

# Using Algebraic Geometry

With 0 Figures

Anakin Dey

Last Edited on 9/4/24 at 08:26

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Polynomials and Ideals . . . . .	1
1.2	Gröbner Bases . . . . .	5
1.3	Affine Varieties . . . . .	6
<b>2</b>	<b>Solving Polynomial Equations</b>	<b>7</b>
2.1	Solving Polynomial Systems by Elimination . . . . .	7
2.2	Finite Dimensional Algebras . . . . .	11
2.3	Gröbner Basis Conversion . . . . .	15

# 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] Ex. 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  $\langle x - y^2, xy, y^2 \rangle \subseteq \langle x, y^2 \rangle$ . 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  $\langle x - y^2, xy \rangle$ . Since  $xy = xy$ , we overall have that  $\langle x^2, xy \rangle \subseteq \langle x - y^2, xy \rangle$ . It remains to check if  $x - y^2 \in \langle x^2, xy \rangle$ . However, notice that every element of  $\langle x^2, xy \rangle$  is divisible by  $x$  while  $x - y^2$  is clearly not divisible by  $x$ . Thus  $x - y^2 \notin \langle x^2, xy \rangle$  and the two ideals are not equal.

□

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

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

**Solution:** [CLO05] Ex. 1.1.4: We claim that  $\langle f_1, \dots, f_s \rangle = \langle g_1, \dots, g_t \rangle$  if and only if  $\{g_1, \dots, g_t\} \subseteq I$  and  $\{f_1, \dots, f_s\} \subseteq J$ . The forward implication is immediate. Then by [CLO05] Ex. 1.1.3, if  $\{g_1, \dots, g_t\} \subseteq I$  then  $J \subseteq I$ . Similarly,  $\{f_1, \dots, f_s\} \subseteq J \implies I \subseteq J$  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  $z - x^3 \in \langle y - x^2, z - xy \rangle$  and  $z - xy \in \langle x - y^2, z - x^3 \rangle$ . 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.  **$\langle d = \gcd(I)$  but I need infinite Bezout.  $\rangle$**  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  $0 \leq \deg(r) < \deg(d)$ . 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  $k$ th 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  $k = \max e_1, \dots, e_n$ . 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  $k$ th 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  $a_1, \dots, a_m \in \mathbb{C}$ .  $\square$

**Solution: [CLO05] Ex. 1.1.8:**

- (a) Let  $\mathfrak{p}$  be a prime ideal in  $k[\bar{x}]$ . Clearly  $\mathfrak{p} \subseteq \sqrt{\mathfrak{p}}$  always. Let  $f(\bar{x}) \in \sqrt{\mathfrak{p}}$ . Then  $f(\bar{x})^m \in \mathfrak{p}$  for some  $m \in \mathbb{Z}_{\geq 1}$ . We prove the reverse inclusion by induction on  $m$ . If  $m = 1$  then  $f(\bar{x}) = f(\bar{x})^1 \in \mathfrak{p}$ . Now let  $m > 1$  and suppose the claim holds for all  $k \leq m$ . Then suppose  $f(\bar{x})^{m+1} \in \mathfrak{p}$ . Then  $f(\bar{x}) \cdot f(\bar{x})^m \in \mathfrak{p}$ . Either  $f(\bar{x}) \in \mathfrak{p}$  or  $f(\bar{x})^m \in \mathfrak{p}$  which by induction implies that  $f(\bar{x}) \in \mathfrak{p}$ . Thus,  $f(\bar{x})^m \in \mathfrak{p} \implies f(\bar{x}) \in \mathfrak{p}$  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  $r \in \mathbb{R}$ . **⟨ What would be a general condition for  $\mathbb{Q}[x]$ ? ⟩**

