The Hilbert Property: from Inverse Galois Problem to the Topology of Varieties

Ana Victoria Martins Quedo

Dissertação de mestrado
Orientadora: Cecília Salgado

Instituto de Matemática
Universidade Federal do Rio de Janeiro
Setembro de 2020

Introduction

The subject of this master thesis is the Hilbert Property. This property was first introduced by Colliot-Thélène and Sansuc in their 1987 article "Principal homogeneous spaces under flasque tori: applications" [2], but to tell the motivation for this property, we have to go back to the end of 19th century.

Almost a hundred years before the introduction of the Hilbert Property, in 1892, Hilbert proved Hilbert's Irreducibility Theorem [1], stated bellow.

Theorem 0.0.1 (Hilbert's Irreducibility Theorem)**.** *For any irreducible polynomial $f \in \mathbb{Q}[X_1, \dots, X_s, Y_1, \dots, Y_r]$ of degree ≥ 1 in $Y_1, \dots, Y_r$, there exist infinitely many $b \in \mathbb{Q}^s$ such that $f(b_1, \dots, b_s, Y_1, \dots, Y_r) \in \mathbb{Q}[Y_1, \dots, Y_r]$ is irreducible.*

This theorem is celebrated for its numerous applications, for example, it is used as a step in Andrew Wiles' proof of Fermat's Last Theorem, done in 1994. However, Hilbert's original motivation was to show that if a finite group G can be realized as a Galois group of an extension over $\mathbb{Q}(X_1, \dots, X_n)$, it can also be realized as a Galois group of an extension over $\mathbb{Q}$. A particular case of the Inverse Galois Problem that can be proved using this strategy is the case when G is a symmetric group.

In 1917, Emmy Noether tried to apply this same strategy for an arbitrary finite group G. She conjectured that $\mathbb{Q}(X_1, \dots, X_n)^G$, the field of elements of $\mathbb{Q}(X_1, \dots, X_n)$ fixed by G, would be rational for every finite group G, and that would solve the Inverse Galois Problem. However, this conjecture was shown to be false in 1969, by a counterexample given by Swan [11].

We can reformulate this problem in a more geometric way, looking at the variety $\mathbb{A}^n/G$ over $\mathbb{Q}$ instead of looking at the field $\mathbb{Q}(X_1, \dots, X_n)^G$ since $\mathbb{Q}(X_1, \dots, X_n)^G$ is the function field of $\mathbb{A}^n/G$. Translating the above results to this geometric perspective, we arrive that if $\mathbb{A}^n/G$ is rational over $\mathbb{Q}$, G is realizable over $\mathbb{Q}$. However, is there a less restrictive condition that we can impose over $\mathbb{A}^n/G$ that guarantees the same result? Searching for such a condition, Colliot-Thélène and Sansuc defined the Hilbert Property in 1987.

This property also permits to look to the Inverse Galois Problem over other fields and asking if $\mathbb{A}^n$ over K has the Hilbert Property is the same of asking if the statement of Hilbert's Irreducibility Theorem is still true if we replace $\mathbb{Q}$ by K.

Colliot-Thèlene and Sansuc also conjectured that, for a number field K, every K-unirational variety has the Hilbert Property and showed that this conjecture implies an affirmative response to the Inverse Galois Problem.

By the above motivation, the Hilbert Property might appear only to convey arithmetical information about a variety. However, in 2016, Zannier and Corvaja gave the first example of a non-unirational variety that holds the Hilbert Property on their article "On the Hilbert Property and the Fundamental Group of Algebraic Varieties" [21]. In this same article, they presented other similarities between non-unirational and unirational that hold the Hilbert Property. In fact, they showed that this property is also intrinsically related to topological aspects of a variety.

We think that all these associations to different branchs of Mathematics make this property a worthy theme of study.

In what follows we give a description of the content of each chapter of this dissertation.

The first two chapters of this work are dedicated to review basic concepts of Galois Theory and Classical Algebraic Geometry that are crucial for the development of our theme.

The third chapter contains the core of this work. We describe it in detail below.

On section 3.1, we reconstruct the path that leaded to the definition of the Hilbert Property, giving the demonstrations of some results mentioned in this introduction. We also present Hilbertian fields along with some examples and non-examples.

On section 3.2, we define thin sets. We remark that non-thin subsets of the set of rational points of a variety could be interpreted as sets having a "strengthened" Zariski dense condition. From this concept, we define the Hilbert Property for varieties in general. We also present some examples of varieties that bear the Hilbert Property as well as varieties that lack it.

On section 3.3, we see how the Hilbert Property is connected to the resolution of the Inverse Galois Problem, giving the proof that the conjecture stablished by Colliot-Thèléne and Sansuc implies that the Inverse Galois Problem is true.

On section 3.4, we explain the relation of the Hilbert Property with algebraic topology.

Finally, we conclude this work presenting, in section 3.5, some conjectures made by Zannier and Corvaja in their 2016 article [21].

Agradecimentos

Primeiramente, gostaria de agradecer a minha mãe, que não só me apoiou durante o processo de escrita dessa dissertação, mas em todos os outros momentos que me guiaram até aqui. Obrigada, te amo.

Em segundo lugar, gostaria agradecer a minha orientadora, a professora Cecília. Obrigada por sugerir um tema tão rico e que conecta tantas áreas interessantes da matemática, pela disponibilidade e paciência para com minhas dúvidas, pelas palavras de incentivo e por ser um exemplo como matemática.

Gostaria também de agradecer aos meus amigos do Pedro II: Bruna, Gabriela, Karina, Luciana e Luis. Obrigada pelas conversas, pelos momentos divertidos e por me inspirarem a ser uma versão melhor de mim mesma, sendo cada dia versões melhores de vocês mesmos.

Gostaria de agradecer ao Arthur e ao Felipe por me acompanharem nessa jornada de estudar geometria algébrica, pelas diversas discussões e por me ajudarem a revisar detalhes da minha dissertação. Gostaria também de agradecer a vários outros amigos que eu conheci na UFRJ que foram muito importantes tanto no meu crescimento pessoal quanto acadêmico, entre eles: Larissa, Isabela, Pedro e Rodrigo.

E por fim, gostaria de agradecer as professoras Carolina Araújo, Luciane Quoos, Maral Mostafazadehfard e Miriam Abdón por aceitarem a fazer parte da banca dessa dissertação. Obrigada por disponibilizarem seu tempo para a leitura desse trabalho, especialmente nesse momento tão conturbado de pandemia.

Contents

Chapter 1

A Brief Review of Galois Theory

1.1 First Definitions about Field Extensions

Throughout this dissertation, we use a collection of definitions and theorems of Galois Theory. The intention of our first chapter is to recall these definitions and results and give the reference needed when appropriated.

We start by introducing the concept of field extensions and some basic definitions related to it.

Let F and K be fields, such that $F \subset K$. Then K is called a field extension of F, this relation will be denoted by K/F.

Definition 1.1.1 (Degree of K/F and Finite extension)**.** The *degree of* K/F, denoted by $[K : F]$, is the dimension of K as a F-vector space. We say that K/F is a *finite extension* if it has finite degree.

Definition 1.1.2 (Algebraic extension)**.** Given $\alpha \in K$, we say that α is *algebraic over* F if there is a nonzero polynomial $f(x) \in F[x]$ such that $f(\alpha) = 0$. If every element of K is algebraic over F, we say that K/F is an *algebraic extension.*

Definition 1.1.3 (Generators of a field)**.** Consider an extension K/F. If X is a subset of K, we define the *ring generated by* F *and* X, denoted by $F[X]$, as the intersection of all subrings of K that contain F and X. The field $F(X)$ generated by F and X is the intersection of all subfields of K that contain F and X. We say that a field extension L is *finitely generated over* F if $L = F(a_1, \dots, a_n)$.

Theorem 1.1.4. *Let K be an extension of F. We have that K is a finite extension of F if and only if K is algebraic and finitely generated over F.*

Proof. The proof of this theorem can be found in Lemma 1.19, Proposition 1.20 and Proposition 1.21 of [3]. □

1.2 Normal Extensions, Algebraic Closure and Separable Extensions

In this section, we see some ways of relating polynomials f of F with finite extensions K of F, so that K/F hold some interesting properties. We start this section presenting a special type of extension K of F, one that is associated to the roots of a polynomial (or a set of polynomials) in $F[x]$. They are the normal extensions.

But first, we introduce some terminology. We say that a polynomial $f \in F[x]$ *splits over* K if f factors completely into linear factors in $K[x]$. Given $f \in F[x]$, there is always a finite extension of F over which f splits (see Theorem 3.3 of [3]).

Definition 1.2.1 (Splitting field)**.** Let K be an extension field of F.

- If $f \in F[x]$, then K is a *splitting field* of f over F if f splits over K and $K = F(a_1, \dots, a_n)$, where $a_1, \dots, a_n$ are the roots of f.
- If S is a set of non-constant polynomials over F, then K is a *splitting field* of S over F if each $f \in S$ splits over K and $K = F(X)$, where X is the set of all roots of all $f \in S$.

Definition 1.2.2 (Normal Extension)**.** Given K/F a field extension, we say that K is *normal* over F if K is a splitting field of a set of polynomials over F.

Normal extensions have a very interesting property that is described in the next proposition.

Proposition 1.2.3. *If K is an algebraic extension of F, then the following statements are equivalent:*

- *The field K is normal over F.*
- *For any irreducible polynomial $f \in F[x]$, if f has a root in K, then f splits over K.*

Proof. See Proposition 3.28 in [3]. □

Thanks to the Fundamental Theorem of Algebra (Theorem 5.15 in [3]), we know that every polynomial in $\mathbb{C}[x]$ splits over $\mathbb{C}$. We want to characterize other fields with this same property.

Proposition 1.2.4. *If K is a field, the following statements are equivalents:*

- *There are no algebraic extensions of K other than K itself.*
- *There are no finite extensions of K other than K itself.*

- *Every $f \in K[x]$ splits over K.*

Proof. See Lemma 3.10 in [3]. □

Definition 1.2.5 (Algebraically closed)**.** If K satisfies the equivalent conditions of the previous proposition, we say that K is *algebraically closed.* If K is an algebraic extension of F that is algebraically closed, we say that K is an *algebraic closure* of F.

Remark 1.2.6. It can be shown that every field F has an algebraic closure and that it is unique up to an isomorphism that fixes F. For this reason, we denote by $\overline{F}$, the algebraic closure of F. These results can be found in chapter 3 of [3].

The next definitions introduce another special type of algebraic extension.

Definition 1.2.7 (Separable polynomials)**.** An irreducible polynomial $f \in F[x]$ is said to be *separable* over a field F if its roots are all distinct in any splitting field. A polynomial $g \in F[x]$ is said to be *separable* over F if all irreducible factors of g are separable.

In order to relate separable polynomials over F to what will be the separable extensions of F, we need to relate the polynomials with elements of extensions of F. For this, we introduce the minimal polynomials.

Definition 1.2.8 (Minimal polynomial)**.** Given $\alpha \in K$, an algebraic element over F, the irreducible monic polynomial f such that $f(\alpha) = 0$ is called the *minimal polynomial* of α in F and it is denoted by $Min(F, \alpha)$.

Definition 1.2.9 (Separable extension)**.** Given $\alpha \in K$, an algebraic element over F, we say that α is *separable* over F if $Min(F, \alpha)$ is a separable polynomial. An extension K/F is *separable* if every $\alpha \in K$ is separable over F.

Proposition 1.2.10. *Let $f \in F[x]$ be an irreducible polynomial, if $char(F) = 0$, then f is separable over F. As a consequence, if $char(F) = 0$, every algebraic extension of F is separable.*

Proof. The proof can be found in [3], Proposition 4.6. □

Fields that have this same property have a special name as we see in the next definition.

Definition 1.2.11 (Perfect field)**.** A field F is said to be perfect if every algebraic extension of F is separable.

As we have seen, every field F with $char(F) = 0$ is perfect. When $char(F) \neq 0$, the following proposition gives us a criterion to determine whether F is perfect or not.

Proposition 1.2.12. *Let F be a field of characteristic p. Then F is perfect if and only if $F^p = F$.*

Proof. See Theorem 4.13 in [3]. □

We conclude this section with two examples. To start, we see that extensions can be separable despite not being normal.

Example 1.2.13. The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal because the minimal polynomial of $\sqrt[3]{2}$, $x^3 - 2$, does not split over $\mathbb{Q}(\sqrt[3]{2})$. However, this extension is separable because this same polynomial is separable.

On the next section, we will see the importance of extensions that are both separable and normal, so here is an example of one.

Example 1.2.14. The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal and separable because the minimal polynomial of $\sqrt{2}$ is $x^2 - 2$, which is a separable polynomial that splits over $\mathbb{Q}(\sqrt{2})$.

1.3 Galois Groups, Galois Extensions and the Fundamental Theorem of Galois theory

In this section, we finally introduce the Galois group of a field extension and the concept of a Galois extension. We see that these extensions are special because of the relation that we can establish between them and their Galois groups. We also see how the properties defined in the last section will help us to determine when a field extension is Galois.

The group of automorphisms of a field K, denoted by $Aut(K)$, is formed by the isomorphisms (as a ring) from K to itself. When studying Galois theory, we want to look at a special subgroup of this group.

Definition 1.3.1 (Galois group)**.** Given a field extension K over a field F. We define the *Galois group* of K/F, denoted by $\mathrm{Gal}(K/F)$, as:

$$\mathrm{Gal}(K/F) := \{\sigma \in Aut(K) | \ \sigma|_F = Id\}.$$

Let S be a subset of $Aut(K)$, we set

$$K^S = \{x \in K | \ \sigma(x) = x \text{ for all } \sigma \in S\}.$$

K^S is a subfield of K, called the *field fixed by S*.

The elements of $\mathrm{Gal}(K/F)$ have some interesting properties as the one in next proposition.

Proposition 1.3.2. *Consider $\sigma \in \mathrm{Gal}(K/F)$ and $\alpha \in K$, algebraic over F. Given a polynomial $f \in F[x]$, such that $f(\alpha) = 0$, we have that $f(\sigma(\alpha)) = 0$. Therefore, σ permutes the roots of $Min(F, \alpha)$.*

Proof. See Lemma 2.3 in [3]. □

Definition 1.3.3 (Galois extension)**.** Let K be an algebraic extension of F. Then K is said to be *Galois* over F if $F = K^{\mathrm{Gal}(K/F)}$.

Proposition 1.3.4. *Let G be a finite group of $Aut(K)$ with $F = K^G$. Then $|G| = [K : F]$, and so $G = \mathrm{Gal}(K/F)$.*

Proof. The proof can be found in [3], Proposition 2.14. □

Proposition 1.3.5. *Let K be a finite extension of F. Then K is Galois over F if and only if $|Gal(K/F)| = [K : F]$.*

Proof. The proof can be found in [3], Corollary 2.16. □

There are other criteria to verify if a field extension is Galois. The next theorem relates Galois extensions with normal and separable ones.

Theorem 1.3.6. *Let K be an algebraic extension of F, then the following statements are equivalent:*

- *K/F is Galois.*
- *K/F is normal and separable.*
- *K is a splitting field for a set of separable polynomials over F.*

Proof. This theorem and its proof can be found in [3], Theorem 4.9. □

A field L with $F \subseteq L \subseteq K$ is called an *intermediate field* of the extension K/F. Galois field extensions are special because we can establish a 1-1 correspondence between its intermediate fields and the subgroups of $\mathrm{Gal}(K/F)$, allowing us to translate Field Theory problems to Group Theory problems, and vice-versa. This result is called the Fundamental Theorem of Galois Theory and it is stated in detail bellow:

Theorem 1.3.7 (Fundamental Theorem of Galois Theory)**.** *Let K be a finite Galois extension of F, and let $G = \mathrm{Gal}(K/F)$. There is a bijection between the intermediate fields of K/F and the subgroups of G, given by:*

$$L \mapsto \mathrm{Gal}(K/L)$$
$$H \mapsto K^H.$$

If the field L and subgroup H are correspondent to each other by this bijection, then $[K : L] = |H|$ and $[L : F] = [G : H]$.

Proof. See Theorem 5.1 in [3]. □

To conclude this section, we present some examples of Galois extensions and of the relation stated in the Fundamental Theorem of Galois Theory.

Example 1.3.8. As we have already seen the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal and separable, therefore it is Galois. The elements of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ are:

$$\begin{aligned} id\colon \sqrt{2} &\mapsto \sqrt{2} \\ \sigma\colon \sqrt{2} &\mapsto -\sqrt{2}. \end{aligned}$$

The subgroups of $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ are $< id >$ and itself.
The correspondent intermediate fields are: $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}$.

Example 1.3.9. The extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is clearly separable, since $char(\mathbb{Q}) = 0$. It is also normal because it is the splitting field for the polynomials $\{x^2-2, x^2-3\}$. Therefore, it is a Galois extension. Since $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, its Galois group G is given by the four following elements:

$$\begin{aligned} id\colon \sqrt{2} &\mapsto \sqrt{2}, \sqrt{3} \mapsto \sqrt{3} \\ \sigma\colon \sqrt{2} &\mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3} \\ \tau\colon \sqrt{2} &\mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3} \\ \sigma\tau\colon \sqrt{2} &\mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}. \end{aligned}$$

The subgroups of G are: $< id >, < \sigma >, < \tau >, < \sigma\tau >, G$.
The correspondent intermediate fields are: $\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6}), \mathbb{Q}$.

