Chapter 1

Basic Notions

Throughout this document, we work with a fixed algebraically closed field k (or sometimes denoted K), called **ground field**.

1.1 Algebraic Closed Fields

Let k be an algebraic closed field, then for every $f \in k[x]$ (where $k[x]$ denotes the set of all polynomials over the field k), we have that if f is non-constant, then f has a root on k.

Example 1.1.1
$\mathbb{C}$ is an algebraic closed extension of $\mathbb{R}$, and $\mathbb{Q}$.

Turns out algebraic closed fields are important due to the following fact:

There is a one to one correspondence between geometric and algebraic objects using algebraic closed fields.

We will first deal with simple objects and then we'll scalate to more complex in order to generalize certain notions defined in algebraic geometry.

Definition 1.1.1 (**Affine Space**)
Let k be a field. We denote by $\mathbb{A}^n$ the **n-dimensional affine space over the field** k, that is:

$$\mathbb{A}^n = \left\{ (\alpha_1, \ldots, \alpha_n) \middle| \alpha_i \in k, \quad \forall i \in \left[\left|1, n\right|\right] \right\}$$

All the geometric concepts we will be dealing with are within this space, this is due to the following fact:

Definition 1.1.2 (**Closed Subsets of Affine Space**)
Let $X \subseteq \mathbb{A}^n$ be a subset, then X is **closed** if there exists $f_1, \ldots, f_m \in k[x_1, \ldots, x_m]$ polynomials over the field k such that:

$$f_i(u) = 0, \quad \forall i \in \left[\left|1, m\right|\right] \iff u \in X$$

From now on, we will write $F(T)$ to denote a polynomial in n-variables, allowing T to stand for the set of variables $T_1, \ldots, T_n$.

Observation 1.1.1 (**Equations of a Set**)
If a closed subset X consists of all common zeros of polynomials $F_1(T), \ldots, F_m(T)$, then we refer to:

$$F_1(T) = \cdots = F_n(T) = 0$$

as the **equations of the set** X.

One really useful definition and fact that are proved in the notes of Algebra Moderna III are the following:

Definition 1.1.3 (Noetherian Ring)
Let R be a ring. We say that R is **noetherian** if for all I ideal of R there exists $a_1, \ldots, a_n \in R$ such that:

$$I = (a_1, \ldots, a_n),$$

where $(a_1, \ldots, a_n)$ denotes the ideal generated by the set $\{a_1, \ldots, a_n\}$.

Observation 1.1.2 (Ideal Generated by a Set S)
Let R be a commutative ring with identity, then the ideal generated by $S \subseteq R$ is:

$$(S) = \left\{ \sum_{i=1}^{n} r_i s_i \middle| r_i \in R, s_i \in S, \forall i \in \left[\left|1, n\right|\right]; n \in \mathbb{N} \right\}$$

Theorm 1.1.1 (Hilbert Basis Theorem)
Let R be a noetherian ring, then $R[x]$ is noetherian.

A useful fact about the Hilbert basis theorem is that it generalizes neatly to an arbitrary number of indeterminates:

Corollary 1.1.1
Let R be a noetherian ring, then $R[T]$ is noetherian.

This useful fact is fundamental in the proof of the following result:

Proposition 1.1.1
Let X be a set defined by an infinite system of equations $\{F_\alpha(T)\}_{\alpha \in I}$ with $I \neq \emptyset$. Then X is closed.

Proof:
Let $\mathfrak{U}$ be the ideal generated by the system of equations $\{F_\alpha(T)\}_{\alpha \in I}$. Since $k[T]$ is noetherian due to the fact that k is a field (in particular, every field is noetherian), then there exists $G_1, \ldots, G_m \in k[T]$ such that:

$$\left(\{F_\alpha(T)\}_{\alpha \in I}\right) = (G_1(T), \ldots, G_m(T))$$

We claim that $u \in X$ iff $G_i(u) = 0$, for all $i \in \left[\left|1, m\right|\right]$. If $u \in X$, then $F_\alpha(u) = 0$ for all $\alpha \in I$, so in particular by Observation (1.1.2):

$$F(u) = 0, \quad \forall F \in \left(\{F_\alpha(T)\}_{\alpha \in I}\right)$$

which is the same as:

$$F(u) = 0, \quad \forall F \in (G_1(T), \ldots, G_m(T))$$

so $G_i(u) = 0$, for all $i \in \left[\left|1, m\right|\right]$. ■

It follows from this proposition that the arbitrary intersection of closed subsets of $\mathbb{A}^n$ is closed. Also, it happens that $\emptyset$ and $\mathbb{A}^n$ are closed (using the polynomials $F = 1$ and $F = 0$).

