Math 6170 C, Lecture on Feb 19, 2020

Yongchang Zhu

Textbook: Silverman "The Arithmetic of Elliptic Curves", GTM 106.

Reference books: (1) A. Knapp "Elliptic Curves"
(2) Hartshorne "Algebraic Geometry" Chapter I.

Notations in Chapter 1.

K: A perfect field (i.e., every algebraic extensions of K is separable),

Examples: Characteristic 0 fields and finite fields are perfect

$\bar{K}$: algebraic closure of K

$G_{\bar{K}/K}$: the Galois group of $\bar{K}/K$.

Definition. Affine n-space is

$$\mathbb{A}^n(\bar{K}) = \{(x_1, \dots, x_n) : x_i \in \bar{K}\}.$$

For an ideal $I \subset \bar{K}[X_1, \ldots, X_n] = \bar{K}[X]$, the zero set of I is

$$V_I = \{x = (x_1, \ldots, x_n) \mid f(x) = 0 \quad \text{for all } f \in I\}.$$

A set of the form V_I, where I is an ideal, is called an **algebraic set**.

Since $\bar{K}[X_1, \ldots, X_n]$ is Noetherian, every ideal is finitely generated. Suppose

$$I = \bar{K}[X]g_1 + \cdots + \bar{K}[X]g_m$$

then $x \in V_I$ iff

$$g_1(x) = \cdots = g_m(x) = 0.$$

So V_I is the solution set of the system

$$g_1(x) = \cdots = g_m(x) = 0.$$

Examples.

If $I = \bar{K}[X]$, then V_I is the empty set.

If $I = \{0\}$, then $V_I = \mathbb{A}^n(\bar{K})$.

Every linear subspace of $\bar{K}^n$ is an algebraic set.

The algebraic subsets in $\mathbb{A}^1(\bar{K})$ are precisely finite subsets and $\mathbb{A}^1(\bar{K})$ itself.

The intersection of any family of algebraic sets is an algebraic set. This follows from the identity

$$\cap_k V_{I_k} = V_{\sum_k I_k}.$$

The union of **finitely** many algebraic sets is an algebraic set. This follows from the identity

$$V_I \cup V_J = V_{IJ}.$$

So we can define the **Zariski topology** in $\mathbb{A}^n(\bar{K})$ such that the algebraic sets V_I are the closed sets (their complements are the open sets).

For an algebraic set $V \subset \mathbb{A}^n(\bar{K})$, its ideal $I(V)$ is given by

$$I(V) \stackrel{\text{def}}{=} \{f \in \bar{K}[X] \mid f(x) = 0 \text{ for all } x \in V\}.$$

It can be proved that $I(V)$ is the largest ideal J such that $V_J = V$.

In fact, $I(V_J) = \sqrt{J}$ by Hilbert's nullstellensatz.

An algebraic set V is called an **(affine) variety** if $I(V)$ is a prime ideal.

$\mathbb{A}^n(\bar{K})$ is an variety, because $\{0\}$ is a prime ideal. The empty set is not a variety, because $\bar{K}[X]$ itself is not a prime ideal of $\bar{K}[X]$.

The **coordinate ring** of an affine variety V is defined to be

$$\bar{K}[V] \stackrel{\mathrm{def}}{=} \bar{K}[X]/I(V),$$

which is always an integral domain.

An element $f + I(V) \in \bar{K}[V] = \bar{K}[X]/I(V)$ defines a function

$$V \to \bar{K}, \quad x \mapsto f(x).$$

The field of fractions of $\bar{K}[V]$ is called the function field of V, and is denoted by $\bar{K}(V)$.

$$\bar{K}(V) = \operatorname{Frac} \bar{K}[V].$$

Example. The function field of $\mathbb{A}^1(\bar{K})$ is the field of fractions of one variable polynomial ring $\bar{K}[X]$.

Let V be a variety, the **dimension of** V, denoted by $\dim(V)$, is the transcendence degree of $\bar{K}(V)$ (over $\bar{K}$).

$$\dim(\mathbb{A}^n(\bar{K})) = n.$$

If V is a hyper-surface in $\mathbb{A}^n(\bar{K})$, i.e., $I(V)$ is a principal ideal, then $\dim(V) = n - 1$.

If W is a k-dimensional linear subspace of $\mathbb{A}^n(\bar{K})$, then $\dim(W)$, as a variety, is k.