1.4 Simple Extensions

An extension K/F is called *simple* if there is an element $\alpha \in K$ such that K can be written as $F(\alpha)$. We present now some special properties of simple extensions that help us doing some calculations.

Proposition 1.4.1. *Given a finite simple extension $F(\alpha)/F$, we have that*

$$[F(\alpha) : F] = deg(Min(F, \alpha)).$$

Proof. See [3], Proposition 1.15. □

As a consequence of the above theorem, we have the following examples:

Example 1.4.2. Every extension with degree 2 is a simple normal extension. If $[K : F] = 2$, then we have that $K = F(\alpha)$, where α is a root of an irreducible polynomial p of degree 2. Hence, $p(x) = (x - \alpha)g(x)$, then g must have degree 1, therefore K is a splitting field for p.

Example 1.4.3. The extension $\mathbb{F}_2(\sqrt{t})/\mathbb{F}_2(t)$ is normal, however it is not separable. This extension is normal because $[\mathbb{F}_2(\sqrt{t}) : \mathbb{F}_2(t)] = 2$, however, the polynomial $X^2 - t$ has only one root in $\mathbb{F}_2(\sqrt{t})$ that is $\sqrt{t}$.

Proposition 1.4.4. *Let* $\deg(Min(F, \alpha)) = n$*. The simple extension* $F(\alpha)/F$ *is Galois if and only if* $Min(F, \alpha)$ *have* n *distinct roots in* $F(\alpha)$*. Furthermore,* $\mathrm{Gal}(F(\alpha)/F)$ *have* n *elements and each element of the group takes* α *to a different root of* $Min(F, \alpha)$*.*

Proof. If $F(\alpha)/F$ is Galois, then $Min(F, \alpha)$ splits over $F(\alpha)$ because $F(\alpha)/F$ is normal, and $Min(F, \alpha)$ have n different roots because $F(\alpha)/F$ is separable.

On the other hand, if $Min(F, \alpha)$ have n distinct roots in $F(\alpha)$, then $F(\alpha)$ is a splitting field for the separable polynomial $Min(F, \alpha)$, and therefore $F(\alpha)/F$ is Galois, by Theorem 1.3.6.

The last part of the proposition is a direct consequence of the Propositions 1.3.2 and 1.3.5. □

Another reason to focus on simple extensions is that every finite extension over a field with characteristic zero is a simple extension. This is a consequence of the next theorem.

Theorem 1.4.5 (Primitive element theorem)**.** *Let* K/F *be a separable extension of finite degree. Then* K/F *is a simple extension.*

Proof. See Corollary 5.7 in [3]. □

We give now some examples of simple extensions:

Example 1.4.6. The extension $\mathbb{C}/\mathbb{R}$ is a classic example of a simple extension. We can write $\mathbb{C} = \mathbb{R}(i)$.

Example 1.4.7. Every finite extension over $\mathbb{Q}$ is simple. For example the extension $\mathbb{Q}(\sqrt{3}, \sqrt{7})/\mathbb{Q}$ can be rewritten as $\mathbb{Q}(\sqrt{3} + \sqrt{7})/\mathbb{Q}$.

We have seen that given a finite Galois extension we can find a finite group that is associated to it. But is the converse true, i.e., fixed a field F and given a finite group G, is there any finite extension K of F such that $G = \mathrm{Gal}(K/F)$? This problem is known as **Inverse Galois Problem**, and it will be one of the motivations behind the property at the core of this dissertation: The Hilbert Property.

Chapter 2

Preliminaries on Classical Algebraic Geometry

2.1 Algebraic Varieties

On this second chapter, we introduce some concepts from classical algebraic geometry that are used through the dissertation. Let k be an algebraically closed field. We denote by $\mathbb{A}^n_k$ (or simply $\mathbb{A}^n$) the affine space k^n. We start by introducing a topology for this space that connects its closed sets with ideals in $k[x_1, \ldots, x_n]$. This topology is called *Zariski topology.*

Definition 2.1.1 (Zariski Closed set of $\mathbb{A}^n$)**.** Let $A = k[x_1, \ldots, x_n]$ be the ring of polynomials in n variables with coefficients in the field k. Given a family T of polynomials in A, we denote by $Z(T) = \{x \in \mathbb{A}^n | f(x) = 0 \text{ for every } f \in T\}$. We say that $X \subseteq \mathbb{A}^n_k$ is a *Zariski closed set* if $X = Z(T)$ for some family T of polynomials in A.

Remark 2.1.2. Given a family of polynomials T in $k[x_1, \ldots, x_n]$, $Z(T) = Z(\mathcal{A})$, where $\mathcal{A}$ is the ideal generated by the polynomials of T. Also, since $k[x_1, \ldots, x_n]$ is noetherian, every ideal $\mathcal{A} \subset k[x_1, \ldots, x_n]$ is finitely generated, thus $Z(T)$ can be expressed as a common zero of a finite family of polynomials.

In what follows we verify that this definition of closed set endows indeed the affine space with a topology.

Proposition 2.1.3.

- *Any finite union of closed sets is also a closed set.*
- *Any arbitrary intersection of closed sets is a closed set.*
- *The empty set and $\mathbb{A}^n$ are closed sets.*

Therefore, calling τ the collection of complements of the closed sets (open sets), we have that the pair $(\mathbb{A}^n, \tau)$ is a topological space.

Proof. See Proposition 1.1, chapter I of [4]. $\square$

In our study, we want to look to a special class of closed sets. This is why we introduce the next definition.

Definition 2.1.4 (Irreducible set)**.** A non-empty set Y of a topological space is said to be *irreducible* if it cannot be written as the union of two proper subsets that are closed in Y.

Example 2.1.5. The closed set defined by $Z(x^2+1)$ is not an irreducible set over $\mathbb{C}$ because it can be written as $Z(x-i) \cup Z(x+i)$.

Definition 2.1.6 (Affine Variety)**.** A closed irreducible set of $\mathbb{A}^n$ (with the induced topology) is called an *affine variety.*

Example 2.1.7. Consider $f \in k[x_1, \dots, x_n]$, f is an irreducible polynomial. Then, $Z(f)$ is an affine variety. Moreover, varieties of this type have a special name. They are called *hypersurfaces* of $\mathbb{A}^n$.

We have just seen that we can associate every closed set to an ideal in $k[x_1, \dots, x_n]$. We see now that we can reverse the direction.

Given $Y \subseteq \mathbb{A}^n$, we define $I(Y)$ the ideal of Y in $k[x_1, \dots, x_n]$ as:

$$I(Y) = \{f \in k[x_1, \dots, x_n] | f(x) = 0, \text{ for all } x \in Y\}.$$

In fact, there is a bijection between the closed sets and some of the ideals of $k[x_1, \dots, x_n]$. The next definition will be important to establish this correspondence.

Definition 2.1.8 (Radical Ideal)**.** An ideal I of the commutative ring A is a radical ideal if $I = \sqrt{I}$, where $\sqrt{I} = \{a \in A | a^n \in I \text{ for some } n \in \mathbb{N}\}$.

The next result is a very famous theorem called the Nullstellensatz. It was proven by David Hilbert in 1893, and it lies in the core of algebraic geometry because it gives us a "dictionary" between algebraic objects and geometric ones.

Theorem 2.1.9 (Nullstellensatz)**.** *Let k be an algebraically closed field, and $\mathcal{A}$ an ideal of $k[x_1, \dots, x_n]$. Consider f a polynomial in $k[x_1, \dots, x_n]$ such that $f(a) = 0$ for every $a \in Z(\mathcal{A})$, then $f^r \in \mathcal{A}$ for some integer r.*

Proof. See Corollary of Proposition A.9 in [5]. $\square$

We have the following corollary.

Corollary 2.1.10. For any ideal $\mathcal{A} \subset k[x_1, \dots, x_n]$, $I(Z(\mathcal{A})) = \sqrt{\mathcal{A}}$. Therefore, there is a bijection between the Zariski closed subsets and the radical ideals of $k[x_1, \dots, x_n]$. This happens by associating a closed set Y to $I(Y)$ and a radical ideal $\mathcal{A}$ to $Z(\mathcal{A})$. Moreover, a closed set is irreducible if and only if its associated ideal is prime.

Proof. See Corollary 1.4 of chapter I in [4]. □

The fact that k is algebraically closed is essential to theorem as we can see in the next example:

Example 2.1.11. Consider the ideal $J = (x^2 + 1)$ in $\mathbb{R}[x]$. We have that $Z(J) = \emptyset$, and then $I(Z(J)) = I(\emptyset) = \mathbb{R}[x]$. However, $\sqrt{J} = J \neq \mathbb{R}[x]$.

Consider Y an affine variety. Given f and p polynomials in $k[x_1, \dots, x_n]$, if $f - p \in I(Y)$, we have that $f(y) = p(y)$ for every $y \in Y$. This is the motivation to introduce the concept of affine coordinate ring.

Definition 2.1.12 (Affine coordinate ring)**.** If $Y \subseteq \mathbb{A}^n$ is closed set, we define the *affine coordinate ring* $A(Y)$ of Y to be $k[x_1, \dots, x_n]/I(Y)$. When Y is an algebraic variety, we have that $I(Y)$ is prime, and so $A(Y)$ is a domain.

We also want to study the open sets of affine varieties.

Definition 2.1.13 (Quasi-affine Varieties)**.** The open set of an affine variety is called *quasi-affine variety.* We define the Zariski topology of quasi-affine varieties as the topology induced by Zariski topology on affine varieties.

Example 2.1.14. Since every point is a closed set of $\mathbb{A}^n$, $\mathbb{A}^n \backslash \{0\}$ is a quasi-affine variety.

Now, we look at varieties in the projective space. For that purpose, let us first recall the definition of projective space.

Definition 2.1.15 (Projective Space)**.** Let k be a field. Consider the equivalence relation in $\mathbb{A}^{n+1} \backslash \{0\}$ given by: $(a_0, \dots, a_n) \sim (\lambda a_0, \dots, \lambda a_n)$ for all $\lambda \in k, \lambda \neq 0$. We define the *projective space of dimension* n, denoted by $\mathbb{P}^n$, as the quotient of $\mathbb{A}^{n+1} \backslash \{0\}$ under the above equivalence relation. We represent the elements of $\mathbb{P}^n$ as $(a_0 : \cdots : a_n)$.

We want to define the closed sets of $\mathbb{P}^n$ in a similar way that we have defined for $\mathbb{A}^n$. However, we want to choose polynomials f such that $f(P) = 0$ for any choice of coordinates. Hence, f needs to be homogeneous.

Definition 2.1.16 (Zariski Closed set of $\mathbb{P}^n$)**.** A subset $Y \subseteq \mathbb{P}^n$ is said to be a *Zariski closed set* if $Y = Z(T)$, where T is a set of homogeneous polynomials in $k[x_0, \dots, x_n]$.

A version of the Proposition 2.1.3 can be shown for the closed sets of $\mathbb{P}^n$, allowing us to define a topology for $\mathbb{P}^n$.

Definition 2.1.17 (Projective and Quasi-Projective Varieties)**.** An irreducible closed set of $\mathbb{P}^n$ is called a *projective variety.* An open set of a projective variety is called a *quasi-projective variety.*

We also have a relation between the closed sets of the projective space $\mathbb{P}^n$ and certain ideals of $k[x_0, \dots, x_n]$. However, now we have to look to the homogeneous ideals of $k[x_0, \dots, x_n]$, ideals that can be generated by homogeneous elements.

In this case, given $Y \subseteq \mathbb{P}^n$, we define

$$I(Y) = \{f \in k[x_0, \dots, x_n] \text{ and homogeneous } | f(x) = 0 \text{ for all } x \in Y\}.$$

We can define the homogeneous coordinate ring of Y, which we denote by $S(Y)$, to be $k[x_0, \dots, x_n]/I(Y)$.

Then, we can state an analogous version of Corollary 2.1.10:

Proposition 2.1.18. *Let k be an algebraically closed field. There is a bijection between the closed sets of $\mathbb{P}^n$ and the radical homogeneous ideals of $k[x_0, \dots, x_n]$, except for the ideal $(x_0, \dots, x_n)$. This happens by associating a closed set $Y \mapsto I(Y)$ and a radical homogeneous ideal $\mathcal{A} \mapsto Z(\mathcal{A})$. Moreover, a closed set is irreducible if and only if its associated ideal is prime.*

This relation between ideals and closed sets and the fact that $k[x_1, \dots, x_n]$ is a noetherian ring permit us to conclude the following result:

Theorem 2.1.19. *Every closed set X can be written in a unique way as a finite union of irreducible closed subsets.*

Proof. See Theorems 1.4 and 1.5 in [5], Section 3.1, chapter 1. □

The irreducible closed subsets mentioned in the above theorem are called the *irreducible components of X.*

To conclude this section, we show that every projective variety can be written as a finite union of open sets that are homeomorphic to affine varieties.

Let us consider the following injection:

$$\phi_0 \colon \mathbb{A}^n \to U_0 := \mathbb{P}^n \backslash Z(x_0)$$
$$(x_1, \dots, x_n) \mapsto (1 : x_1 : \dots : x_n)$$

and its inverse:

$$\psi_0 \colon U_0 \to \mathbb{A}^n$$
$$(x_0 : x_1 : \dots : x_n) \mapsto (\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}).$$

These two functions are homeomorphisms with respect to the Zariski topology. Furthermore, we can write $\mathbb{P}^n = \bigcup_{i=0}^n U_i$, where $U_i = \mathbb{P}^n \backslash Z(x_i)$. Given a projective variety (a closed and irreducible set) $Y \subseteq \mathbb{P}^n$, we can write $Y = \bigcup_{i=0}^n (Y \cap U_i)$, showing what we claimed.

2.2 Morphisms

When studying algebra, we are not just interested in the objects, but also on the relations between them that preserve some kind of structure, namely the morphisms. In what follows, we define morphisms of algebraic varieties. However, in order to do it, we need first to introduce the concept of regular functions.

Definition 2.2.1 (Regular function for a quasi-affine variety)**.** Let $Y \subseteq \mathbb{A}^n$ be a quasi-affine variety. A function $f \colon Y \to k$ is *regular at a point* P if there is an open neighbourhood U, $P \in U \subseteq Y$ and polynomials g and h, such that h is nowhere zero on U, and $f = g/h$ on U. We say that f is *regular on* Y if it is regular at every point of Y.

Definition 2.2.2 (Regular function for a quasi-projective variety)**.** Let $X \subseteq \mathbb{P}^n$ be a quasi-projective variety. A function $f \colon X \to k$ is *regular at a point* P if there is an open neighbourhood U, $P \in U \subseteq X$, and homogeneous polynomials F and G with the same degree, such that G is nowhere zero on U, and $f = F/G$ on U. We say that f is *regular on* X if it is regular at every point of X.

From now on, we use the word variety when referring to any affine, quasi-affine, projective or quasi-projective variety.

Remark 2.2.3.

1. We denote by $\mathcal{O}(X)$, the set of regular functions of a variety X, which is a k-algebra.

2. When X is an affine variety, $\mathcal{O}(X) = A(X)$ (the coordinate ring of X). (See Theorem 3.2 in [4]).

3. When X is a projective variety $\mathcal{O}(X) = k$ (see Theorem 5.2 in [5]).

Definition 2.2.4 (Morphisms)**.** If X and Y are two varieties, a map $\phi \colon X \to Y$ is said to be a *morphism* if:

1. ϕ is continuous.

2. For every open set $V \subset Y$ and for every regular function $f \colon V \to k$, the function $f \circ \phi \colon \phi^{-1}(V) \to k$ is regular.

We say that a morphism ϕ is an *isomorphism* if its inverse is also a morphism.

We see an example.

Example 2.2.5. The functions ϕ_0 and ψ_0 defined in the end of the last section are morphisms. Therefore, the open sets $U_i = \mathbb{P}^n \backslash Z(x_i)$ are isomorphic to $\mathbb{A}^n$.

We notice that since $\mathbb{A}^n$ is isomorphic to a open set of $\mathbb{P}^n$, every affine and quasi-affine varieties can be seen as quasi-projective varieties.

This example also gives the cue for our next definition.

Definition 2.2.6 (Affine open set)**.** An open U of a quasi-projective variety is called *affine open set* if it is isomorphic to an affine variety.

We can rewrite the result of the of the last section by saying that every projective variety has a cover of affine open sets. In fact, this is true for every quasi-projective variety (See Lemma 1.3, section 4.2, chapter 1 in [5]). This affine open cover is, in fact, a finite one, since $\mathbb{P}^n$ with Zariski topology is a noetherian topological space, i.e., every ascending chain of open sets is stationary.

