Integer values of polynomials

Giulio Peruginelli

Integer values of polynomials

PhD Thesis

defended on the 13th of December 2008

Advisor:

Prof. Umberto Zannier

Candidate:

Giulio Peruginelli

Università degli Studi di Pisa, Italy

Jury

Prof. Ilaria Del Corso	President
Prof. Andrea Bandini	Member
Prof. Roberto Dvornicich	Referee
Prof. Umberto Zannier	Advisor

Contents

Introduction

Let $f(X)$ be a polynomial with rational coefficients, S be an infinite subset of the rational numbers and consider the image set $f(S)$. If $g(X)$ is a polynomial such that $f(S) = g(S)$ we say that g *parametrizes* the set $f(S)$. Besides the obvious solution $g = f$ we may want to impose some conditions on the polynomial g; for example, if $f(S) \subset \mathbb{Z}$ we wonder if there exists a polynomial with integer coefficients which parametrizes the set $f(S)$.

Moreover, if the image set $f(S)$ is parametrized by a polynomial g, there comes the question whether there are any relations between the two polynomials f and g. For example, if h is a linear polynomial and if we set $g = f \circ h$, the polynomial g obviously parametrizes the set $f(\mathbb{Q})$. Conversely, if we have $f(\mathbb{Q}) = g(\mathbb{Q})$ (or even $f(\mathbb{Z}) = g(\mathbb{Z})$) then by Hilbert's irreducibility theorem there exists a linear polynomial h such that $g = f \circ h$. Therefore, given a polynomial g which parametrizes a set $f(S)$, for an infinite subset S of the rational numbers, we wonder if there exists a polynomial h such that $f = g \circ h$. Some theorems by Kubota give a positive answer under certain conditions.

The aim of this thesis is the study of some aspects of these two problems related to the parametrization of image sets of polynomials.

In the context of the first problem of parametrization we consider the following situation: let f be a polynomial with rational coefficients such that it assumes integer values over the integers. Does there exist a polynomial g with integer coefficients such that it has the same integer values of f over the integers?

This kind of polynomials f are called *integer-valued* polynomials. We remark that the set of integer-valued polynomials strictly contains polynomials with integer coefficients: take for example the polynomial $X(X-1)/2$, which is integer-valued over the set of integers but it has no integer coefficients. So, if f is an integer-valued polynomial, we investigate whether the set $f(\mathbb{Z})$ can be parametrized by a polynomial with integer coefficients; more in general we look for a polynomial $g \in \mathbb{Z}[X_1, \ldots, X_m]$, for some natural number $m \in \mathbb{N}$, such that $f(\mathbb{Z}) = g(\mathbb{Z}^m)$. In this case we say that $f(\mathbb{Z})$ is $\mathbb{Z}$*-parametrizable*.

In a paper of Frisch and Vaserstein it is proved that the subset of pythagorean triples of $\mathbb{Z}^3$ is parametrizable by a single triple of integer-valued polynomials in four variables but it cannot be parametrized by a single triple of integer coefficient polynomials in any number of variables. In our work we show that there are examples of subset of $\mathbb{Z}$ parametrized by an integer-valued polynomial in one variable which cannot be parametrized by an integer coefficient polynomial in any number of variables.

If $f(X)$ is an integer-valued polynomial, we give the following characterization of the parametrization of the set $f(\mathbb{Z})$: without loss of generality we may suppose that $f(X)$ has the form $F(X)/N$, where $F(X)$ is a polynomial with integer coefficients and N is a minimal positive integer. If there exists a prime p different from 2 such that p divides N then $f(\mathbb{Z})$ is not $\mathbb{Z}$-parametrizable. If $N = 2^n$ and $f(\mathbb{Z})$ is $\mathbb{Z}$-parametrizable then there exists a rational number β which is the ratio of two odd integers such that $f(X) = f(-X + \beta)$. Moreover $f(\mathbb{Z}) = g(\mathbb{Z})$ for some $g \in \mathbb{Z}[X]$ if and only if $f \in \mathbb{Z}[X]$

or there exists an odd integer b such that $f \in \mathbb{Z}[X(b-X)/2]$. We show that there exists integer-valued polynomials $f(X)$ such that $f(\mathbb{Z})$ is $\mathbb{Z}$-parametrizable with a polynomial $G(X_1, X_2) \in \mathbb{Z}[X_1, X_2]$, but $f(\mathbb{Z}) \neq g(\mathbb{Z})$ for every $g \in \mathbb{Z}[X]$.

In 1963 Schinzel gave the following conjecture: let $f(X, Y)$ be an irreducible polynomial with rational coefficients and let S be an infinite subset of $\mathbb{Q}$ with the property that for each x in S there exists y in S such that $f(x, y) = 0$; then either f is linear in Y or f is symmetric in the variables X and Y.

We remark that if a curve is defined by a polynomial with Schinzel's property then its genus is zero or one, since it contains infinite rational points; here we use a theorem of Faltings which solved the Mordell-Weil conjecture (if a curve has genus greater or equal to two then the set of its rational points is finite). We will focus our attention on the case of rational curves (genus zero). Our objective is to describe polynomials $f(X, Y)$ with Schinzel's property whose curve is rational and we give a conjecture which says that these rational curves have a parametrization of the form $(\varphi(T), \varphi(r(T)))$.

This problem is related to the main topic of parametrization of image sets of polynomials in the following way: if $(\varphi(T), \psi(T))$ is a parametrization of a curve $f(X, Y) = 0$ (which means $f(\varphi(T), \psi(T)) = 0$), where f is a polynomial with Schinzel's property, let $S = \{\varphi(t) | t \in S'\}$ be the set of the definition of Schinzel, where $S' \subset \mathbb{Q}$. Then for each $t \in S'$ there exists $t' \in S'$ such that $\psi(t) = \varphi(t')$, hence $\psi(S') \subset \varphi(S')$. So, in the case of rational curves, the problem of Schinzel is related to the problem of parametrization of rational values of rational functions with other rational functions (we will show that under an additional hypothesis we can assume that $(\varphi(T), \psi(T))$ are polynomials). In particular, if $(\varphi(T), \psi(T))$ is a parametrization of a curve defined by a symmetric polynomial, then $\psi(T) = \varphi(a(T))$, where $a(T)$ is an involution (that is $a \circ a = Id$). So in the case of rational symmetric plane curves we have this classification in terms of the parametrization of the curve.

It turns out that this argument is also related to Ritt's theory of decomposition of polynomials. His work is a sort of "factorization" of polynomials in terms of indecomposable polynomials, that is non-linear polynomials f such that there are no g, h of degree less than $\deg(f)$ such that $f = g \circ h$. The indecomposable polynomials are some sort of "irreducible" elements of this kind of factorization.

In the first chapter we recall some basic facts about algebraic function fields in one variable, the algebraic counterpart of algebraic curves. In particular we state the famous Luroth's theorem, which says that a non trivial subextension of a purely trascendental field of degree one is purely trascendental.

We give the definition of minimal couple of rational functions that we will use later to characterize algebraically a proper parametrization of a rational curve. We conclude the chapter with the general notion of valuation ring of a field and we characterize valuation rings of a purely trascendental field in one variable (which corresponds geometrically to

the Riemann sphere, if for example the base field is the field of the complex numbers). Moreover valuation rings of algebraic function fields in one variable are discrete valuation rings.

In the second chapter we state the first theorem of Ritt, which deals with decomposition of polynomials with complex coefficients with respect to the operation of composition. In a paper of 1922 Ritt proved out that two maximal decompositions (that is a decomposition whose components are neither linear nor further decomposable) of a complex polynomial have the same number of components and their degrees are the same up to the order. We give a proof in the spirit of the original paper of Ritt, which uses concepts like monodromy groups of rational functions, coverings and theory of blocks in the action of a group on a set.

This result can be applied in the case of an equation involving compositions of polynomials: thanks to Ritt's theorem we know that every side of the equation has the same number of indecomposable component.

In the third chapter we give the classical definition of plane algebraic curves, both in the affine and projective case. We show that there is a bijection between the points of a non-singular curve and the valuation rings of its rational function field (which are called places of the curve). More generally speaking, if we have a singular curve C, the set of valuation rings of its rational function field is in bijection with the set of points of a non-singular model C' of the curve (that is the two curves C and C' are birational), called desingularization of the curve.

Then we deal with curves whose points are parametrized by a couple of rational functions in one parameter; we call these curves rational. From a geometric point of view a rational curve has desingularization which is a compact Riemann surface of genus zero, thus isomorphic to $\mathbb{P}^1$. Finally we expose some properties of parametrizations of rational curves; we show a simple criterium which provides a necessary and sufficient condition that lets a rational curve have a polynomial parametrization in terms of places at infinity.

In the fourth chapter we study the aforementioned conjecture of Schinzel.

For example, if $f(X,Y) = Y - a(X)$ then by taking S the full set of rational numbers we see that the couple (f,S) satisfies the Schinzel's property. If f is symmetric and the set of rational points of the curve determined by f is infinite, then if we define S to be the projection on the first coordinate of the rational points of the curve we obtain another example of polynomial with the above property.

The hypothesis of irreducibility of the polynomial f is required because we want to avoid phenomenon such as $f(X,Y) = X^2 - Y^2$ and $S = \mathbb{Q}$, where f is neither linear nor symmetric. In general if a polynomial $f(X,Y)$ has $X - Y$ as a factor, then it admits the full set of rational numbers as set S. Another example is the following (private communication of Schinzel): let

$$f(X,Y) = (Y^2 - XY - X^2 - 1)(Y^2 - XY - X^2 + 1)$$

and $S = \{F_n\}_{n\in\mathbb{N}}$, where F_n is the Fibonacci sequence which satisfies the identity $F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n$ for each natural number n; if $f_1, f_2 \in \mathbb{Q}[X,Y]$ are the two irreducible factors of f then for each $n \in \mathbb{N}$ the couple of integers (F_n, F_{n+1}) is a point of the curve associated to the polynomial f_1 or f_2, according to the parity of n.

Zannier has recently given the following counterexample to Schinzel's conjecture:

$$f(X,Y) = Y^2 - 2(X^2+X)Y + (X^2-X)^2$$

with S equal to the set of rational (or integer) squares. The idea is the following: it is well known that for each couple of rational functions $(\varphi(t), \psi(t))$ with coefficients in a field k there exists a polynomial $f \in k[X,Y]$ such that $f(\varphi(t), \psi(t)) = 0$. In fact $k(t)$ has trascendental degree one over k; we also say that φ and ψ are algebraically dependent. Moreover if we require that the polynomial f is irreducible then it is unique up to multiplication by constant.

This procedure allows us to build families of polynomials with Schinzel's property: it is sufficient to take couples of rational functions $(\varphi(t), \varphi(r(t)))$, where $\varphi(t), r(t)$ are rational functions. If we consider the irreducible polynomial $f \in \mathbb{Q}[X,Y]$ such that $f(\varphi(t), \varphi(r(t))) = 0$ and the set $S = \{\varphi(t) | t \in \mathbb{Q}\}$, we see that (f, S) has Schinzel's property. In particular Zannier's example is obtained from the couple of rational functions $(\varphi(t), r(t)) = (t^2, t(t+1))$. If $\deg(\varphi) > 1$ and $\deg(r(t)) > 1$ then it turns out that f is neither linear nor symmetric in X and Y, but it is a polynomial with Schinzel's property.

In the last chapter we deal with the problem of parametrization of integer-valued polynomials and we prove the results mentioned at the beginning of this introduction. The idea of the proof is the following: let $f(X) = F(X)/N$ be an integer-valued polynomial as above; since the set of integer-valued polynomials is a module over $\mathbb{Z}$, we can assume that N is a prime number p. We remark that a bivariate polynomial of the form $f(X) - f(Y)$ has over $\mathbb{Q}$ only two linear factors; moreover, the set of integer values n such that there exists $q \in \mathbb{Q}$ such that (n, q) belongs to an irreducible component of the curve $f(X) - f(Y) = 0$ which is not linear in Y, has zero density, by a theorem of Siegel. If $f(\mathbb{Z})$ is $\mathbb{Z}$-parametrizable by a polynomial $g \in \mathbb{Z}[X_1, \ldots, X_m] = \mathbb{Z}[\underline{X}]$ then by Hilbert's irreducibility theorem there exists $Q \in \mathbb{Q}[\underline{X}]$ such that $F(Q(\underline{X})) = pg(\underline{X})$; we obtain necessary conditions for such polynomial Q in order to satisfy the previous equality. In the same hypothesis, for each $n \in \mathbb{Z}$ there exists $\underline{x}_n \in \mathbb{Z}^m$ such that $f(n) = f(Q(\underline{x}_n))$. So we study how the points $(n, Q(\underline{x}_n))$, for $n \in \mathbb{Z}$, distribute among the irreducible components of the curve $f(X) - f(Y) = 0$; by the aforementioned theorem of Siegel it turns out that, up to a subset of density zero of $\mathbb{Z}$, they belong to components determined by linear factors of $f(X) - f(Y)$. For each of them, the projection on the first component of this kind of points is a set of integers contained in a single residue class modulo the prime p. So if p is greater then two, which is the maximum number of linear factors of a bivariate separated polynomial over $\mathbb{Q}$, the set $f(\mathbb{Z})$ is not $\mathbb{Z}$-parametrizable.

The problem of factorization of bivariate separated polynomials, that is polynomials of the form $f(X) - g(Y)$, is a topic which has been intensively studied for years (Bilu, Tichy, Zannier, Avanzi, Cassou-Noguès, Schinzel, etc...)

Our next aim is the classification of the integer-valued polynomials $f(X)$ such that $f(\mathbb{Z})$ is parametrizable with an integer coefficient polynomial in more than one variable (for example $f(X) = 3X(3X-1)/2$). I conjecture that such polynomials (except when $f \in \mathbb{Z}[X]$) belong to $\mathbb{Z}[p^k X(p^k X - a)/2]$, where p is a prime different from 2, a is an odd integer coprime with p and k a positive integer. I show in my work that if $f(X)$ is such a polynomial, then $f(\mathbb{Z})$ is $\mathbb{Z}$-parametrizable.

Moreover we want to study the case of number fields, that is the parametrization of sets $f(O_K)$, where O_K is the ring of integers of a number field K and $f \in K[X]$ such that $f(O_K) \subset O_K$, with polynomials with coefficients in the ring O_K.

Acknowledgements I wish to warmly thank prof. Umberto Zannier for suggesting me the problem of parametrization of integer-valued polynomials and the useful help he gave me in the proof of the theorem which describes these parametrizations. Without his help I couldn't have stated and proved this theorem in such a nice and simple form. He also pointed me out two mistakes I made.

I am also in debt with prof. Sheram S. Abhyankar and prof. Andrzej Schinzel. I had with them useful discussions which allowed me to see some problems in greater depth. In particular I owe Schnizel a debt of gratitude for the time he dedicated to me listening to the problems arosen in the development of my work of thesis.

I want to thank also prof. Mario Poletti who read some pages of my work and pointed me out some errors.

I wish to thank also all my colleagues in Pisa, especially Lorenzo Brasco, Luca Caputo, Sara Checcoli and Laura Paladino. They helped me both with mathematics and the English language. For the latter I want to thank my brother's wife Elena, who suffered in reading something she couldn't understand the meaning of.

Chapter 1

Algebraic function fields in one variable

The algebraic analogue of algebraic plane curves, that is the zero-locus of a polynomial $f(X, Y)$ (see chapter 4), are algebraic function fields in one variable; we are going to explain some basic facts about them.

Let k be a field which from now on we call the **base field**; an **algebraic function field in one variable over** k is a field K finitely generated over k such that the trascendence degree of K over k is equal to 1 and k is algebraically closed in K.

1.1 Lüroth theorem

The "simplest", so to speak, algebraic function field in one variable is the pure trascendental field in one indeterminate $k(t)$. Here we give some details about this kind of algebraic function fields.

Definition 1.1.1 *If $f(t) = \frac{\varphi(t)}{\psi(t)}$ is a rational function in reduced form (that is φ and ψ are coprime polynomials) then the degree of f is defined as*

$$\deg(f(t)) \doteqdot \max\{\deg(\varphi(t)), \deg(\psi(t))\}$$

Lemma 1.1.2 *If $f(t)$ is a rational function over k then the extension of field $k(f) \subset k(t)$ is finite and its degree is equal to* $\deg(f)$.

Proof : Let $f(t)$ be of the form $\frac{r(t)}{s(t)}$ where $r, s \in k[t]$ are coprime polynomials; then t satisfies the following polynomial with coefficients in $K(f)$:

$$F(X) = r(X) - f \cdot s(X)$$

This polynomial is irreducible in $k[f, X] = k[X][f]$ because it has degree 1 in f and it is primitive over the ring $k[X]$; by Gauss Lemma it is irreducible in $k(f)[X]$. The X-degree of F is equal to $\deg(f)$. $\square$

Every non-trivial subextension of a pure trascendental extension of degree one is a pure trascendental extension of degree one, as the following theorem says (this is false for trascendental extension of higher degree).

Theorem 1.1.3 ***(Lüroth)*** *Let k be a field and t a trascendental element over k. If K is a field such that $k \subsetneq K \subset k(t)$ then there exists a rational function g in $k(t)$ such that $K = k(g)$.*

Proof : The field $k(t)$ is a finite algebraic extension of K because if $g \in K - k$ then $k(t)/k(g)$ is a finite extension by previous lemma.

Let

$$f(X) = X^n + a_{n-1}(t)X^{n-1} + \ldots + a_0(t)$$

be the minimal polynomial of t over K, where $a_i(t) \in K \subset k(t)$ for each $i = 0, \ldots, n-1$; since t is trascendental over k, there exists an index $j \in \{0, \ldots, n-1\}$ such that $a_j(t) \notin k$. If we multiply $f(X)$ by the least common multiple of the denominators of the coefficients $a_i(t)$'s we obtain a primitive irreducible polynomial in $k[t, X]$

$$f_0(t, X) = \alpha_n(t)X^n + \ldots + \alpha_0(t)$$

where $\alpha_i \in k[t]$ for each $i = 0, \ldots, n$; let m be the degree of $f_0(t, X)$ in t, that is the maximum of the degrees of the $\alpha_i(t)$'s.

If $\theta = p(t)/q(t)$ is the reduced representation of $a_j(t)$, where $p, q \in k[t]$ are coprime, then t is root of the polynomial

$$H(X) = q(X)\theta - p(X)$$

with coefficients in the field $k(\theta) \subset K$; indeed $H(X)$ is the minimal polynomial of t over $k(\theta)$. So $f(X)$ divides $H(X)$ in $K[X]$ and consequently $f_0(t, X)$ divides the primitive polynomial $H_0(t, X) = q(X)p(t) - p(X)q(t)$ in $k[t, X]$. We have the following equality in $k[t, X]$

$$q(X)p(t) - p(X)q(t) = f_0(t, X)s(t, X)$$

where $s \in k[t, X]$.

Observe now that the degree in t of the first member is less or equal than m, since θ is a coefficient of $f(X)$; then the degree in t of $s(t, X)$ is equal to 0. So $s(t, X) = s(X)$ is a polynomial in the variable X and it divides $H_0(t, X)$ which is primitive in $k[X]$: this implies that the polynomial s is constant. Hence the degree in X of $H_0(t, X)$, which is the degree $[k(t) : k(\theta)]$, is equal to the degree in X of $f(t, X)$. Hence we have proved that $K = k(\theta)$. $\square$

The proof works for each non-constant coefficients $a_i(t)$ of $f(X)$: the field K can be generated over k by each coefficient $a_i(t)$ which is not constant.

The following theorem is the polynomial version of the Lüroth theorem: if a non-trivial subextension of $k(t)$ contains a polynomial then it can be generated by a polynomial.

Theorem 1.1.4 *(**Lüroth in polynomial form**) Let k be a field and t a trascendental element over k. If K is a field such that $k \subsetneq K \subset k(t)$ and it contains a polynomial $f \in K[t]$, then there exists $g \in k[t]$ such that $K = k(g)$.*

A proof of this theorem was already known to Ritt (see [35]) and it is the one we are going to show.

Proof : From Lüroth's theorem there exists a rational function $r \in k(t)$ such that $K = k(r)$; from the inclusion of fields $k(f) \subset k(r) \subset k(t)$ it follows that $f = s \circ r$ where $s \in K(r)$.

The natural map

$$F : k \cup \{\infty\} \to k \cup \{\infty\}$$
$$t \mapsto f(t)$$

associated to the polynomial f is totally ramified over ∞, which means that the fiber of F over ∞ has only one point since $F^{-1}(\infty) = \{\infty\}$; we obviously have that $F = S \circ R$, where S and R are the maps from $k \cup \{\infty\}$ in itself associated to s and r respectively.

This fact implies that the maps S and R are totally ramified over ∞ and $R(\infty)$ respectively; in fact

$$F^{-1}(\infty) = (S \circ R)^{-1}(\infty) = R^{-1}(S^{-1}(\infty)) = \overset{\circ}{\bigcup_{\alpha \in S^{-1}(\infty)}} R^{-1}(\alpha)$$

So if $S^{-1}(\infty) = \{\alpha\}$ we can choose a rational function $\lambda \in k(t)$ of degree 1 such that $\lambda(\alpha) = \infty$ (for example if $\alpha \in k$ we can choose $\lambda(t) = 1/(t - \alpha)$; if $\alpha = \infty$ then s and r are polynomials). Hence the rational function $s' = s \circ \lambda^{-1}$ satisfies $s'^{-1}(\infty) = \{\infty\}$ and so it is a polynomial. For the same reason $r' = \lambda \circ r$ is a polynomial and we have that $f = s' \circ r'$. Obviously $k(r) = k(r')$ since λ has degree 1. □

1.2 Minimal couples of rational functions

Let k be a fixed field and consider the pure trascendental field $k(t)$. If $(\varphi(t), \psi(t))$ is a couple of rational functions of $k(t)$ then, since the trascendence degree of $k(t)$ over k is one, they are algebraically dependent in $k(t)$, which means that there exists a polynomial $F(X, Y) \in k[X, Y]$ such that the following equality holds in $k(t)$

$$F(\varphi(t), \psi(t)) = 0 \tag{1.1}$$

By proposition 3.1.2 there is a unique minimal irreducible polynomial $F(X, Y)$ modulo constant factor such that (1.1) holds. We call this polynomial **minimal polynomial** of $(\varphi(t), \psi(t))$.

Lemma 1.2.1 *Let $\varphi, \psi \in k(t)$ be such that $k(\varphi, \psi) = k(t)$ and $f \in k[X, Y]$ be irreducible such that $f(\varphi(t), \psi(t)) = 0$. Then $\deg(\varphi) = \deg_Y(f)$ and $\deg(\psi) = \deg_X(f)$.*

Proof : Given a rational function $\varphi \in k(t)$ the degree of the field extension $k(\varphi) \subset k(t)$ is equal to the degree $\deg(\varphi)$ by lemma 1.1.2. The field $k(\varphi, \psi)$ is an algebraic function field in one variable since $x = \varphi(t), y = \psi(t)$ are algebraically dependent; since f is irreducible, the polynomial $f(x, Y) \in k(x)[Y]$ is the minimal polynomial of y over the field $k(x)$ and so the degree of $k(x, y)$ over $k(x)$ is equal to the degree in Y of f. By hypothesis we have $k(x, y) = k(t)$ from which the thesis follows immediately for the rational function φ. Symmetrically we conclude for ψ. □

¿From now on we call **minimal** a couple of rational functions (φ, ψ) which satisfies the hypothesis of the lemma; from a geometric point of view this means that the map $F : \mathbb{A}^1 \to C$, given by $t \mapsto (\varphi(t), \psi(t))$, where C is the image curve of the application F (defined as the zero-locus of the minimal polynomial f of (φ, ψ)), has degree one, that is a birational map (see chapter 4).

In general if a couple (φ, ψ) of rational functions is not minimal then its miminal polynomial $f(X, Y)$ satisfies an algebraic equation $f(\varphi_1(t), \psi_1(t)) = 0$ where (φ_1, ψ_1) is minimal: this follows by Lüroth theorem (see 1.1.3).

In fact by this theorem, the field generated by φ and ψ over k, that is $k(\varphi(t), \psi(t))$ which is a subfield of $k(t)$, is equal to $k(\eta(t))$ for a certain rational function $\eta \in k(t)$; the couple (φ, ψ) is minimal exactly in the case when the degree of η is equal to one: in this case it follows that $k(\eta) = k(t)$ by lemma 1.1.2.

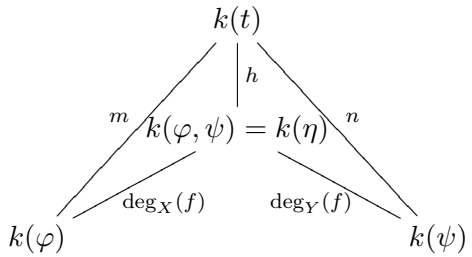
If the degree of $h = \deg(\eta)$ is greater than one we have that $\varphi = \varphi_1 \circ \eta$ and $\psi = \psi_1 \circ \eta$ for certain rational functions φ_1 and ψ_1 of degree less than the degrees of φ and ψ respectively. If an irreducible polynomial $f \in k[X, Y]$ satisfies the relation $f(\varphi_1(\eta), \psi_1(\eta)) = 0$ (η is seen as a trascendental element over k) then we also have that $f(\varphi_1(\eta(t)), \psi_1(\eta(t))) = 0$; conversely if we have f irreducible such that

$$f(\varphi_1(\eta(t)), \psi_1(\eta(t))) = 0$$

then for the surjectivity of rational functions of $\mathbb{P}^1(\overline{k}) = \overline{k} \cup \{\infty\}$ in itself (given by rational functions in $\overline{k}(t)$) it follows that $f(\varphi_1(\eta), \psi_1(\eta)) = 0$.

Observe that $k(\varphi_1, \psi_1) = k(\eta)$ (φ_1 and ψ_1 are rational functions of $k(\eta)$). Hence we have proved the following lemma, which generalizes the previous one:

Lemma 1.2.2 *Let $\varphi, \psi, \eta \in \mathbb{Q}(t)$ be such that $k(\varphi, \psi) = k(\eta) \subset k(t)$. Let $f \in k[X, Y]$ be irreducible such that $f(\varphi(t), \psi(t)) = 0$; then $\deg(\varphi) = h \cdot \deg_Y(f)$ e $\deg(\psi) = h \cdot \deg_X(f)$ where $h = [k(t) : k(\eta)]$.*



The proof of this lemma also shows that we can associate to each couple of rational functions (φ, ψ) a minimal couple (φ_1, ψ_1) of rational functions which defines the same curve $C = \{(x, y) \in \mathbb{A}^2(k) | f(x, y) = 0\}$. We also say that (φ_1, ψ_1) is a minimal parametrization of the curve C.

The following lemma is an immediate consequence of the previous results.

Lemma 1.2.3 *Let $\varphi, \psi \in k(t)$. If $(\deg \varphi, \deg \psi) = 1$ then (φ, ψ) is minimal.*

1.3 Valuation rings

Valuation rings of algebraic function fields in one variable are the algebraic counterpart of geometric points of algebraic curves. More precisely the set of valuation rings of an algebraic function fields K corresponds bijectively to the geometric point a non-singular model of a curve with rational function field isomorphic to K (see paragraph 3.4) .

Definition 1.3.1 *Let K be a field. A valuation ring of K is a subring $O \subset K$ such that for each $x \in K$ we have $x \in O$ or $x^{-1} \in O$.*

If $k \subset K$ is a field extension and O is a valuation ring of K such that $k \subset O$ then we say that O is a valuation ring of K over k.

Lemma 1.3.2 *Valuation rings are local rings integrally closed.*

Proof : The ideal $P = \{x \in O | x^{-1} \notin O\}$ is maximal and $O - P = O^*$.

If F is the quotient field of O (O is a domain because it is contained in a field) and $x \in F$ is integral over O, then

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$$

with $a_i \in O$. If $x \notin O$ then $x^{-1} \in O$. If we multiply the previous equality by x^{-n} we obtain

$$1 = -a_{n-1}x^{-1} - \ldots - a_0 x^{-n}$$

Hence we have a contradiction: the right member is in O so 1 would be an element of O. $\square$.

Let K/k be an algebraic function field in one variable. If O is a valuation ring of K over k with maximal ideal P then $k \subset O/P$ since $k \cap P = \{0\}$; the field O/P is called **residue field** of the valuation ring O. The following proposition shows that the extension $k \subset O/P$ is finite (for a proof of this fact see Rosen, [36] chap. 5, pg. 46):

Proposition 1.3.3 *Let K/k be an algebraic function field in one variable and let (O, P) be a valuation ring of K over k; then the residue field of O is a finite extension of k.*

If we assume that the base field k is algebraically closed then the residue field of valuation rings are all equal to k.

The next result classifies valuation rings of a purely trascendental extension of trascendence degree one, which is, as we said above, the "simplest" case of algebraic function field (geometrically it corresponds to the curve $\mathbb{P}^1$). These field has two type of valuation rings: the localization of $k[t]$ with respect to a prime ideal of $k[t]$ and the valuation ring at infinity, which is the ring of rational functions which are regular at infinity, that is the rational functions $f(t)/g(t)$, with $\deg(g) \geq \deg(f)$.

Proposition 1.3.4 *Let $K = k(t)$ be a purely trascendental extension of degree 1 and let O be a valuation ring of K over k; then either O is the localization of $k[t]$ for a certain prime ideal $\mathfrak{p}$ of $k[t]$ or $O = k[1/t]_{(1/t)}$.*

Proof : Let $P = \{x \in O | x^{-1} \notin O\}$ be the maximal ideal of O.

If $t \in O$ then $k[t] \subset O$ since O is a ring. The ideal $\mathfrak{p} = P \cap k[t]$ is a prime ideal of $k[t]$, different from the zero ideal (otherwise $O = K$); let $f \in k[t]$ be an irreducible polynomial which generates the ideal $\mathfrak{p}$. If $x \in k[t]_{\mathfrak{p}}$ then $x = h(t)/g(t)$ with $h, g \in k[t]$ coprime and $g \notin \mathfrak{p} \subset M$; hence $g^{-1} \in O^*$ and so $h/g \in O$.

Let x be in O of the form $x = h(t)/g(t)$, where $h, g \in k[t]$ are coprime polynomials and suppose that $x \notin k[t]_{\mathfrak{p}}$: then $x^{-1} \in \mathfrak{p}k[t]_{\mathfrak{p}}$, the maximal ideal of the localization $k[t]_{\mathfrak{p}}$; hence $g \in \mathfrak{p} \subset P$ and $h \notin \mathfrak{p}$. So $h \in O^*$ and $1/h \cdot x = 1/g \in O$. Since $g \in P$ this leads to a contradiction. So if $t \in O$ we have proved that $O = k[t]_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime ideal of $k[t]$.

