CHAPTER 1

ALGEBRAIC VARIETIES

In this chapter, we follow roughly [**Sil09**, Chap. I] and [**NX09**, Chap. 2].

Throughout this chapter: k will denote a perfect field (*i.e.* every extension of k is separable), $\overline{k}$ is a fixed algebraic closure of k, and G_k denote the Galois group of $\overline{k}/k$. The hypothesis that k be perfect is not absolutely necessary but it simplifies the exposition. Note that finite fields and their algebraic closures are perfect.

For more details on algebraic geometry, one can have a look at [**Har77**], [**Mum99**], [**Kem93**], [**Rei95**], ...

1.1. Affine varieties

We begin by defining the affine space and its algebraic subsets.

1.1.1. Affine space. —

Definition 1.1. — The affine space of dimension $n \geq 1$ over k is the set of n-tuples:

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

An element $P = (x_1, \dots, x_n) \in \mathbb{A}^n$ is called a point, and the x_i's are called the coordinates of P. For a finite extension k'/k inside $\overline{k}$, a point $P \in \mathbb{A}^n$ is called k'-rational if all its coordinates are elements of k': in other words, the set of k'-rational points on $\mathbb{A}^n$ is the subset

$$\mathbb{A}^n(k') = \left\{P = (x_1, \dots, x_n) : x_i \in k'\right\}.$$

We denote by G_k the Galois group $\mathrm{Gal}(\overline{k}/k)$: since it acts on $\overline{k}$, it certainly acts on $\mathbb{A}^n$ too:

$$\text{for all } \sigma \in G_k \text{ and all } P = (x_1, \dots, x_n) \in \mathbb{A}^n, \quad \sigma(P) := (\sigma(x_1), \dots, \sigma(x_n)).$$

Check that this actually defines an action on $\mathbb{A}^n$. Then, the set of k-rational points $\mathbb{A}^n(k)$ can be characterized as the set of fixed points under the action of G_k:

$$\mathbb{A}^n(k) = \{P \in \mathbb{A}^n : \sigma(P) = P \ \forall \sigma \in G_k\}.$$

This follows essentially from the fact that $k \subset \overline{k}$ is exactly the set of elements of $\overline{k}$ that are fixed under the action of G_k.

Example 1.2. — Assume that $k = \mathbb{F}_q$. In this case, the Galois group G_k is (topologically) generated by the Frobenius morphism $\mathrm{Fr}_q : \overline{k} \to \overline{k}$, defined by $x \mapsto x^q$. It is easy to check that

$$\mathbb{A}^n(\mathbb{F}_q) = \left\{P \in \mathbb{A}^n(\overline{\mathbb{F}_q}) : \mathrm{Fr}_q(P) = P\right\}.$$

Definition 1.3. — For a point $P \in \mathbb{A}^n$, the set $\{\sigma(P), \sigma \in G_k\}$ is called a closed point over k (or a k-closed point). Two points in a closed point over k are called conjugate (over k).

By construction, a closed point over k is a subset of $\mathbb{A}^n$. Notice that a point is k-rational if and only if the corresponding closed point has only one element. We will discuss closed points in more details later on.

1.1.2. Affine sets. — Let $\overline{k}[X] = \overline{k}[x_1, \dots, x_n]$ be a polynomial ring in n variables over $\overline{k}$. Note the slight abuse of notation here. A polynomial $f \in \overline{k}[X]$ can be evaluated at any n-tuple of elements $x_i \in \overline{k}$, *i.e.* at any point $P = (x_1, \dots, x_n)$ of $\mathbb{A}^n$. Note that the Galois group G_k acts on $\overline{k}[X]$ by acting on the coefficients of the polynomials: a polynomial $f \in \overline{k}[X]$ is in $k[X]$ if and only if $\sigma(f) = f$ for all $\sigma \in G_k$. The actions of G_k on $\mathbb{A}^n$ and on $\overline{k}[X]$ are compatible:

$$\text{for all } f \in \overline{k}[X], \text{ all } P \in \mathbb{A}^n \text{ and all } \sigma \in G_k, \quad \sigma(f(P)) = \sigma(f)(\sigma(P)). \tag{1}$$

(Exercise: check this relation, say for $n = 1$, see [**NX09**, Lem. 2.2.2, p.38]).

For a subset $S \subset \overline{k}[X]$, we define the zero set $Z(S)$ of S to be the subset of $\mathbb{A}^n$ formed by the common zeroes of all $f \in S$:

$$Z(S) = \{P \in \mathbb{A}^n : f(P) = 0 \ \forall f \in S\}.$$

If S is as above, and if I_S denotes the ideal of $\overline{k}[X]$ generated by the elements of S, then it is not difficult to check that $Z(S) = Z(I_S)$. Therefore, we do not loose much generality by restricting our attention to zero sets of ideals.

Definition 1.4. — An affine algebraic set is any set of the form $Z(I)$ for some ideal I of $\overline{k}[X]$ (again, this is the same as considering all the zero sets $Z(S)$ for any subset $S \subset \overline{k}[X]$).

If V is an algebraic set, the ideal of V is given by:

$$I(V) = \left\{f \in \overline{k}[X] : f(P) = 0 \ \forall P \in V\right\}.$$

(Check that this indeed defines an ideal).

An (affine) algebraic set V is said to be defined over k if its ideal $I(V)$ can be generated by polynomials with coefficients in $k[X]$. For short, we will denote this situation by V/k. Let V be an algebraic set and consider the ideal $I(V/k)$ of $k[x]$ defined by

$$I(V/k) = \{f \in k[X] : f(P) = 0 \ \forall P \in V\} = I(V) \cap k[X].$$

Then $I(V/k) \cdot \overline{k}[X] \subset I(V)$, and V is defined over k if and only if $I(V) = I(V/k) \cdot \overline{k}[X]$.

If V is defined over k, then it makes sense to consider the set of k-rational points of V: it is the set

$$V(k) := V \cap \mathbb{A}^n(k) = \{P \in V : \sigma(P) = P \ \forall \sigma \in G_k\}.$$

Further, the compatibility (1) implies that, if $P \in V$ then all its conjugates $\sigma(P)$ (for $\sigma \in G_k$) are in V. In other words, the action of G_k on $\mathbb{A}^n$ restricts to an action on V and, clearly,

$$V(k) = \{P \in V : P^\sigma = P \ \forall \sigma \in G\}.$$

More explicitely, let $f_1, \dots, f_m \in k[X]$ be generators of the ideals $I(V/k)$ (by Hilbert's basis theorem, all ideals in $k[X]$ or $\overline{k}[X]$ are finitely generated). Then $V(k)$ is precisely the set of solutions $(x_1, \dots, x_n) \in k^n$ to the system of polynomial equations:

$$f_1(X) = \cdots = f_m(X) = 0 \qquad \text{with } X = (x_1, \dots, x_n) \in k^n.$$

Before going further, let us give a few examples:

Example 1.5. — The affine space $\mathbb{A}^n$ itself is an algebraic set: its ideal is $I(\mathbb{A}^n) = \{0\} \subset \overline{k}[x_1, \dots, x_n]$, which can be generated by a polynomial with coefficients in k (namely, the 0 polynomial). The affine set whose ideal is the whole of $\overline{k}[x_1, \dots, x_n]$ is the empty set.

A singleton $\{P\}$, where $P = (a_1, \dots, a_n) \in \mathbb{A}^n$, is also an algebraic set. Indeed, it is the zero set of the ideal generated by $x_1 - a_1$, ..., $x_n - a_n$ in $\overline{k}[x_1, \dots, x_n]$. Over what field is the singleton $\{P\}$ defined? It can be shown that the map which maps $(a_1, \dots, a_n) \in \mathbb{A}^n(\overline{k})$ to the ideal generated by $x_1 - a_1$, ..., $x_n - a_n$ in $\overline{k}[x_1, \dots, x_n]$ gives a one-to-one correspondence between the points of $\mathbb{A}^n(\overline{k})$ and the maximal ideals of $\overline{k}[x_1, \ldots, x_n]$ (Hilbert's Nullstellensatz, see [**Ful89**, Chap. I, §7], [**Mum99**, I.§2]). Note this map is not one-to-one if one replaces $\overline{k}$ by k.