We see now the importance of the second condition of the definition of morphism. Given a morphism $\phi\colon X \to Y$, we can define a homomorphism $\phi^*\colon \mathcal{O}(Y) \to \mathcal{O}(X)$ between k-algebras, where $\phi^*(f) = f \circ \phi$. We say that ϕ^* is the *pullback of* ϕ. The correspondence $\phi \to \phi^*$ is functorial, in particular, if X and Y are isomorphic as algebraic varieties, then $\mathcal{O}(X)$ and $\mathcal{O}(Y)$ are isomorphic as k-algebras. The reciprocal is not generally true, however it is in the case that both X and Y are affine (see Corollary 3.7 in [4]).

We conclude this section with examples of morphisms and of the pullback homomorphisms induced by them.

Example 2.2.7. Consider $X = \mathbb{A}^1$ and $Y = Z(y - x^2) \subset \mathbb{A}^2$. The function

$$\begin{aligned} f\colon Y &\to X \\ (x,y) &\mapsto x \end{aligned}$$

is an isomorphism.

Its inverse is given by the following morphism

$$\begin{aligned} g\colon X &\to Y \\ t &\mapsto (t, t^2). \end{aligned}$$

The pullbacks of f and g are defined bellow

$$\begin{aligned} f^*\colon \mathcal{O}(X) = k[t] &\to \mathcal{O}(Y) \\ t &\mapsto \ t \end{aligned}$$

$$\begin{aligned} g^*\colon \mathcal{O}(Y) = &\to \mathcal{O}(X) \\ \phi(\bar{x}, \bar{y}) &\mapsto \phi(t, t^2) \end{aligned}$$

Therefore, we conclude that $\mathcal{O}(X) \simeq \mathcal{O}(Y) = k[t]$.

Example 2.2.8. Consider $X = \mathbb{A}^1 \backslash \{0\}$ and $Y = Z(xy - 1) \subset \mathbb{A}^2$. The function

$$\begin{aligned} f\colon Y &\to X \\ (x, y) &\mapsto x \end{aligned}$$

is a morphism and its inverse g is defined bellow

$$\begin{aligned} g\colon X &\to Y \\ t &\mapsto (t, 1/t). \end{aligned}$$

In the same way we did in the previous example, we conclude that

$$\mathcal{O}(Y) \simeq \mathcal{O}(X) = k[x, 1/x].$$

2.3 Function Fields and Rational maps

In this section, we introduce an essential concept: function fields. We also discuss the relation that exists between two varieties that have the same function field.

Definition 2.3.1 (Function field)**.** Let X be a variety. We define the *function field of* X, denoted by $k(X)$, by defining its elements, the rational functions. A *rational function* is an equivalence class of pairs (U, f_U), where U is a non-empty open set and $f_U \in \mathcal{O}(U)$. Two pairs (U, f_U) and (V, f_V) are equivalent if $f_U = f_V$ on $U \cap V$.

Remark 2.3.2. Notice that given $U \subset X$ an open set, $k(U) = k(X)$.

We are interested now in studying transformations between varieties that are not necessarily defined on the entire domain. This is the motivation for the next definition.

Definition 2.3.3 (Rational map)**.** Consider the varieties X and Y. A *rational map* $\phi\colon X \dashrightarrow Y$ is an equivalence class of pairs (U, ϕ_U), where U is a non-empty open set and $\phi_U\colon U \to Y$ is a morphism. Two pairs (U, ϕ_U) and (V, ϕ_V) are equivalent if $\phi_U = \phi_V$ on $U \cap V$.

The domain of definition of ϕ is the biggest open set $U \subset X$ such that it exists a representative of ϕ with the form (U, ϕ_U).

The composition of two rational maps is not necessarily well-defined. For this reason, we will be interested on dominant rational maps, defined as bellow:

Definition 2.3.4 (Dominant rational map)**.** A rational map $\phi \colon X \dashrightarrow Y$ is said to be *dominant* if there is a representative (U, ϕ_U) such that $\phi_U(U)$ is dense in Y.

Definition 2.3.5 (Birational map)**.** A dominant rational map $\phi \colon X \dashrightarrow Y$ is said to be *birational* if it has an inverse that is also a dominant rational map. In this case, we say that X and Y are *birationally equivalent.*

Birational maps preserve some properties between varieties, and for that reason, it is natural to give a special attention to varieties that are birationally equivalent to $\mathbb{A}^n$ or to $\mathbb{P}^n$.

Definition 2.3.6 (Rational Variety)**.** A variety X is called *rational* if it is birationally equivalent to $\mathbb{A}^n$ or $\mathbb{P}^n$ for some n.

Let $\phi \colon X \dashrightarrow Y$ be a dominant rational map, we can verify that given $f \in k(Y)$, then $f \circ \phi \in k(X)$. This allows us to define $\phi^* \colon k(Y) \to k(X)$ a injective homomorphism between function fields over k (ϕ^* is injective because ϕ is dominant).

The next theorem gives us more relations between two birationally equivalent varieties and their function fields.

Theorem 2.3.7. *Consider the varieties X and Y. Then the following conditions are equivalent:*

- *X and Y are birationally equivalent.*
- *There are non-empty open sets $U \subseteq X$ and $V \subseteq Y$ such that U and V are isomorphic.*
- *$k(X)$ is isomorphic to $k(Y)$ as k-algebras.*

Proof. See Corollary 4.5 in [4]. □

Remark 2.3.8. An interesting particular case happens when X is a non-singular projective curve. In this case, X can be uniquely determined by its function field $k(X)$. This result can found in [7], Corollary of Theorem 3, chapter 7.

Another special type of variety that will have a fundamental role in our study are the unirational varieties.

Definition 2.3.9 (Unirational Variety)**.** We say that a variety X is *unirational* if there is a dominant rational map $\phi \colon \mathbb{P}^n \dashrightarrow X$.

A unirational variety has also the following properties:

Theorem 2.3.10. *Let X be a variety over k. The following are equivalent:*

- *X is unirational.*
- *$k(X)$, the function field of X, is contained in a purely transcendental field extension of k.*
- *There is a finite extension of $k(X)$ which is a purely transcendental field extension of k.*

Proof. The proof can be found in Lemma 7.8 in [6]. □

Remark 2.3.11. We can ask ourselves: Is every unirational variety also rational? This question is known as the Lüroth Problem, and although it is true for one and two dimensional varieties over algebraically closed fields with characteristic zero, we can find some counterexamples in dimension 3, see [8].

To conclude this section, we introduce a definition that is very useful when we study local properties of a variety X, the local ring of X at a point x. We start giving two definitions of commutative algebra.

Definition 2.3.12 (Local ring and residue field)**.** A ring A is said to be *local* if A has only one maximal ideal m. The field A/m is called the *residue field of A*.

Definition 2.3.13 (Localization at a prime ideal)**.** Consider an integral domain A and P a prime ideal of A. The localization of A at P is denoted by A_P and given by

$$A_P = \Big\{ \frac{f}{g} | f, g \in A \text{ and } g \notin P \Big\}.$$

Definition 2.3.14 (Local ring at a point)**.** Consider a variety X and a point $x \in X$. The local ring of X at x is denoted by $\mathcal{O}_{x,X}$ and it is defined in the following way

$$\mathcal{O}_{x,X} = \big\{ f \in K(X) | f \text{ is regular at } x, \text{ i.e. there is an open set } U \text{ such that } x \in U \text{ and } f \in \mathcal{O}(U) \big\}.$$

The following remarks are immediate consequences of the definition.

Remark 2.3.15.

1. $\mathcal{O}_{x,X}$ is a local ring with maximal ideal $m_x = \{ f \in \mathcal{O}_{x,X} | f(x) = 0 \}$.
2. The residue field of $\mathcal{O}_{x,X}$ is isomorphic to k.
3. If U is an open set, $x \in U$, then $\mathcal{O}_{x,U} \simeq \mathcal{O}_{x,X}$.

2.4 Finite Morphisms

In this section, we introduce the finite morphisms. We start with a basic concept of commutative algebra, necessary for the definition of finite morphisms.

Definition 2.4.1 (Integral Extension of a ring)**.** Let A and B be commutative rings such that $A \subset B$. We say that an element $b \in B$ is *integral over* A if it is the root of a monic polynomial in $A[x]$. We say that B is *integral over* A if every element of B is integral over A.

Remark 2.4.2. If B is finitely generated as an A-algebra, B is integral over A if and only if B is a finite A-module (See [9], Proposition 5.1 and Corollary 5.2).

Remark 2.4.3. If x and y are integral over A, then $x + y$ and xy are also integral over A.(See [9], Corollary 5.3).

We first define finite morphisms between affine varieties.

Definition 2.4.4 (Finite morphisms of affine varieties)**.** Let X and Y be affine varieties and $f\colon X \to Y$ a dominant morphism. Since f is a dominant morphism, $f^*\colon \mathcal{O}(Y) \to \mathcal{O}(X)$ is injective. We say that f is *finite* if $\mathcal{O}(X)$ is integral over $f^*(\mathcal{O}(Y))$.

Example 2.4.5. Let $Y = Z(y^2 - x^3) \subset \mathbb{A}^2$. Consider the morphism

$$\begin{aligned} \psi\colon \mathbb{A}^1 &\to Y \\ t &\mapsto (t^2, t^3). \end{aligned}$$

Notice that $\mathcal{O}(Y) = k[t^2, t^3]$ and that ψ^* is the inclusion of $k[t^2, t^3]$ in $k[t] = \mathcal{O}(\mathbb{A}^1)$. It is easy to see that t is integral over $k[t^2, t^3]$, hence ψ is finite.

Example 2.4.6. Let $Y = Z(xy - 1) \subset \mathbb{A}^2$. Consider the morphism ϕ

$$\begin{aligned} \phi\colon Y &\to \mathbb{A}^1 \\ (x, y) &\mapsto x. \end{aligned}$$

ϕ is not finite. In fact, we have that ϕ^* is the inclusion of $k[t]$ in $k[t, 1/t] = \mathcal{O}(Y)$ and $k[t, 1/t]$ is not a finite $k[t]$-module.

We now see some properties of finite morphisms.

Theorem 2.4.7. *Let X and Y be affine varieties and $f\colon X \to Y$ a finite map . Then f holds the following properties:*

1. *For every $y \in Y$, $f^{-1}(y)$ is a finite set.*

2. f is surjective.

3. f is a closed map, i.e, takes closed sets to closed sets.

Proof. The proof of these three properties can be found in page 61, section 5.3 of [5]. □

When X is affine, $k(X)$ is isomorphic to the quotient field of $\mathcal{O}(X)$ (see Theorem 3.2 in [4]). Therefore, an injective homomorphism $f^*\colon \mathcal{O}(Y) \to \mathcal{O}(X)$ induces a injective homomorphism $\hat{f}\colon k(Y) \to k(X)$, $\hat{f}(a/b) = f^*(a)/f^*(b)$. We see that the existence of a finite morphism between X and Y give us some information about the extension $k(X)/k(Y)$.

Theorem 2.4.8. *Let X and Y be affine varieties and $f\colon X \to Y$ a finite morphism. Then, $k(X)/\hat{f}(k(Y))$ is a finite field extension.*

Proof. We have that $k(X)$ is finitely generated as a field over k, since $k(X)$ is the fraction field of the finitely generated k-algebra $k[x_1, \dots, x_n]/I(X)$. Hence $k(X)$ is clearly finitely generated as a field over $\hat{f}(k(Y))$. Hence, to show that $k(X)/\hat{f}(k(Y))$ is a finite extension, it is enough to prove that $k(X)$ is algebraic over $\hat{f}(k(Y))$.

Since f is finite, $\mathcal{O}(X)$ is algebraic over $\hat{f}(k(Y))$. Since the elements that are algebraic over a field form a subring, to complete the proof, we only need to show that $1/b$ is algebraic over $\hat{f}(k(Y))$, for every $b \in \mathcal{O}(X)$. Since b is integral over $f^*(\mathcal{O}(Y))$, there are $a_0, \dots, a_{k-1} \in f^*(\mathcal{O}(Y))$ such that

$$b^k + a_n b^{k-1} + \cdots + a_0 = 0.$$

Multiplying this expression by $1/b^k$, we obtain

$$1 + a_n/b + \cdots + a_0/b^k = 0$$

and so $1/b$ is algebraic over $\hat{f}(k(Y))$. □

This last theorem motivates another definition.

Definition 2.4.9 (Degree of a finite morphism)**.** Given X and Y two affine varieties and $f\colon X \to Y$ a finite morphism. Then, we define the *degree of f*, denoted by $\deg f$ as

$$\deg f = [k(X) : \hat{f}(k(Y))].$$

We can extend this definition for a general quasi-projective variety as we see now.

Definition 2.4.10 (Finite morphims for quasi-projective varieties)**.** Let $f\colon X \to Y$ be a dominant morphism between quasi-projective varieties. We say that f is *finite* if every $y \in Y$ has an affine neighbourhood V such that the set $U = f^{-1}(V)$ is affine and $f|_U\colon U \to V$ is finite.

An affine variety is a particular case of quasi-projective variety, and so we must verify that this definition of finite morphisms for quasi-projective varieties is compatible with the original one. We see this in the next theorem.

Theorem 2.4.11. *Let $f\colon X \to Y$ be a dominant morphism between affine varieties. Suppose that every $y \in Y$ has an affine neighbourhood V such that the set $U = f^{-1}(V)$ is affine and $f|_U\colon U \to V$ is finite. Then, f is a finite morphism according to the definition 2.4.4.*

Theorems 2.4.7 and 2.4.8 still hold for finite morphisms between quasi-projective varieties. We can also define the degree of a finite morphism between quasi-projective varieties in the same way we have done for the affine case.

The next two theorems give us some motivation for defining a dimension of projective varieties, the topic of the next section. The first one is a geometric version of a famous theorem in commutative algebra, called Noether's Normalisation Theorem.

Theorem 2.4.12 (Noether's Normalisation Theorem)**.** *Let X be a projective variety. Then, for some $n \in \mathbb{N}$, there exists a finite morphism $f\colon X \to \mathbb{P}^n$.*

Proof. The proof can be found in [5], Theorem 1.17, section 5.3, chapter 1. □

Theorem 2.4.13. *Let Y be an affine variety. Then, for some $m \in \mathbb{N}$, there exists a finite morphism $\phi\colon Y \to \mathbb{A}^m$.*

Proof. The proof can be found in [5], Theorem 1.18, section 5.3, chapter 1.

□

2.5 Dimension

In this section, we introduce the notion of dimension for quasi-projective varieties. Before giving a definition, we discuss some properties that this definition must satisfy.

First, we expect the dimensions of $\mathbb{P}^n$ and of $\mathbb{A}^n$ to be equal n (1). Since every non-empty open set U of a variety X is dense, we also expect the dimension of U to be equal the dimension of X (2). Classical algebraic geometry was in many aspects inspired by differential geometry, thus it is also natural to demand that, given two varieties X and Y, the dimension of $X \times Y$ is equal to the sum of dimensions of X and Y, in the same way that occurs with manifolds (3). Given F an irreducible homogeneous polynomial in $k[x_0, \dots, x_n]$, we also want $Z(F) \subset \mathbb{P}^n$ to have the same dimension as the hypersurfaces of differential geometry, that is $\dim Z(F) = n - 1$ (4).

We see two equivalent definitions for dimension, the motivation for the first one comes from the end of the last section. We have seen that given an affine variety

X, there is always a finite morphism $f\colon X \to \mathbb{A}^n$, for some $n \in \mathbb{N}$. We could define the dimension of X to be equal to n in this case, however is this definition well-defined? In fact, by Theorem 2.4.8, the existence of the finite morphism f implies that $k(X)/\hat{f}(k(x_1, \dots, x_n))$ is a finite extension, hence the transcendence degree of $k(X)/k$ is equal to n. This leads to our first definition of dimension.

Definition 2.5.1 (First definition of dimension)**.** Let X be a quasi-projective variety such that $k(X)/k$ is a finitely generated extension. We define the *dimension of* X, denoted by $\dim X$, to be equal the transcendence degree of the extension $k(X)/k$. The *dimension* of a closed set $Y \subset \mathbb{P}^n$ is the maximum of the dimension of its irreducible components.

From this definition, it is immediate to see that the dimension is invariant by birational equivalence, and that the properties (1) and (2) are satisfied. We also notice that if there is a finite morphism between two varieties, they have the same dimension. The proof of property (3) can be found in [5], example 1.33 of section 6.1, chapter 1. We now present property (4) and other interesting related results.

