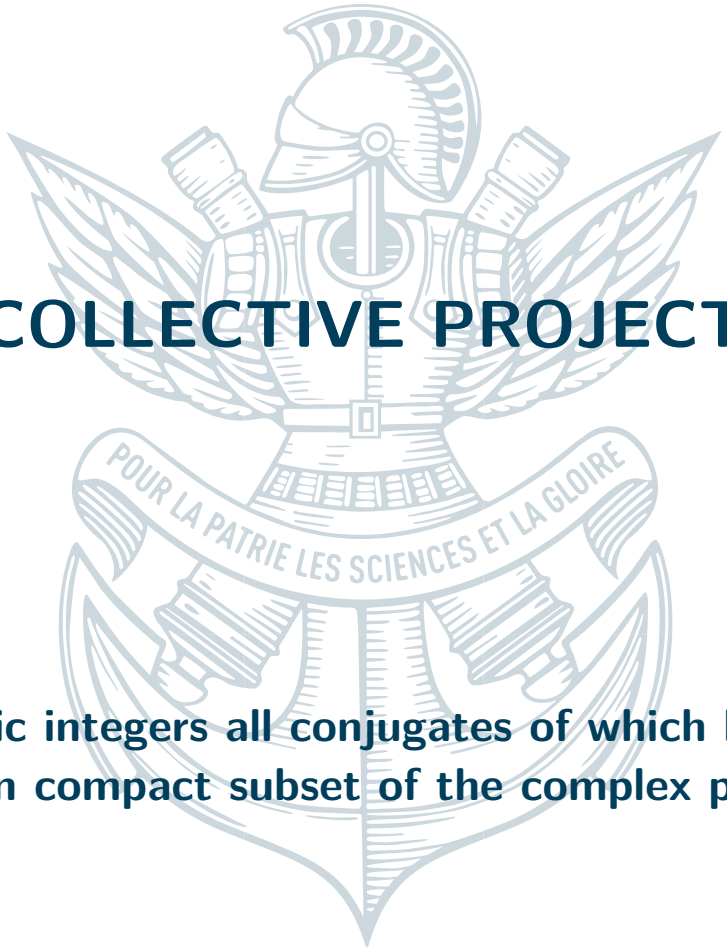


COLLECTIVE PROJECT

On algebraic integers all conjugates of which belong to a given compact subset of the complex plane

September 4, 2019

Marc Fersztand, Benjamin Gourevitch, Arnaud Rippol
Rubing Shen, Ian-Christopher Tanoh, Yicheng Zhou

Supervisor : Javier Fresán



ABSTRACT

The study of Frobenius endomorphism provides numerous information about its corresponding Abelian variety. To understand the action of the Frobenius endomorphism, one may be interested in its eigenvalues. According to Weil's third conjecture ("Riemann hypothesis over finite fields"), they all have absolute value less than or equal to $2g\sqrt{p}$. Thus, the eigenvalues of the Frobenius endomorphism all belong to the same compact subset of the complex plane, and are roots of the same monic polynomial with integer coefficients (the characteristic polynomial of the Frobenius endomorphism). Such complex numbers are called *algebraic integers "totally" in a compact subset*, which means algebraic integers all conjugates of which belong to a same given compact subset of the complex plane.

The study of such algebraic integers helps to understand the eigenvalues of the Frobenius endomorphism, especially their distribution. In this paper, we will study the following question : in what conditions a compact subset of the complex plane has a finite or infinite number of algebraic integers *totally* in it ? The problem can be studied in light of the notion of capacity of a compact subset, which comes from potential theory. In this paper, we will present the theory of capacity and some theorems (Fekete, Szegö, Robinson) derived from it that partially answer the question: in the case of a union of real segments, when the capacity is smaller (resp. larger) than 1, it contains a finite (resp. infinite) number of algebraic integers totally in it. For instance, for real line segments, the limit length is 4.

This paper is written as part of a collective project conducted in École Polytechnique (France). It is aimed towards undergraduate audience in mathematics, with basic knowledge in algebra, topology, analysis, and dwells into a modern topic of research.

ACKNOWLEDGEMENTS

We are very grateful to our supervisor Javier Fresán. This project could not exist without Javier, without his involvement, his availability, his good humour and his always relevant advice. Most importantly, thanks to him, we experienced the pleasure of studying mathematics during this project.

We would also like to thank our coordinator Stéphane Bijakowski for his kindness and constructive comments on our work.

CONTENTS

0.1 Motivation . . . 4
0.2 Outline of the paper . . . 5

1 Elementary remarks **6**
1.1 First results . . . 6
1.2 Algorithmic approach . . . 7
1.2.1 The algorithmic principle . . . 7
1.2.2 Results . . . 8
1.3 Two elementary cases : $\mathbb{U}$ and $[-2,2]$ . . . 11
1.3.1 $K = \mathbb{U}$: Kronecker's theorem . . . 11
1.3.2 $K = [-2,2]$ . . . 12

2 Capacity theory **15**
2.1 Transfinite diameter, Fekete points . . . 15
2.2 Passage from discrete to continuous : equilibrium measure and logarithmic capacity . . . 19
2.3 Potentials and semi harmonic functions . . . 27
2.3.1 Frostman's theorem . . . 27
2.3.2 Calculation of capacities . . . 30
2.4 Chebyshev constant . . . 34

3 Fekete's theorem. Fekete-Szegö's theorem **39**
3.1 Fekete's theorem . . . 39
3.2 Fekete-Szegö's theorem . . . 40

4 Robinson's theorem **44**
4.1 A few notions on algebraic curves . . . 44
4.1.1 Algebraic curve: affine case . . . 45
4.1.2 Divisors . . . 45
4.1.3 A naive compactification . . . 46
4.1.4 Interlude: adjunction of two affine algebraic curves . . . 46
4.1.5 Smooth completion . . . 47
4.1.6 Hyperelliptic curves and Pell-Abel equation . . . 49
4.1.7 A visual example . . . 50
4.2 Proof of Robinson's theorem . . . 52
4.2.1 Pell-Abel case . . . 52
4.2.2 Proof of proposition 4.5 in the case $g = 0$ . . . 53
4.2.3 Proof of proposition 4.5 when $g > 0$ . . . 55
4.2.4 End of the proof of Robinson's theorem . . . 58
4.2.5 From the Pell-Abel case to the general case . . . 60

A Measure theory **64**
A.1 Measures . . . 64
A.2 Weak-$*$ convergence . . . 65
A.3 Lower semi-continuous functions . . . 67

B Semi-harmonic functions **69**

C Some technical proofs **72**
C.1 Proof of proposition 2.6 . . . 72
C.2 Proof of theorem 2.8 . . . 74

PREAMBLE

0.1 Motivation

Since the XIX-th century, research in arithmetic uses concepts from other branches of mathematics, leading to great progress with surprising efficiency. One of the branches created by this diversification is arithmetic geometry, which combines algebra and geometry to solve number theory problems. A quick description of the success of this union can be found in [1].

One of the main subject of study in this area is the behavior of geometric objects (*e.g.* "curves") defined over finite fields. These "curves" are rigorously defined as the domain on which a certain number of multi-variable polynomials defined over the considered finite field vanish. For instance, the first bisector is the domain in which the polynomial $P(X,Y) = X - Y$ vanishes. As a reminder, a finite field is a finite set with a well defined addition and multiplication. For example, we can take the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, where p is a prime number, as well as the extensions $\mathbb{F}_{p^n}$ obtained by adding the root of an irreducible polynomial of degree n.

One of the remarkable properties of these curves is that we can associate them with abelian groups in which it is possible – in a certain way – to "sum" two points on the curve, and to find an opposite to each point. These groups, called *abelian varieties* exhibit very interesting properties and are still today an active area of mathematical research, with numerous results [2][3].

To study the curves over finite fields, a classical method is to study the action of homomorphisms (*i.e.* applications compatible with the algebraic structure of the field) on those curves. One of the most famous and important homomorphisms in such cases is the so-called Frobenius endomorphism Fr which raises the coordinates of a point of the curve to the *p-th* power, where p is the characteristic of the field (the smallest integer such that $p \times 1 = 0$ in the field, with 1 the unit of the field). In general algebra, the study of Frobenius endomorphism allows to deduce a number of properties on the set on which it acts. As such, it is natural to try to study it in the case of curves over finite fields. Especially, since $x^p = x$ for all $x \in \mathbb{F}_p$, the number of fixed points of the Frobenius endomorphism is the number of points of the curve with coordinates in $\mathbb{F}_p$. In the same way, the fixed points of Fr^n are the points of the curve whose coordinates belong to $\mathbb{F}_{p^n}$.

It is then possible to construct the generating function $\exp(\sum_{n\geq 1} N_n \frac{T^n}{n})$, where N_n is the number of points of the curve with coordinates in $\mathbb{F}_{p^n}$. According to the Weil conjectures [4], this power series is actually a rational function : more precisely, a quotient $P(T)/(1-T)(1-pT)$ with $P \in \mathbb{Z}[X]$ a monic polynomial with integer coefficients. This polynomial is the characteristic polynomial of Fr acting – not on the curve as previously seen – but on the abelian variety defined from the curve. The eigenvalues of this Frobenius endomorphism are the root of the characteristic polynomial, which, according to Weil's third conjecture, ("Riemann hypothesis over finite fields"), are all inferior in absolute value to $2g\sqrt{p}$, in which g is the dimension of the abelian variety. In particular, they are all included in the same compact subset (*i.e.* closed and bounded) K of the complex plane. The roots of such a polynomial are called *algebraic integers totally included in* K. Of course, all monic polynomials with such roots are not associated with Frobenius endomorphisms. But understanding the behavior of this kind of polynomials allows a better comprehension of Frobenius endomorphisms.

With that being said, it is natural to inquire about the distribution of those eigenvalues, which can be deduced from the distribution of algebraic integers totally in a compact subset. This distribution itself can be deduced from the case where K is a real line segment, studied by Robinson who showed in 1962 the following result: if the length of K is strictly more than 4, there is an infinite number of algebraic integers totally in it; if the length is strictly inferior to 4, there is only a finite number of such numbers. The case in which the length is exactly 4 is – for now – only solved for a few special cases. The paper we present here gives a proof of this result.

0.2 Outline of the paper

In a formal way, *algebraic integers* are complex numbers which are the roots of a monic polynomial with coefficients in $\mathbb{Z}$. We shall call $\mathbb{Q}$-conjugates of an algebraic integer α the roots of the unique monic polynomial P with rational coefficients of minimal degree for which $P(\alpha) = 0$ (minimal polynomial). Given a compact set K of $\mathbb{C}$, we say that an algebraic integer is totally in K if all his $\mathbb{Q}$-conjugates are in K. We call *degree of an algebraic integer* the degree of his minimal polynomial.

The study of the distribution of algebraic integers totally in a real line began in the beginning of the XX-th century, with a first result from Schur in 1918 which solves the case of real lines with length strictly below 4. Many other results follow in the next years. Then, some 40 years later, Robinson eventually demonstrates his theorem, leaving only the case of length 4 unresolved.

The proof we shall give here for Robinson's theorem follows an article from Jean-Pierre Serre [5] which summarizes a lecture given during the Bourbaki seminar of March 2018 in Paris. The purpose of the present paper is to be understandable by a non-specialist audience, but one that has a solid grasp on the basic elements of algebra (group, polynomials), topology (weak convergence) and analysis (continuity, basic complex analysis). It seems to us that an undergraduate audience can follow our work and the proof we shall give without too much trouble. The more interested readers can find in the appendix additions on measure theory, on more subtle analysis points used in our reasoning, as well as proofs deemed too technical and without much interest as far as understanding the essence of this proof goes.

In the first part (Elementary remarks), we shall make a range of first observations on this problem, which will lead to ideas of proof, or invalidate certain proof schemes that could be thought of. This part includes an algorithmic approach that allows us to get an intuition on the result (although the programs' complexity does not allow for a very deep dive into polynomials of high degrees). Finally, we will demonstrate a first result first found by Kronecker (1857) which deals with the case where the compact subset of the complex plane is the unit circle. From this case, we will deduce the behavior of the real line $[-2, 2]$, and, more widely, of any real line of the form $[n-2, n+2]$, with $n \in \mathbb{Z}$. From these remarks, we will give first bounds for the length of real lines containing an infinite/finite number of algebraic integers totally in it.

In the second part, we will look into the theory of capacity, which is the natural frame of study for dealing with the " size" of a compact set for this problem. This notion of capacity is deeply linked to the concepts introduced in measure theory, and some of the results from this part – once combined with results from the last part – allow us to prove a slightly stronger result than Robinson's theorem. In particular, we prove the convergence (in a certain sense) of a measure associated with a sub-sequence of polynomials towards the measure of equilibrium of the compact set.

We will then show in the third part Fekete's theorem 3.1 which solves the case of a real line of length strictly less than four, then, Fekete-Szegö's theorem 3.3 which is the equivalent of Robinson's theorem for complex compact subset of the complex plane (as opposed to the real lines of Robinson's theorem). We will see how the proof of this theorem is not sufficient to yield the real case, although some ideas can be reused to solve the latter, which is why the study of this theorem is very interesting for this proof.

In the last part of this paper, we will eventually give the full proof of Robinson's theorem, using the tools developed in the first parts as well as a few results pertaining to the field of algebraic geometry. After a quick introduction to the core concept of algebraic curves, we will use those results to finish the proof of the main result of this paper.

1
ELEMENTARY REMARKS

Let us start by reminding ourselves of the definition of our object of study: algebraic integers totally in a compact set.

Definition 1.1 (i) An *algebraic integer* is a complex number that is a root of some monic polynomial with coefficients in $\mathbb{Z}$.

(ii) Given an algebraic integer $\zeta \in \mathbb{C}$, we call *minimal polynomial of* ζ the unique monic polynomial with integer coefficients among these with ζ as a root.

(iii) Let us denote by $\mathrm{Gal}(\zeta)$ the set of all roots of the minimal polynomial of ζ.

(iv) Let E be a subset of $\mathbb{C}$ and ζ an algebraic integer. We say that $\zeta \in \mathbb{C}$ is *totally in* E if $\mathrm{Gal}(\zeta) \subset E$.

1.1 First results

In this first section, we will start by stating three "elementary" remarks about the problem: first, at a fixed degree, there is only a finite number of algebraic integers totally in a given compact set; then, the derivatives of a minimal polynomial of algebraic integers totally in a compact set have interesting properties; finally, if $K_1 \subset K_2$ are two compact sets, then the numbers of algebraic integers totally in K_1 and K_2 respectively, can be compared.

Remark 1.1 Let K be a compact subset of $\mathbb{C}$. Let P be a monic polynomial of degree n the roots of which are all in K, we can upper bound the k-th coefficient of P by $\sup(K)^k \binom{n}{k}$. It is enough to assure that, at fixed degree, there exists a finite number of such polynomials with all roots in K, and therefore a finite number of algebraic integers of degree n totally in K.

This remark leads us to several interesting approaches:

- We can find (algorithmically) the adequate polynomials of small degrees.
- If we want to prove that there exists a finite number of algebraic integers in a compact set, it is enough to prove that the degree of such an integer is bounded.

Remark 1.2 Let us consider a monic polynomial P with integer coefficients whose roots are algebraic integers totally in a compact set K, where the degree of P is greater than or equal to 2, its derivative is not a monic polynomial. However it is still a polynomial with integer coefficients, and its roots are still in K, if this compact set is convex (which is the case for real line segments). Indeed, it follows from Gauss-Lucas theorem that the roots of P' are in the convex hull of the set of roots of P.

Therefore we notice that the knowledge of P' gives us information on the roots of P. This idea will be useful when we compute algorithmically algebraic integers totally in a compact set.

Remark 1.3 Let K_1 and K_2 be 2 compact sets such that $K_1 \subset K_2$, then there is at least as many algebraic integers totally in K_2 as those totally in K_1 (since any algebraic integer totally in K_1 is an algebraic integer totally in K_2). This somewhat obvious remark will be of great use for proofs where it is easier to work on a

smaller compact set.

1.2 Algorithmic approach

In order to get an intuition about the algebraic integers totally in a compact set, we have decided to conceive and implement an algorithm listing algebraic integers totally in a line segment, the minimal polynomial of which, is of fixed degree. These results will later be compared to the demonstrated theorems.

Let K be a compact subset of $\mathbb{C}$. Two questions were kept to be answered by numerical experiments:

- What are the algebraic integers totally in K? A particular focus is done on the distribution of such numbers. The results can be compared to the cases studied in section 1.3. This question seems difficult because it requires a fine knowledge of the algebraic integers totally in K. That is why the core question of our paper is actually :
- Is there an infinite number of algebraic integers totally in K ? The numerical answer to this question can be compared to the results of sections 3 and 4.

First, we will state the algorithmic principle that we use, then we will comment on the results we obtained.

1.2.1 • The algorithmic principle

In order to get numerical results, only monic polynomials with integer coefficients, the degree of which, is less than a given integer n will be studied. The goal is to find a list as short as possible with all minimal polynomials, with degree less than n, of algebraic integers totally in K.

The remark 1.1 allows to give bounds to the coefficients of polynomial with a given degree, the roots of which, are all in K. Therefore, for a given degree, the polynomials that could be the minimal polynomial of an algebraic integer totally in K can be enumerated:

Algorithm 1 Naive algorithm

```
l empty list
for all P monic polynomial of degree less than n, the coefficients of which, are integers in the bounds of remarks 1.1 do
  if the roots of P are totally in K then
    add the roots of P to l
  end if
end for
return l
```

However, this method is not very efficient. Indeed, the complexity is greater than the product of the double of the bounds:

$$\prod_{k=1}^{n} (2\sup(K))^k \binom{n}{k} C(n) \geqslant (2\sup(K))^{n^2/2},$$

where $C(n)$ is the complexity of computing the roots of a polynomial of degree n (done by computing the eigenvalues of the companion matrix). For instance, when the compact set K is a line segment subset of [-2.5,2.5], this algorithm cannot list the algebraic integers totally in K with minimal polynomial of degree higher than $n = 4$. This data is unfortunately not enough to make interesting conjectures.

Since we mainly focus on the case of real segments, we implemented another specific algorithm for segments of $\mathbb{R}$. Remark 1.2 can therefore apply and gives a great improvement in efficiency. Indeed, when K is a segment of $\mathbb{R}$, for all algebraic integers totally in K, all the derivatives of its minimal polynomial have simple roots and all the zeros are in K. More generally, let $l < n-1$ and let us consider the polynomials $P = \sum_{k=0}^{n} a_k X^k$ where the $n-l-1$ greatest coefficients $a_{l+1}, \ldots, a_{n-1}$ are fixed and $a_n = 1$. Then $P^{(l)} = l!a_l + \sum_{k=1}^{n-l} \frac{(l+k)!}{k!} a_{l+k} X^k$ has $n-l$ roots in K. More specifically, $-a_l$ is between the maximum of all local minimums and the minimum of all local maximums of $\sum_{k=1}^{n-l} \frac{(l+k)!}{k!} a_{l+k} X^k$. Thus, by repeating for l ranging from $n-2$ to 0, we obtain stricter constraints on $a_0, \ldots, a_{n-1}$ and thus a list of polynomials likely to have all their roots in K much more restricted than in the naive algorithm. In summary, the limits of the remark 1.1 have been refined by taking into account the value of the other coefficients already set. Thus the polynomials whose roots are calculated are much less numerous and of lower degree, which explains why this algorithm is more efficient than the previous one. Thanks to this optimization, it was possible to obtain all algebraic integers, whose minimum polynomial's degree is at most $n = 7$ for segments included in $[-2.5, 2.5]$. The analysis of figure 1 corroborates this observation. While it has been calculated that the naive algorithm has a complexity of at least C^{n^2}, the second algorithm has an experimental complexity close to 15^n.

After writing this algorithm, we tried to compare it with the state of the art. In [6], the authors combine techniques very close to ours but more refined with algebraic properties to solve a problem close to ours. Their algorithm allows to go up to degree 13 in a reasonable time. But unfortunately, we cannot directly apply their algorithm to our problem.

1.2.2 • Results

Considering remark 1.3, an algebraic integer totally in a compact set K is totally in all compact sets containing K. We can think that "large" compact sets will have an infinite number of algebraic integers while "small" compact sets will have a finite number.

To verify this, we have plotted the evolution of the number of algebraic integers totally in K according to the degree of their minimal polynomial for different segments K of $\mathbb{R}$. The results in figure 3 show that the length 4 is the boundary between "small" and "large" segments. For segments with lengths less than 4, there are fewer and fewer new algebraic integers as the degree increases (blue, orange). On the contrary, for segments longer than 4, there are more and more (green, red, purple). This observation remains valid when translating the segments.

These observations are in accordance with the theorems that we will demonstrate in this paper. The behavior of "small" segments is treated by Fekete's theorem 3.1 and that of "large" segments by Robinson's theorem 4.3.

When $K = [-2.2]$, we can notice that the number of new algebraic integers totally in K found at the n degree seems to increase, but not exponentially (figure 2). We can verify that the algebraic integers found are of the form $2\cos(\frac{2k\pi}{m})$ with k and m integers. We will see in the following subsection (1.1) that the algebraic integers totally in $[-2.2]$ are the $2\cos(\frac{2k\pi}{m})$ with k and m integers. However, the algorithm does not find them by increasing m.

Beyond the finiteness of the set of algebraic integers totally in a compact set, one can be interested in the distribution of these numbers. The figure 4 shows that the distribution is essentially the same both when translating slightly and when the length changes. Moreover, this distribution is similar to that of the roots of the Chebyshev polynomials.

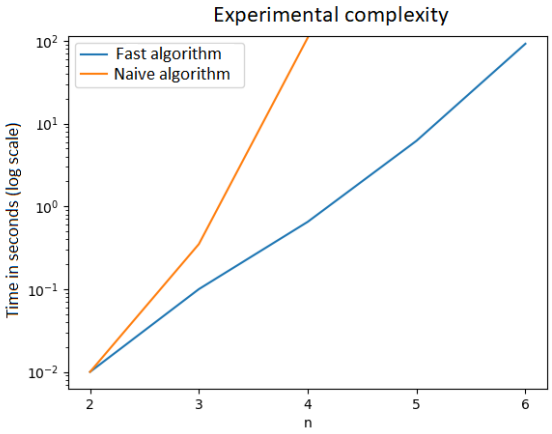


Figure 1: Experimental complexity of the two algorithms (length = 3.9)

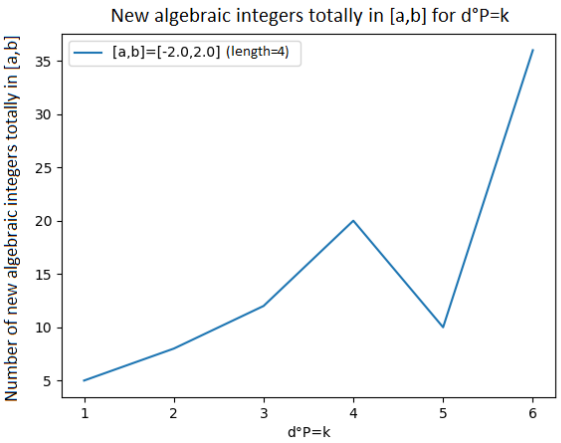


Figure 2: Number of new algebraic integers in function of the degree of the minimum polynomials for $K = [-2, 2]$

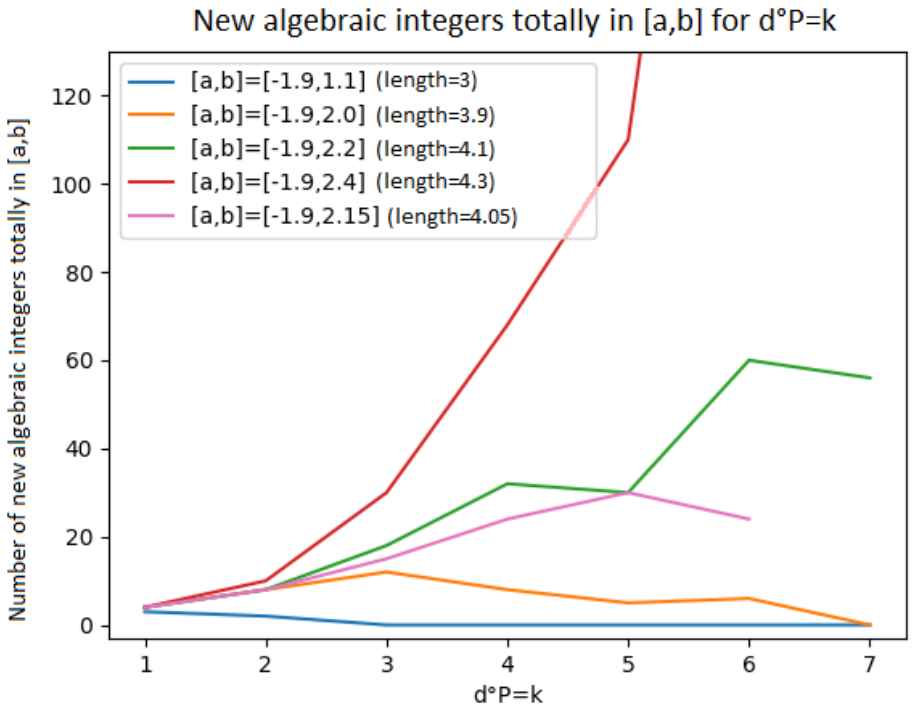


Figure 3: Number of new algebraic integers found in function of the degree of the polynomials traversed

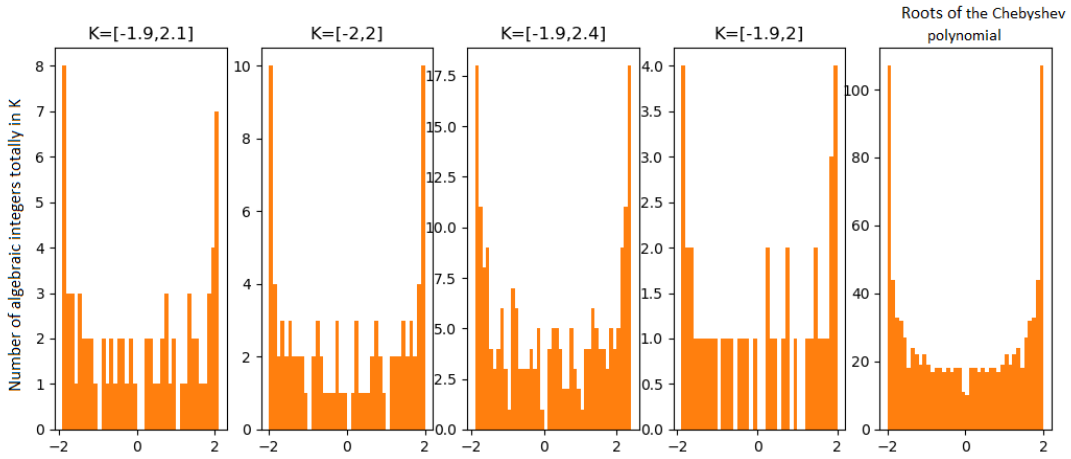


Figure 4: Distribution of algebraic integers of lower degree for different segments compared to that of the roots of Chebyshev polynomials

1.3 Two elementary cases : $\mathbb{U}$ and $[-2, 2]$

Let us start with the well known cases of the unit circle and segments with length 4 and integer end points.

