MATH-GA 2150.001 : Advanced Topics in Algebra (Introduction to Algebraic Geometry and Elliptic Curves)

ALENA PIRUTKA

Contents

1 Affine and projective algebraic varieties **2**
1.1 Affine varieties, Nullstellensatz 2
1.1.1 Finiteness properties 6
1.2 The structure of maximal ideals 7
1.3 Additional exercises 1 9

Chapter 1

Affine and projective algebraic varieties

1.1 Affine varieties, Nullstellensatz

In this section we introduce affine algebraic varieties : the base objects of study in algebraic geometry. The main theorem of this section is the famous Hilbert's Nullstellensatz on zero locus of a system of polynomial equations over an algebraically closed field.

Let k be a field. The main cases of interest for this course is $k = \mathbb{C}$, k algebraically closed, $k = \mathbb{R}$, $k = \mathbb{Q}$ or a finite extension (a number field), k finite.

We identify the affine space $\mathbb{A}^n_k$ with the set k^n.

An *affine algebraic variety* over k is the subset of k^n defined as zero locus of a system of polynomials in $k[x_1, \ldots, x_n]$:

Definition 1.1.1. For I an ideal in $k[x_1, \ldots, x_n]$ we denote

$$V(I) = \{x = (x_1, \ldots, x_n) \in k^n \mid f(x) = 0 \, \forall f \in I\}$$

the **affine algebraic variety** defined by I.

If $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ is a finite family of polynomials, we write $V(f_1, \ldots, f_m)$ instead of $V((f_1, \ldots, f_m))$ for the affine variety defined by the ideal generated by $f_1, \ldots, f_m$.

Recall that the ring $k[x_1, \ldots, x_n]$ is noetherian : any ideal I of this ring is generated by a finite number of elements, so that any algebraic variety is of the form $V(f_1, \ldots, f_m)$ as above.

Example 1.1.2. In the affine plane $\mathbb{A}^2_k$ we have $V(x, y) = (0, 0)$, $V(x - 1, y - 2) = (1, 2)$, $V(y^2 - x^3 + x)$ is a curve (we will see that it is an example of an elliptic curve).

Remark 1.1.3. In a more advanced course on algebraic geometry an affine variety corresponds to an ideal in $k[x_1, \ldots, x_n]$; saing that $X = V(I)$ is an affine variety means that we recall the data of X and I. Speaking about the *set of rational points* $X(k) \subset k^n$ of X means that we consider the set $X(k) = V(I)$ but we «forget» the data of I. If K/k is an extension of k we denote $X(K) = V(I_K) \subset K^n$ for $I_K \subset K[x_1, \ldots, x_n]$ the idéal generated by I.

Note that if k is not algebraically closed, the set $V(I)$ could be empty: for example, for $I = (x^2 + y^2 + 1) \subset \mathbb{R}[x, y]$. If $k = \mathbb{C}$ and $I = (f)$ with $f \in k[x]$ a non constant polynomial, the fundamental theorem of algebra says that $V(I)$ is not empty. In the case of polynomials in many variables, we have an analogous statement:

Theorem 1.1.4. [weak Nullstellensatz] *Let k be an algebraically closed field and let I be an ideal of $k[x_1, \ldots, x_n]$, $I \neq (1)$. The set $V(I)$ is nonempty.*

Proof. This theorem follows from a theorem on the structure of maximal ideals in $k[x_1, \ldots, x_n]$, that we give below, for the proof see the next section. In fact, the ideal I is contained in a maximal ideal $\mathfrak{m}$ (Krull's theorem), and we can write $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ by 1.1.5. As $V(\mathfrak{m})$ is nonempty, we see that $V(I)$ is nonempty as well. □

Theorem 1.1.5. *Let k be an algebraically closed field. Any maximal ideal $\mathfrak{m}$ in $k[x_1, \ldots, x_n]$ is of the form $\mathfrak{m} = (x_1 - a_1, \ldots, x_n - a_n)$ with $a_1, \ldots, a_n \in k$.*

Definition 1.1.6. If X is a subset of k^n we denote

$$I(X) = \{f \in k[x_1, \ldots, x_n],\ f(x) = 0\, \forall x \in X\}$$

the ideal of X.