Proposition 1.1.2
If X_1 and X_2 are closed subsets of $\mathbb{A}^n$, then $X_1 \cup X_2$ is also a closed subset of $\mathbb{A}^n$.

Proof:
Let $F_1, \ldots, F_n$ and $G_1, \ldots, G_m$ polinomials over the ring $k[T]$ such that:

$$F_i(u) = 0, \quad \forall u \in X_1 \text{ and } G_j(v) = 0, \quad \forall v \in X_2$$

for all $(i, j) \in [|1, n|] \times [|1, m|]$. We define $H_{i,j} \in k[T]$ as:

$$H_{i,j} = F_i G_j, \quad \forall (i, j) \in [|1, n|] \times [|1, m|]$$

Then:

$$H_{i,j}(w) = 0, \quad \forall w \in X_1 \cup X_2$$

for all $(i, j) \in [|1, n|] \times [|1, m|]$. It follows that $X_1 \cup X_2$ is closed. ∎

By all this it follows that family of all the complements of closed subsets of $\mathbb{A}^n$ are a topology over $\mathbb{A}^n$.

Example 1.1.2 (**Closed Subsets of** $\mathbb{A}^1$)
Let $X \subseteq \mathbb{A}^1$ be a closed subset of $\mathbb{A}^1$, then there exists $f_1, \ldots, f_m \in k[x]$ (polynomials in one variable) such that:

$$f_i(u) = 0, \quad \forall i \in [|1, m|] \iff u \in X$$

Let $d \in [x]$ the highest degree polynomial with leading coefficient one such that:

$$f_i = u_i d, \quad \forall i \in [|1, n|]$$

where $u_i \in k[x]$. If $u_1 = 1$, then $X = \emptyset$ if one of the polynomials is non zero and $X = \mathbb{A}^1$ if all of them are equal to zero, otherwise it follows that X is the family of all the roots of d, which is finite.

If $X = \{\alpha_1, \ldots, \alpha_n\}$, then X is closed because X is the family of zeros of the polynomial:

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

Example 1.1.3 (**Closed Subsets of** $\mathbb{A}^2$)

Definition 1.1.4 (**Hypersurface**)
A set $X \subseteq \mathbb{A}^n$ defined by one equation $F(T_1, \ldots, T_n) = 0$ is called a **hypersurface**.

1.2 Regular Functions on Closed Subsets

Definition 1.2.1 (**Regular Functions**)
Let X be a closed subset of $\mathbb{A}^n$ over the ground field k. A function $f : X \to k$ is called **regular** if there exists a polynomial $F \in k[T]$ such that:

$$f(u) = F(u), \quad \forall u \in X$$

In general, there's not a unique polynomial that defines a regular function.

Observation 1.2.1
We can add to F any polynomial entering in the system of equations that defines the set X, this doesn't always result in an alteration of F.

For the next proposition, we need to remember the definition of an algebra:

Definition 1.2.2 (**k-Algebra**)
A k-algebra is a cuatruplet $(A, k, +, \cdot)$ such that:

(1) $(A, +, \cdot)$ is a ring.

(2) $(A, +)$ is a vector space over the field k.

(3) The ring multiplication is k-bilinear, that is:

$$\alpha(ab) = (\alpha a)b = a(\alpha b), \quad \forall \alpha \in k, a, b \in A$$

We will usually denote a k-algebra simply by A.

Proposition 1.2.1 (**Algebra of Regular Functions**)
Let X be a closed subset of $\mathbb{A}^n$ over the ground field k. The set of all regular functions over X is a k-algebra with the usual addition and multiplication of functions.

The ring obtained is denoted by $k[X]$ and is called the **ring of regular functions over X**.