□

**Solution: [CLO05] Ex. 1.1.9:**

- (a) First, observe that  $\langle x_1, \dots, x_n \rangle$  is the ideal consisting exactly of polynomials which have no constant term. Let  $I$  be an ideal in  $k[x_1, \dots, x_n]$  such that  $\langle x_1, \dots, x_n \rangle \subsetneq I$ . Thus there exists  $f(x_1, \dots, x_n) \in I \setminus \langle x_1, \dots, x_n \rangle$ . 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  $g(x_1, \dots, x_n)$  in  $\langle x_1, \dots, x_n \rangle$ . Thus, we have that  $z = f(x) - g(x) \in I$ . Since  $I$  contains a nonzero constant term, we must have that  $I = k[x_1, \dots, x_n]$ .
- (b) Recall that an ideal  $I$  is maximal if and only if  $R/I$  is a field. Let  $I = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ . Consider the evaluation map  $\text{ev}_{\bar{a}}: k[x_1, \dots, x_n] \rightarrow k$  sending  $f(x_1, \dots, x_n) \mapsto f(a_1, \dots, a_n)$ . Clearly this map is surjective. Then since for all  $i$  we have that  $x_i \equiv a_i \pmod{I}$ , we have that  $f(x_1, \dots, x_n) \equiv f(a_1, \dots, a_n) \pmod{I}$  for all  $f(x_1, \dots, x_n) \in k[x_1, \dots, x_n]$ . Thus,  $\text{ev}_{\bar{a}}(f) = f(a_1, \dots, a_n) = 0$  if and only if  $f(x_1, \dots, x_n) \in I$ . Thus,  $\ker(\text{ev}_{\bar{a}}) = I$  and  $k[x_1, \dots, x_n]/I$  is a field, meaning  $\langle x_1 - a_1, \dots, x_n - a_n \rangle$  is maximal.
- (c) Since  $\mathbb{R}[x]$  is a principal ideal domain, any ideal  $I$  strictly containing  $\langle x^2 + 1 \rangle$  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  $\langle g(x) \rangle = \langle x^2 + 1 \rangle$  or  $\langle g(x) \rangle = \mathbb{R}[x]$ . Thus,  $\langle x^2 + 1 \rangle$  is maximal. However, in  $\mathbb{C}[x]$ , we have that  $x^2 + 1 = (x + i)(x - i)$  and so  $\langle x^2 + 1 \rangle \subsetneq \langle x - i \rangle \subsetneq \mathbb{C}[x]$ .

□

**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  $f(x_{\ell+1}, \dots, x_n), g(x_{\ell+1}, \dots, x_n)$  are two polynomials in  $I$  who do not depend on the first  $\ell$  variables, then so is  $f + g$ . Finally, let  $r(x_\ell + 1, \dots, x_n) \in k[x_{\ell+1}, \dots, x_n]$ . Then  $r \cdot f \in I_\ell$  since  $r \cdot f \in I$  and still does not depend on any of the first  $\ell$  variables.

□

**Solution:** [CLO05] Ex. 1.1.11:

- (a) **<< meh >>**
- (b) **<< meh >>**
- (c) We claim that  $I + J = \langle f_1, \dots, f_s, g_1, \dots, g_t \rangle$ . Clearly  $I, J \subseteq \langle f_1, \dots, f_s, g_1, \dots, g_t \rangle$  and thus so is  $I \cup J$ . By (b), this shows that  $I + J \subseteq \langle f_1, \dots, f_s, g_1, \dots, g_t \rangle$ . 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.

□

**Solution:** [CLO05] Ex. 1.1.12:

- (a) **<< meh >>**
- (b) Suppose that  $h(\bar{x}) \in IJ$ . Note that  $IJ$  is generated by the products  $f(\bar{x}) \cdot g(\bar{x})$  for  $f(\bar{x}) \in I$ , and  $g(\bar{x}) \in J$ . Then  $h(\bar{x})$  consists of sums of terms of the form  $r(\bar{x}) \cdot f(\bar{x}) \cdot g(\bar{x})$  for  $r(\bar{x}) \in k[\bar{x}]$ ,  $f(\bar{x}) \in I$ , and  $g(\bar{x}) \in J$ . Thus, each term is in both  $I$  and  $J$  and overall so is  $h(\bar{x})$ .  
  
To see an example where  $IJ \subsetneq I \cap J$ , consider  $I = \langle x^2y \rangle$  and  $J = \langle xy^2 \rangle$  in  $k[x, y]$ . Then  $I \cap J = \langle x^2y^2 \rangle$  and  $IJ = \langle x^3y^3 \rangle$ . Thus  $IJ \subsetneq I \cap J$  as  $I \cap J$  contains  $x^2y^2$  and  $IJ$  does not contain  $x^2y^2$ .

□

## 1.2 Gröbner Bases

Solution:  $\langle \text{[CLO05] Ex. 1.3.11} \rangle :$





### 1.3 Affine Varieties

Solution:  $\langle \text{[CLO05] Ex. 1.4.9} \rangle :$



## Chapter 2

# Solving Polynomial Equations

### 2.1 Solving Polynomial Systems by Elimination

Solution:  $\langle\langle$  [CLO05] Ex. 2.1.1  $\rangle\rangle$  :

□

Solution:  $\langle\langle$  [CLO05] Ex. 2.1.2  $\rangle\rangle$  :

□

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

$$|\bar{z}|^n = |a_{n-1}\bar{z}^{n-1} + \dots + a_0| \leq |a_{n-1}||\bar{z}|^{n-1} + \dots + |a_0| \leq |a_{n-1}||\bar{z}|^{n-1} + \dots + |a_0||\bar{z}|^{n-1}.$$

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

Solution:  $\langle\langle$  [CLO05] Ex. 2.1.4  $\rangle\rangle$  : 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