If $t \notin O$ then $s = t^{-1} \in P$; by considering again the prime ideal $\mathfrak{p} = P \cap k[s]$ we have that $s \in \mathfrak{p}$ and so s is a generator of $\mathfrak{p}$ (its degree is the least possible). We conclude that $O = k[s]_s = k[1/t]_{1/t}$. $\square$.

In particular we observe that if k is algebraically closed then the valuation rings of $k(t)$ are in bijection with the elements of $k \cup \{\infty\}$. From a geometric point of view the valuation ring O_p of $k(t)$, for $p \in k$, is the set of rational functions $\varphi(t) = f(t)/g(t)$ such that $g(p) \neq 0$, that is φ does not have a pole in p; the valuation ring at infinity O_∞ is the set of rational functions $\varphi(t) = f(t)/g(t)$ such that $\deg(g) \geq \deg(f)$ (which implies that φ does not have a pole at infinity). Observe that maximal ideals of valuation rings of $k(t)$

are principal ideal; this particular kind of valuation ring is called **discrete valuation ring** (DVR for short, see Serre [40]). Actually valuation rings of algebraic function fields in one variable are discrete valuation rings (see next results).

The next result can be seen as a particular case of Noether normalization lemma, valid in the case of separable extension (and hence simple extension if they are finite).

Lemma 1.3.5 *Let $E = K(\alpha)$ be a finite extension of a field K and A a subring of K such that K is the quotient ring of A. Then there exists $\alpha' \in E$ such that $E = K(\alpha')$ and α' is integral over A.*

Proof : By hypothesis α is a root of a monic polynomial:

$$f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$$

where $a_i \in K$. Since K is the quotient field of A then there exists $d \in A$ such that $da_i \in A$ for every $i = 0, \ldots, n-1$. If we multiply the equation $f(\alpha) = 0$ by d^n we obtain:

$$(d\alpha)^n + da_{n-1}(d\alpha)^{n-1} + \ldots + d^{n-1}a_1(d\alpha) + d^n a_0 = 0$$

If we define $\alpha' = d\alpha$ we obtain the desired element. □

If A is a subring of a field K, the integral closure of A in K is defined to be the set of all elements of K which are integral over A (i.e. they satisfy a monic equation over A). Next proposition (see [9]) characterizes integral closure in terms of valuation rings.

Proposition 1.3.6 *Let A be a ring and let K be a field such that $A \subset K$. Then the integral closure of A in K is equal to the intersection of all the valuation rings of K which contain A.*

Proof : Let O be a valuation ring of K which contains A; it is integrally closed by lemma 1.3.2. If an element $x \in K$ is integral over A then it is integral over O and so it belongs to O.

Conversely let $x \in K$ be such that it is not integral over A: then it is clear that $x \notin A[\frac{1}{x}] = A[y]$. Since y is not invertible in $A[y]$ there exists a maximal ideal $\mathcal{M}$ of $A[y]$ which contains y. By a classic theorem of Chevalley (see [9], chap.1 §.4) there exists a valuation ring (O, P) of K which contains the ring $A[y]$ and such that $P \subset \mathcal{M}$; since the maximal ideal of a valuation ring is equal to the set $\{\alpha \in O | \alpha^{-1} \notin O\}$ we immediately see that $x \notin O$. The proof is complete. □

This last lemma prove that valuation rings of algebraic function fields are discrete valuation rings, as we said before.

Lemma 1.3.7 *Let k be a perfect field and K an extension of k of trascendence degree one. Then the valuation rings of K are discrete valuation rings.*

Proof : Let $x \in K$ be a trascendental element over k; then there exists $y \in K$ algebraic over $k(x)$ such that $K = k(x, y)$. The intersection of a valuation ring O of K with $k(x)$ is a discrete valuation ring (see above; this is true also in the case of k not algebraically closed: $O \cap k(x) = k[x]_{\mathfrak{p}}$, where $\mathfrak{p} \subset k[x]$ is a prime ideal). The extension of discrete valuation rings in finite algebraic extension are discrete valuation rings (see Lang, [26]); so O is a discrete valuation ring. $\square$

Chapter 2

Ritt's decomposition theorem for polynomials

In this chapter we want to expose an article of Ritt of 1922, "*Prime and composite polynomials*" (see [35]), which deals with decomposition of polynomial with respect to the operation of composition of functions. Strictly speaking Ritt proved that there is a sort of factorization in terms of indecomposable polynomials (i.e. polynomials $f \in \mathbb{C}[X]$ of degree greater than one such that there do not exist non-linear $g, h \in \mathbb{C}[X]$ such that $f = g(h(X))$): the number of terms of a maximal decomposition is unique and the order of the terms of two maximal decomposition are the same up to the order.

¿From this article many others arise (see [11], [12], [29], among the others); they do not add anything new but they prove the same result with other methods, such as ramification theory of valuations in algebraic function fields.

2.1 Introduction

We work with the monoid $(\mathbb{C}(X), \circ)$ and the submonoid $(\mathbb{C}[X], \circ)$, the field of rational functions and the ring of polynomials over $\mathbb{C}$, where $\circ$ denotes the operation of composition of functions; this operation will be denoted in the following ways

$$f \circ g(X) = f(g(X))$$

where f and g are two rational functions.

Lemma 2.1.1 *If $f(X)$ and $g(X)$ are rational functions, then* $\deg(f \circ g) = \deg(f)\deg(g)$.

The following lemma describes the units of $(\mathbb{C}(X), \circ)$.

Lemma 2.1.2 $(\mathbb{C}(X), \circ)^* = \{f(X) \in \mathbb{C}(X) | \deg(f) = 1\} = \{\frac{ax+b}{cx+d} \in \mathbb{C}(X) | ad - bc \neq 0\} \cong PSL(2, \mathbb{C})$.

Definition 2.1.3 *A rational functions $f(X)$ is called **indecomposable** (**prime** in the original article of Ritt) if its degree is strictly larger than one and there do not exist rational functions $g(X), h(X)$ of degree strictly less of* $\deg(f)$ *such that*

$$f(X) = g \circ h(X)$$

It is natural to study how a rational function decomposes into indecomposable functions; by induction any rational functions of degree more then one can be written as the composition of indecomposable functions. A decomposition of a rational function

$$F(X) = f_1 \circ \ldots \circ f_n(X)$$

is called **maximal** if the rational functions f_i are indecomposable; the rational functions f_i of this decomposition are called components of the decomposition of F.

Proposition 2.1.4 *Let $F \in \mathbb{C}(X)$. Then there is a bijection between the set of decomposition of F and chain of subfield between $\mathbb{C}(F)$ and $\mathbb{C}(X)$.*

Maximal decompositions correspond to maximal chain of fields.

Proof : Let $F = f_1 \circ \ldots \circ f_r$ be a decomposition. We associate to this decomposition the chain of field $\mathbb{C}(F) \subset \mathbb{C}(f_2 \circ \ldots \circ f_r) \subset \ldots \subset \mathbb{C}(f_r) \subset \mathbb{C}(X)$.

The opposite map is defined in this way: if $\mathbb{C}(F) \subset K_1 \subset \ldots \subset K_s \subset \mathbb{C}(X)$ is a chain of subfields then $K_s = \mathbb{C}(f_s)$, $K_{s-1} = \mathbb{C}(f_{s-1}(f_s))$, $K_i = \mathbb{C}(f_i(f_{i+1}(\ldots(f_s))))$ for $i = 1, \ldots, s-2$, by Lüroth's theorem. So we have the following decomposition of F: $F = f_1 \circ \ldots \circ f_s$.

Obviously these maps are inverse to each other.

The other statement follows immediately. □.

Corollary 2.1.5 *Let $f \in \mathbb{C}(X)$. The numbers of maximal non-equivalent decompositions is finite.*

Proof : In fact the extension $\mathbb{C}(f) \subset \mathbb{C}(X)$ is separable so the numbers of intermediate fields between $\mathbb{C}(f)$ and $\mathbb{C}(X)$ is finite. □.

Lemma 2.1.6 *Let $F \in \mathbb{C}[X]$ and let $F = f \circ g$ be a decomposition of F, where f and g are in $\mathbb{C}(X)$.*

Then there exists a linear function $\mu \in \mathbb{C}(X)$ such that $f \circ \mu$ and $\mu^{-1} \circ g$ are polynomials.

This lemma implies that we can assume that (indecomposable) factors of a polynomial are themselves polynomials.

Proof : The proof follows from the polynomial version of Lüroth's theorem; consider the field extension $\mathbb{C}(F) \subset \mathbb{C}(g) \subset \mathbb{C}(X)$: by theorem 1.1.4 there exists a polynomial

$g' \in \mathbb{C}[X]$ such that $\mathbb{C}(g) = \mathbb{C}(g')$. Then $F = f' \circ g'$ and it is immediate to see that $f'^{-1}(\infty) = \{\infty\}$ so f' is a polynomial. □

This lemma is straightforward.

Lemma 2.1.7 *If $f \circ g = h \circ g$ then $f = h$.*

In the case of a polynomial, Ritt's work shows that the decomposition is not necessarily unique but the degree of the indecomposable factors are unique up to permutation and also the number of indecomposable components of a maximal decomposition does not depend on the maximal decomposition.

Ritt's work in [35] for decomposition of polynomials contains the following two theorem, now known as first and second theorem of Ritt.

Theorem 2.1.8 ***(First theorem of Ritt)*** *Let $f(X)$ be a polynomial with complex coefficients and let*

$$f(X) = f_1 \circ \ldots \circ f_r(X)$$
$$f(X) = g_1 \circ \ldots \circ g_s(X)$$

be two maximal decomposition of f, where $\{f_i(X)\}_{i=1\ldots r}$ and $\{g_j(X)\}_{i=1\ldots s}$ are indecomposable polynomials.

Then $r = s$ and $\{\deg(f_i)\}_{i=1,\ldots,r} = \{\deg(g_j)\}_{j=1,\ldots,s}$.

So the number of indecomposable factors of a maximal decomposition of a polynomial is unique and the degrees of factors are the same up to permutation.

Two decompositions with the same numbers of components

$$f = f_1 \circ \ldots \circ f_r = g_1 \circ \ldots \circ g_r$$

are equivalent if there exist $r-1$ linear polynomials $\{\lambda_1, \ldots, \lambda_{r-1}\}$ such that

$$g_1 = f_1 \circ \lambda_1, \ \ldots \ g_i = \lambda_{i-1}^{-1} \circ f_i \circ \lambda_i, \ \ldots \ g_r = \lambda_{r-1}^{-1} \circ f_r$$

hence

$$g_1 \circ \ldots \circ g_r = (f_1 \circ \lambda_1^{-1}) \ldots (\lambda_{i-1}^{-1} \circ f_i \circ \lambda_i) \ldots (\lambda_{r-1}^{-1} \circ f_r)$$

The first theorem of Ritt implies that this is an equivalence relation between maximal decompositions of a polynomial F.

After that, Ritt studied the equation

$$\varphi \circ \alpha = \psi \circ \beta$$

where $\varphi, \alpha, \psi, \beta$ are indecomposable polynomials.

For example there are two cases where this equality is satisfied:

- $X^n \circ X^r g(X^n) = X^r g(X)^n \circ X^n$, where $g(X)$ is a polynomial

- $T_n \circ T_m = T_m \circ T_n$, where T_n is the n-th Tchebychev polynomial

In the case of polynomial these are the only case where maximal bidecompositions occur.

We will prove the following lemma.

Lemma 2.1.9 *Let f be a polynomial with complex coefficients and let*

$$f = \varphi \circ \alpha = \psi \circ \beta$$

be two decompositions of f with α and β indecomposable. Then $\deg(\alpha) = \deg(\beta)$ *or* $(\deg(\alpha), \deg(\beta)) = 1$.

Next theorem is now known as the second theorem of Ritt (see [38]) and it concerns maximal bidecompositions of polynomials.

Theorem 2.1.10 ***(Second theorem of Ritt)*** *If $\varphi, \alpha, \psi, \beta$ are indecomposable polynomials such that*

$$\varphi \circ \alpha = \psi \circ \beta$$

with $\deg(\varphi) = \deg(\beta) = m$, $\deg(\alpha) = \deg(\psi) = n$ *and* $(n, m) = 1$ *then the decomposition is equivalent to one of the examples shown above.*

If $f \in \mathbb{C}[X]$ let K the splitting field of $\mathbb{C}(X)$ over $\mathbb{C}(f)$; the monodromy group of f is the Galois group $\mathrm{Gal}(K/\mathbb{C}(f))$ and it is denoted with $\mathrm{Mon}(f)$.

Ritt's results can be grouped together in the following theorem:

Theorem 2.1.11 *Let $f(X)$ be a polynomial with complex coefficients and let*

$$f(X) = f_1 \circ \ldots \circ f_r(X)$$

$$f(X) = g_1 \circ \ldots \circ g_s(X)$$

be two maximal decomposition, where $\{f_i(X)\}_{i=1\ldots r}$ and $\{g_j(X)\}_{i=1\ldots s}$ are polynomials. Then $r = s$, $\{\deg(f_i)\}_{i=1,\ldots,r} = \{\deg(g_j)\}_{j=1,\ldots,s}$ and $\{\mathrm{Mon}(f_i)\}_{i=1,\ldots,r} = \{\mathrm{Mon}(g_j)\}_{j=1,\ldots,s}$.

Moreover it is possible to pass from one decomposition to another by means of the following three ways:

- *$f_i \circ f_{i+1} = (f_i \circ L) \circ (L^{-1} \circ f_{i+1})$, where L is a linear polynomial*
- *$X^n \circ X^r g(X^n) = X^r g(X)^n \circ X^n$, where $g(X)$ is a polynomial*
- *$T_n \circ T_m = T_m \circ T_n$, where T_n is the n-th Tchebychev polynomial*

The result of the monodromy groups is due to Mueller (see his article [31]).

Ritt's work about decomposition of a polynomial function was the study of monodromy groups of a polynomial $f \in \mathbb{C}[X]$ and the link between the monodromy groups of the components of a maximal decomposition of f. We will show a proof of the first theorem of Ritt; in the next paragraphs we will recall some facts about coverings of topological spaces and theory of blocks which arise in the action of a finite group on a finite set. We will need these two theories in the proof of Ritt's results.

2.2 Monodromy and Galois covering

In this section we recall some basic facts about coverings (for more references see [19] and [30]).

Let X and Y be topological spaces; a **covering** from X to Y is a continue and surjective map φ such that for each $y \in Y$ there exists an open neighbourhood $V \subset Y$ of y such that the preimage of V is a disjoint union of open sets U_i of X which are homeomorphic via φ to V, that is $\varphi_{|U_i} : U_i \to V$ is a homeomorphism. The covering is finite if for each y in Y the fiber $\varphi^{-1}(y)$ is finite; if we assume, as we will do from now on, that Y is connected then the cardinality of the fibers of a finite covering is constant and it is called the **degree** of the covering. If we want to specify the base points of the covering, that is elements $x_0 \in X$ and $y_0 \in Y$ such that $\varphi(x_0) = y_0$, we will use the classical notation $\varphi : (X, x_0) \to (Y, y_0)$.

If $\varphi : (X, x_0) \to (Y, y_0)$ is a covering, the following map between fundamental groups of X and Y is well defined

$$\begin{array}{rccc} \varphi_* : & \pi_1(X, x_0) & \to & \pi_1(Y, y_0) \\ & [\gamma] & \mapsto & [\varphi(\gamma)] \end{array}$$

where $[\gamma]$ is the homotopy class of a closed path γ in X with base point x_0 and in the same way $[\varphi(\gamma)]$ (we will omit the square brackets); by monodromy lemma the homomorphism of groups φ_* is injective (see [19]). We call **characteristic subgroup** the subgroup $H = \varphi_*(\pi_1(X, x_0))$ of $G = \pi_1(Y, y_0)$; the index of H in the fundamental group $\pi_1(Y, y_0)$ is equal to the degree of the covering: in fact there is a bijection between the fiber $\varphi^{-1}(y_0)$ and the set G/H (see [19]).

Two coverings $\varphi_1 : (U_1, u_1) \to (V, v_0)$ and $\varphi_2 : (U_2, u_2) \to (V, v_0)$ are **isomorphic** if there exists a homeomorphism $\phi : U_1 \to U_2$ such that $\varphi_2 \circ \phi = \varphi_1$ (note that we do not impose that $\phi(u_1) = u_2$). If $U_1 = U_2 = U$ and $\phi : (U, u_0) \to (V, v_0)$ is a covering then we define the group $\mathrm{Deck}(\phi)$, the **group of automorphisms of the covering**

$$\mathrm{Deck}(\phi) \doteqdot \{\phi : U \to U | \varphi \circ \phi = \varphi\}$$

It is easy to check that every element of $\mathrm{Deck}(\phi)$ preserves the fibers of φ, that is $\phi(\varphi^{-1}(v)) = \varphi^{-1}(v)$, for all $v \in V$.

Proposition 2.2.1 *Two coverings of a topological space (V, v_0) are isomorphic if and only if their characteristic subgroups are conjugate in $\pi_1(V, v_0)$.*

For a proof of this proposition see [19].

Theorem 2.2.2 *If (V, v_0) is a topological space then there is a bijection*

$$\{\varphi : (U, u_0) \to (V, v_0) \textit{covering}\}/_\sim \to \{\textit{conjugacy class of } H < \pi_1(V, v_0)\}$$

Proof : If $H < G = \pi_1(V, v_0)$ we consider the universal covering $\mathcal{U}$ di V (see [19]); then G acts freely on $\mathcal{U}$ through lift of paths and $V \cong \mathcal{U}/G$. We consider the induced action of H on $\mathcal{U}$ and we obtain a covering $\varphi : \mathcal{U}/H \to V$ which has H as characteristic subgroup.

Conversely we associate to a covering φ the conjugacy class of its characteristic subgroup. □

Let $\varphi : (U, u_0) \to (V, v_0)$ be a finite covering of degree n. We define the **monodromy** of the covering as the homomorphism induced by the action of the fundamental group $G = \pi_1(V, v_0)$ on the fiber $\varphi^{-1}(v_0)$:

$$\begin{array}{rccc} \Phi: & \pi_1(V, v_0) & \to & S_{\varphi^{-1}(v_0)} \cong S_n \\ & \gamma & \mapsto & \{u_i \mapsto \widetilde{\gamma}_{u_i}(1)\} \end{array}$$

where $S_{\varphi^{-1}(v_0)}$ is the set of permutations of the finite set $\varphi^{-1}(v_0)$ and $\widetilde{\gamma}_{u_i}$ is the unique lifting in U of γ with base point u_i, where u_i belongs to the fiber $\varphi^{-1}(v_0)$; for the uniqueness of lifting of paths with fixed base point the application Φ is well defined (see [19]). The group $\Phi(\pi_1(V, v_0)) \subset S_n$, permutation group of the set $\varphi^{-1}(v_0)$, is called the **monodromy group** of the covering φ and it is denoted with $\mathrm{Mon}(\varphi)$; since U is connected it follows that this group acts transitively on the fiber $\varphi^{-1}(v_0)$ and so it is a transitive subgroup of S_n. It also acts faithfully on the set $\varphi^{-1}(v_0)$ and it is isomorphic to $\pi_1(V, v_0)/\ker(\Phi)$.

Theorem 2.2.3 *If (V, v_0) is a topological space then there is a bijection*

$$\{\varphi : (U, u_0) \to (V, v_0) \textit{covering}\}/_\sim \to \{\textit{transitive action of } \pi_1(V, v_0) \textit{ on a finite set}\}/_\sim$$

Proof : We have already seen that if $\varphi : (U, u_0) \to (V, v_0)$ is a covering then $\pi_1(V, v_0)$ acts transitively on the set $\varphi^{-1}(v_0)$.

Conversely suppose that the group $G = \pi_1(V, v_0)$ acts transitively on a finite set I; let H be the stabilizer of an element $i \in I$. Then by the same argument of the proof of theorem 2.2.2 there exists a covering $\varphi : (U, u_0) \to (V, v_0)$ with characteristic subgroup H. The fiber $\varphi^{-1}(v_0)$ is identified with the set I, since they are both in bijection with the quotient G/H. □

The following lemma describes the characteristic group of a covering $\phi : (U, u_0) \to (V, v_0)$ in terms of the action of the fundamental group of V in v_0 on the fiber $\phi^{-1}(v_0)$.

Lemma 2.2.4 *Let $\varphi : (U, u_0) \to (V, v_0)$ be a covering. Then the stabilizer of u_0 under the action of the fundamental group $\pi_1(V, v_0)$ is equal to the characteristic group of the covering.*

Next lemma describes the kernel of the monodromy map associated to a covering.

Lemma 2.2.5 *If $\varphi : (U, u_0) \to (V, v_0)$ is a covering, Φ the monodromy and H the characteristic subgroup, then*

$$\ker(\Phi) = \bigcap_{\gamma \in \pi_1(V, v_0)} \gamma H \gamma^{-1}$$

Proof : The statement follows easily from previous lemma. We consider a generic point u on the fiber $\varphi^{-1}(v_0)$: its stabilizer is equal to $\gamma H \gamma^{-1}$, where γ is a path in V obtained as image via φ of a path σ in U with initial point in u_0 and final point in u. The kernel of Φ is the intersection of all stabilizers of the points of the fiber $\varphi^{-1}(v_0)$, which form a conjugacy class of subgroups in $\pi_1(V, v_0)$. □

We now give a definition: if H is a subgroup of a group G we set

$$\mathrm{core}_G(H) \doteqdot \bigcap_{g \in G} g H g^{-1}$$

which is the maximal normal subgroup of G contained in H. The subgroup H is normal in G if and only if $\mathrm{core}_G(H) = H$. So in the previous lemma we have that $\ker(\Phi) = \mathrm{core}_G(H)$, where $G = \pi_1(V, v_0)$.

Let f, φ, ψ be coverings such that $f = \psi \circ \varphi$, and consider the fiber $f^{-1}(v_0)$ under the action of the monodromy group of f. The following proposition permits us to prove that the map φ determines a decomposition in blocks of $f^{-1}(v_0)$ (for the definition of blocks see section 2.3).

Proposition 2.2.6 *Let the following one be a diagram of finite coverings*

$$\begin{array}{ccc} (W, w_0) & \xrightarrow{\varphi} & (U, u_0) \\ & \searrow^{f} & \downarrow \psi \\ & & (V, v_0) \end{array}$$

and let the following ones be the monodromy homomorphisms of f and ψ respectively defined before

$$F : \pi_1(V, v_0) \to S_{f^{-1}(v_0)}$$
$$\Psi : \pi_1(V, v_0) \to S_{\psi^{-1}(v_0)}$$

If $\gamma \in \pi_1(V, v_0)$ then

$$\varphi \circ F(\gamma) = \Psi(\gamma) \circ \varphi$$

that is the following diagram is commutative

$$\begin{array}{ccc} f^{-1}(v_0) & \xrightarrow{F(\gamma)} & f^{-1}(v_0) \\ \varphi \downarrow & & \downarrow \varphi \\ \psi^{-1}(v_0) & \xrightarrow{\Psi(\gamma)} & \psi^{-1}(v_0) \end{array}$$

Proof : If $\psi^{-1}(v_0) = \{u_0, \ldots, u_{m-1}\}$ then $f^{-1}(v_0) = B_0 \cup \ldots \cup B_{m-1}$ where $B_i = \{z \in f^{-1}(v_0) | \varphi(z) = u_i\} = \{z_j^{(i)} | j = 1, \ldots, n\}$.

Let $\gamma \in \pi_1(V, v_0)$ and $F(\gamma)(z_j^{(i)}) = \widehat{\gamma}_{z_j^{(i)}}$ be the unique lifting of γ via f in W with initial point $z_j^{(i)}$.

Observe that $\overline{\gamma} \doteqdot \varphi(\widehat{\gamma}_{z_j^{(i)}})$ is a path in U with initial point $\varphi(z_j^{(i)}) = u_i$ such that $\psi(\overline{\gamma}) = \gamma$ and so it is the unique lifting $\overline{\gamma}_{u_i}$ of γ via ψ in U with initial point u_i, that is $\overline{\gamma} = \Psi(\gamma)(u_i)$.

Hence

$$\varphi(F(\gamma)(z_j^{(i)})) = \varphi(\widehat{\gamma}_{z_j^{(i)}}(1)) = \overline{\gamma}_{u_i}(1) = \Psi(\gamma)(u_i) = \Psi(\gamma)(\varphi(z_j^{(i)}))$$

$$\Rightarrow \varphi \circ F(\gamma) = \Psi(\gamma) \circ \varphi$$

which proves the proposition. □

A consequence of this theorem is the following corollary:

Corollary 2.2.7 *Let the following one be a diagram of finite coverings*

$$\begin{array}{ccc} (W, w_0) & \xrightarrow{\varphi} & (U, u_0) \\ & \searrow^{f} & \downarrow{\scriptstyle \psi} \\ & & (V, v_0) \end{array}$$

For each $u \in \psi^{-1}(v_0)$ we set $B_u \doteqdot \{z \in f^{-1}(v_0) | \varphi(z) = u_0\}$; then the sets B_u, for $u \in \psi^{-1}(v_0)$, are transitively permuted by the group $G = \pi_1(V, v_0)$.

Moreover we have that $H = G_{B_{u_0}}$, where $H = \psi_*(\pi_1(U, u_0))$ and $G_{B_{u_0}}$ is the stabilizer in G of the set B_{u_0}.

Proof : The sets B_u, for $u \in \psi^{-1}(v_0)$, satisfy this property: for all $\sigma \in G$ we have either $\sigma(B_u) = B_u$ or $\sigma(B_u) \cap B_u = \emptyset$ (where $\sigma(B_u)$ has to be intended as $F(\sigma)(B_u)$). This fact implies that G acts on the set $\mathcal{B} = \{B_u\}_{u \in \psi^{-1}(v_0)}$.

In fact suppose that $\sigma(B_i) \cap B_i \neq \emptyset$, that is for some $z \in B_i$ the element $\sigma(z_i)$ is in B_i; then by proposition 2.2.6

$$u_i = \varphi(F(\sigma)(z)) = \Psi(\sigma)(\varphi(z)) = \Psi(u_i)$$

Then if z' is in B_i we have

$$\varphi(F(\sigma)(z')) = \Psi(\sigma)(\varphi(z')) = \Psi(u_i) = u_i$$

so $\sigma(z')$ is in B_i. The set $\mathcal{B}$ is permuted transitively by G, since $f^{-1}(v_0) = \bigcup_{u \in \psi^{-1}(v_0)} B_u$ and G acts transitively on $f^{-1}(v_0)$.

For the second statement, H is the stabilizer in G of the point u_0. If $\sigma \in H$ then $\sigma(u_0) = \Psi(\sigma)(u_0) = u_0$. So for $z \in B_{u_0}$ we have

$$\varphi(F(\sigma)(z)) = \Psi(\sigma)(\varphi(z)) = \Psi(\sigma)(u_0) = u_0$$

hence $\sigma(B_{u_0}) = B_{u_0}$. Conversely let $\sigma \in B_{u_0}$; then

$$\Psi(\sigma)(u_0) = \Psi(\sigma)(\varphi(z)) = \varphi(F(\sigma)(z)) = \varphi(z') = u_0$$

where z, z' are elements of B_{u_0}. □

Proposition 2.2.8 *Let the following one be a diagram of finite coverings*

$$\begin{array}{ccc} (W, w_0) & \xrightarrow{\varphi} & (U, u_0) \\ & \searrow^{f} & \downarrow{\scriptstyle \psi} \\ & & (V, v_0) \end{array}$$

and let the following ones be the natural maps defined above

$$\psi_* : \pi_1(U, u_0) \hookrightarrow \pi_1(V, v_0)$$

$$F : \pi_1(V, v_0) \to S_{f^{-1}(v_0)}$$

$$\Phi : \pi_1(U, u_0) \to S_{\varphi^{-1}(u_0)}$$

Let $B_{u_0} = \{w \in f^{-1}(v_0) | \varphi(w) = u_0\}$; then for each $\gamma \in \pi_1(U, u_0)$ it follows that:

$$F \circ \psi_*(\gamma)_{|B_{u_0}} = \Phi(\gamma)$$

Proof : By previous corollary the stabilizer of B_{u_0} in $G = \pi_1(V, v_0)$ is equal to $H = \{\psi_*(\gamma) | \gamma \in \pi_1(U, u_0)\}$; so if $\gamma \in \pi_1(U, u_0)$ then $\overline{\gamma} = \psi_*(\gamma) \in H$. Hence $F(\overline{\gamma})$ is a permutation of the set B_{u_0}. The statement says that the action of $F(\overline{\gamma})$ on B_{u_0} is the same of the action of $\Phi(\gamma)$ on the same set.

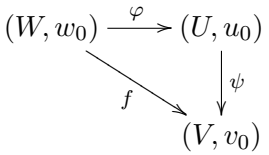
Let z be an element of B_{u_0}

$$\Phi(\gamma)(z) = \widetilde{\gamma}_z(1)$$

$$F(\overline{\gamma})(z) = \widetilde{\overline{\gamma}}_z(1)$$

Since $f = \psi \circ \varphi$ it follows that the lifting $\widetilde{\gamma}_z$ of γ via φ with initial point z coincides with the lifting of $\widetilde{\overline{\gamma}}_z$ of $\overline{\gamma}$ via f with initial point z, so they have the same ending point.□

We end this section with the following diagram of finite coverings (we will have to do with this situation later in the proof of Ritt's theorem):



We set $G = \pi_1(V, v_0)$, $J = \pi_1(U, u_0)$ and $H = \pi_1(W, w_0)$. Then we have $H < J < G$ (viewing all the groups inside the others through monodromy lemma).

The monodromy groups of the three coverings are equal to
$\mathrm{Mon}(f) = G/\mathrm{core}_G(H)$
$\mathrm{Mon}(\varphi) = J/\mathrm{core}_J(H)$
$\mathrm{Mon}(\psi) = G/\mathrm{core}_G(J)$

2.2.1 Ramified coverings

A **ramified covering** is a continuos, open and surjective map $\phi : X \to Y$ between topological spaces such that there exists a discrete subset $\Delta \subset Y$ such that the map

$$\phi_{|X-\phi^{-1}(\Delta)} - \phi^{-1}(\Delta) \to Y - \Delta$$

is a covering. The characteristic subgroup of a ramified covering is the characteristic subgroup of the associated covering. The set Δ is called the ramification points of the ramified covering ϕ.

Examples of ramified covering are holomorphic maps between compact Riemann surfaces.

If $\phi : X \to Y$ a ramified covering we define the monodromy of ϕ in the following way: if $\Delta \subset Y$ is the set of ramification points of ϕ we consider the covering

$$\varphi \doteqdot \phi_{|U} : U \to V$$

where $U \doteqdot X - \phi^{-1}(\Delta)$ and $V \doteqdot Y - \Delta$. We fix a base point v_0 in V and we define the monodromy of ϕ as the monodromy of φ. We will assume that U is connected.