Example 1.6. — Let $S \subset \mathbb{A}^1$ be an infinite set (Exercise: for a field k, its algebraic closure $\overline{k}$ has infinite cardinality). Then S is not algebraic: if it were, there would be a polynomial $f \in \overline{k}[x]$ with infinitely many zeroes (the elements of S).

If $k = \mathbb{R}$, the graph $\Gamma = \{(x, \cos x),\ x \in \mathbb{R}\}$ of the cosine $\subset \mathbb{A}^2$ is not algebraic.

Example 1.7. — Let $\ell(x_1, x_2) = \alpha x_1 + \beta x_2 \in \overline{k}[x_1, x_2]$ with α, β not both zero. The zero zet $L = Z(\ell)$ is called a line in $\mathbb{A}^2$. By definition, it is an affine algebraic set, given by the equation:

$$L : \alpha x_1 + \beta x_2 = 0$$

Let $f(x_1, x_2) := x_1^2 - x_2^2 - 1 \in k[x_1, x_2]$ and $I := (f)$, the ideal generated by f in $\overline{k}[x_1, x_2]$. Let $V = Z(I)$ be the algebraic set in $\mathbb{A}^2$ associated to I. One says that V is defined by the equation $f(x_1, x_2) = 0$. Clearly, V is defined over k (for any field k). Make a picture of $V(k)$, in the cases when $k = \mathbb{R}$, $k = \mathbb{F}_5$ and $k = \mathbb{F}_7$. Let us assume for simplicity that $\mathrm{char}(k) \neq 2$. Then the set $V(k)$ is in bijection with $\mathbb{A}^1(k) \smallsetminus \{0\}$, one possible map is given by

$$t \in \mathbb{A}^1(k) \smallsetminus \{0\} \to V(k), \quad t \mapsto \left(\frac{t^2+1}{2t}, \frac{t^2-1}{2t}\right).$$

Example 1.8. — Now let $g(x_1, x_2) := x_1^2 + x_2^2 - 1 \in k[x_1, x_2]$, denote by $J := (g)$ the ideal generated by g in $\overline{k}[x_1, x_2]$, and let $W = Z(J)$ be the zero set of J in $\mathbb{A}^2$. Equivalently, one writes:

$$W : x_1^2 + x_2^2 - 1 = 0$$

Again, W is defined over k (for any field k) and one can make pictures of $W(k)$ in specific examples. Can you find a bijection between $W(k)$ and $\mathbb{A}^1(k) \smallsetminus \{0\}$?

Example 1.9. — Let us give more details about algebraic sets in $\mathbb{A}^1$. For $n = 1$, the ring $\overline{k}[x]$ is a unique factorization domain (and thus a principal ideal domain). This property fails when $n > 1$: what is still true is that all ideals in $\overline{k}[x_1, \ldots, x_n]$ are finitely generated (Hilbert's basis theorem, see [**AM69**, Thm. 7.5, p. 81]).

If $V \subset \mathbb{A}^1$ is an algebraic set, its ideal $I(V) \subset \overline{k}[x]$ is principal: let us choose $g_V \in \overline{k}[x]$ such that $I(V) = (g_V)$. If $I(V) = (0)$ then $V = \mathbb{A}^1$, and if $I(V) = (1)$ then $V = \varnothing$. Otherwise, g has positive degree d, and roots $b_1, \ldots, b_d$ in $\overline{k} = \mathbb{A}^1$. So, as a set, one has $V = \{b_1, \ldots, b_d\} \subset \mathbb{A}^1$. Conversely, given a finite set of points $V = \{b_1, \ldots, b_d\}$, set $g = \prod(x - b_i) \in \overline{k}[x]$: one has $V = Z(g)$. In conclusion, the algebraic sets $\subset \mathbb{A}^1$ are $\mathbb{A}^1$ itself, $\varnothing$, and the finite subsets of $\mathbb{A}^1$.

Proposition 1.10. — *As before, we write $\overline{k}[X]$ for $\overline{k}[x_1, \ldots, x_n]$.*

(i) Let S be a nonempty subset of $\overline{k}[X]$. If I is the ideal generated by S, then $Z(S) = Z(I)$.

(ii) For any two subsets $S' \subset S$ of $\overline{k}[X]$, we have $Z(S') \supset Z(S)$.

(iii) If S, S' are two nonempty subsets of $\overline{k}[X]$, then $Z(S \cup S') = Z(S) \cap Z(S')$.

(iv) Any intersection of affine algebraic sets is an algebraic set.

(v) For any polynomials $f, g \in \overline{k}[X]$, we have $Z(f \cdot g) = Z(f) \cup Z(g)$. More generally, if S, S' are two nonempty subsets of $\overline{k}[X]$ and if we let $S \cdot S' = \{fg, f \in S, g \in S'\}$, then $Z(S \cdot S') = Z(S) \cup Z(S')$.

(vi) Any finite union of affine algebraic sets is an algebraic set.

Proof. — Left as an exercise. □

Proposition 1.11. — *Let V be an affine algebraic set.*

(i) There exists a finite set $S_0 \subset \overline{k}[X]$ such that $V = Z(S_0)$.

(ii) The zero set of $I(V)$ is V: $Z(I(V)) = V$.

(iii) If $V = Z(I)$ for some ideal I of $\overline{k}[X]$, then the ideal $I(V)$ of V is the radical of I:

$$I(Z(I)) = \mathrm{rad}(I) := \left\{ f \in \overline{k}[X] : \exists r \geq 1, f^r \in I \right\}.$$

Proof. — (i) Let S be a non empty subset of $\overline{k}[X]$ such that $V = Z(S)$, and I be the ideal generated by S. From the above proposition, one has $Z(S) = Z(I)$. Now, by Hilbert's basis theorem, I is finitely generated: this means that I can choose S_0 a finite set of polynomials such that S_0 generates I. Then $V = Z(I) = Z(S_0)$.

(ii) Again, we write that $V = Z(S)$ and we denote by $I = I_V$ the ideal of $\overline{k}[X]$ generated by S. Since $S \subset I$, the inclusion-reversing property implies that $Z(I) \subset Z(S) = V$. But, from the definitions, one has $V \subset Z(I)$.

(iii) This part is a bit more subtle. One inclusion is straightforward though: if $f \in \mathrm{rad}(I)$, then $f^r \in I$ for some $r \geq 1$ and, by definition, this means that $f(P)^r = 0$ for all $P \in V = Z(I)$; but then $f(P) = 0$ for all $P \in V$, and $f \in I(V)$. We have proved the inclusion $\mathrm{rad}(I) \subset I(Z(I))$.