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

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

**Solution:** << [CLO05] Ex. 2.1.6 >> : □

**Solution:** << [CLO05] Ex. 2.1.7 >> : □

**Solution:** [CLO05] Ex. 2.1.8:

- (a) Let  $\bar{z}$  be a simple root of  $p(z)$ , so  $p(\bar{z}) = 0$  but  $p'(\bar{z}) \neq 0$ . 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

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

where  $B$  is the value from [CLO05] Ex. 2.1.3 and  $\text{LC}(p)$  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

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

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

- (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

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

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  $\bar{z}_1, \dots, \bar{z}_k$  with multiplicities  $m_1, \dots, m_k \geq 1$ , then  $\gcd(p(z), p'(z)) = (z - \bar{z}_1)^{m_1} \dots (z - \bar{z}_k)^{m_k}$ . 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.

□

**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

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

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

□

## 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  $r(x_i) = f(x_i) - q(x_i)p_i(x_i) \in I$  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  $\{1, [x_i], \dots, [x_i^{m_i}]\}$  is linearly dependent in  $k[\bar{x}]/I$ . In fact, we may use the Finiteness Theorem to set  $m_i$  to the smallest integer such that  $x_i^{m_i} = \text{LT}(g)$  for some  $g \in G$ . Since  $k[x_1, \dots, x_n]/I$  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  $(x - \bar{z})$  of  $p(x)$  divides  $f(x)^m$  and so divides  $f(x)$  as  $(x - \bar{z})$  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  $\bar{z}_1, \dots, \bar{z}_r$ , each  $\bar{z}_i \in \bar{k}$ . Then for each  $i$ ,  $(x - \bar{z}_i) \mid f(x)$ . Let  $m_i$  be the multiplicity of  $z_i$  in  $p(x)$  and  $m = \max\{m_1, \dots, m_r\}$ . 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:**  $\langle \langle \text{[CLO05] Ex. 2.2.5} \rangle \rangle$  : 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

$$y^4x + 3x^3 - y^4 - 3x^2 = y^4(x-1) + 3x^2(x-1) = (y^4 + 3x^2)(x-1)$$

$$x^2y - 2x^2 = x^2(y-2)$$

$$2y^4x - x^3 - 2y^4 + x^2 = 2y^4(x-1) - x^2(x-1) = (2y^4 - x^2)(x-1).$$

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  $V(\sqrt{I}) = V(I)$ .  $\square$

**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 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.  $\square$

**Solution:** [CLO05] Ex. 2.2.7: We implement the algorithm described in  $\langle \langle \text{[CLO05] Ex. 1.3.11} \rangle \rangle$ . See /code/ch2/2\_2\_7.sage for the code in action.  $\square$

**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.  $\square$

**Solution: [CLO05] Ex. 2.2.9:**

- (a) Let  $f(\bar{x}) \in I + \langle p \rangle$  and let  $1 \leq j \leq d$ . Then  $f(\bar{x}) = g(\bar{x}) + h(\bar{x})p(x_1)$  for some  $g(\bar{x}) \in I$  and  $h(\bar{x}) \in k[\bar{x}]$ . We have that  $(x_1 - a_j) \mid p(x_1)$  and so  $h(\bar{x})p(x_1) \in \langle x_1 - a_j \rangle$ . Thus,  $f(\bar{x}) = g(\bar{x}) + h(\bar{x})p(x_1) \in I + \langle x_1 - a_j \rangle$ . As  $j$  was arbitrary, we have that  $f(\bar{x}) \in \bigcap_j (I + \langle x_1 - a_j \rangle)$ .
- (b) Let  $f(\bar{x}) \in p_j \cdot (I + \langle x_1 - a_j \rangle)$ . Then  $f(\bar{x}) = p_j(x_1) \cdot (g(\bar{x}) + h(\bar{x})(x_1 - a_j))$  for some  $g(\bar{x}) \in I$  and  $h(\bar{x}) \in k[\bar{x}]$ . We have that  $p_j(x_1)g(\bar{x}) \in I$  and  $p_j(x_1)h(\bar{x})(x_1 - a_j) = h(\bar{x})p(x_1) \in \langle p \rangle$ . Thus,  $f(\bar{x}) = p_j(x_1)g(\bar{x}) + h(\bar{x})p(x_1) \in I + \langle p \rangle$ .
- (c) Let  $d = \gcd(p_1, \dots, p_d)$ . 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  $c \leq d$  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  $k[\bar{x}]$  and  $p_i$  and  $p_j$  are coprime. By Bezout's Lemma, there exists polynomials  $h_1, \dots, h_d \in k[\bar{x}]$  such that  $1 = \sum_{j=1}^d h_j(\bar{x})p_j(x_1)$ .
- (d) Now let  $h(\bar{x}) \in \bigcap_{j=1}^d (I + \langle x_1 - a_j \rangle)$ . As all the  $p_j$  are coprime, we have that there exist polynomials  $h_1, \dots, h_d \in k[\bar{x}]$  such that  $1 = \sum_{j=1}^d h_j(\bar{x})p_j(x_1)$ . Thus,  $h = \sum_{j=1}^d h_j(\bar{x})p_j(x_1)h(\bar{x})$ . Then for all  $1 \leq j \leq d$ , we have that as  $p_j(x_1)h(\bar{x}) \in p_j \cdot (I + \langle x_1 - a_j \rangle) \subseteq I + \langle p \rangle$ . Thus, each summand of  $\sum_{j=1}^d h_j(\bar{x})p_j(x_1)h(\bar{x})$  is in  $I + \langle p \rangle$  and so overall  $h \in I + \langle p \rangle$ .

