Project Sigma

Algebraic Geometry

Reference & Exercise

Yunhai Xiang

May 25, 2021

Contents

Chapter 1

Affine Algebraic Sets

Problem 1.0.1. List all points in $V = \mathcal{V}(\{Y - X^2, X - Y^2\})$.

Proof. Since $V = \{(x, y) : y = x^2, x = y^2\}$, we have $x = y^2 = (x^2)^2 = x^4$ if $(x, y) \in V$. By solving $x^4 - x = 0$ we have that $x \in \{0, 1, w, w^2\}$ where $w = e^{2\pi i/3}$. If $x = 0$, then $y = 0$, if $x = 1$ then $y = 1$. We can easily verify that $y = x^2$ and $x = y^2$ in these cases. If $x = w$ then $y = x^2 = w^2$, then we can verify $x = w = w^4 = y^2$. If $x = w^2$, then $y = x^2 = w^4 = w$, and we can verify $x = w^2 = y^2$. Therefore $V = \{(0, 0), (1, 1), (w, w^2), (w^2, w)\}$. $\square$

Problem 1.0.2. Show that $W = \{(t, t^2, t^3) : t \in \mathbf{C}\}$ is an algebraic set.

Proof. Consider $V = \mathcal{V}(\{Y - X^2, Z - X^3\})$. For $(x, y, z) \in V$, we have $y - x^2 = 0$ and $z - x^3 = 0$, so $y = x^2$ and $z = x^3$, therefore $(x, y, z) = (x, x^2, x^3) \in W$. Conversely, let $(x, y, z) = (t, t^2, t^3) \in W$, then $y - x^2 = t^2 - t^2 = 0$ and $z - x^3 = t^3 - t^3 = 0$, hence $(x, y, z) \in V$. Thus $V = W$. $\square$

Problem 1.0.3. Suppose that C is an affine plane curve and L is a line with $L \not\subseteq C$. Suppose that $C = \mathcal{V}(\{F\})$ where $F \in \mathbf{C}[X, Y]$ a polynomial of degree n. Show that $L \cap C$ is a finite set of no more than n points.

Proof. Suppose that $(x, y) \in L \cap C$, since L is a line, we have $y = mx + c$ for some m, c, therefore $F(x, mx + c) = 0$. We note that $\deg F(x, mx + c) \leq n$ since $mx + c$ has degree 1. By the fundamental theorem of algebra, we have $F(x, mx + c) = 0$ has at most n solutions. Hence $L \cap C$ is a finite set of no more than n points. $\square$

Problem 1.0.4. Show that $\mathcal{V}((Y - X^2))$ is irreducible, and that $\mathcal{I}(\mathcal{V}((Y - X^2))) = (Y - X^2)$.

Proof. We will show that $(Y - X^2)$ is prime. Consider $\varphi : \mathbf{C}[X, Y] \to \mathbf{C}[X]$ given by $X \mapsto X$ and $Y \mapsto X^2$ extended to the whole ring, then φ is a homomorphism and $\mathrm{Ker}(\varphi) = (Y - X^2)$. Hence by the first isomorphism theorem, we have $\mathbf{C}[X, Y]/(Y - X^2) \cong \mathbf{C}[X]$ is an integral domain, hence $(Y - X^2)$ is prime. Since prime ideals are radical ideals, we have $\mathcal{I}(\mathcal{V}((Y - X^2))) = (Y - X^2)$. $\square$

Problem 1.0.5. Let $I = (Y^2 - X^3 - X^2, X)$, then $X \in I$ since it is a generator, hence $X^2, X^3 \in I$ as well. Next, $Y^2 - X^3 - X^2 \in I$ since it is a generator, therefore, $Y^2 - X^3 - X^2 + X^3 + X^2 = Y^2 \in I$. Assume for sake of contradiction that I is a radical ideal, then $Y \in I$ since $Y^2 \in I$. Since $Y \in I$, we have $Y = U(X, Y)(Y^2 - X^3 - X^2) + V(X, Y)X$ for some polynomials $U(X, Y), V(X, Y)$. Let $X = 0$ on both sides, then we have $Y = U(0, Y)Y^2$ as polynomials in the indeterminant Y. This is a contradiction since the dergee of Y on the LHS is 1 and the degree of Y on the RHS is not 1. Since I is not a radical ideal, and $\mathcal{I}(D)$ must be a radical ideal, we have $\mathcal{I}(D) \neq I$.

Problem 1.0.6. Show that $\mathcal{V}(F) \cong \mathcal{V}(G)$ where $F(X,Y) = X^2 + Y^2 - 1$ and $G(X,Y) = X^2 - Y^2 - 1$.