For example, if $X = \{0, 0\} \subset \mathbb{A}^2_k$, then $I(X)$ is the ideal of polynomials in $k[x, y]$ with zero constant term.

Note that $I(X)$ is indeed an ideal: if $f \in I(X)$ and $g \in k[x_1, \ldots, x_n]$, then the polynomial fg vanishes at every point of X.

Proposition 1.1.7. *1. Let I, J be the ideals of $k[x_1, \ldots, x_n]$.*

- *(a) $I \subset J \Rightarrow V(J) \subset V(I)$;*
- *(b) $V(I) \cap V(J) = V(I + J)$;*
- *(c) $V(I) \cup V(J) = V(I \cdot J) = V(I \cap J)$.*

2. If $X \subset Y$ are subsets of k^n, then $I(Y) \subset I(X)$.

3. If J is an ideal in $k[x_1, \ldots, x_n]$, then $J \subseteq I(V(J))$.

4. If $X \subset k^n$ is an algebraic variety, then $X = V(I(X))$.

Proof. We give a proof for *1(b)* et *1(c)*, the other properties follow immediately from the definitions.

1(b). Let $x \in V(I) \cap V(J)$. We then have $f(x) = 0$ and $g(x) = 0$ for all $f \in I$ and $g \in J$. We deduce $h(x) = 0$ for all $h \in I + J$. In the other direction, if $h(x) = 0$ for all $h \in I + J$, we have in particular that $f(x) = 0$ and $g(x) = 0$ for all $f \in I$ and $g \in J$, so that $x \in V(I) \cap V(J)$.

1(c). Let $x \in V(I) \cup V(J)$. We then have either $f(x) = 0$ for all $f \in I$, or $g(x) = 0$ for all $g \in J$. We deduce $h(x) = 0$ for all $h \in I \cdot J$ (resp. for all $h \in I \cap J$). In the other direction, assume $h(x) = 0$ for all $h \in I \cdot J$ (resp. for all $h \in I \cap J$). If $x \notin V(I)$, there exists $f \in V(I)$ such that $f(x) \neq 0$. Let $g \in J$. As $fg \in I \cdot J$ (resp. in $I \cap J$), we deduce $g(x) = 0$, so that $x \in V(J)$. □

The previous properties imply that the sets $V(I)$ are the closed sets of some topology, called **Zariski topology** on k^n. If $X \subset k^n$ is an affine algebraic variety, we call the induced topology on X **Zariski topology on** X as well.

Note that we do not necessarily have the equality $J = I(V(J))$. In fact, there could be two types of problems:

1. for $J = (x^2)$ an ideal in $k[x]$, we have $I(V(J)) = (x)$;
2. if k is not algebraically closed : for example, for $J = (x^2 + y^2)$ an ideal in $\mathbb{R}[x, y]$, we have $I(V(J)) = (x, y)$.

Hilbert theorem of zeros says that these two problems are essentially the only ones.

Recall the notion of a radical of an ideal:

Definition 1.1.8. If A is a (commutative) ring and $I \subset A$ is an ideal, the **radical of** I is

$$\sqrt{I} = \{a \in A \,|\, a^m \in I \text{ for some } m \geq 1\}.$$

One checks that $\sqrt{I}$ is also an ideal of A. The ideal I is **radical** if $I = \sqrt{I}$.

Example 1.1.9. For $J = (x^2)$ an ideal in $k[x]$, we have $\sqrt{J} = (x)$.

Theorem 1.1.10. [Nullstellensatz] *Let k be an algebraically closed field and let J be an ideal in $k[x_1, \ldots, x_n]$. Then $I(V(J)) = \sqrt{J}$.*