Proof:
Let $k[X]$ be the set of all regular functions over X. We will prove that $k[X]$ is a k-algebra by checking the three conditions of the definition:

(1) $(k[X], +, \cdot)$ **is a ring**. This is obvious since the sum and product of polynomials is a polynomial.

(2) $(k[X], +)$ **is a vector space over the field k**. This is also obvious since the sum of polynomials and the multiplication of a polynomial by a scalar is a polynomial.

(3) **The ring multiplication is k-bilinear**. This is also immediate from the fact that the multiplication of elements in the field k is commutative.

It follows that $k[X]$ is a k-algebra. ■

Definition 1.2.3 (**Coordinate Ring**)
Let X be a closed subset of $\mathbb{A}^n$ over the ground field k. The k-algebra $k[X]$ is called the **coordinate ring of X**.

We will only deal with the ring structure of the algebra of regular functions, leaving the vector space structure aside (for the moment). We write $k[T]$ for the polynomial ring in $T_1, \ldots, T_n$-variables over the field k.

Observation 1.2.2
Let $ap : k[T] \to k[X]$ be the function defined as:

$$ap(F) = f, \quad \forall F \in k[T]$$

where $f : X \to k$ is defined as $f(u) = F(u)$ for all $u \in X$. It's immediate that ap is a epimorfism of rings.

Due to the latter obsevation and using the first isomorphism theorem, it follows that:

$$k[X] \cong k[T]/\ker(ap)$$

where:

$$\ker(ap) = \left\{ F \in k[T] \middle| F(u) = 0, \quad \forall u \in X \right\}$$

is an ideal of $k[T]$.

Definition 1.2.4 (**Ideal of a Closed Set**)
Let X be a closed subset of $\mathbb{A}^n$ over the ground field k. The ideal $\ker(ap)$ of $k[T]$ is called the **ideal of the closed set** X and is denoted by $\mathfrak{I}_X$.

From the above, it follows that:

$$k[X] \cong k[T]/\mathfrak{I}_X$$

Thus, the ring is fully determined by the ideal $\mathfrak{I}_X$. We will now focus on studying this ideal in order to understand better the structure of the ring of regular functions over a closed set.

Example 1.2.1
If $X \subseteq \mathbb{A}^n$ is such that $X = \{(x_1, \ldots, x_n)\}$, then:

$$k[X] \cong k[T]/\mathfrak{I}_X$$

where $\mathfrak{I}_X$ is the ideal of all polynomials vanishing at the point $x = (x_1, \ldots, x_n)$, which is given by:

$$\mathfrak{I}_X = \left\{ F \middle| \text{ where } F(T) = \alpha(T - x); \alpha \in k \right\}$$

So, $k[T]/\mathfrak{I}_X \cong k$. It follows that $k[X] \cong k$.

Example 1.2.2
If $X = \mathbb{A}^n$, then $\mathfrak{I}_X = \{0\}$, where 0 is the 0 polynomial, so $k[X] \cong k[T]$.

Example 1.2.3
Let $X \subseteq \mathbb{A}^2$ be given by the equation:

$$X = \left\{ (x_1, x_2) \in \mathbb{A}^2 \middle| x_1 x_2 - 1 = 0 \right\}$$

Then, the ideal $\mathfrak{I}_X$ is given by:

$$\mathfrak{I}_X = \left\{ F \in k[T_1, T_2] \middle| F(T_1, T_2) = (T_1 T_2 - 1) G(T_1, T_2); G \in k[T_1, T_2] \right\}$$

It is not so difficult to show that there is a ring isomorphism between $k[X]$ and $k[T_1, T_1^{-1}]$, the ring of Laurent polynomials in one variable over the field k.

Observation 1.2.3
Let R be a ring and I and ideal of R. We know that there is a correspondence between the ideals of R/I and the ideals of R that contain I. This correspondence is given by:

$$J \mapsto J/I, \text{ were } J \text{ is an ideal of } R \text{ such that } I \subseteq J$$

Since $k[T]$ is Noetherian, it follows that $k[X]$ is also Noetherian, no matter the closed subset X of $\mathbb{A}^n$.