Consider the case of a polynomial

$$F(Z,T) = a_n(Z)T^n + a_{n-1}(Z)T^{n-1} + \ldots + a_1(Z)T + a_0(Z) \in \mathbb{C}[Z,T]$$

which determines the algebraic function T over $\mathbb{C}(Z)$ and let $\overline{\pi} : \overline{\mathcal{C}} \to \mathbb{P}^1(\mathbb{C})$ be the associated ramified covering of compact Riemann surfaces, where $\overline{\mathcal{C}}$ is the compact Riemann surface associated to the polynomial $F(Z,T)$ (roughly is the desingularization of the curve $\{(z,t) \in \mathbb{A}^2 | F(z,t) = 0\}$).

The monodromy is both the action of the fundamental group $G = \pi_1(\mathbb{P}^1(\mathbb{C}) - \Delta, z_0)$ on the fiber of z_0 of the covering $\overline{\pi} : \overline{\mathcal{C}} - \overline{\pi}^{-1}(\Delta) \to \mathbb{P}^1(\mathbb{C}) - \Delta$ where Δ is the finite

set of ramification points of $\overline{\pi}$, and also the action of G on the set of the n branches of the algebraic function T in a neighbourhood of z_0. The group G is known to be finitely generated; we fix a system of generators in this way: let $k = \#\Delta$ and for each $z_i \in \Delta$ let σ_i be a closed path based on z_0 which turns around z_i and no other $z_j \in \Delta - \{z_i\}$, without intersecting the other paths σ_j.

The following propositions describes the fundamental group of a the Riemann sphere with a finite number of holes (see [44]):

Proposition 2.2.9 *If Δ is a finite subset of $\mathbb{P}^1(\mathbb{C})$ and $z_0 \in \mathbb{P}^1(\mathbb{C}) - \Delta$ then the fundamental group $\pi_1(\mathbb{P}^1(\mathbb{C}) - \Delta, z_0)$ is generated by the paths $\sigma_1, \ldots, \sigma_k$ defined above with the only relation $\prod_{i=1,\ldots,k} \sigma_i = 1$.*

Proposition 2.2.10 *Let $F(Z,T) \in \mathbb{C}[Z,T]$ be a polynomial of degree n in T and $\overline{\pi} : \overline{\mathcal{C}} \to \mathbb{P}^1(\mathbb{C})$ be the associated covering of compact Riemann surfaces; if $z_0 \in \mathbb{P}^1(\mathbb{C}) - \Delta$ is a fixed point, we consider $\Phi : \pi_1(\mathbb{P}^1(\mathbb{C}) - \Delta, z_0) \to S_n$ the monodromy of the covering $\overline{\pi}$. Let $\overline{z} \in \Delta$ and $\pi^{-1}(\overline{z}) = \{p_1, \ldots, p_s\}$, where $s < n$ and let m_i be the ramification index $mult_{p_i}(\overline{\pi})$ of $\overline{\pi}$ in p_i, for $i = 1, \ldots, s$.*

If $\sigma_{\overline{z}}$ is a generator of the fundamental group $\pi_1(\mathbb{P}^1(\mathbb{C}) - \Delta, z_0)$ which turns around $\overline{z}$ then

$$\Phi(\sigma_{\overline{z}}) = (t_1, \ldots, t_{m_1}) \ldots (t_{n-m_s}, \ldots, t_n)$$

that is the permutazion associated to $\sigma_{\overline{z}}$ of the branches of algebraic function of F defined locally in z_0 decompones in s cycles, each of them of lenght m_i.

Lemma 2.2.11 *If $F : X \to Z$, $\Phi : X \to Y$ and $\Psi : Y \to Z$ are ramified coverings between compact Riemann surfaces such that $F = \Psi \circ \Phi$ then $\Delta_F = \Delta_\Psi \cup \Psi(\Delta_\Phi)$*

Proof : Since

$$F^{-1}(z_0) = \Phi^{-1}(\Psi^{-1}(z_0)) = \bigcup_{y \in \Psi^{-1}(z_0)} \Phi^{-1}(y)$$

it follows that

$$\#F^{-1}(z_0) = \sum_{y \in \Psi^{-1}(z_0)} \#\Phi^{-1}(y)$$

¿From this equality we can easily deduce the statement of the lemma. □.

If $f \in \mathbb{C}(Z)$ we denote with Φ_f the monodromy associated to the ramified covering

$$\begin{array}{rccc} f: & \mathbb{P}^1(\mathbb{C})_x & \to & \mathbb{P}^1(\mathbb{C})_t \\ & x & \mapsto & t = f(x) \end{array}$$

and with $\mathrm{Mon}(f)$ the monodromy group of the covering. We will prove that if we pass to the extension of algebraic function fields $\mathcal{M}(\mathbb{P}^1(\mathbb{C})_t) \subset \mathcal{M}(\mathbb{P}^1(\mathbb{C})_x)$ that is $\mathbb{C}(t) \subset \mathbb{C}(x)$

which has degree equal to $\deg(f)$ as we have already seen, its Galois closure has Galois group isomorphic to $\mathrm{Mon}(f)$.

2.2.2 Galois coverings

If $\varphi : (U, u_0) \to (V, v_0)$ is a covering, besides the transitive action of the fundamental group $\pi_1(V, v_0)$ on the fiber $\varphi^{-1}(v_0)$, we also have the action of the group $\mathrm{Deck}(\varphi)$ of automorphisms of the covering on the same set, since every automorphism preserves the fibers; such two group actions commute, that is

$$g(\gamma(u)) = \gamma(g(u))$$

for each $g \in \mathrm{Deck}(\varphi)$, $\gamma \in \pi_1(V, v_0)$ and $u \in \varphi^{-1}(v_0)$ (see [44]).

The action of $\mathrm{Deck}(\varphi)$ is free, that is the stabilizers of the points of the fiber are trivial (this follows from the uniqueness of liftings).

The following proposition shows the relation between the group of automorphisms of a covering and the characteristic group of the covering (see [19] and [30]).

Proposition 2.2.12 *If $\varphi : (U, u_0) \to (V, v_0)$ is a covering and $\mathrm{Deck}(\varphi)$ is the group of automorphisms, then $\mathrm{Deck}(\varphi)$ is isomorphic to $N_G(H)/H$, where $G = \pi_1(V, v_0)$, H is the characteristic subgroup and $N_G(H)$ is the normalizer of H in G.*

A covering $\varphi : (U, u_0) \to (V, v_0)$ is called a **Galois covering** if the group $\mathrm{Deck}(\varphi)$ acts transitively on the fibers of the covering; in this case it is immediate to prove that the cardinality of $\mathrm{Deck}(\varphi)$ is equal to the cardinality of the fiber $\varphi^{-1}(v_0)$ since the action is free. The following lemma characterizes Galois coverings in terms of the characteristic subgroup.

Lemma 2.2.13 *Let $\varphi : (U, u_0) \to (V, v_0)$ be a covering; then φ is a Galois covering if and only if the characteristic subgroup $H \cong \pi_1(U, u_0)$ is normal in $G = \pi_1(V, v_0)$. In this case the group of the automorphisms $\mathrm{Deck}(\varphi)$ is isomorphic both to the quotient group G/H and to the monodromy group of the covering.*

Proof : If $H \lhd G$ then by previous propositon $\mathrm{Deck}(\varphi)$ acts transitively on the fibers, since G acts transitively on fibers.

Conversely, if φ is a Galois covering, since $\mathrm{Deck}(\varphi)$ acts freely we have that its order is equal to the degree n of the covering. But $n = \#G/\#H$ and $\#\mathrm{Deck}(\varphi) = \#N_G(H)/\#H$; it follows that $\#G = \#N_G(H)$, so H is normal in G.

The last statement follows both from previous proposition and from lemma 2.2.5. □

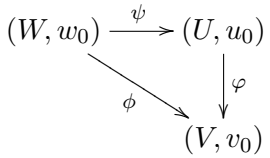
So characteristic subgroups of Galois coverings are equal to the kernel of the monodromy homomorphism; we remind that in general the equality of lemma 2.2.5 holds.

We note that if $\varphi : (U, u_0) \to (V, v_0)$ is a Galois covering then $V \cong U/\mathrm{Deck}(\varphi)$, where $\mathrm{Deck}(\varphi)$ is the group of automorphisms of the covering (see [19]).

Definition 2.2.14 *Let $\varphi : (U, u_0) \to (V, v_0)$ be a finite covering. The* ***Galois closure*** *of φ is defined as the Galois covering $\psi : (W, w_0) \to (U, u_0)$ with characteristic subgroup $K = \ker(\Phi) \lhd \pi_1(U, u_0)$, where Φ is the monodromy homomorphism of φ.*

Note that $\phi = \psi \circ \varphi : (W, w_0) \to (V, v_0)$ is a Galois covering since its characteristic subgroup K is normal in $\pi_1(V, v_0)$. Observe also that $\mathrm{Mon}(\varphi)$ is equal to $\mathrm{Mon}(\phi)$ and that this group acts transitively and faithfully on the set $\varphi^{-1}(v_0)$ and it acts transitively and freely on the set $\phi^{-1}(v_0)$.

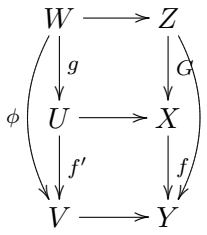
We have the following commutative diagram



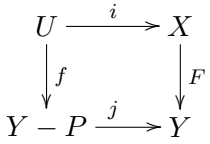
We can also define the Galois closure of φ as the Galois covering $\phi : (W', w_0') \to (V, v_0)$ with characteristic subgroup $K = \ker(\Phi)$. Let H be the characteristic subgroup of φ (isomorphic to the fundamental group of (U, u_0)) and let G be the fundamental group of (V, v_0); since $K < H < G$ then $(W', w_0') \cong (W, w_0)$ because they are coverings of (V, v_0) (via ϕ and $\varphi \circ \psi$ respectively) with the same characteristic subgroup (see proposition 2.2.1).

Moreover the monodromy group of φ, $\mathrm{Mon}(\varphi)$, is isomorphic to the group of automorphisms of the covering $\phi = \varphi \circ \psi$.

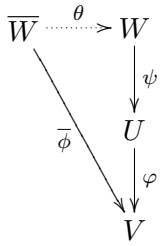
In the case of a finite ramified covering $f : X \to Y$ of compact Riemann surfaces in order to define the Galois closure we consider first the finite covering $f' : U \to V$ obtained by removing the ramification values and their fibres as already seen; then we consider the Galois closure of f', that is $g : W \to U$. By the following proposition (see [28]) there exists a compact Riemann surface Z such that $W \to Z$ is an embedding with $Z - W$ finite and there exists a ramified covering $G : Z \to X$ that extends the covering g ($G_{|W} = g$), that is the following diagram is commutative (we omit the base points)



Proposition 2.2.15 *Let Y be a compact Riemann surface and $P \subset Y$ be a finite set. If $f : U \to Y - P$ is a finite covering then there exists a compact Riemann surface X, a biholomorphic inclusion $i : U \to X$ and a holomorphic map $F : X \to Y$ (that is a finite ramified covering) such that $F \circ i = j \circ f$, where $j : Y - P \hookrightarrow Y$ is the natural inclusion.*



Lemma 2.2.16 *Let $\varphi : U \to V$ a covering with characteristic subgroup H and $\psi : W \to U$ its Galois closure. If $\overline{\phi} : \overline{W} \to V$ is a Galois covering such that its characteristic subgroup is contained in H, then there exists a covering $\theta : \overline{W} \to W$ such that $\overline{\phi} = \varphi \circ \psi \circ \theta$.*



Proof : The statement follows from the fact that $K = \ker(\Phi)$ is the maximum subgroup of H which is normal in $\pi_1(V)$. □

Theorem 2.2.17 *Let $f(T) \in \mathbb{C}(T)$ be a rational function.*

Let K be the Galois closure of the finite algebraic extension of fields $\mathbb{C}(Z) \subset \mathbb{C}(T)$, where $Z = f(T)$ and let G be the Galois group of the extension $K/\mathbb{C}(Z)$.

Let $\mathcal{G}$ be the group of automorphisms of the Galois closure of the finite covering determined by the rational function f

$$f : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$$

$$t \mapsto x = f(t)$$

.

Then G is isomorphic to $\mathcal{G}$. In particular we have that $L^{\mathcal{G}} = \mathbb{C}(f)$.

Proof : The group $\mathcal{G}$ is isomorphic to the monodromy group of f, as we have already observed.

We have the following extension of fields

$$\mathbb{C}(Z) \subset \mathbb{C}(T) \subset K$$

We also have the following coverings of compact Riemann surfaces

$$\mathbb{P}^1(\mathbb{C})_z \leftarrow \mathbb{P}^1(\mathbb{C})_t \leftarrow \overline{\mathcal{C}}$$

where $\overline{\mathcal{C}}$ is the compact Riemann surface (unique up to biolomorphisms) which is the Galois closure of $\mathbb{P}^1(\mathbb{C})_t \to \mathbb{P}^1(\mathbb{C})_z$.

Obviously we have that $\mathcal{M}(\mathbb{P}^1(\mathbb{C})_z) = \mathbb{C}(Z)$ and $\mathcal{M}(\mathbb{P}^1(\mathbb{C})_t) = \mathbb{C}(T)$.

We want to show that the field $K' = \mathcal{M}(\overline{\mathcal{C}})$ of the meromorphic functions of $\overline{\mathcal{C}}$ is isomorphic to the field K. In fact let $\widetilde{C}$ be the compact Riemann surface associated to the algebraic function field K; we have the following maps

$$\widetilde{C} \to \mathbb{P}^1(\mathbb{C})_t \to \mathbb{P}^1(\mathbb{C})_z$$

such that $\widetilde{C} \to \mathbb{P}^1(\mathbb{C})_z$ is a Galois covering (see [44], theorems 5.9 and 5.12) and the kernel of its monodromy homomorphism is contained in the characteristic subgroup of the covering $\mathbb{P}^1(\mathbb{C})_t \to \mathbb{P}^1(\mathbb{C})_z$; by proposition 2.2.16 we have the following maps

$$\widetilde{C} \to \overline{\mathcal{C}} \to \mathbb{P}^1(\mathbb{C})_t \to \mathbb{P}^1(\mathbb{C})_z$$

and the following inclusion of fields

$$\mathbb{C}(Z) \subset \mathbb{C}(T) \subset K' \subset K$$

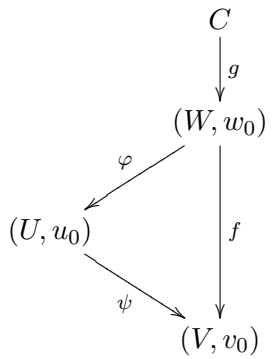
since $K'/\mathbb{C}(Z)$ is a Galois extension (see [44]) it follows that $K = K'$ (K is the splitting field of $f(T) - Z$ over $\mathbb{C}(Z)$ and K' contains a root of this polynomial, since it contains $\mathbb{C}(T)$). Hence $\widetilde{C} = \overline{\mathcal{C}}$.

We define the following map between $\mathcal{G}$ and G

$$\begin{array}{rccl} \Psi: & \mathcal{G} & \to & G \\ & \phi & \mapsto & \Psi(\phi) \doteq \{\lambda \mapsto \lambda \circ \phi^{-1}\} \end{array}$$

By theorem 5.9 of [44] (which uses a non-trivial result like Riemann's existence theorem) it is an isomorphism of groups. □

Corollary 2.2.18 *Let $f \in \mathbb{C}(T)$ be a rational function such that $f = \psi \circ \varphi$, where $\psi, \varphi \in \mathbb{C}(T)$. We have the following diagram of finite coverings (once removed ramification points):*



where $g : C \to (W, w_0)$ *is the Galois closure of* $f : (W, w_0) \to (V, v_0)$. *Set* $G = \pi_1(V, v_0)$, $J = \pi_1(U, u_0)$, $H = \pi_1(W, w_0)$ *and* $K = \pi_1(C, c_0)$.

Then $\mathrm{Deck}(g) \cong H/K$ *and* $\mathrm{Deck}(\varphi \circ g) \cong J/K$.

Proof : The proof follows immediately from the fact that $g : (C, c_0) \to (W, w_0)$ and $\varphi \circ g : (C, c_0) \to (U, u_0)$ are Galois covering, since $K \lhd H$ and $K \lhd J$ (remember that K is normal in G). We conclude by applying lemma 2.2.13. □.

In the proof of Ritt's theorem we will pass from the algebraic point of view (the extension of algebraic function fields $\mathbb{C}(Z) \subset \mathbb{C}(T) \subset L$) to the topological point of view (the finite ramified coverings $\overline{C} \to \mathbb{P}^1(\mathbb{C})_t \to \mathbb{P}^1(\mathbb{C})_z$) without problems.

2.3 Blocks

Let G be a group acting on a finite set Ω: a **block** or G-**block** is a subset B of Ω such that for all $g \in G$ we have either $g(B) = B$ or $g(B) \cap B = \emptyset$. The sets Ω, $\emptyset$, $\{\alpha\}$, where $\alpha \in \Omega$, are examples of blocks; these are called trivial blocks.

The group G is called **primitive** if there are no non-trivial blocks; otherwise it is called **imprimitive**. If G is imprimitive then the set $\Omega_B = \{g(B) | g \in G\}$ is called fundamental system of blocks, where G acts transitively as a permutation group; we denote G_B the subgroup of G which stabilizes B, that is the set of $g \in G$ such that $g(B) = B$. If B is a block then the set $\{G_{B_i} | B_i \in \Omega_B\}$ is a conjugacy class of subgroups of G.

The intersection of two G-blocks is a G-block. If G acts transitively on Ω then the union of blocks of a fundamental system of blocks is equal to Ω, hence in this case $\#B$ divides $\#\Omega$.

We remind that the action of a group is free if all the stabilizers are trivial, and it is faithful if $g(\alpha) = \alpha$ for all $\alpha \in \Omega$ implies that $g = Id$.

If B is a G-block and $\alpha \in B$ then $G_\alpha \subset G_B$, where G_α is the stabilizer of α.

The following lemma describes the structure of blocks in the particular case of a cyclic group of order n acting on a finite set of order n.

Lemma 2.3.1 *Let* G *be a cyclic group of order* n *which acts transitively over a finite set* Ω *of* n *elements. Then for each divisor* d *of* n *there exists exactly one fundamental system of blocks* Ω_B *of* Ω, *whose blocks have cardinality* d *and* $\#G_B = d$. *Moreover if* $d_1 | d_2 | n$ *then* $B_{d_1} \subset B_{d_2}$ *and*

$$B_{d_2} = \bigcup_{g \in G_{B_{d_2}}} g(B_{d_1}) = \bigcup_{g \in G_{B_{d_2}}/G_{B_{d_1}}} g(B_{d_1})$$

Proof : Observe that the action is free since G and Ω have the same cardinality.

The set $\Omega = \{x_0, \ldots, x_{n-1}\}$ is in bijection with $G =< g >= \{1, g, \ldots, g^{n-1}\}$ via the map $\Psi : G \to \Omega$, $g^i \mapsto g^i(x_0) = x_i$. So if $n = dk$ and $H_d =< g^k >$ is the subgroup of G of cardinality d then the set $\Psi(H_d) = \{x_0, x_k, \ldots, x_{(d-1)k}\} = B_d$ is a block of d elements whose stabilizer G_{B_d} is H_d; the conjugates of B_d under the action of G form a fundamental system of blocks whose elements have cardinality d.

The second statement follows both from the structure of subgroups of a cyclic group and from the fact that $G_{B_{d_1}} \subset G_{B_{d_2}}$ if $d_1 | d_2 | n$. □

Proposition 2.3.2 *Let G be a group acting transitively on a finite set Ω*

$$\begin{array}{rccc} \Phi : & G & \to & \mathcal{S}_\Omega \\ & g & \mapsto & \{x \mapsto g(x)\} \end{array}$$

where $\mathcal{S}_\Omega$ is the permutation group of Ω. Then $\ker(\Phi) = \mathrm{core}_G(H)$, where $H = St_G(x_0)$ is the stabilizer of an element $x_0 \in \Omega$ in G ; moreover $\mathcal{G} = G/\ker(\Phi)$ is a group which acts faithfully and transitively on Ω.

If $\mathcal{B}$ is a fundamental system of G-blocks then G acts transitively on $\mathcal{B}$:

$$\begin{array}{rccc} \Phi_B : & G & \to & \mathcal{S}_\mathcal{B} \\ & g & \mapsto & \{B \mapsto g(B)\} \end{array}$$

and $\ker(\Phi_B) = \mathrm{core}_G(K)$, where $K = St_G(B)$ is the stabilizer of a block $B \in \mathcal{B}$ in G. The group $\mathcal{G}_\mathcal{B} = G/\ker(\Phi_B)$ acts transitively and faithfully on $\mathcal{B}$; without loss of generality we may suppose that $x_0 \in B$ and so $H \subset K$.

The kernel of the natural projection

$$\pi : \mathcal{G} \to \mathcal{G}_\mathcal{B}$$

is equal to $\mathrm{core}_\mathcal{G}(\mathcal{K})$, where $\mathcal{K}$ is the image of K in $\mathcal{G}$, thus $St_\mathcal{G}(B)$, the stabilizer of B in $\mathcal{G}$.

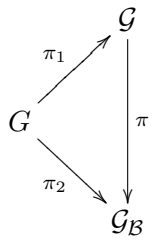
Proof : Since G acts transitively then the set of stabilizers $\mathcal{S} = \{St_G(x) | x \in \Omega\}$ is a conjugacy class of subgroups of G, which means it is equal to $\{gHg^{-1} | g \in G\}$, where $H = St_G(x_0)$ for some $x_0 \in \Omega$. The kernel of Φ is the subgroup

$$\{g \in G |\ g(x) = x\ \forall\ x \in \Omega\} = \bigcap_{x \in \Omega} St_G(x) = \mathrm{core}_G(H)$$

Observe that $\mathcal{B}$ is also a fundamental system of blocks for the group $\mathcal{G}$.

In the same way we have $\ker(\Phi_B) = \mathrm{core}_G(K)$. It is clear that the action of the groups $\mathcal{G}$ and $\mathcal{G}_\mathcal{B}$ over Ω and Ω_B respectively is faithful and transitive.

For the last statement we proceed as follows: since $\ker(\Phi) \subset \ker(\Phi_B)$ we have the following diagram of group homomorphisms



where π_1 and π_2 are the canonical quotient maps, with $\ker(\pi_1) = \mathrm{core}_G(H)$ and $\ker(\pi_2) = \mathrm{core}_G(K)$. The map π is canonically defined as $\pi(\overline{g}) = \pi_2(g)$ for $\overline{g} = \pi_1(g) \in \mathcal{G}$, such that $\pi \circ \pi_1 = \pi_2$.

We have

$$\begin{aligned}\ker(\pi) &= \{\overline{g} \in \mathcal{G} \mid \pi(\overline{g}) = 0\} \\ &= \{\pi_1(g) \in \mathcal{G} \mid \pi_2(g) = 0\} \\ &= \{\pi_1(g) \in \mathcal{G} \mid g \in \ker(\pi_2)\} \\ &= \pi_1(\mathrm{core}_G(K))\end{aligned}$$

Since $\mathrm{core}_G(K) = \bigcap_{g\in G} gKg^{-1}$ then $\pi_1(\mathrm{core}_G(K)) = \bigcap_{\overline{g}\in\mathcal{G}} \overline{g}\pi_1(K)\overline{g}^{-1}$ (if $p : G \to G/H$ is a group homomorphism and $H < A, B < G$ are subgroups, then $p(A \cap B) = p(A) \cap p(B)$).

Hence $\ker(\pi) = \pi_1(\mathrm{core}_G(K)) = \mathrm{core}_{\pi_1(G)}(\pi_1(K))$. □

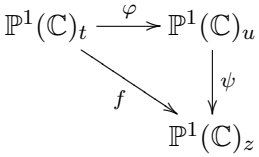
A first remarkable result is the following criterion which relates decomposability of rational functions and their monodromy groups:

Theorem 2.3.3 *Let $f \in \mathbb{C}(T)$ be a rational function of degree $N > 1$. Then f is indecomposable if and only if* $\mathrm{Mon}(f)$ *is primitive.*

Proof : We prove that f is decomposable if and only if the group $\mathcal{G} = \mathrm{Mon}(f)$ is imprimitive; we remind that $\mathrm{Mon}(f)$ acts over the set of the N roots of $F(T, Z)$ over $\mathbb{C}(Z)$, where $F(T, Z) \doteqdot f(T) - Z$ if f is a polynomial or $F(T, Z) \doteqdot f_1(T) - Zf_2(T)$ if $f = f_1/f_2$ is a rational function.

Note that this action is transitive because F is irreducible over $\mathbb{C}(Z)$ and $\mathrm{Mon}(f)$ is isomorphic to the Galois group of F over $\mathbb{C}(Z)$.

Suppose that $f = \psi \circ \varphi$, where ψ, φ are rational functions such that $\deg(\psi) = m > 1$ and $\deg(\varphi) = n > 1$; we have the following holomorphic maps



(the letters mark the variable of the "differents" $\mathbb{P}^1(\mathbb{C})$).

Let $z_0 \in \mathbb{P}^1(\mathbb{C})$ be a regular value of f (that is $\#f^{-1}(z_0) = \deg(f)$) and consider the sets $B_{u_i} = \{t \in f^{-1}(z_0) | \varphi(t) = u_i\}$, where $\{u_i\}_{i=1,\dots,m} = \psi^{-1}(z_0)$; by corollary 2.2.7 the sets B_{u_i}, for $u_i \in \psi^{-1}(z_0)$, form a fundamental system of blocks for the group $G = \pi_1(\mathbb{P}^1(\mathbb{C}) - \Delta)$, hence by proposition 2.3.2 they form a fundamental system of blocks for the group $G/(\ker(F)) = \mathrm{Mon}(f)$ (where F is the usual monodromy homomorphism of f). The cardinality of each block B_{u_i} is $\deg(\varphi)$ and there are $\deg(\psi)$ of them. So the group $\mathcal{G}$ acts imprimitively on the set $f^{-1}(z_0)$.

Suppose now that $\mathcal{G}$ acts imprimitively: we want to show that f is decomposable in a non-trivial way. Let z_0 be a regular value of f and $\{t_1, \dots, t_N\}$ be the fiber of z_0.

If $B_1 = \{t_1, \dots, t_n\}$ is a non-trivial $\mathcal{G}$-block ($1 < n < N$), consider the fundamental system of blocks $\mathcal{B} = \{B_i = g(B_i) | g \in \mathcal{G}\}$; trivially this is also a fundamental system of blocks for the group G, since $\mathcal{G} = G/\ker(\Phi)$ and $\ker(\Phi)$ is the kernel of the action of G on $f^{-1}(z_0)$ (see proposition 2.3.2).

By proposition 2.3.2 the group G acts transitively on the set $\mathcal{B}$ so by theorem 2.2.3 there exists a covering $\psi : U \to \mathbb{P}^1(\mathbb{C}) - \Delta$ with characteristic subgroup G_{B_1}, which has index $m = N/n$ in G so the covering ψ has degree m.

$$\begin{array}{ccc} (\mathbb{P}^1(\mathbb{C}) - f^{-1}(\Delta), t_1) & & (U, u_0) \\ & \searrow^{f} & \downarrow \psi \\ & & (\mathbb{P}^1(\mathbb{C}) - \Delta, z_0) \end{array}$$

If $H = G_{t_1}$ is the stabilizer of the element $t_1 \in f^{-1}(z_0)$ then $H < G_{B_1} \cong \pi_1(U, u_0)$, since $H = G_{t_1}$ is the stabilizer in G of $t_1 \in B_1$, which is a block; so by theorem 2.2.2 there exists a covering $\varphi : (W, w_0) \to (U, u_0)$ of degree $n = [G_{B_1} : H]$ with characteristic subgroup H. By proposition 2.2.1 the topological space W is isomorphic to $\mathbb{P}^1(\mathbb{C})_t - f^{-1}(\Delta)$ since their coverings over U have the same characteristic subgroup H; so without loss of generality we may assume that $W = \mathbb{P}^1(\mathbb{C})_t - f^{-1}(\Delta)$. The situation is the following

$$\begin{array}{ccc} (\mathbb{P}^1(\mathbb{C}) - f^{-1}(\Delta), t_1) & \xrightarrow{\varphi} & (U, u_0) \\ & \searrow^{f} & \downarrow \psi \\ & & (\mathbb{P}^1(\mathbb{C}) - \Delta, z_0) \end{array}$$

By an argument similar to proposition 2.2.15 we can "compactify" all the Riemann surfaces to obtain finite ramified coverings of compact Riemann surfaces

$$\begin{array}{ccc} (\mathbb{P}^1(\mathbb{C}), t_1) & \xrightarrow{\varphi} & (C, u_0) \\ & \searrow^{f} & \downarrow \psi \\ & & (\mathbb{P}^1(\mathbb{C}), z_0) \end{array}$$

where C is a compact Riemann surface. By Riemann-Hurwitz theorem (for example) we have $C \cong \mathbb{P}^1(\mathbb{C})$ and so φ and ψ are rational functions.

Finally we have

$$f(t) = z = \psi(u) = \psi(\varphi(t))$$

So the function f is decomposable. □

¿From previous theorem we deduce the following important corollary.

Corollary 2.3.4 *Let $f \in \mathbb{C}(T)$ be a rational function of degree N and let $z_0 \in \mathbb{P}^1(\mathbb{C})$ be a regular value of the covering map $\mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$, $z \mapsto f(z)$. Then there is a bijection from the set of right components of decomposition of f modulo equivalence and the set of fundamental system of blocks of* $\mathrm{Mon}(f)$ *(which act over $f^{-1}(z_0)$), that is:*

$$\{\varphi | f = \psi \circ \varphi\}/\sim \leftrightarrow \{\mathcal{B} = \{B_1, \ldots, B_m\} \text{ fundamental system of blocks for } \mathrm{Mon}(f)\}$$

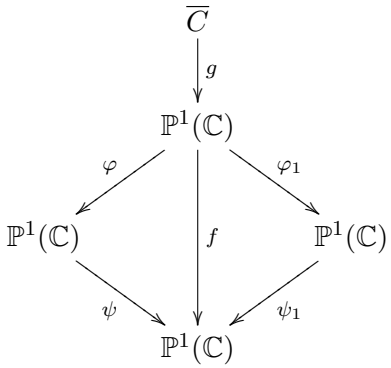
The degree of φ corresponds to the cardinality of the corresponding block B. Moreover φ is indecomposable if and only if the associated block B_φ cannot be decomposed in smaller blocks.

Proof : Let $f = \psi \circ \varphi$ and z_0 be a regular value of f ; for each $u \in \psi^{-1}(z_0)$, we set $B_u = \{t_1, \ldots, t_n \in f^{-1}(v_0) |\ \varphi(t_i) = u\}$. We have already seen that B_u is a $\mathrm{Mon}(f)$-block and the set $\mathcal{B} = \{B_u | u \in \psi^{-1}(z_0)\}$ is a fundamental system of blocks for $\mathrm{Mon}(f)$ (see corollary 2.2.7).