Proof. We deduce the theorem from its weak version. This argument is due to Artin and Tate. Let $f \in I(V(J))$, so that f vanishes at all common zeros of elements of J. Consider the ideal J' of $k[x_1, \ldots, x_{n+1}]$:

$$J' = (x_{n+1}f - 1, J).$$

By construction, $V(J') = \emptyset$. Using weak Nullstellensatz, $1 \in J'$, that is, we can write in the quotient ring $A = k[x_1, \ldots, x_{n+1}]/(x_{n+1}f - 1)$:

$$1 = \sum b_i a_i$$

with $b_i \in J, a_i \in A$, so that (writing by degrees of x_{n+1})

$$1 = c_0 + c_1 x_{n+1} + \ldots + c_m x_{n+1}^m$$

with $c_i \in J$. As $x_{n+1}f - 1 = 0$ in A, we deduce

$$f^m = c_0 f^m + c_1 f^{m-1} + \ldots + c_m,$$

that is, $f^m - c = 0$ with $c = c_0 f^m + c_1 f^{m-1} + \ldots + c_m \in J$. As the natural map $k[x_1, \ldots, x_n] \to A$ is injective, we deduce $f^m - c = 0$ in $k[x_1, \ldots, x_n]$, so that $f^m \in J$. □

Remark 1.1.11. Note that if $J = I(X)$, then $J = \sqrt{J}$: in fact, if $f^m \in J$, then $(f(x))^m = 0$ for all $x \in X$, so that $f(x) = 0$ for all $x \in X$, which implies that $f \in J$.

For the moment we introduced the objects of the category of affine algebraic varieties over k. One is then also interested to understand the morphisms between these objects.

Definition 1.1.12. Let X be an algebraic variety in k^n. A **polynomial function** on X is the restriction of a function in $k[x_1, \ldots, x_n]$ to X. If Y is another algebraic variety in k^m, the function $f : X \to Y$ is **polynomial** if every coordinate function is.

Note that a polynomial function $X \to Y$ is continuous for Zariski topology: if $Z = V(I) \cap Y \subset Y$ is closed, where I is an ideal in $k[y_1, \ldots, y_m]$ generated by $(h_1, \ldots h_r)$, then $f^{-1}(Z) = X \cap V(h_1 \circ f, \ldots h_r \circ f)$ is closed in X.

Proposition 1.1.13. *The algebra of polynomial functions on X is the algebra*

$$k[X] := k[x_1, \ldots, x_n]/I(X).$$

Proof. Let $f, g \in k[x_1, \ldots, x_n]$ be two polynomials inducing the same polynomial function on X. We then have $f - g = 0$ at all points of X, so that $f - g \in I(X)$. □

Let $f : X \to Y$ be a polynomial map between two affine varieties defined over a field k. We define the map $f^* : k[Y] \to k[X]$ by

$$f^*(\bar{P}) = \overline{P \circ f}$$

where $\bar{P}$ (resp. $\overline{P \circ f}$) is the class of P (resp. $P \circ f$) in $k[Y]$ (resp. $k[X]$). This map is well defined : if $P_1 - P_2 \in I(Y)$ then for all $x \in X$ we have $P_1(f(x)) = P_2(f(x))$ as $f(x) \in Y$.

Proposition 1.1.14. *Let X, Y be two affine varieties. Let $g : k[Y] \to k[X]$ be a morphism of algebras. There exists a polynomial map $f : X \to Y$ such that $g = f^*$.*

Proof. We write $k[X] = k[x_1, \ldots, x_n]/I(X)$ and $k[Y] = k[y_1, \ldots, y_m]/I(Y)$ by the previous proposition. Let G be the composition

$$k[y_1, \ldots, y_m] \to k[y_1, \ldots, y_m]/I(Y) \xrightarrow{g} k[x_1, \ldots, x_n]/I(X).$$

Let $f_i = G(y_i)$. Let $P_i \in k[x_1, \ldots, x_n]$ such that $f_i = \bar{P}_i$. Write $f = (P_1, \ldots, P_m)$. As $f^*(\bar{y}_i) = \bar{P}_i = g(\bar{y}_i)$ by construction, it is enough to see that f has its values in Y.