And furthermore, we have that $k[X]$ satisfies the following analogue of the Nullstellensatz Theorem. Before that, we shall give the following definition:

Definition 1.2.5 (Radical Ideal)
Let R be a ring and I an ideal of R. The radical of the ideal I, denoted by $\operatorname{rad}(I)$ or $\sqrt{I}$, is given by:

$$\operatorname{rad}(I) = \left\{ a \in R \middle| a^n \in I, \text{ for some } n \in \mathbb{N} \right\}$$

Proposition 1.2.2
Let X be a closed subset of $\mathbb{A}^n$ over the ground field k. Then, if $f, g_1, \ldots, g_m \in k[X]$ are functions such that f vanishes at all points where $g_1, \ldots, g_m$ vanish, then there exists $r \in \mathbb{N}$ such that:

$$f^r \in (g_1, \ldots, g_m)$$

where $(g_1, \ldots, g_m)$ denotes the ideal of $k[X]$ generated by the set $\{g_1, \ldots, g_m\}$.

Proof:
Let F and $G_1, \ldots, G_m \in k[T]$ be polynomials such that:

$$i(F) = f \text{ and } i(G_j) = g_j, \quad \forall j \in \left[\left|1, m\right|\right]$$

where $i : k[T]/\mathfrak{I}_X \to k[X]$ is given by:

$$i(H + \mathfrak{I}_X) = h, \quad \forall H \in k[T]$$

being $h : X \to k$ the function defined as $h(u) = H(u)$ for all $u \in X$.

Let $F_1, \ldots, F_l$ be the equations of X, that is:

$$F_i(u) = 0, \quad \forall u \in X, \quad \forall i \in \left[\left|1, l\right|\right]$$

If $u \in X$ is such that $G_j(u) = 0$ for all $j \in \left[\left|1, m\right|\right]$, then $F_i(u) = 0$ for all $i \in \left[\left|1, l\right|\right]$ and $F(u) = 0$. It follows from the Nullstellensatz Theorem that there exists $r \in \mathbb{N}$ such that:

$$F^r \in (G_1, \ldots, G_m, F_1, \ldots, F_l)$$

Therefore, since $F_1, \ldots, F_l \in \mathfrak{I}_X$, it follows that $f^r \in (g_1, \ldots, g_m)$. ■

Question 1.2.1
What's the relation between the ideal $\mathfrak{I}_X$ of a closed set X and a system $F_1 = \cdots = F_m = 0$ of defining equations of X?

Solution:
Clearly, by definition we have that $F_i \in \mathfrak{I}_X$, for all $i \in [|1, m|]$. Therefore, the ideal generated by the set $\{F_1, \ldots, F_m\}$ is contained in $\mathfrak{I}_X$.

However, it is not always true that $\mathfrak{I}_X$ is equal to the ideal generated by the set $\{F_1, \ldots, F_m\}$. $\square$

Example 1.2.4
Let $X \subseteq \mathbb{A}^2$ be given by the equation:

$$T^2 = 0$$

Then, $X = \{0\}$, so $\mathfrak{I}_X$ consists of all the polynomials vanishing at 0, that is, all polynomials without constant term. However, the ideal generated by the polynomial T^2 doesn't contain the polynomial T, so they are not equal.

However, we can always define the same closed set X with a system of equations $G_1 = \cdots = G_l = 0$ whose generated ideal is equal to $\mathfrak{I}_X$. This follows from the Hilbert's Basis Theorem, since $\mathfrak{I}_X$ is finitely generated.

Observation 1.2.4 (**Generating System of Equations**)
Let X be a closed subset of $\mathbb{A}^n$, and let $G_1, \ldots, G_m \in k[T]$ be polynomials such that:

$$\mathfrak{I}_X = (G_1, \ldots, G_m)$$

then, for all $F \in \mathcal{I}_X$ we have that there exists $H_1, \ldots, H_m \in k[T]$ such that:

$$F = H_1G_1 + \cdots + H_mG_m$$

Since $G_i \in \mathfrak{I}_X$ it follows that X is defined by the system of equations $G_1 = \cdots = G_m = 0$.

Therefore, we can always find a system of equations defining X whose generated ideal is equal to $\mathfrak{I}_X$.

