Algebraic Curves

With 0 Figures

Anakin Dey

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

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. As such, I've been primarily looking at *Ideals, Varieties, and Algorithms* [CLO15], I've been doing a bunch of problems from *Ideals, Varieties, and Algorithms* [CLO15], *Using Algebraic Geometry* [CLO05] and stealing glances at Sturmfel's *Algorithms in Invariant Theory* [Str08]. However, this book is such a classic and I'm of the opinion that you can never know too much about curves and varieties. To put my money where my mouth is, I've started to TEX up some exercises from Fulton's *Algebraic Curves* [Ful08].

Chapter 1

Affine Algebraic Sets

1.1 Algebraic Preliminaries

Solution: [Ful08] Ex. 1.1: As normal, we denote a monomial $x_1^{i_1}\cdots x_n^{i_n}$ as $\overline{x}^I$ where $|I| = i_1+\cdots+i_n = d \in \mathbb{N}$ and $I \in \mathbb{N}^n$. Thus, if $f(x_1,\ldots,x_n), g(x_1,\ldots,x_n) \in R[x_1,\ldots,x_n]$ are forms of degree r and s respectively, we have that

$$f(x_1,\ldots,x_n) = \sum_{I\in\mathbb{N}^n,|I|=r} f_I\overline{x}^I,$$
$$g(x_1,\ldots,x_n) = \sum_{J\in\mathbb{N}^n,|J|=s} g_J\overline{x}^J.$$

Then, we have by distribution that

$$f(x_1,\ldots,x_n)\cdot g(x_1,\ldots,x_n) = \sum_{\substack{I\in\mathbb{N}^n,|I|=r\\ J\in\mathbb{N}^n,|J|=s}} f_I\overline{x}^I g_J\overline{x}^J.$$

For each I,J we have that if $f_I, g_J \neq 0$ then $f_I g_J \overline{x}^I\overline{x}^J = (fg)_{I,J}\overline{x}^{I+J}$ where $(fg)_{I,J} = (fg)_{I,J} = f_I g_J$ Notice that $|I+J| = r+s$ by coordinatewise addition and so each term is either 0 or a degree $r+s$ homogeneous form. Thus after combining like terms, we have that $f(x_1,\ldots,x_N)\cdot g(x_1,\ldots,x_n)$ is either degree 0 or a degree $r+s$ homogeneous form. As 0 has any degree we choose, we have that $f\cdot g$ is a degree $r+s$ form.

If we wanted to show that the product of two nonzero polynomials is still nonzero, it can be shown that R a domain implies $R[x_1,\ldots,x_n]$ is a domain. This can be seen by looking at leading terms and inducting on the number of variables. □

Solution: [Ful08] Ex. 1.2: The expression of $z \in K = \text{Frac}(R)$ as $z = \frac{a}{b}$ for some $a \in R, b \in R$ such that a, b have no common factors, is obvious as we only consider finite sums so we can always take common denominators. Suppose that $z = \frac{a}{b} = \frac{a'}{b'}$ two different representatives. Since R is a UFD, say that $a = u_a a_1 \cdots a_{n_a}$ and $a' = u_{a'} a'_1 \cdots a'_{n_{a'}}$ are factorizations of a and a'. We have similar factorizations for b and b'. Then we have that $ab' = a'b \in R$. However, as R is a unique factorization domain, we must have

$$u_a a_1 \cdots a_{n_a} u_{b'} b'_1 \cdots b'_{n_{b'}} = u_{a'} a'_1 \cdots a'_{n_{a'}} u_b b_1 \cdots b_{n_b}$$

are two equivalent factorizations up to unit. This implies that $\frac{a}{b}$ and $\frac{a'}{b'}$ differ only up to unit. □

Solution: [Ful08] Ex. 1.3:

(a) We know that $P = (p)$ for some nonzero, nonunital $p \in R$. Suppose that p was reducible, so $p = ab$ for some nonzero nonunital $a, b \in R$. Then as $p \nmid a$ and $p \nmid b$, since such divisibility would imply that a or b were equal to p up to unit, we have that $a, b \notin (p)$. But then we have elements $a, b \in R$ such that $a \notin (p)$, $b \notin (p)$ but $ab = p \in (p)$ which contradicts the primality of $P = (p)$. Then p is irreducible.