1.3.1 • $K = \mathbb{U}$: Kronecker's theorem

When $K = \mathbb{U}$ is the unit circle, Kronecker's theorem gives us the following result :

Theorem 1.1 (Kronecker). Let $P \in \mathbb{Z}[X]$ be a monic polynomial whose complex roots are all in the unit circle $\mathbb{U}$, then its roots are roots of unity.

Let us start with the following lemma :

Lemma 1.1 Let $n, k \in \mathbb{N}$ and Q be a polynomial with expression $\prod_{i=1}^{n}(X - \alpha_i)$.

If $Q \in \mathbb{Z}[X]$, then $Q_k(X) := \prod_{i=1}^{n}(X - \alpha_i^k) \in \mathbb{Z}[X]$.

Proof.
Let us consider such a polynomial Q and integers n and k. The Frobenius companion matrix M of Q is a matrix of $M_n(\mathbb{Z})$ whose characteristic polynomial is Q. Therefore the α_i are the eigenvalues of M. M is similar to an upper triangular matrix with main diagonal $\alpha_1, \dots, \alpha_n$, which results in M^k being similar to an upper triangular matrix with main diagonal $\alpha_1^k, \dots, \alpha_n^k$. Thus, the α_i^k are the eigenvalues of M^k with the same multiplicity as for M. It implies that Q_k is the characteristic polynomial of M^k. Since this matrix has integer coefficients, Q_k has as well. □

Let us prove Kronecker's theorem:

Proof. Let us consider $P = X^n + p_{n-1}X^{n-1} + \cdots + p_0 \in \mathbb{Z}[X]$ a monic polynomial such that $Z(P) \subset \mathbb{U}$, where $Z(P) = \{\alpha_1, \dots, \alpha_n\}$ is the set of the complex roots of P. It follows from the Vieta's formulas that:

$$p_{n-k} = (-1)^k \sum_{J \in \mathcal{P}_k([1,\dots,n])} \prod_{i=1}^{k} \alpha_{j_i}.$$

Since the α_i are of magnitude 1, the triangle inequality gives us that $|p_{n-k}| \leq \binom{n}{k}$. The coefficients of P being integers, we deduce that $\mathcal{E}_n$, the set of polynomials of degree n which verify the hypotheses of the theorem, is a finite set. It implies that $\mathcal{R}_n$, the set of roots of polynomials in $\mathcal{E}_n$ is also finite.

Let α_i be a root of P and let us consider the multiplicative group generated by α_i, $G = \{\alpha_i^k, k \in \mathbb{Z}\}$. With the notations from lemma 1.1, for all $k \in \mathbb{Z}$, α_i^k is a root of $Q_k \in \mathcal{E}_n$ according to the lemma. Therefore, G is a finite group since $G \subset \mathcal{R}_n$. As a result, there exists integers $k < k'$ such that $\alpha^k = \alpha^{k'}$, which means $\alpha^{k'-k} = 1$. □

Remark 1.4 Let us give another proof of lemma 1.1 using symmetric polynomials. Let us consider $P = \sum_{j=1}^{n} p_j X^j = \prod_{i=1}^{n}(X - \alpha_i) \in \mathbb{Z}[X]$ and $Q = \sum_{j=1}^{n} q_j X^j = \prod_{i=1}^{n}(X - \alpha_i^k)$. Let S_j denote the j-th elementary

symmetric polynomial in n variables. It follows from the Vieta's formulas that : $p_{n-j} = (-1)^j S_j(\alpha_1, \dots, \alpha_n)$ and $q_{n-j} = (-1)^j S_j(\alpha_1^k, \dots, \alpha_n^k)$. According to the fundamental theorem of symmetric polynomials, there exists a polynomial $R \in \mathbb{Z}[X_1, \dots, X_n]$ such that

$$S_j(X_1^k, \dots, X_n^k) = R(S_1, \dots, S_n)$$

Therefore, the coefficients of Q

$$q_{n-j} = (-1)^j S_k(\alpha_1^k, \dots, \alpha_n^k) = (-1)^j R(-p_{n-1}, \cdots, (-1)^n p_0)$$

are integers.

Actually, the fundamental theorem of symmetric polynomials applies to all the symmetric polynomials, so that all the symmetric combinations of $\alpha_1, \dots, \alpha_n$, with integer coefficients, are integers.

Remark 1.5 Note that the use of companion matrices in the proof of lemma 1.1 allows us to give a direct proof of this following particular case of the fundamental theorem of symmetric polynomials: "there exists $R \in \mathbb{Z}[X_1, \dots, X_n]$, such that $S_j(X_1^k, \dots, X_n^k) = R(S_1, \dots, S_n)$".

Indeed, using the previous notations, let M be the companion matix of P.

$$\forall\, 1 \leqslant i, j \leqslant n, \quad M_{i,j} \in \{S_j(\alpha_1, \dots, \alpha_n)) \,|\, 0 \leqslant j \leqslant n\} \cup \{0, 1\}.$$

We deduce from it that :

$$\forall\, (i, j), \quad M_{i,j} \in \mathbb{Z}[S_0(\alpha_1, \dots, \alpha_n), \dots, S_n(\alpha_1, \dots, \alpha_n)].$$

Thus the coefficients of the characteristic polynomial of M^k are in $\mathbb{Z}[S_0(\alpha_1, \dots, \alpha_n), \dots, S_n(\alpha_1, \dots, \alpha_n)]$. However, these coefficients turn out to be, regardless of the sign, the $(S_i(\alpha_1^k, \dots, \alpha_n^k))_{0 \leqslant i \leqslant n}$.
We conclude that :

$$\forall\, 0 \leqslant i \leqslant n, \quad S_i(\alpha_1^k, \dots, \alpha_n^k) \in \mathbb{Z}[S_0(\alpha_1, \dots, \alpha_n), \dots, S_n(\alpha_1, \dots, \alpha_n)].$$

Conclusion of the case $K = \mathbb{U}$: algebraic integers totally in $\mathbb{U}$ are the roots of unity, and there is an infinite number of them. We have an example of a compact set with an infinite number of algebraic integers totally in it.

1.3.2 • $K = [-2, 2]$

Proposition 1.1 Let us consider $P \in \mathbb{Z}[X]$ a monic polynomial such that $Z(P) \subset [-2; 2]$.
The roots of P all have the following expression: $z + \overline{z}$, where z is a root of unity.

Proof. Let P be a polynomial of degree n verifying the assumptions of the proposition. Let us consider $Q = X^n P(X + \frac{1}{X})$. Using the binomial formula, we show that Q is a monic polynomial of degree $2n$ with integer coefficients. Let us note that 0 is not a root of Q since the polynomial's constant coefficient equals 1. Therefore, for all $z \in \mathbb{C}$,

$$Q(z) = 0 \Leftrightarrow P(z + \frac{1}{z}) = 0.$$

Let z be a complex root of Q. Then, $z + \frac{1}{z}$ is a root of P, and $z + \frac{1}{z} \in [-2, 2]$. In particular, $z + \frac{1}{z}$ is a real number. If we write the obvious equality between this real number and its complex conjugate, we get that $\rho \sin(\theta) = \frac{1}{\rho} \sin(\theta)$, where ρ and θ are the modulus and an argument of z respectively. Two cases are possible:

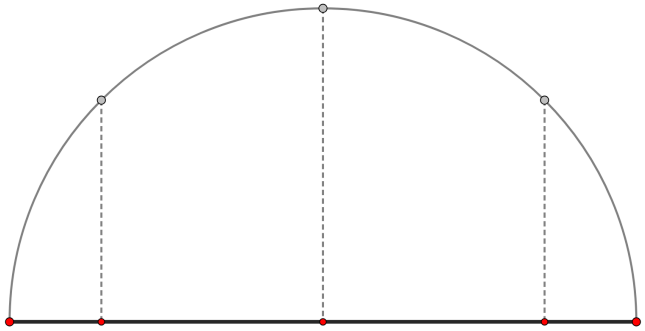


Figure 5: examples of points totally in $K = [-2, 2]$

- if $\sin(\theta) = 0$, then $z \in \mathbb{R}$. In order to verify $z + \frac{1}{z} \in [-2, 2]$, studying the sign of this expression shows us that $z = \pm 1$.
- if $\rho = \frac{1}{\rho}$, $\rho = 1$, since the modulus is a non-negative number.

In all cases, $z \in \mathbb{U}$. It follows from Kronecker's theorem that all the roots of Q are roots of unity.

Let r be a root of P. Since $r \in [-2, 2]$, we can write $r = z + \overline{z}$, with $z = \frac{r}{2} + i\sqrt{1 - \frac{r^2}{4}}$. Since $z \in \mathbb{U}$, $r = z + \frac{1}{z}$. Therefore, z is a root of Q, which means that z is a root of unity. □

Corollary 1.1 The algebraic integers totally in $[-2, 2]$ are real numbers with the following expression: $z + \overline{z}$, where z is a root of unity.

Proof. The previous proposition shows us that the algebraic integers totally in $[-2, 2]$ all have the following expression: $z + \overline{z}$, where z is a root of unity. Let us prove the reciprocal implication.

Let $(U_n)_n$ be the Chebyshev polynomials of the second kind defined as follows:

$$U_0 = 1 \text{ et } U_{n+1} = 2XU_n - U_{n-1}, \quad \forall n \geq 1.$$

We use induction on n to show that $P_n(X) = U_n(\frac{X}{2})$ are monic polynomials of degree n and with integer coefficients. They verify that $\forall \theta \in \mathbb{R} \setminus \pi\mathbb{Z} \quad \frac{\sin((n+1)\theta)}{\sin\theta} = P_n(2\cos\theta)$. We deduce from it that:

$$\forall n \geqslant 1, Z(P_n) = \{2\cos\frac{k\pi}{n+1}, \quad \forall k \in \{1, \ldots, n\}\} \subset [-2, 2].$$

Therefore, for all $n \geqslant 1, Z(P_n)$ is a set of algebraic integers totally in $[-2, 2]$, which implies that for any root of unity z, $z + \overline{z}$ is totally in $[-2, 2]$. □

Conclusion of the case $K = [-2, 2]$: algebraic integers totally in $[-2, 2]$ are the $z + \frac{1}{z}$, with z some root of unity.

It follows from translating the previous result, this claim for any segment of $\mathbb{R}$ with length 4 and integer end

points:

Corollary 1.2 Let $K = [n-2, n+2]$ be a real segment with length 4, integer endpoints and $n \in \mathbb{Z}$ its middle point. The algebraic integers totally in K are $n + z + \frac{1}{z}$, with z a root of unity.

Proof. Let $P \in \mathbb{Z}[X]$ be a monic polynomial such that $Z(P) \subset [n-2, n+2]$ and let us consider $Q = P(X+n)$. Since $n \in \mathbb{Z}$, Q is a monic polynomial with integer coefficients, and $Z(Q) \subset [-2, 2]$. The proposition 1.1 allows us to conclude. □

From this particular case, we deduce a more general theorem which gives us a first piece of information:

Theorem 1.2 (Upper bound of the minimal length to contain an infinite number of algebraic integers totally in a segment). Segments with length greater than or equal to 5 have an infinite number of algebraic integers totally in them.

Proof. Segments with length 5 contain a segment with length 4 and integer endpoints, and according to remark 1.3, they contain at least as many algebraic integers as the smaller segments, therefore containing an infinite number, according to corollary 1.2. □

A first stage of the work was done with general remarks, an algorithmic approach to convince ourselves of the result and a first particular case. Let us now build a general framework to tackle the general case of the theorem.

2
CAPACITY THEORY

First and foremost, let us focus our interest on the notion of *capacity*. It is a non-negative number describing the size of a set, but not a geometric size related to its measure : the terminology comes from physics, more specifically, from the *capacity of a capacitor*, which describes the ability of a set to contain electric charges. We shall see that it is an "adequate " definition of the size of a compact set when it comes to algebraic integers. This notion gives us a criterion which allows us to determine whether or not a compact set has an infinite number of algebraic integers totally in it (cf. 4), with Fekete's and Fekete-Szegö's theorems.

The goal of this section is to give three equivalent definitions of the notion of capacity : transfinite diameter (2.1), logarithmic capacity (2.2) and the Chebyshev's constant (2.4). The main theorem of this section is theorem 2.10 which proves the equivalence between the three definitions, and states important properties of objects which allow us to link these three approaches: Fekete's measures, equilibrium measure, equilibrium potential, Fekete's polynomials, Chebyshev polynomials... In section 2.3, we will also prove a formula to calculate a type of capacity thanks to semi harmonic functions: this section, which is quite technical, can be skipped at first reading.

We will first introduce the notion of transfinite diameter of a compact set thanks to Fekete points ; then we will study the notion of logarithmic capacity and equilibrium measure before unifying these two notions. Finally we will give a third definition of the capacity using Chebyshev polynomials. Thanks to this last approach we will be able to calculate the capacity of segments.

2.1 Transfinite diameter, Fekete points

To get a first intuition, let us consider a geometric problem from electrostatics: let us place electrons in a bounded domain. These electrons will tend to maximize their mutual distances in order to minimize the overall energy. In 3 dimensions, the force is proportional to the square of the inverse of the distance, and the potential is proportional to the inverse of the distance. Since we are working in the two-dimensional complex plane, the force is proportional to the inverse of the distance and the potential is proportional to log of the distance.

Given K a compact subset of $\mathbb{C}$ and $z_1, \dots, z_n \in K$, let us define the *potential* at point z_i (which can be equal to $+\infty$) as follows :

$$U_{z_1,\dots,z_n}(z_i) = -\sum_{j \neq i} \log |z_j - z_i| .$$

Let us also define the energy of the configuration $(z_1, \dots, z_n)$ as the mean of the potentials at each point :

$$E(z_1, \dots, z_n) = -\frac{2}{n(n-1)} \sum_{i<j} \log |z_i - z_j| = -\log \prod_{i<j} |z_i - z_j|^{\frac{2}{n(n-1)}}$$

Let us focus on minimizing the energy of the compact set K for a given number n of points :

$$E(K) = \min_{z_1,\dots,z_n \in K} E(z_1, \dots, z_n) = -\log \max_{z_1,\dots,z_n \in K} \prod_{i<j} |z_i - z_j|^{\frac{2}{n(n-1)}}$$

The lower bound is reached since K is compact, hence the min in the optimization formula. The points where this minimum is reached are called the *Fekete points* :

Definition 2.1 **(Fekete points).** Let K be a compact subset of $\mathbb{C}$. Let us define

$$\delta_n(K) = \max_{z_1,\dots,z_n \in K} \prod_{i<j} |z_i - z_j|^{2/n(n-1)}$$

This maximum value is reached at the *Fekete points* (of degree n).

Remark 2.1 It matches the definition of the usual diameter for $n = 2$.

Lemma 2.1 let $f : K \times K \to \mathbb{R} \cup \{-\infty\}$ be a function and for all $n \in \mathbb{N}^*$, let us consider

$$m_n^f(K) = \sup_{x_1,\dots,x_n \in K} \frac{1}{n(n-1)} \sum_{i \neq j} f(x_i, x_j).$$

The sequence $(m_n^f(K))_n$ is decreasing.

Proof. Let $n \geq 1$, and $x_1, \dots, x_{n+1} \in K$ (not necessarily distinct). We obtain the following equality:

$$\frac{1}{n(n+1)} \sum_{i \neq j} f(x_i, x_j) = \frac{1}{n+1} \sum_{k=1}^{n+1} \left(\frac{1}{n(n-1)} \sum_{i \neq j, i \neq k, j \neq k} f(x_i, x_j) \right);$$

indeed, it is easily verified by calculating the coefficients of $f(x_i, x_j)$ on each side: the term $f(x_i, x_j)$ on the right is only affected by the $k \in [\![1, n+1]\!] \backslash \{i, j\}$ so there are $n-1$ choices. Given a k, the sum $\sum_{i \neq j, i \neq k, j \neq k}$ on the right can be considered as $\sum_{i \neq j}$ where $i, j \in [\![1, n+1]\!] \backslash \{k\}$, which is lower or equal to $m_n^f(K)$ by definition. Then, as we consider the supremum on $x_1, \dots, x_n \in K$, we obtain that :

$$m_{n+1}^f(K) \leqslant \sup_{x_1,\dots,x_n \in K} \frac{1}{n+1} \sum_{k=1}^{n+1} m_n^f(K) = m_n^f(K).$$

□

Definition 2.2 **(Transfinite diameter).** The sequence $(\delta_n(K))_{n \geqslant 2}$ is non-negative and decreasing. The limit

$$\tau(K) = \lim_{n \to \infty} \delta_n(K)$$

is called the *transfinite diameter*.

Proof. We deduce the fact that $(\delta_n(K))_{n \geqslant 2}$ is decreasing from lemma 2.1. □

We have given our first definition of the notion of capacity : the transfinite diameter. Let us now prove a few elementary properties and give a few examples as well.

Proposition 2.1 Let K be a compact subset of $\mathbb{C}$, then

1. if $a, b \in \mathbb{C}$, then $\tau(aK + b) = |a|\,\tau(K)$;
2. $\delta_n(K) = \delta_n(\partial K)$ and then $\tau(K) = \tau(\partial K)$.

Proof. (a) can be easily deduced from the definition.

(b) Let us consider $n \geq 2$ and $h(z_1, \ldots, z_n) = \prod_{1 \leq i < j \leq n}(z_i - z_j)$. It is a holomorphic function of n complex variables on $\mathbb{C}^n$, therefore $\|h\|_{K^n} = \|h\|_{(\partial K)^n}$ (we can use the maximum modulus principle of a holomorphic function of one variable), where $\delta_n(K) = \delta_n(\partial K)$. □

Proposition 2.2 (Unit circle). The Fekete points on $\mathbb{U}$ are the n-th roots of unity, up to a rotation. The transfinite diameter of the unit circle equals 1.

Proof. Let us consider $n \geqslant 2$ and $x_1, \ldots, x_n \in \mathbb{U}$, let us denote by $D(x_1, \ldots, x_n)$ the determinant of the Vandermonde matrix $D(x_1, \ldots, x_n) = \det((x_i^{j-1})_{1 \leq i,j \leq n}) = \prod_{i<j}(x_j - x_i)$.
We have $\delta_n(\mathbb{U}) = \max\limits_{x_1, \ldots, x_n \in \mathbb{U}} |D(x_1, \ldots, x_n)|^{\frac{2}{n(n-1)}}$. Hadamard's inequality gives us

$$|D(x_1, \ldots, x_n)| \leq \left\| \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \right\|_2 \left\| \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \right\|_2 \ldots \left\| \begin{pmatrix} x_1^{n-1} \\ \vdots \\ x_n^{n-1} \end{pmatrix} \right\|_2 = n^{\frac{n}{2}}.$$

Therefore, $\delta_n(\mathbb{U}) \leq n^{\frac{1}{n-1}}$.

The equality is reached when the row vectors form a family of orthogonal vectors that are linearly independent or contains a null vector, which can be written as follows :

$$\begin{aligned} D(x_1, \ldots, x_n) = n^{\frac{n}{2}} &\Leftrightarrow \forall i < j \in [\![1, n]\!], \begin{pmatrix} x_i^0 \\ \vdots \\ x_i^{n-1} \end{pmatrix} \cdot \begin{pmatrix} x_j^0 \\ \vdots \\ x_j^{n-1} \end{pmatrix} = 0 \\ &\Leftrightarrow \forall i < j \in [\![1, n]\!], \sum_{k=0}^{n-1} (x_j \overline{x_i})^k = 0 \\ &\Leftrightarrow \forall i < j \in [\![1, n]\!], x_j \neq x_i \text{ et } \frac{1 - (x_j \overline{x_i})^n}{1 - x_j \overline{x_i}} = 0 \\ &\Leftrightarrow \forall i < j \in [\![1, n]\!], x_j \overline{x_i} \in \mathbb{U}_n - \{1\} \\ &\Leftrightarrow \{x_1, \ldots, x_n\} = x_1 \mathbb{U}_n \end{aligned}$$

Therefore $\delta_n(\mathbb{U}) = n^{\frac{1}{n-1}}$, the Fekete points on $\mathbb{U}$ are the n-th roots of unity, up to a rotation, and then $\tau(\mathbb{U}) = \lim\limits_{n \to \infty} n^{\frac{1}{n-1}} = 1$. □

Corollary 2.1 We have $\tau(\overline{B}(0,\rho)) = \rho$.

Proof. It follows from Prop. 2.1 and Prop. 2.2 that

$$\tau(\overline{B}(0,\rho)) = \rho\,\tau(B(0,1)) = \rho\,\tau(\partial B(0,1)) = \rho\,\tau(\mathbb{U}) = \rho.$$

□

Proposition 2.3 Let us consider $K = \{0\} \cup \{1, \frac{1}{2}, \frac{1}{3}, \dots\}$. We have $\tau(K) = 0$.

Proof. Let us consider $n \geq 2$. Let $x_n \leq y \leq x_{n-1} \leq \cdots \leq x_1$ be a choice of Fekete points in $K \subset [0,1]$, then

$$\begin{aligned}\delta_{n+1}(K)^{\frac{(n+1)n}{2}} &= (y - x_n)\left(\prod_{i=1}^{n-1}(x_i - y)\right)\left(\prod_{1\leq i<j\leq n}(x_i - x_j)\right)\\ &\leq (y - x_n)\left(\prod_{i=1}^{n-1}(x_i - y)\right)\delta_n(K)^{\frac{n(n-1)}{2}}\end{aligned}$$

We can obtain an upper bound using $x_n \geqslant 0$ and since all points are distinct, $x_i \leq \frac{1}{i}$ for $i \in [\![1, n-1]\!]$ and $y \leq \frac{1}{n}$, therefore

$$(y - x_n)\left(\prod_{i=1}^{n-1}(x_i - y)\right) \leq \left(\frac{1}{n} - 0\right)\prod_{i=1}^{n-1}\left(\frac{1}{i} - 0\right) = \frac{1}{n\,!}$$

Hence

$$\delta_{n+1}(K)^{\frac{(n+1)n}{2}} \leq \frac{1}{n\,!}\delta_n(K)^{\frac{n(n-1)}{2}}$$

Therefore we obtain by induction, using $\delta_2(K) = 1$, the following inequality

$$\delta_{n+1}(K) \leq \left(\prod_{i=2}^{n} i\,!\right)^{-\frac{2}{(n+1)n}}$$

Finally, let us notice that this last term tends to 0 when $n \to \infty$. Indeed, we obtain for $n \geq 8$

$$\begin{aligned}\log\left(\prod_{i=2}^{n} i\,!\right) &= \sum_{i=2}^{n}\sum_{j=2}^{i}\log j = \sum_{j=2}^{n}(n+1-j)\log j\\ &\geq \sum_{j=[\frac{n}{4}]}^{3[\frac{n}{4}]}\cdots \geq \sum_{j=[\frac{n}{4}]}^{3[\frac{n}{4}]}\frac{n}{4}\log\left[\frac{n}{4}\right] = \Theta(n^2\log n), \quad n\to\infty\end{aligned}$$

□

We will be able to give another proof later (cf. Ex. 2.4, Thm. 2.3).

2.2 Passage from discrete to continuous : equilibrium measure and logarithmic capacity

In this section, we will use probability measures on a compact set and a few results on measures. Notions from the theory of measures are provided in the appendix A.

Fekete points describe an equilibrium when dealing with a finite number of particles. The transfinite diameter describes the ability of a compact set to have electric charges (like in a capacitor). When the number of charges tends to infinity, their distribution becomes continuous.

This passage to the limit can be formalized using the concept of weak convergence-$*$ of measures. Let us remind ourselves of the definition here:

Definition 2.3 (Weak-$*$ convergence). Let us consider $D \subset \mathbb{C}$ and $(\mu_n)_{n\in\mathbb{N}}$ a sequence of measures on D. Let μ be a measure on D. We say that $(\mu_n)_{n\in\mathbb{N}}$ converges weakly to μ, written $\mu_n \xrightarrow{*} \mu$, if and only if

$$\forall f \in C_c^0(D,\mathbb{R}),\ \lim_{n\to\infty} \int_D f \ \mathrm{d}\mu_n = \int_D f \ \mathrm{d}\mu$$

.

Example 2.1 (Riemann integral). The Riemann integral can be considered as the limit measure of a sequence of counting measures: indeed, if $f : [0,1] \to \mathbb{R}$, we have

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{n} f\left(\frac{k}{n}\right) = \int_0^1 f \ \mathrm{d}x$$

If we denote by ν_n the counting measure with respect to the points $\{\frac{k}{n} \mid k = 0,\dots,n\}$, the continuous linear form $\int_0^1$ is the limit measure of the sequence (ν_n) for the weak convergence-$*$.

Example 2.2 If ν_n is the counting measure with respect to the set of the n-th roots of unity $\{e^{\frac{2\pi i k}{n}} \mid k = 0,\dots,n-1\}$, then

$$\lim_{n\to\infty} \int f \ \mathrm{d}\nu_n = \frac{1}{2\pi} \int_0^{2\pi} f(e^{i\theta}) \ \mathrm{d}\theta$$

The space of probability measures on a compact set can be equipped with a topology associated with this notion of convergence: the weak-* topology. The main result is that this space is sequentially compact.