The following fact is often called "the weak Nullstellensatz" (we don't prove it here):

$$\text{if } I \text{ is a proper ideal of } \overline{k}[X], \text{ then } Z(I) \neq \varnothing.$$

Note that this theorem is only true for $\overline{k}[X]$ (and not necessarily for $k[X]$ when k is not algebraically closed). Using this, we can conclude the proof of item (iii) (which is called "the Nullstellensatz"). By Hilbert's basis theorem, the ideal I_V is finitely generated: choose $f_1, \ldots, f_r$ a finite set of polynomials that generates $I \subset \overline{k}[x_1, \ldots, x_n]$. Let $g \in I(Z(I)) = I(Z(f_1, \ldots, f_r))$. We need to show that there exists $r \geq 1$ such that $g^r \in I$. Consider the ideal J of $\overline{k}[x_1, \ldots, x_n, x_{n+1}]$ generated by the f_i's and $x_{n+1}g - 1$:

$$J = (f_1, \ldots, f_r, x_{n+1}g - 1) \subset \overline{k}[x_1, \ldots, x_n, x_{n+1}].$$

Then $Z(J)$ is an algebraic subset of $\mathbb{A}^{n+1}$. Since g vanishes wherever all the f_i's do, $Z(J)$ is actually empty. By the weak Nullstellensatz, this means that J is the whole of $\overline{k}[x_1, \ldots, x_{n+1}]$: in particular, $1 \in J$ and there are polynomials a_i's and b in $\overline{k}[x_1, \ldots, x_{n+1}]$ such that

$$\text{(R)} \qquad 1 = \sum a_i(x_1, \ldots, x_{n+1}) \cdot f_i + b(x_1, \ldots, x_{n+1}) \cdot (x_{n+1}g - 1) \in \overline{k}[x_1, \ldots, x_n, x_{n+1}].$$

Putting $y = 1/x_{n+1}$ and multiplying (R) by a big power of y to get rid of denominators, one obtains a relation

$$\text{(R')} \qquad y^r = \sum c_i(x_1, \ldots, x_n, y) \cdot f_i + d(x_1, \ldots, x_n, y) \cdot (g - y) \in \overline{k}[x_1, \ldots, x_n, y],$$

for some $r \geq 1$. Substituting $y = g$ in (R'), we obtain that

$$g^r = \sum c_i(x_1, \ldots, x_n, g) \cdot f_i \in (f_1, \ldots, f_r) = I,$$

which concludes the proof.

□

1.1.3. Irreducibility, affine varieties. —

Definition 1.12. — An affine algebraic set V is called irreducible if its ideal $I(V)$ is a prime ideal in $\overline{k}[X]$. An affine algebraic variety is an irreducible affine algebraic set.

Recall that an ideal I in a ring R is called prime when the quotient ring R/I is an integral domain. Another way of phrasing this condition is to require that, for all $a, b \in R \smallsetminus I$, $ab \notin I$.

Remark 1.13. — If V is defined over k, we also say that V is absolutely irreducible (or geometrically irreducible) if V is irreducible. Note that it is *not* enough to check that $I(V/k)$ is prime in $k[X]$. On the other hand, if V/k is (absolutely) irreducible (*i.e.* if $I(V) \subset \overline{k}[X]$ is prime), then $I(V/k)$ is a prime ideal of $k[X]$ because $k[X]/I(V/k)$ is a subring of $\overline{k}[X]/I(V)$, which is a domain.

For example, consider $f(x_1, x_2) = x_1^2 + x_2^2 \in k[x_1, x_2]$ (where k is of characteristic $\neq 2$). Then $V = Z(f)$ is an affine algebraic set (in $\mathbb{A}^2$) defined over k, with ideal $I = (f) \subset \overline{k}[x_1, x_2]$. The ideal I is not prime because, denoting by α one of the two square roots of -1 in $\overline{k}$, one has

$$f(x_1, x_2) = (x_1 - \alpha x_2)(x_1 + \alpha x_2) \in \overline{k}[x_1, x_2],$$

and thus I decomposes in a product $I = (x_1 - \alpha x_2) \cdot (x_1 + \alpha x_2)$. However, if $\alpha \notin k$, f is irreducible in $k[x_1, x_2]$ so $I(V/k) = (f) \subset k[x_1, x_2]$ is a prime ideal.

Example 1.14. — The affine space $\mathbb{A}^n$ is irreducible, because its ideal $I(\mathbb{A}^n) = (0) \subset \overline{k}[x_0, \ldots, x_n]$ certainly is prime.

One can give a complete classification of varieties $V \in \mathbb{A}^1$ (exercise).

Example 1.15. — A non-example: let V_1 be the affine set $\subset \mathbb{A}^2$ defined by $x^2 - y^2 = 0$, and let V_2 be the affine set $\subset \mathbb{A}^3$ defined by $z^3 = 0$.

The ideal $I(V_1)$ of V_1 is generated by $x^2 - y^2 = (x - y)(x + y)$ so it can not be prime (because $\overline{k}[x, y]/(x^2 - y^2) \simeq k \times k$). The ideal of V_2 is $(z^3) \subset \overline{k}[x, y, z]$ and, again, it is not prime: the quotient ring $\overline{k}[x, y, z]/(z^3)$ contains nilpotent elements, for example $z \bmod z^3$).

Example 1.16. — Let $f \in k[X]$ be an absolutely irreducible polynomial (that is, not only is f irreducible in $k[X]$, but it remains irreducible in $\overline{k}[X]$). Then, the ideal $I = (f)$ of $\overline{k}[X]$ is prime and the associated algebraic set $V = Z(f) \subset \mathbb{A}^n$ is an affine variety. One often simply writes: "let V be the affine variety defined by

$$V : f(x_1, \ldots, x_n) = 0.''$$

If $n = 2$, such a V is called a plane curve and, in general for $n \geq 3$, a hypersurface.

Example 1.17. — Let $f \in \overline{k}[x]$ be a polynomial in one variable, one can see f as a function $\overline{k} \to \overline{k}$. Let $\Gamma_f \subset \mathbb{A}^2$ be the "graph of f", *i.e.* the set

$$\Gamma_f := \left\{(x, f(x)),\ x \in \overline{k}\right\} \subset \mathbb{A}^2.$$

This is an example of an algebraic variety. Indeed, the ideal of Γ_f in $\overline{k}[x, y]$ is generated by $F(x, y) = y - f(x)$. It is not difficult to check that $F \in \overline{k}[x, y]$ is irreducible, so the ideal it generates is prime.

1.1.4. Coordinate ring(s). — Polynomials in $\overline{k}[X] = \overline{k}[x_1, \ldots, x_n]$ can be seen as functions on $\mathbb{A}^n$: indee, any $f \in \overline{k}[X]$ can be seen as the function $P \mapsto f(P)$. Here, we want to define the natural notion of "functions on an affine variety $V \subset \mathbb{A}^n$": a function on V should also be a polynomial, but we should consider $f, g \in \overline{k}[X]$ as the same function if $f - g$ vanishes on V. This should motivate the following definitions.

Let V be an affine variety, with ideal $I(V) \subset \overline{k}[X]$. We define the affine coordinate ring of V to be the quotient:

$$\overline{k}[V] := \overline{k}[X]/I(V).$$

By construction, the ideal $I(V) \subset \overline{k}[X]$ is prime, so the ring $\overline{k}[V]$ is an integral domain. Its field of fractions will be denoted by $\overline{k}(V)$ and will be called the function field of V.

Since an element $k \in \overline{k}[V]$ is well-defined up to adding a polynomial vanishing on V, it induces a well-defined (polynomial) function $f : V \to \overline{k}$. Note that $\overline{k}[V]$ contains (an isomorphic copy of) $\overline{k}$ (the constant functions). Thus, $\overline{k}[V]$ naturally has the structure of a $\overline{k}$-vector space.

Example 1.18. — Let V be an affine algebraic set, and let $S = \{P_1, \ldots, P_r\}$ be a finite subset of V. By an earlier example, we know that points of $\mathbb{A}^n$ (and thus of V) are algebraic sets. We also know that a finite union of algebraic set is algebraic. So S is an algebraic set, and we denote by $I_S \subset \overline{k}[X]$ its ideal.