Definition. Let $V \subset \mathbb{A}^n(\bar{K})$ be a variety, and $f_1, \ldots, f_m$ be a set of generators of $I(V)$. A point $x = (x_1, \ldots, x_n) \in V$ is called a **non-singular point** (or **smooth point**) of V if the $m \times n$

$$\partial_i g_j(x_1, \ldots, x_n)$$

has rank $n - \dim(V)$. If V is non-singular at every point, then we say that V is a **non-singular variety** (smooth variety).

Example.

Let $f(x)$ be an one variable polynomial without repeated roots, then the principal ideal I generated by $y^2 - f(x)$ in $\bar{K}[x, y]$ is a prime ideal. V_I is one dimensional and it is a smooth variety.

For a point $P \in V$, let

$$M_P = \{f \in \bar{K}[V] \mid f(P) = 0\}.$$

M_P is a maximal ideal of $\bar{K}[V]$ (as the quotient ring $\bar{K}[V]/M_P$ is isomorphic to $\bar{K}$).

Proposition 1.7. *P is a non-singular point of V iff*

$$\dim_{\bar{K}} M_P/M_P^2 = \dim V.$$

For a point $P \in V$, the **local ring** of V at P, denoted by $\bar{K}[V]_P$ is the localization of $\bar{K}[V]$ at M_P. That is

$$\bar{K}[V]_P = \{\frac{f}{g} \mid f, g \in \bar{K}[V], g(P) \neq 0\}.$$

By definition, $\bar{K}[V]_P$ is a subring of $\bar{K}(V)$.

For every subfield $K \subset L \subset \bar{K}$, the set of L-rational points in $\mathbb{A}^n$ is the set

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

The Galois group $G_{\bar{K}/K}$ acts on $\mathbb{A}^n(\bar{K})$; for $\sigma \in G_{\bar{K}/K}$, $x = (x_1, \ldots, x_n) \in \mathbb{A}^n(\bar{K})$,

$$x^\sigma = (x_1, \ldots, x_n)^\sigma = (x_1^\sigma, \ldots, x_n^\sigma).$$

It is clear that $x^\sigma = x$ for all $\sigma \in G_{\bar{K}/K}$ iff $x \in \mathbb{A}^n(K)$.

K is separable implies that $\bar{K}^{G_{\bar{K}/K}} = K$.

An algebraic set $V \subset \mathbb{A}^n(\bar{K})$ is **defined over** K if $I(V)$ can be generated by polynomials in $K[X]$.

In this case, $G_{\bar{K}/K}$ acts on V, and the fixed point set

$$V^{G_{\bar{K}/K}} = V \cap \mathbb{A}^n(K).$$

We denote

$$V(K) = V \cap \mathbb{A}^n(K).$$

$V(K)$ is called the set of K-**rational points** of V.

If algebraic set $V \subset \mathbb{A}^n(\bar{K})$ is **defined over** K, we define the affine coordinate ring of V over K by

$$K[V] = K[X]/(I(V) \cap K[X]).$$

Definition. Projective n-space is

$$\mathbb{P}^n(\bar{K}) = \{(x_0, x_1, \ldots, x_n) : x_i \in \bar{K}, \text{not all } x_i\ 0\}/\bar{K}^*.$$

That is, $\mathbb{P}^n(\bar{K})$ is the orbit space of the multiplicative group $\bar{K}^*$ on $\bar{K}^{n+1} - \{0\}$, where the action is given by

$$a \cdot (x_0, x_1, \ldots, x_n) = (ax_0, ax_1, \ldots, ax_n).$$

We will denote by $[x_0, x_1, \ldots, x_n]$ the point in $\mathbb{P}^n(\bar{K})$ represented by $(x_0, x_1, \ldots, x_n)$. $[x_0, x_1, \ldots, x_n]$ is called a **homogeneous coordinate** of the point.

It is easy to see that $\mathbb{P}^n(\bar{K})$ is the set of all one dimensional $\bar{K}$-linear subspaces in $\bar{K}^{n+1}$.