Theorem 2.1 (Banach-Alaoglu-Bourbaki). Let K be a compact subset of $\mathbb{C}$. Let us denote by $\mathcal{P}(K)$ the set of probability measures on K. $\mathcal{P}(K)$ is sequentially a compact set for the weak topology-*.

In other words, for any sequence of probability measures $(\mu_n)_n$, there exists a sub-sequence $(\mu_{\varphi(n)})_n$ and a probability measure μ such that $\mu_{\varphi(n)} \xrightarrow{*} \mu$, *i.e.*

$$\forall \phi \in C(X), \int_X \phi \ \mathrm{d}\mu_{\varphi(n)} \longrightarrow \int_X \phi \ \mathrm{d}\mu$$

The proof of this claim is given in the appendix A.

Let $K \subset \mathbb{C}$ be a compact set and use again the electrostatic model introduced in sub-subsection 2.1. We can consider a probability measure $\mu \in \mathcal{P}(K)$ as a distribution of positive electric charges in K. For example,

a punctual charge at point z can be modelled by δ_z a Dirac measure centered on z, and a discrete distribution can be modelled by a counting measure.

Definition 2.4 (Potential, energy). Let $K \subset \mathbb{C}$ be a compact set. Let us consider $\mu \in \mathcal{P}(K)$ a probability measure on K.

Let us define *the potential of μ in z*

$$U^\mu(z) = \int_K \log \frac{1}{|z-t|} \, \mathrm{d}\mu(t)$$

and the energy of the compact set K, with respect to μ

$$I(\mu) = \int_K U^\mu(z) \, \mathrm{d}\mu(z) = \iint_{K^2} \log \frac{1}{|z-t|} \, \mathrm{d}\mu(z) \, \mathrm{d}\mu(t)$$

At equilibrium, the distribution of the charges tends to minimize the overall energy. We therefore have an energy minimization problem on the space of measures on K.

Definition 2.5 (Logarithmic capacity, equilibrium measure). Let us define the *Robin constant*

$$V_K = \inf_{\mu \in \mathcal{P}(K)} I(\mu)$$

and the *logarithmic capacity*

$$\mathrm{Cap}(K) = e^{-V_K}.$$

If the infimum $V_K = \inf_{\mu \in \mathcal{P}(K)} I(\mu)$ is reached for a measure μ_K, this measure is called *equilibrium measure*. In that case, we have $\mathrm{Cap}(K) = e^{-I(\mu_K)}$.

The potential U^{μ_K} associated with the equilibrium measure is called *the equilibrium potential*.

Definition 2.6 The capacity of a borel set $B \subset \mathbb{C}$ is defined as

$$\mathrm{Cap}(B) = \sup \{\mathrm{Cap}(K) : K \subset B, K \text{ compact}\}$$

Definition 2.7 ("quasi-almost everywhere"). Let K be a compact set. We write that *some property holds quasi-almost everywhere (q-a. e.) in a set K*, if there exists a compact subset S of capacity zero such that the property holds for all $\zeta \in K \backslash S$.

Example 2.3 Let us consider $\mu \in \mathcal{P}(K)$; if there exists a point $z \in K$ such that $\mu(\{z\}) > 0$, then $I(\mu) = +\infty$ by definition. Furthermore, if for all $\mu \in \mathcal{P}(K)$ there exists such a point, then $\mathrm{Cap}(K) = 0$.

Example 2.4 A countable set has a capacity of zero. In fact, a probability measure on such a set is atomic. The previous example gives us the expected result.

Remark 2.2 (Heuristic approach). If we consider ν_F the averaged counting measure with respect to $F = \{z_1, \dots, z_n\}$, by neglecting the divergent terms, we find the discrete definition given in sub-section 2.1

$$I(\nu_F) = -\frac{1}{n(n-1)} \sum_{i \neq j} \log |z_i - z_j| = -\log \prod_{i \neq j} |z_i - z_j|^{\frac{2}{n(n-1)}}$$

To determine the measure that minimizes the energy, it becomes natural to consider the limit measure of the counting measures with respect to the Fekete points.

This intuition will be justified later.

Lemma 2.2 Let (μ_n) be a sequence of measures of $\mathcal{P}(K)$ such that $\mu_n \xrightarrow{*} \mu$, then for all $z \in \mathbb{C}$,

$$U^{\mu}(z) \leqslant \liminf_{n\to\infty} U^{\mu_n}(z)$$

hence

$$I(\mu) \leqslant \liminf_{n\to\infty} I(\mu_n)$$

Proof. This lemma is a consequence of proposition A.3 applied to $t \mapsto \log \frac{1}{|z-t|}$ which is l.s.c. :

$$\int_K \log \frac{1}{|z-t|}\, \mathrm{d}\mu(t) \leqslant \liminf_{n\to\infty} \int_K \log \frac{1}{|z-t|}\, \mathrm{d}\mu_n(t)$$

for all $z \in K$, hence the first inequality. The second inequality follows by integrating with respect to $\mathrm{d}\mu(z)$ and by applying Fatou's lemma. □

Theorem 2.2 (Equilibrium measure). There always exists an equilibrium measure. Moreover, if $V_K < +\infty$ (or equivalently $\mathrm{Cap}(K) > 0$), the equilibrium measure is unique.

Proof. The uniqueness follows directly from the fact that $\mu \mapsto I(\mu)$ is strictly convex on $\{\mu \in \mathcal{P}(K) : I(\mu) < \infty\}$ ([7], Chap. I, Thm. 1.3(b), Lem. 1.8). The existence results from theorem A.1 which states that the space of probability measures on a compact set is a compact set. In fact,

$$V_K = \inf_{\mu\in\mathcal{P}(K)} I(\mu)$$

Let (μ_n) be a sequence of measures such that $I(\mu_n) \to V_K$. By compactness, there exists $\mu \in \mathcal{P}(K)$ and a sub-sequence (μ_{n_k}) such that $\mu_{n_k} \xrightarrow{*} \mu$. By lemma 2.2 :

$$I(\mu) \leqslant \liminf_{k\to+\infty} I(\mu_{n_k}) = V_K \leqslant I(\mu)$$

since V_K is the infimum. Hence $V_K = I(\mu)$. □

We now have all the keys to prove the equivalence between the two definitions of the capacity which were previously defined.

Theorem 2.3 Let K be a compact subset of $\mathbb{C}$. We have

$$\tau(K) = \mathrm{Cap}(K).$$

Moreover, if $\mathrm{Cap}(K) > 0$ and we denote by μ_K the equilibrium measure of K and by ν_n the counting measures with respect to the Fekete points, then

$$\nu_n \xrightarrow{*} \mu_K$$

The Fekete points are said to be equidistributed with respect to the equilibrium measure of K.

Proof. Let us rather compare $V_K = \log \frac{1}{\mathrm{Cap}(K)}$ and $\log \frac{1}{\tau(K)}$. First of all, let us show that $\log \frac{1}{\mathrm{Cap}(K)} \geqslant \log \frac{1}{\tau(K)}$.

Let us define for $z_1, \dots, z_n \in K$:

$$F(z_1, \dots, z_n) := \sum_{i<j} \log \frac{1}{|z_i - z_j|}$$

Let us remind ourselves of the definition of $\delta_n(K)$ in definition 2.1 :

$$\delta_n(K) = \max_{z_1,\dots,z_n \in K} \prod_{i<j} |z_i - z_j|^{2/n(n-1)}$$

and that $\tau(K) = \lim \delta_n(K)$. Let us also define the minimal energy associated with a n-point configuration:

$$\mathcal{E}_n := \min_{z_1,\dots,z_n \in K} F(z_1, \dots, z_n) = \frac{n(n-1)}{2} \log \frac{1}{\delta_n(K)}$$

Let μ_K be an equilibrium measure on K. Let us consider

$$\begin{aligned} J &:= \int \cdots \int F(z_1, \dots, z_n)\, \mathrm{d}\mu_K(z_1) \dots\, \mathrm{d}\mu_K(z_n) \\ &= \sum_{i<j} \int \cdots \int \log \frac{1}{|z_i - z_j|}\, \mathrm{d}\mu_K(z_1) \dots\, \mathrm{d}\mu_K(z_n) \\ &= \sum_{i<j} \int \int \log \frac{1}{|z_i - z_j|}\, \mathrm{d}\mu_K(z_i)\, \mathrm{d}\mu_K(z_j) \\ &= \sum_{1 \leqslant i<j \leqslant n} V_K \\ &= \frac{n(n-1)}{2} V_K \end{aligned}$$

On the other hand

$$\begin{aligned} J &\geqslant \int \cdots \int \mathcal{E}_n\, \mathrm{d}\mu_K(z_1) \dots\, \mathrm{d}\mu_K(z_n) \\ &= \mathcal{E}_n \\ &= \frac{n(n-1)}{2} \log \frac{1}{\delta_n(K)} \end{aligned}$$

Hence $V_K = \log \frac{1}{\mathrm{Cap}(K)} \geqslant \log \frac{1}{\tau(K)}$.

Let us denote by ν_n the counting measures with respect to the Fekete points $\{z_1, \ldots, z_n\}$. By compactness, there exists a sub-sequence (ν_{n_k}) and $\mu \in \mathcal{P}(K)$ so that $\nu_{n_k} \xrightarrow{*} \mu$. Then

$$\begin{aligned}
I(\mu) &= \iint \log \frac{1}{|z-t|} \, \mathrm{d}\mu(z) \, \mathrm{d}\mu(t) \\
&= \lim_{M \to +\infty} \iint \min[M, \log \frac{1}{|z-t|}] \, \mathrm{d}\mu(z) \, \mathrm{d}\mu(t) \\
&= \lim_{M \to +\infty} \lim_{k \to +\infty} \iint \min[M, \log \frac{1}{|z-t|}] \, \mathrm{d}\nu_{n_k}(z) \, \mathrm{d}\nu_{n_k}(t) \\
&= \lim_{M \to +\infty} \lim_{k \to +\infty} \frac{1}{n_k^2} \sum_{1 \leqslant i,j \leqslant n_k} \min[M, \log \frac{1}{|z_i - z_j|}] \\
&\leqslant \lim_{M \to +\infty} \lim_{k \to +\infty} \frac{1}{n_k^2} (\sum_{i=1}^{n_k} M + 2 \sum_{1 \leqslant i < j \leqslant n_k} \log \frac{1}{|z_i - z_j|}) \\
&\leqslant \lim_{M \to +\infty} \lim_{k \to +\infty} \frac{1}{n_k^2} (n_k M + n_k(n_k - 1) \log \frac{1}{\delta_{n_k}(K)}) \\
&= \log \frac{1}{\tau(K)}
\end{aligned}$$

Then

$$I(\mu) \leqslant \log \frac{1}{\tau(K)} \leqslant \log \frac{1}{\mathrm{Cap}(K)} = V_K \leqslant I(\mu)$$

Therefore, $\tau(K) = \mathrm{Cap}(K)$.

Furthermore, $I(\mu) = V_K = I(\mu_K)$. In the case where $\mathrm{Cap}(K) > 0$, $\mu = \mu_K$ the unique equilibrium measure on K. (ν_n) is a sequence of elements of a compact set with μ_K as its unique accumulation point, therefore

$$\nu_n \xrightarrow{*} \mu_K$$

□

Example 2.5 The equilibrium measures $\mu_{\mathbb{U}}$ and $\mu_{\overline{B}}$ of the unit circle $\mathbb{U}$ and the unit disk $\overline{B}$ are both $\frac{\mathrm{d}\theta}{2\pi}$ on $\mathbb{U}$, and the corresponding equilibrium potential is

$$U^{\mu}(z) = -\log^{+} |z| = -\max(0, \log |z|)$$

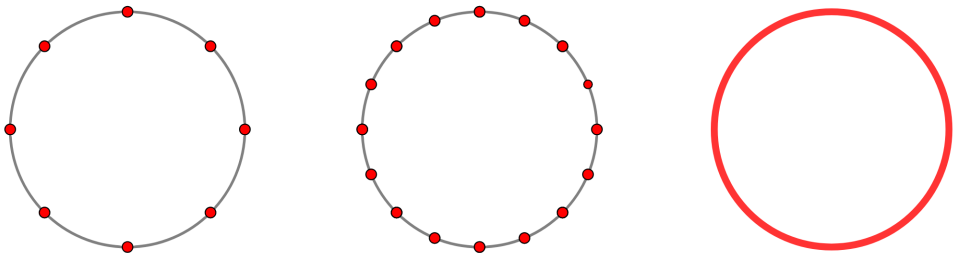


Figure 6: Fekete points for $n \in \{8, 16\}$ and equilibrium measure with $K = \mathbb{U}$

Proof.

- Let f be a continuous function. By applying the convergence theorem of Riemann sums to $\theta \mapsto f(e^{i\theta})$, we obtain :
$$\nu(\mathbb{U}_n)(f) = \frac{1}{n}\sum_{k=0}^{n-1} f(\exp\frac{2ik\pi}{n}) \underset{n\to\infty}{\to} \int_0^{2\pi} f(e^{i\theta})\frac{\mathrm{d}\theta}{2\pi}$$
But $\mathbb{U}_n$ is a set of Fekete points of $\mathbb{U}$ (Prop. 2.2) therefore $\nu(\mathbb{U}_n) \xrightarrow{*} \mu_{\mathbb{U}}$ (Thm. 2.3). Hence $\boxed{\mu_{\mathbb{U}} = \frac{\mathrm{d}\theta}{2\pi}}$.

- By making the substitution $t := \theta + \phi$:
$$U^{\mu_{\mathbb{U}}}(z) = -\int_0^{2\pi} \log(\left|z - e^{i\theta}\right|)\frac{\mathrm{d}\theta}{2\pi} = -\int_0^{2\pi} \log(\left|ze^{i\phi} - e^{it}\right|)\frac{\mathrm{d}t}{2\pi} = U^{\mu_{\mathbb{U}}}(|z|)$$
Let us consider $r \in \mathbb{R}_+$
$$U^{\nu(\mathbb{U}_n)}(r) = -\frac{1}{n}\log\left|\prod_{k=0}^{n-1}(r - e^{\frac{2ik\pi}{n}})\right| = -\frac{1}{n}\log|r^n - 1|$$
  - If $r < 1$, $|r^n - 1| \to 1$, therefore $U^{\nu(\mathbb{U}_n)}(r) = -\frac{1}{n}\log|r^n - 1| \underset{n\to\infty}{\to} 0$
  - If $r > 1$, $U^{\nu(\mathbb{U}_n)}(r) = -\frac{1}{n}\log|r^n - 1| = -\log(r) - \frac{1}{n}\log\left|\frac{1}{r}^n - 1\right| \underset{n\to\infty}{\to} -\log(r)$

  When $r \neq 1$, the function $t \in \mathbb{U} \mapsto -\log|z - t| \in \mathbb{C}$ is continuous, therefore
  $U^{\mu_{\mathbb{U}}}(r) = \lim_{n\to\infty} U^{\nu(\mathbb{U}_n)}(r) = \begin{cases} 0 \text{ if } r < 1 \\ \log\frac{1}{r} \text{ if } r > 1 \end{cases}$
  When $r = 1$, by using 2.2 and 2.3 we obtain : $0 = -\log(\tau(\mathbb{U})) = V_{\mathbb{U}} = \int_{\mathbb{U}} U^{\mu_{\mathbb{U}}}(z)\ \mathrm{d}\mu_{\mathbb{U}}(z) = U^{\mu_{\mathbb{U}}}(1)$
  Hence $\boxed{U^{\mu_{\mathbb{U}}}(z) = -\log^+|z|}$

- From the proposition 2.4(c), it follows that $\mathrm{Cap}(\mathbb{U}) = \mathrm{Cap}(\overline{B})$ and $V_{\overline{B}} = I(\mu_{\mathbb{U}}) \neq +\infty$ thanks to the uniqueness of the equilibrium measure, hence $\mu_{\overline{B}} = \mu_{\mathbb{U}}$ and $U^{\mu_{\overline{B}}} = U^{\mu_{\mathbb{U}}}$.

□

Now that we have unified the two notions of capacity previously defined, let us introduce a few properties of our capacity.

Proposition 2.4 Let us consider (K_n) compact subsets of $\mathbb{C}$.

(a) Let us consider $K_1 \subset K_2$, then $\mathrm{Cap}(K_1) \leq \mathrm{Cap}(K_2)$.

(b) Let us consider $\alpha, \beta \in \mathbb{C}$, then $\mathrm{Cap}(\alpha K + \beta) = |\alpha|\,\mathrm{Cap}(K)$.

(c) $\mathrm{Cap}(K) = \mathrm{Cap}(\partial K)$.

(d) Let us consider $(K_n)_n$ a decreasing sequence and let us consider $K = \bigcap_n K_n$, then $\mathrm{Cap}(K) = \lim_n \mathrm{Cap}(K_n)$.

(e) Let us consider $(K_n)_n$ an increasing sequence and let us assume that $K = \bigcup_n K_n$ is a compact set, then $\mathrm{Cap}(K) = \lim_n \mathrm{Cap}(K_n)$.

(f) Assume that $\mathrm{Cap}(K) = 0$. Then $\nu(K) = 0$, for all finite measures with compact support ν on $\mathbb{C}$ such that $I(\nu) < +\infty$. In particular, Lebesgue measure $m_2(K) = 0$.

Proof. (a) and (b) are immediate consequences of the definition.

(c) results from theorem 2.3 and proposition 2.1.

(d) According to (a), it is enough to show that $\mathrm{Cap}(K) \geq \lim_n \mathrm{Cap}(K_n)$, and moreover we can assume that $\mathrm{Cap}(K_n) > 0$ for all n. Let μ_{K_n} be the equilibrium measure of K_n, then $\mu_{E_n} \in \mathcal{P}(K_0)$. According to Banach-Alaoglu-Bourbaki theorem, we can extract a sub-sequence $(\mu_{E_{\varphi(n)}})_n$ which converges weakly-* to a measure $\mu^\star \in \mathcal{P}(K_0)$. Then lemma 2.2 gives us

$$I(\mu^\star) \leq \liminf_n I(\mu_{\varphi(n)}) = \liminf_n \left(-\log \mathrm{Cap}(K_{\varphi(n)})\right) = -\lim_n \log \mathrm{Cap}(K_n)$$

On the other hand, Prop. A.1 implies that

$$\operatorname{supp} \mu^\star \subset \bigcap_n \operatorname{supp} \mu_{E_{\varphi(n)}} \subset \bigcap_n K_{\varphi(n)} = \bigcap_n K_n = K$$

Therefore $\mu^\star \in \mathcal{P}(K)$, then

$$\mathrm{Cap}(K) \geq e^{-I(\mu^\star)} \geq \exp\left(\lim_n \log \mathrm{Cap}(K_n)\right) = \lim_n \mathrm{Cap}(K_n)$$

(e) According to (a), it is enough to show that $\mathrm{Cap}(K) \leq \lim_n \mathrm{Cap}(K_n)$, and moreover we can assume that $\mathrm{Cap}(K) > 0$. Let us consider $\mu \in \mathcal{P}(K)$. Since $\lim_n \mu(K_n) = \mu(K) = 1$, we have $\mu(K_n) > 0$ for a sufficiently large n . Then for such a n, we consider $\frac{\mu|_{K_n}}{\mu(K_n)} \in \mathcal{P}(K_n)$. We have

$$-\log \mathrm{Cap}(K_n) \leq I\left(\frac{\mu|_{K_n}}{\mu(K_n)}\right) = \frac{1}{\mu(K_n)^2} \int_{K_n}\int_{K_n} \log \frac{1}{|z-t|}\, \mathrm{d}\mu(t)\, \mathrm{d}\mu(z)$$

Since the domain of integration $K_n \times K_n$ increases with n and tends to $K \times K$, because (K_n) is increasing and tends to K, we obtain that

$$-\log\left(\lim_n \mathrm{Cap}(K_n)\right) \leq \frac{1}{\lim_n \mu(K_n)^2} \int_K \int_K \log \frac{1}{|z-t|}\, \mathrm{d}\mu(t)\, \mathrm{d}\mu(z) = I(\mu)$$

where we apply the monotone convergence theorem, after verifying that on $K \times K$, $\log \frac{1}{|z-t|}$ is lower bounded by $\log(1/\delta_2(K))$. In particular, when $\mu = \mu_K$ the equilibrium measure of K, $I(\mu_K) = -\log \mathrm{Cap}(K)$, we obtain that $\mathrm{Cap}(K) \leq \lim_n \mathrm{Cap}(K_n)$.

(f) Let ν be a measure verifying the theorem's assumptions. If $\nu(K) > 0$, then $\frac{\nu|_K}{\nu(K)} \in \mathcal{P}(K)$, therefore since $\mathrm{Cap}(K) = 0$, we have

$$I\left(\frac{\nu|_K}{\nu(K)}\right) = \frac{1}{\nu(K)^2} \int_K \int_K \log \frac{1}{|z-t|}\, \mathrm{d}\nu(t)\, \mathrm{d}\nu(z) = +\infty$$

Then

$$\begin{aligned} I(\nu) &= \iint \log \frac{1}{|z-t|}\, \mathrm{d}\nu(t)\, \mathrm{d}\nu(z) \\ &= \left(\int\int_{(K\times K)^c} + \int_K \int_K \right) \log \frac{1}{|z-t|}\, \mathrm{d}\nu(t)\, \mathrm{d}\nu(z) \\ &\geqslant \left(1-\nu(K)^2\right) \log \frac{1}{\delta_2(\mathrm{supp}(\nu))} + \nu(K)^2 I\left(\frac{\nu|_K}{\nu(K)}\right) = +\infty \end{aligned}$$

which is contradicted by $I(\nu) < +\infty$.

If $K \subset B(0,r)$, we have $m_2|_{B(0,r)}(\mathbb{C}) = \pi r^2$ and $I(m_2|_{B(0,r)}) < +\infty$. In fact, for all $z \in B(0,r)$,

$$\begin{aligned} \int_{B(0,r)} \log \frac{1}{|z-t|}\, \mathrm{d}m_2(t) &\leq \int_{B(z,2r)} \log \frac{1}{|z-t|}\, \mathrm{d}m_2(t) \\ &= \int_0^{2\pi} \int_0^{2r} \left(\log \frac{1}{\rho}\right) \rho\, \mathrm{d}\rho \leq 4\pi r \left\|\rho \log \rho\right\|_{L^\infty(]0,r])} < +\infty \end{aligned}$$

Therefore we can apply what we have just proved to obtain that $m_2(K) = 0$. □

Corollary 2.2 Let $a = (a_1 < \cdots < a_{2n})$ be a set of strictly increasing real numbers. Let us consider $E_a = \bigcup_{k=0}^{n-1} [a_{2k+1}, a_{2k+2}]$. The capacity of E_a continuously varies with a.

Proof. Let us consider $d = \min_i\{a_{i+1} - a_i\}$ and $\varepsilon \in]0, d/2[$. Let

$$a_{\varepsilon,+} = (a_1 - \varepsilon, a_2 + \varepsilon, \ldots a_{2n-1} - \varepsilon, a_{2n} + \varepsilon),\ a_{\varepsilon,-} = (a_1 + \varepsilon, a_2 - \varepsilon, \ldots a_{2n-1} + \varepsilon, a_{2n} - \varepsilon),$$

We have $E_{a_{\varepsilon,-}} \subset E_a \subset E_{a_{\varepsilon,+}}$.

The left (resp. right) continuity of $\mathrm{Cap}(E_a)$ with respect to a is equivalent to $\mathrm{Cap}(E_a) = \sup \mathrm{Cap}(E_{a_{\varepsilon,-}})$ (resp. $\mathrm{Cap}(E_a) = \inf \mathrm{Cap}(E_{a_{\varepsilon,+}})$). These two conditions are insured by points (d) and (e) of the previous proposition.

□

Definition 2.8 Let $K \subset \mathbb{C}$ be a compact subset. Let us denote by Ω_K the unbounded connected component of $\mathbb{C}\backslash K$. Let us define *the external boundary* of a compact set $K \subset \mathbb{C}$ as the boundary of Ω_K, subset of $\mathbb{C}$:

$$\partial_\infty K := \partial \Omega_K$$

and *the essential closure* as the complement of Ω_K with respect to $\mathbb{C}$:

$$K^{ce} := \mathbb{C}\backslash \Omega_K$$

Corollary 2.3 Let $K \subset \mathbb{C}$ be a compact set, then:

(a) If $\mathring{K}$ is non-empty, then $\mathrm{Cap}(K) > 0$; in other words, $\mathrm{Cap}(K) = 0$ implies that $K = \partial K$;

(b) $\Omega_K = \Omega_{\partial K} = \Omega_{\partial_\infty K} = \Omega_{K^{ce}}$;

(c) $\partial_\infty K = \partial K^{ce}$, $K^{ce} \supset K \supset \partial_\infty K$;

(d) $\mathrm{Cap}(K^{ce}) = \mathrm{Cap}(\partial_\infty K) = \mathrm{Cap}(K) = \mathrm{Cap}(\partial K)$.

(e) Let μ_K be the equilibrium measure of K. If $\mathrm{Cap}(K) > 0$, then $\mathrm{supp}(\mu_K) \subset \partial_\infty K$ and $\mu_K = \mu_{K^{ce}} = \mu_{\partial_\infty K}$.

(f) Let (K_n) be an increasing sequence of compact subsets of $\mathbb{C}$, and $B = \bigcup_n K_n$. Then $\mathrm{Cap}(B) = \lim_n \mathrm{Cap}(K_n)$.

Proof. (a) results from Prop. 2.4 (f) using Lebesgue measure.

(b) and (c) result from the definition.

(d) can be deduced from (c) and Prop. 2.4 (a),(c). And (e) results from it, given the uniqueness (Thm. 2.2).

(f) Let us suppose K_n of finite capacity. Let $K \subset B$ be a compact. Then $(K \cap K_n)$ is an increasing sequence that converges to K, then we have

$$\mathrm{Cap}(K) = \lim_n \mathrm{Cap}(K \cap K_n)$$

hence $\mathrm{Cap}(B) \leq \lim_n \mathrm{Cap}(K_n)$. The other inequality is trivial. □

2.3 Potentials and semi harmonic functions

For some probability measure μ, the associated potential U^μ is a function of a complex variable belonging to a specific family of functions: *semi-harmonic functions*. These are semi-continuous functions which verify the maximum/minimum modulus principle. Notions on these functions are provided in the appendix B.