From Propositions 1.10 and 1.11, we know that the ideal I_k of $S \smallsetminus \{P_k\}$ contains strictly the ideal I_S of S. Choose an element $f_k \in I_k \smallsetminus I_S$ for all $k \in [1, r]$. Then, it is easy to check that $f_1, \ldots, f_r$ are linearly independent over $\overline{k}$ in the coordinate ring $\overline{k}[V]$ (it follows essentially from the fact that $f_i(P_i) \neq 0$ while $f_i(P_j) = 0$ for all $j \neq i$). This leads to the inequality: $r = \#S \leq \dim_{\overline{k}} \overline{k}[V]$. In particular, if $\overline{k}[V]$ is finite-dimensional over $\overline{k}$, then $\overline{k}(V)/\overline{k}$ is a finite extension of fields and V is a finite set.

Conversely, suppose that $V = S = \{P_1, \ldots, P_r\} \subset \mathbb{A}^n$ is a finite set. Let $P_j = (a_{1j}, \ldots, a_{nj})$ for all $j \in [1, r]$, and consider $g_i := \prod_{j=1}^{r}(x_i - a_{ij})$ for all $i \in [1, n]$. Then the polynomials g_i are in the ideal $I(V)$ of V, and this implies that, in the coordinate ring $\overline{k}[V]$, one can express x_i^r as a $\overline{k}$-linear combinationod $1, \ldots, x_i^{r-1}$. Thus, the finite set $\{\prod_{i=1}^{n} x_i^{e_i},\ 0 \leq e_i \leq r-1\}$ generates the whole vector space $\overline{k}[V]$. In particular, $\overline{k}[V]$ has finite dimension over $\overline{k}$.

Example 1.19. — By an earlier example, there is a bijective correspondence between the points of V and the maximal ideals of $\overline{k}[X]$ containing $I(V)$.

Passing to the quotient ring $\overline{k}[V]$, we obtain a one-to-one correspondence between the points of V and the maximal ideals of $\overline{k}[V]$!

When V/k is an affine variety defined over k, one makes similar definitions:

Definition 1.20. — Let V/k be an affine variety (*i.e.* V is an affine variety defined over k). The affine coordinate ring of V/k is the quotient:

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

The ring $k[V]$ is an integral domain, and its field of fractions will be denoted by $k(V)$ and will be called the k-rational function field of V/k.

Proposition 1.21. — *Let V/k be an affine variety defined over k. Then*

$$\overline{k}[V] = \overline{k} \cdot k[V] \quad \text{and} \quad \overline{k}(V) = \overline{k} \cdot k(V).$$

Proof. — By definition, the ideal $I(V) \subset \overline{k}[X]$ can be generated by polynomials in $k[X]$, so $I(V) = I(V/k) \cdot \overline{k}[X]$. Hence,

$$\overline{k}[V] = \overline{k}[X]/I(V) = \overline{k}[X]/(I(V/k) \cdot \overline{k}[X]) = \overline{k} \cdot k[X]/I(V/k) = \overline{k} \cdot k[V].$$

Finally, note that the fraction field of $\overline{k} \cdot k[V]$ is $\overline{k} \cdot k(V)$. $\square$

If $f \in \overline{k}[X]$ is any polynomial, then G_k acts on f by acting on its coefficients. We denote the action of $\sigma \in G_k$ on f by $f \mapsto f^\sigma$. If V is defined over k, the action of G_k takes $I(V)$ into itself, and we obtain an action of G_k on $\overline{k}[V]$ and $\overline{k}(V)$, also denoted by $f \mapsto \sigma(f)$. For all points $P \in V$, one has $\sigma(f(P)) = \sigma(f)(\sigma(P))$.

Proposition 1.22. — *Let V/k be an affine variety defined over k. Then*

$$k[V] = \left\{f \in \overline{k}[V] : \sigma(f) = f\ \forall \sigma \in G_k\right\},$$

and similarly $k(V) = \left\{f \in \overline{k}(V) : \sigma(f) = f\ \forall \sigma \in G_k\right\}$.

Proof. — Let $A = \left\{f \in \overline{k}[V] : \sigma(f) = f\ \forall \sigma \in G_k\right\}$. It is clear that $k[V] \subset A$, and we need to show that $A \subset \overline{k}[V]$. For $f \in A$, by the preceding proposition, one can write $f = \sum_{i=1}^{r} \alpha_i f_i$, with $f_i \in k[V]$ and $\alpha_i \in \overline{k}$. Denote by E the $\overline{k}$-vector space generated by the f_i's ($i = 1, \ldots, r$).

Up to removing some f_i's, we may assume that $\{f_1, \ldots, f_s\}$ form a basis of E over $\overline{k}$. Then $f = \sum_{i=1}^{s} \beta_i f_i$ for some $\beta_i \in \overline{k}$ and, for all $\sigma \in G_k$,

$$0 = \sigma(f) - f = \sum_{i=1}^{s} (\sigma(\beta_i) - \beta_i) f_i.$$

Since $(f_i)_{i=1}^{s}$ forms a basis of E, one has $\sigma(\beta_i) = \beta_i$ for all $i \in [1, s]$. And this holds for any $\sigma \in G_k$, so β_i actually is an element of k. Thus f has the form $\sum \beta_i f_i$ where $\beta_i \in k$ and $f_i \in k[X]$.

The very same argument gives the same result for $k(V)$. □

1.1.5. Dimension. — Recall the following definition:

Definition 1.23. — Let L/K be an extension of fields. A subset S of L is algebraically independent over K if the elements of S do not satisfy any non-trivial polynomial relation with coefficients in K. In particular, if $S = \{\alpha\}$ with $\alpha \in L$, S is algebraically independent if and only if α is transcendental over K. In general, is S is algebraically independent over K, the elements α of S are necessarily transcendental over K (and also transcendental over all the extensions of K generated by the elements of $S \smallsetminus \{\alpha\}$).

One then defines the transcendence degree of L/K as the largest cardinality of an algebraically independent subset of L over K. A subset S is a transcendance basis of L/K if S is algebraically independant over K and if L is an algebraic extension of the extension $K(S)$ generated by the elements of S.

One can show that every field extension L/K has a transcendence basis, and that all transcendence bases of L/K have the same cardinality: this common cardinality is the transcendence degree of L/K and is denoted $\operatorname{tr.deg}_K L$. An extension L/K is called purely transcendental if there is an algebraically independent subset S of L over K such that $L = K(S)$. A typical example is: let $L = K(x_1, \ldots, x_n)$ be the field of rational functions in n variables $x_1, \ldots, x_n$ with coefficients in K (*i.e.* L is the quotient field of the polynomial ring $K[x_1, \ldots, x_n]$), then $\operatorname{tr.deg}_K L = n$.

For more details about the transcendence degree, you can have a look at the corresponding section in Lang's *Algebra* (Part II, Chapter VIII, §1), or Matsumura's *Commutative Ring Theory.* We use this notion to define the dimension of an affine variety:

Definition 1.24. — Let V be a variety. The dimension of V, denoted by $\dim V$ is the transcendence degree of $\overline{k}(V)$ over $\overline{k}$. The dimension is an integer ≥ 0.

An affine algebraic variety of dimension 1 is called a curve.

Example 1.25. — The dimension of $\mathbb{A}^n$ is n since $\overline{k}(\mathbb{A}^n) = \overline{k}(X_1, \ldots, X_n)$.

Similarly, if $V \subset \mathbb{A}^n$ is an algebraic variety given by a single nonconstant polynomial equation (say, $V : f(x_1, \ldots, x_n) = 0$), then $\dim V = n - 1$.

Remark 1.26. — There is another common definition of the dimension of a variety, as follows:

Definition 1.27. — Let R be a ring (commutative, with identity). The height of a prime ideal $\mathfrak{p}$ of R, denoted by $\operatorname{ht}(\mathfrak{p})$ is the supremum of all $n \in \mathbb{N}$ such that there exists a chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$$

of distinct prime ideals of R. The Krull dimension of R is the supremum of the heights $\operatorname{ht}(\mathfrak{p})$ of all prime ideals $\mathfrak{p}$ of R.