Idea 1.2.1
It is sometimes even convenient to consider a closed set as defined by the infinite system of equations $F = 0$ for all polynomials $F \in \mathfrak{I}_X$. Indeed, if $(F1, ..., Fm) = \mathfrak{I}_X$ then these equations are all consequences of $F_1 = \cdots = F_m = 0$.

It turns out that relations between closed sets can be translated to relations between their corresponding ideals.

Example 1.2.5
Let X and Y be closed subsets of $\mathbb{A}^n$. Then, $Y \subseteq X$ if and only if $\mathfrak{I}_X \subseteq \mathfrak{I}_Y$.

This follows directly from the definitions. The latter example allows us to asociate to every closed subset of a closed set X of the afine space $\mathbb{A}^n$ an ideal of the coordinate ring $k[X]$.

Indeed, if $Y \subseteq X$ is a closed subset of X, then we can asociate to Y the ideal $\mathfrak{a}_Y = \mathfrak{I}_Y/\mathfrak{I}_X$ of the ring $k[X] = k[T]/\mathfrak{I}_X$ (using correspondence theorem).

Conversely, if $\mathfrak{a}$ is an ideal of $k[X]$, then we can asociate to $\mathfrak{a}$ the closed subset Y of X defined by the equations $F = 0$ for all polynomials $F \in \mathfrak{a}$.

Observation 1.2.5
$Y = \emptyset$ if and only if $\mathfrak{I}_Y = k[X]$

Something interesting happens when we consider isolated points of X. Indeed, if $x \in X$ is an isolated point of X, then the ideal $\mathfrak{m}_x = \mathfrak{I}_{\{x\}}/\mathfrak{I}_X$ has to be a maximal ideal of $k[X]$.

Observation 1.2.6
By definition, this ideal is the kernel of the homomorphism $ap : k[T] \to k[X]$, so:

$$\mathfrak{m}_x = \left\{ F \in k[T] \middle| F(x) = 0 \right\}$$

Since k is an algebraically closed field, then:

$$\mathfrak{m}_x = \left\{ \alpha(x - T) \middle| \alpha \in k \right\}$$

So, $k[T]/\mathfrak{m}_x = k$. It follows that $\mathfrak{m}_x$ has to be a maximal ideal of $k[X]$.

We can do the converse too, and to each maximal ideal of $k[X]$ there is an isolated point of X associated.

Definition 1.2.6 (Hypersurface)
Let X be a closed subset of $\mathbb{A}^n$ over the ground field k. We say that X is an **hypersurface** if there exists $F \in k[T]$ such that:

$$X = \left\{ u \in \mathbb{A}^n \middle| F(u) = 0 \right\}$$

1.3 Regular Maps

From now on, X will denote a closed subset of $\mathbb{A}^n$ and Y a closed subset of $\mathbb{A}^m$.

Definition 1.3.1 (Regular Maps)
A map $f : X \to Y$ is called **regular** if there exists $f_1, \dots, f_m \in X$ regular functions on X such that:

$$f(x) = (f_1(x), \dots, f_m(x)), \quad \forall x \in X$$

Any regular map $f : X \to \mathbb{A}^m$ is always given by m-functions $f_1, \dots, f_m \in k[X]$.

Observation 1.3.1
In order to know that this maps into the closed subset $Y \subseteq \mathbb{A}^n$, we need to check that:

$$G(f_1(x), \dots, f_m(x)) = 0, \quad \forall x \in X$$

for all $G \in \mathfrak{I}_Y$.

Example 1.3.1
A regular function is the same thing as a regular map $f : X \to \mathbb{A}^1 = k$.

Example 1.3.2
A linear map $L : \mathbb{A}^n \to \mathbb{A}^m$ is a regular map.

Proof:
It suffices to show that the components of L, let say $L = (L_1, \dots, L_m)$ are regular functions. Indeed, since L is linear, it follows that L_j is k-linear for all $j \in [|1, m|]$, so there exists $\alpha_1, \dots, \alpha_m \in \mathbb{A}^n$ such that:

$$L_j(x) = \alpha_j \cdot x, \quad \forall x \in \mathbb{A}^n$$

where $\alpha_j \cdot x$ denotes the usual dot product. Since each L_j is a polynomial of degree 1, it follows that L_j is a polynomial function, so it's regular. ■

Example 1.3.3
The projection map $(x, y) \mapsto x$ defines a regular map of the curve defined by $xy = 1$ to $\mathbb{A}^1$.