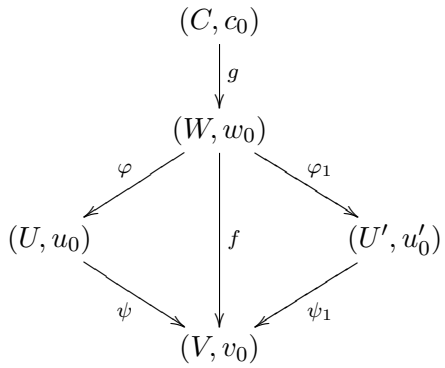
¿From the proof of the previous theorem we see that the map from the set of right components of f to the set of fundamental system of blocks of $\mathrm{Mon}(f)$, which sends φ to $\mathcal{B}_\varphi$, is surjective.

We need only to prove that this map is injective, that is if $f = \psi \circ \varphi = \psi_1 \circ \varphi_1$ such that $\mathcal{B} = \mathcal{B}_\varphi = \mathcal{B}_\varphi$ then $\varphi = \mu \circ \varphi_1$, for some linear rational function μ. Observe that in particular we have $\deg(\varphi) = \deg(\varphi_1) = \#B$, where $B \in \mathcal{B}$, and $\deg(\psi) = \deg(\psi_1) = \#\mathcal{B}$.

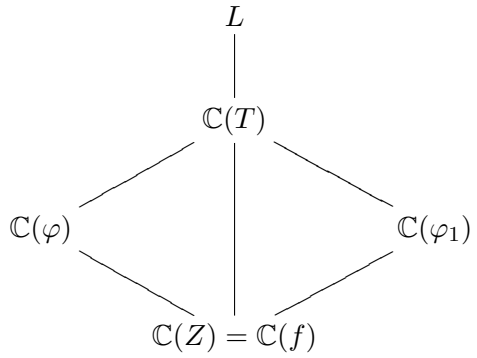
We have the following diagram of ramified coverings



where $\overline{C}$ is the Galois closure of $f : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$,
In terms of unramified coverings we have



This become the following diagram of inclusion of fields (see theorem 2.2.17)



By corollary 2.2.18 we have $\mathrm{Mon}(\varphi \circ g) \cong J/K$ and $\mathrm{Mon}(\varphi_1 \circ g) \cong J_1/K$, where $J = \pi_1(U, u_0)$, $J_1 = \pi_1(U', u_0')$ and $K = \pi_1(C, c_0) = \ker(\Phi)$, where Φ is the monodromy homomorphisms associated to f.

Observe now that by corollary 2.2.7 we have

$$J \cong G_{B_{u_0}}$$

and similarly

$$J_1 \cong G_{B_{u_0'}}$$

But since B_{u_0} and $B_{u_0'}$ belong to the same fundamental system of blocks $\mathcal{B}$ then $G_{B_{u_0}}$ is conjugate to $G_{B_{u_0'}}$. Along with theorem 2.2.17 this implies that $\mathbb{C}(\varphi) \cong \mathbb{C}(\varphi_1)$, so φ is a linear rational function of φ_1. $\square$

2.4 First theorem of Ritt

By lemma 2.1.6 a decomposition of a polynomial F in rational functions is equivalent to a decomposition in polynomials. This result is based on the fact that the map $F : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ is totally ramified over ∞, in fact $F^{-1}(\infty) = \{\infty\}$; we get the same result if F is totally ramified over a generic point of $\mathbb{P}^1(\mathbb{C})$. Ritt's results on decomposition of polynomials are based on this simple observation.

Theorem 2.4.1 *Let $f \in \mathbb{C}[T]$ be of degree n. Then for each divisor d of n there exists at most one block of the monodromy group* $\mathrm{Mon}(f)$ *of cardinality d.*

Proof : By proposition 2.2.10 the permutation σ_∞ associated to the path $\gamma_\infty \in \pi_1(\mathbb{P}^1(\mathbb{C}) - \Delta, z_0)$ which turns around to ∞ is a n-cycle, since ∞ is a totally ramified point of the covering $f : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$; let us suppose that $\sigma_\infty = (1, \ldots, n)$ (by numbering the roots of $f(T) - Z$ over $\mathbb{C}(Z)$ in a suitable way).

Let H_∞ be the cyclic subgroup of $G = \mathrm{Mon}(f)$ generated by σ_∞; a G-block is also a H_∞-block, so by lemma 2.3.1 a G-block of cardinality d ($n = dk$) has the form

$$B = \{1, k+1, \ldots, (d-1)k+1\}$$

and this proves the theorem. □

¿From this result and from corollary 2.3.4 it follows that if $F \in \mathbb{C}[T]$ of degree N then for each divisor d of N there exists at most one field K of degree d over $\mathbb{C}(F)$ such that $\mathbb{C}(F) \subset K \subset \mathbb{C}(T)$.

¿From now on, if $f \in \mathbb{C}[T]$, we denote H_∞ the cyclic subgroup of $G = \mathrm{Mon}(f)$ generated by the permutation $\sigma_\infty = (1, \ldots, n)$. Obviously this subgroup acts transitively on the set of roots of $f(T) - Z \in \mathbb{C}(Z)[T]$.

The following theorem (reformulation of lemma 2.1.9) tell us something more of the previous theorem.

Theorem 2.4.2 *Let $f \in \mathbb{C}[T]$ and let $\varphi, \psi \in \mathbb{C}[T]$ be indecomposable of degree n and m respectively such that $f = \phi \circ \varphi = \sigma \circ \psi$, for some $\phi, \sigma \in \mathbb{C}[T]$. Then either $n = m$ or $(n, m) = 1$.*

Proof : Let N be the degree of f.

It follows immediately from the previous theorem that the first case holds if and only if φ and ψ are linearly equivalent (in fact if $n = m$ then by corollary 2.3.4 we have $\#\mathcal{B}_\varphi = \#\mathcal{B}_\psi$ and so by the previous theorem these fundamental system of blocks are the same).

Suppose that $n \neq m$ and let $\delta \doteqdot (n, m) > 1$; let $N = nk = mh$. Let $\mathcal{B} = \mathcal{B}_\varphi$ be the fundamental system of k blocks determined by φ:

$$B_1 = \{1, k+1, \ldots, (n-1)k+1\}, \ldots, B_k = \{k, 2k, \ldots, nk\}$$

and let $\mathcal{C} = \mathcal{B}_\psi$ be the fundamental system of h blocks determined by ψ:

$$C_1 = \{1, h+1, \ldots, (m-1)h+1\}, \ldots, C_h = \{h, 2h, \ldots, mh\}$$

By lemma 2.3.1 there exists a fundamental system of blocks $D_1, \ldots, D_{N/\delta}$ of $H_\infty =< \sigma_\infty >$, each of them of δ elements.

Since B_1 is a G-block then it is also a H_∞-block; by lemma 2.3.1 it follows that $D_1 \subset B_1$. For the same reason $D_1 \subset C_1$.

Since the intersection of two G-blocks is a G-block then $B_1 \cap C_1$ is a G-block, which is non-trivial because it contains D_1 which has cardinality $\delta > 1$. Then by corollary 2.3.4 the polynomials φ and ψ would be decomposable, contrary to our assumption. □

¿From this theorem it follows that if f is a polynomial such that $f = \phi \circ \varphi = \sigma \circ \psi$, where φ and ψ are indecomposable of different degree (hence coprime degree), each block of $\mathcal{B}_\varphi$ has only one element in common with each block of $\mathcal{B}_\psi$, that is for each $B \in \mathcal{B}_\varphi$ and for each $C \in \mathcal{B}_\psi$ we have $\#(B \cap C) = 1$.

We can now prove the first theorem of Ritt by induction on the degree of polynomial f. Up to degree 6 the theorem is true; we suppose the theorem for those polynomials f with $\deg(f) < N$, $N > 6$, and we prove it for those of degree N.

Let

$$f(X) = f_1 \circ \ldots \circ f_r(X)$$

$$f(X) = g_1 \circ \ldots \circ g_s(X)$$

be two maximal decomposition of a polynomial f of degree N; if $\deg(f_r) = \deg(g_s)$ then the two polynomials f_r and g_s determine the same fundamental system of blocks, so $\mathbb{C}(f_r) = \mathbb{C}(g_s)$. By induction it follows that $r - 1 = s - 1$ and the degrees of the components of the two decompositions are the same up to the order.

If $\deg(f_r) = n \neq \deg(g_s) = m$ then $(n, m) = 1$ by previous theorem; then N is divisible by nm and there exists a fundamental system of blocks $D_1, \ldots, D_{N/nm}$ of H_∞, each of them of cardinality nm.

Lemma 2.4.3 *The H_∞-block D_1 is a G-block.*

Proof : We keep the notation of theorem 2.4.2.

For what we saw before D_1 contains B_1; moreover it follows from lemma 2.3.1 that

$$D_1 = \bigcup_{g \in H_{D_1}/H_{B_1}} g(B_1)$$

where H_{D_1} and H_{B_1} are the stabilizers of D_1 and B_1 respectively in H_∞ (that is the intersections of G_{D_1} and G_{B_1} respectively with H_∞).

In the same way we have

$$D_1 = \bigcup_{g \in H_{D_1}/H_{C_1}} g(C_1)$$

Then D_1 is both the union of m blocks of $\mathcal{B}$ and the union of n blocks of $\mathcal{C}$:

$$D_1 = \bigcup_{i \in I} B_i = \bigcup_{j \in J} C_j$$

where $\#I = m$ and $\#J = n$.

¿From this identity and the fact that two blocks of $\mathcal{B}$ and $\mathcal{C}$ can have at most one element in common (see previous theorem: g_s and f_r are indecomposable) it follows that for each $i \in I$ and $j \in J$ we have $\#(B_i \cap C_j) = 1$.

Set $K \doteqdot \{g \in G | g(1) \in D_1\}$. We have the following lemma.

Lemma 2.4.4 *For each $g \in K$ we have $g(D_1) = D_1$.*

Proof : Let $g \in K$ and let B_t be a block of $\mathcal{B}$ such that $g(1) \in B_t \subset D_1$. Then $g(B_1) = B_t$.

We have the following equalities

$$B_1 = \bigcup_{j \in J} B_1 \cap C_j,\ B_t = \bigcup_{j \in J} B_t \cap C_j$$

$$g(B_1) = \bigcup_{j \in J} g(B_1 \cap C_j) = \bigcup_{j \in J} g(B_1) \cap g(C_j) = \bigcup_{j \in J} B_t \cap g(C_j)$$

$$\Rightarrow g(\{C_j | j \in J\}) = \{C_j | j \in J\} \Rightarrow g(D_1) = D_1$$

which proves the lemma. □

In particular from this lemma it follows that K is a group, and it is equal to the stabilizer of D_1 in G: $K = \{g \in G | g(D_1) = D_1\}$.

Let $g \in G$ be such that $g(D_1) \cap D_1 \neq \emptyset$: then there exist $i, k \in I$ such that $g(B_i) = B_k$.

$$B_i = \bigcup_{j \in J} B_i \cap C_j,\ B_k = \bigcup_{j \in J} B_k \cap C_j$$

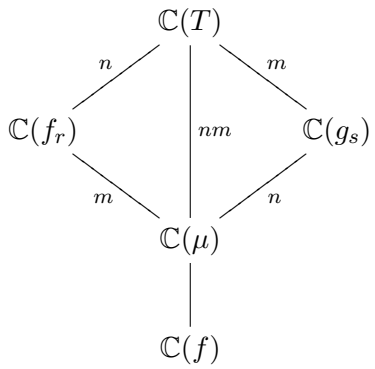
$$g(B_i) = \bigcup_{j \in J} g(B_i \cap C_j) = \bigcup_{j \in J} g(B_i) \cap g(C_j) = \bigcup_{j \in J} B_k \cap g(C_j)$$

$$\Rightarrow g(\{C_j | j \in J\}) = \{C_j | j \in J\} \Rightarrow g(D_1) = D_1$$

Hence D_1 is a G-block of cardinality nm. Lemma 2.4.3 is now proved. □

Since D_1 is a G-block of cardinality nm it follows by corollary 2.3.4 that there exists a polynomial $\mu \in \mathbb{C}[T]$ of degree nm such that $f = \sigma\mu$. Moreover we have $\mu = \gamma f_r$ and $\mu = \eta g_s$, since D_1 is both union of blocks of $\mathcal{B}$ and union of blocks of $\mathcal{C}$.

We summarize the situation in the following diagram:



where $(n, m) = 1$.
So

$$f = f_1 \circ \ldots \circ f_r = \sigma \circ \gamma \circ f_r = \sigma \circ \eta \circ g_s = g_1 \circ \ldots \circ g_s$$

the following lemma concludes the proof of the theorem.

Lemma 2.4.5 *The polynomials γ and η are indecomposables.*

Proof : Like before we keep the notation of theorem 2.4.2.
If $\gamma = \gamma_1 \circ \gamma_2$ with $1 < m_2 = \deg(\gamma_2) < m$ then $f = \sigma \circ \mu = \sigma \circ \gamma \circ f_r = \sigma \circ \gamma_1 \circ (\gamma_2 \circ f_r)$; by corollary 2.3.4 there exists a G-block E_1 of cardinality nm_2 such that $B_1 \subset E_1 \subset D_1$. By lemma 2.3.1 we also have that (we recall that every G-block is also a H_∞-block)

$$E_1 = \bigcup B_i$$

Given a block C_j of $\mathcal{C}$ we have that

$$E_1 \cap C_j = \bigcup B_i \cap C_j$$

and so the G-block $E_1 \cap C_j$ has cardinality $m_2 > 1$; then g_s would be decomposable, contradiction.
In the same way η is indecomposable.□

By lemma 2.1.7 we have $f_1 \circ \ldots \circ f_{r-1} = \sigma \circ \gamma$, so since this is a polynomial of degree less than N, by induction we have that the number of indecomposable components of σ is $r - 2$. For the same reason $g_1 \circ \ldots \circ g_{s-1} = \sigma \circ \eta$, so the number of indecomposable components of σ is $s - 2$. So $r - 2 = s - 2$ and the degrees of the components of the two decompositions are the same up to the order. □

If we have two maximal decompositions of a polynomial

$$f = f_1 \circ \ldots \circ f_r = g_1 \circ \ldots \circ g_r$$

is possible to pass from one to another through a finite number of steps:

- there exists i such that

$$f_1 \circ \ldots \circ f_i \circ f_{i+1} \ldots \circ f_r = f_1 \circ \ldots (f_i \circ \lambda) \circ (\lambda^{-1} f_{i+1}) \ldots \circ f_r$$

- there exists i such that $f_i \circ f_{i+1} = g_i \circ g_{i+1}$ where $\deg(f_i) = \deg(g_{i+1})$ and $\deg(f_{i+1}) = \deg(g_i)$ such that

$$f_1 \circ \ldots f_{i-1} \circ (f_i \circ f_{i+1}) \circ f_{i+2} \ldots \circ f_r = f_1 \circ \ldots f_{i-1} \circ (g_i \circ g_{i+1}) \circ f_{i+2} \ldots \circ f_r$$

  in this last case we have to apply Ritt's second theorem.

Chapter 3

Plane algebraic curves

3.1 Affine curves

We adopt the definition of plane algebraic curve we are going to give; our base field is a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. For a more general definition of algebraic curve (algebraic affine or projective variety of dimension one over an algebraically closed field) see other books like Shafarevich ([42]) or Hartshorne ([17]).

Definition 3.1.1 *A **plane affine algebraic curve** (from now on simply* curve*) is a subset C of the affine plane $\mathbb{A}^2(\overline{\mathbb{Q}})$ defined as the zero-locus of a non-zero polynomial in two variables $f \in \overline{\mathbb{Q}}[X,Y]$, that is:*

$$C = C_f = \{(x,y) \in \mathbb{A}^2(\overline{\mathbb{Q}}) | f(x,y) = 0\}$$

*The couples $(x,y) \in C$ are called **points** of the curve.*

*Let K be a number field. A curve C is **defined over** K if the polynomial defining the curve is in $K[X,Y]$. We indicate a curve C defined over a number field K as C/K. The points of C with coordinates in K are called K-rational points (or simply rational if $K = \mathbb{Q}$). We call $C(K)$ the set of K-rational points.*

*A curve C_f defined over K is **irreducible** (resp. **absolutely irreducible**) if $f(X,Y)$ is irreducible in the ring of polynomials $K[X,Y]$ (resp. irreducible in $\overline{\mathbb{Q}}[X,Y]$).*

*If C/K is a curve, we define the **coordinate ring** of C as:*

$$K[C] \doteqdot \frac{K[X,Y]}{I(C/K)}$$

where $I(C/K) = \{f \in K[X,Y] | f_{|C} \equiv 0\}$: we identify polynomials which coincide over C; observe that $K[C]$ is an integral domain if and only if $I(C/K) = (f)$ is a prime ideal, which corresponds to the fact that f is irreducible in $K[X,Y]$. In similar way we define $\overline{\mathbb{Q}}[C]$.

*In the case of an irreducible (resp. absolutely irreducible) curve, the field of quotients of $K[C]$ (resp. of $\overline{\mathbb{Q}}[C]$) is denoted by $K(C)$ (resp. $\overline{\mathbb{Q}}(C)$) and it is called the **field of rational functions** of the curve C with coefficients in K (resp. in $\overline{\mathbb{Q}}$).*

Note that the elements of $\overline{\mathbb{Q}}[C]$ induce well-defined functions on C with values in $\overline{\mathbb{Q}}$ which are called regular functions of the curve; the elements of the field $\overline{\mathbb{Q}}(C)$ define functions on C which are regular over an open set (in the sense of Zariski topology, see [42]). We obviously have that $K[C] = K[x, y]$ where x and y are the class modulo the ideal $I(C/K)$ of the coordinates X and Y, considered as regular functions on the curve.

The following classical theorem (see [42]) shows in effect that the ideal of an irreducible curve is generated by the polynomial f which defines the curve itself. If f is not irreducible it is generated by the radical of the ideal generated by the polynomial f.

Proposition 3.1.2 *Let k be a field and let $f \in k[X, Y]$ be an irreducible polynomial. If $g \in k[X, Y]$ is not divisible by f then the sistem of equation $f(x, y) = g(x, y) = 0$ has only a finite number of solutions.*

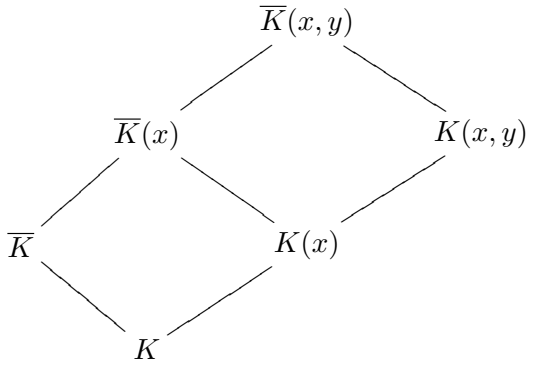
Lemma 3.1.3 *An irreducible curve C defined over a number field K is absolutely irreducible if and only if the field K is algebraically closed in the field $K(C)$ of rational functions of the curve C with coefficients in K, that is $K(C) \cap \overline{K} = K$, where $\overline{K}$ is a fixed algebraic closure of the field K.*

Proof : Let $C = C_f$, where $f \in K[X, Y]$ is irreducible and let $K(C) = K(x, y)$.
If $f(X, Y)$ is absolutely irreducible let $\overline{K}(C) = \overline{K}(x, y)$. It follows that

$$[K(C) : K(x)] = [\overline{K}(C) : \overline{K}(x)]$$

By corollary 9.2 of [14] it follows that $K(C)$ and $\overline{K}(x)$ are linearly disjoint over $K(x)$. Since $\overline{K}$ and $K(x)$ are linearly disjoint over K it follows that $\overline{K}$ and $K(C)$ are linearly disjoint over K which in particular implies that $K(C) \cap \overline{K} = K$.

Conversely if K is algebraically closed in $K(C)$ then $\overline{K}$ and $K(C)$ are linearly disjoint over K (see theorem 2 pg. 56 Lang, [27]) and therefore for the tower property ([26], Prop.1 pg. 50) it follows that $\overline{K}(x)$ and $K(C)$ are linearly disjoint over $K(x)$ and for the previously mentioned corollary of [14] we have that $[K(C) : K(x)] = [\overline{K}(C) : \overline{K}(x)]$, which implies that $f(X, Y)$ is irreducible in $\overline{\mathbb{Q}}[X, Y]$. The following diagram summarizes the situation:



□

Every algebraic curve is defined over a number field: take the finite extension of $\mathbb{Q}$ generated by the coefficients of the polynomial $f(X,Y) \in \overline{\mathbb{Q}}[X,Y]$ which defines the curve.

Observe also that a curve C can be defined over a number field K but its set of K-rational points can be empty, see for example the curve defined by the absolutely irreducible polynomial $f(X,Y) = X^2 + Y^2 + 1$ which has no rational points.

The set $C(\overline{\mathbb{Q}})$ is always infinite (see [20]).

Definition 3.1.4 *A point $p \in C_f$ is **non-singular** if at least one of the two derivatives of f in p is non-zero. A curve C is non-singular if all of its points are non-singular.*

The following proposition holds (see [42], chap. 2, §. 5) :

Proposition 3.1.5 *An absolutely irreducible curve C is non singular if and only if its coordinate ring $\overline{\mathbb{Q}}[C]$ is integrally closed.*

If an absolutely irreducible curve C/K is non singular then also $K[C]$ is integrally closed.

An absolutely irreducible curve C is a **rational curve** (also said of genus zero since the desingularization of C is a compact Riemann surface of genus zero) if its points can be parametrized by rational functions of a parameter t, that is there exist two rational functions $\varphi, \psi \in \overline{\mathbb{Q}}(t)$ such that for almost every points $p = (x,y)$ of the curve (except a finite number of points) there exists $\overline{t} \in \overline{\mathbb{Q}}$ such that $(x,y) = (\varphi(\overline{t}), \psi(\overline{t}))$.

The parametrization (φ, ψ) is **proper** if for almost every point $p = (x,y)$ of the curve there exists exactly one $\overline{t} \in \mathbb{Q}$ such that $(x,y) = (\varphi(\overline{t}), \psi(\overline{t}))$; observe that a parametrization is proper if and only if the couple of rational functions of the parametrization is minimal (see paragraph 1.2). By Lüroth's theorem every rational curve admits a proper parametrization.

If the components of the parametrization φ, ψ can be chosen in $\overline{\mathbb{Q}}[t]$ then we say that the curve is polynomially parametrized or the curve is polynomial. The polynomial version of Lüroth's theorem (see theorem 1.1.4) shows that if a rational curve admits a polynomial parametrization then it admits a proper polynomial parametrization.

3.2 Projective curves

Let $\mathbb{P}^2(\overline{\mathbb{Q}}) \doteqdot (\overline{\mathbb{Q}}^3 - \{(0,0,0)\})/\sim$ be the projective plane over $\overline{\mathbb{Q}}$ with usual equivalence relation: given $x = (x_0, x_1, x_2)$ and $y = (y_0, y_1, y_2)$ in $\overline{\mathbb{Q}}^3 - \{(0,0,0)\}$ we define $x \sim y$ if and only if there exists $\lambda \in \overline{\mathbb{Q}}^*$ such that $\lambda x = y$. We denote $x = (x_0 : x_1 : x_2)$ the equivalence class of $x = (x_0, x_1, x_2)$ and $\mathbb{P}^2$ the projective plane $\mathbb{P}^2(\overline{\mathbb{Q}})$. We remind that $\mathbb{P}^2$ can be covered by subsets which are copies of $\mathbb{A}^2$, for example $U_i \doteqdot \{(x_0 : x_1 : x_2) |\ x_i \neq 0\}$, for $i = 0, 1, 2$; in particular $\mathbb{A}^2$ is a subset of $\mathbb{P}^2$, through the map $(x : y) \mapsto (x : y : 1)$ (if $i = 1$; likewise if $i = 2$ or 3); the image points of $\mathbb{A}^2$ through this

map are called finite points of $\mathbb{P}^2$ and the points $(x_0 : x_1 : 0)$ are called points at infinity of $\mathbb{P}^2$.

Definition 3.2.1 *A **plane projective curve** $\overline{C}$ is a subset of the projective plane $\mathbb{P}^2$ defined as the zero-locus of a non-zero homogeneous polynomial $\overline{f} \in \overline{\mathbb{Q}}[X, Y, Z]$:*

$$\overline{C} = \overline{C}_{\overline{f}} = \{(x : y : z) \in \mathbb{P}^2 |\ \overline{f}(x : y : z) = 0\}$$

In the same way of affine curves we define points of projective cruves, projective curves defined over a number field and (absolutely) irreducible projective curves.

Every affine curve can be considered as a subset of a projective curve by homogenizing the polynomial which defines the curve. If $C_f \subset \mathbb{A}^2$ is an affine curve, we define its **projective closure** as the projective curve $\overline{C}_{\overline{f}}$ given by the homogeneous polynomial $\overline{f}$ associated to f:

$$\overline{f}(X, Y, Z) \doteq Z^{\deg(f)} f(X/Z, Y/Z)$$

Conversely if $\overline{C}_{\overline{f}} \subset \mathbb{P}^2$ is a projective curve we define its dehomogeneization with respect to Z as the curve $C_f \subset \mathbb{A}^2$ given as the zero-locus of the polynomial $f(X, Y) = \overline{f}(X, Y, 1)$ (this in the case when Z does not divide $\overline{f}$). From a geometric point of view, the projective curve $\overline{C}_{\overline{f}}$ is the topological closure of C_f in $\mathbb{P}^2$ with respect to the Zariski topology (if we see $C_f \subset \mathbb{A}^2$ in $\mathbb{P}^2$ through the immersion $\mathbb{A}^2 \hookrightarrow \mathbb{P}^2$ defined above; see [42]).

If C is a curve we call points at infinity of C the elements of $\overline{C} - C$: they correspond to the points of $\mathbb{P}^1$ which satisfies $f_d(X_0, X_1) = 0$, where f_d is the homogeneous part of highest degree of the polynomial f which defines the curve C. So the number of points at infinity of an affine curve are equal to the number of irreducible distinct factor of the homogeneous component of f of highest degree. Obviously we have $C = \overline{C} \cap \mathbb{A}^2$.

A point $p \in \overline{C}$ is non singular if there exists $i \in \{1, 2, 3\}$ such that $p \in U_i$ and p is non singular for the affine curve $U_i \cap \overline{C}$.

We have to pay more attention to the definition of rational function field of a irreducible projective curve $\overline{C}$. Let $f, g \in \overline{\mathbb{Q}}[X, Y, Z]$ be two homogeneous polynomials of the same degree such that $g \notin I(\overline{C})$: then f/g is a well-defined function in the points of $\overline{C}$ where $g \neq 0$. The set of all these functions is a ring $O_{\overline{C}}$; the quotient of $O_{\overline{C}}$ for the maximal ideal $M_{\overline{C}}$ of the funtions $f/g \in O_{\overline{C}}$ such that $f \in I(\overline{C})$ is the field $\overline{\mathbb{Q}}(\overline{C})$ of rational functions of $\overline{C}$ (we identify two rational functions f/g and f'/g' if $g'f - gf' \in I(\overline{C})$).

¿From now on we assume that our curves, affine or projective, are absolutely irreducible.

3.3 Rational maps between curves

Now we define map between curves; first we treat the case of affine curves, then the case of projective curves.

- Affine case

Definition 3.3.1 *Let C_1 and C_2 be curves. A rational map from C_1 to C_2 is a map*

$$\phi : C_1 \to C_2$$

such that there exist $\phi_1, \phi_2 \in \overline{\mathbb{Q}}(C_1)$ such that for each $p \in C_1$ where ϕ_1, ϕ_2 are both defined we have $\phi(p) = (\phi_1(p), \phi_2(p)) \in C_2$.

If K is a number field and C_1, C_2 are defined over K, the map ϕ is defined over K if $\phi_1, \phi_2 \in K(C_1)$.

A rational map $\phi : C_1 \to C_2$ between two curves is defined over an open set of C_1 (with respect to the Zariski topology of $\mathbb{A}^2(\mathbb{Q})$), that is in the points of C_1 where ϕ_1 and ϕ_2 are defined. If ϕ is defined over a number field K then it restricts to a map from the K-rational points of C_1 to the K-rational points of C_2, that is $\phi : C_1(K) \to C_2(K)$.

- Projective case

Definition 3.3.2 *Let $\overline{C}_1$ and $\overline{C}_2$ be projective curves. A rational map from $\overline{C}_1$ to $\overline{C}_2$ is a map*

$$\overline{\phi} : \overline{C}_2 \to \overline{C}_2$$

of the form $\overline{\phi} = [\varphi_1 : \varphi_2 : \varphi_3]$ where $\varphi_i \in \mathbb{Q}(\overline{C}_1)$ for $i = 1, 2, 3$ and for each $P \in C_1$ where $\{\varphi_i\}$ are defined we have $\overline{\phi}(P) = [\varphi_1(P) : \varphi_2(P) : \varphi_3(P)] \in \overline{C}_2$.

If K is a number field and $\overline{C}_1, \overline{C}_2$ are defined over K, the map $\overline{\phi}$ is defined over K if there exists $\lambda \in \overline{\mathbb{Q}}$ such that $\lambda\varphi_1, \lambda\varphi_2, \lambda\varphi_3 \in K(\overline{C}_1)$ (note that $\overline{\phi} = [\lambda\varphi_1 : \lambda\varphi_2 : \lambda\varphi_3]$).

If $\overline{\phi} = [\varphi_1 : \varphi_2 : \varphi_3]$ is a rational map between two projective curves with $\varphi_i = \phi_i/\psi_i \in \overline{\mathbb{Q}}(\overline{C}_1)$ and ϕ_i, ψ_i are homgeneous polynomials of the same degree n_i, we consider the homogeneous polynomial $\psi = mcm\{\psi_i\}$ and we multiply the three rational functions φ_i by ψ. We obtain the following expression for ϕ

$$\phi = [f_1 : f_2 : f_3]$$

where f_i are homogeneous polynomial of the same degree. If there is some common factor between the f_i we can divide by it in order to suppose that the f_i's are coprime.

Let $\phi : C_1 \to C_2$ be a rational map between two irreducible affine curves, where $C_i = \{(x, y) \in \mathbb{A}^2 | f_i(x, y) = 0\}$; suppose also that the projective closure of C_1 is non-singular. We want to show that ϕ can be extended to a rational map $\overline{\phi} : \overline{C}_1 \to \overline{C}_2$ between the projective closure of C_1 and C_2 respectively.

First of all if such an extension exists then it is unique by lemma 4.1, chap. 1 of [17], since by 3.3.6 the map $\overline{\phi}$ is regular.