With this notion, if V is an algebraic variety, one defines the dimension of V as the Krull dimension of the coordinate ring $\overline{k}[V]$. These two definitions of dimension actually coincide (see a book of commutative algebra):

Theorem 1.28. — *Let k be a field, R be an integral domain, which is a finitely generated k-algebra, and denote by K the quotient field of R. Then the Krull dimension of R is equal to the transcendence degree of K over k.*

1.1.6. Local rings. — Let V be an affine variety. As was remarked earlier, elements of $f \in \overline{k}[V]$ define polynomial functions $V \to \overline{k}$. Given a point $P \in V$, we define

$$\mathfrak{M}_P := \left\{ f \in \overline{k}[V] : \ f(P) = 0 \right\}.$$

It can be checked that $\mathfrak{M}_P$ is an ideal in $\overline{k}[V]$: indeed, $\mathfrak{M}_P$ is the kernel of the evaluation map $ev_P : f \mapsto f(P)$. Since $ev_P : \overline{k}[V] \to \overline{k}$ is onto, there is an isomorphism $\overline{k}[V]/\mathfrak{M}_P \simeq \overline{k}$. In particular, the ideal $\mathfrak{M}_P$ is maximal.

Definition 1.29. — The local ring of V at P, denoted by $\mathcal{O}_P$ is the localization of $\overline{k}[V]$ at $\mathfrak{M}_P$. That is to say,

$$\mathcal{O}_P = \left\{ F \in \overline{k}(V) : F = f/g \text{ for some } f, g \in \overline{k}[V] \text{ with } g(P) \neq 0 \right\}.$$

Notice that, if $F = f/g \in \overline{k}[V]_P$, then $F(P) = f(P)/g(P)$ is well-defined. The functions $F \in \mathcal{O}_P$ are said to be regular at P (or defined at P). The local ring at P is indeed a local ring, its maximal ideal is $\mathfrak{M}_P$.

There are two equivalent ways to "obtain" $\mathcal{O}_P$:

- start from $\overline{k}[V]$ and localize it at $\mathfrak{M}_P$ as above.
- or start from $\overline{k}[X]$, localize it at $M_P = \left\{ F \in \overline{k}(X) \mid F(P) = 0 \right\}$, and take the quotient of the localized ring by the ideal I_{M_P} ($I = I(V)$ localized at M_P).

1.2. Projective varieties

1.2.1. Projective space. — The projective space is obtained from $\mathbb{A}^n$ by "adding points at infinity". More formally, this is done by considering the set of lines in $\mathbb{A}^{n+1}$ passing through the origin.

Definition 1.30. — The projective space of dimension n over k, denoted by $\mathbb{P}^n$ (or $\mathbb{P}^n(\overline{k})$), is the set of equivalence classes of $(n+1)$-tuples $(x_0, \ldots, x_n) \in \mathbb{A}^{n+1} \smallsetminus \{(0, \ldots, 0)\}$, under the equivalence relation given by:

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \iff \exists \lambda \in \overline{k}^* : x_i = \lambda \cdot y_i \ \forall i.$$

An equivalence class $\{(\lambda x_0, \ldots, \lambda x_n), \ \lambda \in \overline{k}^*\}$ is called a point of $\mathbb{P}^n$ and is denoted by $[x_0 : \ldots : x_n]$. The x_i's are called homogeneous coordinates for P (by which one should understand "a choice of homogeneous coordinates").

Example 1.31. — For $k = \mathbb{R}$, one can draw "pictures" of $\mathbb{P}^1$ and $\mathbb{P}^2$.

The Galois group G_k acts on $\mathbb{P}^n(\overline{k})$ by acting on homogeneous coordinates:

$$\text{for all } \sigma \in G_k \text{ and all } P = [x_0 : \ldots : x_n] \in \mathbb{P}^n, \quad \sigma(P) := [\sigma(x_0) : \ldots : \sigma(x_n)].$$

This action is well-defined and actually is an action. Among others, one needs to check that the definition is independent of choice of homogeneous coordinates. This is done as follows:

$$\sigma([\lambda x_0 : \ldots : \lambda x_n]) = [\sigma(\lambda x_0) : \ldots : \sigma(\lambda x_n)] = [\sigma(\lambda)\sigma(x_0) : \ldots : \sigma(\lambda)\sigma(x_n)] = [\sigma(x_0) : \ldots : \sigma(x_n)].$$

With this definition at hand, it is not difficult to check that one recovers the set of k-rational points on $\mathbb{P}^n$ as the set of fixed points of this action:

$$\mathbb{P}^n(k) = \left\{ P \in \mathbb{P}^n(\overline{k}) : \sigma(P) = P \ \forall \sigma \in G_k \right\}.$$

By construction of $\mathbb{P}^n$, there is a canonical projection $\pi : \mathbb{A}^{n+1} \smallsetminus \{0\} \twoheadrightarrow \mathbb{P}^n$. Notice that $\mathbb{P}^n(k) = \pi(\mathbb{A}^{n+1}(k) \smallsetminus \{0\})$.

Remark 1.32. — Be warned that a point $P = [x_0 : \ldots : x_n] \in \mathbb{P}^n$ is an equivalence class. For example, the condition that P is k-rational does not imply that all x_i's are in k (Example: $[\sqrt{2} : \sqrt{2} : 0] = [1 : 1 : 0]$ is a $\mathbb{Q}$-rational point in $\mathbb{P}^2$, even if $\sqrt{2} \notin \mathbb{Q}$).

However, if $P \in \mathbb{P}^n(k)$, there is an element $\lambda \in \overline{k}$ such that all λx_i are elements of k. This is equivalent to requiring that all the quotients $x_0/x_i, \ldots, x_n/x_i$ are elements of k (for any i with $x_i \neq 0$). For this reason, when $P = [x_0 : \ldots : x_n] \in \mathbb{P}^n$, the field

$$k(P) := k(x_0/x_i, \ldots, x_n/x_i) \qquad \text{for any } i \text{ with } x_i \neq 0,$$

is called the minimal field of definition for P (over k). The extension $k(P)/k$ is finite, and one calls its degree the degree of P. (Check that these definitions make sense, see [**NX09**, Rk. 2.1.10, p. 36]). One can show that $k(P)$ is the subfield of $\overline{k}$ that is fixed by the subgroup $\{\sigma \in G_k : \sigma(P) = P\}$ of G_k (exercise).

As in the case of $\mathbb{A}^n$, one define closed points of $\mathbb{P}^n$ over k to be sets of the form $\{\sigma(P), \sigma \in G_k\}$ for some point $P \in \mathbb{P}^n$. Here too, two points in a closed point over k are called conjugate (over k).

Remark 1.33. — If $k = \mathbb{F}_q$, note that closed points are finite subsets of $\mathbb{P}^n$. Indeed, if $P = [x_0 : \ldots : x_n] \in \mathbb{P}^n$, then for each $i \in [0, n]$, there exists $m_i \geq 1$ such that $a_i \in \mathbb{F}_{q^{m_i}}$. Choose m to be a common multiple of all m_i's (so that $\mathbb{F}_{q^m}/\mathbb{F}_q$ is a finite extension containing all the $\mathbb{F}_{q^{m_i}}$ as subfields). Then P is a $\mathbb{F}_{q^m}$-rational point of $\mathbb{P}^n$, and the corresponding closed point satisfies:

$$\#\{\sigma(P),\ \sigma \in \mathrm{Gal}_{\mathbb{F}_q}\} = \#\{\sigma(P),\ \sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)\} \leq \#\,\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = m.$$

Example 1.34. — Again, assume that $k = \mathbb{F}_q$ and denote by $\mathrm{Fr}_q : \overline{k} \to \overline{k}$ the Frobenius morphism, $x \mapsto x^q$. One can check that

$$\mathbb{P}^n(\mathbb{F}_q) = \left\{P \in \mathbb{P}^n(\overline{\mathbb{F}_q}) : \mathrm{Fr}_q(P) = P\right\}.$$

1.2.2. Projective sets. — As in the case of $\mathbb{A}^n$, we now define the subsets of $\mathbb{P}^n$ that we're interested in.