Proof. We let $\varphi : \mathcal{V}(F) \to \mathcal{V}(G)$ be $(x,y) \mapsto (x, iy)$ which is obviously a polynomial map with an inverse $\varphi^{-1} : \mathcal{V}(G) \to \mathcal{V}(F)$ given by $(x,y) \mapsto (x, -iy)$ which is also a polynomial map. We easily verify that $\varphi(\varphi^{-1}(x,y)) = (x,y)$ and $\varphi^{-1}(\varphi(x,y)) = (x,y)$. We note that if $(x,y) \in \mathcal{V}(F)$ then $x^2 + y^2 - 1 = 0$, and we have $G(\varphi(x,y)) = x^2 - (iy)^2 - 1 = x^2 + y^2 - 1 = 0$. And if $(x,y) \in \mathcal{V}(G)$ then $x^2 - y^2 - 1 = 0$ then $F(\varphi^{-1}(x,y)) = x^2 + (-iy)^2 - 1 = x^2 - y^2 - 1 = 0$. Therefore φ, φ^{-1} are well-defined. Therefore $\mathcal{V}(F) \cong \mathcal{V}(G)$. □

Problem 1.0.7. Let $V = \mathcal{V}(Y^2 - X^3)$ and let $\phi : \mathbf{A}^1 \to V$ be $\phi(t) = (t^2, t^3)$, show that ϕ is a bijective polynomial map which is not an isomorphism.

Proof. Assume $s \neq t$ and $(t^2, t^3) = (s^2, s^3)$ then we have $s^2 = t^2$ and $s^3 = t^3$. Since $s \neq t$ we have $s - t \neq 0$. Since $s^2 = t^2$ we have $s^2 - t^2 = (s+t)(s-t) = 0$. Since $s - t \neq 0$, we have $s + t = 0$, thus $s = -t$, hence $s^3 = (-t)^3 = -t^3$. Since $s^3 = t^3$ and $s^3 = -t^3$, we have $t^3 = -t^3$, so $t = 0$. Since $t = 0$ we have $s = -t = 0 = t$ which contradicts the hypothesis that $s \neq t$. This shows that ϕ is injective. Next, for each $(x,y) \in \mathcal{V}(\{Y^2 - X^3\})$, we have $y^2 - x^3 = 0$ and thus $y^2 = x^3$. We know that x has square roots α and $-\alpha$ for some α. We show that one of them is also a cube root of y. We have $\alpha^6 = (\alpha^2)^3 = x^3 = y^2$, therefore $y = \alpha^3$ or $y = -\alpha^3$. Since $y = \alpha^3$ or $y = (-\alpha)^3$, we have one of $\pm\alpha$ is a cube root of y. Let $t = \alpha$ if α is a cube root of y and $t = -\alpha$ otherwise. We then have $\phi(t) = (t^2, t^3) = (x,y)$. Thus ϕ is surjective, hence bijective. Suppose for contradiction that there is a polynomial map inverse $\phi^{-1} : V \to \mathbf{A}^1$ which can be represented by a polynomial $f \in \mathbf{C}[X,Y]$. Then have $\phi^{-1}(\phi(t)) = t$, so $f(t^2, t^3) = t$. We note that $[t^1]f(t^2, t^3) = 0$, since for each term aX^nY^m, substituding $X = t^2$ and $Y = t^3$ gives at^{2n+3m}, and there is no n, m with $2n + 3m = 1$. This is a contradiction since $[t^1]t = 1$. □

Problem 1.0.8. Let $\phi : \mathbf{A}^1 \to V$ be $\phi(t) = (t^2 - 1, t(t^2 - 1))$ where $V = \mathcal{V}(\{Y^2 - X^2(X+1)\})$. Show that ϕ is one-to-one and onto except at $\phi(\pm 1) = (0,0)$.

Proof. Suppose that $s \neq t$ and $(s^2 - 1, s(s^2 - 1)) = (t^2 - 1, t(t^2 - 1))$, we then have $s^2 - 1 = t^2 - 1$ thus $s^2 - t^2 = (s-t)(s+t) = 0$. Since $s \neq t$, we have $s = -t$. Next, since $s(s^2 - 1) = t(t^2 - 1)$ we have $-t(t^2 - 1) = t(t^2 - 1)$. Thus $t = 0$ or $t^2 = 1$. If $t = 0$ then $s = -t = 0 = t$ which contradicts $s \neq t$, so $t^2 = 1$. Thus $t = \pm 1$ and $s = \mp 1$. Thus ϕ is injective except at $t = \pm 1$. Next, let $(x,y) \in V$ then $y^2 - x^2(x+1) = 0$ so $y^2 = x^2(x+1)$. Let α and $-\alpha$ be the square roots of $x + 1$. By $y^2 = x^2(x+1)$, we have $y = \alpha x$ or $y = -\alpha x$. Let $t = \alpha$ if $y = \alpha x$ and $t = -\alpha$ otherwise. We thus have $y = tx$. Since t is a square root of $x + 1$, we have $t^2 = x + 1$, so $x = t^2 - 1$. Thus $x = t^2 - 1$ and $y = t(t^2 - 1)$. Hence $\phi(t) = (x,y)$. Thus ϕ is surjective. □

