Elliptic Curves

Alec Zabel-Mena

June 23, 2023

Contents

Chapter 1

Algebraic Varieties

1.1 Affine Varieties

Definition. Let k be a perfect field. We define **affine n-space** over k to be the set

$$\mathbb{A}^n(\overline{k}) = \{P = (x_1, \ldots, x_n) : x_i \in \overline{k}\}$$

where $\overline{k}$ is the algebraic closure of k. We define the set of all **k-rational points** of $\mathbb{A}^n$ to be

$$\mathbb{A}^n(k) = \{P = (x_1, \ldots, x_n) : x_i \in k\}$$

Lemma 1.1.1. *Let k be a perfect field, and $\overline{k}$ its algebraic closure. Then $\mathrm{Gal}\,{}^{\overline{k}}\!/_{k}$ acts on $\mathbb{A}^n$ via the action*

$$P = (x_1, \ldots, x_n) \to \sigma P = (\sigma x_1, \ldots, \sigma x_n)$$

Moreover

$$\mathbb{A}^n(k) = \{P \in \mathbb{A}^n : \sigma P = P \textit{ for all } \sigma \in \mathrm{Gal}\,{}^{\overline{k}}\!/_{k}\}$$

Proof. It is not hard to check that the action described above is indeed an action on $\mathbb{A}^n$. Moreover, since $\mathrm{Gal}\,{}^{\overline{k}}\!/_{k}$ consists of all k-automorphisms (i.e. automorphisms of $\overline{k}$ that fix k), then for any $\sigma \in \mathrm{Gal}\,{}^{\overline{k}}\!/_{k}$, and $P \in k$, we have $\sigma P = P$. ∎

Definition. Let k be a perfect field, and let $\mathfrak{a}$ be an ideal of $\overline{k}[x_1, \ldots, x_n]$. We define an **affine algebraic set** to be a set

$$V_{\mathfrak{a}} = \{P \in \mathbb{A}^n(\overline{k}) : f(P) = 0 \text{ for all } f \in \mathfrak{a}\}$$

That is, it is the set of all zeros of all polynomials in $\mathfrak{a}$. We define the **ideal** of $\mathbb{V}_{\mathfrak{a}}$ to be the set

$$I(V_{\mathfrak{a}}) = \{f \in \overline{k}[x_1, \ldots, x_n] : f(P) = 0 \text{ for all } P \in V_{\mathfrak{a}}\}$$

Lemma 1.1.2. *Let k be a perfect field, and V an affine algebraic set. Then $I(V)$ is an ideal in $\overline{k}[x_1, \ldots, x_n]$. Moreover, it is finitely generated.*

Proof. We have that $I(V)$ forms a subgroup of $\overline{k}[x_1,\dots,x_n]$, indeed, if $f,g \in I(V)$, then $-f \in I(V)$ and $g \in I(V)$. Moreover, if $g \in \overline{k}[x_1,\dots,x_n]$, then $gf \in I(V)$. Now, since $\overline{k}$ is a field, it is a PID, and hence Noetherian, so that by Hilbert's theorem (see [1] or [2]), $\overline{k}[x_1,\dots,x_n]$ is Noetherian, and so every ideal in $\overline{k}[x_1,\dots,x_n]$ must be finitely generated. ■

Lemma 1.1.3. *Let V be an algebraic set over a perfect field, and consider the set $I({}^{V}\!/_{k}) = I(V) \cap \overline{k}[x_1,\dots,x_n]$. Then $I({}^{V}\!/_{k})$ is defined over k if, and only if*

$$I(V) = I({}^{V}\!/_{k})\overline{k}[x_1,\dots,x_n]$$

Moreover, $I({}^{V}\!/_{k})$ is an ideal of $\overline{k}[x_1,\dots,x_n]$.