By using properties of these functions, we will prove several important results on potentials and capacities. First, we will prove Frostman's theorem (Thm. 2.5) which states that the equilibrium potential of a compact set K has the shape of a platter on K. Secondly we will prove theorem 2.8 which states that under a few assumptions of regularity, a holomorphic function transforms the capacity of a compact set according to its monomial of highest degree. This theorem and its two corollaries 2.10, 2.11, provide a useful tool to calculate some capacities.

A few technical proofs are gathered in the appendix B.1.

2.3.1 • Frostman's theorem

To begin with, let us remind ourselves of the definition of semi-harmonic functions and give two important examples of super-harmonic functions.

Definition 2.9 ((super-,sub-)harmonic functions). Let $D \subset \mathbb{C}$ be an open set. A function $f : D \to \mathbb{R}$ is called *harmonic* (*resp. super-harmonic, sub-harmonic*) if it is continuous (*resp.* lower semi-continuous, upper semi-continuous) and if it verifies the *mean value property* (*resp. super-mean, sub-mean*): for all $z \in D$, if the disk $\{|\zeta - z| \leq r\} \subset D$, we have

$$f(z) = \frac{1}{2\pi} \int_0^{2\pi} f(z + re^{i\theta})\, \mathrm{d}\theta \quad (resp.\ \geq, \leq)$$

Example 2.6 $g(z) = \log \frac{1}{|z-t|}$ is superharmonic and harmonic at points $z \neq t$. □

Example 2.7 Let μ be a positive measure with compact support K, then the potential

$$U^{\mu}(z) = \int \log \frac{1}{|z-t|} \, \mathrm{d}\mu(t)$$

is superharmonic on $\mathbb{C}$ and harmonic on $\mathbb{C}\backslash K$.

Proof. U^{μ} is lower semi-continuous since $\log \frac{1}{|z-t|}$ is for all t. By using Fubini-Tonelli theorem, we obtain

$$\frac{1}{2\pi} \int_0^{2\pi} U^{\mu}(z + re^{i\theta}) \, \mathrm{d}\theta = \int \frac{1}{2\pi} \int_0^{2\pi} \log \frac{1}{|z + re^{i\theta} - t|} \, \mathrm{d}\theta \, \mathrm{d}\mu(t).$$

The example 2.6 gives us that this last integral is smaller than $\int \log \frac{1}{|z-t|} \, \mathrm{d}\mu(t) = U^{\mu}(z)$. Therefore, U^{μ} is superharmonic on $\mathbb{C}$. By considering $z \notin K$ and $r < \mathrm{dist}(z, K)$, it follows from example 2.6 that this last integral is equal to $U^{\mu}(z)$, hence the harmonicity. □

Theorem 2.4 (Maximum principle for potentials). Let μ be a finite positive measure with compact support. If $U^{\mu}(z) \leq M$ for all $z \in \mathrm{supp}(\mu)$, then the same goes for all $z \in \mathbb{C}$.

The proof is given in the appendix B, Corollary B.1.

Let us state and prove an important theorem on equilibrium potentials : Frostman's theorem, which claims that the equilibrium potential has the shape of a platter and is upper bounded every where by Robin's constant (cf. Figure 7).

Theorem 2.5 (Frostman). Let K be a compact subset of $\mathbb{C}$ such that $\mathrm{Cap}(K) > 0$, then

1. $U^{\mu_K}(z) \leqslant V_K$ for all $z \in \mathbb{C}$
2. $U^{\mu_K}(z) = V_K$ for all $z \in K - S$ where $\mathrm{Cap}(S) = 0$
3. $U^{\mu_K}(z) < V_K$ for all $z \in \Omega$ where Ω is the non bounded connected component of $\mathbb{C} - K$

Proof. The formal argument proceeds in three steps. First of all, let us define for $n \geq 1$ the following sets: $K_n = \{z \in K | U^{\mu_K} \leq V_K - 1/n\}$ and $L_n = \{z \in \mathrm{support}\,(\mu_K) \, | U^{\mu_K}(z) > V_K + 1/n\}$. We will first show that the K_n have capacity zero, then that the L_n are empty, and we will finally conclude, using the maximum principle for potentials (2.4).

Let us argue by contradiction to prove that $\mathrm{Cap}(K_n) = 0$. Assume there exists $n \geq 1$ such that $\mathrm{Cap}(K_n) > 0$. We remind that $V_K = I\,(\mu_K) = \int U^{\mu_K} d\mu_K$, therefore, there exists some z_0 in the support of μ_K verifying $U^{\mu_K}\,(z_0) \geq V_K$. By using the lower semi-continuity of U^{μ_K}, there exists a closed ball denoted by B with radius $r > 0$ and center z_0, on which we have $U^{\mu_K}(z) > V_K - 1/2n$. Then, we have $B \cap K_n = \emptyset$, and $\mu_K(B) = a > 0$ because z_0 is in the support of μ_K. To get a contradiction, we want to build a measure that contradicts the fact that V_K is minimal. To do so, we use the assumption that $\mathrm{Cap}(K_n) > 0$. In fact, we can

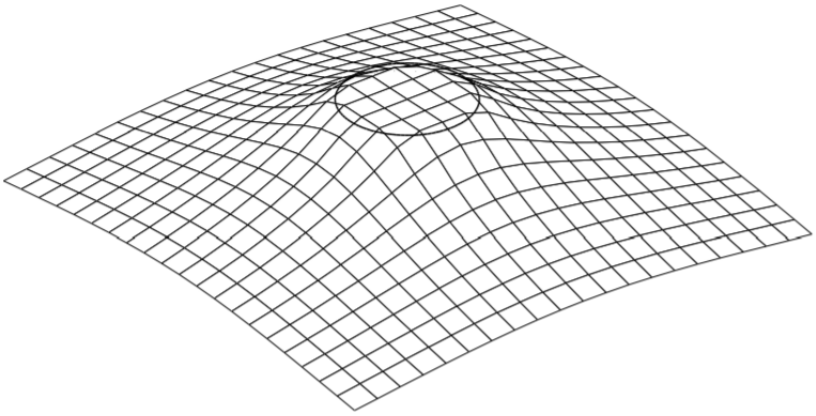


Figure 7: Frostman's theorem

consider a measure μ on K_n such that $I(\mu)$ is finite. We then build the following measure:

$$\sigma = \begin{cases} \mu, & \text{on } K_n \\ -\mu_K/a, & \text{on } B \\ 0, & \text{on the rest} \end{cases}$$

Let us then consider the family of probability measures $\mu_t = \mu_K + t\sigma$ for $t \in]0; a[$. Given how we built B, we obtain :

$$I(\mu_K) - I(\mu_t) \geq 2t\left(V_K - 1/2n - V_K + 1/n\right) + O\left(t^2\right)$$

Therefore for all t sufficiently close to 0 (we remind that here n is fixed), we have $I(\mu_K) = V_K \geq I(\mu_t)$, which contradicts the fact that μ_K is minimal since here , $\mu_t \neq \mu_K$.

Secondly, let us show by contradiction that $L_n = \emptyset$. If one of the L_n is non-empty, using the same argument as earlier, there exists a closed ball $\tilde{B}$ on which $U^{\mu_K}(z) > V_K + 1/n$. As we did earlier, we consider $\tilde{a} = \mu_K(\tilde{B}) > 0$. According to the previous point, we obtain for all n, $\mu_K(K_n) = 0$, therefore, $U^{\mu_K}(z) \geq V_K$ except on a set with measure zero. We then have :

$$\begin{aligned} V_K = I(\mu_K) &= \int_K U^{\mu_K} d\mu_K \\ &= \int_{\tilde{B}} U^{\mu_K} d\mu_K + \int_{K\setminus\tilde{B}} U^{\mu_K} d\mu_K \\ &\geq \left(V_K + \frac{1}{n}\right)\tilde{a} + V_K(1-\tilde{a}) > V_K \end{aligned}$$

We obtain a contradiction, and the L_n are empty.

These two facts allow us to prove the three claims of the theorem : since all the L_n are empty, we have the inequality of the first claim on the support of μ_K, therefore, on $\mathbb{C}$, thanks to the maximum principle. The second claim results from the fact that $\mathrm{Cap}(\bigcup_n K_n) = 0$ which gives us that $U^{\mu_K}(z) \geq V_K$ on $K\setminus\bigcup_n K_n$,

and from the first claim which states that $U^{\mu_K}(z) \leq V_K$. Finally, the last claim results from the harmonicity of U^{μ_K} on Ω.

□

Example 2.8 When $K = \mathbb{U}$ (Prop. 2.5), the potential $U^{\mu_{\mathbb{U}}}(z) = \begin{cases} 0 = V_{\mathbb{U}} \text{ if } |z| \leqslant 1 \\ \log(\frac{1}{|z|}) \text{ if } |z| > 1 \end{cases}$ verifies Frostman's theorem with $S = \emptyset$.

Corollary 2.4 Let $K \subset \mathbb{C}$ be a compact set with $\mathrm{Cap}(K) > 0$ and μ_K its equilibrium measure. Then $U^{\mu_K} \equiv V_K$ in the interior of K. Moreover, since $\mu_K = \mu_{K^{ce}}$ (Cor. 2.3(e)), we have $U^{\mu_K} \equiv V_K$ in the interior of K^{ce}.

Proof. Frostman's theorem implies that

$$U^{\mu_K}(z) = V_K, \quad q - a.e. \text{ in } \partial K$$

On the other hand, U^{μ_K} is superharmonic and lower bounded by $\log(1/d_2(K))$ in K. Then the maximum principle can be applied to U^{μ_K} on each connected component of $\mathring{K}$ to obtain $U^{\mu_K} \geq V_K$ in $\mathring{K}$. However, Frostman's theorem already gives us an upper bound, V_K. Therefore $U^{\mu_K} = V_K$ in $\mathring{K}$.

□

2.3.2 • Calculation of capacities

The goal of this section is theorem 2.8, which states that a holomorphic function transforms the capacity according to its monomial of highest degree, and two corollaries which serve as tools to calculate some capacities.

The main tool of this proof is Green's function with respect to a compact set.

Theorem 2.6 Let $K \subset \mathbb{C}$ be a compact set with $\mathrm{Cap}(K) > 0$ and Ω_K the non bounded connected component of $\mathbb{C}\backslash K$. Then there exists a *unique* function $g_K(\cdot, \infty) : \Omega_K \to \mathbb{R}$ *characterized* by the following properties:

1. $g_K(\cdot, \infty)$ is harmonic on Ω_K and bounded outside of all the neighborhoods of ∞;
2. $g_K(\cdot, \infty) - \log|\cdot|$ is bounded on a neighborhood of ∞;
3. $\lim_{z \to \zeta} g_K(z, \infty) = 0$ *q-a.e.* in $\partial\Omega_K$.

Proof. The existence is given by Frostman's theorem and example 2.7 if we consider

$$g_K(z, \infty) = V_K - U^{\mu_K}(z). \tag{1}$$

Let g, g' be two functions verifying these three properties, then $g - g'$ is harmonic and bounded on Ω_K, and therefore can be extended to a harmonic function on $\Omega_K \cup \{\infty\}$. According to the second point, we have $g(z) > 0$ (*resp.* $g'(z) > 0$) for $R \gg 0$ so that $K \subset B(0, R)$; the minimum principle applied on $\Omega_K \cap B(0, R)$ gives us that $g(z) > 0$ (*resp.* $g'(z) > 0$) on $\Omega_K \cap B(0, R)$, and then on Ω_K. The uniqueness results from the third property and the minimum principle applied twice on $\Omega_K \cup \{\infty\}$ to $g(z) - g'(z)$ and $g'(z) - g(z)$ respectively. □

Definition 2.10 Let us denote by $g_K(\cdot,\infty):\Omega_K\to\mathbb{R}$ *the Green's function with respect to* K*, with a pole at infinity.*

Corollary 2.5 Let $K\subset\mathbb{C}$ be a compact set such that $\mathrm{Cap}(K)>0$. We then have $g_K(\cdot,\infty)>0$ on Ω_K.

Corollary 2.6 If two compact sets $K_1,K_2\subset\mathbb{C}$ are such that $\mathrm{Cap}(K_1)>0$ or $\mathrm{Cap}(K_2)>0$, and that $\Omega_{K_1}=\Omega_{K_2}$, then

$$g_{K_1}(\cdot,\infty)=g_{K_2}(\cdot,\infty).$$

In particular, let $K\subset\mathbb{C}$ be a compact set with $\mathrm{Cap}(K)>0$, then

$$g_K(\cdot,\infty)=g_{\partial K}(\cdot,\infty)=g_{\partial_\infty K}(\cdot,\infty)=g_{K^{ce}}(\cdot,\infty).$$

Proof. Note that the three claims in Thm. 2.6 only depend on Ω_K, the non bounded connected component of $\mathbb{C}\backslash K$; therefore the result immediately follows from the definition and Cor. 2.3. □

Theorem 2.7 Let $K\subset\mathbb{C}$ be a compact set with $\mathrm{Cap}(K)>0$ and $g_K(\cdot,\infty)$ Green's function with respect to K, with a pole at infinity. Then

1. $g_K(z,\infty)=\log|z|+V_K+o_{z\to\infty}(1)$;
2. The equilibrium potential of K is $U^{\mu_K}=V_K-g_K(\cdot,\infty)$; then (Thm. 2.5) $g_K(\cdot,\infty)>0$ on Ω_K.

Proof. It immediately results from the formula (1) given in the proof of theorem 2.6 and in the definition of the potential U^{μ_K}. □

Let us define the notion of regularity of a compact set. We will see later that it is the right assumption to link the capacity of two compact sets and thanks to Prop 2.7, it is a special case that will be useful in a more general approach.

Definition 2.11 Let $K\subset\mathbb{C}$ be a compact set such that $\mathrm{Cap}(K)>0$. We call $\zeta_0\in\partial\Omega_K$ a *regular point* if

$$\lim_{\Omega_K\ni z\to\zeta_0}U^{\mu_K}(z)=V_K;$$

otherwise, we write that ζ_0 is an *irregular point*. We write that Ω_K is a *regular set* if all the points of $\partial\Omega_K$ are regular.

According to the relation between the potential and Green's function (Thm. 2.7), we have the following property :

Corollary 2.7 A point $\zeta_0\in\partial\Omega_K$ is regular if and only if $\lim_{z\to\zeta_0}g_K(z,\infty)=0$.

Proposition 2.5 Let $K\subset\mathbb{C}$ be a compact set such that $\mathrm{Cap}(K)>0$. Then $U^{\mu_K}(\zeta_0)=V_K$ implies the continuity of U^{μ_K} at point ζ_0. The reciprocal implication is true if $\zeta_0\in\mathrm{supp}(\mu_K)$.

Proof. It follows from the semi-continuity of U^{μ_K} and Frostman's theorem that:

$$U^{\mu_K}(\zeta_0) \leq \liminf_{z\to\zeta_0} U^{\mu_K}(z) \leq \limsup_{z\to\zeta_0} U^{\mu_K}(z) \leq V_K.$$

Therefore if $U^{\mu_K}(\zeta_0) = V_K$, U^{μ_K} is continuous at point ζ_0.

Conversely, if U^{μ_K} is continuous at point ζ_0 and $U^{\mu_K}(\zeta_0) < V_K$, then there exists $r > 0$ such that $U^{\mu_K} < V_K$ on $\overline{B(\zeta_0, r)}$, therefore according to Frostman's theorem, $\mathrm{Cap}(\overline{B(\zeta_0, r)}) \cap K) \leq \mathrm{Cap}(S) = 0$, then according to Prop. 2.4(f), we have

$$\mu_K(\overline{B(\zeta_0, r)} \cap K) = 0.$$

Therefore $\mu_K(\overline{B(\zeta_0, r)}) = 0$ and we deduce from it that $\zeta_0 \notin \mathrm{supp}(\mu_K)$. □

Corollary 2.8 Let us consider $\zeta_0 \in \mathrm{supp}(\mu_K)$ then for all $r > 0$, $\mathrm{Cap}(B(\zeta_0, r) \cap K) > 0$.

Proof. It is indeed the contrapositive of the last argument of the previous proof. □

Corollary 2.9 The set of all irregular points has capacity zero.

Proof. Let us assume that $\mathrm{Cap}(K) > 0$. Then the corollary results from Frostman's theorem. □

To get a sufficient condition of regularity, let us introduce the following notion:

Definition 2.12 Let us consider $\Omega \subset \mathbb{C}$. We write that Ω verifies the *cone condition* if for all $\zeta \in \partial\Omega$, there exists $\zeta_1 \neq \zeta$ such that the segment $[\zeta, \zeta_1] \subset \mathbb{C}\backslash\Omega$.

Proposition 2.6 Let $K \subset \mathbb{C}$ be a compact set with $\mathrm{Cap}(K) > 0$. If Ω_K verifies the cone condition, then Ω_K is a regular set.

The proof is given in appendix C.1.

The following proposition will be useful in order to consider the domain regular.

Proposition 2.7 Let $K \subset \mathbb{C}$ be a non-empty compact set and let $K^\epsilon = \{z \in \mathbb{C} : \mathrm{dist}(z, K) \leq \epsilon\}$. Then $\mathrm{Cap}(K^\epsilon) > 0$ and Ω_{K^ϵ} verifies the cone condition, therefore Ω_{K^ϵ} is regular.

Proof. Since the interior of K^ϵ is non-empty, we have $\mathrm{Cap}(K^\epsilon) > 0$. Moreover, by definition, all points ζ in ∂K^ϵ are exactly at a distance of ϵ from K, therefore there exists $\zeta_1 \in K$ such that $[\zeta, \zeta_1] \subset K^\epsilon \subset \mathbb{C}\backslash\Omega_K$. □

We will now prove a few results that allow us to compare the capacity of two compact sets thanks to holomorphic functions and the notion of regularity previously defined.

Lemma 2.3 Let f be a non locally constant holomorphic function defined at ∞ by $f(\infty) = \infty$. Then there exists some integer $n \in \mathbb{N}^*$ and some $A \neq 0$ such that

$$f(z) \sim Az^n, \quad z \to \infty$$

$$\log|f(z)| = n\log|z| + \log|A| + o(1), \quad z \to \infty$$

Let us define $A_f = A, n_f = \mathrm{ord}_\infty(f) = n$. □

Theorem 2.8 Let $K_1, K_2 \subset \mathbb{C}$ be two non-empty compact sets. Let $f : \Omega_{K_1} \cup \{\infty\} \to \Omega_{K_2} \cup \{\infty\}$ be a non constant holomorphic function such that $f(\infty) = \infty$. Then,

(a) $|A_f| \operatorname{Cap}(K_1)^{n_f} \geq \operatorname{Cap}(K_2)$.

(b) Moreover assume that :

(i) $\operatorname{Cap}(K_2) > 0$;
(ii) $f^{-1}(\infty) = \{\infty\}$;
(iii) Ω_{K_2} is regular;
(iv) f can be continuously extended to the boundaries $\partial\Omega_{K_1} \to \partial\Omega_{K_2}$.

Then, $\operatorname{Cap}(K_1)>0$, Ω_{K_1} is a regular set and

$$g_{K_1}(\cdot, \infty) = \frac{1}{n_f} g_{K_2}(f(\cdot), \infty)$$

$$|A_f| \operatorname{Cap}(K_1)^{n_f} = \operatorname{Cap}(K_2).$$

The complete proof is provided in the appendix B.1.

To understand how to apply this theorem, let us see when the conditions in (b) are verified:

(ii) holds when f is biholomorphic, or when f is a polynomial;
(iii) holds when Ω_K verifies the cone condition (Prop. 2.6).

We therefore have the two following corollaries (by applying the same technique as in Prop. 2.7 if necessary):

Corollary 2.10 If f is biholomorphic, we have $n_f = n_{f^{-1}} = 1$ and $A_f A_{f^{-1}} = 1$; Let us apply (a) twice to obtain (with notation $f'(\infty) = A_f$)

$$|f'(\infty)| \operatorname{Cap}(K_1) = \operatorname{Cap}(K_2).$$

□

Corollary 2.11 Assume that f is a polynomial function of degree n:

$$f(z) = \sum_{i=0}^{n} a_i x^i, \quad a_n \neq 0.$$

Let $K \subset \mathbb{C}$ be a compact set. Then

$$|a_n| \operatorname{Cap}(f^{-1}(K))^n = \operatorname{Cap}(K).$$

Proof. Assume that $K \neq \emptyset$. Let us try to apply theorem 2.8 (b). Since f is a polynomial function, (ii) is verified for all compacts in $\mathbb{C}$. For $\epsilon > 0$, let us consider $K^\epsilon = \{z \in \mathbb{C} : \operatorname{dist}(z, K) \leq \epsilon\}$. Let us show that the conditions (i),(iii),(iv) of the theorem are verified for the compact sets $f^{-1}(K^\epsilon)$ and K^ϵ and that $f(\Omega_{f^{-1}(K^\epsilon)}) \subset \Omega_{K^\epsilon}$; It will result in

$$|a_n| \operatorname{Cap}(f^{-1}(K^\epsilon))^n = \operatorname{Cap}(K^\epsilon).$$

When $\epsilon \to 0$, it allows us to conclude.

(i) K^ϵ has a non-empty interior, therefore $\operatorname{Cap}(K^\epsilon) > 0$ (Cor. 2.3).

(iii) results from Prop. 2.6 and Prop. 2.7.

(iv) We will actually prove this claim for all compact sets K (instead of K^ϵ). A topological analysis shows that $f(\partial f^{-1}(K)) = \partial K$. We have left to prove that $f(\partial\Omega_{f^{-1}(K)}) \subset \partial\Omega_K$. We have $f(\infty) = \infty$ and K a compact set, therefore $f^{-1}(K)$ is a compact set; likewise, the inverse image of each (open) bounded connected component of $\mathbb{C}\backslash K$ is bounded, therefore included in one of the bounded component of $f^{-1}(K)$. Therefore $\Omega_{f^{-1}(K)} \subset f^{-1}(\Omega_K)$, then

$$f(\Omega_{f^{-1}(K)}) \subset \Omega_K$$

$$f(\partial\Omega_{f^{-1}(K)}) \subset \overline{\Omega_K}.$$

We finally obtain that

$$f(\partial\Omega_{f^{-1}(K)}) \subset \overline{\Omega_K} \cap \partial K = \partial\Omega_K,$$

which allows us to apply theorem 2.8 (b) to obtain the final result. □

2.4 Chebyshev constant

Let us now give a third equivalent definition of the capacity, defined thanks to Chebyshev polynomials. This point of view is very useful to calculate the capacity of segments of $\mathbb{R}$.

First, let us state the equioscillation theorem :

Theorem 2.9 (Equioscillation). Let us consider $n \in \mathbb{N}$. Let f be a continuous function on $[a, b]$. Let us consider $P \in \mathbb{R}_n[X]$. P minimizes $||f - P||_{\infty,[a,b]}$ if and only if there exists $n + 2$ points $a \leqslant x_0 < x_1 < \dots x_{n+1} \leqslant b$ such that $f(x_i) - P(x_i) = \pm(-1)^i ||f - P||_{\infty,[a,b]}$

The proof of this theorem is not that hard but is quite long. In order not to overfill this paper, we advise the reader to read article [8] for a complete and illustrated proof.

Definition 2.13 (The Chebyshev constant). Let us consider some $n \in \mathbb{N}$ and K a compact subset of $\mathbb{C}$, let us denote by $||\cdot||_K$ the uniform norm on K and :

$$t_n(K) = \inf_{P \in \mathbb{C}_{n-1}[X]} ||X^n + P||_K.$$

If K contains an infinite number of points, there exists a unique monic polynomial $T_n \in \mathbb{R}_n[X]$, called Chebyshev polynomial such that $t_n(K) = ||T_n||_K$.

Let us define the Chebyshev constant as follows :

$$\mathrm{Cheb}(K) = \lim_{n\to+\infty} t_n(K)^{\frac{1}{n}}.$$

Proof.

- If K is an infinite set, $||\cdot||_K$ is a norm on $\mathbb{C}[X]$. The existence of T_n follows from the fact that the distance to a closed vector subspace is reached. The uniqueness follows from the reciprocal implication of the equioscillation theorem (2.9).
- Let us consider $n, m \in \mathbb{N}$. Since T_nT_m is a monic polynomial of degree $n+m$, we have

$$||T_{n+m}||_K = \inf_{\substack{P\in\mathbb{C}_{n+m}[X]\\ \text{monic}}} ||P||_K \leqslant ||T_nT_m||_K \leqslant ||T_n||_K||T_m||_K$$

  Therefore $t_{n+m}(K) \leqslant t_n(K)t_m(K)$ and $(\log(t_n(K)))_{n\in\mathbb{N}}$ is sub-additive. It follows from the sub-additivity lemma that $(\frac{1}{n}\log(t_n(K)))_{n\in\mathbb{N}}$ converges, which proves that $\mathrm{Cheb}(K)$ is well defined.

□

The Chebyshev constant is equivalent to the logarithmic capacity and the transfinite diameter :

Theorem 2.10 Let us consider K a compact subset of $\mathbb{C}$, then

$$\tau(K) = \mathrm{Cap}(K) = \mathrm{Cheb}(K).$$

Let $\mathcal{F}_n = \{z_1^{(n)}, \dots, z_n^{(n)}\}$ be a set of n Fekete points and $F_n(X) = \prod_{i=1}^{n}(X - z_n^{(i)})$ the associated Fekete polynomial. We have

$$\lim_{n\to+\infty} ||F_n||_K^{1/n} = \mathrm{Cheb}(K).$$

Moreover, if $\mathrm{Cap}(K) > 0$, noting μ_K the equilibrium measure of K, we have

$$\forall z \in \mathbb{C}\backslash K, \lim_{n\to+\infty} F_n(z)^{\frac{1}{n}} = \exp(-U^{\mu_K}(z))$$

The convergence is uniform on all compact subsets of $\mathbb{C}\backslash K$.

Proof. We argue using theorem 2.3.

