

# Using Algebraic Geometry

With 0 Figures

Anakin Dey

Last Edited on 7/29/24 at 11:01

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Polynomials and Ideals . . . . .	1

# 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

**Exercise 1.1 (CLO05 1.1.1):**

- (a) Show that  $x^2 \in \langle x - y^2, xy \rangle$  in  $k[x, y]$ .
- (b) Show that  $\langle x - y^2, xy, y^2 \rangle = \langle x, y^2 \rangle$ .
- (c) Is  $\langle x - y^2, xy \rangle = \langle x^2, xy \rangle$ ? Why or why not?

**Proof:**

- (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.

□

**Exercise 1.2 (CLO05 1.1.2):**

Show that  $\langle f_1, \dots, f_s \rangle$  is closed under sums in  $k[x_1, \dots, x_n]$ . Also show that if  $f \in \langle f_1, \dots, f_s \rangle$  and  $p \in k[x_1, \dots, x_n]$  then  $p \cdot f \in \langle f_1, \dots, f_s \rangle$ .

**Proof:**

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  $p \cdot f = p \sum_{i=1}^s p_i f_i = \sum_{i=1}^s (p \cdot p_i) \cdot f_i$  which shows that  $\langle f_1, \dots, f_s \rangle$  is an ideal.  $\square$

**Exercise 1.3 (CLO05 1.1.3):**

Show that  $\langle f_1, \dots, f_s \rangle$  is the smallest ideal containing  $\{f_1, \dots, f_s\}$ .

**Proof:**

We already know that  $\langle f_1, \dots, f_s \rangle$  is an ideal by Exercise 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,  $\langle f_1, \dots, f_s \rangle \subseteq J$ .  $\square$

**Exercise 1.4 (CLO05 1.1.4):**

Using Exercise 1.3, formulate and prove a general criterion for the equality of  $I = \langle f_1, \dots, f_s \rangle$  and  $J = \langle g_1, \dots, g_t \rangle$ .

**Proof:**

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 Exercise 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 Exercise 1.1 (b).  $\square$

**Exercise 1.5 (CLO05 1.1.5):**

Show that  $\langle y - x^2, z - x^3 \rangle = \langle y - x^2, z - xy \rangle$  in  $\mathbb{Q}[x, y, z]$ .

**Proof:**

It suffices to show that  $z - x^3 \in \langle y - x^2, z - xy \rangle$  and  $z - xy \in \langle y - x^2, z - x^3 \rangle$ . Indeed we have that  $(z - xy) + x(y - x^2) = z - x^3$  which also yields that  $z - xy = z - x^3 - x(y - x^2)$ .  $\square$

**Exercise 1.6 (CLO05 1.1.6):**

Show that every ideal  $I \subseteq k[x]$  is generated by a single polynomial.

**Proof:**

If  $I = \{0\}$  then  $I = \langle 0 \rangle$ . So suppose  $I \neq 0$ . Let  $d \in I$  be of minimal degree.  **$\langle d = \gcd(I) \rangle$  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  $0 \leq \deg(r) < \deg(d)$ . 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  $\langle d \rangle = I$ .  $\square$

**Exercise 1.7 (CLO05 1.1.7):**

- (a) Show that  $\sqrt{\langle x^n \rangle} = \langle x \rangle$  in  $k[x]$ .
- (b) If  $p(x) = (x - a_1)^{e_1} \cdots (x - a_m)^{e_m}$ , find  $\sqrt{\langle p(x) \rangle}$ .
- (c) Let  $k = \mathbb{C}$ . What are the radical ideals in  $\sqrt{\mathbb{C}[x]}$ ?

**Proof:**

- (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  $a_1, \dots, a_m \in \mathbb{C}$ .  $\square$

**Exercise 1.8 (CLO05 1.1.8):**

- (a) Show that a prime ideal is radical.
- (b) What are the prime ideals in  $\mathbb{C}[x]$ ? What about the prime ideals in  $\mathbb{R}[x]$  or  $\mathbb{Q}[x]$ ?

**Proof:**

- (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  $\mathbb{Q}[x]$ ? >>**

□

**Exercise 1.9 (CLO05 1.1.9):**

- (a) Show that  $\langle x_1, \dots, x_n \rangle$  is maximal in  $k[x_1, \dots, x_n]$ .
- (b) Show that for any point  $(a_1, \dots, a_n) \in k^n$  that  $\langle x_1 - a_1, \dots, x_n - a_n \rangle$  is maximal in  $k[x_1, \dots, x_n]$ .
- (c) Show that  $\langle x^2 + 1 \rangle$  is maximal in  $\mathbb{R}[x]$ . Is  $\langle x^2 + 1 \rangle$  maximal in  $\mathbb{C}[x]$ ?

**Proof:**

- (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  $\text{ev}_{\vec{a}}: k[x_1, \dots, x_n] \rightarrow k$  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,  $\text{ev}_{\vec{a}}(f) = f(a_1, \dots, a_n) = 0$  if and only if  $f(x_1, \dots, x_n) \in I$ . Thus,  $\ker(\text{ev}_{\vec{a}}) = I$  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  $\langle x^2 + 1 \rangle \subsetneq \langle x - i \rangle \subsetneq \mathbb{C}[x]$ .

□



**Exercise 1.10 (CLO05 1.1.10):**

- (a) Let  $I = \langle x^2 + y^2, x^2 - z^3 \rangle \subseteq k[x, y, z]$ . Show that  $y^2 + z^3$  is in the first elimination ideal with respect to the ordering  $x > y > z$ .
- (b) Show that if  $I$  is an ideal in  $k[x_1, \dots, x_n]$  then for all  $\ell \geq 1$ ,  $I_\ell$  is an ideal in  $k[x_{\ell+1}, \dots, x_n]$ .

**Proof:**

- (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.

□

**Exercise 1.11 (CLO05 1.1.11):**

Let  $I, J$  be ideals in  $k[\bar{x}]$ .

- (a) Show that  $I + J$  is an ideal.
- (b) Show that  $I + J$  is the smallest ideal containing  $I \cup J$ .
- (c) If  $I = \langle f_1, \dots, f_s \rangle$  and  $J = \langle g_1, \dots, g_t \rangle$ , what is a finite generating set of  $I + J$ ?

**Proof:**

- (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.

□

**Exercise 1.12 (CLO05 1.1.12):**

Let  $I, J$  be ideals in  $k[\bar{x}]$ .

- (a) Show that  $I \cap J$  is an ideal.

(b) Show that  $IJ \subseteq I \cap J$ . Give an example where  $IJ \subsetneq I \cap J$ .

**Proof:**

(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  $x^2y^2$ .

□

# 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>.