Let $x = (a_1, \ldots, a_n) \in X$ and let $h \in I(Y)$. We have

$$h(f(x)) = h(P_1(a_1, \ldots, a_n), \ldots, P_m(a_1, \ldots a_n)).$$

For all $i = 1, \ldots, m$ we see that the value $P_i(a_1, \ldots, a_n)$ depends only on the values $\bar{P}_i$ of P_i in $k[X]$. As $\bar{P}_i = G(y_i)$ we get

$$\begin{aligned} h(f(x)) &= h(G(y_1), \ldots, G(y_n))(a_1, \ldots, a_n) = \\ &= [G \text{ is a homomorphism of algebras }] = Gh(y_1, \ldots y_m)(a_1, \ldots, a_n) = 0. \end{aligned}$$

so that $f(x) \in V(I(Y)) = Y$. □

Definition 1.1.15. Let X be an affine algebraic variety. We say that X is **irreductible** if

$$X = X_1 \cup X_2,\ X_1, X_2 \text{ closed in } X \Rightarrow X = X_1 \text{ or } X = X_2.$$

A variety X is irreductible if and only if $I(X)$ is a prime ideal (see the exercises). We deduce that the ring $k[X]$ is integral. Then we define **the field of functions** of X as the field of fractions $k(X)$ of the ring $k[X]$: the elements of $k(X)$ are the functions f/g with $f, g \in k[X]$ and $f/g = f_1/g_1$ if and only if $fg_1 = f_1 g$.

1.1.1 Finiteness properties

In this section we recall some properties of rings and modules.

Definition 1.1.16. Let A be a ring and B an A-algebra. We say that B is **of finite type** over A if B is generated, as an A-algebra, by a finite number of elements: $B \simeq A[x_1, \ldots, x_n]$ (where the elements $(x_i)_{1 \leq i \leq n}$ are not necessarily algebraically independent). We say that B is a finite A-algebra if B is of finite type as A-module, that is, B is generated by a finite number of elements as an A-module : $B \simeq Ax_1 + \ldots + Ax_n$.

Example 1.1.17. 1. If k is a field and $K = k(x)$ is an algebraic extension of k generated by x, then K is a k-module of finite type. In fact, if $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ is a minimal polynomial of x, then K is generated by $1, x, \ldots x^{n-1}$.

2. Let A be a ring. If B is an A-algebra of finite type (resp. a finite A-algebra) and C is a B-algebra of finite type (resp. finite), then C is an A-algebra of finite type (resp. finite).

Definition 1.1.18. Let A be a ring and let M be an A-module. We say that M is **noetherien** if any increasing sequence $M_1 \subseteq M_2 \subseteq \ldots M_n \subseteq \ldots$ of submodules of M is constant starting from some $n = n_0$. A ring A is **noetherian** if A is noetherian as an A-module, that is any increasing sequence $I_1 \subseteq I_2 \subseteq \ldots I_n \subseteq \ldots$ is constant starting from some $n = n_0$.

Proposition 1.1.19. *An A-module M is noetherian iff any submodule of M could be generated by a finite number of elements. In particular, a ring A is noetherian if and only if any ideal of A could be generated by a finite number of elements.*

Example 1.1.20. 1. Let M be an A-module. If M is noetherian, then any submodule of M is noetherian, any quotient of M is noetherian and any module of finite type over M is noetherian.

2. If A is noetherian, then the ring $A[x]$ is also noetherian, in particuliar, $k[x_1, \ldots, x_n]$ is noetherian. If B is an A-algebra of finite type, then B is a noetherian ring : in fact, B is a quotient of $A[x_1, \ldots x_n]$.

3. The ring $A = k[x_i]_{i\in\mathbb{N}}$ is not noetherian. The field of fractions K of A, being a field, is noethérien. This shows that a subring of a noetherian ring is not necessarily noetherian.

1.2 The structure of maximal ideals

Lemma 1.2.1. *Let $A \subseteq B \subseteq C$ be the inclusions of rings such that*

(i) A is a noetherian ring,

(ii) C is an A-algebra of finite type,

(iii) C is a B-module of finite type.

Then B is an A-algebra of finite type.