The polynomial ring $\bar{K}[X] = \bar{K}[X_0, X_1, \ldots, X_n]$ has a gradation

$$\bar{K}[X] = \oplus_{m=0}^{\infty} \bar{K}[X]_m,$$

where $\bar{K}[X]_0 = \bar{K}$, and for $m \geq 1$, $\bar{K}[X]_m$ is the $\bar{K}$-linear span of monomials $X_0^{k_0} X_1^{k_1} \cdots X_n^{k_n}$ with $k_0 + k_1 + \cdots + k_n = m$.

$$\bar{K}[X]_k \, \bar{K}[X]_m = \bar{K}[X]_{m+k}.$$

$f \in \bar{K}[X]$ is called a homogeneous polynomial if $f \in K[X]_m$ for some m,

such a f satisfies the property that

$$f(\lambda x) = \lambda^m f(x)$$

for every $\lambda \in \bar{K}^*$.

An ideal $I \subset \bar{K}[X]$ is called a **homogenous ideal** if I is generated by homogeneous polynomials of positive degree.

If I is a homogenous ideal, the set

$$\{(x_0, \ldots, x_n) \in \bar{K}^{n+1} - \{0\} \mid f(x) = 0 \ \text{for all } f \in I\}$$

is stable under the K^*-action, the orbit space is denoted by V_I.

The set of the form V_I is called a **(projective) algebraic set** of $\mathbb{P}^n(\bar{K})$.

Since

$$\cap_k V_{I_k} = V_{\sum_k I_k}, \quad V_I \cup V_J = V_{IJ},$$

we can define the **Zariski topology** on $\mathbb{P}^n(\bar{K})$ such that V_I's are the closed subsets.

For a projective algebraic set V in $\mathbb{P}^n(\bar{K})$, we let $I(V)$ be the ideal generated by the homogeneous polynomials

$$\{f \in \bar{K}[X] \mid f \text{ homogeneous and } f(x) = 0 \text{ for all } x \in V\}.$$

$I(V)$ is called **the ideal of** V.

A non-empty projective algebraic set V is called a **projective variety** if $I(V)$ is a prime ideal.

Now $\bar{K}[X]/I(V)$ is an integral domain. Because $I(V)$ is a homogeneous ideal, so $I(V) = \oplus_{m=0}^{\infty} I(V)_m$, where $I(V)_m$ is the space of homogeneous elements of degree m in $I(V)$. Then $\bar{K}[X]/I(V)$ is graded, i.e.,

$$\bar{K}[X]/I(V) = \oplus_{m=0}^{\infty} \left(\bar{K}[X]/I(V)\right)_m$$

where $\left(\bar{K}[X]/I(V)\right)_m$ is $\bar{K}[X]_m + I$.

We consider its field of fractions $\operatorname{Frac} \bar{K}[X]/I(V)$, an element is called a **homogenous element of degree** 0 if it can be written as

$$\frac{f}{g}$$

if $f, g \in \bar{K}[X]/I(V)$ are homogeneous with **the same degree**.

The set of all the homogenous elements of degree 0 is a subfield of $\operatorname{Frac} \bar{K}[X]/I(V)$.

It is called the **function field** of projective variety V and is denoted by $\bar{K}(V)$.

We define

$$\mathbb{P}^n(K) = \{[x_0, x_1, \ldots, x_n] \mid x_i \in K,\ i = 0, 1, \ldots, n\}$$

called the set of K-rational points of $\mathbb{P}^n$.

The Galois group $G_{\bar{K}/K}$ acts on $\mathbb{P}^n(\bar{K})$ by

$$[x_0, \ldots, x_n]^\sigma = [x_0^\sigma, \ldots, x_n^\sigma].$$

$$\mathbb{P}^n(K) = \mathbb{P}^n(\bar{K})^{G_{\bar{K}/K}}$$

An projective variety V is defined over K if $I(V)$ can be generated by the homogeneous elements in $K[X]$. In this case $G_{\bar{K}/K}$ acts on V, its fixed point set is

$$V \cap \mathbb{P}^n(K) \stackrel{\mathrm{def}}{=} V(K).$$

Relations between Affine Varieties and Projective varieties

For each $0 \leq i \leq n$, there is an inclusion

$$\phi_i : \mathbb{A}^n(\bar{K}) \to \mathbb{P}^n(\bar{K})$$

$$(y_1, \ldots, y_n) \mapsto [y_1, \ldots, y_{i-1}, 1, y_i, \ldots, y_n].$$

what is the image of ϕ_i? If we denote H_i be the hyperplane in $\mathbb{P}^n(\bar{K})$, given by the equation $X_i = 0$, then

$$\mathrm{Image}(\phi_i) = U_i = \mathbb{P}^n(\bar{K}) - H_i.$$

It is Zariski open.

$$U_i = \{[x_0, \ldots, x_n] \in \mathbb{P}^n(\bar{K}) \mid x_i \neq 0\}$$

The inverse map $\phi_i^{-1} : U_i \to \mathbb{A}^n(\bar{K})$ is

$$[x_0, \ldots, x_n] \mapsto (\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}).$$

Let V be a projective algebraic set in $\mathbb{P}^n(\bar{K})$ with homogeneous ideal $I(V)$.