Proof. Exercise ■

Corollary. *If V is defined over k such that $I({}^{V}\!/_{k}) = (f_1,\dots,f_m)$, where $f_1,\dots,f_m \in k$, then V is the set of all solutions to the polynomial equations*

$$f_1(x_1,\dots,x_n) = \cdots = f_m(x_1,\dots,x_n) = 0 \text{ for all } x_1,\dots,x_n \in k$$

Corollary. *If V is defined over k, then the action of $\mathrm{Gal}\,{}^{\overline{k}}\!/_{k}$ on $\mathbb{A}^n$ induces an action on V, and*

$$V = \{P \in V : \sigma P = P \text{ for all } \sigma \in \mathrm{Gal}\,{}^{\overline{k}}\!/_{k}\}$$

Proof. This result follows, in fact, immediately from lemma 1.1.1 ■

Example 1.1. (1) Let k be a perfect field and let V the algebraic set in $\mathbb{A}^2$ given by the equation

$$x^2 - y^2 = 1$$

That is,

$$V = \{P \in \mathbb{A}^2 : x^2 - y^2 - 1 = 0\}$$

Suppose that $\operatorname{char} k \neq 2$. Then V is in 1–1 correspondence onto the set $\mathbb{A}^2 \backslash \{0\}$ given by the map

$$t \to \Big(\frac{t^2+1}{2t}, \frac{t^2-1}{2t}\Big)$$

That is, the set of all k-rational points, for $\operatorname{char} k \neq 0$ of the set is given by

$$\Big(\frac{t^2+1}{2t}, \frac{t^2-1}{2t}\Big)$$

Now take $k = \mathbb{Q}$, whose algebraic closure is $\mathbb{R}$, then notice that the equation $x^2 - y^2 = 1$ over $\mathbb{A}^2 = \mathbb{R}^2$ defines the unit hyperbola. We can derive the formula for the $\mathbb{Q}$-rational points on V then by considering the line intersecting the curve $x^2 - y^2 - 1$ at the points P, $(-1,0)$ and intersection the y-axis at $(0,-1)$ as shown in figure 1.1.

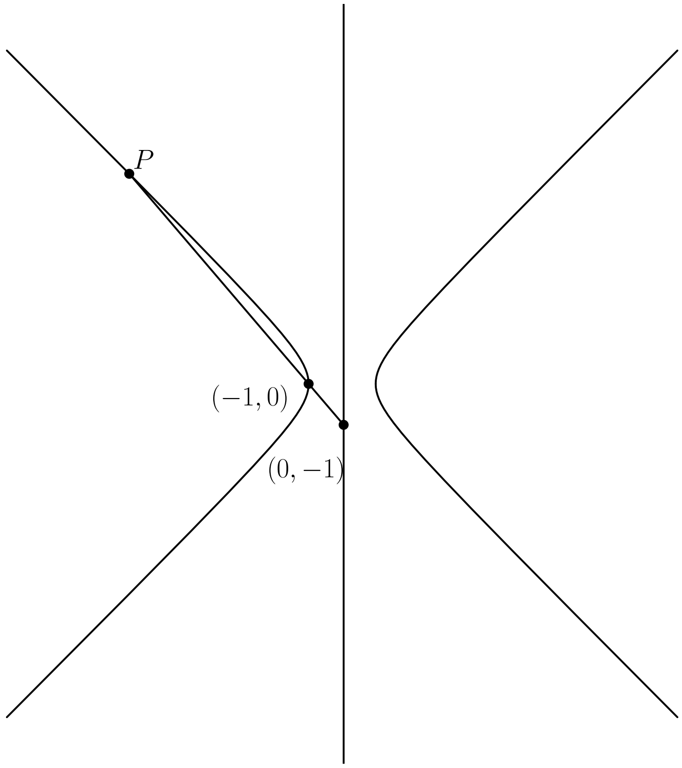

Figure 1.1:

(2) Fermat's Last Theorem, states that the algebraic set $V : x^n + y^n = 1$ has as $\mathbb{Q}$-rational points the set consisting of

$$V(\mathbb{Q}) = \begin{cases} (1,0),(0,1), \text{ if } n \equiv 0 \mod 2 \\ (\pm 1,0),(0,\pm 1) \text{ if } n \equiv 1 \mod 2 \end{cases}$$

(3) The algebraic set $V : y^2 = x^3 + 17$ has many $\mathbb{Q}$-rational points, of which are

$$(-2,3) \qquad (5234, 37866) \qquad \left(\frac{137}{64}, \frac{2651}{512}\right)$$

Definition. We call an affine algebraic set V over a perfect field k an **affine variety** if $I(V)$ is a prime ideal in $\overline{k}[x_1,\ldots,x_n]$. We define the **affine coordinate ring** of V to be the factor ring

$$k[V] = {}^{k[x_1,\ldots,x_n]}\big/_{I(V/k)}$$

We call the field of fractions of $k[V]$ the **function field** of V over k and denote it $k(V)$. We similarly define $\overline{k}[V]$ to be

$$\overline{k}[V] = {}^{\overline{k}[x_1,\ldots,x_n]}\big/_{I(V/\overline{k})}$$

and $\overline{k}(V)$ to be the field of fractions of $\overline{k}(V)$.