If $\phi = (\phi_1, \phi_2)$, where $\phi_i \in \overline{\mathbb{Q}}(C_1)$ is equal to φ_i/ψ_i, we set

$$\overline{\phi}_i(X,Y,Z) = (\varphi_i(X/Z, Y/Z)Z^{\deg(\phi_i)})/(\psi_i(X/Z, Y/Z)Z^{\deg(\phi_i)}) = \overline{\varphi}_i(X,Y,Z)/\overline{\psi}_i(X,Y,Z)$$

This rational function is a ratio of two homogeneous polynomials of the same degree $deg(\phi_i)$. We then define the map $\overline{\phi}$

$$\overline{\phi} = [\overline{\phi}_1 : \overline{\phi}_2 : 1] = [\overline{\phi}'_1 : \overline{\phi}'_2 : \overline{\psi}]$$

where $\overline{\psi} = mcm\{\overline{\psi}_1, \overline{\psi}_2\}$ and $\overline{\phi}'_1, \overline{\phi}'_2, \overline{\psi}$ are homogeneous polynomials of the same degree. Since

$$f_2\left(\frac{\varphi_1}{\psi_1}, \frac{\varphi_2}{\psi_2}\right) = 0$$

we have that

$$F_2(\overline{\phi}'_1, \overline{\phi}'_2, \overline{\psi}) = 0$$

If $D \subset C_1$ is the domain of definition of ϕ (the complementary of the set of zero of ψ_1 and ψ_2 in C_1) then it is immediate to see that for each $(x,y) \in D$ we have $\phi(x,y) = \overline{\phi}(x : y : 1)$.

If (x,y) is a pole either of ϕ_1 or of ϕ_2 then

$$\overline{\phi}(x : y : 1) = [\overline{\phi}'_1(x : y : 1) : \overline{\phi}'_2(x : y : 1) : 0] \in \overline{C}_2 - C_2$$

so the points where ϕ is not defined are sent through $\overline{\phi}$ to the points at infinity of C_2, that is the set $\overline{C}_2 - C_2$.

$$\begin{array}{ccc} C_1 & \hookrightarrow & \overline{C}_1 \\ \downarrow & & \downarrow \\ C_2 & \hookrightarrow & \overline{C}_2 \end{array}$$

It can happen that a point of $\overline{C}_1 - C_1$ is sent through $\overline{\phi}$ to a point of C_2. Take for example the map $\phi : \mathbb{A}^1 \to C$, where $C = \{(x,y) | x^2 + y^2 = 1\}$, given by

$$t \mapsto \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right)$$

The corresponding map $\overline{\phi} : \mathbb{P}^1 \to \overline{C} = \{(x : y : z) | x^2 + y^2 = z^2\}$ is given by

$$(t : s) \mapsto (2ts : t^2 - s^2 : t^2 + s^2)$$

We have $\overline{\phi}(1,0) = (0 : 1 : 1)$.

Proposition 3.3.3 *A regular map between two curves $\phi : C_1 \to C_2$ is constant or surjective.*

Proof : The proof follows from the fact that ϕ is a finite map since C_1 and C_2 are algebraic varieties of dimension 1 (see Shafarevich, [42], chap.1 §5.3). □

Proposition 3.3.4 *Let C_1/K and C_2/K be curves and let $\phi : C_1 \to C_2$ be a rational map defined over K, such that $\phi(C_1)$ is dense in C_2 (we call such a map dominant). Then the map*

$$\phi^* : K(C_2) \to K(C_1)$$

$\varphi \mapsto \varphi \circ \phi$ is well defined and $K(C_2) \subset K(C_1)$ is a finite extension of fields.

Proof : The map $\phi^* : K(C_2) \to K(C_1)$, $\varphi \mapsto \varphi \circ \phi$, is well defined since $\varphi_{|C_2} = 0$ implies $\varphi \circ \phi_{|C_1} = 0$. It is also injective: if $f \in K[C_2]$ such that $\phi^*(f) = 0$ it follows that $f_{|\phi(C_1)} = 0$, so $\phi(C_1) \subset \{f(p) = 0\}$ which means $C_2 = \overline{\phi(C_1)} \subset \{f(p) = 0\}$.

This map extends in a natural way to a map $\phi^* : K(C_2) \to K(C_1)$ which is an inclusion of field; this extension is finite since $K(C_2)$ and $K(C_1)$ have trascendence degree 1 over K. □

Definition 3.3.5 *If $\phi : C_1 \to C_2$ is a dominant rational map defined over a number field K between two curves $C_1/K, C_2/K$, then the degree of the map ϕ is defined as the degree of the extension of fields $K(C_2) \subset K(C_1)$.*

Proposition 3.3.6 *Let $\phi : C_1 \to C_2$ be a rational map between two projective curves; if $p \in C_1$ is a non-singular point then ϕ is defined in p.*

For a proof of this simple fact, which uses only that O_p, the local ring of C_1 at p, is a discrete valuation ring, see Proposition 2.1 of [41].

Definition 3.3.7 *A non-constant rational map $\phi : C_1 \to C_2$, where C_1, C_2 are curves, is called **birational** if there exists a rational map $\psi : C_2 \to C_1$ sich that $\psi \circ \phi = Id_{C_1}$ e $\phi \circ \psi = Id_{C_2}$ (on the open set where this functions are defined).*

We can say that a rational curve is a curve which is birational to $\mathbb{A}_1$ (or to $\mathbb{P}^1$, if the curve is projective).

In general a curve C is birational to a curve C' if and only if their rational function fields are isomorphic. More precisely there is an equivalence between the category of absolutely irreducible curve defined over a number field K with morphisms given by dominant rational map defined over K which are not constant and the category of algebraic function fields in one variable $\mathbb{K}/K$ with $\mathbb{K} \cap \overline{\mathbb{Q}} = K$ and morphisms given by inclusion of fields which leaves K fixed; this functor associates to a curve C/K the field $K(C)$ and to a dominant rational map $\phi : C_1 \to C_2$ defined over K the inclusion of fields $\phi^* : K(C_2) \to K(C_1)$, which restricted to K is the identity.

3.4 Geometric points and places

Now we show that geometric points of a non-singular curve correspond bijectively to valuation rings of the field $\overline{\mathbb{Q}}(C)$ which contain the base field $\overline{\mathbb{Q}}$; the latter are usually called places of the curve.

Lemma 3.4.1 *Let C be an absolutely irreducible, non-singular curve defined over a number field K and let p be a point of C; let $\mathcal{O}_{p,K} = \{f \in K(C) | f$ is defined in $p\}$ the local ring of C in p with coefficients in K and $\mathcal{M}_{p,K} = \{f \in \mathcal{O}_{p,K} | f(p) = 0\}$ its maximal ideal.*

If $p = (a, b)$ then the residue field $K(p) \doteqdot \mathcal{O}_{p,K}/\mathcal{M}_{p,K}$ is equal to $K(a, b)$ and so it is a finite extension of K.

Proof : Since $K \cap \mathcal{M}_{p,K} = \{0\}$ then $K \subset K(p)$. Consider the projection map $\pi : \mathcal{O}_{p,K} \to \mathcal{O}_{p,K}/\mathcal{M}_{p,K}$; the image set of π is equal to $\{f(\overline{x}, \overline{y}) | f \in \mathcal{O}_{p,K}\}$, where $\overline{x} = \pi(x)$ and $\overline{y} = \pi(y)$ (x and y are elements of $\mathcal{O}_{p,K}$).

Take now the minimal polynomials $g(T)$ and $h(T)$ over K of a and b respectively; the non-zero regular functions $g(x)$ and $h(y)$ are obviously contained $\mathcal{M}_{p,K}$, so their images $g(\overline{x})$ and $h(\overline{y})$ are zero in $K(p)$. Hence $\overline{x}$ and $\overline{y}$ are algebraic over K and they satisfy the same minimal polynomial of a and b respectively over K. So the field $K(p)$ is isomorphic to the finite algebraic extension $K(a, b)$. □

A simple consequence of this lemma is the fact that a point p of a curve C/K is defined over K (that is an elements of $C(K)$) if and only if its residue field is equal to K. The residue field $K(p)$ is also called the field of definition of the point p.

Proposition 3.4.2 *Let $\overline{C}$ be a non-singular, projective and absolutely irreducible curve. Then the points of the curve are in bijection with the valuation rings of the field $\overline{\mathbb{Q}}(\overline{C})$ which contains the base field $\overline{\mathbb{Q}}$.*

Moreover if C is defined over a number field K, its rational points $C(K)$ are in bijection with the valuation rings of $K(C)$ whose residue field is isomorphic to K.

Proof : Let p be a point of C, an affine model of $\overline{C}$. We associate to p the local ring of C in p, that is $O_p = \{f \in \overline{\mathbb{Q}}(C) | f$ is regular in $p\}$, which is the localized of $\overline{\mathbb{Q}}[C]$ at the maximal ideal of the regular functions of $\overline{\mathbb{Q}}[C]$ which are zero in p. It is a discrete valuation ring since the curve has dimension one and p is non singular (see Shafarevich, [42]). This map is injective since there is a bijection between the points of C and maximal ideals of $\overline{\mathbb{Q}}[C]$ (by Hilbert's Nullstellensatz theorem).

Conversely let O be a valuation ring of $\overline{\mathbb{Q}}(C) = \overline{\mathbb{Q}}(x, y)$ which contains $\overline{\mathbb{Q}}(x)$; then $A = O \cap \overline{\mathbb{Q}}(x)$ is a valuation ring of $\overline{\mathbb{Q}}(x)$ which contains x and it corresponds to an element $x_0 \in \overline{\mathbb{Q}}$ (see proposition 1.3.4). Hence $x - x_0$ is a generator for the maximal ideal $P = P_{x_0}$ of $A = A_{x_0}$; since by lemma 1.3.5 we can assume that y is integral over $\overline{\mathbb{Q}}[x]$ then $y \in O$ by proposition 1.3.6. So there exists $y_0 \in \overline{\mathbb{Q}}$ such that $y - y_0 \in M$, the

maximal ideal of O; then the relation $f(x,y) = 0$ in $\overline{\mathbb{Q}}(C)$ implies $f(x_0, y_0) = 0$ in $\overline{\mathbb{Q}}$, and so $p_0 = (x_0, y_0) \in C_f$ is the associated point of the valuation ring O.

The point p_0 is unique, since it is uniquely determined by the maximal ideal $M \cap \overline{\mathbb{Q}}[x,y]$.

If $x \notin O$ then it is easy to observe that there exists another affine model C' of $\overline{C}$ such that $\overline{\mathbb{Q}}[C'] = \overline{\mathbb{Q}}[x', y'] \subset O$. □

Let C be an algebraic curve; if $\mathcal{S}$ is the set of valuation rings of $\overline{\mathbb{Q}}(C)$ then we can give a topology to $\mathcal{S}$ in order to obtain a compact Riemann surfaces which is the desingularization of the curve C: there exists a holomorphic map $\pi : \mathcal{S} \to C$ such that $\pi_{|\mathcal{S}-\pi^{-1}(\Delta)} : \mathcal{S} - \pi^{-1}(\Delta) \to C - \Delta$ is biholomorphic, where Δ is the set of singular points of C.

For more references see chapter 2 of [26] and also [7].

3.5 Parametrization with rational coefficients

If a rational curve is defined over a number field K it is not true in general that it admits a parametrization with coefficients in the field K; for example the curve $f(X,Y) = X^2 + Y^2 + 1$ which is rational but $C_f(\mathbb{Q}) = \emptyset$.

If the curve is non-singular and the set of rational points is not empty then there exists a parametrization with rational coefficients, as the following proposition shows.

Proposition 3.5.1 *Let C be a non-singular rational curve, defined over $\mathbb{Q}$ and absolutely irreducible. If C has at least one rational point, then there exists a parametrization of C which is defined over $\mathbb{Q}$, that is a couple of rational functions (φ, ψ) with coefficients in $\mathbb{Q}$ such that $f(\varphi(t), \psi(t)) = 0$.*

Proof : Let $p \in C(\mathbb{Q})$ and consider the set

$$L(p) = \{\varphi \in \overline{\mathbb{Q}}(C) | \varphi \text{ has at most a simple pole in } p\}$$

This is a vector space over $\overline{\mathbb{Q}}$ and since the curve is rational then by Riemann-Roch theorem the space $L(p)$ has dimension 2 over $\overline{\mathbb{Q}}$ (see [18]). Its elements are the constants and functions which have a simple pole in p ; the latter correspond to rational maps from C to $\mathbb{A}_1(\overline{\mathbb{Q}})$ of degree 1.

We want to show that there exists a base of $L(p)$ of the form $1, \varphi$, where 1 is the constant function and $\varphi \in \mathbb{Q}(C) - \mathbb{Q}$. First we observe that $L(p)$ is stable under the action of the Galois group $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, since p has coordinate in $\mathbb{Q}$: if $\varphi \in L(p)$ is not constant and $\sigma \in G$ then $\sigma(\varphi)$ has a simple pole in $\varphi(p) = p$.

If $\phi \in L(p)$ then there exists a number field K such that $\phi \in K(C)$; without loss of generality we can suppose that $K/\mathbb{Q}$ is a Galois extension. Let $\alpha_1, \ldots, \alpha_n$ a base of K over $\mathbb{Q}$ and let $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}$; it is well known that the determinant of the matrix $M = (\sigma_i(\alpha_j))_{1 \le i,j \le n}$ is different from zero (see Lang, [24]).

Now we define the following rational functions, for $j = 1, \ldots, n$:

$$g_j \doteqdot \sum_{i=1,\ldots,n} \sigma_i(\alpha_j \phi) = \sum_{i=1,\ldots,n} \sigma_i(\alpha_j)\sigma_i(\phi)$$

It is immediate to verify that $\{g_j\}$ are invariant under the action of $\mathrm{Gal}(K/\mathbb{Q})$, so they belong to the field $\mathbb{Q}(C)$; since the matrix M with coefficients in K is invertible then it is possible to express $\sigma_i(\phi)$ (and in particular ϕ) as a linear combination with coefficients in K of $g_1, \ldots, g_n \in \mathbb{Q}(C)$. Hence every elements of $L(p)$ is a $\overline{\mathbb{Q}}$-linear combination of elements of $\mathbb{Q}(C)$. Let $\varphi \in \mathbb{Q}(C) - \mathbb{Q}$ be such that $1, \varphi$ is a base of $L(p)$ as a $\overline{\mathbb{Q}}$-vector space.

To conclude the proof we observe that the rational function $\varphi \in \mathbb{Q}(C) \subset \overline{\mathbb{Q}}(C)$ determines a rational map from C to $\mathbb{A}_1(\overline{\mathbb{Q}})$ of degree 1 which is defined over $\mathbb{Q}$; this map is an isomorphism since C is non-singular (see 3.3.3). Its inverse $\psi : \mathbb{A}_1(\overline{\mathbb{Q}}) \to C$ is defined over $\mathbb{Q}$ and it has the form $\psi(t) = (\psi_1(t), \psi_2(t))$, $\psi_1, \psi_2 \in \mathbb{Q}(t)$. $\square$

¿From the remarks of the previous paragraphs, in the same hypothesis of the proposition we can find a parametrization $(\varphi(t), \psi(t))$ with rational coefficients which is also proper.

More in general if a rational curve has a rational point which is non singular then it has a parametrization with rational coefficients. Similar arguments if we replace the field $\mathbb{Q}$ with a number field K.

So in effect almost every rational points of the curve can be obtained in terms of a parametrization with rational coefficients by choosing a rational parameter t.

3.6 Standard parametrization of rational curves

An example of rational curve defined over $\mathbb{Q}$ with a parametrization with rational coefficients is given by $f(X, Y) = X^2 + Y^2 - 1$, which is parametrized by the rational functions $(\varphi(t), \psi(t)) = (2t/(t^2+1), (t^2-1)/(t^2+1))$.

This parametrization of the curve C_f has a particular form: each component has the same denominator (that is they have the same set of poles). This can be done in general up to birationality.

Proposition 3.6.1 *Let C be an irreducible curve defined over $\overline{\mathbb{Q}}$; then there exists a model C' birational to C such that if $\overline{\mathbb{Q}}(C') = \overline{\mathbb{Q}}(x', y')$ then x' and y' have the same divisor of poles.*

Proof : The statement means that x' and y' have the same set of poles with the same multiciplicity. Suppose that $\overline{\mathbb{Q}}(C) = \overline{\mathbb{Q}}(x, y)$ and consider the rational linear transformations Φ with coefficients a, b, c, d in $\overline{\mathbb{Q}}$ defined on $\overline{\mathbb{Q}}(C)$:

$$\Phi(x, y) \doteqdot (x', y') = (ax + by, cx + dy)$$

such that $ad - bc \neq 0$ and $abcd \neq 0$; its image is $\overline{\mathbb{Q}}(x', y') = \overline{\mathbb{Q}}(C)$.
This map establishes an isomorphism of field $\overline{\mathbb{Q}}(x, y) \cong \overline{\mathbb{Q}}(x', y')$ which corresponds to a birationality of C with a curve C', whose defining polynomial $f'(X, Y)$ is given by $f'(x', y') = 0$.

We want to show that there exist $a, b, c, d \in \overline{\mathbb{Q}}$ such that the statement of the proposition holds.

We set P_x the support of the divisor of poles of x and P_y the support of the divisor of poles of y; let $P = P_x \cup P_y$ be the set of poles of x or y. Obviously if $p \in (P_x - P_y) \cup (P_y - P_x)$ then p is a pole for x' and y' with the same multiciplicity; if $p \in P_x \cap P_y$ we distinguish two cases:

- $ord_p(x) = ord_p(y) = k$

If t is a local parameter in p we write x and y as Laurent expansion in a neighbourhood of p:

$$x = \frac{a_k}{t^{-k}} + \ldots + a_0 + a_1 t + \ldots$$

$$y = \frac{b_k}{t^{-k}} + \ldots + b_0 + b_1 t + \ldots$$

Then $ord_p(x') = ord_p(ax + by) = k$ provided $(a, b) \notin \{(u, v) | a_k u + b_k v = 0\}$. Same arguments for y'.

- $ord_p(x) \neq ord_p(y)$

In this case $ord_p(x') = ord_p(ax + by) = min\{ord_p(x), ord_p(y)\} = ord_p(cx + dy) = ord_p(y')$.

If we choose the coefficients a, b, c, d of the map Φ outside a finite number of hyperplanes we obtain what we wanted. □

Corollary 3.6.2 *Let C be a rational non-singular curve which is absolutely irreducible. Then there exists a curve C' birational to C such that it admits a parametrization of the following type:*

$$(\varphi(t), \psi(t)) = \left(\frac{\varphi_1(t)}{\phi(t)}, \frac{\psi_1(t)}{\phi(t)} \right)$$

where $\varphi_1, \psi_1, \phi \in \overline{\mathbb{Q}}[t]$.

Proof : Suppose that the curve C is defined over a number field K; by proposition 3.6.1 there exists a model C' of the curve C such that $K(C') = K(x, y)$ and the rational functions x and y of the curve C' have the same divisor of poles.

By hypothesis $K(C')$ is a purely trascendental field over K of degree one; so there exists $t \in K(C')$ such that $K(x, y) = K(t)$ and $x = \varphi(t), y = \psi(t)$, where $\varphi, \psi \in K(T)$.

Since x and y have the same divisor of poles, and these correspond to the poles of the rational functions φ and ψ, we have that

$$\varphi(t) = \frac{\phi_1(t)}{\phi(t)}$$

$$\psi(t) = \frac{\psi_1(t)}{\phi(t)}$$

The corollary is proved. □

3.7 Polynomial parametrization of rational curves

The following theorem (see for example [1]) gives a criterium to determine whether a rational curve C has a polynomial parametrization.

Theorem 3.7.1 *Let $\overline{C}$ be a non-singular rational projective curve and $C = \overline{C} \cap U_3$ be an affine model of the curve. Then C admits a polynomial parametrization if and only if $\overline{C}$ has exactly one point at infinity.*

Proof : Suppose that C has a polynomial parametrization Φ of the following type

$$\Phi : \mathbb{A}^1 \to C$$

$$t \mapsto (\varphi(t), \psi(t))$$

where $\varphi(t), \psi(t) \in \overline{\mathbb{Q}}[t]$; if we compose this map with the canonical inclusion of $\mathbb{A}^2$ in $\mathbb{P}^2$, $(x, y) \mapsto (x : y : 1)$, we obtain the map $t \mapsto (\varphi(t) : \psi(t) : 1)$, from $\mathbb{A}^1$ to $\overline{C}$. By proposition 3.3.3 the map Φ is surjective since Φ is regular on $\mathbb{A}^1$.

$$\begin{array}{ccc} \mathbb{A}^1 & \xrightarrow{\Phi} & C \\ \downarrow & & \downarrow \\ \mathbb{P}^1 & \xrightarrow{\overline{\Phi}} & \overline{C} \end{array}$$

Consider the extension $\overline{\Phi}$ of Φ at $\mathbb{P}^1$ as we saw in section 3.3; by proposition 3.3.6, $\overline{\Phi}$ is regular at $(1 : 0) \in \mathbb{P}^1 - \mathbb{A}^1$ (which is the point at infinity) so $\overline{\Phi}$ is surjective by proposition 3.3.3. This implies that $\overline{C} - C$ has only one point, which is given by $\overline{\Phi}(1 : 0)$.

Conversely suppose that $\overline{C} - C = \{P_0\}$ and let $\Phi(t) = (\varphi(t)/\phi_1(t), \psi(t)/\phi_2(t))$ be a parametrization of C; we have

$$\overline{\Phi}(t : s) = (\varphi'(t, s) : \psi'(t, s) : \phi(t, s))$$

where φ', ψ', ϕ are homogeneous polynomials of the same degree n and $\overline{\Phi} : \mathbb{P}^1 \to \overline{C}$ such that $\overline{\Phi}_{|\mathbb{A}^1} = \Phi$. Since $\mathbb{P}^1$ and $\overline{C}$ are non-singular and the map $\overline{\Phi}$ has degree 1, it is an isomorphism.

We have

$$\overline{\Phi}^{-1}(\overline{C} - C) = \{(t : s) \in \mathbb{P}^1 | \phi(t, s) = 0\}$$

and by the previous remark $\overline{\Phi}^{-1}(\overline{C} - C)$ has only one point in $\mathbb{P}^1$. Hence the polynomial ϕ has the form

$$\phi(t, s) = (\alpha t - \beta s)^n$$

for some $\alpha, \beta \in \overline{\mathbb{Q}}$.

We have

$$\Phi(t) = \overline{\Phi}(t : 1) = (\varphi'(t, 1) : \psi'(t, 1) : (\alpha t - \beta)^n)$$

and if $(t : 1) \neq (\beta/\alpha : 1)$ we have

$$\Phi(t) = \left(\frac{\varphi'(t)}{(\alpha t - \beta)^n}, \frac{\psi'(t)}{(\alpha t - \beta)^n} \right)$$

If we compose the map $\Phi(t)$ with the rational linear function $\lambda(t) = 1/t + \beta/\alpha$ (which is a birationality of $\mathbb{A}^1$ with itself) we obtain a polynomial parametrization $\Phi \circ \lambda(t)$ as wanted. □

In general if C is a rational plane curve (singular or not) we have to check that $\overline{C} - C$ has only one point P_0 and also that the curve is analytically irreducible at P_0 in order to obtain a polynomial parametrization.

If P_0 is non singular then there is only one place at P_0; the converse is not true: take for example the curve $y^2 = x^3$ which is singular at the origin but there is only one place at the origin.

It is useful to rephrase the same result from a completely algebraic point of view. We have the following proposition (see [13]).

Proposition 3.7.2 *Let k be a field and t a trascendental element over k; let z be a rational function in t, that is an element of $k(t)$.*

Then z is a polynomial in t if and only if the valuation ring at infinity $\mathfrak{O}_\infty$ of $k(t)$ is the only valuation ring of $k(t)$ over the valuation ring at infinity $\mathfrak{o}_\infty$ of $k(z)$.

If this happens then $\mathfrak{O}_\infty$ is totally ramified over $\mathfrak{o}_\infty$.

Proof : First we observe that if a valuation ring $\mathfrak{O}$ with maximal ideal $\mathfrak{B}$ of $k(t)$ is above $O_{1/z}$ then $1/z \in P$, since $1/z$ is a local parameter of $\mathfrak{o}_\infty$; this means that $z \notin \mathfrak{O}$. Conversely if a valuation ring $\mathfrak{O}$ of $k(t)$ does not contain z then $\mathfrak{O} \cap k(z) = \mathfrak{o}_\infty$.

Suppose that $\mathfrak{O}_\infty$ is the only valuation ring of $k(t)$ above $\mathfrak{o}_\infty$; the integral closure of $k[t]$ in $k(t)$ (which is equal to $k[t]$ since it is integrally closed) is equal to the intersection of all the valuation rings of $k(t)$ which contain $k[t]$ (see proposition 1.3.6), that is all the valuation rings of $k(t)$ with the only exception of $\mathfrak{O}_\infty$. But z belongs to all of them

because the only valuation ring of $k(t)$ which does not contain z is $\mathfrak{O}_\infty$, by the previous remark.

Conversely let $z = f(t) \in k[t]$; suppose that $\mathfrak{O}_a$ is a valuation ring of $k(t)$ different from $\mathfrak{O}_\infty$ which is above $\mathfrak{o}_\infty$. Then $1/z \in \mathfrak{B}_a$, the maximal ideal of $\mathfrak{O}_a$, so $1/z = (t-a)^n f(t)/g(t)$, with $n \geq 1$ e g, f coprime, $f(a)g(a) \neq 0$; hence $z = 1/(t-a)^n g(t)/f(t)$ which does not belong to $k[t]$, contradiction.

The valuation ring at infinity of $k(t)$ has residue field $\mathfrak{O}_\infty/\mathfrak{B}_\infty = k$; in the same way for the valuation ring at infinity of $k(z)$. Hence if $\mathfrak{O}_\infty$ is the only valuation ring above $\mathfrak{o}_\infty$, it is totally ramified. □

Proposition 3.7.3 *Let $C \subset \mathbb{A}^2$ be a rational irreducible curve. Then C admits a polynomial parametrization if and only if there exists a unique valuation ring O of $\overline{\mathbb{Q}}(C)$ above the valuation ring at infinity of $\overline{\mathbb{Q}}(x)$.*

Proof : As we have already seen we can suppose that y is integral above $\overline{\mathbb{Q}}[x]$, so the set of poles of y is contained in the set of poles of x. By hypothesis there exists $t \in \overline{\mathbb{Q}}$ such that $\overline{\mathbb{Q}}(C) = \overline{\mathbb{Q}}(t)$; then there exists a unique valuation ring O of $\overline{\mathbb{Q}}(C)$ above the valuation ring at infinity of $\overline{\mathbb{Q}}(x)$ if and only if x has a unique pole P_0 on C which is pole also for y (the only rational functions of a curve which does not have poles are the constants).

With same reasonings of theorem 3.7.1 we can compose with an automorphism of $\mathbb{P}^1 \cong \overline{C}$ to bring P_0 at infinity, so x and y are polynomials in a parameter t. □

We can also say that the curve C has only one place at infinity if and only if there is only one place of $\overline{\mathbb{Q}}(C)$ which does not contain the coordinate ring $\overline{\mathbb{Q}}[C]$ of the curve.

Of course if $\overline{C}$ is a rational projective curve, there can be affine models of $\overline{C}$ with a polynomial parametrization and other affine models which do not have a polynomial parametrization. For example the projective curve $\overline{C} = \{(X : Y : Z) \in \mathbb{P}^2 | XY = Z^2\}$ has the affine model $C_z = \{(x, y) \in \mathbb{P}^2 | xy = 1\}$ which does not have a polynomial parametrization; instead the affine model $C_y = \{(x, z) \in \mathbb{P}^2 | x = z^2\}$ has a polynomial parametrization.

Chapter 4

Curves of Schinzel

The problem of this chapter is to characterize pairs (f, S), where $f \in \mathbb{Q}[X, Y]$ is an irreducible polynomial and S is an infinite subset of $\mathbb{Q}$ such that for all x in S there exists y in S such that $f(x, y) = 0$.

We shall see that in the case of rational curves this problem is related to the parametrization of image set of rational functions (or polynomials, if the curve has a polynomial parametrization).

4.1 Introduction

We give the following definition:

Definition 4.1.1 *A polynomial $f(X, Y) \in \mathbb{Q}[X, Y]$ has the **Schinzel's property (SP)** if there exists an infinite subset $S = S_f \subset \mathbb{Q}$ such that for every $x \in S$ the equation $f(x, Y) = 0$ has a solution $y \in S$.*

This lemma is straightforward.

Lemma 4.1.2 *Let $f \in \mathbb{Q}[X, Y]$ and suppose that f is symmetric (that is $f(X, Y) = f(Y, X)$) and $C_f(\mathbb{Q})$ is infinite. Then f has the **SP** with $S = p_1(C_f(\mathbb{Q}))$, where $p_1 : C_f(\mathbb{Q}) \to \mathbb{A}^1(\mathbb{Q})$ is the projection on the first coordinate.*

Let f be a polynomial with SP; from the property of the set S we can construct sequences of elements of S in the following way.

Let $x_0 \in S$: there exists $x_1 \in S$ such that $f(x_0, x_1) = 0$. Since $x_1 \in S$ there exists $x_2 \in S$ such that $f(x_1, x_2) = 0$, and so on. If there exists $k, m \in \mathbb{N}$, $k < n$ such that $x_k = x_m$ then we say that $\{x_n\}_{n\in\mathbb{N}}$ is a preperiodic sequence; if $k = 0$ the we call it periodic sequence. In the other case, if $\{x_n\}_{n\in\mathbb{N}}$ goes on without repetition, then we call it infinite sequence.

We can also recursively define the set S as :

$$S_0 = \{x_0 \in \mathbb{Q} \,|\exists\, x_1 \in \mathbb{Q}\ s.t. f(x_0, x_1) = 0\} = p_1(C_f(\mathbb{Q}))$$

$$S_1 = \{x_0 \in S_0 \,|\exists\, x_2 \in \mathbb{Q}\ s.t. f(x_1, x_2) = 0\} = \{x_0 \in S_0 | x_1 \in S_0\}$$

$$\dots$$

$$S_n = \{x_0 \in S_{n-1} \,|\exists\, x_{n+1} \in \mathbb{Q}\ s.t. f(x_n, x_{n+1}) = 0\} = \{x_0 \in S_0 | x_1 \in S_{n-1}\}$$

Note that for each $n \in \mathbb{N}$ we have $S_n \subset S_{n-1}$.
We can set

$$S = \bigcap_{n=0,\dots,\infty} S_n \tag{4.1}$$

Now we use the following theorem of Faltings, which proved a conjecture by Mordell (see [18]):

Theorem 4.1.3 (Faltings) *Let C an irreducible curve defined over $\mathbb{Q}$. If $C(\mathbb{Q})$ is infinite then the genus of C is 0 or 1.*

We cite also the following theorem due to Siegel which deal with the case of curves with infinite integer points (see [39]).