Proof. Let $x_1, \ldots, x_n$ be the elements of C generating C as an A-algebra. Let $y_1, \ldots, y_m \in C$ generating C as a B-module :

$$C = By_1 + \ldots + By_m.$$

We can then write, for all $1 \leq i, j \leq n$:

$$x_i = \sum_{t=1}^{m} b_{it} y_t$$

with $b_{it} \in B$ and

$$y_i \cdot y_j = \sum_{t=1}^{m} c_{ijt} y_t.$$

Let $B' \subset B$ be a subring generated over A by families (b_{it}) and (c_{ijt}). As B' is of finite type over A and A is a noetherian ring, we have that B' is noetherian. By construction, C is generated by $y_1, \dots y_m$ as a B'-module. We then have that C, viewed as a B'-module, is noetherien. As B is a submodule of C, we deduce that B is generated by a finite number of elements as a B'-module: $B = B'd_1 + \ldots + B'd_s$. We get that B is an A-algebra of finite type, generated by families (b_{it}) and (c_{ijt}) and (d_i). □

Proof of theorem 1.1.5. Let $K = k[x_1, \dots, x_n]/\mathfrak{m}$. The statement of the theorem is equivalent to

$$K = k[x_1, \dots, x_n]/\mathfrak{m} \simeq k.$$

In fact, it is enough to take a_i the image of x_i by the isomorphism above.

Next, as k is algebraically closed, it is enough to show that K is algebraic over k. Up to renumbering, we may assume that $x_1, \dots x_r \in K$ are algebraically independent over k and that $x_{r+1}, \dots x_n$ are algebraic over $k(x_1, \dots, x_r)$, that is K is a $k(x_1, \dots, x_r)$-module of finite type. If $r = 0$, there is nothing to prove. Assume that $r > 0$.

We apply proposition 1.2.1, to $B = k(x_1, \dots x_r)$, $C = K$ and $A = k$, B is a k-algebra of finite type. We write

$$B = k[z_1, \dots, z_s]$$

with

$$z_i = \frac{P_i(x_1, \dots x_r)}{Q_i(x_1, \dots x_r)}, P_i, Q_i \in k[x_1, \dots x_r].$$

Let $f \in k[x_1, \dots, x_r]$ be an irreducible polynomial. We have $\frac{1}{f} \in B$. As $B = k[z_1, \dots z_s]$, we can write $1/f$ as a polynomial in z_i, in particular, this implies that f divides at least one Q_i. But there is only a finite number of polynomials verifying this property. As k is algebraically closed, it is in particular infinite. We then have an infinite family $(x - a)_{a \in k}$ of irreducible polynomials over k, contradiction. □

1.3 Additional exercises 1

1. Show that the polynomial $f(x,y) = y^2 - x(x-1)(x+1) \in k[x,y]$ is irreducible over any field. Deduce that $X = V(f)$ is an irreducible variety. Draw a picture in the case $k = \mathbb{R}$.

2. (a) Let $X = V(y - x^2)$. Show that $k[X]$ is isomorphic to the polynomial ring in one variable.

   (b) Let $X = V(xy - 1)$. Show that $k[X]$ is not isomorphic to the polynomial ring in one variable.

3. Let k be a non algebraically closed field.

   (a) Show that there exists a polynomial $f \in k[x,y]$ such that $V(f) = (0,0)$. Deduce that for any $n > 0$ there exists a polynomial $F \in k[x_1, \ldots, x_n]$ such that $V(F) = (0, \ldots, 0)$.

   (b) If X is an affine variety over k, show that X could be defined by a single equation.

4. Let k be an algebraically closed field.

   (a) Let $f, g \in k[x,y]$ with f an irreducible polynomial and g not divisible by$f$.

      i. Show that there exists $u, v \in k[x,y]$ and $h \in k[x] \setminus \{0\}$ such that $uf + vg = h$.

      ii. Deduce that the curves $V(f)$ and $V(g)$ intersect only in a finite number of points.

   (b) Let I ne a prime ideal in $k[x,y]$. Show that either $I = (f)$ with f an irreducible polynomial, or I is maximal.

5. (**Algebraic groups**) Let k be a field.

   (a) Show that the determinant $det(x_{ij})_{1 \leq i \leq n, 1 \leq j \leq n}$ is an irreducible polynomial in n^2 variables.

   (b) Show that $GL_n(k)$ is open in $M_n(k) \simeq k^{n^2}$ for the Zariski topology.

   (c) Show that for all $0 \leq r \leq n$ the set M_r od matrices of rank at most r is irreducible closed subset of M_k^n.