(b) We show that $P = (p)$ is maximal. There exists a maximal ideal $M = (m)$ such that $(p) \subseteq (m)$. Thus, $p \mid m$. Notice that by **(a)** that both p and m are irreducible elements of R. As such, if $p \mid m$ we must have that $m \mid p$ as if not, m would be reducible. Thus, $p = um$ for some unit $u \in R^\times$. Thus, $(p) = (m)$ and $P = (p)$ is maximal.

□

Solution: [Ful08] Ex. 1.4: We prove by induction on the number of variables n. If $n = 1$ then any nonzero polynomial of degree d has at most d distinct zeros. Thus if $F(x) \in k[x]$ is a nonzero polynomial, there exists a $z \in k$ such that $F(z) \neq 0$. Now let $n \geq 1$. Let $F(x_1, \ldots, x_n, y) \in k[x_1, \ldots, x_n, y]$ be a nonzero polynomial. Letting $d = \deg_y(F)$, we can find $F_0[x_1, \ldots, x_n], \ldots, F_d[x_1, \ldots, x_n]$ such that

$$F(x_1, \ldots, x_n, y) = \sum_{i=0}^{d} F_i(x_1, \ldots, x_n) \cdot y^i.$$

Regard $F(x_1, \ldots, x_n, y)$ as a nonzero polynomial $g(y)$ in $F(x_1, \ldots, x_n)[y]$. As k is infinite and $g(y)$ is nonzero, then we must have there exists $z_y \in k$ such that $g(z_y) \neq 0$. Thus, we have that $F(x_1, \ldots, x_n, z_y) \in k[x_1, \ldots, x_n]$ is nonzero. By induction, there exists $(z_1, \ldots, z_n) \in k^n$ such that $F(z_1, \ldots, z_n, z_y) \neq 0$. □

Solution: [Ful08] Ex. 1.5: This is Euclid's proof of there being infinitely many primes. Omitted. □

Solution: [Ful08] Ex. 1.6: Let k be an algebraically closed field. Then the irreducible monic polynomials of $k[x]$ are of the form $(x-a)$ for each $a \in k$. Thus, they are in bijection with the elements of k. By [Ful08] Ex. 1.5, there are infinitely many monic irreducible polynomials over any field. Thus, k is an infinite field. □

Solution: [Ful08] Ex. 1.7:

(a) Let $F(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$. Then we may express $F(x_1, \ldots, x_n)$ as

$$F(x_1, \ldots, x_n) = \sum_{I=(i_1,\ldots,i_n)\in\mathbb{N}^n} \lambda_I (x_1)^{i_1} \cdots (x_n)^{i_n} = \sum_{I=(i_1,\ldots,i_n)\in\mathbb{N}^n} \lambda_I ((x_1 - a_1) + a_1)^{i_1} \cdots ((x_n - a_n) + a_n)^{i_n}.$$

Expanding and combining like terms yields the desired results.

(b) Suppose $F(a_1, \ldots, a_n) = 0$. By **(a)**, we may express $F(x_1, \ldots, x_n)$ as

$$F(x_1, \ldots, x_n) = \sum_{I=(i_1,\ldots,i_n)\in\mathbb{N}^n} \lambda_I (x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n}$$

The claim says that this expression has no constant term, i.e. $\lambda_{\overline{0}} = 0$. This is immediate as the constant term corresponds to $F(a_1, \ldots, a_n) = 0$.

□

1.2 Affine Space and Algebraic Sets

Solution: [Ful08] Ex. 1.8: This corresponds to the fact that any nonzero univariate polynomial has finitely many zeroes and the zero polynomial vanishes everywhere by definition. □

Solution: [Ful08] Ex. 1.14: □

Solution: [Ful08] Ex. 1.15: Let $V = \mathbf{V}(I)$ for some ideal $I \subseteq k[\overline{x}]$ and $W = \mathbf{V}(J)$ for some ideal $J \subseteq k[\overline{y}]$. We may consider $I, J \subseteq k[\overline{x}, \overline{y}]$ as well by identifying I with $\langle I \rangle$ where we generated the ideal over $k[\overline{x}, \overline{y}]$ and do similarly for J. $\langle\langle$ **It is clear** $\rangle\rangle$ that $V \times W = \langle I \cup J \rangle \subseteq k[\overline{x}, \overline{y}]$. □