Lemma 1.1.4. *The affine coordinate ring of a affine variety is an integral domain.*

Proof. Let k be a perfect set, and V an affine variety over k. By definition, we have that $I(V)$ is a prime ideal in $\overline{k}[x_1, \ldots, x_n]$; moreover, since k is a field, $k[x_1, \ldots, x_n]$ is a commutative ring with identity. This means that $k[V]$ must be an integral domain (see proposition 13; [3]). ■

Lemma 1.1.5. *Let k be a perfect field, and V an affine variety over k. Then $k[V]$ and $k(V)$ are subsets of $\overline{k}[V]$ and $\overline{k}(V)$ fixed by* $\mathrm{Gal}\,{}^{\overline{k}}\!/_{k}$.

Proof. Excersice (see exercise 1.12; [4]). ■

Definition. Let k be a perfect field. A **transcendental base** of ${}^{\overline{k}}\!/_{k}$ is a maximally algebraically independent subset of $\overline{k}$ over k. We define the **transcendence degree** of ${}^{\overline{k}}\!/_{k}$ to be the cardinality of any given transcendental base of ${}^{\overline{k}}\!/_{k}$, and denote it $\mathrm{trdim}\,{}^{k}\!/_{k}$. We define the dimension on an affine variety over k to be

$$\dim V = \mathrm{trdim}\,{}^{\overline{k}(V)}\!/_{k}$$

Example 1.2. $\dim \mathbb{A}^n = n$ since $\overline{k}(\mathbb{A}^n) = \overline{k}(x_1, \ldots, x_n)$. Now, if $V \subseteq \mathbb{A}^n$ is a variety given by the polynomial equation

$$f(x_1, \ldots, x_n) = 0$$

then $\dim V = n - 1$.

Definition. Let V be an affine variety over k such that $I(V) = (f_1, \ldots, f_m)$ with $f_1, \ldots f_m \in \overline{k}[x_1, \ldots, x_n]$, and let $P \in V$. We call V **nonsingular** (or **smooth**) at P if the $m \times n$ matrix

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \end{pmatrix}$$

has rank $n - \dim V$. If V is nonsingular at any point, then we call V **nonsingular** (or **smooth**). We call V **singular** if it is not nonsingular.

Lemma 1.1.6. *Let V be an affine variety over a perfect field k, and $I(V) = (f)$ for some $f \in \overline{k}[x_1, \ldots, x_n]$. Then V is singular if, and only if*

$$\frac{\partial f}{\partial x_1} = \cdots = \frac{\partial f}{\partial x_1} = 0$$

Proof. We prove the contrapositve. Since f is given by the polynomial equation $f(x_1, \ldots, x_n) = 0$, then $\dim V = n - 1$, so that if V is nonsingular, then the $1 \times n$ matrix

$$\begin{pmatrix} \frac{\partial f}{\partial x_1} & \cdots & \frac{\partial f}{\partial x_n} \end{pmatrix}$$

has rank $n - (n - 1) = 1$; in which case, we have for for all $1 \leq i \leq n$

$$\frac{\partial f}{\partial x_i} \neq 0$$

The converse holds by similar reasoning. ■

Example 1.3. Consider the affine varieties

$$V_1 : y^2 = x^3 + x \text{ and } V_2 : y^2 = x^3 + x^2$$

Then a point of V_1, and V_2, respectively, is singular if

$$2y = 3x^2 + 1 = 0 \text{ and } 2y = 3x^2 + 2x = 0$$

Then V_1 is nonsingular, where as V_2 is singular at the point $P = (0, 0)$. Letting $k = \mathbb{Q}$, and graphing the curves $y^2 - x^3 - x$ and $y^2 - x^3 - x^2$ in $\mathbb{R}^2$ in figure 1.2 shows us the singular and nonsingular points