Definition 1.35. — A polynomial $F \in \overline{k}[y_0, \ldots, y_n] = \overline{k}[Y]$ is said to be homogeneous of degree d if and only if

$$\forall \lambda \in \overline{k}, \qquad F(\lambda y_0, \ldots, \lambda y_n) = \lambda^d \cdot F(y_0, \ldots, y_n).$$

An ideal I of $\overline{k}[y_0, \ldots, y_n]$ is homogeneous if it can be generated by homogeneous polynomials (not necessarily all of the same degree).

Let F be a homogeneous polynomial and let $P \in \mathbb{P}^n$. It makes sense to ask whether $F(P) = 0$ since the answer is independent of the choice of homogeneous coordinates for P. So, to each homogeneous ideal, we can associate a subset of $\mathbb{P}^n$ by the rule:

$$Z_h(I) := \{P \in \mathbb{P}^n : F(P) = 0 \text{ for all homogeneous } F \in I\}.$$

Definition 1.36. — A projective algebraic set is any set of the form $Z_h(I)$ for a homogeneous ideal I. If V is any projective algebraic set, the homogeneous ideal of V, denoted by $I(V)$ is the ideal of $\overline{k}[Y]$ generated by

$$\left\{F \in \overline{k}[Y] : F \text{ is homogeneous and } F(P) = 0\ \forall P \in V\right\}.$$

By definition, the ideal $I(V)$ of an algebraic set is homoegeneous. We say that such a V is defined over k (denoted V/k) if its ideal $I(V)$ can be generated by homogeneous polynomials in $k[Y]$. If V is defined over k, then the set of k-rational points of V is the set $V(k) := V \cap \mathbb{P}^n(k)$.

As usual, $V(k)$ may also be described as $V(k) = \{P \in V : P^\sigma = P\ \forall \sigma \in G_k\}$.

Example 1.37. — A line in $\mathbb{P}^2$ is an algebraic set given by a single linear equation (homogeneous of degree 1):

$$ax_0 + bx_1 + cx_2 = 0,$$

with $a, b, c \in \overline{k}$, not all zero. If, say, $c \neq 0$, then such a line is defined over any field containing a/c and b/c. More generally, a hyperplane in $\mathbb{P}^n$ is given by an equation

$$a_0x_0 + a_1x_1 + \cdots + a_nx_n = 0,$$

with $a_i \in \overline{k}$ not all zero.

Example 1.38. — Let V be the algebraic set in $\mathbb{P}^2$ given by the single equation

$$V : x^2 + y^2 = z^2.$$

Then, for any field with $\mathrm{char}(k) \neq 2$, the set $V(k)$ is isomorphic to $\mathbb{P}^1(k)$, for example by the map

$$\mathbb{P}^1(k) \to V(k), \quad [s : t] \mapsto \left[s^2 - t^2 : 2st : s^2 + t^2\right].$$

(see below for the precise definition of isomorphism). What does V look like when $k = \mathbb{R}$? (and when $k = \mathbb{F}_2$?)

Example 1.39. — The projective space of dimension n is a projective algebraic set, the empty set too. If $P \in \mathbb{P}^n$ is a point, the singleton $\{P\}$ is a projective set. Indeed, choose homogeneous coordinates $P = [a_0 : \ldots : a_n]$ for P: one of the a_i is nonzero and up to renumbering we can assume that $a_0 \neq 0$. Consider the ideal I_P generated by the homogeneous $n+1$ polynomials $c_i = a_0X_i - a_iX_0 \in \overline{k}[X_0, \ldots, X_n]$. Then it is easy to check that $Z(I_P) = \{P\}$ and that the ideal I_P does not depend on the choice of homogeneous coordinates.

The following proposition is the projective counterpart of the corresponding proposition about affine sets:

Proposition 1.40. — *We write $\overline{k}[Y]$ for $\overline{k}[y_0, \ldots, y_n]$.*

(i) Let S be a nonempty set of homogeneous polynomials in $\overline{k}[Y]$. If I is the ideal generated by S, then $Z_h(S) = Z_h(I)$.

(ii) For any two sets $S' \subset S$ of homogeneous polynomials in $\overline{k}[Y]$, we have $Z_h(S') \supset Z_h(S)$.

(iii) If S, S' are two nonempty sets of homogeneous polynomials of $\overline{k}[Y]$, then $Z_h(S \cup S') = Z_h(S) \cap Z_h(S')$.

(iv) Any intersection of projective sets is a projective set.

(v) For any homogeneous polynomials $F, G \in \overline{k}[Y]$, we have $Z_h(F \cdot G) = Z_h(F) \cup Z_h(G)$. More generally, if S, S' are two nonempty sets of homogeneous polynomials in $\overline{k}[Y]$ and if we let $S \cdot S' = \{FG, F \in S, G \in S'\}$, then $Z_h(S \cdot S') = Z_h(S) \cup Z_h(S')$.

(vi) Any finite union of projective algebraic sets is a projective algebraic set.

(vii) $Z_h(0) = \mathbb{P}^n$ and $Z_h(1) = \varnothing$.

Proof. — Exercise. □

Proposition 1.41. — *Let V be a projective algebraic set.*

(i) There exists a finite set $S_0 \subset \overline{k}[X]$, formed of homogeneous polynomials, such that $V = Z_h(S_0)$.

(ii) The projective zero set of $I(V)$ is V: $Z_h(I(V)) = V$.

(iii) If $V = Z_h(I)$ for some homogeneous ideal I of $\overline{k}[X]$, then the ideal $I(V)$ of V is the radical of I:

$$I(Z_h(I)) = \mathrm{rad}(I) := \left\{f \in \overline{k}[X] : \exists r \geq 1, f^r \in I\right\}.$$

Note that the radical of a homogeneous ideal is again a homogeneous ideal.

1.2.3. Projective varieties. —

Definition 1.42. — A projective variety is a projective algebraic set V whose homogeneous ideal $I(V)$ is a prime ideal of $\overline{k}[Y]$.

Which one of the examples above is a projective variety? Find a projective algebraic set that is not projective variety (you can draw inspiration from the corresponding section about affine sets).

Note the following fact: if I is a homogeneous ideal in $\overline{k}[Y]$, then I is prime if and only if, for all $F, G \in \overline{k}[Y]$ homogeneous of the same degree, one has $FG \in I \Rightarrow F \in I$ or $G \in I$ (you might want to decompose any polynomial $f \in \overline{k}[Y]$ into a sum $f = F_0 + \cdots + F_d$ where F_i is homogeneous of degree i, and prove by induction that, if $f \in I$ then $F_i \in I$ for all i). Exercise: if I is a homogeneous ideal, then its radical is also homogeneous.

1.2.4. Covering $\mathbb{P}^n$ by affine pieces. — The projective space $\mathbb{P}^n$ contains many copies of $\mathbb{A}^n$, which together cover the whole of $\mathbb{P}^n$. This fact is useful to extend to projective varieties the definitions of some properties of affine varieties.