Theorem 4.1.4 (Siegel) *Let C be an irreducible curve defined over $\mathbb{Q}$. If $C(\mathbb{Z})$ is infinite then the genus of C is 0 and the desingularization $\widetilde{C}$ of C has at most two points at infinity.*

By Falting's theorem if $f(X, Y)$ is an irreducible polynomial with Schinzel's property then its associated curve has genus zero or one. In this chapter we consider only the case of genus zero curves.

If $f(X, Y)$ defines a rational curve, by definition there exist rational functions $\varphi, \psi \in \overline{\mathbb{Q}}(t)$ such that

$$f(\varphi(t), \psi(t)) = 0$$

We may assume that

- $\varphi, \psi \in \mathbb{Q}(t)$ since $C_f(\mathbb{Q})$ is not empty and there exists a non singular point of the curve in $C_f(\mathbb{Q})$ since there are at most a finite number of singular points (see section 3.5)
- the couple (φ, ψ) is minimal (see the definition in section 1.2)

We impose also that $\varphi(t), \psi(t)$ are polynomials, which it is equivalent to say that the desingularization of the curve C has only one point at infinity (see section 3.7).

In the case of rational curves whose polynomial has Schinzel's property we reduce the problem to the study of parametrization of the set of rational values of a rational function with another rational function.

More precisely, let $(\varphi(t), \psi(t))$ be a fixed parametrization of a rational curve $C = \{(x, y) \in \mathbb{A}^2 | f(x, y) = 0\}$; then there exists an infinite subset S' of the rational numbers such that

$$S = \{\varphi(t) | t \in S'\}$$

since S is a subset of the projection on the first coordinate of the set of rational points of the curve, which is equal to $\{\varphi(t) | t \in \mathbb{Q}\}$.

By an argument similar to the one of the previous paragraph, for each $t_0 \in S'$ the point $(\varphi(t_0), \psi(t_0))$ is in C, with $\psi(t_0) \in S$. So there exists $t_1 \in S'$ such that $\psi(t_0) = \varphi(t_1)$; since $t_1 \in S'$ there exists $t_2 \in S'$ such that $\psi(t_1) = \varphi(t_2)$ and so on.

Hence if $(\varphi(t), \psi(t))$ is a parametrization of a rational curve with Schinzel's property, we have that

$$\psi(S') \subset \varphi(S')$$

for some S' infinite subset of the rational numbers.

We conjecture that there exists $r \in \mathbb{Q}[t]$ such that

$$\varphi(r(t)) = \psi(t)$$

So we have the following:

Conjecture 1

Let $(\varphi(t), \psi(t))$ a minimal couple of rational functions with rational coefficients and let S an infinite subset of the rational numbers such that

$$\psi(S) \subset \varphi(S)$$

Then there exists $r \in \mathbb{Q}(t)$ such that $\varphi(r(t)) = \psi(t)$.

Of course conjecture 1 is true when $S = \mathbb{Q}$ or also $S = \mathbb{Z}$ (for example by Hilbert's irreducibility theorem). Moreover if in these cases we have that $\psi(S) = \varphi(S)$ then there exists a linear $r \in \mathbb{Q}(t)$ such that $\varphi(r(t)) = \psi(t)$.

Conjecture 1 implies this other one:

Conjecture 2

Let $f(X, Y)$ an irreducible polynomial with rational coefficients and with Schinzel's property. Let $S \subset \mathbb{Q}$ be the set as defined in (4.1).

If the curve $C = \{(x, y) \in \mathbb{A}^2 | f(x, y) = 0\}$ is rational then there exists a parametrization of C of the form

$$f(\varphi(t), \varphi(r(t))) = 0$$

where φ and r are rational functions, and the set S is equal to $\{\varphi(t)|t \in \mathbb{Q}\}$.

If we do not suppose that the couple $(\varphi(t), \psi(t))$ is minimal then our first conjecture is false. For example take the polynomials

$$\varphi(t) = t^2$$

$$\psi(t) = -t^2 + 1$$

This couple of polynomials is not minimal since $[\mathbb{Q}(t) : \mathbb{Q}(\varphi, \psi)] = 2$. It can be immediately seen that there is no rational function r such that $\psi(t) = \varphi(r(t))$ (note that r should have degree one).

If we set $S = \pi_1(C_f(\mathbb{Q}))$, where $f(X, Y) = X^2 + Y^2 - 1$, we see that $\psi(S) = \varphi(S)$. In particular the polynomial $\psi(X) - \varphi(Y)$ has Schinzel's property.

So in case of rational curves we have reduced the problem to the study of bivariate polynomials with separated variables (that is $\psi(X) - \varphi(Y)$) with Schinzel's property.

¿From the example of the introduction we can take rational functions $r(t), s(t) \in \mathbb{Q}(t)$ and define the irreducible minimal polynomial $f(X, Y)$ such that $f(r(t), r(s(t))) = 0$; this polynomial has the SP, and the set S is $\{r(t)|t \in \mathbb{Q}\}$ (or also $\{r(t)|t \in \mathbb{Z}\}$). The map $t \mapsto (r(t), r(s(t)))$ is a minimal parametrization of the curve $C_f = \{(x, y) \in \mathbb{A}^2 | f(x, y) = 0\}$ which, by construction, is a rational curve.

Lemma 4.1.5 *If (φ, ψ) and (φ_1, ψ_1) are minimal parametrizations of $f(X, Y) = 0$ and $\psi = \varphi \circ h$ then $\psi_1 = \varphi_1 \circ h_1$*

So this lemma shows that Conjecture 2 is independent of the chosen parametrization of a rational curve.

4.2 Symmetric case

The following proposition shows the connection between rational symmetric curves and polynomials with Schinzel's property.

Proposition 4.2.1 *Let $f(X,Y) \in \mathbb{Q}[X,Y]$ be an irreducible polynomial and suppose that the curve $C = \{(x,y) \in \mathbb{A}^2 | f(x,y) = 0\}$ is rational. If f is symmetric then f has Schinzel's property and there exists a parametrization of the form*

$$f(\varphi(t), \varphi(a(t))) = 0$$

Conversely if there exists such a parametrization then f has Schinzel's property with $S = \{\varphi(t) | t \in \mathbb{Q}\}$.

Proof : Denote Θ the automorphism of $\mathbb{A}^2$ such that $\Theta(x,y) = (y,x)$; note that it is an involution: $\Theta \circ \Theta = Id$.

Let $\Phi : \mathbb{A}^1(\overline{\mathbb{Q}}) \to C_f$ be a parametrization of the curve C, with $\Phi(t) = (\varphi(t), \psi(t))$, $\varphi, \psi \in \overline{\mathbb{Q}}(t)$ and inverse $\lambda(x,y)$, $\lambda \in \overline{\mathbb{Q}}(x,y)$. Since by hypothesis $\Theta(C) = C$, then $\Phi^\Theta \doteqdot \Theta \circ \Phi$ is another parametrization of C with inverse $\lambda^\Theta \doteqdot \lambda \circ \Theta$.

Let $P = \Phi(t) = (\varphi(t), \psi(t))$ be a point of the curve C; since

$$P^\Theta \doteqdot \Theta(P) = \Phi^\Theta(t) = (\psi(t), \varphi(t))$$

is another point of C and Φ is a parametrization, then there exists $\bar{t} \in \mathbb{Q}$ such that $\Phi(\bar{t}) = P^\Theta$, except for a finite number of cases. But

$$\bar{t} = \lambda(P^\Theta) = \lambda \circ \Phi^\Theta(t) = \lambda^\Theta \circ \Phi(t) \doteqdot a(t)$$

where $a(t) \in \overline{\mathbb{Q}}(t)$.

Hence $\Phi(a(t)) = \Theta(\Phi(t))$, so $\psi(t) = \varphi(a(t))$ and $\Phi(t) = (\varphi(t), \varphi(a(t)))$; the set S is equal to $\{\varphi(t) | t \in \mathbb{Q}\}$.

If the curve C has a parametrization defined over $\mathbb{Q}$ (see chapter 4) then $S \subset \mathbb{Q}$ otherwise it is contained in the number field K generated over $\mathbb{Q}$ by the coefficients of $\varphi(t)$ and $a(t)$. □

The following corollary is an immediate consequence.

Corollary 4.2.2 *In the same hypothesis and notation of the previous proposition, $a(t)$ has the following expression:*

$$a(t) = \frac{\alpha t + \beta}{\gamma t - \alpha}$$

with $\alpha, \beta, \gamma \in \overline{\mathbb{Q}}$ e $\alpha^2 + \beta\gamma \neq 0$.

Proof : Note that

$$a \circ a(t) = (\lambda \circ \Phi^\Theta) \circ (\lambda \circ \Phi^\Theta) = \lambda \circ (\Phi^\Theta \circ \lambda^\Theta) \circ \Phi = \lambda \circ Id \circ \Phi = Id(t) = t$$

so a is an involution: it is a rational function of degree one and it can be easily proved that a has the desired expression. □

Corollary 4.2.3 *Let $f(X,Y) \in \mathbb{Q}[X,Y]$ be an irreducible polynomial and suppose that the curve $C = \{(x,y) \in \mathbb{A}^2 | f(x,y) = 0\}$ is rational.*

Then f is symmetric if and only if there exist $\varphi, a \in \mathbb{Q}(t)$ with $\deg a = 1$ and $a^2 = Id$ such that $(\varphi(t), \varphi(a(t))$ is a parametrization of C.

Proof : The 'only if' part has already been proved in the previous proposition.

The 'if' part follows from the next two lemmas. □

Lemma 4.2.4 *Let $f(X,Y) \in \mathbb{Q}[X,Y]$ be an irreducible polynomial and let*

$$C = \{(x,y) \in \mathbb{A}^2 | f(x,y) = 0\}$$

be the associated curve in $\mathbb{A}^2(\overline{\mathbb{Q}})$. Then f is symmetric if and only if there exists an infinite subset $A \subset C$ such that for every $(x,y) \in A$ we have $(y,x) \in C$.

Proof : This lemma follows immediately from proposition 3.1.2: it is sufficient to consider the irreducible curves C and $C' = \{(x,y) \in \mathbb{A}^2 | g(x,y) = 0\}$, where the polynomial $g(X,Y) \doteqdot f(Y,X)$ is irreducible too. Since by hypothesis $C \cap C'$ has infinite points it follows that f and g divide each other, so they are equal since they have the same degree. The lemma is proved. □

Lemma 4.2.5 *Let $r, s \in \mathbb{Q}(t)$ be two rational functions and $f(X,Y) \in \mathbb{Q}[X,Y]$ be the minimal polynomial such that $f(r(t), r(s(t)) = 0$. If $s(t)$ is an involution then f is symmetric.*

Proof : If $s(t)$ in an involution then $s^{-1}(t)$ is well defined and is equal to $s(t)$. So if we set $\tau \doteqdot s(t)$ we have

$$f(r(s(t)), r(t)) = f(r(\tau), r(s^{-1}(\tau))) = f(r(\tau), r(s(\tau))) = 0$$

So for the previous lemma f is symmetric.

Since the rational function $s(t)$ has degree one it determines a birationality of $\mathbb{A}^1$ with itself. □

Lemma 4.2.6 *Let k be a field and $f(X,Y) \in k[X,Y]$ be the minimal polynomial such that $f(r(t), r(s(t))) = 0$, for $r, s \in k(t)$. If f is symmetric then $\deg s(t) = 1$.*

Proof : Since f is symmetric then $\deg_X(f) = \deg_Y(f)$. The statement follows from lemma 1.2.1. □

4.3 Kubota's results

The only known result in this direction so far are the followings theorems by Kubota (see his articles [21], [22] and [23]).

The main contribution of Kubota in [21] was to show that the following conjecture of Narkiewicz was false (see [33]): let f, g two polynomials in $\mathbb{Q}[T]$ and $S \subset \mathbb{Q}$ infinite such that $f(S) = g(S)$; then $\deg(f) = \deg(g)$.

Theorem 4.3.1 (Kubota) *Let f and g be two polynomials in $\mathbb{Q}[T]$, with $\deg(g) > \deg(f)$, and suppose that there exists an infinite subset S of $\mathbb{Q}$ such that $g(S) \subset f(S)$. If every component of the curve $g(X) - f(Y) = 0$ containing an infinity of points of $S \times S$ has a polynomial parametrization, then $g = f \circ h$ for some $h \in \mathbb{Q}[T]$.*

This theorem is based on the following other one (see [23]):

Theorem 4.3.2 (Kubota) *Let $f(X) - g(Y) \in \mathbb{Q}[X, Y]$, where $\deg(f) \neq \deg(g)$; then every component of the curve $\{(x, y) | f(x) = g(y)\}$ which admits a polynomial parametrization is of the form $f_1(X) - g_1(Y)$, for some polynomials $f_1, g_1 \in \mathbb{Q}[T]$.*

Theorem 4.3.3 (Kubota) *Let f and g be two polynomials in $\mathbb{Q}[T]$, with $n = \deg(f)$ and $m = \deg(g)$; suppose also that there exists an infinite sequence $S = \{s_n\}_{n \in \mathbb{N}} \subset \mathbb{Q}$ such that $g(s_n) = f(s_{n+1})$ for all $n \in \mathbb{N}$. Then $m \geq n$.*

The following theorem deals with the case of equal degree. A $(f, g) -$ cycle is a finite set $A = \{a_i\}_{i=0,\ldots,n}$ such that $g(a_i) = f(a_{i+1})$ for all $i = 0, \ldots, n-1$ and $g(a_n) = f(a_0)$. Note that a $(f, g) -$ cycle is also a $(g, f) -$ cycle.

Theorem 4.3.4 (Kubota) *Let f and g be two polynomials in $\mathbb{Q}[T]$, with $\deg(f) = \deg(g)$; suppose also that there exists an infinite subset S of $\mathbb{Q}$ such that $f(S) = g(S)$ with $\#\{(f, g) - \text{cycles}\} < \infty$. Then there exists a linear polynomial $h(t) \in \mathbb{Q}[t]$ such that $g = f \circ h$.*

Chapter 5

Parametrization of integer-valued polynomials

5.1 Introduction

The set of **integer-valued polynomials** is defined as

$$\mathrm{Int}(\mathbb{Z}) = \{f(X) \in \mathbb{Q}[X] \mid f(\mathbb{Z}) \subset \mathbb{Z}\}$$

(see for example [6]). It is a $\mathbb{Z}$-module which contains the ring of polynomials over $\mathbb{Z}$. It also contains the binomial polynomials

$$\binom{X}{n} \doteqdot \frac{X(X-1)\dots(X-(n-1))}{n!}$$

where $n \in \mathbb{N}$.
The following theorem, due to Polya, holds

Theorem 5.1.1 *The set* $\mathrm{Int}(\mathbb{Z})$ *is a free* $\mathbb{Z}$*-module. The set of the binomial polynomials* $\{\binom{X}{n} \mid n \in \mathbb{N}\}$ *is a basis of* $\mathrm{Int}(\mathbb{Z})$.

For a proof see [32] or [6].

More explicitly if $f \in \mathrm{Int}(\mathbb{Z})$ has degree n then we have

$$f(X) = f(0)\binom{X}{0} + \Delta f(0)\binom{X}{1} + \ldots + \Delta^n f(0)\binom{X}{n}$$

where $\Delta g(X) = g(X) - g(X+1)$ and this expression for f as $\mathbb{Z}$-linear combination of $\binom{X}{i}$ is unique.

Given a polynomial $f \in \mathrm{Int}(\mathbb{Z})$ we want to parametrize the set of integer values of f over $\mathbb{Z}$ (that is the set $f(\mathbb{Z})$) with a polynomial with integer coefficients in one or several variables. We give the following definition.

Definition 5.1.2 *Let $f(X)$ be an integer-valued polynomial.*
*We say that $f(\mathbb{Z})$ is $\mathbb{Z}$-**parametrizable** if there exists $m \in \mathbb{N}$ and a polynomial $g \in \mathbb{Z}[\underline{X}] = \mathbb{Z}[X_1, \ldots, X_m]$ such that $f(\mathbb{Z}) = g(\mathbb{Z}^m)$.*

As an example consider the integer-valued polynomial $f(X) = X(X-1)/2$. We define the following polynomials with integer coefficients

$$g_1(X) = f(2X)$$
$$g_2(X) = f(2X+1)$$

Since $\mathbb{Z} = P \cup D$, where P is the set of even integers and D is the set of odd integers, it follows that $f(\mathbb{Z}) = f(P) \cup f(D) = g_1(\mathbb{Z}) \cup g_2(\mathbb{Z})$. But $f(X) = f(1-X)$ so we have that $g_2(X) = f(-2X) = g_1(-X)$ so g_1 and g_2 have the same values over the integers and $f(\mathbb{Z})$ can be parametrized by a single polynomial with integer coefficients in one variable.

It is crucial that f has a symmetry axis of this kind, that is $f(h(X)) = f(X)$, where $h(X) = 1 - X$, and h swaps P with D; this implies that $f(P) = f(D)$.

Here we state the main theorem of this chapter.

Theorem 5.1.3 *Let $f \in \mathrm{Int}(\mathbb{Z})$ be of the form $f(X) = F(X)/N$ where $F \in \mathbb{Z}[X]$ and $N \in \mathbb{N}$ is minimal.*

If N is divisible by a prime number different from 2 then $f(\mathbb{Z})$ is not $\mathbb{Z}$-parametrizable.

If $N = 2^n$, where $n \in \mathbb{N}$, and $f(\mathbb{Z})$ is $\mathbb{Z}$-parametrizable then there exists $\beta \in \mathbb{Q}$ which is the ratio of two odd integers such that $f(X) = f(-X + \beta)$.

The set $f(\mathbb{Z})$ is equal to $g(\mathbb{Z})$ for some $g \in \mathbb{Z}[X]$ if and only if $f(X)$ is an integer coefficient polynomial or it belongs to $\mathbb{Z}[X(b-X)/2]$ for some odd integer b.

The content of a polynomial $f \in \mathbb{Z}[X]$ is defined as the greatest common divisor of the coefficients and it is denoted with $\mathrm{cont}(f)$; the hypothesis on N means that $(N, \mathrm{cont}(F)) = 1$. The ring $\mathbb{Z}_{(2)}$ is the localization of $\mathbb{Z}$ at the prime ideal $(2) \subset \mathbb{Z}$; so β is an element of $\mathbb{Z}^*_{(2)}$, the group of invertible elements of $\mathbb{Z}_{(2)}$.

Observe also that if $f(X) = F(X)/N$ with $N \in \mathbb{N}$ and $F \in \mathbb{Z}[X]$ such that $(N, cont(F)) = 1$ then $f(X)$ is an integer-valued polynomial if and only if $F(\mathbb{Z}) \subset N\mathbb{Z}$.

In a paper of Frisch (see [15]) the author deals with parametrization of subsets of $\mathbb{Z}^k$ with integer coefficient polynomials and integer-valued polynomials. In an another article of the same author and Vaserstein (see [16]) it is showed that the subset of $\mathbb{Z}^3$ of pythagorean triples is parametrizable by a single triple of integer-valued polynomials in four variables, but it cannot be parametrized by a single triple of integer coefficients polynomials in any number of variables. Our theorem shows that there exist subsets of $\mathbb{Z}$ parametrizable by an integer-valued polynomial which are not parametrizable by an integer coefficient polynomial in any number of variables.

The theorem 5.1.3 will be proved in several steps.

We need the following theorem by Siegel (see [39] or [25]):

Theorem 5.1.4 ***(Siegel)*** *Let $f \in \mathbb{Q}[X,Y]$ be an irreducible polynomial such that $\deg_Y(f) \geq 2$. Let Ω be the set*

$$\Omega \doteqdot \{n \in \mathbb{Z} \mid \exists\, q \in \mathbb{Q} \; s.t. \; f(n,q) = 0\}$$

If $B \in \mathbb{R}_{\geq 0}$ then

$$\#(\Omega \cap [-B,B]) = O(B^{1/2})$$

In particular the set Ω has zero density, that is

$$\lim_{B \to +\infty} \frac{\#(\Omega \cap [-B,B])}{\#(\mathbb{Z} \cap [-B,B])} = 0$$

5.2 Linear factors of bivariate separated polynomials

Given a non-constant polynomial $f \in \mathbb{Z}[X]$, we define the polynomial in two variables

$$F_f(X,Y) \doteqdot \frac{f(X) - f(Y)}{X - Y}$$

We remark that $f(X) - f(Y)$ as a polynomial in the variable Y over the ring $\mathbb{Q}[X]$ is separable (for instance by the derivative criterion). This implies that it has distinct irreducible factors in $\mathbb{Q}[X,Y]$.

Proposition 5.2.1 *Let $f \in \mathbb{Z}[X]$. If for all $n \in \mathbb{Z}$ there exists $q \in \mathbb{Q}$ such that $F_f(n,q) = 0$, then there exists $\beta \in \mathbb{Q}$ such that $f(X) = f(-X + \beta)$.*

Proof : Let $F_f(X,Y) = \prod_{i=1,\ldots,s} g_i(X,Y)$ be the factorization of F_f in $\mathbb{Q}[X,Y]$ and let d_i be the Y-degree of the factor $g_i \in \mathbb{Q}[X,Y]$ for $i = 1,\ldots,s$. For each positive constant $B \in \mathbb{R}$ we define the sets

$$Z_{i,B} \doteqdot \{n \in \mathbb{Z} |\; |n| \leq B \;\; , \exists\, q \in \mathbb{Q} \;\; s.t. \; g_i(n,q) = 0\} \tag{5.1}$$

For those indexes i such that $d_i \geq 2$, each of the sets $Z_{i,B}$ has cardinality $O(B^{1/2})$ (this follows from Siegel's theorem 5.1.4). Since by hypothesis $\mathbb{Z} \cap [-B,B] = \bigcup_{i=1,\ldots,s} Z_{i,B}$, it follows that there exists $j \in \{1,\ldots,s\}$ such that $d_j = 1$, which means that $g_j(X,Y) = Y - Q_j(X)$ where $Q_j \in \mathbb{Q}[X]$.

Since $F_f(X,Y)$ divides $f(X) - f(Y)$ it follows that $f(X) = f(Q_j(X))$ so $\deg(Q_j) = 1$, that is $Q_j(X) = \alpha X + \beta$ with $\alpha, \beta \in \mathbb{Q}$. From the equality $f(X) = f(\alpha X + \beta)$ we deduce that $\alpha = \pm 1$. If $\alpha = 1$ then it follows immediately that $\beta = 0$ (a non constant polynomial cannot be periodic) but this possibility has to be excluded since $X - Y$ is an irreducible factor of $f(X) - f(Y)$ that has been removed in $F_f(X,Y)$. As we have remarked $f(X) - f(Y)$ has distinct irreducible factors.

So we have that $f(X) = f(-X + \beta)$. Observe that the corresponding sets $Z_{i,B}$ are equal to $\mathbb{Z} \cap [-B, B]$. $\square$

We easily get the same conclusion if there exists a constant $M \in \mathbb{R}_{>0}$ such that for all $n \in \mathbb{Z}$, $|n| > M$, there exists $q \in \mathbb{Q}$ such that $F_f(n, q) = 0$.

Corollary 5.2.2 *Let $f \in \mathbb{Q}[X]$. Then $f(X) - f(Y) \in \mathbb{Q}[X, Y]$ has at most two linear factors.*

Proof : Observe that $X - Y$ divides $f(X) - f(Y)$ for all $f \in \mathbb{Q}[X]$.
If $\alpha \in \mathbb{R}$ is chosen out of a bounded set, the set

$$\Gamma_\alpha = \{\gamma \in \mathbb{Q} | f(\gamma) = f(\alpha)\}$$

has at most two elements, according to the parity of $\deg(f)$, since f is definitely strictly increasing-decreasing. So for $|\alpha| \gg 0$ the set Γ_α has cardinality two if and only if $\deg(f) \equiv 0 \pmod 2$ and there exists $\beta \in \mathbb{Q}$ such that $f(X) = f(-X + \beta)$ (see the remark after the previous proposition).
If $f(X) - f(Y) = \prod g_i(X, Y)$ is the factorization then $f(X) - f(\alpha) = \prod g_i(X, \alpha)$, where $\alpha \in \mathbb{R}$ is chosen out of a bounded set. If $f(X) - f(Y)$ had more than two linear factors then $f(X) - f(\alpha)$ would have more than two roots which is impossible.

We give also another direct proof of the last fact.
If $f(X) = f(-X+\beta_1) = f(-X+\beta_2)$, where $\beta_1 \neq \beta_2$, then if we set $T \doteqdot -X+\beta_1$ we have that $f(T) = f(T-\beta_1+\beta_2)$, which is true if and only if $-\beta_1+\beta_2 = 0$ (a polynomial cannot be periodic), which leads to a contradiction. $\square$

5.3 Preliminary results

Definition 5.3.1 *Let K be a number field and $f \in K[\underline{X}] = K[X_1, \ldots, X_m]$ of the form*

$$f(\underline{X}) = \sum_{\underline{i}} a_{\underline{i}} \underline{X}^{\underline{i}}$$

where $\underline{i} = (i_1, \ldots, i_m) \in \mathbb{N}^m$ and $\underline{X}^{\underline{i}} = X_1^{i_1} \ldots X_m^{i_m}$.
*Let v be a valuation of the field K and $|\ |_v$ the associated norm. The **Gauss norm** of f is defined as (see [34], pg.119):*

$$\|f\|_v \doteqdot \max_{\underline{i}} \{|a_{\underline{i}}|_v\}$$

The Gauss norm coincides with $|\ |_v$ over K. If v is a non-archimedian valuation the Gauss norm is multiplicative on $K[\underline{X}]$ by Gauss Lemma, since we have the equality

$$\|f\|_v = |\mathrm{cont}(f)|_v$$

Moreover if $\underline{x} \in O_v^m$, where $O_v \subset K$ is the valuation ring of v, then it follows that

$$|f(\underline{x})|_v \leq \|f\|_v$$

Lemma 5.3.2 *Let $p \in \mathbb{N}$ be a prime, let $f \in \mathbb{Z}[X] - p\mathbb{Z}[X]$, let $g \in \mathbb{Z}[\underline{X}] = \mathbb{Z}[X_1, \ldots, X_m]$ and let $Q \in \mathbb{Q}[\underline{X}]$ be such that*

$$f(Q(\underline{X})) = pg(\underline{X})$$

Then there are two possibilities: either

$$Q(\underline{X}) = \frac{a_0 + pR(\underline{X})}{D}$$

where $a_0 \in \mathbb{Z}$, $R \in \mathbb{Z}[\underline{X}]$, $R(\underline{0}) = 0$ and $D \in \mathbb{N}$ is such that $p \nmid D$, or there exist algebraic numbers ξ, π in the splitting field K of f over $\mathbb{Q}$, a non-archimedian valuation v of K above p with valuation ring O_v such that $v(\pi) = 1$ and $\xi \notin O_v$, and a polynomial $R(\underline{X}) \in O_v[\underline{X}]$ such that

$$Q(\underline{X}) = \xi(1 + \pi R(\underline{X})).$$

Proof : Let K be the splitting field over $\mathbb{Q}$ of the polynomial $f(X)$ and let v be a valuation of K over the valuation v_p of $\mathbb{Q}$ with valuation ring $O_v \subset K$ and uniformizer π (that is $v(\pi) = 1$). In $K[X]$ the polynomial f factorizes in the following way

$$f(X) = c_0 \prod_i (\alpha_i X - \beta_i)$$

where $c_0 \in K$, $\alpha_i, \beta_i \in O_v$ such that $(\alpha_i, \beta_i) = 1$ (remember that O_v is integrally closed in K since it is a valuation ring). Note that $c_0 \in \mathbb{Z} - p\mathbb{Z}$ since the product of primitive polynomials is a primitive polynomial in $O_v[X]$ by Gauss Lemma (O_v is a UFD and K is its quotient field); so the content of f is c_0, and c_0 is an integer because $f \in \mathbb{Z}[X]$. Since by hypothesis $f \in \mathbb{Z}[X] - p\mathbb{Z}[X]$ then $p \nmid c_0$. Then

$$f \circ Q(\underline{X}) = c_0 \prod_i (\alpha_i Q(\underline{X}) - \beta_i)$$

and applying the Gauss norm relative to the valuation v

$$\|f \circ Q(\underline{X})\|_v = \prod_i \|\alpha_i Q(\underline{X}) - \beta_i\|_v = \|pg(\underline{X})\|_v < 1$$

So there is an index j such that $\|\alpha_j Q(\underline{X}) - \beta_j\|_v < 1$ which implies

$$\|Q(\underline{X}) - \xi_j\|_v < |\alpha_j|_v^{-1} \tag{5.1}$$

where $\xi_j = \beta_j/\alpha_j \in K$ is the corresponding root of f.
Suppose $Q(\underline{X}) = \sum_{\underline{i}\geq \underline{0}} a_{\underline{i}} \underline{X}^{\underline{i}}$ where $a_{\underline{i}} \in \mathbb{Q}$.

First we consider the case $\pi \nmid \alpha_j$, which implies $|\alpha_j|_v = 1$ and $\|Q(\underline{X}) - \xi_j\|_v < 1$.
We have $|a_{\underline{i}}|_v = |a_{\underline{i}}|_p < 1$ for each $\underline{i} > \underline{0}$ and $|a_{\underline{0}} - \xi_j|_v < 1$. ¿From the first inequality we deduce that all the coefficients of Q (except the constant term) are elements of $p\mathbb{Z}_{(p)}$, where $\mathbb{Z}_{(p)}$ is the localization of $\mathbb{Z}$ at the prime ideal (p).
Let us focus on the second inequality. If $a_{\underline{0}} = a/b$, where $a, b \in \mathbb{Z}$ are coprime integers, we have

$$\left|\frac{a}{b} - \frac{\beta_j}{\alpha_j}\right|_v = \left|\frac{\alpha_j a - b\beta_j}{b\alpha_j}\right|_v = \frac{|\alpha_j a - b\beta_j|_v}{|b|_v} < 1$$

since $|\alpha_j|_v = 1$.
Suppose that $p|b$ or equivalently $|b|_v = |b|_p < 1$. Then we have $|\alpha_j a - b\beta_j|_v < |b|_p < 1$: this is impossible since a is coprime with b which implies $|\alpha_j a|_v = |\alpha_j|_v |a|_p = 1$. Hence $p \nmid b$ and so the constant term of Q belongs to $\mathbb{Z}_{(p)}$.
So in this case the polynomial Q has the following form

$$Q(\underline{X}) = \frac{a + pR(\underline{X})}{D}$$

where $R(\underline{X}) \in \mathbb{Z}[\underline{X}]$ with $R(\underline{0}) = 0$ and $D \in \mathbb{Z}$ with $p \nmid D$, as we stated.