1.3 The Ideal of a Set of Points

Solution: [Ful08] Ex. 1.16: This follows immediately from the fact that $V \subseteq W \implies \mathbf{I}(V) \supseteq \mathbf{I}(W)$. □

Solution: [Ful08] Ex. 1.17:

(a) Note that as single points are algebraic sets, and the union of two algebraic sets is algebraic, $V \cup \{\overline{P}\}$ is algebraic. Since $V \subsetneq V \cup \{\overline{P}\}$, we have that $\mathbf{I}(V) \supsetneq \mathbf{I}(V \cup \{\overline{P}\})$ by [Ful08] Ex. 1.16. Let $\tilde{F}(\overline{x}) \in \mathbf{I}(V) \setminus \mathbf{I}(V \cup \{\overline{P}\})$. Then $\tilde{F}(\overline{z}) = 0$ for all $\overline{z} \in \mathbf{I}(V)$ but $\tilde{F}(\overline{P}) = c$ for some $c \in k^\times$. Then $F(\overline{x}) := \frac{\tilde{F}(\overline{x})}{c}$ is 0 on V but $F(\overline{P}) = 0$.

(b) Let $U = V \cup \{\overline{P}_1, \ldots, \overline{P}_r\}$ and for $1 \leq i \leq r$ let $U_i = U \setminus \{\overline{P}_i\}$. These are algebraic sets still. Let $F_i(\overline{x})$ be the polynomial given by **(a)** for each $U_i \subsetneq U$. As $V \subseteq U_i$ for each i and each $F_i(\overline{x}) \in \mathbf{I}(U_i)$, we have that $F_i(\overline{x}) \in \mathbf{I}(V)$.

(c) Let $\overline{P}_1, \ldots, \overline{P}_r$, V, and $F_1, \ldots, F_r$ be as in **(b)**. For $1 \leq i \leq r$, let $G_i(\overline{x}) = \sum_{k=1}^{r} a_{i,k} F_k(\overline{x})$. Then

$$G_i(\overline{P}_j) = \sum_{k=1}^{r} a_{i,k} F_k(\overline{P}_j) = a_{i,j} F_j(\overline{P}_j) = a_{i,j}.$$

Finally, as each $F_i(\overline{x}) \in \mathbf{I}(V)$, an ideal, we have that each $G_i \in \mathbf{I}(V)$.

□

Solution: [Ful08] Ex. 1.18: ⟨⟨ Meh I know how to do this. ⟩⟩ □

Solution: [Ful08] Ex. 1.20: As $I \subseteq \sqrt{I}$ we have that $\mathbf{V}(\sqrt{I}) \subseteq \mathbf{V}(I)$ always. Let $\overline{z} \in \mathbf{V}(I)$ and let $p(\overline{x}) \in \sqrt{I}$ such that $p^n(\overline{x}) \in I$. Then $p^n(\overline{z}) = 0$ which implies, as k is a field, that $p(\overline{z}) = 0$. Thus, $\overline{z} \in \mathbf{V}(\sqrt{I})$.

Now let $p(\overline{x}) \in \sqrt{I}$ such that $p^n(\overline{x}) \in I$ and let $\overline{z} \in \mathbf{V}(I)$. Then again, $p^n(\overline{z}) = 0$ which implies that $p(\overline{z}) = 0$. Then $p(\overline{z}) \in \mathbf{I}(\mathbf{V}(I))$. □

Solution: [Ful08] Ex. 1.21: ⟨⟨ Meh I know how to do this. ⟩⟩ □

1.4 The Hilbert Basis Theorem

Solution: [Ful08] Ex. 1.22:

(a) ⟨⟨ **Meh I know how to do this.** ⟩⟩

(b) We prove first that J' is radical if and only if J is radical. Suppose that $J' = \sqrt{J'}$ is radical. We automatically have $J \subseteq \sqrt{J}$ so let $f \in \sqrt{J}$. Then $\exists n > 0$ such that $f^n \in J$. Thus, $\pi(f)^n = \pi(f^n) \in J'$ meaning that $\pi(f) \in \sqrt{J'} = J'$. Thus, $f \in \pi^{-1}(J') = J$. Suppose that $J = \sqrt{J}$ is radical. We again have $J' \subseteq \sqrt{J'}$ so let $f \in \sqrt{J'}$. Then $\exists n > 0$ such that $f^n \in J'$. As π is surjective, there exists $a \in J$ such that $\pi(a) = f^n$ and $\pi(b) = f$. We have that

$$\pi(a) = f^n = \pi(b)^n = \pi(b^n)$$

and so $a - b^n \in \ker(pi) = I \subseteq J$. Since $a \in J$, we have that $b^n \in J = \sqrt{J}$ meaning that $b \in \sqrt{J}$. Thus, $f = \pi(b) \in \pi(\sqrt{J}) = \pi(J) = J'$.