- Let us consider $n \in \mathbb{N}$, $z \in \mathbb{C}$ and $\mathcal{F}_n = \{z_1^{(n)}, \dots, z_n^{(n)}\}$ a set of n Fekete points.
  Let us consider $\{y_1, \dots, y_{n+1}\} = \{z_1^{(n)}, \dots, z_n^{(n)}, z\}$, then

$$\delta_{n+1}(K)^{n(n+1)/2} = \max_{\{y_1,\dots,y_{n+1}\}\subset K} \prod_{1\leqslant i<j\leqslant n+1} |y_i - y_j| \geqslant \prod_{i=1}^{n} |z - z_i^{(n)}| \prod_{1\leqslant i<j\leqslant n} |z_i^{(n)} - z_j^{(n)}|$$

  Let $F_n = \prod_{i=1}^{n}(X - z_i^{(n)})$. Since $\mathcal{F}_n$ is a set of Fekete points :

$$\delta_{n+1}(K)^{n(n+1)/2} \geqslant |F_n(z)|\delta_n(K)^{(n-1)n/2}.$$

By considering $\sup_{z\in K}$, we obtain $||F_n||_K \leqslant \left(\frac{\delta_{n+1}(K)}{\delta_n(K)}\right)^{(n-1)n/2} \delta_{n+1}(K)^n$. However, the $\delta_n(K)$ are decreasing, therefore $||F_n||_K^{1/n} \leqslant \delta_{n+1}(K)$. Moreover by definition, $t_n(K) \leqslant ||F_n||_K^{1/n} \leqslant \delta_{n+1}(K)$. Finally, by considering the limit, we have

$$\tau(K) \geqslant \limsup_{n\to\infty} ||F_n||_K^{1/n} \geqslant \liminf_{n\to\infty} ||F_n||_K^{1/n} \geqslant \mathrm{Cheb}(K).$$

- To conclude, it is enough to show that $\mathrm{Cheb}(K) \geqslant \tau(\mathrm{K})$. If $\tau(K) = 0$, it is trivial, otherwise K contains an infinite number of points and we can consider $T_n = \prod_{i=1}^{n}(X - x_i)$, the n-th Chebyshev polynomial with respect to K and $\nu(T_n)$ the counting measure with respect to $x_1, \dots, x_n$.
  Since $x \in \mathbb{R}_+^* \mapsto \log\frac{1}{x}$ is a decreasing function,

$$\frac{1}{n}\log\frac{1}{t_n(K)} = \inf_{z\in K}\frac{1}{n}\log\frac{1}{|T_n(z)|} = \inf_{z\in K}\frac{1}{n}\sum_{i=1}^{n}\log\frac{1}{|z-x_i|} = \inf_{z\in K} U^{\nu(T_n)}(z).$$

  It follows from prop A.3 that:

$$\inf_{z\in K} U^{\nu(T_n)}(z) = \mu_K(\inf_{z\in K} U^{\nu(T_n)}(z)) \leqslant \mu_K(U^{\nu(T_n)}).$$

  Then,

$$\mu_K(U^{\nu(T_n)}) = \mu_K(\frac{1}{n}\sum_{i=1}^{n}\log\frac{1}{|z-x_i|}) = \frac{1}{n}\sum_{i=1}^{n}\mu_K(\log\frac{1}{|z-x_i|}) = \nu(T_n)(U^{\mu_K})$$

  Frostman's theorem 2.5 gives us that

$$\frac{1}{n}\log\frac{1}{t_n(K)} \leqslant \nu(T_n)(U^{\mu_K}) \leqslant V_K.$$

  Finally, passing to the limit $n \to +\infty$ and composing by $x \mapsto e^{-x}$, we obtain :

$$\mathrm{Cheb}(K) \geqslant \mathrm{Cap}(K) = \tau(K),$$

  which concludes the first claim of the theorem.

- Let $f_n(z) = \log(|F_n(z)|^{1/n}) = \frac{1}{n}\sum_{k=1}^{n}\log|z - t_k|$ where $t_1, \dots, t_n$ are the roots of F_n. Let L be a compact subset of $\mathbb{C} - K$, then :

$$\forall t \in K, \forall z \in L, \log d(L,K) \leqslant \log|z-t| \leqslant \log\sup_{z'\in L, t'\in K}|z'-t'|.$$

  However, by compactness of L and K, $d(L,K) \geqslant 0$ and $\sup_{z'\in L,t'\in K}|z'-t'| < \infty$.
  Moreover, we have

$$\begin{aligned}\forall n \in \mathbb{N}, \forall z \in L,\ |f_n(z)| &\leqslant \frac{1}{n}\sum_{k=1}^{n}\left|\log\left(\frac{1}{d(L,K)} + \sup_{z'\in L,t'\in K}|z'-t'|\right)\right| \\ &\leqslant \left|\log\left(\frac{1}{d(L,K)} + \sup_{z'\in L,t'\in K}|z'-t'|\right)\right| < \infty.\end{aligned}$$

therefore the f_n are uniformly bounded on L. Therefore, f_n is a sequence of holomorphic functions, uniformly bounded on all compact sets, which converges pointwise on $\mathbb{C}\backslash K$. It follows from Vitali theorem that the convergence is uniform on all compact sets.

□

This new definition of capacity allows us to calculate the capacity of a segment in a simple manner.

Example 2.9 (Capacity of a segment). The capacity of a segment with length $2l$ is equal to $\frac{l}{2}$.

Proof.

- Let us first prove the claim when the segment can be written as $[-l, l]$.
  Let us denote by $\tilde{T}_n$ the unique polynomial verifying:

$$\forall \theta \in \mathbb{R}, \tilde{T}_n(l\cos(\theta)) = lcos(n\theta)$$

  The uniform norm of $\tilde{T}_n$ is obviously equal to l. And like in the well-known case $[-1, 1]$, we show easily that our polynomial reaches alternatively $\pm l$ at $n+1$ distinct points. (1)
  Using De Moivre's formula, we show that the leading coefficient of $\tilde{T}_n$ is equal to $c := (\frac{2}{l})^{n-1}$.
  Minimizing $\|P\|_{[-l,l]}$, for $P \in \mathbb{C}_n[X]$ a monic polynomial, is equivalent to minimizing $\|X^n - Q\|_{[-l,l]}$ for Q living in $\mathbb{C}_{n-1}[X]$. In other words, we are trying to calculate the distance of X^n to $\mathbb{C}_{n-1}[X]$. Let us consider $Q^\star := X^n - \frac{1}{c}\tilde{T}_n(X)$. We obviously have that $Q^\star \in \mathbb{C}_{n-1}[X]$. Moreover, $X^n - Q^\star = \frac{1}{c}\tilde{T}_n(X)$, which *equioscillates* at $n+1$ points according to (1). Therefore, it follows from lemma 2.1 that $Q^\star$ minimizes the distance of X^n from polynomials of $\mathbb{C}_{n-1}[X]$. Therefore $\frac{1}{c}\tilde{T}_n$ is the Chebyshev polynomial with respect to $[-l, l]$.
  Hence $t_n([-l, l]) = \|\frac{1}{c}\tilde{T}_n(X)\| = \frac{l}{c} = l(\frac{l}{2})^{n-1}$.
  Therefore, $\text{Cheb}([-l, l]) = \lim\limits_{n\to\infty} t_n([-l, l])^{\frac{1}{n}} = \frac{l}{2}$.

- In the general case of a segment of the form $[a, b]$, with length $2l$, it is enough to consider the following polynomial function: $\tilde{T}_n(X - (a+l))$ which, on $[a, b]$, has the same behavior as $\tilde{T}_n$ on $[-l, l]$. Therefore, the capacity is not changed by the translation. Hence $\text{Cheb}([a, b]) = \frac{l}{2}$.

□

Let us now calculate the capacity of the union of two segments, which is symmetric with respect to the origin 0.

Example 2.10 Let us consider $0 \leqslant b < a$. Then $\text{Cheb}([-a, -b] \cup [b, a]) = \frac{\sqrt{a^2-b^2}}{2}$.

Proof. Let us consider F an infinite compact subset of $\mathbb{C}$ and denote by T_n^F the Chebyshev polynomial of degree n with respect to F. Let us consider $E = [-a, -b] \cup [b, a]$.

- Let us consider $k \in \mathbb{N}$. Let us show that T_{2k}^E is even.

$$\left\| \frac{T_{2k}^E(X) + T_{2k}^E(-X)}{2} \right\|_E \leqslant \frac{1}{2}(\left\|T_{2k}^E(X)\right\|_E + \left\|T_{2k}^E(-X)\right\|_E)$$

  But E is symmetric with respect to the origin, therefore

$$\left\|T_{2k}^E(-X)\right\|_E = \sup_{z\in E} \left|T_{2k}^E(-z)\right| = \sup_{z\in E} \left|T_{2k}^E(z)\right| = \left\|T_{2k}^E(-X)\right\|_E .$$

  Thus $\left\| \frac{T_{2k}^E(X)+T_{2k}^E(-X)}{2} \right\|_E \leqslant \left\|T_{2k}^E\right\|_E$ and by the uniqueness of the Chebyshev polynomial of degree $2k$, $T_{2k}^E = \frac{T_{2k}^E(X)+T_{2k}^E(-X)}{2}$. Therefore T_{2k}^E is even.

- We deduce from it that T_{2k}^E can be written as follows: $q(X^2)$ with $q \in \mathcal{P}_k$, the set of monic polynomials of degree k. As a result :

$$\begin{aligned} t_{2k}(E) &= \inf_{q\in\mathcal{P}_k} \sup_{x\in E} |q(x^2)| \\ &= \inf_{q\in\mathcal{P}_k} \sup_{x^2\in[b^2,a^2]} |q(x^2)| \\ &= \inf_{q\in\mathcal{P}_k} \sup_{y\in[b^2,a^2]} |q(y)|. \end{aligned}$$

  Therefore $T_{2k}^E = T_k^{[b^2,a^2]}(X^2)$. But in the example 2.9 we saw that $(\frac{2}{l})^{k-1} T_k^{[-l,l]}(l\cos(\theta)) = l\cos(k\theta)$. Therefore, by considering $x = l\cos(\theta)$, we have :

$$T_k^{[-l,l]}(x) = \frac{l^k}{2^{k-1}} \cos\left(k \arccos\left(\frac{x}{l}\right)\right).$$

  Then by translation we obtain :

$$T_k^{[b^2,a^2]}(x) = \frac{(a^2-b^2)^k}{2^{2k-1}} \cos\left(k \arccos\left(2\frac{x-b^2}{a^2-b^2} - 1\right)\right).$$

  And finally $T_{2k}^E(x) = \frac{(a^2-b^2)^k}{2^{2k-1}} \cos\left(k \arccos\left(2\frac{x^2-b^2}{a^2-b^2} - 1\right)\right)$.

- $t_{2k}(E) = \left\|T_{2k}^E\right\|_E = 2\left(\frac{\sqrt{a^2-b^2}}{2}\right)^{2k}$. Hence

$$\mathrm{Cheb}(E) = \lim_{k\to\infty} t_{2k}(E)^{\frac{1}{2k}} = \lim_{k\to\infty} \left(2\left(\frac{\sqrt{a^2-b^2}}{2}\right)^{2k}\right)^{\frac{1}{2k}} = \frac{\sqrt{a^2-b^2}}{2}.$$

□

3
FEKETE'S THEOREM. FEKETE-SZEGÖ'S THEOREM

Now that we have introduced the notion of capacity and showed the equivalence between the three definitions (transfinite diameter/potential/Chebyshev polynomials), let us now focus on how this notion gives us information on the fact that there is (or not) an infinite number of algebraic integers totally in a given compact set. The goal of this section is to prove Fekete's theorem (Thm. 3.1) and Fekete-Szegö's theorem (Thm. 3.3) : the former states that if the capacity of a compact set is strictly smaller than 1, there is a finite number of algebraic integers totally in it; the latter states that if the capacity of the compact set is greater than or equal to 1, we can find an infinite number of algebraic integers totally in any neighborhood (with respect to $\mathbb{C}$) of the compact set.

3.1 Fekete's theorem

This section is dedicated to the proof of Fekete's theorem.

Theorem 3.1 (Fekete). Let $K \subset \mathbb{C}$ be a compact set with $\mathrm{Cap}(K) < 1$. Then there exists an open neighborhood U of K such that the set of the algebraic integers totally in U is finite. In particular, there is a finite number of algebraic integers totally in K.

The proof mainly comes from the fact that $\tau(K) = \mathrm{Cap}(K)$.

Proof. It is enough to prove the last claim of the theorem; in fact, since $\mathrm{Cap}(K) < 1$, we have $\mathrm{Cap}(K^\epsilon) < 1$ for some $\epsilon > 0$ sufficiently small, where $K^\epsilon = \{z \in \mathbb{C} : \mathrm{dist}(z, K) \leq \epsilon\}$; for such a ϵ, $U = \overset{\circ}{K^\epsilon}$ verifies the assumption of the theorem. Assume that E_K, the set of algebraic integers totally in K, is infinite and let us argue by contradiction.

Let us start with the case where the degrees of all the minimal polynomials p of $\zeta \in E_K$ are bounded by an integer $N > 0$. Then the coefficient before $X^{\deg(p)-i}$ is bounded by

$$\binom{\deg(p)}{i} \|K\|_\infty^i \leq \binom{N}{i} \|K\|_\infty^i, \quad \text{where } \|K\|_\infty = \max_{z \in K} |z| .$$

There is only a finite number of such minimal polynomials (we remind that the coefficients are integer), hence $\#E_K < \infty$, which contradicts our initial assumption.

Otherwise, there exists a sequence $\zeta_n \in E_K$ such that the sequence $d_n = \deg(p_n)$ is strictly increasing, where $p_n \in \mathbb{Z}[X]$ is the (monic) minimal polynomial of ζ_n.

Let us remind ourselves of the notion of n-distance (Definition 2.1) :

$$\delta_n(K) = \max_{z_1,\dots,z_n \in K} \prod_{i<j} |z_i - z_j|^{2/n(n-1)}$$

And the capacity as the transfinite diameter :

$$\tau(K) = \lim_{n \to +\infty} \delta_n(K)$$

Let us notice that

$$\delta_{d_n}(K)^{d_n(d_n-1)} \geq \left| \prod_{\xi \neq \eta \in \mathrm{Gal}(\zeta_n)} (\xi - \eta) \right| = \left| \prod_{\xi \in \mathrm{Gal}(\zeta_n)} p_n'(\xi) \right| \geqslant 1$$

The equality in the middle results from the fact that p_n only has simple roots. Moreover, as a symmetric combination with integer coefficients of the ξ (the roots of p_n), $\prod_{\xi \in \mathrm{Gal}(\zeta_n)} p_n'(\xi)$ is an integer, according to remark 1.4, non-zero since the roots are simple, therefore greater than 1.

Therefore $\delta_{d_n}(K) \geq 1$, hence $\tau(K) \geq 1$ by passing to the limit $n \to +\infty$, which leads to a contradiction because $\tau(K) = \mathrm{Cap}(K) < 1$. □

3.2 Fekete-Szegö's theorem

This section is dedicated to the proof of Fekete-Szegö's theorem 3.3. Let us first define a set which plays a major part in the proof, the *Hilbert lemniscate* :

Definition 3.1 Let $p \in \mathbb{C}[X]$ be a *monic* polynomial of degree $d > 0$ and $\rho \in \mathbb{R}_+^\star$ a real constant. The *lemniscate of polynomial p and constant ρ* is the following set

$$L = L_{p,\rho} = p^{-1}\big(\overline{B}(0, \rho^d)\big) = \{z \in \mathbb{C} |\, |p(z)| \leq \rho^d\}.$$

Remark 3.1 According to corollary 2.11, we have $\mathrm{Cap}(L_{p,\rho}) = \mathrm{Cap}\big(\overline{B}(0,\rho^d)\big)^{1/d}$, which is equal to ρ thanks to corollary 2.1 and theorem 2.3.

The idea of the proof of Fekete-Szegö's theorem is to find an infinite number of algebraic integers totally in a set. Hilbert lemniscates provide us with examples of such sets :

Proposition 3.1 Let $P \in \mathbb{Z}[X]$ be a monic polynomial. The lemniscate $L_{P,1} = \{z \in \mathbb{C} \mid |P(z)| \leqslant 1\}$ contains an infinite number of algebraic integers totally in it.

Proof. Let us consider $S = \bigcup_{n \in \mathbb{N}^*} \{z \in \mathbb{C} \mid P(z)^n = 1\}$. The function $\left\{ \begin{array}{ccc} S & \to & \mathbb{U} \\ z & \mapsto & P(z) \end{array} \right.$ is well defined, surjective since $\mathbb{C}$ is algebraically closed. Therefore S is infinite. Moreover, the elements of S are algebraic integers totally in S (since they are the roots of $P^n - 1 \in \mathbb{Z}[X]$ monic, for some n). We conclude by noticing that $S \subset L_{P,1}$.

□

The main step of the proof is the following theorem which states that, under some assumptions, we can always find a Hilbert lemniscate in any neighborhood of the compact set.

Theorem 3.2 (Hilbert's lemniscate). Let $K \subset \mathbb{C}$ be a compact set with $\mathrm{Cap}(K) > 0$ and $U \supset K$ an open neighborhood of K such that $\mathbb{C} \backslash U$ is connected. Then there exists a monic polynomial $p \in \mathbb{C}[X]$ of degree $d > 0$ and a constant $\rho > \mathrm{Cap}(K)$ such that

$$K \subset L_{p,\rho} \subset U.$$

Proof. This proof relies on theorem 2.10 (Chebyshev constant) and theorem 2.5 (Frostman).

Even if it means restricting U, we can assume that U is bounded. Let us consider $R > 0$ such that

$$K \subset U \subset B(0, R)$$

It follows from Frostman's theorem that $U^{\mu_K}(z) < V_K$ for all $z \in \overline{B}(0, R)\backslash U$. Therefore there exists $\varepsilon > 0$ such that

$$\forall z \in \overline{B}(0, R)\backslash U,\ U^{\mu_K}(z) \leqslant V_K - \varepsilon$$

This upper bound is uniform since $\overline{B}(0, R)\backslash U$ is compact.

According to the last claim of theorem 2.10, $\log \frac{1}{F_n^{\frac{1}{n}}}$ uniformly converges to U^{μ_K} : there exists $n_0 \in \mathbb{N}$ such that for all $n \geqslant n_0$,

$$\forall z \in \overline{B}(0, R)\backslash U,\ \left| \log \frac{1}{|F_n(z)|^{\frac{1}{n}}} - U^{\mu_K}(z) \right| < \varepsilon/2$$

which implies that

$$\forall z \in \overline{B}(0, R)\backslash U, \log \frac{1}{|F_n(z)|^{\frac{1}{n}}} < V_K - \varepsilon/2$$

in other words,

$$\forall z \in \overline{B}(0, R)\backslash U,\ |F_n(z)|^{\frac{1}{n}} > e^{-V_K + \varepsilon/2} = \mathrm{Cap}(K) e^{\varepsilon/2}$$

But $z \mapsto \frac{1}{F_n(z)}$ is holomorphic on $\mathbb{C}\backslash U$, therefore it follows from the maximum modulus principle that the previous inequality holds for all $z \in \mathbb{C}\backslash U$. Let us consider $\rho := \mathrm{Cap}(K) e^{\varepsilon/2}$, we then have $L_{F_n, \rho} \subset U$ for all $n \geqslant n_0$. On the other hand, according to theorem 2.10, there exists $n_1 \in \mathbb{N}$ such that for all $n \geqslant n_1$,

$$||F_n||_K^{\frac{1}{n}} < \mathrm{Cap}(K) e^{\varepsilon/2} = \rho$$

By considering $d = \max(n_0, n_1)$, we have $K \subset L_{F_d, \rho} \subset U$.

□

Let us now prove Fekete-Szegö's theorem :

Theorem 3.3 (Fekete-Szegö). Let $K \subset \mathbb{C}$ be a compact set that is symmetric with respect to complex conjugation and such that $\mathrm{Cap}(K) \geq 1$. If U is an open set containing K such that $C\backslash U$ is connected, then U contains an infinite number of algebraic integers totally in U.

Proof. The idea is to find a known set included in U, which contains an infinite number of algebraic integers totally in it. According to proposition 3.1, the lemniscate of a monic polynomial with integer coefficients seems to be a good contender. The theorem 3.2 gives us a lemniscate $L_{p,\rho}$ included in U, but for a polynomial P with complex coefficients (and $\rho > 1$). We must now bring its coefficients to $\mathbb{Z}$.

Even if it means considering $U \cup U^\star$ (where $U^\star$ is the set of the complex conjugates of the elements of U), we can assume that U is symmetric with respect to the real axis. Under this assumption, we have

$$\forall z \in \mathbb{C}\backslash U,\ |p(z)| > \rho^d > 1,$$

then

$$\forall z \in \mathbb{C}\backslash U,\ |p(z)\,\overline{p}(z)| > \rho^{2d} > 1,$$

Therefore $L_{p\,\overline{p},\rho} \subset U$ and $p\,\overline{p} \in \mathbb{R}[X]$. We keep on denoting p this polynomial with real coefficients.

Then assume that $U \subset \overline{B}(0,R)$, even if it means restricting the open set U. We have

$$\forall z \in \overline{B}(0,R)\backslash U,\ \left|\frac{1}{p(z)}\right| < \rho^{-d}.$$

It follows from the density of $\mathbb{Q}$ in $\mathbb{R}$ and the continuity of the roots (since $|z| \leqslant R$) that we can choose a polynomial $q \in \mathbb{Q}[X]$ whose roots are still all in U and such that

$$\forall z \in \overline{B}(0,R)\backslash U,\ \left|\frac{1}{q(z)}\right| < \rho^{-d}.$$

And since $\frac{1}{q}$ is holomorphic on $\mathbb{C}\backslash U$, the maximum modulus principle gives:

$$\forall z \in \mathbb{C}\backslash U,\ \left|\frac{1}{q(z)}\right| < \rho^{-d},$$

which implies that $L_{q,\rho} \subset U$.

We now have to bring the coefficients of q to $\mathbb{Z}$, which is the goal of the two following lemmas (3.1, 3.2). □

Lemma 3.1 Let us consider $p \in \mathbb{Q}[X]$ of degree $d \geq 1$ and $n \in \mathbb{N}^*$ such that

$$p(X) = X^d + \frac{1}{n}\gamma(x), \quad \gamma(X) \in \mathbb{Z}[X].$$

Let us consider $\mu \in \mathbb{N}^*$, $\sigma = \mu\, d$ and $\nu = \sigma!\, n^\sigma$. Then there exists a monic polynomial $\Gamma(X) \in \mathbb{Z}[X]$ of degree $\nu\, d = \deg(p^\nu)$ such that $r(X) := p^\nu(X) - \Gamma(X)$ is a polynomial which can be written as follows:

$$r(X) = \sum_{l=0}^{\nu-\mu-1} p^l(X) q_l(X)$$

where the $(q_l)_{0\leq l\leq \nu-\mu-1}$ are polynomials of degree not greater than $d-1$, with coefficients in $\mathbb{Q} \cap [0,1[$.

Proof. Let us consider the following decomposition:

$$p^\nu(X) = E(X) + R(X)$$

where

$$E(X) = \sum_{i=0}^{\sigma} \binom{\nu}{i} \frac{1}{n^i} X^{(\nu-i)d} \gamma^i(X) \quad \text{(monic)}$$

$$R(X) = \sum_{i=\sigma+1}^{\nu} \binom{\nu}{i} \frac{1}{n^i} X^{(\nu-i)d} \gamma^i(X).$$

Let us study the coefficients of $E(X)$: for $0 \leq i \leq \sigma$, since $i!\, n^i$ divides $\sigma!\, n^\sigma = \nu$, then $\binom{\nu}{i}\frac{1}{n^i} \in \mathbb{Z}$. Therefore $E(X) \in \mathbb{Z}[X]$.

Let us now take a look at $R(X)$: for $i \geq \sigma+1$, we have $\deg(X^{(\nu-i)d}\gamma^i(X)) \leq (\nu-i)d + i(d-1) \leq \nu d - \sigma - 1 = (\nu-\mu)d - 1$, therefore $\deg(R) \leq (\nu-\mu)d - 1$.

Since $\{p^l(X)X^k \mid 0 \leq l \leq \nu-\mu-1, 0 \leq k \leq d-1\}$ forms a basis of $\mathbb{Q}_{d(\nu-\mu)-1}[X]$, $R(X)$ is a $\mathbb{Q}$-linear combination of this basis. Moreover, $p^l(X)X^k$ are monic polynomials which are, pairwise, of different degrees, therefore we can find by induction $c_{l,k} \in \mathbb{Q} \cap [0,1[$ in the order $k = d-1, \ldots, 0$ and $l = \nu-\mu-1, \ldots, 0$, such that

$$p^\nu(X) - \sum^{l,k} c_{l,k} p^l(X) X^k \in \mathbb{Z}[X].$$

Let us finally consider

$$q_l = \sum_{k=0}^{d-1} c_{l,k} X^k$$

$$r(X) = \sum_{l=0}^{\nu-\mu-1} p^l(X) q_l(X).$$

Then $\Gamma(X) := p^\nu(X) - r(X) \in \mathbb{Z}[X]$ is the monic polynomial we were looking for.

□

Lemma 3.2 Let L be a lemniscate of polynomial $p \in \mathbb{Q}[X]$ of degree $d \geq 1$ and constant $\rho > 1$, then there exists a lemniscate of polynomial $\Gamma \in \mathbb{Z}[X]$ and constant 1 included in L.

Proof. It is obvious that $\partial L = \{z \in \mathbb{C} \mid |p(z)| = \rho^d\}$.

Let us consider $M = \sup_{z \in \partial L}(1 + |z| + \cdots + |z|^{d-1})$, $\mu \in \mathbb{N}^*$ such that $\frac{M}{\rho^{\mu d}(\rho^d - 1)} \leq 1/2$ and $\frac{\rho^{\mu d}}{2} > 1$. Let Γ be the polynomial in the previous lemma, which corresponds to our choice of μ, and let us use the same notations as in the lemma.