Suppose now that $\pi|\alpha_j$ which implies $\pi \nmid \beta_j$, since α_j and β_j are coprime. Hence $|\beta_j|_v = 1$ and $\xi_j = \beta_j/\alpha_j \notin O_v$, which means $|\xi_j|_v > 1$.
¿From equation (5.1) we have

$$\|Q - \xi_j\|_v < |\xi_j|_v.$$

We deduce that $a_{\underline{i}} = \xi_j \pi^{n_{\underline{i}}} u_{\underline{i}}$ for $\underline{i} > \underline{0}$ and $a_{\underline{0}} = \xi_j(1 + \pi^{n_{\underline{0}}} u_{\underline{0}})$ where $n_{\underline{i}} > 0$ and $u_{\underline{i}} \in O_v^*$. So there exists a polynomial $R \in O_v[\underline{X}]$ such that

$$Q(\underline{X}) = \xi_j(1 + \pi R(\underline{X}))$$

as we want to prove. □

Observe that in the second case of the lemma for all $\underline{x} \in \mathbb{Z}^m$ we have that

$$|Q(\underline{x})|_p = |\xi_j|_v |1 + \pi R(\underline{x})|_v = |\xi_j|_v = k > 1$$

since $1+\pi R(\underline{x}) \in O_v^*$, where k is a constant independent from the polynomial Q and the integer vector $\underline{x}$. If $Q(\underline{X}) = Q_D(\underline{X})/D$, where $Q_D \in \mathbb{Z}[\underline{X}]$ and $D \in \mathbb{Z}$ such that $(D, \mathrm{cont}(Q_D)) = 1$, this implies that $|Q_D(\underline{x})|_p \leq 1$ is constant for all $\underline{x} \in \mathbb{Z}^m$ and $p|D$.

This condition is weaker than the second one contained in the lemma: take for example the polynomial $(X^2+1)/2$ which is 2-adically constant but it is not of the form of the second case of the lemma.

Lemma 5.3.3 *Let $H \in \mathbb{Q}[\underline{Y}]$ and let T be the set*

$$T \doteqdot \{n \in \mathbb{Z} | \exists\, \underline{y} \in \mathbb{Z}^m \; s.t. \; n = H(\underline{y})\}$$

Let v be a non-archimedean absolute value of $\overline{\mathbb{Q}}$ which extends a p-adic absolute value $|\ |_p$ of $\mathbb{Q}$.

If T is dense in $\mathbb{Q}$ for the topology induced by $|\ |_p$, then for all $\gamma \in \overline{\mathbb{Q}}$ we have the inequality

$$\|X - \gamma\|_v \leq \|H - \gamma\|_v$$

Proof : Let γ be an algebraic number and let $n \in T$. Then we have $n - \gamma = (H - \gamma)(\underline{y}_n)$ and so

$$|n - \gamma|_v \leq \|H - \gamma\|_v$$

since $\underline{y}_n \in \mathbb{Z}^m$.

We define $r_\gamma \doteqdot \|H - \gamma\|_v$.

If $|\gamma|_v > 1$ then $|\gamma|_v = |n - \gamma|_v \leq r_\gamma$.

If $|\gamma|_v \leq 1$ then $r_\gamma \geq 1$ otherwise we have $|n - \gamma|_v < 1$ for every $n \in T$. But this means that n is constant modulo the valuation v: this is absurd because $T \subset \mathbb{Q}$ is dense for $|\ |_p$. In fact let $\overline{n} \in T$ be fixed, then for all $n \in T$ we have

$$|n - \overline{n}|_p = |n - \overline{n}|_v = |n - \gamma + \gamma - \overline{n}|_v \leq \max\{|n - \gamma|_v, |\gamma - \overline{n}|_v\} < 1$$

so T would be contained in a single residue class modulo p.

So we have $r_\gamma \geq \max\{1, |\gamma|_v\}$, which implies that

$$\|H - \gamma\|_v = r_\gamma \geq \|X - \gamma\|_v$$

This proves the lemma. □

5.4 Main results

The following proposition generalizes the example shown in the introduction.

Proposition 5.4.1 *Let $f \in Int(\mathbb{Z})$ be of the form $f(X) = F(X)/2$ where $F \in \mathbb{Z}[X] - 2\mathbb{Z}[X]$. If there exists an odd integer b such that $f(X) = f(-X + b)$ then $f(\mathbb{Z})$ is $\mathbb{Z}$-parametrizable.*

Proof : Observe that $f \in \mathrm{Int}(\mathbb{Z})$ is equivalent to $F(\mathbb{Z}) \subset 2\mathbb{Z}$. In particular 2 divides a_0, the constant term of $F(X)$.

We define the following two polynomials

$$g_1(X) \doteqdot f(2X) \ , \ \ g_2(X) \doteqdot f(2X + 1)$$

These polynomials have integer coefficients, in fact if $f(X) = (\sum_{i\geq 1} a_i X^i + a_0)/2$ where $a_i \in \mathbb{Z}$ for $i = 0, \ldots, n$, then

$$g_1(X) = (\sum_{i\geq 1} a_i 2^i X^i + a_0)/2$$

and it is obviously a polynomial in $\mathbb{Z}[X]$. For the second polynomial we have

$$2g_2(X) = \sum_{i\geq 1} a_i(2X + 1)^i + a_0 \equiv \sum_{i\geq 1} a_i + a_0 \pmod{2\mathbb{Z}[X]} = f_2(1) \equiv 0 \pmod{2\mathbb{Z}[X]}$$

which means that $g_2 \in \mathbb{Z}[X]$.

Since $\mathbb{Z} = P \cup D$, where P is the set of even integers and D the set of odd integers, then $f(\mathbb{Z}) = f(P) \cup f(D) = g_1(\mathbb{Z}) \cup g_2(\mathbb{Z})$. Now we want to show that $g_1(\mathbb{Z}) = g_2(\mathbb{Z})$. The following equality holds

$$g_2(X) = f(-2X - 1 + b)$$

Since $b - 1 \equiv 0 \pmod 2$ then g_2 has the same image over $\mathbb{Z}$ of g_1 (if $n \in \mathbb{Z}$ then for $m = n + (1 - b)/2 \in \mathbb{Z}$ we have $g_1(n) = g_2(m)$). $\square$

The fact is that the map $h : X \mapsto -X + b$ swaps the odd integers with even integers and moreover $f(h(X)) = f(X)$, as we have already remarked.

Proposition 5.4.2 *Let $q \in \mathbb{N}$ let $f \in \mathrm{Int}(\mathbb{Z})$ be of the form $f(X) = F(X)/q$ where $F \in \mathbb{Z}[X]$ and $(cont(F), q) = 1$.*

If $q = 2^a$, where $a \in \mathbb{N} - \{0\}$ and $f(\mathbb{Z})$ is $\mathbb{Z}$-parametrizable, then there exists $\beta \in \mathbb{Z}^*_{(2)}$ such that $f(X) = f(-X + \beta)$.

If q is a prime different from 2 then $f(\mathbb{Z})$ is not $\mathbb{Z}$-parametrizable.

Proof : Suppose that there exists $g \in \mathbb{Z}[\underline{X}]$ such that $f(\mathbb{Z}) = g(\mathbb{Z}^m)$.

Since $g(\mathbb{Z}^m) \subset f(\mathbb{Z})$ then by Hilbert's irreducibility theorem (see [39]) there exists $Q \in \mathbb{Q}[\underline{X}]$ such that $f(Q(\underline{X})) = g(\underline{X})$. Therefore we can write

$$F(Q(\underline{X})) = pg(\underline{X}) \tag{5.2}$$

where p is equal to 2 if $q = 2^a$ and $p = q$ if q is a prime different from 2.

From the inclusion $f(\mathbb{Z}) \subset g(\mathbb{Z}^m)$ we have that for every $n \in \mathbb{Z}$ there exists $\underline{x}_n \in \mathbb{Z}^m$ such that $f(n) = g(\underline{x}_n)$; from this fact and equation (5.2) we deduce

$$F(n) = F(Q(\underline{x}_n)) \tag{5.3}$$

Therefore for all $n \in \mathbb{Z}$ the couple $(n, Q(\underline{x}_n)) \in \mathbb{Z} \times (\mathbb{Z}/D)$, where $D \in \mathbb{Z}$ is the denominator of Q, is a point of the plane curve

$$C_f = \{(x, y) \in \mathbb{A}^2 | F(x) = F(y)\}$$

Let

$$F(X) - F(Y) = \prod_{i \in I} g_i(X, Y)$$

be the factorization of $F(X) - F(Y)$ over $\mathbb{Q}[X, Y]$ (remember that there is at least one linear factor and at most two of them). From (5.3) we have

$$\mathbb{Z} = \bigcup_{i \in I} \{n \in \mathbb{Z} \mid (n, Q(\underline{x}_n)) \in C_i\}$$

where C_i is the plane curve $\{(x, y) \in \mathbb{A}^2 | g_i(x, y) = 0\}$. For $i \in I$ we define the sets

$$T_i \doteqdot \{n \in \mathbb{Z} \mid (n, Q(\underline{x}_n)) \in C_i\}$$

The sets T_i, for $i \in I$, cover $\mathbb{Z}$. For every $B \in \mathbb{R}$, $B \geq 0$, and $i \in I$ we also define the sets $T_{i,B} \doteqdot T_i \cap [-B, B]$; they cover $\mathbb{Z}_B$, where $\mathbb{Z}_B \doteqdot \mathbb{Z} \cap [-B, B]$.

If I' is the subset of I of those indexes i such that the Y-degree of $g_i(X, Y)$ is greater or equal than 2, then by a theorem of Siegel (see [39]) we have

$$\#(\bigcup_{i \in I'} Z_{i,B}) = O(B^{1/2})$$

where B varies over the real positive numbers and $Z_{i,B}$'s are the sets defined in (5.1). Since for every $i \in I$ we have $T_{i,B} \subset Z_{i,B}$ then $\#(T_{i,B}) = O(B^{1/2})$ for $i \in I'$. In particular $\bigcup_{i \in I'} T_{i,B}$ is a set of integers of density zero.

So we focus our attention on the remaining sets T_i for $i \in I - I'$. They correspond to linear factors of the polynomial $F(X) - F(Y)$.

Equation (5.2) implies that we can apply lemma 5.3.2.

Suppose that we are in the first case of lemma 5.3.2: $Q(\underline{X}) = \frac{a_0+pR(\underline{X})}{D}$, where $a_0 \in \mathbb{Z}$, $R \in \mathbb{Z}[\underline{X}]$, $R(\underline{0}) = 0$ and $D \in \mathbb{N}$ such that $p \nmid D$.

Let us say that for $i = 0$ the corresponding factor $g_0(X, Y)$ is $X - Y$. Then for all $n \in T_0$ we have

$$n = Q(\underline{x}_n) = \frac{a_0 + pR(\underline{x}_n)}{D}$$

which implies

$$Dn = a_0 + pR(\underline{x}_n) \tag{5.4}$$

and considering this last equation modulo p we obtain

$$n \equiv a_0 D' \pmod{p}$$

where $D' \in \mathbb{Z}$ such that $DD' \equiv 1 \pmod{p}$.

So we have obtained that

$$T_0 \subset \{n \in \mathbb{Z} |\ n \equiv a_0 D' \pmod{p}\} \tag{5.5}$$

that is T_0 is contained in a single residue class modulo p. Therefore $\#(T_{0,B}) \leq B/p$.

As B goes to infinity we have that $T_{0,B} \cup \bigcup_{i \in I'} T_{i,B}$ does not cover $\mathbb{Z}_B$ (because the function $B - B^{1/2} - B/p$ is definitely positive). By proposition 5.2.1 it follows that there exists $\beta \in \mathbb{Q}$ such that $F(X) = F(-X + \beta)$, that is $I = I' \cup \{0\} \cup \{i_0\}$ and $g_{i_0}(X, Y) = Y + X - \beta$. From corollary 5.2.2 there are no other linear factors of $F(X) - F(Y)$ in $\mathbb{Q}[X, Y]$. We suppose that $i_0 = 1$.

For all $n \in T_1$ we have

$$n = -Q(\underline{x}_n) + \beta = -\frac{a_0 + pR(\underline{x}_n)}{D} + \beta$$

and

$$Dn = -(a_0 + pR(\underline{x}_n)) + D\beta \tag{5.6}$$

which in particular implies that $D\beta = D'' \in \mathbb{Z}$ and $\beta \in \mathbb{Z}_{(p)}$, since $p \nmid D$. Considering as before this equation modulo p we obtain

$$n \equiv -a_0 D' + D''D' \pmod{p}$$

hence

$$T_1 \subset \{n \in \mathbb{Z} |\ n \equiv -a_0 D' + D''D' \pmod{p}\} \tag{5.7}$$

and T_1 is contained in a single residue class modulo p.

If $p = 2$ then $D''D' \not\equiv 0 \pmod 2$, otherwise by (5.5) and (5.7) T_0 and T_1 would be contained in the same residue class, so there would be a residue class not covered by $\bigcup_{i \in I} T_i$. Hence if $p = 2$ we have that $\beta \in \mathbb{Z}^*_{(2)}$.

For each $B \geq 0$ we have

$$\begin{array}{rcl} 0 = \#\mathbb{Z}_B - & \#(\bigcup_{i\in I} T_{i,B}) & \geq \\ \#\mathbb{Z}_B - & \#(\bigcup_{i\in I'} T_{i,B}) & -\#(T_{0,B}) - \#(T_{i_0,B}) = \\ B - & B^{1/2} & -B/p - B/p = \\ & & \dfrac{p-2}{p}B - B^{1/2}. \end{array}$$

If p is a prime different from 2 we have a contradiction: the sets $T_{i,B}$ for $i \in I$ does not cover $\mathbb{Z}_B$ as B goes to infinity.

In the second case of lemma 5.3.2 we have that for every $\underline{x} \in \mathbb{Z}^m$ the value $|Q(\underline{x})|_p$ is a constant greater then one. Then the set $T_{0,B}$ is empty since the equation

$$n = Q(\underline{x}_n)$$

has no solution: $|n|_p \leq 1$ for every $n \in \mathbb{Z}$ but $|Q(\underline{x}_n)|_p > 1$.

As before by proposition 5.2.1 there exists $\beta \in \mathbb{Q}$ such that $f(X) = f(-X + \beta)$. Therefore $\mathbb{Z} = T_{i_0} \cup (\bigcup_{i\in I'} T_i)$ and T_{i_0} contains an Hilbert set, the complement of $\bigcup_{i\in I'} Z_i$, which is dense in $\mathbb{Q}$ for each p-adic absolute value $|\ |_p$ (see Corollary 2.5 of chapter 9 of [25]). Hence we can apply lemma 5.3.3 to the polynomial $-Q(\underline{X}) + \beta$ and the set T_{i_0}: for all $\gamma \in \overline{\mathbb{Q}}$ we have that

$$\|X - \gamma\|_v \leq \| - Q + \beta - \gamma\|_v \tag{5.8}$$

where v is a valuation in $\overline{\mathbb{Q}}$ which extends the p-adic valuation of $\mathbb{Q}$.

Let

$$F(X) = c_0 \prod (X - \xi_i)$$

be the factorization of $F(X)$ in $\overline{\mathbb{Q}}$ and fix a valuation v of the splitting field of f over $\mathbb{Q}$ over the p-adic valuation of $\mathbb{Q}$.

We have the following relations (here we use inequality (5.8)):

$$\begin{array}{rcl} \|F\|_v & = & |c_0|_v \prod \|X - \xi_i\|_v \leq \\ & & |c_0|_v \prod \| - Q + \beta - \xi_i\|_v = \\ & & \|c_0 \prod (-Q + \beta - \xi_i)\|_v = \\ & & \|F(-Q + \beta)\|_v = \\ & & \|F(Q)\|_v = \\ & & \|pg\|_v < 1 \end{array}$$

but this is a contradiction since $F \in \mathbb{Z}[X] - p\mathbb{Z}[X]$.

Therefore in the second case of lemma 5.3.2 the sets $T_{i,B}$ for $i \in I$ do not cover $\mathbb{Z}_B$ as B goes to infinity (even in the case $p = 2$). $\square$

If $f \in \mathrm{Int}(\mathbb{Z})$, $f(X) = F(X)/2^a$, is such that $f(\mathbb{Z})$ is $\mathbb{Z}$-parametrizable, then the first case of lemma 5.3.2 holds: in equation (5.2) the polynomial $Q(\underline{X})$ belongs to $\mathbb{Z}_{(2)}[\underline{X}]$. Moreover, if $Q(\underline{X}) = \frac{a_0+2R(\underline{X})}{D}$ such that $a_0 \equiv 1 \pmod 2$ we have that

$$g(\underline{X}) = f(Q(\underline{X})) = f(-Q(\underline{X}) + \beta) = f\left(\frac{2R(\underline{X}) + a_0 + a'}{D}\right)$$

since $f(X) = f(-X + \beta)$, with $\beta \in \mathbb{Z}^*_{(2)}$, and $D\beta \in \mathbb{Z}$. Observe that $a' \equiv 1 \pmod 2$. Hence in any case we may assume that $Q(\underline{X}) \in 2\mathbb{Z}_{(2)}[\underline{X}]$, that is $Q(\underline{X}) = 2R(\underline{X})/D$. Moreover we have

$$\mathbb{Z} = T_0 \cup T_1 \cup T \tag{5.9}$$

where $T_0 \subset 2\mathbb{Z}$, $T_1 \subset 2\mathbb{Z} + 1$ and $T = \bigcup_{i \in I'} T_i$ has zero density.

If $n \in T_0$ then $n = 2k$ for some $k \in \mathbb{Z}$; by (5.4) we have for all $k \in \mathbb{Z}$ except for a set of density zero that

$$Dk = R(\underline{x}) \tag{5.10}$$

for some $\underline{x} \in \mathbb{Z}^m$.

If $n \in T_1$ then $n = 2k + 1$ for some $k \in \mathbb{Z}$; by (5.6) we have for all $k \in \mathbb{Z}$ except for a set of density zero that

$$Dk = -R(\underline{x}) + (D\beta - D)/2 \tag{5.11}$$

for some $\underline{x} \in \mathbb{Z}^m$.

We set $\alpha \doteqdot (D\beta - D)/2 \in \mathbb{Z}$ and we remark that $\alpha \not\equiv 0 \pmod D$.

Corollary 5.4.3 *Let $f \in \mathrm{Int}(\mathbb{Z})$ be of the form $f(X) = F(X)/N$ where $N \in \mathbb{N}$ and let $F \in \mathbb{Z}[X]$ be such that $(N, cont(F)) = 1$. If there exists a prime p different from 2 such that $p|N$ then $f(\mathbb{Z})$ is not $\mathbb{Z}$-parametrizable.*

Proof : Suppose that $f(\mathbb{Z})$ is $\mathbb{Z}$-parametrizable and let p be a prime factor of N, different from 2. Since $\mathrm{Int}(\mathbb{Z})$ is a $\mathbb{Z}$-module then $g(X) = \frac{N}{p} f(X) \in \mathrm{Int}(\mathbb{Z})$ and $g(\mathbb{Z})$ is $\mathbb{Z}$-parametrizable, too. But this is in contradiction with proposition 5.4.2. $\square$

5.4.1 Case $f(\mathbb{Z}) = g(\mathbb{Z})$, with $g \in \mathbb{Z}[X]$

In this section we characterize integer valued polynomials $f(X)$ such that $f(\mathbb{Z})$ is parametrizable with an integer coefficient polynomial $g(X)$ in one variable.

If $f \in \mathrm{Int}(\mathbb{Z})$ is such that $f(\mathbb{Z}) = g(\mathbb{Z})$ for some $g \in \mathbb{Z}[X]$, then there exists $\beta \in \mathbb{Z} - 2\mathbb{Z}$ such that $f(X) = f(-X + \beta)$, as the following corollary shows.

Corollary 5.4.4 *Let $f \in \mathrm{Int}(\mathbb{Z}) - \mathbb{Z}[X]$ be of the form $f(X) = F(X)/2^a$, where $F \in \mathbb{Z}[X] - 2\mathbb{Z}[X]$ and $a \in \mathbb{N} - \{0\}$.*

If there exists $\beta \in \mathbb{Z}^*_{(2)} - \mathbb{Z}$ (that is: β is the ratio of two odd integers) such that $f(X) = f(-X + \beta)$ then $f(\mathbb{Z})$ is not $\mathbb{Z}$-parametrizable with an integer coefficient polynomial in one variable.

If $f(\mathbb{Z}) = g(\mathbb{Z})$ for some $g \in \mathbb{Z}[X]$ then there exists an odd integer b such that $f(X) = f(-X + b)$ and $g'(X) \doteqdot f(2X) \in \mathbb{Z}[X]$ is such that $f(\mathbb{Z}) = g'(\mathbb{Z})$.

Proof : Suppose that there exists $\beta \in \mathbb{Z}^*_{(2)} - \mathbb{Z}$ such that $f(X) = f(-X + \beta)$.

We remark that

$$f(X) - f(Y) = (X - Y)(X + Y - \beta) \prod_{i \in I} g_i(X, Y) \tag{5.12}$$

where for each $i \in I$ the polynomial $g_i \in \mathbb{Q}[X, Y]$ is irreducible and $\deg_Y(g_i) \geq 2$.

Suppose also that there exists $g \in \mathbb{Z}[X]$ such that $f(\mathbb{Z}) = g(\mathbb{Z})$. Then by Hilbert's Irreducibility theorem there exist $\alpha, \delta \in \mathbb{Q}$ such that

$$g(X) = f(\alpha X + \delta)$$

Moreover lemma 5.3.2 and proposition 5.4.2 imply that $\alpha, \delta \in \mathbb{Z}_{(2)}$, with $\alpha \in 2\mathbb{Z}_{(2)}$. Let us write $\alpha = \alpha_1/\alpha_2$, with $(\alpha_1, \alpha_2) = 1$, and $\alpha_2 \equiv 1 \pmod 2$. Without loss of generality we may suppose also that $\alpha_2, \alpha_1 > 0$ (if $g(X)$ parametrizes $f(\mathbb{Z})$ then also $g(-X)$ parametrizes $f(\mathbb{Z})$).

Since $f(\mathbb{Z}) \subset g(\mathbb{Z})$ we have that for each $n \in \mathbb{Z}$ there exist $m \in \mathbb{Z}$ such that

$$f(n) = g(m) = f(\alpha m + \delta)$$

We define the sets of integers

$$T_0 \doteqdot \{n \in \mathbb{Z} |\ n = \alpha m + \delta \text{ for some } m \in \mathbb{Z}\}$$

$$T_1 \doteqdot \{n \in \mathbb{Z} |\ n + \alpha m + \delta = \beta \text{ for some } m \in \mathbb{Z}\}$$

$$T_2 \doteqdot \{n \in \mathbb{Z} | \exists\, i \in I, m \in \mathbb{Z}\, s.t.\, g_i(n, \alpha m + \delta) = 0\}$$

By (5.12) we have $\mathbb{Z} = T_0 \cup T_1 \cup T_2$; by Siegel's theorem 5.1.4, T_2 is a subset of $\mathbb{Z}$ of zero density. We saw in the proof of proposition 5.4.2 (see also (5.9)) that T_0 and T_1 cannot be empty.

For $n \in T_0$ there exists $m \in \mathbb{Z}$ such that $n = \alpha m + \delta$; if we multiply this last equation by α_2 we have that $\alpha_2\delta \in \mathbb{Z}$.

For $n \in T_1$ there exists $m \in \mathbb{Z}$ such that $n + \alpha m + \delta = \beta$. Hence $\alpha_2\beta \in \mathbb{Z}$, as we have already seen in proposition 5.4.2. Since we are assuming that $\beta \notin \mathbb{Z}$ and α_2 is an odd integer we have that $\alpha_2 \geq 3$.

Since $g(\mathbb{Z}) \subset f(\mathbb{Z})$ we have that for each $n \in \mathbb{Z}$ there exist $m \in \mathbb{Z}$ such that

$$g(n) = f(\alpha n + \delta) = f(m)$$

Like before we define the sets of integers

$$S_0 \doteqdot \{n \in \mathbb{Z} |\ \alpha n + \delta = m \text{ for some } m \in \mathbb{Z}\}$$

$$S_1 \doteqdot \{n \in \mathbb{Z} |\ \alpha n + \delta + m = \beta \text{ for some } m \in \mathbb{Z}\}$$

$$S_2 \doteqdot \{n \in \mathbb{Z} |\ \exists\, i \in I, m \in \mathbb{Z}\, s.t.\, g_i(\alpha n + \delta, m) = 0\}$$

By (5.12) we have $\mathbb{Z} = S_0 \cup S_1 \cup S_2$. For all $i \in I$ we define $g_i'(X, Y) \doteqdot g_i(\alpha X + \delta, Y) \in \mathbb{Q}[X, Y]$ which is an irreducible polynomial of degree in Y greater or equal to 2; by Siegel's theorem 5.1.4, S_2 is a subset of $\mathbb{Z}$ of zero density.

If $n \in S_0$ we have $\alpha n + \delta \in \mathbb{Z}$, hence $\alpha_1 n + \delta\alpha_2 \equiv 0 \pmod{\alpha_2}$ (remember that $\delta\alpha_2 \in \mathbb{Z}$), so

$$n \equiv -\delta\alpha_2 k \pmod{\alpha_2}$$

where $k \in \mathbb{Z}$, $k\alpha_1 \equiv 1 \pmod{\alpha_2}$ (such k exists since α_1 and α_2 are coprime).

For each $n \in S_1$ we have $\alpha n + \delta - \beta \in \mathbb{Z}$ so

$$n \equiv -\delta\alpha_2 k + \beta\alpha_2 k \pmod{\alpha_2}$$

(remember that $\beta\alpha_2 \in \mathbb{Z}$).

Since $\alpha_2 \geq 3$ there are residue class modulo α_2 which are not covered by S_0 or S_1: contradiction.

In particular, if $f \in \mathrm{Int}(\mathbb{Z}) - \mathbb{Z}[X]$ is such that $f(\mathbb{Z}) = g(\mathbb{Z})$ with $g \in \mathbb{Z}[X]$, then there exists an odd integer β such that $f(X) = f(-X + \beta)$. Moreover $g(X) = f(\alpha X + \delta)$, where $\alpha = 2$ and $\delta \in \mathbb{Z}$. In fact $\alpha \in \mathbb{Z}$ (otherwise S_0, S_1, S_2 do not cover $\mathbb{Z}$), which implies that $\delta \in \mathbb{Z}$, since for each $n \in T_0$ we have that $n - \alpha m = \delta$, for some $m \in \mathbb{Z}$. Moreover for each $n \in T_0$ we have that $n \equiv -\delta \pmod{\alpha}$ and for each $n \in T_1$ we have that $n \equiv \beta - \delta \pmod{\alpha}$. If $\alpha \neq 2$ there are residue classes which are not covered by T_0 and T_1.

We may also assume that $\delta = 0$. In fact in general if $f \in \mathbb{Q}[X]$ such that $f(X) = f(b - X)$ for some odd integer $b = 2m + 1$ then $f(2X + \delta) \in \mathbb{Z}[X]$ for some integer δ if and only if $f(2X) \in \mathbb{Z}[X]$. If $\delta \equiv 0 \pmod{2}$ then $f(2X + \delta) = f(2(X + k)) \doteqdot g(X) \in \mathbb{Z}[X]$; then

$g(X-k) = f(2X) \in \mathbb{Z}[X]$. If $\delta \equiv 1 \pmod 2$ then $f(2X+\delta) = f(2(X+k)+1) \div g(X) \in \mathbb{Z}[X]$; then $g(-X-k+m) = f(-2X+b) \in \mathbb{Z}[X]$. And this implies that $f(2X) \in \mathbb{Z}[X]$. Finally it is easy to observe that if $g(X) = f(2X+\delta)$ parametrizes $f(\mathbb{Z})$ for some $\delta \in \mathbb{Z}$ then $h(X) = f(2X+\delta') \in \mathbb{Z}[X]$ parametrizes $f(\mathbb{Z})$ for every $\delta' \in \mathbb{Z}$. □

Proposition 5.4.5 *Let $f \in \mathrm{Int}(\mathbb{Z}) - \mathbb{Z}[X]$.*

Then $f(\mathbb{Z}) = g(\mathbb{Z})$ for some polynomial $g \in \mathbb{Z}[X]$ if and only if there exists an odd integer b such that $f(X) = f(-X+b)$ and $f(2X) \in \mathbb{Z}[X]$.

Proof : If $f(\mathbb{Z}) = g(\mathbb{Z})$ with $g \in \mathbb{Z}[X]$, then there exists $b \in \mathbb{Z} - 2\mathbb{Z}$ such that $f(X) = f(-X+b)$ (proposition 5.4.2 and corollary 5.4.4). We can assume that $g(X) = f(2X)$ (see corollary 5.4.4).

If there exists an odd integer b such that $f(X) = f(-X+b)$ and $f(2X) \in \mathbb{Z}[X]$ then we define $g(X) \div f(2X)$. We have that $\mathbb{Z} = (2\mathbb{Z}) \cup (2\mathbb{Z}+1)$, so $f(\mathbb{Z}) = f(2\mathbb{Z}) \cup f(2\mathbb{Z}+1)$.

We have $f(h(X)) = f(X)$, where $h(X) = -X+b$. Then

$$f(2\mathbb{Z}) = f(h(2\mathbb{Z})) = f(2\mathbb{Z}+1)$$

So $f(\mathbb{Z}) = g(\mathbb{Z})$. □

Note that for all $f \in \mathrm{Int}(\mathbb{Z})$ of the form $f(X) = F(X)/2$ we have that $f(2X) \in \mathbb{Z}[X]$.

If $f(X) = F(X)/2^n$, $n > 1$, the condition $f(X) = f(b-X)$, for some integer $b \equiv 1 \pmod 2$ is not sufficient in order for $f(\mathbb{Z})$ to be equal to $g(\mathbb{Z})$, for some $g \in \mathbb{Z}[X]$.
For example take the polynomial $f(X) = X(X-1)(X-2)(X-3)/8$.

Lemma 5.4.6 *Let $b \in \mathbb{Z}$. Then we have*

$$\{f \in \mathbb{Z}[X] \mid f(X) = f(-X+b)\} = \mathbb{Z}[X(b-X)]$$

Proof : The inclusion $\supset$ is obvious.

Let $f \in \mathbb{Z}[X]$ be such that $f(X) = f(-X+b)$. We remark that the degree n of $f(X)$ is an even integer $2m$. We prove that $f \in \mathbb{Z}[X(b-X)]$ by induction on m.