Example 1.3.4
The map $f(t) = (t^2, t^3)$ is a regular map of the line $\mathbb{A}^1$ to the curve defined by $x^3 - y^2 = 0$ in $\mathbb{A}^2$.

1.3.1 The Zeta Function of a Variety over $\mathbb{F}_p$

This example is very important to number theorists, since it relates algebraic geometry with number theory in a very deep way.

Let p be a prime number and $\mathbb{F}_p$ the finite field with p elements. Let X be a closed subset of $\mathbb{A}^n$, where the afine space is defined over the closure of the field $\mathbb{F}_p$, denoted by $\overline{\mathbb{F}_p}$, where the coefficients of the equations $F_i(T)$ that define X are in $\mathbb{F}_p$.

Observation 1.3.2
Let's consider the closed set $X \subseteq \mathbb{A}^n$ and $F_1 = \cdots = F_m$ the polynomials defining X. We have that $x \in X$ if and only if:

$$F_i(x) = 0, \quad \forall i \in [|1, m|]$$

since $F_i \in \mathbb{F}_p[T]$, its clear that $x \in X$ if and only if x is a solution of the system of congruences:

$$F_i(T) \equiv 0 \mod p$$

Let's consider the map $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ given by:

$$\varphi(x_1, \dots, x_n) = (x_1^p, \dots, x_n^p)$$

It's immediate to see that φ is a regular map. Furthermore, if $x \in X$, then $\varphi(x) \in X$. First, let $\alpha_1, \dots, \alpha_n \in X$, we will prove that:

$$F(\alpha_1^p, \dots, \alpha_n^p) = (F(\alpha_1, \dots, \alpha_n))^p$$

First, since $F \in \mathbb{F}_p[T] = \mathbb{F}_p[T_1, \dots, T_n]$, we have that F is a polynomial with coefficients in $\mathbb{F}_p$, so we can write F as a finite sum:

$$F(T_1, \dots, T_n) = \sum_{i_1, \dots, i_n} f_{i_1, \dots, i_n} T_1^{i_1} \cdots T_n^{i_n}$$

where $f_{i_1, \dots, i_n} \in \mathbb{F}_p$. Now, since $\overline{\mathbb{F}_p}$ is a field of characteristic p, we have the following facts:

- $(a+b)^p = a^p + b^p$ for all $a, b \in \overline{\mathbb{F}_p}$. This fact is generalyzsed to more than two summands by induction.

- $a^p = a$ for all $a \in \mathbb{F}_p \subseteq \overline{\mathbb{F}_p}$.

So,

$$\begin{aligned}
F(\alpha_1^p, \ldots, \alpha_n^p) &= \sum_{i_1,\ldots,i_n} f_{i_1,\ldots,i_n} (\alpha_1^p)^{i_1} \cdots (\alpha_n^p)^{i_n} \\
&= \sum_{i_1,\ldots,i_n} f_{i_1,\ldots,i_n}^p \alpha_1^{pi_1} \cdots \alpha_n^{pi_n} \\
&= \sum_{i_1,\ldots,i_n} \left(f_{i_1,\ldots,i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n}\right)^p \\
&= \left(\sum_{i_1,\ldots,i_n} f_{i_1,\ldots,i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n}\right)^p \\
&= F(\alpha_1, \ldots, \alpha_n)^p
\end{aligned}$$

So, if $\alpha = (\alpha_1, \ldots, \alpha_n) \in X$, then $\varphi(\alpha) = (\alpha_1^p, \ldots, \alpha_n^p) \in X$, because:

$$F_i(\alpha_1^p, \ldots, \alpha_n^p) = (F_i(\alpha_1, \ldots, \alpha_n))^p = 0^p = 0$$

for all $i \in [|1, m|]$. This proves that $\varphi(X) \subseteq X$, so the restriction of φ to X defines a regular map from X to itself.