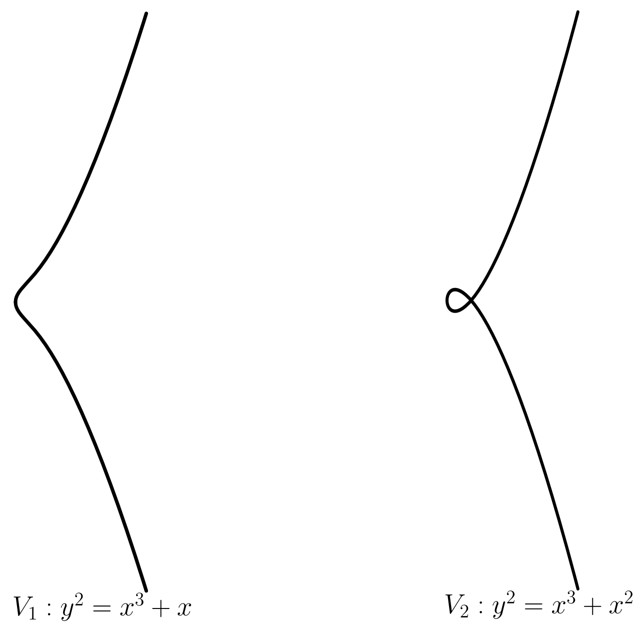

Figure 1.2:

Lemma 1.1.7. *Let V be an affine variety over a perfect field k, and let $P \in V$. Define $\mathfrak{m}_P$ of $\overline{k}[V]$ by*

$$\mathfrak{m}_P = \{f \in \overline{k}[x_1, \dots, x_n] : f(P) = 0\}$$

Then $\mathfrak{m}_P$ is an idela of $\overline{k}[x_1, \dots, x_n]$, and P is a nonsingular point of V if, and only if

$$\dim_{\overline{k}} \mathfrak{m}_P / \mathfrak{m}_P^2 = \dim V$$

where $\mathfrak{m}_P / \mathfrak{m}_P^2$ is considered as a vector space.

Example 1.4. Consider again the varieties of example 1.3. Then $\mathfrak{m}_P$ is the ideal $\mathfrak{m}_P = (x, y)$ in $\overline{k}[x, y]$, and $\mathfrak{m}_P^2 = (x^2, xy, y^2)$. Then we have

$$x = y^2 - x^3 \equiv 0 \mod \mathfrak{m}_P^2$$

so that $\mathfrak{m}_P / \mathfrak{m}_P^2 = (y)$ in the variety V_1. On the other hand, there is no nontrivial relation between x and y in $\mathfrak{m}_P^2$ for V_2, so that $\mathfrak{m}_P / \mathfrak{m}_P^2$ must have x and y as generators. Now, $\dim V_1 = \dim V_2 = 1$, implying, by lemma 1.1.7 that V_1 is nonsingular and V_2 is singular.

Definition. Let V be an affine variety over a perfect field k. We define the **local ring** of V at P, denoted $\overline{k}[V]_P$ to be the localization of $\overline{k}[V]$ at $\mathfrak{m}_P$. That is

$$\overline{k}[V]_P = \left\{ F \in \overline{k}(V) : f = \frac{f}{g}, f, g \in \overline{k}[x_1, \ldots, x_n] \text{ and } g(P) \neq 0 \right\}$$

1.2 Projective Varieties

Bibliography

[1] M. Atiyah and I. MacDonald, *Introduction to Commutative Algebra.* Addison-Wesly Series in Mathematics, CRC Press.

[2] D. Eisenbud, *Commutative Algebra: Wit a View Toward Algebraic Geometry.* Graduate Texts in Mathematics, Springer Verlag.

[3] D. Dummit and R. Foote, *Abstract algebra.* Hoboken, NJ: John Wiley & Sons, Inc, 2004.

[4] J. Silverman, *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics, Springer Verlag.

[5] I. N. Herstein, *Topics in algebra.* New York: Wiley, 1975.

[6] R. Hartshorne, *Algebraic Geometry.* Graduate Texts in Mathematics, Springer Verlag.