For each $0 \leq i \leq n$, consider the map

$$\phi_i : \mathbb{A}^n \hookrightarrow \mathbb{P}^n, \quad (y_1, \ldots, y_n) \mapsto [y_1 : \ldots : y_{i-1} : 1 : y_i : \ldots : y_n].$$

Clearly, ϕ_i is injective and "defined over k" (in the sense that, for all $P \in \mathbb{A}^n$ and all $\sigma \in G_k$, $\sigma(\phi_i(P)) = \phi_i(\sigma(P))$). We let $H_i \subset \mathbb{P}^n$ denote the hyperplane in $\mathbb{P}^n$ given by $X_i = 0$:

$$H_i = \{P = [x_0 : x_1 : \ldots : x_n] \in \mathbb{P}^n : x_i = 0\},$$

and we let U_i denote the complement of H_i in $\mathbb{P}^n$:

$$U_i = \{P = [x_0 : x_1 : \ldots : x_n] \in \mathbb{P}^n : x_i \neq 0\} = \mathbb{P}^n \smallsetminus H_i.$$

Then, there is a natural bijection

$$\phi_i^{-1} : U_i \to \mathbb{A}^n, \qquad [x_0 : \ldots : x_{i-1} : x_i : x_{i+1} : \ldots : x_n] \mapsto \left(\frac{x_0}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right).$$

Note that this map is well-defined since, for any point in $\mathbb{P}^n$ with $x_i \neq 0$, the ratios x_j/x_i are well-defined (independent of a choice of homogeneous coordinates). For a given i, we identify $\mathbb{A}^n$ with $U_i \subset \mathbb{P}^n$ via the map ϕ_i (usually, implicitely). Notice that the sets $U_0, U_1, \ldots, U_n$ cover the whole of $\mathbb{P}^n$.

1.2.5. Dehomogenizing and homogenizing. — Let $F \in \overline{k}[y_0, \ldots, y_n]$ be a homogeneous polynomial. For any $k \in [0, n]$, one defines the dehomogenisation of F in the k-th variable to be

$$F_{dh}(y_0, \ldots, y_n) := F(y_0, \ldots, y_{k-1}, 1, y_{k+1}, \ldots, y_n),$$

a polynomial in n variables. Conversely, if $k \in [1, n]$ and if $f \in \overline{k}[x_1, \ldots, x_n]$ is a polynomial in n variables, we define its homogenisation with respect to the k-th variable to be

$$f^h(x_0, \ldots, x_n) := x_k^r \cdot f\left(\frac{x_0}{x_k}, \ldots, \frac{x_{k-1}}{x_k}, \frac{x_{k+1}}{x_k}, \ldots, \frac{x_n}{x_k}\right),$$

where r is the smallest integer such that f^h is a polynomial. These two processes are somehow "inverse to each other":

Proposition 1.43. — *Let F, G be two homogeneous polynomials in $\overline{k}[x_0, \ldots, x_n]$, and f, g be two polynomials in $\overline{k}[x_1, \ldots, x_n]$. Then, for a given $k \in [0, n]$ or $[1, n]$:*

(i) $(F \cdot G)_{dh} = F_{dh} \cdot G_{dh}$ *and* $(F + G)_{dh} = F_{dh} + G_{dh}$.

(ii) $(f \cdot g)^h = f^h \cdot g^h$ *and* $x_k^t \cdot (f + g)^h = x_k^{d_g} \cdot f^h + x_k^{d_f} \cdot g$ *where d_f (resp. d_g) is the degree of f (resp. g) in the k-th variable and $t = d_f + d_g - d_{f+g}$.*

(iii) $(f^h)_{dh} = f$.

(iv) if F is non zero and r is the maximal power of x_k dividing F, then $x_k^r \cdot (F_{dh})^h = F$.

Proof. — Exercise. □

An ideal I of $\overline{k}[X]$ is called homogeneous if it can be generated by homogeneous polynomials.

Lemma 1.44. — *(i) An ideal I is homogeneous if and only if it has the following property: for every $f = \sum f_d$ in I, where all the f_d are homogeneous of degree d, we also have $f_d \in I$.*

(ii) A homoegeneous ideal I is prime if and only if: for all F, G homogeneous polynomials in $\overline{k}[X]$, if $FG \in I$ then either $F \in I$ or $G \in I$.

(iii) Let I be an ideal in $\overline{k}[x_1, \ldots, x_n]$, and let I^h be the ideal of $\overline{k}[x_0, \ldots, x_n]$ generated by the homogenisation of polynomials in I (with respect to the 0-th variable say). Then I is prime if and only if I^h is prime.

1.2.6. Affine varieties and projective varieties. — Let V be an affine algebraic subset of $\mathbb{A}^n$, and $I = I(V) \subset \overline{k}[x_1, \ldots, x_n]$ be its ideal. Let $I^h \subset \overline{k}[x_0, \ldots, x_n]$ be the ideal generated by the homogeneized polynomials f^h with $f \in I$ (with respect to the k-th variable, say). One can naturally define a projective algebraic variety from V:

Definition 1.45. — Let $V \subset \mathbb{A}^n$ be an affine algebraic set with ideal $I(V)$. Consider V as a subset of $\mathbb{P}^n$ via the composition $V \hookrightarrow \mathbb{A}^n \to \mathbb{P}^n$ of the inclusion $V \subset \mathbb{A}^n$ with $\phi_k : \mathbb{A}^n \to \mathbb{P}^n$. The projective closure of V, denoted by $\overline{V}$, is the projective algebraic set whose homogeneous ideal $I(\overline{V})$ is generated by

$$\left\{ f^h(X),\ f \in I(V) \right\}.$$

Conversely, let W be a projective algebraic set with homogeneous ideal $J := I(W) \subset \overline{k}[x_0, \ldots, x_n]$. Let J_{dh} be the ideal of $\overline{k}[x_1, \ldots, x_n]$ generated by the F_{dh}'s when F runs through homogeneous polynomials in J. We define $V := Z(J_{dh}) \subset \mathbb{A}^n$. Then $W \cap \mathbb{A}^n$ (by which we mean $\phi_k^{-1}(W \cap U_k)$ for some chosen k) is an affine algebraic set with ideal $I(W \cap \mathbb{A}^n) \subset \overline{k}[Y]$ given by:

$$I(W \cap \mathbb{A}^n) = \{ f(Y_1, \ldots, Y_{k-1}, 1, Y_{k+1}, \ldots, Y_n) : f \in I(W) \} = J_{dh}.$$

Since the subsets U_k cover $\mathbb{P}^n$, any projective variety $W \subset \mathbb{P}^n$ is covered by its subsets $W \cap U_0$, $W \cap U_2$, ..., $W \cap U_n$ and each of these sets is an affine algebraic variety in $\mathbb{A}^n$ via an appropriate map ϕ_k (draw a picture).

Example 1.46. — Start with the affine variety $V \subset \mathbb{A}^2$ defined by

$$V : y^2 = x^3 + x, \qquad i.e.\ V : y^2 - (x^3 + x) = 0.$$

We put $f(x, y) = y^2 - (x^3 + x)$. There are three embeddings $\phi_i : \mathbb{A}^2 \to \mathbb{P}^2$.

(1) First we consider $\phi_2 : \mathbb{A}^2 \to \mathbb{P}^2$ (sending (x, y) to $[x : y : 1]$). To see what W is, we need only compute the homogeneization of f with respect to x_2:

$$F := f^h(x_0, x_1, x_2) = x_2^r f\left(\frac{x_0}{x_2}, \frac{x_1}{x_2}\right) = x_2^r \left(\frac{x_1^2}{x_2^2} - \frac{x_0^3}{x_2^3} - \frac{x_0}{x_2}\right) = x_1^2 x_2 - x_0^3 - x_0 x_2^2,$$

because the smallest r such that F is a polynomial is $r = 3$. So $W_2 \subset \mathbb{P}^2$ associated to V in this embedding is given by

$$W_2 = \left\{ [x_0 : x_1 : x_2] \in \mathbb{P}^2 :\ x_1^2 x_2 - x_0^3 - x_0 x_2^2 = 0 \right\}.$$

One recovers V by looking at $W_2 \cap \{x_2 = 1\} = W_2 \cap \{x_2 \neq 0\}$, *i.e.* by substituting 1 for x_2 in the equation of W_2... which is exactly the process of dehomogeneizing F with respect to its third variable! Now, how much does W_2 differ from V? Since we already know that $V = W_2 \cap \{x_2 \neq 0\}$, the extra points we added in passing from V to W_2 are exactly $W_2 \cap \{x_2 = 0\}$. Substituting 0 for x_2 in the equation of W_2, we find that $W_2 \cap \{x_2 = 0\} = \{[0 : 1 : 0]\}$ (this is called the point at infinity of V).