Then $\phi_i^{-1}(U_i \cap V)$ is an affine algebraic set with ideal $I(U_i \cap V)$ given by

$$\begin{aligned} I(U_i \cap V) \qquad &= \{f(X_1, \ldots, X_{i-1}, 1, X_i, \ldots, X_n) \,|\, f \in I(V)\} \\ &\subset \bar{K}[X_1, \ldots, X_n] \end{aligned}$$

$f(X_1, \ldots, X_{i-1}, 1, X_i, \ldots, X_n)$ is called the dehomogenization of f with respect to X_i.

Conversely, for $f(X) \in \bar{K}[X_1, \ldots, X_n]$, we let

$$f^*(X_0, X_1, \ldots, X_n) = X_i^d f(\frac{X_0}{X_i}, \frac{X_1}{X_i}, \ldots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \ldots, \frac{X_n}{X_i})$$

where $d = \deg f$. Then f^* is a homogeneous polynomial of degree d.

We say that f^* is the **homogenization of f with respect to X_i**.

Definition.

Let V be an affine algebraic set in $\mathbb{A}^n(\bar{K})$ with ideal $I(V)$, and consider V as a subset via the map

$$V \subset \mathbb{A}^n(\bar{K}) \xrightarrow{\phi_i} \mathbb{P}^n(\bar{K})$$

The projective closure of V, denoted by $\bar{V}$, is the projective algebraic set whose homogeneous ideal $I(\bar{V})$ is generated by

$$\{f^*(X) : f \in I(V)\}.$$

It can be proved that $\phi_i(V) \subset \bar{V}$.

And it can proved that $\bar{V}$ is the topological closure of $\phi_i(V)$ in the Zariski topology.

Proposition 2.6. (a) Let V be an affine variety. Then $\bar{V}$ is a projective variety. and $V = \bar{V} \cap U_i$.
(b) Let V be a projective veriety. Then $V \cap U_i$ is an affine variety, and either $V \cap U_i = \emptyset$ or $V = \overline{V \cap U_i}$.
(c) If V is affine (respectively proejctive) variety define over K, then $\bar{V}$ (respectively $V \cap U_i$) is also defined over K

For projective variety V, the dimension of V, $\dim V$, is defined to be $\dim V \cap U_i$ for any i with $V \cap U_i$ non-empty.

Theorem. $\dim V$ is equal to the transcendental degree of the field of rational functions $\bar{K}(V)$.

Here we follow Hartshorne Chapter I.

An affine or projective variety has the Zariski topology that is the induced topology from the Zariski topology on $\mathbb{A}^n(\bar{K})$ or $\mathbb{P}^n(\bar{K})$.

Let V be an affine variety, $U \subset V$ be a non-empty open subset. A function $\phi : U \to \bar{K}$ is called a regular function on U if ϕ is **locally** equal to

$$\frac{f}{g}$$

for $f, g \in \bar{K}[V], g \neq 0$.

The set of regular functions on U is denoted by $\mathcal{O}(U)$. $U \mapsto \mathcal{O}(U)$ is a sheaf of rings on V.

Let V be a projective variety, $U \subset V$ be a non-empty open subset. A function $\phi : U \to \bar{K}$ is called a regular function on U if it is locally equal to $\frac{f}{g} \in \bar{K}(V)$.

The set of regular function functions on U, $\mathcal{O}(U)$, is a ring and $U \mapsto \mathcal{O}(U)$ is a sheaf of ring on V.

Let V_1, V_2 be varieties (there are four cases: V_i can be either affine or projective). A map $\varphi : V_1 \to V_2$ is called a **morphism** if
(1) φ is continuous.
(2) The pullback of local regular functions on V_2 under φ is a local regular function on V_1. That is, for every $f \in \mathcal{O}(U)$, where $U \subset V_2$ is open, then $f \circ \varphi : \varphi^{-1}(U) \to \bar{K}$ is a regular function.

The end