Proposition 2.5.2. *Consider X and Y quasi-projective varieties, such that $X \subseteq Y$, then $\dim X \leq \dim Y$. If X is a closed set and $\dim X = \dim Y$, then $X = Y$.*

Proof. See Theorem 1.19 in [5], section 6.1, chapter 1. □

Theorem 2.5.3. *Given a non-constant polynomial $f \in k[x_1, \dots, x_n]$, the dimension of $Z(f) \subset \mathbb{A}^n$ is equal to $n-1$.*

Proof. See Theorem 1.20 in [5], section 6.1, chapter 1. □

The reciprocal result is also true:

Theorem 2.5.4. *Let $X \subset \mathbb{A}^n$ be an affine variety with dimension equal to $n-1$. Then, there is an irreducible polynomial $f \in k[x_1, \dots, x_n]$ such that $Z(f) = n-1$.*

Proof. See Theorem 1.21 in [5], section 6.1, chapter 1. □

Theorem 2.5.3 can be generalized for an arbitrary projective variety as we see bellow:

Theorem 2.5.5. *Let $X \subset \mathbb{P}^n$ be a projective variety of dimension n and F be a homogeneous polynomial in $k[x_0, \dots, x_n]$ such that $F \notin I(X)$. Then every irreducible component of $X \cap Z(F)$ has dimension equal to $n-1$.*

Proof. See Theorem 1.22 in [5], section 6.2, chapter 1. □

This last theorem will allow us to formulate another definition of dimension, a topological one.

Definition 2.5.6 (Second definition of dimension)**.** Let X be a topological noetherian space, i.e. every descending chain of closed sets of X is stationary. The *topological dimension of* X, denoted by $\dim_{\text{top}} X$, is defined as the supremum of all integers n for which there exists a strictly decreasing chain $X = X_0 \supsetneq X_1 \supsetneq \ldots X_n \neq \emptyset$ of length n of subvarieties of X.

Proposition 2.5.7. *Given a quasi-projective variety* X*,* $\dim X = \dim_{\text{top}} X$*.*

Proof. We can consider, without loss of generality, that X is a projective variety. Suppose $\dim_{\text{top}} X = n$, then there is a strictly decreasing chain of varieties

$$X = X_0 \supsetneq X_1 \supsetneq \cdots \supsetneq X_n \neq \emptyset.$$

By Proposition 2.5.2, $\dim X > \dim X_1 > \cdots > \dim X_n$, hence $\dim X \geq n = \dim_{\text{top}} X$. On the other hand, if $\dim X = r$, Theorem 2.5.5 enable us to construct a strictly decreasing chain of varieties

$$X = Y_0 \supsetneq Y_1 \supsetneq \cdots \supsetneq Y_r \neq \emptyset$$

such that $\dim Y_i = n - i$, and so $\dim_{\text{top}} X \geq r$. Therefore, $\dim X = \dim_{\text{top}} X$. □

Remark 2.5.8. In commutative algebra, we define the *height of a prime ideal* $\mathfrak{p}$ as the supremum of all integers n such that there exists a strictly ascending chain of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$. The *Krull dimension of a ring* A, denoted by $\dim_{\text{Krull}} A$, is the supremum of the heights of all prime ideals in A. As we have already seen the Nullstellensatz establishes a bijection between prime ideals and affine varieties. From this bijection, we conclude that for an affine variety X, the $\dim_{\text{top}} X = \dim_{\text{Krull}} \mathcal{O}(X)$.

2.6 Normal Varieties

In the section 2.4, we introduced the concept of integral extension of a ring. In this section, we introduce a related concept, the definition of integrally closed rings. In fact, we are interested in studying varieties X that for every point $x \in X$, the local ring $\mathcal{O}_{x,X}$ is integrally closed.

Definition 2.6.1 (Integrally closed ring)**.** Consider A and B commutative rings such that $A \subset B$. The *integral closure of* A *in* B is a ring formed by elements of B that are integral over A. A domain A is *integrally closed* if every element of its field of fraction K that is integral over A is in A, i.e. if is the integral closure of A in K is equal to A.

Definition 2.6.2 (Normal Variety)**.** An affine variety X is said to be *normal* if $\mathcal{O}(X)$ is a integrally closed ring. A quasi-projective variety is *normal* if every point $x \in X$ has a normal affine neighbourhood.

Remark 2.6.3. From commutative algebra, we have that for an integral domain A to be integrally closed is equivalent to the localization A_m be integrally closed for each maximal ideal m (see this result in [9], Proposition 5.13). Therefore, a variety X is normal if and only if $\mathcal{O}_{x,X}$ is integrally closed for every $x \in X$.

There are several examples of normal varieties. For instance, $\mathbb{A}^n$ and $\mathbb{P}^n$, since $k[x_1, \ldots, x_n]$ is integrally closed over $k(x_1, \ldots, x_n)$. We see now an example of a non-normal variety.

Example 2.6.4. Consider the variety $X = Z(y^2 - x^3) \subset \mathbb{A}^2$. The coordinate ring $\mathcal{O}(X) = k[x, y]/(y^2 - x^3)$ is isomorphic to $k[t^2, t^3]$. The fraction field of $k[t^2, t^3]$ is $k(t)$, hence X is not a normal variety, since the integral closure of $k[t^2, t^3]$ in $k(t)$ is $k[t]$.

Even though X is not normal, there is a normal variety associated to $k[t]$ and a finite morphism between this normal variety and X, the morphism f defined bellow

$$\begin{aligned} f \colon \mathbb{A}^1 &\to X \\ t &\mapsto (t^2, t^3). \end{aligned}$$

We say that $\mathbb{A}^1$ and f in the above example form the *normalization of* X. In what follows, we define this concept properly.

Definition 2.6.5. The *normalization of a variety* X is a normal variety X^ν together with a finite birational morphism $\nu \colon X^\nu \to X$.

This definition lead us to the next theorem.

Proposition 2.6.6. *Every quasi-projective variety has a unique normalization. If X is affine, then X^ν is affine. If X is projective, then X^ν is also projective.*

Proof. See Theorem 7.17 in [16]. □

Remark 2.6.7. For an affine variety X, the normalization of X, X^ν, is such that $\mathcal{O}(X^\nu)$ is the integral closure of $\mathcal{O}(X)$ in its fraction field. This construction can be found at the proof of Theorem 2.20, section 5.2, chapter II, [5].

We give an example of the normalization of a projective variety.

Example 2.6.8. The variety X in $\mathbb{P}^2$ is given by $Z(zy^2 - x^3 - zx^2)$ is called the nodal curve. We show that the morphism

$$\begin{aligned} f \colon \mathbb{P}^1 &\to X \\ (t : u) &\mapsto (u(t^2 - u^2) : t(t^2 - u^2) : u^3) \end{aligned}$$

is a finite birational map and hence $\mathbb{P}^1$ and f are the normalization of X.

First, we have that

$$\begin{aligned} g\colon X &\dashrightarrow \mathbb{P}^1 \\ (x:y:z) &\mapsto (y/x:1) \end{aligned}$$

is the inverse of f, therefore f is birational.

In fact, if we denote by $U_1 = \mathbb{P}^1 \backslash Z(t)$ and by $V_1 = X \backslash Z(z)$, we have that $f\colon U_1 \to V_1$ induces an isomorphism f^* between $\mathcal{O}(V_1)$ and $\mathcal{O}(U_1)$, hence the restriction $f\colon U_1 \to V_1$ is a finite morphism.

In an analogous manner, if we denote by $U_2 = \mathbb{P}^1 \backslash Z(u)$ and by $V_2 = X \backslash Z(y)$, we conclude that the restriction $f\colon U_2 \to V_2$ is a finite morphism. Hence, since $X = V_1 \cup V_2$, f is a finite morphism.

We conclude this chapter introducing a particular case of the definition of ramification point. This definition will be used in section 3.3 and it will be fundamental in section 3.4 to connect the Hilbert Property with Algebraic Topology.

Definition 2.6.9 (Ramification point)**.** Given a finite map $f\colon X \to Y$ between irreducible quasi-projective varieties X and Y such that Y is a normal variety, we say that f *is ramified at* y, or equivalently y *is a ramification point of* f, if $|f^{-1}(y)| < \deg f$. Otherwise, $|f^{-1}(y)| = \deg f$ and we say that f *is unramified at* y. The set of the ramification points of f is often called the *ramification locus of* f.

Remark 2.6.10. This definition of being ramified or unramified is only valid when the codomain Y of $f\colon X \to Y$ is normal. Otherwise, it might exist an $y \in Y$ such that $|f^{-1}(y)| > \deg f$. We can see this in the example 2.6.8, the morphism f has degree 1, however $|f^{-1}([0:0:1])| = 2$.

Theorem 2.6.11. *Given $f\colon X \to Y$ a morphism between quasi-projective varieties, where Y is a normal variety. If $f^*(k(Y)) \subset k(X)$ is a separable field extension, the ramification locus of f is a proper closed set in Y.*

Proof. See Theorem 2.29 in section 6.3, chapter II of [5]. □

Chapter 3

The Hilbert Property and some of its connections

3.1 Historical Motivation

As we have seen in Chapter 1, in Galois theory, when a finite field extension K/F is Galois, we can establish a bijection between the subgroups of $Gal(K/F)$ and its intermediate fields. A natural question is if the converse is still true, that is, given a finite group G, and a field F, is there some Galois field extension K/F such that G is its Galois group? This problem is known as the Inverse Galois Problem (IGP), and we say that G is *realizable over* F if such a field K exists.

It seems reasonable to study this problem for a fixed field F. David Hilbert did that during the 19th century, choosing F as $\mathbb{Q}$, the field of rational numbers. Since the problem was already solved for finite abelian groups (to see the resolution of this particular case, read chapter 3 of [14]), Hilbert decided to focus on the case of finite symmetric groups S_n. In fact, this is an interesting case, specially because we know that every finite group is isomorphic to a subgroup of some S_n (Cayley's Theorem). The Symmetric groups have the following property:

Proposition 3.1.1. *The group S_n can be realized over $\mathbb{Q}(T_0, \dots, T_{n-1})$, a purely transcendental extension of $\mathbb{Q}$ with transcendence degree n.*

Before proving this proposition, let us recall a tool that is important for the proof, namely, the *elementary symmetric polynomials.* We denote by $e_i(X_1, \dots, X_n)$ the elementary symmetric polynomial in n variables $X_1, \dots, X_n$ of degree i. We have that:

$$\begin{aligned} e_0(X_1, X_2, \ldots, X_n) &= 1, \\ e_1(X_1, X_2, \ldots, X_n) &= \sum_{1 \le j \le n} X_j, \\ e_2(X_1, X_2, \ldots, X_n) &= \sum_{1 \le j < k \le n} X_j X_k. \end{aligned}$$

More generally

$$e_k(X_1, X_2, \ldots, X_n) = \sum_{1 \le j_1 < j_2 < \cdots < j_k \le n} X_{j_1} \cdots X_{j_k}.$$

Proof of the Proposition 3.1.1. Denote by K the field of rational functions $\mathbb{Q}(X_1, \ldots, X_n)$. Consider S_n acting on K by permuting the set $\{X_1, \ldots, X_n\}$ and fixing $\mathbb{Q}$. We denote by K^{S_n} the subfield of K fixed by S_n, as we did in the preliminary part. Let us consider the field $\mathbb{Q}(T_0, \ldots, T_{n-1})$, where $T_i = (-1)^{n-i} e_{n-i}(X_1, \ldots, X_n)$ and e_i are the above mentioned symmetric polynomials. This field is a purely transcendental extension of $\mathbb{Q}$ with transcendence degree n.

We start by proving that $K/\mathbb{Q}(T_0, \ldots, T_{n-1})$ is Galois.

Consider $f(x) = \prod_{i=1}^{n}(x - X_i)$. We can develop the product and rewrite f in the following way

$$f(x) = x^n + T_{n-1}x^{n-1} + \cdots + T_1 x + T_0.$$

Then, $f \in \mathbb{Q}(T_0, \ldots, T_{n-1})[x]$. As K is a splitting field for f and f is a separable polynomial, we have that $K/\mathbb{Q}(T_0, \ldots, T_{n-1})$ is Galois by Theorem 1.3.6.

We prove in what follows that $\mathrm{Gal}(K/\mathbb{Q}(T_0, \ldots, T_{n-1})) = S_n$.

The elementary symmetric polynomials are fixed by every permutation in S_n, thus $T_i \in K^{S_n}$ for every $0 \le i \le n-1$. As a consequence, $S_n \subseteq \mathrm{Gal}(K/\mathbb{Q}(T_0, \ldots, T_{n-1}))$. To show the other inclusion, consider $g \in \mathrm{Gal}(K/\mathbb{Q}(T_0, \ldots, T_{n-1}))$. By Proposition 1.3.2, we know that $g(X_i)$ must be another root of f, so g must permute the set $\{X_1, \ldots, X_n\}$, i.e $g \in S_n$. Therefore, $\mathrm{Gal}(K/\mathbb{Q}(T_0, \ldots, T_{n-1})) = S_n$.

□

This motivates another question: given a finite group G that can be realized over a field of the form $\mathbb{Q}(X_1, \ldots, X_n)$, can it also be realized over $\mathbb{Q}$? The answer to this question is positive. This is a consequence of the celebrated Hilbert's Irreducibility Theorem, which is stated bellow.

Theorem 3.1.2 (Hilbert's Irreducibility Theorem). *For any irreducible polynomial $f \in \mathbb{Q}[X_1, \ldots, X_s, Y_1, \ldots, Y_r]$ of degree ≥ 1 in $Y_1, \ldots, Y_r$, there exist infinitely many $b \in \mathbb{Q}^s$ such that $f(b_1, \ldots, b_s, Y_1, \ldots, Y_r) \in \mathbb{Q}[Y_1, \ldots, Y_r]$ is irreducible.*

Proof. There are several proofs for this theorem. The original proof in german can be found at [1]. An explanation in english of this proof can be found at [13].

□

We now demonstrate that a finite group G that is realizable over $\mathbb{Q}(X_1, \ldots, X_n)$, the field of rational functions with n variables over $\mathbb{Q}$, is also realizable over $\mathbb{Q}$. The ideas of the proofs follow the ideas presented in chapter 1 of [27].

We start by defining the specialization of a polynomial. Let K be an infinite field. Suppose that $f \in K(\underline{X})[Y]$, with $\underline{X}$ representing a finite set of variables, $|\underline{X}| = n$ and Y just a single variable. We can write $f = g/h$, where $g \in K[\underline{X}][Y]$ and $h \in K[\underline{X}]\backslash\{0\}$, the least common denominator of the coefficients of f.

Definition 3.1.3 (Specialized polynomial)**.** For every $b \in K^n$ such that $h(b) \neq 0$, we can define $f_b(Y) := f(b, Y) = g(b, Y)/h(b)$, called the *specialized polynomial* in b.

On the next lemma, we see that there are infinitely many ways of specializing a polynomial such that it maintains certain of its original properties.

Lemma 3.1.4. *Consider a finite collection of polynomials $w_0, \ldots, w_r \in \mathbb{Q}(\underline{X})[Y]$. Suppose that w_0 is irreducible and separable, then there are infinitely many points $b \in \mathbb{Q}^n$ such that all $w_i(b, Y)$ are defined, and $w_0(b, Y)$ is irreducible, separable and of the same degree as $w_0(\underline{X}, Y)$ in Y.*

Proof. We first prove it by induction on $|\underline{X}|$. For the case $|\underline{X}| = 1$, we write $w_i(X, Y) = g_i(X, Y)/h_i(X)$ and for each i, the set of points $b \in \mathbb{Q}$ such that $w_i(b, Y)$ is not defined is equal to $Z(h_i)$, the set of zeros of h_i, which is a finite set, since h_i is a one single variable polynomial.

If we call by $c(X)$ the leading coefficient of $w_0(X, Y)$, we have that the set of points $b \in \mathbb{Q}$ such that $w_0(X, Y)$ and $w_0(b, Y)$ do not have the same degree is equal to $Z(c)$, also a finite set.

Since $w_0(X, Y)$ is separable, its discriminant, $\text{Disc}_{w_0}(X)$, is not equal to zero, and the set of points for which $w_0(b, Y)$ is not separable is $Z(\text{Disc}_{w_0})$, a finite set.

By Hilbert's Irreducibility Theorem, the set

$$A = \{b \in \mathbb{Q} | w_0(b, Y) \text{ is irreducible.}\}$$

is infinite. Therefore, the set $A \backslash \big(\cup_{i=0}^{r} Z(h_i) \cup Z(c) \cup Z(\text{Disc}) \big)$ is infinite and all its points satisfy all desired properties.

Suppose the lemma is true for the case $|\underline{X}| = n - 1$. To prove it for the case $|\underline{X}| = n$, we just have to find a $b \in \mathbb{Q}$ such that all $w_i(b, X_2, \ldots, X_n, Y)$ are defined, and $w_0(b, X_2, \ldots, X_n, Y)$ is irreducible, separable and of the same degree as $w_0(\underline{X}, Y)$ in Y. Again by Hilbert's Irreducibility Theorem, the set

$$B = \{b \in \mathbb{Q} | w_0(b, X_2, \ldots, X_n, Y) \text{ is irreducible.}\}$$

is infinite, and if $c(\underline{X})$ or some of $h_i(\underline{X})$ is not a single variable polynomial in X_1, all points of B satisfy all properties. If c or some of h_i is a single variable polynomial in X_1, there are points of B for which at least one of conditions is not satisfied, however, these points constitute a finite set of B, by the same arguments of the first case. Therefore, the lemma is true for the case $|\underline{X}| = n$.