Question 1.3.1
Is it true that $\varphi(X) = X$?

Solution:
Yes, this is true since $\overline{\mathbb{F}_p}$ is algebraically closed, so for all $a \in \overline{\mathbb{F}_p}$ the polynomial:

$$X^p - a$$

has a root in $\overline{\mathbb{F}_p}$. It follows that φ is an automorphism of $\overline{\mathbb{F}_p}$ (and, its easy to verify that $\varphi(X) = X$ using the same argument above). $\square$

Definition 1.3.2 (Fröbenius Map)
The map φ is called **Fröbenius map**.

Its significance is that all the points of X with coordinates in $\mathbb{F}_p$ are the fixed points of the map φ^n.

Observation 1.3.3
Indeed, the solutions of the equation $x^p = x$ are exactly all the elements of $\mathbb{F}_p$.

Using this exact same procedure, we can prove that the elements of the field $\mathbb{F}_{p^r}$ are the solutions of the equation $x^{p^r} = x$, and hence the points $\alpha \in X$ with coordinates in $\mathbb{F}_{p^r}$ are exactly the fixed points of the map φ^r.

Observation 1.3.4
Is worth noticing that:

$$\overline{\mathbb{F}_p} = \bigcup_{r=1}^{\infty} \mathbb{F}_{p^r}$$

so the latter observation makes more sense. In other words:

$$\mathbb{F}_{p^r} \subseteq \overline{\mathbb{F}_p}$$

for all $r \in \mathbb{N}$.

Definition 1.3.3
For each $r \in \mathbb{N}$, let ν_r be the number of points of X with coordinates in $\mathbb{F}_{p^r}$.

To get a better overview of the numbers ν_r, we must consider the following generating function:

$$P_X(t) = \sum_{r=1}^{\infty} \nu_r t^r$$

Definition 1.3.4 (Nombre)
Let $f \in \mathbb{Q}[[t]]$ be a formal series over $\mathbb{Q}$, that is:

$$f(t) = \sum_{i=1}^{\infty} a_i t^i$$

where $a_i \in \mathbb{Q}$. We say that f is a **rational function** if there exists two polynomials $P(t), Q(t) \in \mathbb{Q}[t]$ such that:

$$f(t) = \frac{P(t)}{Q(t)}$$

Observation 1.3.5
A theorem states that this function is always a rational function of t. This proof can be found in chapter V of *p-Adic Numbers, p-Adic Analysis and Zeta Functions* by Koblitz, N.

Which means that basically, the function $P_X(t)$ gives an expression in finite terms for the infinite sequence of numbers ν_r. Turns out that the function P_X associated to a closed set X has some properties analogous to the Riemann zeta function.

Observation 1.3.6
To express these properties, lets note that if $x \in X$ is a point whose coordinates are in $\mathbb{F}_{p^r}$ and generate this field, then X contains all the points $\varphi(x)^i$ for $i \in [\![1, r]\!]$, and these are all distinct.

Proof:
Let $x \in X$ be a point whose coordinates are in $\mathbb{F}_{p^r}$ and generate this field.

1. First, we will prove that $\varphi(x)^i \in X$ for all $i \in [\![1, r]\!]$.
2. Now, we will prove that the points $\varphi(x)^i$ for $i \in [\![1, r]\!]$ are all distinct.

■

1.4 Excersies

Excercise 1.4.1
If X and Y are closed subsets of $\mathbb{A}^n$ and $\mathbb{A}^m$, then $k[X \times Y]$ is isomorphic to $k[X] \otimes_k k[Y]$, where:

$$k[X] \otimes_k k[Y] = \left\{ f \otimes_k g \middle| f \in k[X] \text{ and } g \in k[Y] \right\}$$

where $f \otimes_k g : X \times Y \to k$ is defined as:

$$f \otimes_k g(x, y) = f(x)g(y), \quad \forall (x, y) \in X \times Y$$

Proof:

■

Excercise 1.4.2
If p is a prime number, then:

$$\overline{\mathbb{F}_p} = \bigcup_{r=1}^{\infty} \mathbb{F}_{p^r},$$

where $\mathbb{F}_{p^r}$ is the finite field with p^r elements.

Proof:

■