□

**Solution: [CLO05] Ex. 2.2.10:**

- (a) Let  $\bar{f}^G = \sum_{j=1}^d c_j(f)x^{\alpha(j)}$  and  $\bar{g}^G = \sum_{j=1}^d c_j(g)x^{\alpha(j)}$ . Then by combining like terms, we have that  $\bar{f}^G + \bar{g}^G = \sum_{j=1}^d (c_j(f) + c_j(g))x^{\alpha(j)}$ . On the other hand, we have that  $\overline{f+g}^G = \sum_{j=1}^d c_j(f+g)x^{\alpha(j)}$ . Since  $\bar{f}^G + \bar{g}^G = \overline{f+g}^G$  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  $\overline{\lambda f}^G = \lambda \bar{f}^G$  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  $A \rightarrow k$ .
- (b) Let  $\alpha_j \in A^*$  be the linear map  $\alpha_j(f) = c_j(f)$ . Notice that for all  $1 \leq i, j \leq d$  we have that  $\alpha_j(x^{\alpha(i)}) = c_j(x^{\alpha(i)}) = \delta_{i,j}$ . Suppose there exists  $\lambda_1, \dots, \lambda_d \in k$  such that  $\lambda_1 \alpha_1 + \dots + \lambda_d \alpha_d = 0$ . Then for all  $1 \leq i \leq d$  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  $1 \leq i \leq d$ ,  $\lambda_i = 0$  meaning that  $\{\alpha_1, \dots, \alpha_d\}$  is linearly independent. Since we know that  $d = \dim A = \dim A^*$ , we have that  $\{\alpha_1, \dots, \alpha_d\}$  is a basis for  $A^*$ .

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

□



**Solution: [CLO05] Ex. 2.2.11:**

- (a) We want a linear polynomial  $\ell(\bar{x}) = \ell_1 x_1 + \cdots + \ell_n x_n$  takes distinct values at each of the  $p_i \in \mathbb{C}^n$ . Consider the space of all such  $(\ell_1, \dots, \ell_n)$ . This itself is a  $\mathbb{C}$  vector space, call it  $L$ . Let  $L_{i,j}$  be the subspace of  $L$  corresponding to polynomials  $\ell(\bar{x})$  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  $(\ell_1, \dots, \ell_n) \in L \setminus \bigcup_{1 \leq i \neq j \leq m} L_{i,j}$  such that  $\ell(\bar{x}) = \ell_1 x_1 + \cdots + \ell_n x_n$  takes distinct values at each of the  $p_i$ .

**<< Can we do this constructively? >>**

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

$$g_i(\bar{x}) = \frac{\prod_{1 \leq i \neq j \leq m} \ell(\bar{x}) - \ell(\bar{p}_j)}{\prod_{1 \leq i \neq j \leq m} \ell(\bar{p}_i) - \ell(\bar{p}_j)}.$$

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  $[f] = [g] \in \mathbb{C}[\bar{x}]/I$  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  $[f], [g] \in \mathbb{C}[\bar{x}]/I$ . Then we have

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

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

- (c) We have that  $\varphi$  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. 2.3.1: 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  $\bar{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} > x_1^a$  if and only if  $\alpha_1 > a_1$  which is equivalent to saying that  $x_1^{\alpha_1} \mid x_1^a \mid \bar{x}^\alpha$   $\square$

# Bibliography

- [CLO05] D.A. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Springer-Verlag, 2005. ISBN: 0387207066. DOI: [10.1007/b138611](https://doi.org/10.1007/b138611). URL: <http://dx.doi.org/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. URL: <https://books.google.com/books?id=yL7yCAAQBAJ>.
- [Str08] Bernd Strumfels. *Algorithms in Invariant Theory*. Springer Vienna, 2008. ISBN: 9783211774175. DOI: [10.1007/978-3-211-77417-5](https://doi.org/10.1007/978-3-211-77417-5). URL: <http://dx.doi.org/10.1007/978-3-211-77417-5>.