For all $z \in \partial L$, we have

$$\frac{|p^\nu(z) - \Gamma(z)|}{|p^\nu(z)|} = \frac{|r(z)|}{\rho^{\nu d}} = \frac{\left|\sum_{l=0}^{\nu-\mu-1} p^l(z) q_l(z)\right|}{\rho^{\nu d}} \leqslant \frac{M}{\rho^{\nu d}} \sum_{l=0}^{\nu-\mu-1} \rho^{ld} \leqslant \frac{M(\rho^{(\nu-\mu)d} - 1)}{\rho^{\nu d}(\rho^d - 1)} \leq \frac{M}{\rho^{\mu d}(\rho^d - 1)} \leq \frac{1}{2}.$$

It follows from Rouché's theorem that $\Gamma^{-1}(0) \subset L$. On the other hand, this inequality implies that for all $z \in \partial L$

$$|\Gamma(z)| \geq |p^\nu(z)| - |r(z)| \geq \frac{1}{2}|p^\nu(z)| \geq \frac{\rho^{\mu d}}{2} > 1.$$

But $\frac{1}{\Gamma}$ is holomorphic on $\overline{C} \backslash L$ because $\Gamma^{-1}(\{0\}) \subset L$, therefore, according to the maximum modulus principle, $|\Gamma(z)| > 1$ for all $z \notin L$.

Therefore $L_{\Gamma,1} \subset L$. □

4
ROBINSON'S THEOREM

In this section, we shall state and prove the main theorem of this article: Robinson's theorem. Let us consider some segment K of $\mathbb{R}$. The second section of this piece (2.9) allows us to calculate its capacity. If it is strictly smaller than 1, Fekete's theorem 3.1 gives us that the number of algebraic integers totally in K is finite. On the contrary, when the capacity is greater than or equal to 1, Fekete-Szegö's theorem 3.3 gives us that there is an infinite number of algebraic integers arbitrarily close to K with respect to $\mathbb{C}$. However, when K is a segment of $\mathbb{R}$, this property is not enough to show that there is an infinite number of algebraic integers totally in K. Hence the potential theory is not enough to fully understand the case of compact subsets of $\mathbb{R}$. To prove Robinson's theorem, we will have to use algebraic curves.

In section 4.1, we will first define a few notions on algebraic curves: regular/rational functions on a curve, group of divisors... Then we will build a smooth completion of a hyperelliptic curve. Finally, section 4.2 is dedicated to the proof of Robinson's theorem. We will cleverly use hyperelliptic curves to prove a theorem which, at first sight, has nothing to do with them.

We shall also use charts, holomorphic and meromorphic forms on a Riemann surface. An introduction to this notions is provided in [9], in particular in sections I.1 and B.2.

4.1 A few notions on algebraic curves

An *algebraic curve* is an object of dimension 1 locally defined by an *algebraic* (*i.e.* polynomial) equation. Since all polynomials are analytic functions, the algebraic approach gives us less information than the analytic approach.

We assume that the field $\mathbb{K}$ is $\mathbb{C}$, but we shall use $\mathbb{K}$ or $\mathbb{C}$ according to the approach (algebraic or analytic). Several definitions or results where the field is referred as $\mathbb{K}$ can be generalized, but we will not focus on this here.

We will give a visual example at the end of section 4.1.7, which can be useful to understand the paragraphs that precede.

4.1.1 • Algebraic curve: affine case

Definition 4.1 Let $F \in \mathbb{K}[X,Y]$ be a non-constant polynomial in two variables which is *irreducible*, in other words which cannot be written as the product of two non-constant polynomials of $\mathbb{K}[X,Y]$. An *algebraic curve* C in the affine space $\mathbb{A}^2_{\mathbb{K}}$ (which is isomorphic to $\mathbb{K}^2$) is the set of all the points $(x,y) \in K^2$ verifying the equation $F(x,y) = 0$. It is represented as follows:

$$C : F(x,y) = 0.$$

• **Algebraic approach**:

The ring of regular functions on curve C is by definition the ring

$$A(C) := \mathbb{K}[X,Y]/(F).$$

In other words, it is the ring of polynomials *modulo an equivalence relation*, for which two polynomials are equivalent if and only if they are equal on the points of curve C. $A(C)$ is an *integral domain* since F is *irreducible*; its field of fractions is called *the field of rational functions* of the curve and is referred as $\mathscr{R}(C)$.

• **Analytic approach** (more intuitive):

It follows from the implicit function theorem that, if $\nabla F = (\partial_x F, \partial_y F) \neq \mathbf{0}$ at a point $(x_0, y_0) \in C(\mathbb{C})$, then in a neighborhood of (x_0, y_0), the curve is locally the graph of some holomorphic function $y = y(x)$ or $x = x(y)$. The curve has a good behavior in the neighborhood of such a point (x_0, y_0) : we say that (x_0, y_0) is a *smooth point*. More precisely, the curve has a 1-dimensional complex manifold structure in the neighborhood of (x_0, y_0). That is why it is called a curve (1-dimensional). On the contrary, some point of C with $\nabla F = \mathbf{0}$ is called a *singular point*. A curve without any singular point is called *smooth*. A smooth curve has the natural structure of a Riemann surface.

Let us consider (affine) hyperelliptic curves, whose definition is given in a restricted manner in order to fit our problem.

Definition 4.2 An *hyperelliptic curve* is an algebraic curve

$$C : y^2 = D(x)$$

where $D \in \mathbb{C}[X]$ is a *monic* polynomial in X of degree $2g+2$ ($g \geq 0$) whose roots are *distinct*. We write that C is a *real* hyperelliptic curve if $D \in \mathbb{R}[X]$.

With this definition, we check that a hyperelliptic curve is *smooth*.

4.1.2 • Divisors

Let us consider $F(X,Y) \in \mathbb{C}[X,Y]$ non constant and irreducible, as well as the complex algebraic curve associated with C. The *group of divisors* on C, referred as $\mathrm{div}(C)$, is the free abelian group generated by the basis $\{P\}_{P \in C}$. More precisely, a *divisor* D on C is a formal linear combination with integer coefficients of a finite number of points $P \in C$:

$$D = \sum_{i=1}^{n} n_i P_i, \quad \text{where } n \in \mathbb{N}, n_i \in \mathbb{Z}, P_i \in C.$$

Different points are considered linearly independent. The group of divisors $\mathrm{div}(C)$ refers to the set of divisors on C equipped with a structure of group with the addition of coefficients (point by point). We have a natural group homomorphism called *degree of a divisor* :

$$\deg : \ \mathrm{div}(C) \longrightarrow \mathbb{Z}, \quad \sum n_i P_i \longmapsto \sum n_i.$$

Assume curve C is *smooth*. According to the implicit function theorem, C has a 1-dimensional complex manifold structure. Let us consider $f \in \mathscr{R}(C)^\times$. f can be seen as a *meromorphic function* on C and therefore, $\mathrm{ord}_P(f)$ is well defined for all $P \in C$ as the order of the meromorphic function f at point P. Let us define the *principal divisor* associated with $f \in \mathscr{R}(C)$ as

$$\mathrm{div}(f) := \sum \mathrm{ord}_P(f) P.$$

We have $\mathrm{div}(f) \in \mathrm{div}(C)$ since there is a finite number of non-zero coefficients. We verify that we have just defined a group homomorphism

$$\mathrm{div} : \left(\mathscr{R}(C)^\times, \cdot\right) \longrightarrow \left(\mathrm{div}(C), +\right).$$

Let us define the *jacobian variety* $J(C)$ *of the (smooth) curve* C as the cokernel of the homomorphism above, i.e.

$$J(C) := \mathrm{div}(C) / \mathrm{div}\, \mathscr{R}(C)^\times.$$

We say that two divisors D_1 and D_2 are *linearly equivalent* if $D_1 - D_2$ is a principal divisor, in other words, if $D_1 = D_2$ in $J(C)$.

Notice that the smoothness assumption was necessary to define the notions above. That is why we will look for a *smooth* completion of the hyperelliptic curve in the following sections.

4.1.3 • A naive compactification

When we talk about the compactness of a curve, we talk about the subjacent set of the curve equipped with the induced topology of $\mathbb{C}^2$. A compact curve has interesting properties which motivates us to compactify curves. Moreover, we want the compactified curve to be *smooth* in order to have a Riemann surface structure.

The hyperelliptic curve $y^2 = D(x)$ is not compact : in fact, intuitively, there is (are) a point(s) at infinity which is (are) not on the affine curve. A first possible approach is to use the projective plane $\mathbb{P}^2_{\mathbb{K}}$, which compactifies the affine plane $\mathbb{A}^2_{\mathbb{K}} = \mathbb{K}^2$ by adding a projective line at infinity. The compactification induced on the curve is the closure of C in $\mathbb{P}^2_{\mathbb{K}}$. More precisely, the steps of this compactification are :

- Write the homogeneous form of the equation of the curve $z^{2g} y^2 = z^{2g+2} D(x/z)$;
- Define the compactification as the algebraic curve defined on $\mathbb{P}^2_{\mathbb{K}}$ by this equation.

We will not detail this approach. However, we state that this compactified curve *is not* smooth at point $\infty = [0 : 1 : 0] \in \mathbb{P}^2_{\mathbb{K}}$ when $g > 0$. Therefore we need another compactification.

4.1.4 • Interlude: adjunction of two affine algebraic curves

Before constructing a smooth completion, let us focus on the adjunction of two affine algebraic curves.

$$C_1 : F(x, y) = 0, \quad C_2 : G(u, v) = 0$$

on the affine spaces $\mathbb{K}^2_{x,y}$ and $\mathbb{K}^2_{u,v}$ respectively (with coordinates x, y or u, v).

Definition 4.3 Let $C : F(x, y) = 0$ be an affine algebraic curve. A *closed algebraic* subset of C is the set of the roots *in* C of a finite number of polynomials $H_i \in \mathbb{K}[X, Y]$ for $i \in I$ where I is a finite set. We call it $Z_C(H_i, i \in I)$, or simply $Z(H_i, i \in I)$, if there is no confusion.

Definition 4.4 Let C_1 (*resp.* C_2) be an algebraic curve on $\mathbb{K}^2_{x,y}$ (*resp.* $\mathbb{K}^2_{u,v}$). A function $\varphi : C_1 \to C_2$ is called a *rational homomorphism* if $\varphi = (u(x,y), v(x,y))$ where $u, v \in \mathscr{R}(C_1)$.

In other words, φ is rational if it can be written as $u(x,y) = H_{11}/H_{12}, v(x,y) = H_{21}/H_{22}$ where $H_{ij} \in \mathbb{K}[X,Y]$ and H_{12}, H_{22} are non zero on C_1. Let us notice that such a φ is «ẁell defined» (in terms of subjacent function) on $C_1 \backslash Z(H_{12}, H_{22})$.

Definition 4.5 An *Adjunction* between two Riemann surfaces C_1 and C_2 is given by:

(i) two closed algebraic subsets Σ_1 and Σ_2 respectively of C_1 and C_2;

(ii) a couple of rational homomorphisms

$$C_1 \underset{\psi}{\overset{\varphi}{\rightleftarrows}} C_2$$

inducing a well-defined isomorphism

$$\varphi : \ C_1 \backslash \Sigma_1 \overset{\sim}{\rightleftarrows} C_2 \backslash \Sigma_2 \ : \psi$$

With the notion of adjunction, one can obtain a new algebraic curve C' by considering the disjoint union $C_1 \dot{\cup} C_2$ and identifying the points of $C_1 \backslash \Sigma_1$ and $C_2 \backslash \Sigma_2$ using φ and ψ. When considering a point coming from C_i, we can look at its neighborhood in C' which can be identified to C_i with the corresponding homomorphism. However, the new curve is not necessarily an affine curve.

Notions of field of rational functions, smoothness, divisors, principal divisors, *etc.* can be generalized to the case of curves obtained by the adjunction of two affine curves, by considering the definitions on affine curves C_1 and C_2. For example, f is a rational function on C' if $f|_{C_1}$ and $f|_{C_2}$ are both rational functions, on C_1 and C_2 respectively. We will not get into more details here.

4.1.5 • Smooth completion

Let $D \in \mathbb{K}[x]$ be a monic polynomial of degree $2g+2$ whose roots are all distinct. We have an affine hyperelliptic curve

$$C : y^2 = D(x).$$

Its compactification, referred as $\widetilde{C}$ for now, can be obtained by adding two points at infinity ∞_+ and ∞_-. It is the curve that we will study in the following sections.

This compactification can be built as follows : $\widetilde{C} = U_0 \cup U_\infty$, where

$$U_0 : y^2 = D(x), \quad U_\infty : v^2 = u^{2g+2} D(1/u),$$

the adjunction of this two affine curves being given by

$$\begin{aligned} U_0 \quad &\rightleftarrows \quad U_\infty \\ U_0 \backslash \{x=0\} \ &\overset{\sim}{\rightleftarrows} \ U_\infty \backslash \{u=0\} \\ (x,y) \ &\longmapsto \ (1/x, y/x^{g+1}) \\ (1/u, v/u^{g+1}) \ &\longmapsto \ (u,v). \end{aligned} \tag{2}$$

The points $\infty\pm$ correspond to $(0, \pm 1)$ on U_∞, *i.e.* on the curve $v^2 = u^{2g+2} D(1/u)$. By restricting our study to U_0 or U_∞, we check immediately that the obtained curve $\widetilde{C}$ is smooth ; it is equipped with a natural complex manifold structure. Moreover, we have

Proposition 4.1 $\widetilde{C}$ is a compact Riemann surface of genus equals to g. □

Once we have the compactification $\widetilde{C}$, we will refer to it as C with no risk of confusion.

Proposition 4.2 On a (smooth) compactified hyperelliptic curve, the degree of all the principal divisors is zero. In other words, we have $(\deg \circ \operatorname{div})\mathscr{R}(C)^\times = 0$.

Proof. It follows from the residue theorem on a compact Riemann surface ([9], Prop. B.2.2) that the sum of residues of some meromorphic form is zero. Let f be a rational function, by applying the previous result to the form $\mathrm{d}f/f$, the argument principle gives us that f has as many zeros as it has poles, counted with multiplicity. □

The compactified curve is equipped with an involution ι induced by the function $(x, y) \mapsto (x, -y)$ on the affine space, which swaps ∞_+ and ∞_-. We call ι the *conjugation* of this hyperelliptic curve. This conjugation induces an involution on the group of divisors on the curve: $\sum n_i P_i \mapsto \sum n_i \iota(P_i)$.

Example 4.1 (Calculation of a principal divisor on C). Let us denote by $\alpha_1, \ldots, \alpha_{2g+2}$ the roots of $D(x)$ (which are assumed to be distinct) and by $P_i \in C$ their corresponding points, then

$$\operatorname{div}(1/y^2) = -2 \sum_{i=1}^{2g+2} P_i + (2g+2)\,(\infty_+ + \infty_-)\,. \tag{3}$$

Its degree is zero, as expected.

Proof. Let us first define the function $1/y^2$: It is defined as $1/y^2$ on U_0 and u^{2g+2}/v^2 on U_∞; We check that they coincide on $U_0 \cap U_\infty$ by using the substitution (2), therefore this rational function is well defined.

Then to simplify, let us consider the case where $g = 1, D(x) = x(x^3 - 1)$ and calculate the multiplicity from a "complex analysis" point of view (i.e with charts, etc.). The equation of the curve on U_∞ becomes $v^2 = 1 - u^3$.

Let us calculate its multiplicity at point $\infty\pm$. Let us consider U_∞. Then $\infty_+ = (0, 1)$, and in a neighborhood of ∞_+, we can use the chart (V_1 being some neighborhood of 0)

$$\varphi_1 : \mathbb{C} \supset V_1 \longrightarrow C, \quad z \longmapsto (u, v) = (z, \sqrt{1 - z^3}).$$

For this chart, $\varphi_1(0) = \infty_+$ and

$$1/y^2 = u^4/v^2 = z^4/(1 - z^3),$$

therefore

$$\operatorname{ord}_{\infty_+}(1/y^2) = 4 = 2g + 2.$$

Likewise we have

$$\operatorname{ord}_{\infty_-}(1/y^2) = 4 = 2g + 2.$$

Let us calculate the multiplicity of $1/y^2$ at point $P_1 = (x, y) = (0, 0) \in U_0$, for example. Previously u was a local (holomorphic) parameter of C near $\infty_\pm$. *Now, the variable y will be used as a local parameter of C near P_1.* Therefore

$$\operatorname{ord}_{P_1}(1/y^2) = -2.$$

More precisely, since $D(x) = x(x^3 - 1)$ has a simple root at $x = 0$, the holomorphic function $\psi : x \mapsto w = x(x^3 - 1)$ is locally biholomorphic at points $x = 0$ and $w = 0$, in other words, on sufficiently small

neighborhoods of $x = 0$ and $w = 0$, ψ has a holomorphic inverse function which we will call $\psi^{-1}(w)$. Therefore, by considering the following chart (V_2 being some neighborhood of 0):

$$\varphi_2 : \mathbb{C} \supset V_2 \longrightarrow C, \quad z \longmapsto (x, y) = (\psi^{-1}(z^2), z),$$

we have

$$1/y^2 = 1/z^2,$$

therefore

$$\mathrm{ord}_{P_1}(1/y^2) = -2.$$

The same goes for all the $P_i = (\alpha_i, 0) \in U_0$ where α_i is a root of $D(x)$. Note that $1/y^2$ has no other pole nor root, hence the formula (3). □

Example 4.2 Let $A \in \mathbb{R}[x]$ be a monic polynomial and $\eta_A = \frac{A(x)\ \mathrm{d}x}{y}$ the differential form associated with A. If $\deg A = g$, then η_A has simple poles at points ∞_+ and ∞_-,with residues -1 and $+1$ respectively; if $\deg A < g$, then η_A is a holomorphic form.

Proof. It is enough to make the calculations using the two charts, like in the previous example. □

4.1.6 • Hyperelliptic curves and Pell-Abel equation

Let us prove an important result : A link between the existence of solutions to Pell-Abel equation and hyperelliptic curves.

Definition 4.6 Let $D \in \mathbb{K}[X]$ be a monic polynomial of degree $2g + 2$ with distinct roots. We call *Pell-Abel equation* the equation with unknowns $(P, Q) \in \mathbb{K}[x]^2$ of the form :

$$P^2 - DQ^2 = c, \text{ with } c \in \mathbb{K}^*.$$

The degree of a solution (P, Q) is, by definition, the degree of P.

Theorem 4.1 The following claims are equivalent:

1. The Pell-Abel equation has a solution of degree r in $\mathbb{K}[x]$.
2. The divisor $r((\infty_-) - (\infty_+))$ on the curve C (cf. section 4.1.5) is linearly equivalent to 0.

Proof. Let C be the curve defined by $y^2 = D(x)$. The ring of regular functions on C is a $\mathbb{K}[x]$-module with basis $\{1, y\}$, with $y^2 = D(x)$.

Assume there exists $P, Q \in \mathbb{K}[x]$, $c \in \mathbb{K}^*$ such that $P^2 - DQ^2 = c$. Let us consider $\varphi_+ = P + yQ$, $\varphi_- = P - yQ$. Since φ_+ and φ_- are regular functions on the affine hyperelliptic curve, their poles are in the set $\{\infty_+, \infty_-\}$. However $\varphi_+\varphi_- = P^2 - DQ^2 = c$, therefore their zeros are also in the set $\{\infty_+, \infty_-\}$. Therefore $\mathrm{div}(\varphi_+) = a(\infty_-) + b(\infty_+)$. However $\deg(\mathrm{div}(\varphi_+)) = 0$, therefore $b = -a$ and the degree of P gives us that $a = r$. Therefore $r\left((\infty_-) - (\infty_+)\right)$ is principal (therefore linearly equivalent to 0).

Conversely, assume that $r((\infty_-) - (\infty_+))$ is linearly equivalent to 0. Let ψ be a rational function such that $\mathrm{div}(\psi) = r((\infty_-) - (\infty_+))$. Since ψ has no pole on the affine space, ψ is regular. Therefore ψ can be

written as $\psi = P + yQ$ with $P, Q \in \mathbb{K}[x]$, and $\deg P = r$. Its conjugate is $\overline{\psi} = P - yQ$. However conjugation is involutory and swaps ∞_+ and ∞_-, therefore $\mathrm{div}(\overline{\psi}) = (-r)((\infty_-) - (\infty_+))$, hence $\mathrm{div}(\psi\overline{\psi}) = 0$. Therefore $P^2 - DQ^2 = \psi\overline{\psi}$ is a non-zero constant of $\mathbb{K}$. □

4.1.7 • A visual example

Let us introduce the hyperelliptic curve that we will use in the proof of Robinson's theorem. Let

$$a_0 < b_0 < a_1 < \cdots < a_g < b_g$$

be distinct real numbers. Let us consider $E_j = [a_j, b_j]$, $E = \bigcup_{j=0}^{g} E_j$ and the polynomial

$$D = \prod_{j=0}^{g} (X - a_j)(X - b_j)$$

and let us call C the compactified hyperelliptic curve associated with D (cf. section 4.1.5).

Let us provide an illustration of this curve in the case where $g = 2$.

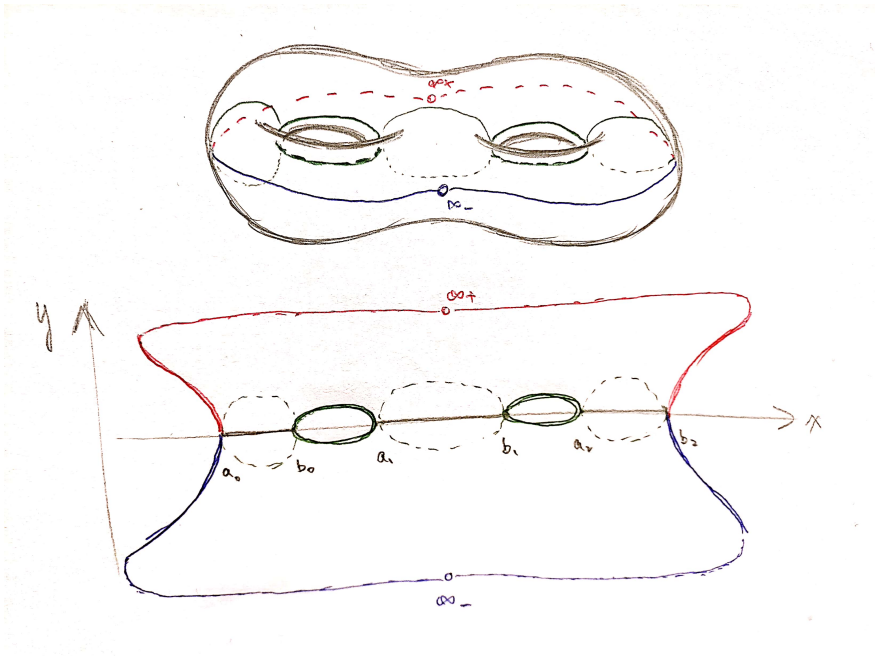


Figure 8: Case $g = 2$: C as a Riemann surface (above) or a curve on the affine plane (bellow)

.

Figure 8 shows the connection between these two representations of curve C. The figure below, on the affine plane (solid lines represent real points) can be obtained by intersecting the surface above with a horizontal plane (and by removing points " at infinity " $\infty\pm$). We clearly see the position of $\infty\pm$, the two points at infinity added to the affine hyperelliptic curve. We also understand the singularity of the naive compactification (cf. section 4.1.3) : it can be found again by attaching the two points $\infty\pm$ in the figure above !

Let us denote by α_j the cycle on the curve which covers the interval $[b_{j-1}, a_j]$. Then there exists a cycle β_j crossing the j-th «hole» of the surface, which only intersects cycle α_j and with multiplicity 1. We say that $\{\alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g\}$ forms a *symplectic basis of the singular homology* $H_1(C, \mathbb{Z})$. This basis is illustrated, when $g = 2$, in Figure 9.

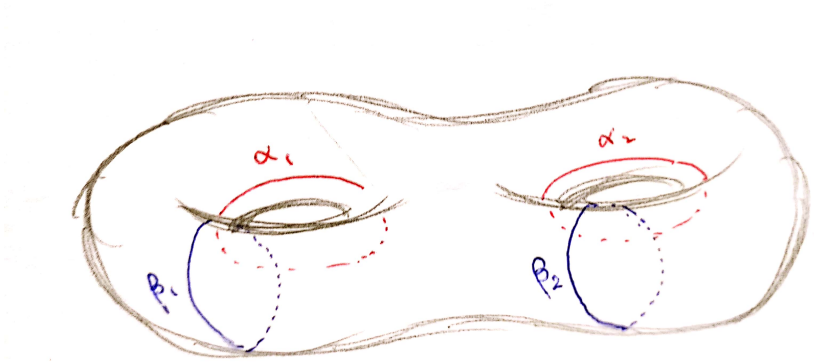


Figure 9: Case $g = 2$: a symplectic basis of $H_1(C; \mathbb{Z})$

.

The genus g, which intuitively corresponds to the number of holes in the surface, also corresponds to the dimension of the space of holomorphic forms.

Proposition 4.3 The complex dimension of the space of holomorphic 1-forms on some Riemann surface of genus g is equal to g.

The integral of a holomorphic form along a cycle provides a *perfect coupling*, as explained below :

Theorem 4.2 Let $\{\alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g\}$ be a symplectic basis of $H_1(C, \mathbb{Z})$. Let $\{\omega_1, \ldots, \omega_g\}$ be a basis of the space of holomorphic 1-forms on C. Then the g-by-g square matrix with coefficients $A_{i,j}$ defined as follows, is invertible:

$$A_{ij} = \int_{\alpha_j} \omega_i.$$

The proof of this theorem is provided in [9], Theorem III.1.2.

4.2 Proof of Robinson's theorem

The goal of the following section is to prove what follows :

Theorem 4.3 (Robinson). Let E be a finite union of intervals of $\mathbb{R}$ such that $\mathrm{Cap}(E) > 1$, then there exists an infinite number of algebraic integers totally in E.

Remark 4.1 It is enough to prove the theorem for a union of disjoint segments, since the union of two non-disjoint segments forms a segment, and the capacity of an open interval is defined as the supremum of the capacities of segments included in the interval.

Let us consider $a_0 < b_0 < a_1 < \cdots < a_n < b_n$, $E_j = [a_j, b_j]$ and $E = \bigcup_{j=0}^{g} E_j$.

Let us consider $D = \prod_{j=0}^{g}(X - a_j)(X - b_j)$. The proof of Robinson's theorem is based on the geometry of the hyperelliptic curve $y^2 = D(x)$. We prove it first for the *Pell-Abel case*, then we generalize the result using density.