□

Before the next lemma, let us introduce some notation:

Given an irreducible polynomial $f \in K[Y]$, we denote by $K_f := \dfrac{K[Y]}{(f)}$. Note that $K_f \simeq K[a_f]$, for any a_f that is a root of f.

Lemma 3.1.5 (Preservation of the Galois group under specialization)**.** *Let f be an irreducible polynomial over $\mathbb{Q}(\underline{X})[Y]$, such that $\mathbb{Q}(\underline{X})_f/\mathbb{Q}(\underline{X})$ is a Galois extension. Then then are infinitely many points b in $\mathbb{Q}^n$ such that f_b is defined, is irreducible, separable and has the same degree of f and the extension $\mathbb{Q}_{f_b}/\mathbb{Q}$ is also Galois and its Galois group is isomorphic to* $\mathrm{Gal}(\mathbb{Q}(\underline{X})_f/\mathbb{Q}(\underline{X}))$*.*

Proof. Given a root a_f of f, we have that $\mathbb{Q}(\underline{X})_f \simeq \mathbb{Q}(\underline{X})[a_f]$. Since $\mathbb{Q}(\underline{X})_f/\mathbb{Q}(\underline{X})$ is a Galois extension, f splits over $\mathbb{Q}(\underline{X})[a_f]$, and it has r different roots, where $r = \deg f$ in Y. Therefore we can write

$$f(\underline{X}, Y) = C(\underline{X}) \prod_{i=1}^{r} (Y - w_i(\underline{X}, a_f)),$$

where $C(\underline{X}) \in \mathbb{Q}(\underline{X})\backslash\{0\}$ and $w_i(\underline{X}, Z)$ are pairwise different polynomials in $\mathbb{Q}(\underline{X})[Z]$.

For b such that f_b is defined and irreducible, we can define the field $\mathbb{Q}_{f_b}$. Given a root a_{f_b} of f_b, we show that if $w_i(b, Y)$ is defined, $w_i(b, a_{f_b})$ is also a root of f_b.

For any arbitrary i, we denote by $F(\underline{X}, Y) = f(\underline{X}, w_i(\underline{X}, Y))$. Since $F(\underline{X}, a_f) = f(\underline{X}, w_i(\underline{X}, a_f)) = 0$ and $f = Min(\mathbb{Q}(\underline{X}), a_f)$, we have that $f|F$. Thus, there is a $g \in \mathbb{Q}(\underline{X})[Y]$ such that $F = gf$. Since $w_i(b, Y)$ and $f(b, Y)$ are defined, so is $g(b, Y)$, and then

$$F_b = f_b g_b \Rightarrow f_b(Y)|f(b, w_i(b, Y)) \Rightarrow f(b, w_i(b, a_{f_b})) = 0$$

By Lemma 3.1.4, there are infinitely many $b \in \mathbb{Q}^n$ such that all $w_i(b, Y)$ are defined and f_b is defined, irreducible, separable, of the same degree as f. From now on, we consider these b, and for them, we can write

$$f_b(Y) = C \prod_{i=1}^{r} (Y - w_i(b, a_{f_b})),$$

where $C \in \mathbb{Q}\backslash\{0\}$.

This allow us to conclude that f_b splits over $\mathbb{Q}_{f_b}$, and since f_b is separable, $\mathbb{Q}_{f_b}/\mathbb{Q}$ is Galois.

We denote by $G_f = \mathrm{Gal}(\mathbb{Q}(\underline{X})_f/\mathbb{Q}(\underline{X}))$ and $G_{f_b} = \mathrm{Gal}(\mathbb{Q}_{f_b}/\mathbb{Q})$. These two Galois groups are isomorphic.

Indeed, since $\mathbb{Q}(\underline{X})_f/\mathbb{Q}(\underline{X})$ is a simple extension, by Proposition 1.4.4, $|G_f| = r$ and an element $g_i \in G_f$ can be uniquely determined if we define $g_i(a_f) = w_i(\underline{X}, a_f)$. Thus, we have

$$G_f = \{g_i | g_i \text{ is a } \mathbb{Q}(\underline{X})\text{-automorphism and } g_i(a_f) = w_i(\underline{X}, a_f), 1 \leq i \leq r\}.$$

In an analogous manner,

$$G_{f_b} = \{\tilde{g}_i | \tilde{g}_i \text{ is a } \mathbb{Q}\text{-automorphism and } \tilde{g}_i(a_{f_b}) = w_i(b, a_{f_b}), 1 \leq i \leq r\}.$$

Hence, we can define the function

$$\begin{aligned} \sigma \colon G_f &\to G_{fb} \\ g_i &\mapsto \tilde{g}_i, \end{aligned}$$

which is clearly an isomorphism. □

This lemma allow us to prove the following result:

Theorem 3.1.6. *Every finite group G that can be realized as a Galois group over $\mathbb{Q}(X_1, \ldots, X_n)$ can be realized as a Galois group over $\mathbb{Q}$.*

Proof. Suppose that G is the Galois group of an extension $k/\mathbb{Q}(X_1, \ldots, X_n)$. Since $char(\mathbb{Q}(X_1, \ldots, X_n)) = 0$, the extension $k/\mathbb{Q}(X_1, \ldots, X_n)$ is a finite and separable and we can apply the Primitive Element Theorem to obtain that $k = \mathbb{Q}(X_1, \ldots, X_n)[\alpha]$.

Consider $f(X_1, \ldots, X_n, Y) = Min(\mathbb{Q}(X_1, \ldots, X_n), \alpha)$, then:

$$\mathbb{Q}(X_1, \ldots, X_n)_f \simeq k.$$

Then, by Lemma 3.1.5, there are infinitely many b such that extension $\mathbb{Q}_{f_b}/\mathbb{Q}$ is defined and is Galois with Galois group equal to G. Therefore, G is realizable over $\mathbb{Q}$.

□

From Theorem 3.1.6 and Proposition 3.1.1, we obtain the following corollary:

Corollary 3.1.7. Every symmetric group S_n can be realized as a Galois group over $\mathbb{Q}$.

A very well-known result in Group Theory, Cayley's theorem, states that every finite group is isomorphic to a subgroup of some S_n (for a proof of this result, see Theorem 2.9.1 in [10]). Then, what prevent us for generalizing this idea for an arbitrary finite group? In fact, if we could show that every finite group G is realizable over $\mathbb{Q}(X_1, \ldots, X_n)$, by Theorem 3.1.6 we would have that every finite group G is realizable over $\mathbb{Q}$.

In 1917, Emmy Noether tried to adapt the proof of Proposition 3.1.1 for any finite group G. For this, she considered S_n acting on $\mathbb{Q}(X_1, \ldots, X_n)$ permuting the set $\{X_1, \ldots, X_n\}$ and fixing $\mathbb{Q}$, and G acting on $\mathbb{Q}(X_1, \ldots, X_n)$ as a subgroup of S_n. As a consequence of Propositions 1.3.4 and 1.3.5, we have that the extension $\mathbb{Q}(X_1, \ldots, X_n)/\mathbb{Q}(X_1, \ldots, X_n)^G$ is Galois with Galois group G. However, in the general case, we do not know whether $\mathbb{Q}(X_1, \ldots, X_n)^G$ is a purely transcendental extension of $\mathbb{Q}$ with transcendence degree n. Emmy Noether raised that problem, and so it became known as Noether's problem.

Nonetheless, a counterexample was found by Swan in 1969. He proved that $\mathbb{Q}(X_1, \ldots, X_n)^G$ is not rational, i.e. purely transcendental, over $\mathbb{Q}$ when G is a cyclic group of order 47 (this result can be seen in [11]).

This problem can be rewritten in geometric terms, looking to the varieties associated to the above function fields. In that way, $\mathbb{Q}(X_1, \ldots, X_n)^G$ not being rational can be translated into the variety $\mathbb{A}^n/G$ not being $\mathbb{Q}$-rational. We also know that in the cases that the variety $\mathbb{A}^n/G$ is $\mathbb{Q}$-rational, G can be realized over $\mathbb{Q}$. However, can we find a less restrictive condition for $\mathbb{A}^n/G$ to hold that also guarantees that G is realizable over $\mathbb{Q}$?

Answering this question, as an attempt to reformulate Noether's strategy, Colliot-Thélène and Sansuc introduced the Hilbert Property in 1987. They also conjectured that every unirational variety satisfy this property and have shown that if this conjecture is correct, then the Inverse Galois Problem is also true. We will see the details of this proof in section 3.3.

To conclude this section, we give the definition of the Hilbert Property for a field in terms of polynomials. We also give some examples and counterexamples of fields satisfying this property.

Definition 3.1.8 (Hilbert Property for a Field)**.** We say that a field K *has the Hilbert property*, or equivalently, that K is *hilbertian*, if for any irreducible polynomial $f(\underline{X}, Y) \in K(\underline{X})[Y]$, there are infinitely many $b \in K^n$ such that $f(b, Y)$ is irreducible.

Remark 3.1.9. In other words, a field K is hilbertian if we can replace $\mathbb{Q}$ by K in the statement of Hilbert's Irreducibility Theorem. Therefore, Lemma 3.1.4 is still true if we substitute a hilbertian field K for $\mathbb{Q}$. As a consequence, Lemma 3.1.5 and Theorem 3.1.6 are also true if we replace $\mathbb{Q}$ by any hilbertian field.

Example 3.1.10. Finite fields are immediate non-examples of hilbertian fields. Algebraically closed fields are also easy non-examples. In fact, for any algebraically closed field K, the polynomial $Y^2 + Y + X \in K(X)[Y]$ is irreducible, however, $Y^2 + Y + b$ is reducible for any $b \in K$.

In order to construct more examples, we prove that every finite extension of an hilbertian field is also hilbertian.

In what follows, we denote by $\mathrm{Gal}(K) := \mathrm{Gal}(\bar{K}/K)$ and by $\mathrm{Gal}(L) := \mathrm{Gal}(\bar{K}/L)$, where $\bar{K}$ is the algebraic closure of K. The action of $\mathrm{Gal}(K)$ on $\bar{K}$ induces a unique action on $\bar{K}(X)[Y]$ fixing X and Y. We denote the action of an element g of $\mathrm{Gal}(K)$ on a polynomial $f \in M(X)[Y]$ by f^g.

The next lemma and theorem are slightly addapted versions of Lemma 12.2.1 and Lemma 12.2.2 presented in [12].

Lemma 3.1.11. *Suppose that L is a separable extension of degree d of an infinite field K and $\sigma_0, \ldots, \sigma_{d-1}$ are distinct representatives of the cosets of* $\mathrm{Gal}(L)$ *in* $\mathrm{Gal}(K)$. *Consider $f \in L[Y]$ a non-constant polynomial. Then, there is an element $c \in L$, such that the $f(Y+c)^{\sigma_i}$, $0 \leq i \leq d-1$ are pairwise relatively prime in $\bar{K}[Y]$.*

Proof. Let α be the primitive element of the extension L/K. Consider t_i, $0 \leq i \leq d-1$, algebraically independent elements. For every i, we define

$$u_i(\mathbf{t}) = u_i(t_0, \ldots, t_{d-1}) = \sum_{j=0}^{d-1} (\alpha^{\sigma_i})^j t_j.$$

The determinant of this linear transformation is given by $\prod_{i<j}(\alpha^{\sigma_j} - \alpha^{\sigma_i})$, which is different from zero because σ_i and σ_j are different representatives of the cosets of $\mathrm{Gal}(L)$ in $\mathrm{Gal}(K)$. Therefore, this transformation is invertible and we can write t_i as linear combinations of u_i with coefficients in $\bar{K}$, which implies that the u_i are algebraically independent over $\bar{K}$.

We write $f = f_1 \ldots f_m$, a product of irreducible factors in $\bar{K}$. We have that $f_\phi^{\sigma_i}(u_i) - f_\nu^{\sigma_j}(u_j) \neq 0$, for $i \neq j$ and for each ϕ and ν, $1 \leq \phi, \nu \leq m$, since the u_i are algebraically independent and f is non-constant. Then, we define the polynomial function

$$h(\mathbf{t}) = \prod_{i<j} \prod_{\phi,\nu} f_\phi^{\sigma_i}(u_i(\mathbf{t})) - f_\nu^{\sigma_j}(u_j(\mathbf{t})) \neq 0.$$

If we fix $a_0, \ldots, a_{d-2} \in K$, we can find $a_{d-1} \in K$, such that $h(a_0, \ldots, a_{d-1}) \neq 0$, since the set of a_{d-1} such that $h(a_0, \ldots, a_{d-1}) = 0$ is finite and K is an infinite field. Consider

$$c = \sum_{j=0}^{d-1} a_j \alpha^j.$$

Notice that $u_i(a_0, \ldots, a_{d-1}) = c^{\sigma_i}$. Thus, $f_\phi(c)^{\sigma_i} \neq f_\nu(c)^{\sigma_j}$ for $i \neq j$. Therefore,

$$f_\phi(Y+c)^{\sigma_i} \neq f_\nu(Y+c)^{\sigma_j},$$

for all i, j, ϕ, ν with $0 \leq i < j \leq d-1$ and $0 \leq \phi, \nu \leq m$.

Since $f_1(Y+c)^{\sigma_i}, \ldots, f_m(Y+c)^{\sigma_i}$ are the irreducible factors of $f(Y+c)^{\sigma_i}$ in $\bar{K}[Y]$, $f(Y+c)^{\sigma_0}, \ldots, f(Y+c)^{\sigma_{d-1}}$ are pairwise relatively prime.

□

Theorem 3.1.12. *If K is hilbertian, any finite separable extension L of K is also hilbertian.*

Proof. Let S be a set of representatives of all left cosets of $\mathrm{Gal}(L)$ in $\mathrm{Gal}(K)$. Given an irreducible polynomial $f \in L(\underline{X})[Y]$, we first consider the case that f^{σ}, with $\sigma \in S$, are pairwise relatively prime in $F[Y]$, where F is the algebraic closure of $K(\underline{X})$.

Consider $p := \prod_{\sigma \in S} f^{\sigma}$. The idea is to show that $p \in K(\underline{X})[Y]$ and is irreducible, and that for every $b \in K^n$ such that p_b is irreducible, f_b is also irreducible. If K is hilbertian, there are infinitely many b such that p_b is irreducible, and since f is an arbitrary irreducible polynomial in $L(\underline{X})[Y]$, this implies that L is also hilbertian.

We start by showing that $p \in K(\underline{X})[Y]$. Given $g \in \mathrm{Gal}(K)$, we calculate $p^g = \prod_{\sigma \in S} f^{\sigma g}$. We notice that $\{\sigma g\}_{\sigma \in S}$ is another set of representatives of all left cosets. We also have that given two different representatives r, s of the same left coset, $r = ls$, for some $l \in \mathrm{Gal}(L)$ and so $f^r = f^{ls} = f^s$. Thus, $p^g = p$ for every $g \in \mathrm{Gal}(K)$. Therefore $p \in K(\underline{X})[Y]$.

Consider a factorization of p in irreducible polynomials of $K(\underline{X})[Y]$. Since f divides p, and is irreducible in $L(\underline{X})[Y] \supseteq K(\underline{X})[Y]$, f divides at one irreducible factor q of p in $K(\underline{X})[Y]$. Then, for every $\sigma \in S$, f^{σ} divides $q^{\sigma} = q$, and since the f^{σ} are pairwise relatively prime, p divides q. Hence, p is irreducible in $K(X)[Y]$.

Let b be an element of K^n such that p_b is well-defined and irreducible. If f_b is reducible, we can write $f_b(Y) = h(Y)w(Y)$, and then $p_b(Y) = \prod_{\sigma \in S} h(Y)^{\sigma} \prod_{\sigma \in S} w(Y)^{\sigma}$, which contradicts the irreducibility of p_b. Therefore, f_b is irreducible as we claimed.

In the general case, we apply Lemma 3.1.11 to find $c(Y) \in L(\underline{X})[Y]$ such that $f(\underline{X}, Y + c(Y))^{\sigma}$, with $\sigma \in S$ are pairwise relatively prime in $F[Y]$. Thus, we conclude that $f(\underline{X}, Y + c(Y))$ is irreducible, which implies on the irreducibility of $f(\underline{X}, Y)$. □

Example 3.1.13. The field of real numbers $\mathbb{R}$ is not hilbertian. Since $\mathbb{C}/\mathbb{R}$ is a finite extension, if $\mathbb{R}$ were hilbertian, $\mathbb{C}$ would also be hilbertian, which lead us to an contradiction, since we have already seen that algebraically closed fields cannot be hilbertian.

Example 3.1.14. A Global field is a field that is either a number field, i.e., a field that is finite extensions of $\mathbb{Q}$, or a field that is a finite extension of $\mathbb{F}_p(T)$, the field of the rational functions in one variable over a finite field with p elements. Both cases of global fields are examples of hilbertian fields.

When defining this property for varieties, we are interested in a more geometrical way of formulating it. For this reason, we introduce in the next section the concept of thin sets.