Problem 1.0.9. Let $V = \mathcal{V}(\{X^2 - Y^3, Y^2 - Z^3\})$, and let $\overline{\alpha} : \Gamma(V) \to \mathbf{C}[T]$ be given by $\overline{\alpha}(X) = T^9$, $\overline{\alpha}(Y) = T^6$ and $\overline{\alpha}(Z) = T^6$. Then

(a) What is the polynomial map $f : \mathbf{A}^1 \to V$ with $f^* = \overline{\alpha}$

(b) Show that f is bijective but not an isomorphism

Proof.

(a) Define the polynomial map $f : \mathbf{A}^1 \to V$ by $f(t) = (t^9, t^6, t^4)$ as in the proof of Theorem 1.6. We can verify that this is well-defined since $X^2 - Y^3 = t^{18} - t^{18} = 0$ and $Y^2 - Z^3 = t^{12} - t^{12} = 0$. We verify that the pullback $f^*(X) = [(x, y, z) \mapsto x] \circ f = T^9$, $f^*(Y) = [(x, y, z) \mapsto y] \circ f = T^6$, and $f^*(Z) = [(x, y, z) \mapsto z] \circ f = T^4$. Thus $f^* = \overline{\alpha}$.

(b) We note that $f(t) = (0, 0, 0)$ iff $t = 0$, so we can assume $t \neq s$ are nonzero and $(t^9, t^6, t^4) = (s^9, s^6, s^4)$. Since $t^4 = s^4$, we have $t \in \{s\zeta_4, s\zeta_4^2, s\zeta_4^3\}$. Since $t^6 = s^6$, we have $t \in \{s\zeta_6, \dots, s\zeta_6^5\}$. Since $t^9 = s^9$, we have $t \in \{s\zeta_9, \dots, s\zeta_9^8\}$. Since $\gcd(9, 6, 4) = 1$, this is a contradiction. To explain in simpler language, $t^4 = s^4$ implies that the angle between t, s is $90°, 180°$ or $270°$; $t^6 = s^6$ implies that the angle between t, s is $60°, 120°, 180°, 240°$ or $300°$; $t^9 = s^9$ implies that the angle between t, s is $40°, 80°, 120°, 160°, 200°, 240°, 280°$ or $320°$. There is no angle between t, s that satisfies our requirement. Thus f is injective. Next, let $(x, y, z) \in V$, we then have $x^2 - y^3 = 0$ and $y^2 - z^3 = 0$, thus $x^2 = y^3$ and $y^2 = z^3$. The 6-th roots of y are $\{\alpha, \alpha\omega, \dots, \alpha\omega^5\}$ for some α where $\omega = e^{\frac{2\pi i}{6}}$. Let s be a 6-th roots of y. Thus $s^{18} = (s^6)^3 = y^3 = x^2$, so $x = \pm s^9$, so $x \in \{s^9, s^9\omega^3\}$. Similarly, $s^{12} = (s^6)^2 = y^2 = z^3$, therefore $\{z, z\omega^2, z\omega^4\} = \{s^4, s^4\omega^2, s^4\omega^4\}$, hence $z \in \{s^4, s^4\omega^2, s^4\omega^4\}$. Suppose that $x = s^9\omega^{3n}$ for $n \in \{0, 1\}$ and $z = s^4\omega^{2m}$ for $m \in \{0, 1, 2\}$. Let $t = s\omega^k$ then t is also a 6-th root of unity, so $y = t^6$. Also, $x = t^9\omega^{3n-9k}$ and $z = t^4\omega^{2m-4k}$. I claim that we can always choose k such that $3n \equiv 9k \pmod 6$ and $2m \equiv 4k \pmod 6$. Note that $3n \equiv 9k \pmod 6$ iff $k \equiv n \pmod 2$, and note that $2m \equiv 4k \pmod 6$ iff $k \equiv 2m \pmod 3$. By the Chinese remainder theorem, such k can always be chosen. Hence we have $x = t^9$, $y = t^6$ and $z = t^4$. Thus $f(t) = (x, y, z)$. Thus f is surjective, so f is bijective.

We see that f is not an isomorphism, since if so there is a polynomial map $g : V \to \mathbf{A}^1$ which can be viewed as a polynomial $g \in \mathbf{C}[X, Y, Z]$ which is the inverse of f, then by $g \circ f = \mathrm{id}$, we have $g(t^9, t^6, t^4) = t$. We note that $[t^1]g(t^9, t^6, t^4) = 0$ since if $aX^pY^qZ^r$ is a term in $g(X, Y, Z)$, then substituding $X = t^9, Y = t^6, Z = t^4$ gives $at^{9p+6q+4r}$, and there is no p, q, r such that $9p + 6q + 4r = 1$. This contradicts the fact that $[t^1]t = 1$.