4.2.1 • Pell-Abel case

Assume the Pell-Abel equation with respect to polynomial D has a solution, *i.e.* there exists $P, Q \in \mathbb{R}[X]$ such that

$$P^2 - DQ^2 = c$$

where c is a non-zero real number. Let us consider $r := \deg(P)$.

Note first that $c > 0$, in fact $c = P(a_0)^2$ since a_0 is a root of D. Let us then consider $M = \sqrt{c}$ and write Pell-Abel equation as follows :

$$P^2 - DQ^2 = M^2.$$

Let us notice immediate properties of polynomials P and Q:

Proposition 4.4 Let us consider $x \in \mathbb{R}$,

1. $|P(x)| \leqslant M \Leftrightarrow x \in E$ or $Q(x) = 0$.
2. $|P(x)| = M \Leftrightarrow x$ is a root of Q or one of the a_i, b_j.

Proof. These two properties directly follow from the Pell-Abel equation, by noticing that $D(x) \leqslant 0 \Leftrightarrow x \in E$. Indeed, D tends to $+\infty$ when x tends to ∞, and changes sign at points a_i, b_j. □

The key to the proof of Robinson's theorem is based on the following property of the roots of polynomials P and Q, illustrated in figure 10.

Proposition 4.5 Let us denote by r_j the number of roots of P in E_j.

1. The roots of P and Q are simple, interlaced, and all belong to $\overset{\circ}{E} = \bigcup_{j=0}^{g}]a_j, b_j[$.
2. The roots of Q in E_j divide E_j into r_j sub-intervals; in each of them, the polynomial P is either strictly increasing, or strictly decreasing, with extreme values M and $-M$.

These properties are illustrated in figure 10 (case $g = 1$, $r_1 = 4$, $r_2 = 6$). The p_i are the roots of P and q_i are the roots of Q.

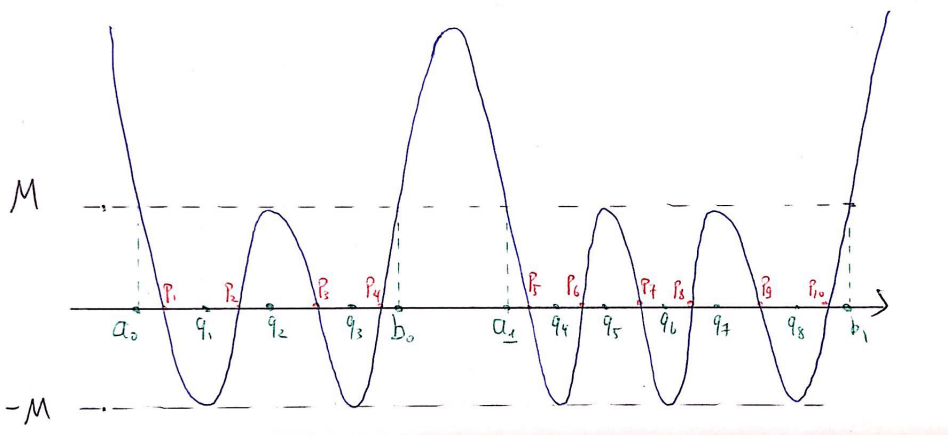


Figure 10: Shape of P, case $g = 1$, $r_1 = 4$, $r_2 = 6$

This proposition is the very key to the proof of Robinson's theorem. Because of its importance, it is very enlightening to prove it in the case $g = 0$ (in other words, $E = [a, b]$ is a single segment). It allows to show the major steps of the proof, by dissociating the difficulties.

4.2.2 • Proof of proposition 4.5 in the case $g = 0$

We focus here on the case where $E = [a, b]$ is a segment of $\mathbb{R}$, therefore $g = 0$ and $D(X) = (X - a)(X - b)$. Let us consider $f = P + yQ$, regular function on the curve $y^2 = D(x)$ completed as in the beginning of the chapter (the curve is not hyperelliptic anymore but only quadratic). Let us start with the calculation of $\mathrm{d}f/f$:

Proposition 4.6 We have $\mathrm{d}f/f = r\ \mathrm{d}x/y$, where $r = \deg P$.

Proof. We know that $\mathrm{div}(f) = r((\infty_-) - (\infty_+))$ (*cf.* the proof of theorem 4.1), therefore, ∞_- is a zero of f with multiplicity r and ∞_+ is a pole with the same multiplicity. Hence, $\mathrm{d}f/f$ has two simple poles at points (∞_+), (∞_-) with residues $-r$ and r. Let us calculate the poles of the form $\mathrm{d}x/y$ and their multiplicity. The only potential poles of $\mathrm{d}x/y$ are either (∞_+), (∞_-), or the roots of polynomial D.

- If α is a root of D in the affine space, since the roots of D are simple, we can write $D(X) = (X-\alpha)H(X)$, with $H(\alpha) \neq 0$. By differentiating $y^2 = (X-\alpha)H(X)$, we obtain in a neighborhood of α : $\mathrm{d}x \sim \frac{2y}{H(\alpha)}\ \mathrm{d}y$.

  Therefore $\mathrm{d}x/y = \frac{2}{H(\alpha)}\ \mathrm{d}y$ has no pole at point α.

- At points $\infty\pm$, with coordinates $(u = \frac{1}{x}, v = \frac{y}{x})$, $\infty_+ = (0,1)$, and the equation of the curve is $v^2 = u^2 D(\frac{1}{u})$. Therefore $\frac{\mathrm{d}x}{y} = -\frac{u}{v}\frac{\mathrm{d}u}{u^2} = -\frac{\mathrm{d}u}{\pm\sqrt{u^2 D(\frac{1}{u})}u} \sim \mp\frac{\mathrm{d}u}{u}$ since the constant coefficient of $u^2 D(\frac{1}{u})$ is 1. Hence ∞_+ is a simple pole of $\mathrm{d}x/y$, and the same goes for ∞_-.

Therefore $\frac{\mathrm{d}f/f}{\mathrm{d}x/y}$ has no zero nor pole neither on the affine space, nor at infinity : It is a constant function. But according to the previous calculation, the residues of $\mathrm{d}x/y$ at $\infty\pm$ are ∓ 1, hence the constant is equal to r. □

Let us now prove proposition 4.5 in the case where E is a segment, illustrated in figure 11 :

Proposition 4.7
1. The roots of P and Q are simple, interlaced, and all belong to $\mathring{E}$.
2. The roots of Q divide E into r sub-intervals; in each of them, the polynomial P is either strictly increasing, or strictly decreasing, with extreme values M and $-M$.

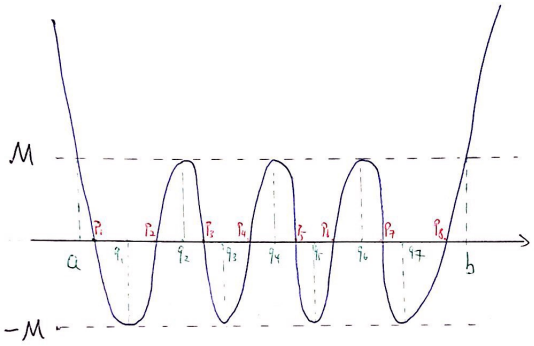


Figure 11: Shape of P, in the case $g = 0$, $r = 8$

Proof. A representative of $f = P + yQ$ in E is $f(x) = P(x) + iy_1(x)Q(x)$, with $y_1(x) = \sqrt{-D(x)}$ since $D(x) \leqslant 0$ for all $x \in E$. The Pell-Abel equation implies that $|f(x)|^2 = P(x)^2 - D(x)Q(x)^2 = M^2$, therefore f has a constant magnitude which is equal to M on E.

We can then write that $f(x) = Me^{i\theta(x)}$, with $\theta : E \to \mathbb{R}$ of class C^1. Hence, we have $P(x) = M\cos(\theta(x))$, $y_1(x)Q(x) = M\sin(\theta(x))$. And since $f(a) = \pm M$, $f(b) = \pm M$, we have $\theta(a) = c_0\pi$, $\theta(a) = c_1\pi$, where $c_0, c_1 \in \mathbb{Z}$. Moreover, we have that $\int_a^b \frac{\mathrm{d}f}{f} = i\int_a^b \mathrm{d}\theta = i(c_1 - c_0)\pi$. However $\frac{\mathrm{d}f}{f} = r\frac{\mathrm{d}x}{y}$, and $\int_a^b \frac{\mathrm{d}x}{y} = \pm i\pi$ (the residue of $\frac{\mathrm{d}x}{y}$ at infinity is ± 1 and the curve $y^2 = D(x)$ is a covering map of degree 2 of $E = [a,b]$. The sign $\pm$ depends on the orientation.) We deduce from it that $|c_1 - c_0| = r$.

However, according to proposition 4.6, f' is never zero on E, therefore θ' is never zero on E. Hence, θ is strictly monotonic on E, taking values in the range $c_0\pi$ to $c_1\pi$, therefore $\cos(\theta(x))$ is equal to zero $|c_1 - c_0| = r$ times, and $\sin(\theta(x))$ is equal to zero $|c_1 - c_0| - 1 = r - 1$ times (end points not included). Since $\deg P = r$, $\deg Q = r - 1$, we found all the roots of P and Q. The other claims of the proposition directly follow from the sinusoidal shapes of P and Q. □

The case where E is a single segment already allows us to use the main steps of the proof in the general case while omitting a major difficulty : when E is the union of segments E_j, we do not know *a priori* how many

roots of P are in each E_j, and how we can state that we have found all the roots. To solve this problem in the general case, we will use the *periods* of a differential form on the hyperelliptic curve of genus $g > 0$.

4.2.3 • Proof of proposition 4.5 when $g > 0$

Let us consider the general case: $E = \bigcup_{i=0}^{g} [a_i, b_i]$.

As previously stated, the difficulty is to determine how many roots are in $E_j = [a_j, b_j]$ and to check that we have indeed found all the roots of P. To do so, we shall use the periods of a particular differential form on the curve $y^2 = D(x)$, called *canonical form*.

Theorem 4.4 There exists a unique polynomial $R \in \mathbb{R}[X]$ of degree g such that, for $j = 1, \dots, g$,

$$\int_{b_{j-1}}^{a_j} \frac{R(x)}{\sqrt{D(x)}}\,\mathrm{d}x = 0.$$

The differential form $\eta = \frac{R(x)\,\mathrm{d}x}{y}$ is said to be of *the third kind*.

Proof. Let us consider the curve $y^2 = D(x)$ as a Riemann surface thanks to the covering map $(x, y) \mapsto x$. The dimension of the space of holomorphic forms is g. A residue calculation with coordinates $(u = \frac{1}{x}, v = \frac{y}{x^{g+1}})$ gives us that for $i = 0, \dots, g-1$, the $x^i\,\mathrm{d}x/y$ are holomorphic forms, therefore form a basis of holomorphic forms.

Let us denote by α_j the cycle on the curve which covers (quadratically) the interval $[b_{j-1}, a_j]$. A monic polynomial of degree g, $R(X) = X^g + \sum_{j=0}^{g-1} c_j X^j$ verifies the wanted condition if and only if its coefficients $c_0, \dots c_{g-1}$ verify the following system of g equations with g unknowns:

$$\sum_{i=0}^{g-1} c_i \int_{\alpha_j} \frac{x^i\,\mathrm{d}x}{y} = -\int_{\alpha_j} \frac{x^g\,\mathrm{d}x}{y}, \qquad j = 1, \dots g.$$

It follows from theorem 4.2 that the determinant associated with this system is non-zero and therefore the system has a unique solution. □

Remark 4.2 By a calculation with coordinates $(u = 1/x, v = y/x^{g+1})$, we can show that η is a meromorphic form which has two simple poles at ∞_+ and ∞_-, with residues -1 and 1 respectively.

Remark 4.3 The relations $\int_{b_{j-1}}^{a_j} \frac{R(x)}{\sqrt{D(x)}}\,\mathrm{d}x = 0$ require that R has at least one zero in each $[b_{j-1}, a_j]$, for $j = 1, \dots, g$. Since R is of degree g, these are all its roots. In particular, R has a constant sign on $E_j = [a_j, b_j]$.

Let us focus on the periods of η on the cycles that cover segments $[a_j, b_j]$ (it is a quadratic covering space, ramified in points a_j, b_j). These periods are equal to $2\eta_j$, with $\eta_j = \int_{a_j}^{b_j} \frac{R(x)}{i\sqrt{-D(x)}}\,\mathrm{d}x$.

Proposition 4.8 Let us note $\eta_j = \displaystyle\int_{a_j}^{b_j} \frac{R(x)}{i\sqrt{-D(x)}}\,\mathrm{d}x$, for $j = 0, \dots g$.
There exists $(\epsilon_j)_{0\leq j\leq g} \in \{-1, 1\}^{g+1}$ such that

$$\sum_{j=0}^{g} \epsilon_j \eta_j = i\pi.$$

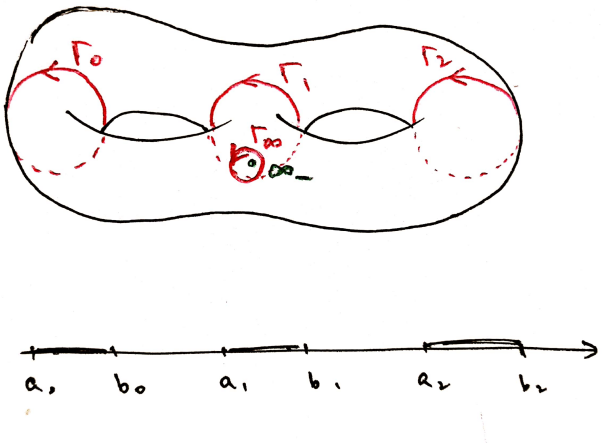


Figure 12: Case where $g = 2$: $\bigcup_{j=0}^{g} \Gamma_j$ is the boundary of the medial hemi-surface.

Proof. Let us denote by Γ_j the cycles which cover the segments $[a_j, b_j]$ (cf. Figure 12), the periods of η on these cycles are equal to $\pm 2\eta_j$. Let us denote by Γ_∞ a cycle around the point ∞_- (cf. Figure 12).

The form η is holomorphic on the domain framed by $\bigcup \Gamma_j$ and Γ_∞. Therefore, Cauchy's theorem on a Riemann surface gives us that

$$\sum_{j=0}^{g} \int_{\Gamma_j} \eta = \int_{\Gamma_\infty} \eta = 2i\pi$$

since the residue of η at ∞_- is equals to 1. Hence $\displaystyle\sum_{j=0}^{g} \epsilon_j \eta_j = i\pi$, the signs depend on the orientation of the cycles. □

Like in the case $g = 0$, the calculation of $\mathrm{d}f/f$ will be useful later :

Proposition 4.9 We have $\mathrm{d}f/f = r\eta$, where $r = \deg P$ and η is the differential form of the third kind previously defined.

Proof. We know that the forms $\mathrm{d}f/f$ and $r\eta$ have ∞_+ and ∞_- as their only poles. These poles are simple, with residues $-r$ and r respectively. Therefore, $\mathrm{d}f/f - r\eta$ is a holomorphic form which can be written as a linear combination of $x^j\,\mathrm{d}x/y$ for $j = 0, \dots g-1$. We know that the periods of η on the $[b_{j-1}, a_j]$ are zero. To show that this linear combination is zero, thanks to theorem 4.2, it is enough to show that the periods of

$\mathrm{d}f/f$ on $[b_{j-1}, a_j]$ are also zero.

Let us consider $j \in \{0, \dots, g\}$. A representative of y on the $[b_{j-1}, a_j]$ is $y = \sqrt{D(x)}$, since $D(x)$ is non-negative. Then $f(x) = P(x) + \sqrt{D(x)}Q(x)$ can be seen as a real function on $[b_{j-1}, a_j]$. We have $|f(b_{j-1})| = |P(b_{j-1})| = M$, $|f(a_j)| = |P(a_j)| = M$. Since $(P + \sqrt{D}Q)(P - \sqrt{D}Q) = M^2$, the function f is never zero, hence has a constant sign $\varepsilon \in \{-1, 1\}$ on $[b_{j-1}, a_j]$. Therefore $f(b_{j-1}) = f(a_j) = \varepsilon M$. Thus,

$$\int_{b_{j-1}}^{a_j} \frac{\mathrm{d}f}{f} = \int_{b_{j-1}}^{a_j} \mathrm{d}(\log(\varepsilon f)) = \log(\varepsilon f(a_j)) - \log(\varepsilon f(b_{j-1})) = 0,$$

hence the final result. □

Let us finally prove proposition 4.5 in the general case. More precisely we have :

Proposition 4.10 Let us consider $\eta_j = \displaystyle\int_{a_j}^{b_j} \frac{R(x)}{i\sqrt{-D(x)}}\,\mathrm{d}x$ and $r_j = r\,|\eta_j|\,/\pi$ for $j = 0, \dots, g$.

1. The number of roots of P in $E_j = [a_j, b_j]$ is r_j.
2. The roots of P and Q are simple, interlaced, and all belong to $\mathring{E}$.
3. The roots of Q in E_j divide E_j into r_j sub-intervals; in each of them, the polynomial P is either strictly increasing, or strictly decreasing, with extreme values M and $-M$.

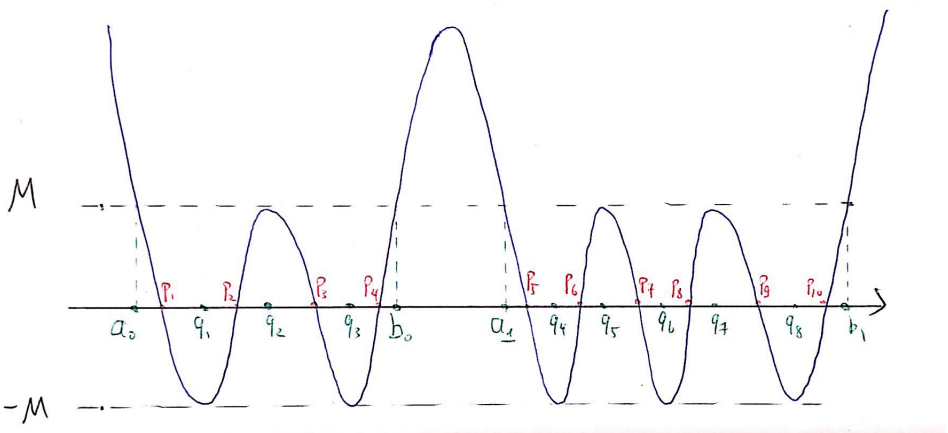


Figure 13: Shape of P in the case $g = 1$, $r_0 = 4$, $r_1 = 6$

Proof. The beginning of the proof is identical to the case where $g = 0$. Let us consider $j \in \{0, \dots, g\}$ and the segment $E_j = [a_j, b_j]$. A representative of f on E_j is $f(x) = P(x) + i\sqrt{-D(x)}Q(x)$. We have $|f| = M$ constant, therefore $f(x) = Me^{i\theta(x)}$, with $\theta : E_j \to \mathbb{R}$ continuous, and $\theta(a_j) = c_0\pi, \theta(b_j) = c_1\pi$, with $c_0, c_1 \in \mathbb{Z}$ since $f(a_j), f(b_j)$ are equal to $\pm M$. We therefore have

$$P(x) = M\cos(\theta(x)), \quad \sqrt{-D(x)}Q(x) = M\sin(\theta(x)).$$

Since $\mathrm{d}f/f = r\eta = rR(x)\,\mathrm{d}x/y$ and R is never zero on E_j according to 4.3, f' is never zero on E_j. Therefore θ is strictly monotonic on E_j, and the number of roots of P in E_j is equal to $|c_1 - c_0|$, the number

of roots of Q in E_j is equal to $|c_1 - c_0| - 1$ (since D is only zero at end points).

Let us calculate $|c_1 - c_0|$. We notice that :

$$(c_1 - c_0)i\pi = i(\theta(b_j) - \theta(a_j)) = i\int_{a_j}^{b_j} \mathrm{d}\theta = \int_{a_j}^{b_j} \mathrm{d}f/f = r\eta_j.$$

As a result, $|c_1 - c_0| = r\,|\eta_j|\,/\pi = r_j$. Therefore the number of roots of P in E_j is equal to r_j. Since P is of degree r, we first have that

$$\sum_{j=0}^{g} r_j \leqslant r.$$

But proposition 4.8 shows that there exists some $(\epsilon_j)_{0\leq j\leq g} \in \{-1, 1\}^{g+1}$ such that

$$\sum_{j=0}^{g} \pm r_j = r.$$

It follows that $\sum_{j=0}^{g} r_j = r$. Hence, the only roots of P are in the E_j. The sinusoidal shapes of P and Q give us the claims 2 and 3 of the proposition, since θ is strictly monotonic. □

4.2.4 • End of the proof of Robinson's theorem

Proposition 4.5, which precisely describes the behavior of polynomials P and Q, is the key to the proof of Robinson's theorem. Let us start with some immediate consequences of this result.

Let us remind ourselves of the notations : $E = \bigcup_{j=0}^{g} E_j$, $E_j = [a_j, b_j]$, $D(X) = \prod_{j=0}^{g}(X - a_j)(X - b_j)$, $P^2 - DQ^2 = M^2$, $\deg P = r$.

Proposition 4.11 $\mathrm{Cap}(E) = (\frac{M}{2})^{1/r}$.

Proof. It is a consequence of corollary 2.11. Indeed, propositions 4.4 and 4.5 show that $P^{-1}([-M, M]) = E$. But $\mathrm{Cap}([-M, M]) = \frac{M}{2}$ and P is a monic polynomial of degree r. Corollary 2.11 gives us that $\mathrm{Cap}(E) = P^{-1}([-M, M]) = (\frac{M}{2})^{1/r}$. □

Proposition 4.12 P is the Chebyshev polynomial of degree r with respect to E.

Proof. Proposition 4.5 shows that P, a monic polynomial of degree r, reaches its extreme values, $\pm M$, $r + 1$ times on E, hence the result using the equioscillation theorem 2.9. □

Let us state a last very simple lemma which plays a major part in the proof : a small perturbation does not change the number of roots of P in E.

Lemma 4.1 Let us consider $q \in \mathbb{R}[X]$ such that $|q(x)| < M$ for all $x \in E$. Then $P - q$ has at least r roots in E.

Proof. Let us denote by $q_1 < \cdots < q_{r-1}$ the roots of Q with the notations $q_0 = a$ and $q_r = b$. $P(q_i) = \pm M$ and since $|q(q_i)| < M$, $P(q_i) - q(q_i)$ has the same sign as $P(q_i)$. Therefore $P - q$ changes sign on each interval $[q_i, q_i + 1]$, for i in range 0 to $r - 1$, hence the result. □

We now have all the elements to finish the proof of Robinson's theorem. Let us transform the real coefficients into rational ones.

Proposition 4.13 We can replace M, P, Q, D, E by $\tilde{M}, \tilde{P}, \tilde{Q}, \tilde{D}, \tilde{E}$, so that proposition 4.5 is still verified, but with $\tilde{M} \in \mathbb{Q}$, $\tilde{P} \in \mathbb{Q}[X]$ (still of degree r), $\tilde{D} \in \mathbb{Q}[X]$, $\tilde{Q} = 1$, $\tilde{E} \subset E$ and $\mathrm{Cap}(\tilde{E})$ arbitrarily close to $\mathrm{Cap}(E)$.

Proof. Let us consider $\tilde{M} \in [0, M] \cap \mathbb{Q}$. According to lemma 4.1 applied to $q = \pm M$, $P^2 - \tilde{M}^2$ has $2r$ roots in E : $u_1 < \cdots < u_{2r}$ with $[u_i, u_{i+1}] \subset [q_i, q_{i+1}]$, where q_i are the roots of Q. By continuity of the roots, we can choose $\tilde{P}$ with rational coefficients sufficiently close to P, so that the roots of $\tilde{P}^2 - \tilde{M}^2$ are still ordered the same way $\tilde{u}_1 < \cdots < \tilde{u}_{2r}$. We then consider $\tilde{D} = \tilde{P}^2 - \tilde{M}^2$, $\tilde{E} = \bigcup [\tilde{u}_i, \tilde{u}_{i+1}] \subset E$. Since $\mathrm{Cap}(\tilde{E}) = (\frac{\tilde{M}}{2})^{\frac{1}{r}}$, we can choose $\tilde{M}$, a rational number sufficiently close to M, so that $\mathrm{Cap}(\tilde{E})$ is arbitrarily close to $\mathrm{Cap}(E)$. □

From now on, assume that P, Q, D, M have rational coefficients. Let us now prove Robinson's theorem, in the Pell-Abel case.

Theorem 4.5 (Robinson). If $\mathrm{Cap}(E) > 1$, then there exists an infinite number of algebraic integers totally in E. More precisely, there exists a sequence of monic polynomials with integer coefficients whose degrees tend to infinity and whose roots are all in E.

Proof. Since $\mathrm{Cap}(E) = (\frac{M}{2})^{1/r}$, $\mathrm{Cap}(E) > 1$ is equivalent to $M > 2$. Let us consider $\lambda = \frac{M}{2}$. We have $\lambda > 1$.

We already have a polynomial with rational coefficients whose roots are all in E : P. To find more of them, the idea is to raise the polynomial to higher powers. But instead of using P, like in the proof of Fekete-Szegö's theorem 3.3, we will implement this method using $f = P + yQ$.

We saw that $f(x) = P(x) + iy_1(x)Q(x) = 2\lambda e^{i\theta(x)}$. Therefore $f(x)^n = (2\lambda)^n e^{in\theta(x)} = 2^{n-1}(P_n(x) + iy_1(x)Q_n(x))$, with $P_n, Q_n \in \mathbb{Q}[X]$ monic polynomials. We can also rewrite P_n as follows

$$P_n(x) = 2\lambda^n \cos(n\theta(x))$$

Let T_n be the Chebyshev polynomial of degree n with respect to $[-2, 2]$, we have $P_n = \lambda^n T_n(P/\lambda)$. With the explicit expression of T_n :

$$T_n = \sum_{k=0}^{n/2} (-1)^k \frac{n}{k} \binom{n-k-1}{k-1} X^{n-2k}$$

We can completely expand the expression of the polynomial P_n to write it the following way:

$$P_n(X) = X^{nr} + \sum_{k=1}^{nr} \alpha_k X^{nr-k}$$

with $\alpha_k \in \mathbb{Q}$. The goal is now to provoke a perturbation of P_n using a polynomial q_n of degree $< nr$, such that $P_n - q_n \in \mathbb{Z}[X]$ and $q_n(x) < 2\lambda^n$ on E. Hence, according to lemma 4.1, $P_n - q_n$ will have all its nr

roots in E and will still be a monic polynomial with integer coefficients. We will see that it is possible for an infinite number of degrees tending to infinity, which will conclude the proof.