Since the map $\sigma : X \mapsto -X+b$ is a homomorphism of the ring $\mathbb{Z}[X]$ in itself, we may suppose that $f(0) = f(b) = 0$ (we write $f(X) = (f(X) - f(0)) + f(0)$).
If $m = 1$ we obviously have that $f(X) = aX(b-X)$, for some $a \in \mathbb{Z}$. Let now the statement holds for every polynomial of degree less than $2m$ and take a polynomial $f(X)$ of degree $2(m+1)$ such that $f(X) = f(-X+b)$. We have that

$$f(X) = X(b-X)g(X)$$

where $g(X) \in \mathbb{Z}[X]$ of degree $2m$ such that $g(X) = g(-X+b)$, since $\sigma(X(b-X)) = X(b-X)$. By inductive hypothesis $g(X) = P(X(b-X))$, for some $P \in \mathbb{Z}[T]$. The lemma is proved. □

Lemma 5.4.7 *Let b be an odd integer and a a positive integer. Let $f(X) = F(X)/2^a$, where $F \in \mathbb{Z}[X] - 2\mathbb{Z}[X]$, $F(X) = F(-X+b)$, such that $f(2X) \in \mathbb{Z}[X]$.*
Then $a \leq \deg(f)/2$.

Proof : We remark that the degree of f is an even integer $2m$. We prove that $a \leq m$ by induction on m. Let $m = 1$, then by lemma 5.4.6

$$f(X) = \frac{F(X)}{2^a} = \frac{A_1(X(b-X)) + A_0}{2^a}$$

where $A_0, A_1 \in \mathbb{Z}$. By hypothesis on $F(X)$ we have that A_1 and A_0 are not both even integer. So

$$f(2X) = \frac{A_1(2X(b-2X)) + A_0}{2^a} = \frac{A_1}{2^{a-1}} X(b-2X) + \frac{A_0}{2^a}$$

This polynomial belongs to $\mathbb{Z}[X]$ if and only if $a = 1$ (note that since $A_0 \equiv 0 \pmod{2^a}$ then $A_1 \equiv 1 \pmod 2$; moreover $b \equiv 1 \pmod 2$, so $b - 2X$ is primitive).

Let now the statement holds for those polynomial $f(X)$ of degree less or equal to $2m$ and consider now $f(X) = F(X)/2^a$ of degree $2(m+1)$. If $a = 1$ we are done. Suppose now $a > 1$.

We have that

$$f(X) = \frac{F(X)}{2^a} = \frac{X(b-X)}{2} \frac{G(X)}{2^{a-1}} + \frac{F(0)}{2^a}$$

where $G \in \mathbb{Z}[X]$ of degree $2m$ such that $G(X) = G(b-X)$. Since $f(2X) \in \mathbb{Z}[X]$ we have that $F(0)/2^a \in \mathbb{Z}$; hence $G \notin 2\mathbb{Z}[X]$. We have

$$f(2X) = \frac{2X(b-2X)}{2} \frac{G(2X)}{2^{a-1}} + \frac{F(0)}{2^a} = X(b-2X) \frac{G(2X)}{2^{a-1}} + \frac{F(0)}{2^a}$$

and this belongs to $\mathbb{Z}[X]$ if and only if $G(2X)/2^{a-1} \in \mathbb{Z}[X]$ (since $X(b-2X)$ is primitive). By inductive hypothesis applied to the polynomial $G(X)/2^{a-1}$ we have that $a - 1 \leq m$. The lemma is proved. □

Lemma 5.4.8 *Let $f \in \mathbb{Q}[X]$, $f(X) = F(X)/N$ where $N \in \mathbb{Z}$, $F \in \mathbb{Z}[X]$ such that $(N, cont(F)) = 1$. Let $f(2X) \in \mathbb{Z}[X]$. If p is a prime different from 2 then $p \nmid N$.*

Proof : We remark that $f(2X) \in \mathbb{Z}[X]$ if and only if $F(2X) \in N\mathbb{Z}[X]$.

Let us write $F(X) = a_n X^n + \ldots + a_0$, where $a_i \in \mathbb{Z}$ for $i = 0, \ldots, n$.

By hypothesis for each prime q which divides N we have that $\|F\|_q = \max\{|a_i|_q\} = 1$.

Suppose now that there exists a prime p different from 2 such that $p|N$.
If $G(X) \doteq F(2X)$ we have $\|G\|_p = \max\{|a_i 2^i|_p\} = \max\{|a_i|_p\} = 1$. Hence $G \notin q\mathbb{Z}[X]$, so $G \notin N\mathbb{Z}[X]$: contradiction. □

Lemma 5.4.9 *Let $f \in \mathbb{Q}[X]$ be such that $f(X) = f(-X+b)$ for some odd integer b and $f(2X) \in \mathbb{Z}[X]$. Then $f \in \mathrm{Int}(\mathbb{Z})$.*

Proof : We have to prove that $f(\mathbb{Z}) \subset \mathbb{Z}$. The proof easily follows from the fact that

$$f(\mathbb{Z}) = f(2\mathbb{Z}) \cup f(2\mathbb{Z}+1)$$

It is clear that $f(2\mathbb{Z}) \subset \mathbb{Z}$. We have to show that $f(2\mathbb{Z}+1) \subset \mathbb{Z}$. But this follows from the fact that $f(2\mathbb{Z}+1) = f(2\mathbb{Z}+1+b) = f(2\mathbb{Z})$. □

We summarize the previous three lemmas in the following proposition.

Proposition 5.4.10 *Let $f \in \mathbb{Q}[X]$ be such that $f(X) = f(-X+b)$ for some odd integer b and $f(2X) \in \mathbb{Z}[X]$. Then we have that $f \in \mathrm{Int}(\mathbb{Z})$ and $f(X) = F(X)/2^a$ for some integer a such that $0 \leq a \leq \deg(f)/2$.*

Note that if $f \in \mathrm{Int}(\mathbb{Z})$, $f(X) = F(X)/2^a$ such that $f(X) = f(b-X)$ for some integer b it is not true in general that $f \in \mathbb{Z}[X(b-X)/2]$. Take for example the polynomial

$$f(X) = \frac{X(X-1)(X-2)(X-3)}{8}$$

which satisfies $f(X) = f(3-X)$ but does not belong to $\mathbb{Z}[X(3-X)/2]$.

Proposition 5.4.11 *Let b be an odd integer. Then we have*

$$\{f \in \mathrm{Int}(\mathbb{Z}) \mid f(X) = f(-X+b), f(2X) \in \mathbb{Z}[X]\} = \mathbb{Z}\left[\frac{X(b-X)}{2}\right]$$

Proof : Let us call $\mathcal{S}_b$ the set of the left member.

If $f \in \mathbb{Z}[X(b-X)/2]$ it is clear that $f \in \mathcal{S}_b$.

Let now $f \in \mathcal{S}_b$. Observe that $\deg(f) = 2m$ for some $m \in \mathbb{N}$.

By lemma 5.4.8 we have that $f(X) = F(X)/2^a$, for some $a \in \mathbb{N}$ and $F \in \mathbb{Z}[X]$. If $a \geq 1$ we assume that $F \notin 2\mathbb{Z}[X]$, that is $f(X)$ is written in reduced form.

We prove by induction on m that $f \in \mathbb{Z}[X(b-X)/2]$.

Let $m = 1$; if $a = 0$ we are done, since $\mathbb{Z}[X(b-X)] \subset \mathbb{Z}[X(b-X)/2]$. Suppose that $a \geq 1$; by lemma 5.4.6 we have $F(X) = A_1X(b-X) + A_0$ for some $A_0, A_1 \in \mathbb{Z}$. Then

$$f(X) = A_1\frac{X(b-X)}{2^a} + \frac{A_0}{2^a}$$

Since $f(2X) \in \mathbb{Z}[X]$ we have that $A_0 \equiv 0 \pmod 2$, so $A_1 \equiv 1 \pmod 2$ (because $F \notin 2\mathbb{Z}[X]$). In particular $a = 1$, so $f \in \mathbb{Z}[X(b-X)/2]$.

Let now the statement holds for those polynomial in $\mathcal{S}_b$ of degree less or equal to $2m$ and take a polynomial $f \in \mathcal{S}_b$ of degree $2(m+1)$. If $a = 0$ we are done; otherwise we have (again by lemma 5.4.6):

$$f(X) = \frac{X(b-X)}{2}\frac{G(X)}{2^{a-1}} + \frac{A_0}{2^a}$$

where $A_0 \in \mathbb{Z}$ and $G \in \mathbb{Z}[X]$ of degree $2m$, such that $G(X) = G(-X+b)$. As before $A_0 \equiv 0 \pmod 2$, so $G \notin 2\mathbb{Z}[X]$. We set $g(X) \doteq G(X)/2^{a-1}$.

We have

$$f(2X) = X(b-2X)\frac{G(2X)}{2^{a-1}} + \frac{A_0}{2^a}$$

and this polynomial belongs to $\mathbb{Z}[X]$ if and only if $g(2X) = G(2X)/2^{a-1} \in \mathbb{Z}[X]$ (the polynomial $X(b-2X)$ is primitive). We summarize the properties of $g(X)$:

- $g \in \mathrm{Int}(\mathbb{Z})$, by lemma 5.4.9
- $g(X) = g(-X+b)$
- $g(2X) \in \mathbb{Z}[X]$

Therefore we may apply inductive hypothesis to $g(X)$: $g(X) = P(X(b-X)/2)$, for some $P \in \mathbb{Z}[T]$. Hence $f(X) = P'(X(b-X)/2)$, where $P'(T) = TP(T) + F(0)$.

The proposition is proved. □

The following theorem characterizes integer valued polynomials $f(X)$ such that $f(\mathbb{Z}) = g(\mathbb{Z})$ for some $g \in \mathbb{Z}[X]$.

Theorem 5.4.12 *We have*

$$\{f \in \mathrm{Int}(\mathbb{Z}) |\ f(\mathbb{Z}) = g(\mathbb{Z}) \text{ for some } g \in \mathbb{Z}[X]\} = \mathbb{Z}[X] \bigcup \left(\bigcup_{b \in 2\mathbb{Z}+1} \mathbb{Z}\left[\frac{X(b-X)}{2}\right] \right)$$

Proof : If $f \in \mathbb{Z}[X(b-X)/2]$, where b is an odd integer, then $f \in \mathrm{Int}(\mathbb{Z})$. We also have that $f(X) = f(-X+b)$ and $f(2X) \in \mathbb{Z}[X]$, so by proposition 5.4.5 we are done.

Conversely let $f \in \mathrm{Int}(\mathbb{Z}) - \mathbb{Z}[X]$ (the case $f \in \mathbb{Z}[X]$ is obvious) be such that $f(\mathbb{Z}) = g(\mathbb{Z})$ for some $g \in \mathbb{Z}[X]$. We saw in proposition 5.4.5 that there exists an odd integer b such that $f(X) = f(-X+b)$ and $f(2X) \in \mathbb{Z}[X]$. By proposition 5.4.11 we have $f \in \mathbb{Z}[X(b-X)/2]$. The theorem is proved. □

5.4.2 General case

In this last section we show that there exist integer valued polynomials $f(X)$ such that $f(\mathbb{Z})$ is $\mathbb{Z}$-parametrizable with an integer coefficient polynomial $g(\underline{X})$ which has more than one variable, but $f(\mathbb{Z}) \neq g(\mathbb{Z})$ for every $g \in \mathbb{Z}[X]$.

Lemma 5.4.13 *Let $f(X) = p^k X(p^k X - a)/2$, where p is a prime different from 2, k a positive integer and a an odd integer such that $(a, p) = 1$. Then $f \in \mathrm{Int}(\mathbb{Z})$ and $f(\mathbb{Z})$ is $\mathbb{Z}$-parametrizable.*

Proof : It is easy to verify that $f \in \mathrm{Int}(\mathbb{Z})$, since a and p are odd.
We define the polynomial

$$Q(X_1, X_2) \doteqdot \frac{2}{p^k}(p^k X_1 + \gamma(X_2^{k(p-1)} - 1)^k)$$

where $\gamma \in \mathbb{Z}$ is such that $(-1)^k \gamma \equiv \alpha \pmod{p^k}$, with $\alpha \doteqdot (a - p^k)/2 \in \mathbb{Z}$. Let us write $\alpha - (-1)^k \gamma = p^k A$, for some $A \in \mathbb{Z}$.
We define $g(X_1, X_2) \doteqdot f(Q(X_1, X_2))$. It is easy to check that $g \in \mathbb{Z}[X_1, X_2]$.
We state that $f(\mathbb{Z}) = g(\mathbb{Z}^2)$. We remark that

$$f(X) - f(Y) = \frac{p^k}{2}(X - Y)(p^k X + p^k Y - a) = \frac{p^{2k}}{2}(X - Y)(X + Y - \frac{a}{p^k})$$

Let $n \in \mathbb{Z}$; we claim that there exists $\underline{m} = (m_1, m_2) \in \mathbb{Z}^2$ such that

$$f(n) = g(m_1, m_2) = f(Q(m_1, m_2))$$

If $n = 2h$ for some $h \in \mathbb{Z}$, then we set $\underline{m} = (h, 1)$; in this case we have that

$$n = Q(\underline{m})$$

If $n = 2h + 1$ for some $h \in \mathbb{Z}$, then we set $\underline{m} = (-h + A, 0)$; in this case we have

$$n = -Q(\underline{m}) + \frac{a}{p^k}$$

Conversely, let $\underline{m} = (m_1, m_2) \in \mathbb{Z}^2$. Then there exists $n \in \mathbb{Z}$ such that

$$g(\underline{m}) = f(Q(\underline{m})) = f(n)$$

In fact if $m_2 \not\equiv 0 \pmod{p}$ then $((m_2^k)^{p-1} - 1)^k \equiv 0 \pmod{p^k}$, by Fermat's little theorem. Therefore

$$Q(\underline{m}) = \frac{2}{p^k}(p^k m_1 + p^k M) = 2(m_1 + M)$$

for some $M \in \mathbb{Z}$. We choose $n = 2(m_1 + M)$ so we have that

$$Q(\underline{m}) = n$$

If $m_2 \equiv 0 \pmod{p}$ then $m_2^{k(p-1)} \equiv 0 \pmod{p^k}$, and so $(m_2^{k(p-1)} - 1)^k \equiv (-1)^k \pmod{p^k}$. Hence

$$Q(\underline{m}) = \frac{2}{p^k}(p^k m_1 + (-1)^k \gamma + p^k M)$$

for some $M \in \mathbb{Z}$. We choose $n = 2(-m_1 - M + A) + 1$ so we have that

$$Q(\underline{m}) = -n + \frac{a}{p^k}$$

The lemma is proved. □

If $f(X) = p^k X(p^k X - a)/2$ with $k \geq 1$, we remark that $f(X) = f(-X + a/p^k)$. Hence by corollary 5.4.4 the set $f(\mathbb{Z})$ is not equal to $g(\mathbb{Z})$, for every $g \in \mathbb{Z}[X]$. We can also use theorem 5.4.12: since $f(X)$ does not belong to $\mathbb{Z}[X(b - X)/2]$, for every odd integer b, then $f(\mathbb{Z}) \neq g(\mathbb{Z})$, for every $g \in \mathbb{Z}[X]$.

Corollary 5.4.14 *Let p be an odd prime, k a non negative integer and a an odd integer, coprime with p. Then*

$$\mathbb{Z}\left[\frac{p^k X(p^k X - a)}{2}\right] \subset \{f \in \mathrm{Int}(\mathbb{Z}) |\ f(\mathbb{Z}) \text{ is } \mathbb{Z}\text{-parametrizable}\}$$

Proof : The statement follows easily from the previous lemma and from the fact that if $f(\mathbb{Z})$ is $\mathbb{Z}$-parametrizable and $P \in \mathbb{Z}[X]$, then $P(f(\mathbb{Z}))$ is $\mathbb{Z}$-parametrizable. □

Lemma 5.4.15 *Let $f(X) = bX(bX - a)/2$, where a and b are odd coprime integers, both different from zero.*
If $f(\mathbb{Z})$ is $\mathbb{Z}$-parametrizable then $b = p^k$, where p is a prime and $k \in \mathbb{Z}$, $k \geq 0$.

Proof : Note that $f \in \mathrm{Int}(\mathbb{Z})$ and $f(X) = f(-X + \beta)$, where $\beta = a/b$.

Suppose that $b = b_1 b_2$, where $b_1, b_2 \in \mathbb{Z} - \{\pm 1\}$ such that $(b_1, b_2) = 1$. Suppose also that $f(\mathbb{Z}) = g(\mathbb{Z}^m)$, for some $g \in \mathbb{Z}[X_1, \ldots, X_m] = \mathbb{Z}[\underline{X}]$.

We saw in proposition 5.4.2 that $g(\underline{X}) = f(2R(\underline{X})/D)$, for some $R \in \mathbb{Z}[\underline{X}]$ and $D \in \mathbb{Z}$ which is odd and $(D, cont(R)) = 1$ (see also the remarks after proposition 5.4.2).

Since $g(\mathbb{Z}^m) \subset f(\mathbb{Z})$ we have that for each $\underline{x} \in \mathbb{Z}^m$ there exists $n \in \mathbb{Z}$ such that

$$g(\underline{x}) = f(Q(\underline{x})) = f(n)$$

where $Q(\underline{X}) = 2R(\underline{X})/D$.

We have that $f(X) - f(Y) = (b^2/2)(X - Y)(X + Y - \beta)$. Hence

$$f(Q(\underline{X})) - f(Y) = \frac{b^2}{2}(Q(\underline{X}) - Y)(Q(\underline{X}) + Y - \beta)$$

We define the sets

$$S_0 \doteqdot \{\underline{x} \in \mathbb{Z}^m \mid Q(\underline{x}) = m \text{ for some } m \in \mathbb{Z}\} = \{\underline{x} \in \mathbb{Z}^m \mid R(\underline{x}) = Dk \text{ for some } k \in \mathbb{Z}\}$$

$$S_1 \doteqdot \{\underline{x} \in \mathbb{Z}^m \mid Q(\underline{x}) = -m + \beta \text{ for some } m \in \mathbb{Z}\} = \{\underline{x} \in \mathbb{Z}^m \mid R(\underline{x}) = -Dk + \alpha \text{ for some } k \in \mathbb{Z}\}$$

where $\alpha = (D\beta - D)/2 \in \mathbb{Z}$ (see also (5.10) and (5.11)). So $\mathbb{Z}^m = S_0 \cup S_1$.
We recall that since $f(\mathbb{Z}) \subset g(\mathbb{Z}^m)$ then $\mathbb{Z} = T_0 \cup T_1$, where

$$T_0 = \{n \in \mathbb{Z} \,|\, n = Q(\underline{x}) \text{ for some } \underline{x} \in \mathbb{Z}^m\}$$

$$T_1 = \{n \in \mathbb{Z} \,|\, n = -Q(\underline{x}) + \beta \text{ for some } \underline{x} \in \mathbb{Z}^m\}$$

We remark that $S_i \neq \emptyset$ since $T_i \neq \emptyset$, for $i = 0, 1$. Moreover, if $i \in \{0, 1\}$ and $\underline{x} \in S_i$, then $\underline{x}' \in S_i$ for all $\underline{x}' \equiv \underline{x} \pmod{D}$ (which means $x'_j \equiv x_j \pmod{D}$ for all $j = 1, \ldots, m$).

Since T_1 is not empty we saw in (5.6) that $D\beta \in \mathbb{Z}$, that is $D = bb' = b_1b_2b'$, where $b' \in \mathbb{Z}$. Moreover $\alpha \not\equiv 0 \pmod{D}$ (see remarks after proposition 5.4.2) and $\alpha = b'(a - b)/2$ with $(b, (a - b)/2) = 1$; we can find two coprime factors d_1, d_2 of D such that $D = d_1d_2$ and $\alpha \not\equiv 0 \pmod{d_i}$ for $i = 1, 2$.

Let $\underline{x} \in S_0$, that is $R(\underline{x}) \equiv 0 \pmod{D}$: then $R(\underline{x}) \equiv 0 \pmod{d_1}$.
So $R(\underline{x}') \equiv 0 \pmod{d_1}$ for all $\underline{x}' \equiv \underline{x} \pmod{d_1}$. For such $\underline{x}'$'s we have that $\underline{x}' \notin S_1$, since $\alpha \not\equiv 0 \pmod{d_1}$. So $\underline{x}' \in S_0$ for all $\underline{x}' \equiv \underline{x} \pmod{d_1}$.

Therefore $R(\underline{x}') \equiv 0 \pmod{d_2}$ for all $\underline{x}' \equiv \underline{x} \pmod{d_1}$.

We state that for all $\underline{y} \in \mathbb{Z}^m$ we have $R(\underline{y}) \equiv 0 \pmod{d_2}$. In fact if we consider the natural projection map

$$\pi_1 : \mathbb{Z}^m \to (\mathbb{Z}/d_1\mathbb{Z})^m$$

and the isomorphism (because $(d_2, d_1) = 1$)

$$\begin{array}{rccc} \Phi: & (\mathbb{Z}/d_1\mathbb{Z})^m & \to & (\mathbb{Z}/d_1\mathbb{Z})^m \\ & \underline{x} & \mapsto & d_2\underline{x} \end{array}$$

We have

$$\pi_1(\underline{y} - \underline{x}) = \Phi(\pi_1((\widetilde{\underline{x}})) = d_2\pi_1(\widetilde{\underline{x}})$$

for some $\widetilde{\underline{x}} \in \mathbb{Z}^m$. Hence

$$\underline{y} - \underline{x} = d_2\widetilde{\underline{x}} + d_1\widetilde{\underline{x}}'$$

for some $\widetilde{\underline{x}}' \in \mathbb{Z}^m$. If we set $\underline{x}' \doteqdot \underline{x} + d_1\widetilde{\underline{x}}'$, we have that $R(\underline{y}) \equiv R(\underline{x}')\pmod{d_2}$. But $\underline{x}' \equiv \underline{x} \pmod{d_1}$, so $R(\underline{y}) \equiv 0 \pmod{d_2}$. Since $\alpha \not\equiv 0 \pmod{d_2}$ this would imply that S_1 is empty, contradiction. □

For example this lemma shows that the polynomial $f(X) = 15X(15X-1)/2$ is in $\mathrm{Int}(\mathbb{Z})$, $f(X) = f(-X + 1/15)$ but $f(\mathbb{Z})$ is not $\mathbb{Z}$-parametrizable.

From corollary 5.4.14 and the previous lemma we can state the following conjecture.

Conjecture
We have

$$\{f \in \mathrm{Int}(\mathbb{Z}) |\ f(\mathbb{Z}) \text{ is } \mathbb{Z}\text{-parametrizable}\} = \mathbb{Z}[X] \bigcup \left(\bigcup_{\substack{a \in 2\mathbb{Z}+1,\ p \neq 2 \\ (a,p)=1,\ k \geq 0}} \mathbb{Z}\left[\frac{p^k X(p^k X - a)}{2}\right] \right)$$

where p runs over the set of odd primes.

The inclusion $\supset$ follows from corollary 5.4.14.

If $f \in \mathrm{Int}(\mathbb{Z}) - \mathbb{Z}[X]$ is such that $f(\mathbb{Z}) = g(\mathbb{Z}^m)$ for some $g \in \mathbb{Z}[\underline{X}]$, then proposition 5.4.2 shows that:

- $f(X) = F(X)/2^n$ for some $n \geq 1$ and $F \in \mathbb{Z}[X] - 2\mathbb{Z}[X]$
- there exists $\beta \in \mathbb{Z}_{(2)}^*$ such that $f(X) = f(-X + \beta)$

5.5 Number field case

We give a conjecture in the number field case.

Let K be a number field with ring of integers O_K. We define the set

$$\mathrm{Int}(O_K) = \{f \in K[X] \mid f(O_K) \subset O_K\}$$

Definition 5.5.1 *Let $f \in K[X]$ be an integer-valued polynomial, that is $f \in \mathrm{Int}(O_K)$. We say that $f(O_K)$ is O_K-**parametrizable** if there exists $m \in \mathbb{N}$ and a polynomial $g \in O_K[\underline{X}]_K[X_1, \ldots, X_m]$ such that $f(O_K) = g(O_K^m)$.*

This lemma is a generalization of lemma 5.3.2.

Lemma 5.5.2 *Let $f \in O_K[X]$, $g \in O_K[\underline{X}]$, $a \in K$ such that*

$$f(Q(\underline{X})) = ag(\underline{X})$$

Let v be a non archimedean valuation of K with uniformizer π and valuation ring O_v such that $v(a) \geq 1$, $\|f\|_v = 1$.

Then there are two possibilities: either

$$Q(\underline{X}) = \frac{a_0 + \pi R(\underline{X})}{D}$$

where $a_0 \in O_v$, $D \in O_v^*$, $R \in O_v[\underline{X}]$, $R(\underline{0}) = 0$ or there exist algebraic numbers ξ, π' in the splitting field K' of f over K, a valuation v' of K' above v with valuation ring $O_{v'}$ such that $v(\pi') = 1$ and $\xi \notin O_{v'}$, and a polynomial $R(\underline{X}) \in O_{v'}[\underline{X}]$ such that

$$Q(\underline{X}) = \xi(1 + \pi' R(\underline{X})).$$

Conjecture:

Let $f \in \mathrm{Int}(O_K) - O_K[X]$ be of the form $f(X) = F(X)/a$, where $F \in O_K[X]$ and $a \in O_K$.

Let v a non archimedean valuation of K such that $v(a) \geq 1$ and $\|F\|_v = 1$. Suppose also that $f(O_K)$ is O_K-parametrizable.

Then $N(v) = q = p^f$ (the cardinality of the residue field of v) is less or equal than the number of linear factors of $f(X) - f(Y)$ in the ring $K[X, Y]$.

Bibliography

[1] S.S. Abhyankar. *What is the difference between a parabola and a hyperbola*. Math. Intell. 10, 26-43, 1988.

[2] R.M. Avanzi, U. Zannier. *The equation $f(X) = f(Y)$ in rational functions $X = X(t)$, $Y = Y(t)$*. Compositio Math. 139 (2003), no. 3, 263-295.

[3] Luigi Bianchi. *Lezioni sulla teoria delle funzioni di variabile complessa e delle funzioni ellittiche*. Enrico Spoerri editore, Pisa, 1901.

[4] Y. F. Bilu, R. F. Tichy. *The Diophantine equation $f(x) = g(y)$*. Acta Arith. 95 (2000), no. 3, 261-288.

[5] Y. F. Bilu. *Quadratic factors of $f(x) - g(y)$*. Acta Arith. 90 (1999), no. 4, 341-355.

[6] P.-J. Cahen and J.-L. Chabert. *Integer-Valued Polynomials* Amer. Math. Soc. Surveys and Monographs, 48, Providence, 1997.

[7] A. Cassa. *Teoria elementare delle curve algebriche piane e delle superfici di Riemann compatte*. Pitagora Editrice, Bologna 1983.

[8] P. Cassou-Noguès, J.-M. Couveignes. *Factorisations explicites de $g(y) - h(z)$*. Acta Arith. 87 (1999), no. 4, 291-317.

[9] C. Chevalley. *Introduction to the theory of algebraic functions of one variable*. American Mathematical Society, 1951.

[10] H. Davenport, D. J. Lewis, A. Schinzel. *Equations of the form $f(x) = g(y)$*. Quart. J. Math. Oxford Ser. (2) 12 1961 304-312.

[11] F. Dorey, G. Whaples. *Prime and composite polynomials*. J. Algebra 28 (1974), 88-101.

[12] H. T. Engstrom. *Polynomial substitutions*. Amer. J. Math. 63, (1941). 249-255.

[13] M. D. Fried, R. E. MacRae. *On Curves with Separated variables*. Math. Ann.180, 220-226 (1969).

[14] M. D. Fried, Moshe Jarden. *Field Arithmetic*. Springer, 1986.

[15] S. Frisch. *Remarks on polynomial parametrization of sets of integer points*. Comm. Algebra 36 (2008), no. 3, 1110-1114.

[16] S. Frisch, L. Vaserstein. *Parametrization of Pythagorean triples by a single triple of polynomials*. Pure Appl. Algebra 212 (2008), no. 1, 271-274.

[17] R. Hartshorne. *Algebraic Geometry*. Springer, 1997.

[18] M. Hindry, J. H. Silverman. *Diophantine Geometry. An Introduction*, Springer, 2000.

[19] C. Kosniowski. *Introduzione alla topologia algebrica*. Zanichelli, 1996.

[20] E. Kunz. *Introduction to plane algebraic curves*. Birkhauser, 2005.

[21] K.K. Kubota. *Note on a Conjecture of W. Narkiewicz*. Journal of Number Theory 4, 181-190 (1972).

[22] K.K. Kubota. *Factors of polynomials under Composition*. Journal of Number Theory 4, 587-595 (1972).

[23] K.K. Kubota. *Image sets of polynomials*. Acta Arithmetica XXIII, 183-194 (1973).

[24] S. Lang. *Algebra*. Springer, Revised third edition 2002.

[25] S. Lang. *Fundamentals of Diophantine Geometry*. Springer-Verlag, 1983.

[26] S. Lang. *Introduction to Algebraic and Abelian Functions*. Springer 2nd edition, 1982.

[27] S. Lang. *Introduction to Algebraic Geometry*. Interscience Publishers, INC. NY, 1958.

[28] F. Lazzeri. *Personal notes on complex analysis*. Pisa (available in italian at http://www.dm.unipi.it/pages/lazzeri/).

[29] H. Levi. *Composite polynomials with coefficients in an arbitrary field of characteristic zero*. Amer. J. Math. 64, (1942). 389-400.

[30] R. Miranda. *Algebraic curves and Riemann surfaces*. American Mathematical Society, 1995.

[31] P. Müller. *Primitive monodromy groups of polynomials*. Contemporary Mathematics, 168, 245-249, Amer. Math. Soc., 1994.

[32] W. Narkiewicz. *Polynomial mappings*, Lecture Notes, vol.1600, Springer-Verlag, 1995.

[33] W. Narkiewicz. *Remark on rational transformations*, Colloq. Math., 10 (1963), 416.

[34] J. Neukirch. *Algebraic Number Theory*. Springer-Verlag, 1999.

[35] J. F. Ritt. *Prime and composite polynomials*, Trans. A. M. S. **23**, (1922), 51-66.

[36] M. Rosen. *Number theory in function fields*. Springer, 2002.

[37] A. Schinzel. *Some unsolved problems on polynomials*. Neki nereseni problemi u matematici, Matematicka Biblioteka 25, Beograd 1963, 63-70.

[38] A. Schinzel. *Polynomials with special regards to reducibility*. Cambridge University Press, 2000.

[39] J.-P- Serre. *Lectures on Mordell-Weil theorem*, Vieweg, 3rd edition, 1997.

[40] J.-P- Serre. *Local fields*, Springer-Verlag, 1979.

[41] J. H. Silverman. *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[42] I. R. Shafarevich. *Basic Algebraic Geometry*, vol.1, 2nd edition, Springer, 1994.

[43] I. R. Shafarevich. *Algebraic geometry I : algebraic curves algebraic monifolds and schemes*, Springer, 1994.

[44] H. Volklein. *Groups as Galois groups. An Introduction*. Cambridge University Press, 1996.

[45] B.L. van der Waerden. *Modern Algebra*. Revised English edition, Frederick Ungar Publishing co. New York, 1950.

[46] H. Wielandt. *Finite Permutation Groups*. Academic Press, New York, 1964.