□

Problem 1.0.10. If $\phi : V \subseteq \mathbf{A}^n \to W \subseteq \mathbf{A}^m$ is an onto polynomial map, show that if X is an algebraic subset of W then $\phi^{-1}[X]$ is an algebraic subset of V, and that X is irreducible if $\phi^{-1}[X]$ is irreducible.

Proof. Suppose that $X = \mathcal{V}(I)$ for some $I \subseteq \mathbf{C}[X_1, \dots, X_m]$, then for $x \in V$, we have

$$x \in \phi^{-1}[X] \iff \phi(x) \in X \iff f(\phi(x)) = 0, \forall f \in I \iff x \in \mathcal{V}(\{f \circ \phi : f \in I\})$$

Therefore $\phi^{-1}[X] = \mathcal{V}(\{f \circ \phi : f \in I\})$ is algebraic. If $X = U \cup V$ where algebraic sets $U, V \subset X$ properly, then $\phi^{-1}[X] = \phi^{-1}[U] \cup \phi^{-1}[V]$. Choose $p \in X \setminus U$, and let x be such that $\phi(x) = p$, then $x \in \phi^{-1}[X] \setminus \phi^{-1}[U]$, so $\phi^{-1}[U] \subset \phi^{-1}[X]$ properly, and similarly $\phi^{-1}[V] \subset \phi^{-1}[X]$ properly. Since $\phi^{-1}[U], \phi^{-1}[V]$ are algebraic as U, V are algebraic, we have $\phi^{-1}[X]$ is reducible. Thus $\phi^{-1}[X]$ is irreducible implies X is irreducible. □

Problem 1.0.11. Let $V \subseteq \mathbf{A}^n$ be a variety, show that TFAE

(i) V is a point

(ii) $\Gamma(V) = \mathbf{C}$

(iii) $\dim_{\mathbf{C}} \Gamma(V)$ is finite

Proof. Assume (i), then let $V = \{(x_1, \ldots, x_n)\}$. We claim that $\mathcal{I}(V) = (X_1 - x_1, \ldots, X_n - x_n)$. Note that $\mathcal{V}((X_1 - x_1, \ldots, X_n - x_n)) = V$ which is straightforward. Next, since $x_1, \ldots, x_n \in \mathbf{C}$, we have

$$\mathbf{C}[X_1, \ldots, X_n]/(X_1 - x_1, \ldots, X_n - x_n) \cong \mathbf{C}[x_1, \ldots, x_n] \cong \mathbf{C}$$

which is an integral domain, so $(X_1 - x_1, \ldots, X_n - x_n)$ is prime, so it's also a radical ideal. Therefore we have $\mathcal{I}(V) = \mathcal{I}(\mathcal{V}((X_1 - x_1, \ldots, X_n - x_n))) = (X_1 - x_1, \ldots, X_n - x_n)$ by Nullstellensatz. Thus, we indeed have $\Gamma(V) = \mathbf{C}[X_1, \ldots, X_n]/\mathcal{I}(V) = \mathbf{C}$. Next, assume (ii), then $\dim_{\mathbf{C}} \Gamma(V) = \dim_{\mathbf{C}} \mathbf{C} = 1 < \infty$ straightforwardly. Assume (iii), then $\Gamma(V) = \mathbf{C}[X_1, \ldots, X_n]/\mathcal{I}(V)$ has finite dimension over $\mathbf{C}$. Let $i \in \{1, \ldots, n\}$. We note that if $\{1, X_i, X_i^2, X_i^3, \ldots\}$ is linearly independent then we cannot have $\dim_{\mathbf{C}} \Gamma(V) < \infty$, thus they are linearly dependent. This means that there exists some polynomial $f_i \in \mathbf{C}[X_i] \subseteq \mathbf{C}[X_1, \ldots, X_n]$ with coefficients not all zero for which $f_i(X_i) \equiv 0 \pmod{\mathcal{I}(V)}$. Hence $f_i \in \mathcal{I}(V)$ for each i. By Hilbert's Nullstellensatz, we have $\mathcal{V}(\mathcal{I}(V)) = V$ as V is an algebraic set. Thus for each $p \in V$, we have $p \in \mathcal{V}(\mathcal{I}(V))$, so $f_i(p) = 0$ for each i. The fact that each f_i is a single-variable polynomial over $\mathbf{C}$ means that it has finitely many roots. Therefore we only have finitely many choices for each coordinate of p. Thus V is a finite set. Since V is a variety, it is irreducible, therefore it must be a single point. $\square$