3.2 Thin Sets and the Hilbert Property

In the last section, we have seen that given an irreducible polynomial $f \in \mathbb{Q}(\underline{X})[Y]$ such that the field extension $\mathbb{Q}(\underline{X})_f/\mathbb{Q}(\underline{X})$ is Galois, there are infinitely many $b \in \mathbb{Q}^n$ such that the specialization into a polynomial f_b preserves the property of $\mathbb{Q}_{f_b}/\mathbb{Q}$ being Galois and the Galois group of the extension.

In this section, we study thin sets and we see that the set of points that constitute the exception for the above mentioned property is an example of them. Also, we use the definition of thin sets to extend the Hilbert property definition for varieties.

From now on, we deal with algebraic varieties over non-algebraically closed fields. We start formally defining them as well as defining another important concept of non-algebraically closed algebraic geometry: the rational points. For us, K is a field of characteristic 0 we denote by $\bar{K}$ the algebraic closure of K, which has infinite transcendence degree over K. We denote by simply $\mathbb{A}^n$ and $\mathbb{P}^n$, the affine space $\mathbb{A}^n_{\bar{K}}$, and the projective space $\mathbb{P}^n_{\bar{K}}$, respectively.

Definition 3.2.1 (K-closed set)**.** Given a set of polynomials S in $K[X_1, \ldots, X_n]$, we define the affine closed set

$$Z(S) = \{x \in \mathbb{A}^n | f(x) = 0 \text{ for all } f \in S\}$$

A K-projective closed set can be defined in an analogous manner and we can verify they form a K- Zariski topology. We also can define morphisms, dimension, function fields and all the concepts introduced in chapter 2 for varieties over a non-algebraically closed field, the major difference is that we always consider $K[X_1, \ldots, X_n]$ instead of $\bar{K}[X_1, \ldots, X_n]$ to define them. From the definition, we also notice that a K-closed set can be view as L-closed set, where L is a field extension of K, however not every L-closed set can be viewed as K-closed set.

Another remark is that, despite of K-closed sets being defined by polynomials in $K[X_1, \ldots, X_n]$, not all of its points have coordinates in K. This is our reason to introduce K-rational points.

Definition 3.2.2. We say a point $P = (p_1, \ldots, p_n)$ of a K-variety is a *K-rational point* if its coordinates $p_1, \ldots, p_n$ belong to K. It is equivalent to say that the residue field of P, $\mathcal{O}_{P,V}/m_P$, is equal to K. We denote the set of K-rational points of a variety V by $V(K)$.

We are now finally prepared to define thin sets. In the definitions bellow, V is an irreducible variety over K, where $char(K) = 0$ and K is non-algebraically closed.

Definition 3.2.3 (Type C_1 set)**.** A subset $A \subseteq V(K)$ is of type C_1 if A is not Zariski dense in V.

Definition 3.2.4 (Type C_2 set)**.** A subset $A \subseteq V(K)$ is of type C_2 if there is an irreducible variety V' over K, $\dim V = \dim V'$ and a dominant morphism $\pi\colon V' \to V$ of degree ≥ 2 with $A \subseteq \pi(V'(K))$.

Definition 3.2.5 (Thin Sets)**.** A subset $A \subseteq V(K)$ is called thin if it is contained in a finite union of sets of type C_1 or C_2.

Sets of type C_1 are sets contained in some closed set. Sets of C_2 can be a little less intuitive. We give some examples bellow.

Example 3.2.6. Let $d \geq 2$ be an integer. The subset $K^d = \{x^d, x \in K\} \subset \mathbb{A}^1(K)$ is a set of type C_2. We can take $\mathbb{A}^1$ as V' and consider the morphism $\pi\colon V' \to \mathbb{A}^1$ defined by $\pi(x) = x^d$.

Example 3.2.7. Consider the elliptic curve E defined by the equation $x^2 = t^3+2t+1$ in $\mathbb{A}^2$. We define the morphism

$$\begin{aligned} \pi\colon E &\to \mathbb{A}^1 \\ (x,t) &\mapsto (x). \end{aligned}$$

The set $\pi(E(K))$ is a type C_2 set.

We say that a K-variety V is *absolutely irreducible* if V remains irreducible over every extension of K. In the next proposition, we see that we can consider V' to be absolutely irreducible in the definition of type C_2. However, we give an example and a non-example of absolutely irreducible variety before.

Example 3.2.8. The curve defined by $x^2 + y^2 - 1 = 0$ in $\mathbb{A}^2$ is an absolutely irreducible variety over $\mathbb{Q}$. The polynomial $x^2 + y^2 - 1$ is still an irreducible polynomial over $\mathbb{C}$ the ideal generated by this polynomial is still a prime ideal in $\mathbb{C}[x, y]$.

Example 3.2.9. The curve C defined by $x^2 + y^2 = 0$ in $\mathbb{A}^2$ is an irreducible variety over $\mathbb{Q}$, however it is not absolutely irreducible. Indeed, this polynomial can be factored as $(x - iy)(x + iy)$, hence, C has two irreducible components when looked over $\mathbb{C}$.

Also, since $(x/y)^2 = -1$, we can embed the field $\mathbb{Q}(i)$ into $\mathbb{Q}(C)$ by taking i into x/y.

Proposition 3.2.10. *Consider V' and π as in the definition of type C_2 set. Then, if V' is not absolutely irreducible over K, then $\pi(V'(K))$ is a type C_1 set.*

Proof. If V' is not absolutely irreducible, the ideal $I(V')$ is not prime over $\bar{K}[X_1, \ldots, X_n]$. As a consequence, the function field of V', $K(V')$, contains a field L that is a finite extension of K. L is algebraic over K, therefore L is integral over K, hence is L integral over $\mathcal{O}_{x,V'}$ for every $x \in V'$.

Given a point $x \in V'(K)$, we have that L is not contained $\mathcal{O}_{x,V'}$, since $\mathcal{O}_{x,V'}/m_x = K$, therefore there are points in $K(V')$ that are integral over $\mathcal{O}_{x,V'}$, but are not contained on it, i.e, $\mathcal{O}_{x,V'}$ is not integrally closed for every $x \in V'(K)$.

We use the fact that $\mathcal{O}_{x,V'}$ is integrally closed when x is non-singular to conclude that $V'(K)$ is contained in the set of singular points of V', a closed set (The results about singular points can be found at [5], chapter II, section 2, Theorem 2.11 and Corollary of Theorem 2.9).

Therefore, since π is a finite map, thus a closed map by Theorem 2.4.7, $\pi(V'(K))$ is a type C_1 set. $\square$

We bring the definitions of sets of type C_1 and C_2 to $\mathbb{A}^n(K)$ to gain more intuition about them. This discussion is based on the discussion presented in section 9.1 of [19].

Polynomial Interpretation

If $A \subset \mathbb{A}(K)^n$ is a type C_1 set, it means that there is a non-zero polynomial $G \in K[X_1, \ldots, X_n]$ such that $G(x) = 0$ for every $x \in A$.

In order to understand the general form of type C_2 sets, we first verify that given a polynomial $F \in K(X_1, \ldots, X_n)[Y]$, such that F has degree at least two in Y and F is irreducible in $\bar{K}(X_1, \ldots, X_n)[Y]$, the set

$$\Omega_F = \left\{t \in \mathbb{A}^n(K) |\ t \text{ is not a pole of the coefficients of } F \text{ and } F(t, Y) \text{ has a root in } K\right\}$$

is a thin set of type C_2.

We can write $F = f/h$, where $f \in K[X_1, \ldots, X_n][Y]$ with the gcd of the coefficients of f is 1 and $h \in K[X_1, \ldots, X_n]$. Therefore, by Gauss' lemma, f is irreducible and we can consider the quasi-affine variety $V' = Z(f)\backslash\mathbb{Z}(h)$.

Then, we define the following morphism

$$\begin{aligned} \phi\colon V' \subset \mathbb{A}^{n+1} &\to \mathbb{A}^n \\ (x_1, \ldots, x_n, Y) &\mapsto (x_1, \ldots, x_n) \end{aligned}$$

ϕ is a dominant morphism, and by Proposition 2.5.3, the dimension of $Z(f)$ is equal n, and since V' is an open set of $Z(f)$, $\dim V' = n = \dim \mathbb{A}^n$.

We also have that

$$K(V') = K(Z(f)) = \left\{\frac{l}{g} \mid l, g \in K[X_1, \ldots, X_n, Y], g \notin (f)\right\} \simeq \frac{K(X_1, \ldots, X_n)[Y]}{(f)}.$$

The degree of ϕ is equal to $[K(V') : K(X_1, \ldots, X_n)]$, that is the degree of f in Y(that is equal the degree of F in Y) thus it is greater or equal than two. Therefore, $\Omega_F = \phi(V'(K))$ satisfies all the necessary conditions to be a thin set of type C_2.

We see now that a general type C_2 in $\mathbb{A}^n(K)$ is contained in a finite union of type C_1 sets and sets of the form Ω_F.

Given $A \subset \mathbb{A}(K)^n$, a type C_2 set, from the definition, we can write A as $\pi(V(K))$ where V is an absolutely irreducible variety with $\dim V = n$ and $\pi\colon V \to \mathbb{A}^n$ is a dominant morphism of degree $d \geq 2$.

Thus, $[K(V) : K(X_1, \ldots, X_n)] = d$, and since $K(V)/K(X_1, \ldots, X_n)$ is a finite separable extension, we can apply the Primitive Element Theorem to obtain that $K(V) = K(X_1, \ldots, X_n)[\alpha]$, where $Min(K(X_1, \ldots, X_n), \alpha) = F$, and the degree of F in Y is equal to d. We can consider F to be an irreducible polynomial over $\bar{K}(X_1, \ldots, X)[Y]$, otherwise, by Proposition 3.2.10, $\pi(V(K))$ is contained in a type C_1 set.

We can use this F to define a variety V' as we did above. The following commutative diagram summarize the relations between $K(V)$, $K(V')$ and $K(X_1, \ldots, X_n)$.

$$\begin{tikzcd}
K(V') \arrow[r, shift left, "\psi"] & K(V) \arrow[l, shift left, "\psi^{-1}"] \\
K(X_1, \ldots, X_n) \arrow[u, "\hat{\phi}"] \arrow[ur, "\hat{\pi}"'] &
\end{tikzcd}$$

Where $\hat{\phi}$ and $\hat{\pi}$ are injective, since ϕ and π are dominant morphisms. Also ψ is a ring isomorphism and ψ^{-1} its inverse.

Therefore, V' and V are birational varieties and by Theorem 2.3.7, there are non-empty open sets $U_V \subseteq V$ and $U_V \subseteq V'$ such that U_V and U'_V are isomorphic. Hence, the above diagram induces the following one.

$$\begin{tikzcd}
U_{V'} \arrow[r, shift left, "\alpha^{-1}"] \arrow[d, "\phi"] & U_V \arrow[l, shift left, "\alpha"] \arrow[dl, "\pi"] \\
\mathbb{A}^n &
\end{tikzcd}$$

Where $\hat{\alpha} = \psi$. We have then that

$$\pi(U_V(K)) = \phi(\alpha(U_V))(K)) \subseteq \phi(V'(K)) = \Omega_F.$$

We denote by Z the closed set $V \backslash U_V$ and conclude that if $A = \pi(V(K))$ is a thin set of type C_2 in $\mathbb{A}^n(K)$,

$$A \subseteq \pi(Z) \cup \Omega_F,$$

where $\pi(Z)$ is a closed set, since π is a finite morphism.

The result of the next proposition give us another example of thin set. This proposition is an adapted version of Lemma 1.9, presented at [27].

Proposition 3.2.11. *Let f be an irreducible polynomial in $K(\underline{X})[Y]$. There is a thin set $A \subset \mathbb{A}^n(K)$ such that if $b \notin A$, then f_b is irreducible.*

Proof. The idea of the proof is to show that there exists a finite collection of irreducible polynomials $p_1, \ldots, p_m \in K(\underline{X})[Y]$ and a closed set Z such that if $b \notin Z$, then the following holds

If f_b is reducible, then one of $p_{1,b}, \ldots, p_{m,b}$ has a root in K.

If this is true, we can construct $A = (\cup_{i=1}^{m} \Omega_{p_i}) \cup Z$, where $\Omega_{p_i} = \left\{ t \in \mathbb{A}^n(K) | \ t \text{ is not a pole of the coefficients of } p_i \text{ and } p_i(t, Y) \text{ has a root in } K \right\}$. Thus A is clearly a thin set and for every $b \notin A$, f_b is irreducible.

We prove the above statement. Without loss of generality, we can assume f to be monic. In the splitting field of f, we have

$$f = \prod_{i \in I} (Y - w_i).$$

Since f is irreducible, for each non-empty set $J \subset I$, one of the coefficients of the polynomial

$$F_J = \prod_{i \in J} (Y - w_i)$$

does not lie in $K(\underline{X})$.

If we develop the above product, we realize that the coefficients of F_J are symmetric polynomials $s_J \in K(\underline{X})[\{Z_i\}_{i \in J}]$ evaluated at $\{Z_i \mapsto w_i\}_{i \in J}$.

Let $p_J = Min(K(\underline{X}), s_J(\{w_i\}_{i \in J}))$. We show that the polynomials $\{p_J\}_{\emptyset \neq J \subset I}$ have the desired property.

We only consider the b such that all $p_{J,b}$ and f are defined, f_b is separable and of the same degree as f. We use the same reasoning of the first part of Lemma 3.1.4 to conclude that there is a closed set $Z \subset \mathbb{A}^n(K)$ such that for all $b \notin Z$, the above properties are satisfied.

Since we consider b such that f_b is separable and of the same degree as f, in some extension of K f_b can be factored as

$$f_b = \prod_{i \in I} (Y - v_i).$$

In fact, we can define a K-algebra homomorphism

$$\begin{aligned} \phi \colon K[\underline{X}, w_1, \dots w_r] &\to K[v_1, \dots, v_r] \\ \underline{X} &\mapsto b \\ w_i &\mapsto v_i. \end{aligned}$$

Suppose f_b is reducible over K. Then for some non-empty $J \subset I$, the polynomial $\prod_{i \in J}(Y - w_i)$ lies in $K[Y]$. This means that for some non-empty $J \subset I$, $s_J(\{v_i\}_{i \in J}) \in K$. Since $p_J(s_J(\{w_i\}_{i \in J})) = 0$,

$$p_{J,b}(s_J(\{v_i\}_{i \in J}))) = \phi(p_J(s_J(\{w_i\}_{i \in J}))) = 0,$$

which proves our claim.

□

As a corollary, we can reformulate the result of 3.1.5 in the following way:

Proposition 3.2.12. *Let f be an irreducible polynomial over $K(\underline{X})$, such that $K(\underline{X})_f/K(\underline{X})$ is a Galois extension. Then, there is a thin set $A \subset \mathbb{A}^n(K)$ such that if $b \notin A$, f_b is defined, is irreducible, separable, has the same degree of f and the extension K_{f_b}/K is also Galois with Galois group isomorphic to* $\mathrm{Gal}(K(\underline{X})_f/K(\underline{X}))$.

From Proposition 3.2.11, we conclude that a field K satisfy Hilbert's irreducibility Theorem, i.e. K be hilbertian, is equivalent to $\mathbb{A}^n(K)$ not to be thin for every $n \in \mathbb{N}$. In fact, this is our motivation to define Hilbert Property for a general variety.

Definition 3.2.13 (Hilbert Property)**.** A variety V over K has the Hilbert Property if $V(K)$ is not thin.

Before giving examples and non-examples, we see that the Hilbert Property is a birational invariant.

Proposition 3.2.14. *The Hilbert Property is preserved by birational maps.*

Proof. Given two birationally equivalent varieties X and Y over K , from Theorem 2.3.7, there are non-empty open sets $U_X \subset X$ and $U_Y \subset Y$ such that U_X and U_Y are isomorphic. Suppose X has the Hilbert Property over K, then $U_X(K)$ is not thin, otherwise $X(K)$ would also be, since $X(K) = (X \backslash U_X)(K) \cup U_X(K)$. Hence $Y(K)$ contains a non-thin set, therefore Y has also the Hilbert Property over K. □

Example 3.2.15. As we have seen, for K hilbertian, as in the case of number fields, $\mathbb{A}^n(K)$ has the Hilbert Property for every $n \in \mathbb{N}$. In fact, by the previous proposition, for a hilbertian field K, all K-rational varieties have the Hilbert Property.

However, even for K hilbertian, there are varieties over K that do not have the Hilbert Property. We see this in the next example.

Example 3.2.16. Elliptic curves over a number field K do not have the Hilbert Property. Given an elliptic curve E over K, we can define the following morphism:

$$\begin{aligned} [n]\colon E &\to E \\ P &\mapsto nP \end{aligned}$$

where $nP = P + P + \cdots + P$ (n terms), $+$ represent the group operation on an elliptic curve. (To see more about the group law of an elliptic curve see [15], sections 3.2 and 3.3, chapter III)

$[n]$ is a finite dominant morphism with degree n^2 (See [15], Theorem 3.6, Corollary 5.4 and Theorem 6.2, chapter III).