Now we prove that J is prime if and only if J' is prime. Suppose that J' is prime and let $a, b \in R$ such that $ab \in J$. Then $\pi(a)\pi(b) \in J' \implies \pi(a)$ or $\pi(b) \in J'$, say $\pi(a)$. Since $\pi(a) \in J'$ we have that $a \in J$. Now suppose that J is prime and let $a', b' \in R/I$ such that $a'b' \in J'$. Then $\exists a, b \in R$ such that $\pi(a) = a'$ and $\pi(b) = b'$. Thus, $\pi(ab) \in J'$ meaning that $ab \in J$ and so either $a \in J$ or $b \in J$, say a. Thus, $\pi(a) = a' \in J'$.

Now we prove that J is maximal if and only if J' is maximal. Suppose that J' is maximal and let K be an ideal such that $J \subseteq K \subseteq R$. Then $\pi(J) = J' \subseteq \pi(K) \subseteq R/I$. If $\pi(K) = R/I$, then $1 \in \pi(K) \implies 1 \in K$ and so $K = R$. Otherwise, if $\pi(K) \neq R/I$ we must have that $J' = \pi(K)$ by maximality which implies that $J = K$. Now suppose that J is maximal and let K' be an ideal such that $J' \subseteq K' \subseteq R/I$. Then $\pi^{-1}(J') = J \subseteq \pi^{-1}(K) \subseteq R$. If $\pi^{-1}(K) = R$, then we must have that $1 \in \pi^{-1}(J) \implies 1 \in K'$ and so $K' = R/I$. Otherwise, by maximality we must have that $J = \pi^{-1}(K')$ which implies that $J' = K'$.

□

1.5 Irreducible Components of an Algebraic Set

Solution: [Ful08] Ex. 1.29: Note that $k[x_1, \ldots, x_n]$ is a domain, so that (0) is prime. As $\mathbb{A}_k^n = \mathbf{V}(0)$, we have that $\mathbb{A}_k^n$ is prime. □

1.6 Algebraic Subsets of the Plane

Solution: [Ful08] Ex. 1.30:

(a) Suppose there was $(x, y) \in \mathbb{A}^2_{\mathbb{R}}$ such that $x^2 + y^2 + 1 = 0$. Then we would have that $-1 = x^2 + y^2 \geq 0$, a contradiction.

(b) Let $V \subseteq \mathbb{A}^2_{\mathbb{R}}$ be an algebraic set, $V = \mathbf{V}(I)$ for some $I \leq \mathbb{R}[x, y]$. Since $\mathbb{R}$ is Noetherian as it is a field, $\mathbb{R}[x, y]$ is Noetherian and so there exists $f_1, \ldots, f_r \in \mathbb{R}[x, y]$ such that $I = \langle f_1, \ldots, f_n \rangle$. Consider $f = f_1^2 + \cdots + f_r^2$. Clearly $V = \mathbf{V}(f_1, \ldots, f_r) \subseteq \mathbf{V}(f)$. Now suppose that $(a, b) \notin V$. Then there exists f_i such that $f_i(a, b) \neq 0$. Thus, we have that

$$f(a, b) = f_1^2(a, b) + \cdots + f_r^2(a, b) \geq f_i^2(a, b) > 0$$

and so $(a, b) \notin \mathbf{V}(f)$. Thus, $V = \mathbf{V}(f)$.

□

Bibliography

[CLO05] D.A. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Springer-Verlag, 2005. ISBN: 0387207066. DOI: 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=yL7yCAAAQBAJ.

[Ful08] W. Fulton. *Algebraic Curves: An Introduction to Algebraic Geometry*. 3rd ed. 2008.

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