose that $\frac{f}{g} + Ik[\overline{x}]_M \in \ker\phi$. Then $\frac{f+I}{g+I} = 0$ implies that $f \in I$. Thus, $f \in Ik[\overline{x}]_M$ which implies that $\frac{f}{g} + Ik[\overline{x}]_M = 0$. Thus, ϕ is an isomorphism which implies that $k[\overline{x}]_M / Ik[\overline{x}]_M$ is a local ring.

To see that $k[\overline{x}]_M / Ik[\overline{x}]_M$ has dimension ≥ 1 as a k-vector-space, we show that evaluation at p, ev_p is a well-defined linear surjection of vector spaces. It is immediate that ev_p is a linear map. To see that it is well defined, suppose $\frac{f}{g} + Ik[\overline{x}]_M = \frac{f'}{g'} + Ik[\overline{x}]_M$. Then we have that $\frac{fg' - f'g}{gg'} \in Ik[\overline{x}]_M$ which implies that $fg' - f'g \in K$. Thus, $\mathrm{ev}_p\left(\frac{f}{g} - \frac{f'}{g'} + Ik[\overline{x}]_M\right) = 0$ and so by linearity of ev_p, we have that $\mathrm{ev}_p\left(\frac{f}{g} + Ik[\overline{x}]_M\right) = \mathrm{ev}_p\left(\frac{f'}{g'} + Ik[\overline{x}]_M\right)$ as desired. Since ev_p is obviously surjective, we must have that $\dim_k k[\overline{x}]_M / Ik[\overline{x}]_M \geq 1$. □

Solution: [CLO05] Ex. 4.2.7: As $\bigcap_{i=1}^n M_i$ is an ideal, it is finitely generated by polynomials $\{f_1, \ldots, f_s\}$. For each $f_j \in \bigcap_{i=1}^n M_i$, we have that for all $1 \leq i \leq n$ that $f_j(p_i) = 0$. Thus, $f_j \in \mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ and so there exists $d_j > 0$ such that $f^{d_j} \in I$. Let $d = \sum_{j=1}^s d_j$. Then for all $f \in \bigcap_{i=1}^n M_i$, we have that $f^d \in I$ and so $\left(\bigcap_{i=1}^n M_i\right)^d \subseteq I$. □

Solution: [CLO05] Ex. 4.2.9: Fix $1 \leq i \leq n$. As $\sum_{j=1}^m e_j \equiv 1 \pmod{I}$ and for $i \neq j$ we have that $e_i e_j \equiv 0 \pmod{I}$, we have that

$$e_i \equiv e_i \sum_{j=1}^m e_j = e_i^2 + \sum_{\substack{j=1 \\ j \neq i}}^m e_i e_j \equiv e_i^2 \pmod{I}.$$

□

Bibliography

[CLO05] D.A. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Springer-Verlag, 2005. ISBN: 0387207066. DOI: 10.1007/b138611.

[CLO15] D.A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer International Publishing, 2015. ISBN: 9783319167213.

[Str08] Bernd Strumfels. *Algorithms in Invariant Theory*. Springer Vienna, 2008. ISBN: 9783211774175. DOI: 10.1007/978-3-211-77417-5.