We also have that, by weak Mordell-Weil Theorem (See [15], Theorem 1.1, Chapter VI), the group $E(K)/nE(K)$ is finite for any $n \in \mathbb{Z}$. Hence, let $g_1, \dots, g_m$ be the representatives of the cosets of $E(K)$, we can define

$$\begin{aligned}\phi_i\colon E(K) &\to E(K)\\ P &\mapsto g_i + [n]P\end{aligned}$$

Therefore,

$$E(K) = \bigcup_{i=1}^{m} \phi_i(E(K))$$

and hence $E(K)$ is thin.

We have already seen that all K-rational varieties over a number field K have the Hilbert Property. However, for curves over K, a stronger statement can be applied: to have the Hilbert Property is equivalent to be a K-rational variety. In other words, every non-rational curve is an example of a curve that does not possess the Hilbert Property. We see this in the next proposition.

Proposition 3.2.17. *Non-rational curves over a number field K do not have the Hilbert Property.*

Proof. For the proof, we use a numerical invariant of a curve called genus, denoted here by g, the number g is a non-negative integer. Since a curve X is rational if and only if $g = 0$, we are interested in showing that when g is positive, $X(K)$ is thin. For $g \geq 2$, we obtain this as a immediate consequence of Falting's Theorem [23]: If X is an algebraic curve over a number field K of genus $g \geq 2$, then the set $X(K)$ of K-rational points is finite. For $g = 1$, if $X(K)$ is non-empty, then X is an elliptic curve, and as we have seen in the example 3.2.16, it does not have the Hilbert Property (an explanation about genus and some of its properties used here can be found at section 8.3 of [7]). □

Example 3.2.18. The Fermat curve is an algebraic curve C defined by $x^n + y^n - z^n = 0$ in $\mathbb{P}^2$, where $n \in \mathbb{N}$. The genus of this curve is given by the following expression

$$g = \frac{(n-1)(n-2)}{2},$$

therefore for $n > 2$, the Fermat curve is not rational. Also, for $n > 2$, Fermat's Last Theorem guarantees that the only rational points in C are the trivial ones, i.e., have $xyz \neq 0$.

Remark 3.2.19. Proposition 3.2.17 cannot be generalized for higher dimensions. In fact, Corvaja and Zannier showed in [21] that the Fermat Surface, a quartic smooth surface defined in $\mathbb{P}^3$ by the equation

$$x^4 + y^4 = z^4 + w^4,$$

has the Hilbert Property. This is the first example of a non-rational surface that has the Hilbert Property, Although we metioned the importance of K-unirational varieties in the study of the Hilbert Property, the referred surface is also non-unirational.

When we first hear about the Hilbert Property, it might sound as an improved version of having a Zariski dense set of K-rational points. This is why we consider the example that ends this section an interesting one: a variety that has a Zariski-dense set of rational points, however it does not have the Hilbert Property. This example was extracted from section 3.2 of [21].

Example 3.2.20. Our example is the Enriques surface S defined in $\mathbb{P}^3$ by the following equation

$$x_0x_2^4 + x_1x_3^4 = x_0^2x_1^3 + x_0^3x_1^2.$$

To prove that $S(\mathbb{Q})$ is a Zariski-dense set, we see that there is a dominant rational map from the Fermat quartic smooth surface F defined in $\mathbb{P}^3$ by $x^4 + y^4 = z^4 + w^4$ to S. We define this dominant rational map in the following way

$$x_0 = x^4, x_1 = y^4, x_2 = xy^2z, x_3 = x^2yw.$$

Since $F(\mathbb{Q})$ is Zariski dense in F, as proved by Swinnerton-Dyer in [24], $S(\mathbb{Q})$ is also Zariski dense in S.

We see now that $S(\mathbb{Q})$ is contained in the union of two sets of type C_2, which permits us to conclude that S does not have the Hilbert Property. We define in $\mathbb{P}^4$ the following projective varieties

$$V^+ = Z(x_0x_2^4 + x_1x_3^4 - x_0^2x_1^3 + x_0^3x_1^2, x_0x_1 - x_4^2)$$
$$V^- = Z(x_0x_2^4 + x_1x_3^4 - x_0^2x_1^3 + x_0^3x_1^2, x_0x_1 + x_4^2).$$

We denote by π the projection $(x_0 \colon x_1 \colon x_2 \colon x_3 \colon x_4) \mapsto (x_0 \colon x_1 \colon x_2 \colon x_3)$. We start by showing that $S(\mathbb{Q}) \subset \pi(V^+)(\mathbb{Q}) \cup \pi(V^-)(\mathbb{Q})$.

Consider $(a_0 \colon a_1 \colon a_2 \colon a_3) \in S(\mathbb{Q})$, we can suppose that a_0, a_1, a_2, a_3 are integers and $\gcd(a_0, a_1, a_2, a_3) = 1$. To prove our assertive is enough to show that either a_0a_1 ou $-a_0a_1$ is a square, where we can assume that $a_0a_1 \neq 0$. Given p a prime number, we denote by e_i the p-adic order of a_i. Suppose by contradiction that $e_0 + e_1$ is odd. This implies that the numbers $e_0 + 4e_2, e_1 + 4e_3, 2e_0 + 3e_1, 3e_0 + 2e_1$ are pairwise distinct because they are congruent modulo 4 to $e_0, e_1, e_1 + 2, e_0 + 2$. But these numbers are the p-adic orders of the terms of the equation defining S, therefore thus lead us to a contradiction. Hence, the p-adic order of every prime dividing a_0a_1 is even, as we claimed.

We only need to verify that $\pi(V^+)(\mathbb{Q})$ is a set of type C_2, the same reasoning can be applied to $\pi(V^-)(\mathbb{Q})$. We first observe that since S is a hypersurface in $\mathbb{P}^3$ and V^+ is the intersection of two hypersurfaces in $\mathbb{P}^4$, both are two-dimensional closed sets.

We denote by S' the set $Z(x_0x_2^4 + x_1x_3^4 - x_0^2x_1^3 + x_0^3x_1^2)$ in $\mathbb{P}^4$. We take the open set $(x_0 \neq 0)$ of S' and denote it by U_0. We have that

$$\mathbb{C}(S') = \mathbb{C}(U_0) = \frac{\mathbb{C}(x_1, x_3)[x_2, x_4]}{(x_2^4 + x_1x_3^4 - x_1^3 + x_1^2)}.$$

Since $V^+ = S' \cap Z(x_4^2 - x_1)$, and $x_4^2 - x_1$ is a irreducible polynomial in $C(S')$, V^+ is an irreducible variety. We can also write

$$\mathbb{C}(V^+) = \frac{\mathbb{C}(S)[x_4]}{(x_1 - x_4^2)}$$

to conclude that the degree of $\pi\colon V^+ \to S$ over $\mathbb{Q}$ is equal or greater than two. Therefore, $\pi(V^+)$ is indeed a type C_2 set.

3.3 Unirational Varieties and the Inverse Galois Problem

In the same year they introduced the definition of the Hilbert Property, Colliot-Thélène and Sansuc conjectured that for a number field K, every unirational variety over K has the Hilbert Property. As we have already mentioned in section 3.1, this conjecture implies that Galois inverse problem is true. In the present section, we show how these two results connect. We start seeing a special example of affine variety.

Let G be a finite subgroup of the group of automorphisms of an affine K-variety W. We can define the action of an element $g \in G$ on an element $f \in \mathcal{O}(W)$ in following way

$$gf(x) = f(g(x)), \text{ for every } x \in W.$$

The algebra $\mathcal{O}(W)^G$ is then a finite algebra with no nilpotent elements (see Proposition A.6 in the appendix of [5]), thus there is an affine variety V such that $\mathcal{O}(V) = \mathcal{O}(W)^G$. V is called *the quotient variety of W by the action of G* and we denote it by W/G.

The name quotient is due to the following fact: the inclusion of $\mathcal{O}(W/G)$ in $\mathcal{O}(W)$ induces a dominant morphism $\pi\colon W \to W/G$ and given two points x_1, x_2 of W, $\pi(x_1) = \pi(x_2)$ if and only if there is a $g \in G$ such that $x_1 = gx_2$ (to see this proof, look at [5] Example 1.21 in chapter one, section 2.3). In other words, V is the quotient of the action of G on W.

We also notice that the morphism π is finite (see Example 1.29 in [5], chapter one, section 5.4) and that $\deg \pi = |G|$, since the field extension $K(W)/K(V)$ is Galois with Galois group equal to G. We see that for certain points of $V(K)$, we can construct a field K_P such that K_P/K is also Galois with the same Galois group G. This is the cue to next definition and the next lemma.

Definition 3.3.1 (Inert point)**.** Given a morphism between K-varieties $\pi\colon X \to Y$, we say that $P \in Y(K)$ is *inert* if $|\pi^{-1}(P)| = \deg \pi$ and $G_K = \mathrm{Gal}(\bar{K}/K)$ acts transitively on $\pi^{-1}(P)$.

Lemma 3.3.2. *Consider W an affine K-irreducible variety, $V = W/G$, where G acts faithfully on W. Let $\pi\colon W \to V$ be the natural projection. If $P \in V(K)$ is Inert, then $K_P = \mathcal{O}(W)/I(\pi^{-1}(P))$ is a field, and K_P/K is a Galois extension with Galois group G.*

Proof. We first show that $I(\pi^{-1}(P))$ is a maximal ideal of $\mathcal{O}(W)$, and thus K_P is a field. Given a point $\mathbf{a} \in \pi^{-1}(P)$, we can write $\mathbf{a} = (a_1, \dots, a_n)$, where each $a_i \in \bar{K}$, since $W \subset \mathbb{A}^n$ for some n. The ideal $I(\mathbf{a}) \subset \mathcal{O}(W)$ is a maximal ideal since

$$\frac{\mathcal{O}(W)}{I(\mathbf{a})} \simeq K(a_1, \dots, a_n).$$

We show that $I(\pi^{-1}(P)) = I(\mathbf{a})$. First, since $\mathbf{a} \in \pi^{-1}(P)$

$$I(\pi^{-1}(P)) \subset I(\mathbf{a}).$$

On the other side, P is inert, thus we can write any element $y \in \pi^{-1}(P)$ as $y = \alpha\mathbf{a}$, for some $\alpha \in G_K$. Hence, for any $\bar{f} \in I(\mathbf{a})$, we can take a representative $f \in K[X_1, \dots, X_n]$

$$0 = \alpha(f(\mathbf{a})) = f(\alpha(\mathbf{a})) = f(y).$$

Thus, $\bar{f}(y) = 0$ for every $y \in \pi^{-1}(P)$, hence $\bar{f} \in I(\pi^{-1}(P))$, and so $I(\pi^{-1}(P)) = I(\mathbf{a})$.
To show the second part, we first see that the action of G on $\mathcal{O}(W)$ induces a well defined action on K_P, thus $G \subset Aut(K_P/K)$.

From the definition of inert point, $P \in V(K)$, thus $\{P\}$ is a closed set and $\pi^{-1}(P)$ is also a closed set. This implies that $Z(I(\pi^{-1}(P))) = \pi^{-1}(P)$, and so we can see K_P as the quotient set of the following equivalence relation

$$K_P = {}^{\mathcal{O}(W)}\!/\!_{\sim}, \text{where } f_1 \sim f_2 \text{ iff } f_1(x) = f_2(x) \text{ for every } x \in \pi^{-1}(P).$$

For every $x \in \pi^{-1}(P)$,

$$gf_1(x) = f_1(g(x)) = f_2(g(x)) = gf_2(x).$$

Hence, if $f_1 \sim f_2$, then $gf_1 \sim gf_2$ and the action of G on K_P is in fact well defined.

We show that $K_P^G = K$. Given $\mathbf{a} = (a_1, \dots, a_n) \in \pi^{-1}(P)$, since $K_P \simeq K(a_1, \dots, a_n)$, $K_P \subset \bar{K}$.

Also for an element $\gamma \in K_P^G$, we can choose a representative $f \in K[X_1, \dots, X_n]$ of γ, $\gamma = f(\mathbf{a})$. Since $P \in V(K)$, for every $\alpha \in G_K$, $\alpha(\mathbf{a}) \in \pi^{-1}(P)$, therefore

$$\alpha(\gamma) = \alpha(f(\mathbf{a})) \Rightarrow \alpha(\gamma) = f(\alpha(\mathbf{a})) = \gamma.$$

Hence, $\gamma \in K$ and thus $K_P^G = K$. We conclude then that K_P/K is a Galois extension with Galois group equal to G. □

The next proposition is crucial in the proof of our final result. It is a more detailed version of Propositiom 3.3.1 presented at [17].

Proposition 3.3.3. *Consider W an affine K-irreducible variety, $V = W/G$, where G acts faithfully on W. Let $\pi \colon W \to V$ be the natural projection. If V has Hilbert property, then there is a Galois extension of K with Galois group G.*

Proof. From Lemma 3.3.2, it is enough to show that there is a thin set $A \subset V(K)$, such that if $P \notin A$, P is inert. We consider just the points outside of the ramification locus of π because G acts freely on these points. By Theorem 2.6.11, since $K(W)/K(V)$ is a separable extension, the ramification locus is just a closed set of V. We denote by Σ the set of proper groups H of G. We consider W/H, the quotient of W by H, and π_H the natural projection of W/H onto V. Then, we define A

$$A = \bigcup_{H \in \Sigma} \pi_H(W/H)(K).$$

We verify that A is thin set. First, as we have seen in the beginning of this section the projection of W onto a quotient by a finite group is finite morphism, therefore

$$\dim V = \dim W = \dim W/H.$$

Also,

$$\deg \pi_H = \frac{[K(W) : K(V)]}{[K(W) : K(W/H)]} = \frac{|G|}{|H|} > 1.$$

Since $\mathrm{Gal}(K(W)/K(V)) = G$ and $\mathrm{Gal}(K(W)/K(W/H)) = H$. Thus, A is a finite union of type C_2 sets, a thin set.

To conclude we only have to verify that if $P \notin A$, G_K acts transitively on $\pi^{-1}(P)$. We can lift P to a point $\bar{P} \in W(\bar{K})$. Consider the following subgroup

$$H = \{g \in G | g\bar{P} = \alpha\bar{P}, \text{ for some } \alpha \in G_K\}.$$

Since $P \notin A$, $H = G$. In fact, if H were a proper group of G, the image of $\bar{P}$ in W/H would be rational, since given a point in the same orbit of $\bar{P}$, $\alpha\bar{P}$, for every $\gamma \in G_K$, the point $\gamma\alpha\bar{P}$ would still be on the orbit of $\bar{P}$. Therefore P would be in A. □

Remark 3.3.4. Notice that since $K(W)/\hat{\pi}(K(V))$ is a finite separable extension, we can write $K(W) \simeq \hat{\pi}(K(V))[X]/(\hat{\pi}(F))$, where F is an irreducible polynomial in $K(V)[X]$, G acts transitively on the roots of F. As a matter of fact, Lemma 3.3.2 is a more general version of Lemma 3.1.5, where we are looking for the points P such that the specialization of F in $\pi(P)$ satisfies the statement of Lemma 3.1.5.

Finally, we connect the conjecture of Colliot-Thélène and Sansuc with the Galois inverse problem.

Theorem 3.3.5. *If every K-unirational variety has the Hilbert property, given a finite group G, there is a Galois extension of K is with Galois group G.*

Proof. Given a finite group G, consider n such that G is isomorphic to a subgroup of S_n. We consider G acting on $K[X_1, \dots, X_n]$ permuting the set $\{X_1, \dots, X_n\}$ as a subgroup of S_n and fixing K. Hence, the quotient variety of $\mathbb{A}^n$ by the action of G, $\mathbb{A}^n/G$, is a unirational variety, since $K(\mathbb{A}^n/G) = K(X_1, \dots, X_n)^G \subset K(X_1, \dots, X_n)$. We can apply Proposition 3.3.3 to obtain the desired result. □

3.4 The Hilbert Property and Algebraic Topology

We have seen the importance of unirational varieties in the study of the Hilbert Property, that if all unirational varieties hold this property, a positive answer for Inverse Galois Problem is obtained. However, in section 3.2, we mentioned an example of a non-unirational variety that bears the Hilbert Property. One might ask what it means for a non-unirational variety to have the Hilbert Property, what kind of information it may express in this case and what are the common characteristics between non-unirational and rational varieties that bear the Hilbert Property.

This question is answered in the Corvaja and Zannier's article, published in 2016, "On the Hilbert Property and the Fundamental Group of Algebraic Varieties"([21]). On this article, they expose some topological properties of varieties that possess the Hilbert Property, considering the complex analytical topology.

The study of relations between Algebraic Geometry and Complex Analytic Topology is not so recent though. In 1956, Serre published his celebrated paper "Géométrie algébrique et géométrie analytique", commonly referred as GAGA. This article contains a series of results that relate algebraic geometry over the complex numbers to complex analytic geometry. For example, Chow's theorem, that states that every closed analytic subspace of a projective algebraic variety is a complex algebraic variety, is implied by the GAGA principle (See Chapter 6 of [17]).

In this section, we expose some results that can be found at [21], in sections 1.2 and 1.4. We start with the definition of algebraically simply connected variety. Also, in this section, we will often refer to finite dominant morphisms between algebraic varieties by covers.