(2) The same process repeats for ϕ_1. This time, $\phi_1 : \mathbb{A}^2 \to \mathbb{P}^2$ is given by $(x, y) \mapsto [x : 1 : y]$ and the computation of the homogeneization of f in the second variable leads to:

$$W_1 = \left\{[x_0 : x_1 : x_2] \in \mathbb{P}^2 :\ x_2^2 x_1 - x_0^3 - x_0 x_1^2 = 0\right\}.$$

Again, we recover V from W_1 by substituting 1 for x_1.

(3) you can work out the details for $\phi_0 : \mathbb{A}^2 \to \mathbb{P}^2$, $(x, y) \mapsto [1 : x : y]$.

Remark 1.47. — In this remark, we work things out for $k = 0$ (but of course, the same computations would hold for any k). Let $W = Z_h(J)$ be an algebraic subset of $\mathbb{P}^n$, and assume that $W \subset U_0$, then it is easy to show that

$$\phi_0^{-1}(W) = \text{“}W \cap U_0\text{”} = Z\left(\{f(1, y_1, \ldots, y_n),\ f \in J \text{ homogeneous polynomial }\}\right).$$

Conversely, let $V = Z(I) \subset \mathbb{A}^n$ be an affine algebraic set. Then one can show:

$$\phi_0(V) = U_0 \cap Z_h\left(\left\{x_0^{\deg f} f(x_1/x_0, \ldots, x_n/x_0),\ f \in I\right\}\right).$$

The following proposition shows that one can easily pass from affine varieties to projective varieties, and vice versa:

Proposition 1.48. — *(i) Let $V \subset \mathbb{A}^n$ be an affine algebraic subset. Then $\phi_k(V) = V^h \cap U_k$ and $(V^h)_{dh} = V$.*

(ii) If V is irreducible (in $\mathbb{A}^n$), then V^h is irreducible (in $\mathbb{P}^n$).

(iii) If $W \subset \mathbb{P}^n$ is a projective algebraic subset such that $W \cap H_k \subsetneq W$ (i.e. $W \cap U_k \neq \varnothing$), then W_{dh} is a (strict) algebraic subset of $\mathbb{A}^n$ and $(W_{dh})^h = W$.

Proof. — (i) is a direct consequence of the proposition in the last subsection. Item (ii) comes from the fact that, if I denotes the ideal of V, then a homogeneous polynomial F is an element of I^h if and only if $F_{dh} \in I$. This fact implies that I^h is prime as soon as I is prime.

For item (iii), we assume that V is irreducible. Then, obviously $\phi_k(V_h) \subset V$ and we need to show that $V \subset (V_{dh})^h$, *i.e.* that $I(V_{dh})^h \subset I(V)$. This is done by using Hilbert's Nullstellensatz: let $f \in I(V_{dh})$, then there exists $N \geq 1$ such that $f^N \in I(V)_{dh}$. So $x_k^t \cdot (f^N)^h$ is an element of $I(V)$ (for some t, see formulae above), where $I(V)$ is prime: thus $x_k^t \in I(V)$ or $(f^N)^h = (f^h)^N \in I(V)$. Since we assumed that V is not contained in H_k, we have $x_k \notin I(V)$. This proves that $f^h \in I(V)$ and concludes the proof.

(see also [**Har77**, I.2.3]). □

Remark 1.49. — In view of this proposition, each affine variety may be identified with a unique projective variety. Notationally, since it is easier to deal with affine coordinates, we will often say "let W be a projective variety" and write down some inhomogenous equations. The understanding is that W is the projective closure of the indicated affine variety V. The points of $W \smallsetminus V$ are called the points at infinity of W.

Example 1.50. — Let V be the projective variety defined by the equation

$$V : Y_2^2 = Y_1^3 + 17.$$

This really means that V is the variety in $\mathbb{P}^2$ given by the homogeneous equation

$$X_1^2 X_2 = X_0^3 + 17X_2^2,$$

the identification being $Y_1 = X_0/X_2$ and $Y_2 = X_1/X_2$. This variety has one point at infinity, namely $[0 : 1 : 0]$, obtained by setting $X_2 = 0$.

1.2.7. Further properties. — Many properties (so-called "local properties") of a projective variety V can be now defined in terms of one of the affine parts $V \cap \mathbb{A}^n$ of V.

Definition 1.51. — The function field of V, denoted by $\overline{k}(V)$, is the function field of $V \cap \mathbb{A}^n$. Note that, for different choices of $\mathbb{A}^n$, the different $\overline{k}(V)$ are canonically isomorphic, so we may identify them.

We will say more about function fields in the second chapter. For now, we use this definition to recover the notion of dimension for projective varieties:

Definition 1.52. — Let V be a projective variety and choose one of the embeddings $\phi_k : \mathbb{A}^n \subset \mathbb{P}^n$ such that $V \cap \mathbb{A}^n := \phi_k^{-1}(V) \neq \varnothing$. The dimension of V is the dimension of $V \cap \mathbb{A}^n$ (as an affine algebraic variety).

Of course, one needs to check that this definition does not depend on the choice of an embedding: since the dimension of $V \cap \mathbb{A}^n$ (an affine variety) is the transcendence degree of its function field $\overline{k}(V \cap \mathbb{A}^n)$, and since the different function fields thus obtained for different choices of ϕ_i are all isomorphic, the transcendence degree of $\overline{k}(V)$ over k is independent of choices.

Remark 1.53. — Let us give an alternative description of the function field of $\mathbb{P}^n$: it may also be described as the subfield of $\overline{k}(\mathbb{A}^n) = \overline{k}(X_0, \dots, X_n)$ consisting of rational functions f/g for which f and g are homogeneous polynomials of the same degree. Such an expression f/g gives a well-defined function on $\mathbb{P}^n$ at all points P where $g(P) \neq 0$.

Remark 1.54. — Similarly, the function field of a projective variety V is the field of rational functions $F = f/g$ such that : f and g are homogeneous of the same degree, $g \notin I(V)$, two functions f_1/g_1 and f_2/g_2 are identified if $f_1g_2 - f_2g_1 \in I(V)$. In other words, if V is a projective variety and its (homogeneous) ideal is $I(V)$ then define $R := \overline{k}[x_0, \dots, x_n]/I(V)$, this ring R is an integral domain and we can consider its quotient field $\overline{k}_h(V)$. The ring of rational functions on V is then

$$\overline{k}(V) = \left\{F \in \overline{k}_h(V) : \ \exists f, g \in R \text{ homogeneous of the same degree such that } F = f/g\right\}.$$

Be aware that $\overline{k}(V)$ is (in general) a strict subfield of $\overline{k}_h(V)$ containing k.

Definition 1.55. — The local ring of V at P, denoted by $\overline{k}[V]_P$, is the local ring of $V \cap \mathbb{A}^n$ at P (we choose an embedding $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$ such that $P \in V \cap \mathbb{A}^n$). A function $F \in \overline{k}(V)$ in the function field of V is regular at P (or defined at P) if it is in the local ring $\mathcal{O}_P$ (of $V \cap \mathbb{A}^n$. In which case, it makes sense to evaluate F at P.

You should check that all these definition actually do not depend on the choice of $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$. One can give a description of the local rings $\mathcal{O}_P$ along the lines of the previous remark.