Definition 3.4.1 (Algebraically simply connected variety)**.** Given a number field K, we say an algebraic variety X over K is *algebraically simply connected* if considering X^ν, the normalization of X, any cover $\phi\colon Y \to X^\nu$ defined over some extension of K and of degree greater than 1 is ramified.

Given a number field K and a variety X over K, we can take $X(\mathbb{C})$. This set carries the complex analytic topology and we can calculate its fundamental group that we denote here by $\pi_1(X)$.

The next proposition give us a (complex analytical) topological criterion to determine if a normal variety is algebraically simply connected or not.

Proposition 3.4.2. *A normal variety X is algebraically simply connected if and only if $\pi_1(X)$ has no subgroup of finite index greater than 1.*

Remark 3.4.3. An immediate observation is that if X is a normal variety such that $X(\mathbb{C})$ is simply connected, then X is algebraically simply connected.

We give some of the main ideas of this proof. However, before doing so, we give an example that illustrates that the normal condition cannot be omitted.

Example 3.4.4. As we have seen in example 2.6.8, the nodal curve in $\mathbb{P}^2$

$$X = Z(zy^2 - x^3 - zx^2)$$

is a non-normal variety and its normalization is equal to $\mathbb{P}^1$. The projective line is normal and $\mathbb{P}^1(\mathbb{C})$ is the Riemann sphere, which is simply connected, therefore $\mathbb{P}^1$ and X are algebraically simply connected. However, $\pi_1(X) = \mathbb{Z}$.

We recall that in algebraic topology, for a "sufficient good space" X, there is a bijection between each subgroup H of $\pi_1(X)$ to a connected covering space of X of degree $[\pi_1(X) : H]$. The degree of a covering $p\colon Y \to X$ is the cardinality of $p^{-1}(x)$ for every $x \in X$ (These results can be founded with more details at section 1.3 of Hatcher [20]).

We also introduce the concept of topologically unibranch at a point that will help us in the proof of the above proposition.

Definition 3.4.5 (Topologically Unibranch)**.** A complex variety X is called *topologically unibranch at x* if for all algebraic subsets $Y \subset X$, there is a fundamental systems of neighbourhoods of x in classical topology $\{U_n\}$, such that $U_n \backslash Y \cap U_n$ is connected in classical topology.

Idea of the proof of the Proposition 3.4.2 $\Rightarrow$ We assume that X is normal and algebraically simply connected. Suppose there is a subgroup H of index $d > 1$. We can find a connected covering space Y of $X(\mathbb{C})$ such that $p\colon Y \to X(\mathbb{C})$ is of degree d. We can endow Y with a unique algebraic structure, and p is a finite morphism (in the algebraic sense) considering this structure (See chapter 6 of [17]).

Since $K(Y)/p^*(K(X))$ is a separable extension, by Theorem 2.6.11, the set of unramified points is a non-empty open set of X. Then if Y is irreducible, since $p^{-1}(x) = d$ for every $x \in X$, p is unramified at every point $x \in X$, hence X is not algebraically simply connected, which leads us to a contradiction.

Notice that we have not used yet the fact that X is a normal variety. We use it now to show that Y is irreducible. Since X is normal, every point of X is topologically unibranch (See Theorem 3.24 in [18]). Since p is a finite morphism, from Theorem 2.4.7, p is a closed map with respect to Zariski topology. Therefore, by Chow's Theorem, p is a homeomorphism considering classical topology, and Y is also topologically unibranch at every point. Then, we can suppose by contradiction that Y is reducible and we have that either Y is disconnected regarding complex analytic topology or that removing the points that are in the intersection of two irreducible components, a neighbourhood of any of these points will be disconnected. Both cases contradict Y being topologically unibranch at every point, therefore if X is a normal and algebraically simply connected variety, $\pi_1(X)$ has no subgroup of finite index greater than 1.

$\Leftarrow$ If X is normal and not algebraically simply connected, there is a finite algebraic cover with no ramification and degree greater than 1. This corresponds to a topological cover, and thus to a subgroup of $\pi_1(X)$ of finite index greater than 1. □

We see that every variety with the Hilbert Property is algebraically simply connected, which show us that the Hilbert Property reveal not only arithmetically information about a variety, but also topological information. In our proof, we need a modified version of the Chevalley-Weil Theorem. We state bellow both the original and the modified version of the Chevalley-Weil Theorem.

Theorem 3.4.6 (Chevalley-Weil Theorem)**.** *Consider $\pi\colon Y \to X$ an unramified finite morphism of projective varieties over the number field K. Then, there is a finite extension K'/K such that $X(K) \subset \pi(Y(K'))$.*

Proof. See section 4.2 of [19]. □

Theorem 3.4.7 (Modified Chevalley-Weil Theorem)**.** *Consider $\pi\colon Y \to X$ an unramified finite morphism of projective varieties over the number field K with degree > 1. Then, there are finitely many finite morphisms $\pi_i\colon Y_i \to X$ of degree > 1, such that $X(K) \subset \cup_i \pi_i(Y_i(K))$.*

The proof of this alternative version of the Chevalley-Weil Theorem comes as a corollary of the original Chevalley-Weil Theorem and of the following proposition.

Proposition 3.4.8. *Consider $\pi\colon Y \to X$ be a finite morphism of degree > 1 defined over K. Let K'/K be a finite extension and let $T \subset Y(K')$ be a set of points such that $\pi(T) \subset X(K)$. Then there exist finitely many covers $\pi_i\colon Y_i \to X$, each of degree > 1, defined and irreducible over k, such that $\pi(T) \subset \cup_i \pi_i(Y_i(K))$.*

For the proof of this proposition, we use the Weil Restriction Functor. This is a covariant functor and given a finite extension K'/K, it takes a variety X over K' into a variety $F(X)$ over K such that the K'- rational points of X are the K-rational points of $F(X)$. Also, if $[K' : K] = d$, we have that $F(X)$ is a variety with dimension equal to $d \cdot \dim X$ and is isomorphic over K' to X^d. To see a precise definition of this functor and some of its properties, you can see section 4.6 of [22].

Proof. We can look to the varieties X, Y and to the morphism $\pi\colon Y \to X$ given at the statement of the proposition as varieties and morphism defined over K' and therefore apply the Weil restriction functor to them. Thus, we can embed X into $F(X)$ using the diagonal morphism, $\Delta\colon X \to X^d$. In the same way, we can embed the K-rational points of X into the K-rational points of $F(X)$. We denote by $\tilde{\pi}\colon F(Y) \to F(X)$ the resultant morphism by the application of the Weil functor to π. Since $T \subset Y(K') \simeq F(Y)(K)$, we can lift the points of $\pi(T)$ to $F(Y)(K)$. All this information is summmarized in the following diagram.

$$\begin{tikzcd}
X(K) \arrow[r, phantom, "\simeq"] & \Delta X(K) \arrow[r, phantom, "\subset"] & F(X)(K) \\
T \arrow[u, "\pi"] \arrow[r, phantom, "\subset"] & Y(K') \arrow[r, phantom, "\simeq"] & F(Y)(K) \arrow[u, "\tilde{\pi}"]
\end{tikzcd}$$

Let Y_i be the irreducible components of $\tilde{\pi}^{-1}(\Delta(X))$. Then, the maps π_i given by the restriction $\tilde{\pi}|_{Y_i}$ give the covers from the statement.

Indeed, they cannot have degree 1, for if they had then ΔX would be birational to Y_i. This means that there is a map $\sigma\colon U \to Y_i$, where U is an open dense subset of ΔX, such that $\sigma \circ \pi_i = Id_U$. Since X is isomorphic to ΔX, this induces a map σ' such that $\sigma' \circ \pi = Id'_U$. This is organized bellow.

$$\begin{tikzcd}
X \supset U' \arrow[d, shift left, "\sigma'"] \arrow[r, phantom, "\simeq"] & \Delta X \supset U \arrow[d, shift left, "\sigma"] \arrow[r, phantom, "\subset"] & F(X) \\
Y \arrow[u, shift left, "\pi"] \arrow[r, phantom, "\simeq"] & \Delta Y \arrow[u, shift left, "\tilde{\pi}"] \arrow[r, phantom, "\subset"] & F(Y)
\end{tikzcd}$$

We conclude then that Y is birational to X, contradicting the fact that $\deg \pi > 1$. □

The modified Chevalley-Weil Theorem implies X over K does not have the Hilbert property if there is an unramified finite morphism $\pi\colon X \to Y$ over K with degree > 1. We use the following proposition to rewrite this result using the concept of being algebraically simply connected.

Proposition 3.4.9. *If $A \subset V(K')$ is thin with respect to K', then $V(K)$ is thin with respect to K.*

Proof. See Proposition 3.2.1 of [17]. □

Theorem 3.4.10. *Consider a projective variety X over K with the Hilbert Property. Then, X is algebraically simply connected.*

Proof. We have seen in the Example 3.2.15, that the Hilbert Property is invariant by birational maps. Hence, we can take X as a normal projective variety in our proof without loss of generality. We show that if X is not algebraically simply connected, the Hilbert Property fails for X. If X is not algebraically simply connected, there is a unramified cover of X, $\pi\colon Y \to X$ with degree > 1, this cover may be defined over a finite extension of K, K'. Thus, we use the modified version of Chevalley-Weil Theorem to show that $V(K')$ is thin. By Proposition 3.4.9, we conclude that $V(K)$ is also thin, in other words, that V does not have the Hilbert Property over K. □

This last theorem gave us a necessary condition that a variety must satisfy in order to have the Hilbert Property, and therefore it permit us to construct some non-examples.

Example 3.4.11. We have seen in the Example 3.2.16 that elliptic curves do not have the Hilbert Property. An elliptic curve is a smooth variety, in particular a normal variety, therefore we can apply Theorem 3.4.2 in order to prove that they are not algebraically simply connected. Given an elliptic curve E over K, $\pi_1(E(\mathbb{C})) = \mathbb{Z} \times \mathbb{Z}$, since elliptic curves over $\mathbb{C}$ are isomorphic to the 1-dimensional (as a complex manifold) complex torus, and so they are not algebraically simply connected, which confirms they do not have the Hilbert Property

In fact, this same reasoning can be applied to any abelian variety over a number field K. Since any abelian variety is smooth and since a n-dimensional abelian variety A is isomorphic to a n-dimensional (as a complex manifold) complex torus that is also an algebraic variety, $\pi_1(A) = \mathbb{Z}^{2n}$ and we conclude that abelian varieties do not have the Hilbert Property.

3.5 Conclusion: New Directions

After seeing the historical motivation for the Hilbert Property, some examples and non-examples, its relation with Inverse Galois Problem and Algebraic Topology, we finally end this study looking for the future: we present a reformulation of this property together with some open problems and its implications. The discussion presented here is based on chapter 2 of Corvaja and Zannier's article [21].

We have seen in Theorem 3.4.10 that a non-algebraically simply connected projective variety does not have the Hilbert Property. This allows one to reformulate the definition of Hilbert Property for normal varieties, disregarding the cases when the variety X has an unramified cover. This is the motivation for the definition of Weak Hilbert Property introduce in [21].

Definition 3.5.1 (Weak Hilbert Property)**.** We say that a normal variety X/K *has the Weak Hilbert Property* if, given finitely many covers $\pi_i : Y_i \to X$ $i = 1, ..., m$, each ramified above a non-empty divisor, $X(k) \setminus \cup_i \pi_i(Y_i(K))$ is Zariski-dense in X.

First, we can verify that this new property is equivalent to the Hilbert Property for algebraically simply connected as we intended.

To understand the difference between these two properties, we may want to see examples of varieties that satisfy this modified version of the Hilbert Property, although they did not satisfy the original one. We have seen in Example 3.2.20 that there are varieties with Zariski-dense set of rational points that do not have the Hilbert Property. Therefore, one might ask the following question

Question 1. Does every variety with Zariski-dense set of rational points has the Weak Hilbert Property?

This question is still unanswered, however, there are a few partial results. For example, for the case of curves, the answer is positive. In fact, by Falting's Theorem [23], we are just interested in the cases where the genus g of the curve is less than two. For $g = 0$, we have the rational curves and since they have the Hilbert Property, they also have the Weak Hilbert Property. However, the case $g = 1$ presents a difference. While we have seen the elliptic curves do not have the Hilbert Property in Example 3.2.16, they do have the Weak Hilbert Property because ramified covers of a curve of genus 1 have genus greater than 1, hence we can apply again Falting's Theorem to obtain the desired result.

Also motivated by Theorem 3.4.10, we can if its converse is also true, this is if any algebraically simply connected variety has the Hilbert Property. We add more conditions that will possibly make our question easier to answer.

Question 2. Is any smooth simply connected projective variety with a Zariski dense set of rational points has the Hilbert Property over K?

First, we notice that the smooth condition is crucial because we can find non-smooth simply connected varities with a Zariski dense set of rational points that do not have the Hilbert Property. One example is the Enriques Surface of example 3.2.20.

The answer to the this question is unknown, however, a positive answer would imply more than an equivalence of the Hilbert Property to a topological aspect of this class of varieties. In fact, since Serre has proved that any smooth model of an unirational variety is simply connected [25], this would imply an affirmative answer to Colliot-Thélène and Sansuc's conjecture, and therefore for Inverse Galois Problem.

Another possible way of relating the Hilbert Property to a positive answer to Inverse Galois Problem is using Manin's Conjecture for singular Fano varieties [26]. This Conjecture might prove the Hilbert Property for the quotients of projective spaces that are of our interest, reformulating the Noether's approach for Inverse Galois Problem.

We conclude our study at this point: where the original motivation finds the future research perspectives.

Bibliography

[1] D. Hilbert, Uber die Irreducibilitat ganzer rationaler Functionen mit ganzzahligen Koefficienten, J. reine angew. Math 110: 104–129, 1892.

[2] J. Colliot-Thélène and J. Sansuc. Principal homogeneous spaces under flasque tori: applications. J. Algebra, 106: 148– 205, 1987.

[3] P. Morandi, Field and Galois Theory, Springer, 1996.

[4] R. Hartshorne, Algebraic Geometry, Springer, 1977.

[5] I. Shafarevich, M. Reid, Basic Algebraic Geometry I - Varieties in Projective Space, Springer, 2013.

[6] J. Mckernan, Rational, Unirational and Rationally Connected Varieties, available at http://math.mit.edu/~mckernan/Teaching/07-08/Spring/18.726/l_7.pdf, 2008.

[7] W. Fulton, Algebraic Curves - An introduction to Algebraic Geometry,III Ed., 2008.

[8] M. Artin, D. Mumford, Some Elementary Examples of Unirational Varieties Which are Not Rational. Proc. London Math. Soc., 1972.

[9] M. Atiyah, I. Macdonald, Introduction to Commutative Algebra, Addison-Wesley Publishing Company, 1969.

[10] I. Herstein, Topics in Algebra,II Ed., John Wiley and Sons, 1975.

[11] R. Swan. Invariant rational functions and a problem of Steenrod, Invent. Math. 7: 148-158, 1969.

[12] M. Fried, M. Jarden, Field Arithmetic, II Ed., Springer, 2005.

[13] M. Villarino, B. Gasarch, K. Regan, Hilbert's Proof of His Irreducibility Theorem. The American Mathematical Monthly, 2016.

[14] H.G.J. Tiesinga, The Inverse Galois Problem, available at https://fse.studenttheses.ub.rug.nl/14148/1/thesisclassic.pdf, 2016.

[15] J. Silverman, The Arithmetic of Elliptic Curves, Springer, 1986.

[16] S. Cutkosky, An Introduction to Algebraic Geometry, American Math. Soc., 2018.

[17] J-P. Serre, Topics in Galois Theory, Jones and Bartlett, Boston 1992.

[18] D. Mumford, Algebraic Geometry I - Complex Projective Varieties, Springer Verlag 1995.

[19] J-P. Serre, Lectures on the Mordell-Weil Theorem, Vieweg, 1982.

[20] A. Hatcher, Algebraic Topology, 2001.

[21] P. Corvaja, U. Zannier, On the Hilbert Property and the Fundamental Group of Algebraic Varieties, Mathematische Zeitschrift 286(1-2):579 - 602, 2017.

[22] B. Poonen, Rational Points on Varieties, American Math. Soc., 2017.

[23] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent Math 73: 349–366, 1989.

[24] H.P.F. Swinnerton-Dyer, $A^4 + B^4 = C^4 + D^4$ revisited, J. London Math. Soc. 43: 149–151, 1968.

[25] J-P. Serre, On the fundamental group of a unirational variety, J. London Math. Soc. , s1-34 (4): 481-484, 1959.

[26] V. Batyrev, Yu. Manin, Sur le nombre de points rationnels des variétés algébriques, Math. Annalen 286: 27-43, 1990.

[27] F. Duhesme, The Inverse Galois Problem over $\mathbb{Q}$ and Hilbert's Irreducibility Theorem, available at https://people.math.ethz.ch/~pink/Theses/2018-Bachelor-Franc%CC%A7ois-Duhesme.pdf, 2018.