Let us consider $m \in \mathbb{N}^*$ such that $P = X^r + \frac{1}{m}\Gamma$, where $\Gamma \in \mathbb{Z}[X]$. Let $l \in \mathbb{N}^*$ be a random integer (we will fix it later). Let us consider $n_l = (l!)^2 m^l$. If $0 \leqslant k \leqslant l$, we have that $k!\, m^k$ divides n_l ; if $0 \leqslant 2i + j \leqslant l$, we have that $m^j\, i!\, j!$ divides n_l. Therefore, we verify that $\alpha_1, \ldots, \alpha_{lr}$ are integers. What remains in the sum is a polynomial R_n of degree not greater than $nr - lr - 1$ whose coefficients belong to $\mathbb{Q}$. Let us choose $(X^j P_k(X))_{0\leqslant j<r,\ 0\leqslant k<n-l}$ as a basis of $\mathbb{Q}_{nr-lr-1}[X]$, and $c_{j,k} \in \mathbb{Q} \cap [0,1[$ such that $P_{n_l} - q_{n_l} \in \mathbb{Z}[X]$ (c.f. the proof of lemma 3.1), where

$$q_{n_l} = \sum_{0\leqslant j<r} \sum_{0\leqslant k<n-l} c_{j,k} X^j P_k$$

Let us remind that P_k oscillates between $\pm 2\lambda^k$. Let us consider $C = \max_{x\in E}(\sum_{k=0}^{r-1} |x|^k)$. Since $\lambda > 1$, there exists l_0 such that for all $l > l_0$, $\frac{C}{\lambda^l(\lambda-1)} < 1$. Therefore for $l \geqslant l_0$:

$$|q_{n_l}(x)| \leqslant \sum_{j,k} |x|^j\, 2\lambda^k \leqslant 2C \sum_{k=0}^{n-l-1} \lambda^k \leqslant 2C\frac{\lambda^{n-l}}{\lambda - 1} < 2\lambda^n$$

Therefore, we built a sequence of monic polynomials with integer coefficients whose degrees tend to infinity and whose roots all belong to E (the sequence being $(P_{n_l} - q_{n_l})_{l\geqslant l_0}$).
QED □

By refining this proof and using the fact that a polynomial function transforms an equilibrium measure into an equilibrium measure, we have the following stronger theorem :

Theorem 4.6 For the sequence P_n previously built, let us denote by μ_{P_n} the (normalized) counting measure with respect to the roots of P_n. We then have $\mu_{P_n} \xrightarrow{*} \mu_K$, where μ_K is the equilibrium measure of E.

This result is deep. Not only have we built an infinite number of algebraic integers totally in compact set E, but we also know that they are equidistributed with respect to the equilibrium measure of E. It partially answers the question asked in the introduction which dealt with the distribution of algebraic integers totally in a compact set. The proof of this theorem can be found in Serre's article [5].

4.2.5 • From the Pell-Abel case to the general case

Let us give arguments that allows us to reduce the general case to Pell-Abel case. Let us consider $g \geqslant 0$ and

$$U = \{(a_0, b_0, \ldots, a_g, b_g) \in \mathbb{R}^{2g+2} \mid a_0 < b_0 < \cdots < a_g < b_g\}$$

U_{PA} is the subset of U such that for polynomial $D = \prod_{j=0}^{g}(X - a_j)(X - b_j)$, Pell-Abel equation has a solution. We have the following result :

Theorem 4.7 U_{PA} is dense in U.

We shall give here the main steps of the proof. With an element $u \in U$ can be associated a point on the jacobian variety of curve $y^2 = D(x)$: $\nu(u) = \infty_- - \infty_+ \in \mathbb{R}^g/\mathbb{Z}^g$. Theorem 4.1 states that $u \in U_{PA}$ if and only if $\nu(u) = \infty_- - \infty_+$ is a point with finite multiplicity (a torsion point) on the jacobian variety. However we can lift $\nu : U \to \mathbb{R}^g/\mathbb{Z}^g$ in order to obtain a continuous function $\theta : U \to \mathbb{Q}^g$, and $\nu(u)$ is a point of finite

multiplicity in $\mathbb{R}^g/\mathbb{Z}^g$ if and only if $\theta(u) \in \mathbb{Q}^g$. We then conclude thanks to the density of $\mathbb{Q}^g$ in $\mathbb{R}^g$. Additional details of this proof are provided in Serre's article [5].

Thanks to theorem 4.6, it is easy to reduce the general case to Pell-Abel case. In fact, if E_u is a union of segments given by $u \in U$ such that $\mathrm{Cap}(E_u) > 1$, we can find $u' \in U_{PA}$ arbitrarily close to u so that we still have $\mathrm{Cap}(E_{u'}) > 1$, by continuity of $\mathrm{Cap}(E_u)$ with respect to u (corollary 2.2).

CONCLUSION

In this paper, we have responded to the initial problem in the majority of cases:

" Which $\mathbb{R}$ segments have an infinity of algebraic integers totally in them ?"

First, based on "elementary" remarks and numerical results, we had the intuition that segments longer than 4 had an infinity of algebraic integers totally included in them, while segments shorter than 4 had only a finite number of them. However, in order to be able to demonstrate these conjectures, it was necessary to consider our problem as a particular case of a more general problem and not only to consider the $\mathbb{R}$ segments, but all the compact subsets of the complex plane.

We had to clarify the notion of size to have an equivalent of the length of a segment for compact subsets of $\mathbb{C}$. Thus, we introduced the notion of capacity resulting from the theory of potential. Using this concept, we have highlighted that the limit value of capacity for this problem is 1. Potential theory gives several results in this direction but in the case of real segments, it is necessary to combine it with properties of algebraic curves to obtain the desired results.

The "elementary" results of the section 1 allowed us to develop the following intuitions:

1. Capacity is the measurement of size adapted to our problem for compact subsets of $\mathbb{C}$.
2. Generally compact sets with a capacity of less than 1 (including segments with a length of less than 4) have a finite number of algebraic integers totally in them.
3. Generally compact sets with a capacity greater than 1 (including segments with a length greater than 4) have an infinity of algebraic integers totally in them.

The rest of our paper consists in proving results that are in the direction of these intuitions. The main ones are set out below.

The first theorem resulting from the theory of potential gives a complete answer for the second point:

Theorem (Fekete). Any compact with capacity strictly smaller than 1 has a finite number of algebraic integers totally in it.

Corollary Any segment with length strictly smaller than 4 has a finite number of algebraic integers totally in it.

The third point is more complex, but the theory of potential manages to give a partial result:

Theorem (Fekete-Szegö). Let us consider a compact subset of $\mathbb{C}$ with capacity greater than or equal to 1, symmetric with respect to complex conjugation. Then any neighborhood (whose complement is connected) of this compact subset has an infinite number of algebraic integers totally in it.

However, unlike the previous theorem, this theorem is not applicable to $\mathbb{R}$ segments. By mixing notions of algebraic curves with the notion of capacity, we obtain a much stronger theorem that completes the discussion for the $\mathbb{R}$ segments.

Theorem (Robinson). Any finite union of intervals of $\mathbb{R}$ with capacity strictly greater than 1 has an infinite number of algebraic integers totally in it.

Corollary Any segment with length strictly greater than 4 has an infinite number of algebraic integers totally in it.

We give here several avenues for reflection for the interested reader. Many problems remain open.

In the case of $\mathbb{R}$ segments, the situation where the segment length is equal to 4 is unknown, except in the case where the boundaries of the segment are integers. We know that there is then an infinite number of algebraic integers totally in it. What happens if the segment has length 4 and the boundaries are not integers ?

Then, in this paper we were mainly interested in the finiteness of algebraic integers totally in a segment. A natural extension would be to seek to know more about these numbers, especially to know their distribution. Some of the results are contained in our paper. For example, we have found all the algebraic integers totally in the $[-2.2]$ segment. In addition, for a segment E with length strictly greater than 4, by refining the demonstration of Robinson's theorem, it is possible to demonstrate the existence of a sequence of monic polynomials with integer coefficients having all their roots in E and whose counting measure with respect to their roots converges weakly-* to the equilibrium measure of E (4.6). Let us consider a sequence of distinct algebraic integers totally in E. Do the counting measure with respect to their conjugates converge weakly-* to the equilibrium measure of E?

A
MEASURE THEORY

A.1 Measures

The notion of measure that we use is Radon measure.

Definition A.1 (Radon measure). Consider $D \subset \mathbb{C}$. Let $C_c^0(D, \mathbb{R})$ denote the space of functions on D with compact support.

We call *Radon measure* any continuous linear functional on $C_c^0(D, \mathbb{R})$.

If μ is a Radon measure, we write $\int_D f \, \mathrm{d}\mu = \mu(f)$.

Example A.1 (Dirac measure). Let us consider $z_0 \in D$. The Dirac measure on z, denoted by δ_{z_0}, is the linear continuous functional which maps $f \in C_c^0(D, \mathbb{R})$ to $f(z_0)$, *i.e.* $\int f \, \mathrm{d}\delta_{z_0} = f(z_0)$.

Example A.2 ((Averaged) Counting measure). Let $F = \{z_1, \dots, z_n\}$ be a finite subset of D, the (averaged) counting measure with respect to F is given by $\nu_F = \frac{1}{n} \sum_{i=1}^{n} \delta_{z_i}$, *i.e.* $\int f \, \mathrm{d}\nu_F = \frac{1}{n} \sum_{i=1}^{n} f(z_i)$.

Definition A.2 (Measure of a set). Let μ be a measure on $D \subset \mathbb{C}$.

1. If D is compact, the measure of D is defined by $\mu(D) := \int_D 1 \, \mathrm{d}\mu$.
2. If $K \subset D$ is a compact subset, then $\mu(K) = \int_D \mathbb{1}_K \, \mathrm{d}\mu = \int_K 1 \, \mathrm{d}\mu$.
3. If $D = \cup_{n \in \mathbb{N}} K_n$ where $(K_n)_{n \in \mathbb{N}}$ is an increasing sequence of compact subsets, then the measure of D is $\mu(D) := \lim_{n \to \infty} \mu(K_n)$.
4. If $\mu(D) = 1$, we call μ a probability measure on D.

Remark A.1 $\int_D \mathbb{1}_K \, \mathrm{d}\mu = \int_K 1 \, \mathrm{d}\mu$ is defined by $\inf\{\mu(f) : f \in C_c^0(D, \mathbb{R}), 0 \leq f \leq 1, f|_K = 1\}$.

Definition A.3 (Support of a measure). Let μ be a measure on $D \subset \mathbb{C}$ and let $U \subset D$. We say that μ has its support in U if and only if

$$\forall f \in C_c^0(D, \mathbb{R}), f|_U = 0 \Rightarrow \int_D f \, \mathrm{d}\mu = 0$$

The *support* of μ is the intersection of all the closures of such U. Equivalently, it is also the smallest closed subset U of D verifying the previous condition. The support of μ is denoted by $\mathrm{supp}(\mu)$.

Definition A.4 (Restriction/Extension of a measure). Let μ be a measure on D whose support is included in a compact subset $K \subset D$. For all $f \in C^0(K, \mathbb{R})$, there exists $\tilde{f} \in C_c^0(D, \mathbb{R})$ such that $\tilde{f}|_K = f$. We define the integral of f with respect to μ by

$$\mu(f) := \int_K f \, \mathrm{d}\mu := \int_D \tilde{f} \, \mathrm{d}\mu$$

The definition does not dependent on the choice of $\tilde{f}$; μ becomes in this way a measure restricted to K (which will be denoted by μ as well for convenience). For all $f \in C^0(D, \mathbb{R})$, the following integral is well-defined.

$$\mu(f) := \int_D f \, \mathrm{d}\mu := \mu(f|_K)$$

This extends the domain of definition of μ to $C^0(D, \mathbb{R})$.

Remark A.2 Let μ be a measure on D with support in a compact subset K, then $\mu(D) = \mu(K) = \int_D 1 \, \mathrm{d}\mu$.

Remark A.3 Following these definitions, we can define a measure $\tilde{\mu}$ by

$$\tilde{\mu}(A) = \inf_{U \supset A} \sup_{K \subset U} \mu(K)$$

where U is open and K is closed. In this way we extend the measure to any mesurable subset of D.

A.2 Weak-$*$ convergence

Let us define now the import notion of weak-$*$ convergence of measures.

Definition A.5 (Weak-$*$ convergence). Let $D \subset \mathbb{C}$ and $(\mu_n)_{n\in\mathbb{N}}$ be a sequence of measures on D. Let μ be a measure on D. We say that $(\mu_n)_{n\in\mathbb{N}}$ converges weakly to μ, denoted by $\mu_n \xrightarrow{*} \mu$, if and only if

$$\forall f \in C_c^0(D, \mathbb{R}), \ \lim_{n\to\infty} \int_D f \, \mathrm{d}\mu_n = \int_D f \, \mathrm{d}\mu.$$

Example A.3 (Riemann integral). We can consider Riemann integral as the limit measure of a sequence of counting measures : indeed, if $f : [0, 1] \to \mathbb{R}$, we have

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{n} f(\frac{k}{n}) = \int_0^1 f \ \mathrm{d}x.$$

Let ν_n denote the counting measure with respect to points $\{\frac{k}{n} \mid k = 0, \ldots, n\}$. The continuous linear functional $\int_0^1$ is the limit measure of the sequence (ν_n) for weak-$*$ convergence.

Example A.4 If ν_n is the counting measure with respect to n-th roots of unity $\{e^{\frac{2\pi ik}{n}} \mid k = 0, \dots, n-1\}$, then

$$\lim_{n\to\infty} \int f \, \mathrm{d}\nu_n = \frac{1}{2\pi} \int_0^{2\pi} f(e^{i\theta}) \, \mathrm{d}\theta.$$

Proposition A.1 Let K be a compact subset of $\mathbb{C}$ such that $K = \bigcap_{n\in\mathbb{N}} B_n$, where $(B_n)_{n\in\mathbb{N}}$ is a decreasing sequence of compact sets. If there exists a sequence of probability measures $(\mu_n)_n$ such that $\mu_n \xrightarrow{*} \mu$ and $\mathrm{supp}(\mu_n) \subset B_n$ for each n, then $\mathrm{supp}(\mu) \subset K$.

Proof. Consider $f \in C_c^0(D, \mathbb{R})$ such that $f|_K = 0$, let us show that for all $\epsilon > 0$, we have $\left|\int_K f \, \mathrm{d}\mu\right| < \epsilon$. The open set ($f$ is continuous) $U := \{|f| < \epsilon\}$ contains $K = \bigcap_n B_n$. Since all K_i are compact, there exists an integer N such that $\forall n \geq N, B_n \subset U$. Consider $\phi_n \in C_c^0(D, \mathbb{R})$ such that

$$\phi_n|_{B_n} = 1, \quad \phi_n|_{U^c} = 0, \quad 0 \leq \phi_n \leq 1$$

Then for all $n \geq N$, $|\phi_n f| < \epsilon, (1-\phi_n)f|_{B_n} = 0$, so that $\left|\int_D f \, \mathrm{d}\mu_n\right| = \left|\int_D \phi_n f \, \mathrm{d}\mu_n\right| < \epsilon$; thus $\mu_n \xrightarrow{*} \mu$ gives $\left|\int_K f \, \mathrm{d}\mu\right| \leq \epsilon$ □

We are now interested in the space of measures on a given topological space. Let X be a compact metric space. Let $C(X)$ denote the set of continuous functions from X to $\mathbb{R}$, and $\mathcal{P}(X)$ denote the set of probability measures on X.

Theorem A.1 (Banach-Alaoglu-Bourbaki). $\mathcal{P}(X)$ is sequentially compact for the topology associated with the weak-$*$ convergence (*i.e.*, weak-$*$ topology).

In other words, for any sequence of probability measures $(\mu_n)_n$, there are a sub-sequence $(\mu_{\varphi(n)})_n$ and a probability measure μ such that $\mu_{\varphi(n)} \xrightarrow{*} \mu$, *i.e.*

$$\forall \phi \in C(X), \int_X \phi \ \mathrm{d}\mu_{\varphi(n)} \longrightarrow \int_X \phi \ \mathrm{d}\mu$$

Proof.

X is a compact metric space, so that $C(X)$ is separable, *i.e.* there is a dense sequence $(\phi_n)_n$ in $C(X)$.

The idea is to do a diagonal extraction. For ϕ_1, we have $(\int_X \phi_1 \, d\mu_n)_n$ which is bounded. So we can extract a sub-sequence $(\mu_{\varphi_1(n)})_n$ such that $(\int_X \phi_1 \, d\mu_{\varphi_1(n)})_n$ converges. We can extract in the same way $(\mu_{\varphi_2(n)})_n$ from the sequence $(\mu_{\varphi_1(n)})_n$. Thus, we construct $(\mu_{\varphi_k(n)})_n$ for all $k \in \mathbb{N}$, which is extracted from the previous sequences.

We consider then the sequence $(\mu_{\varphi_n(n)})_n$. For $k \in \mathbb{N}$, $(\int_X \phi_k \, d\mu_{\varphi_n(n)})_n$ converges : indeed, for some sufficiently large n , φ_n is extracted from φ_k. Using the density of $(\phi_n)_n$, $(\int_X \phi \, d\mu_{\varphi_n(n)})_n$ converges for $\phi \in C(X)$.

Let us define the functional

$$\Lambda : C(X) \longrightarrow \mathbb{R}$$

$$\phi \longmapsto \lim_{n\to+\infty} \int_X \phi \, d\mu_{\varphi_n(n)}$$

It is clearly a positive linear functional. By Riesz–Markov–Kakutani representation theorem, we have : $\Lambda(\phi) = \int_X \phi \, d\mu$ where μ is a measure $C(X)$.

To prove the compactness of $\mathcal{P}(X)$, it is enough to show that $\mu \in \mathcal{P}(X)$, since we have by construction $\forall \phi \in C(X), \int_X \phi \, d\mu_{\varphi_n(n)} \longrightarrow \int_X \phi \, d\mu$. This fact is true because $\int_X d\mu = \lim_{k \to +\infty} \int_X d\mu_{\varphi_n(n)} = 1$. □

A.3 Lower semi-continuous functions

We wish to extend the concept of measure and weak-$*$ convergence to functions that are not necessarily continuous.

Definition A.6 (Lower semi-continuous function). A function $f : D \subset \mathbb{R}^m \to \mathbb{R} \cup \{+\infty\}$ is said to be *lower semi-continuous (l.s.c.)* if one of the following equivalent properties is satisfied:

(i) $\forall z_0 \in D, f(z_0) \leqslant \liminf_{z \to z_0} f(z)$

(ii) On all compact subsets $K \subset D$, f is a pointwise limit of an increasing sequence of continuous functions

(iii) $\forall \alpha \in \mathbb{R}$, $\{f > \alpha\} := f^{-1}(]-\infty, \alpha[)$ is a open set.

Definition A.7 Let f be a l.s.c. function and μ be a positive measure with support in a compact subset $K \subset D$. We define the integral of f with respect to μ :

$$\int_K f \, \mathrm{d}\mu = \lim_{n \to \infty} \int_K f_n \, \mathrm{d}\mu$$

where (f_n) is an increasing sequence of continuous functions on K which converges pointwise to $f|_K$

Proposition A.2 Any l.s.c function defined on a compact set has a minimum point.

Proof. Consider the sets $\{f > n\}_{n \in \mathbb{Z}}$ and $\{f \leq \frac{1}{n} + \inf f\}_{n \in \mathbb{N}^*}$. □

Proposition A.3 Let f be a l.s.c. function verifying $f|_K \geq \alpha$ and let $\mu \in \mathcal{P}(D)$ with $\mathrm{supp}(\mu) = K \subset D$. Then $\int_K f \, \mathrm{d}\mu \geq \alpha$. In addition, $\int_K f \, \mathrm{d}\mu = \alpha$ if and only if $f|_K \equiv \alpha$.

Proof. Since μ is a probability measure, we can assume without loss of generality that $\alpha = 0$. Let (f_n) be an increasing sequence of continuous functions on K which converges pointwise to $f|_K \geq 0$. Then $\forall \epsilon > 0$, $K = \cup_{n \geq 1} \{f_n > -\epsilon\}$. By compactness, $\exists N \, \forall n \geq N, f_n > -\epsilon$ on K, which implies $\int_K f \, \mathrm{d}\mu \geq -\epsilon$. So that $\int_K f \, \mathrm{d}\mu \geq 0$.

For the second assertion, assume there exists $\zeta_0 \in K$ such that $f(\zeta_0) > 0$. Then we have $\int_K f \, \mathrm{d}\mu > 0$. Indeed, there exists two open neighborhoods $B_1 \subset B_2$ of ζ_0 in D such that $f|_{B_2} \geq \frac{1}{2} f(\zeta_0)$. Let $\chi \in C_c^0(B_2, \mathbb{R})$ such that $\chi|_{B_1} = 1$ and $0 \leq \chi \leq 1$. Then $f - \frac{1}{2} f(\zeta_0)\chi$ is a l.s.c function on D and positive on K. By the above, $\int_K (f - \frac{1}{2} f(\zeta_0)\chi) \, \mathrm{d}\mu \geq 0$, so that $\int_K f \, \mathrm{d}\mu \geq \frac{1}{2} f(\zeta_0) \int_K \chi \, \mathrm{d}\mu$. The last quantity is strictly positive, otherwise we would have $\mathrm{supp}(\mu) \subset K \backslash B_1 \subsetneq K$ (let $\phi \in C_c^0(D, \mathbb{R})$ such that $\phi|_{K \backslash B_1} = 0$, then $(1 - \chi)\phi^{\pm}|_K = 0$,

$\int_K \phi^{\pm} \, \mathrm{d}\mu = \int_K \chi\phi^{\pm} \, \mathrm{d}\mu \leq \|\phi\|_\infty \int_K \chi \, \mathrm{d}\mu = 0$, then $\int_K \phi \, \mathrm{d}\mu = 0$), which is a contradiction. □

Proposition A.4 Let f be a l.s.c. function and (μ_n) be a sequence of positive measures with support included in a compact subset K such that $\mu_n \xrightarrow{*} \mu$. Then:

$$\int_K f \, \mathrm{d}\mu \leqslant \liminf_{n\to\infty} \int_K f \, \mathrm{d}\mu_n$$

Proof. Let (f_n) be an increasing sequence of continuous functions which converges pointwise to f. Let $\epsilon > 0$. There exists $n \in \mathbb{N}$ such that $\int_K f_n \, \mathrm{d}\mu \geq \int_K f \, \mathrm{d}\mu - \epsilon$. There exists $m_0 \in \mathbb{N}$ such that for $m \geq m_0$, $\int_K f_n \, \mathrm{d}\mu_m \geq \int_K f_n \, \mathrm{d}\mu - \epsilon$. Then :

$$\forall m \geq m_0, \int_K f d\mu_m \geq \int_K f_n \, \mathrm{d}\mu_m \geq \int_K f \, \mathrm{d}\mu - 2\epsilon$$

Thus $\liminf_{m\to\infty} \int_K f \, \mathrm{d}\mu_m \geq \int_K f \, \mathrm{d}\mu - 2\epsilon$ □

Example A.5 Let $z \in \mathbb{C}$, the function $t \mapsto \log(1/|z-t|)$ is lower semi-continuous, because it is continuous on $t \neq z$ and equal to $+\infty$ on $t = z$.

B
SEMI-HARMONIC FUNCTIONS

Definition B.1 **((super-,sub-)harmonic functions).** Let $D \subset \mathbb{C}$ be an open subset. A function $f : D \to \mathbb{R}$ is said to be *harmonic* (*resp.* *super-harmonic, sub-harmonic*) if it is continuous (*resp.* lower/upper semi-continuous) and satisfies the *mean value property*: for all $z \in D$ and a disc $\{|\zeta - z| \leq r\} \subset D$, we have

$$f(z) = \frac{1}{2\pi} \int_0^{2\pi} f(z + re^{i\theta})\, \mathrm{d}\theta \quad (resp.\ \geq, \leq)$$

A function is called *semi-harmonic* if it is harmonic or super-harmonic or sub-harmonic.

Intuitively, a *super*-harmonic function takes values *larger* than its local mean values. However, it cannot take too large values because of the lower semi-continuity.

$$f(z) \leq \liminf_{\zeta \to z} f(\zeta).$$

Remark B.1 Let $f : D \to \mathbb{R}$ be a continuous (*resp.* lower semi-continuous, upper semi-continuous) function. Then f is harmonic (*resp.* super-harmonic, sub-harmonic) if and only if it satisfies the mean (*resp.* super-mean, sub-mean) value property : for all $z \in D$, there exists $\delta > 0$ such that the disk $\{|\zeta - z| \leq \delta\} \subset D$ and for all $0 < r \leq \delta$, we have

$$f(z) = \frac{1}{2\pi} \int_0^{2\pi} f(z + re^{i\theta})\, \mathrm{d}\theta \quad (resp.\ \geq, \leq)$$

Remark B.2 Assume $f \in C^2(D)$. Then f is super-harmonic if and only if $-\Delta f \geq 0$. To understand this claim, we can consider the function

$$m(r; z) = \frac{1}{2\pi} \int_0^{2\pi} f(z + re^{i\theta})\, \mathrm{d}\theta$$

and use the following formula

$$\partial_r m(r; z) = \frac{1}{2\pi\, |r|} \int_{B(z,|r|)} \Delta f.$$

Proof. Consider f as a function from $\mathbb{R}^2$ to $\mathbb{R}$. Let $\overrightarrow{n}(\theta) = (\cos\theta, \sin\theta)$:

$$\partial_r f((Re(z), Im(z)) + r\mathbf{n}(\theta)) = \overrightarrow{\nabla} f \cdot \overrightarrow{n}(\theta).$$

By Green's theorem:

$$\begin{aligned} \partial_r m(r; z) &= \frac{1}{2\pi} \oint_{\partial B(z,r)} \overrightarrow{\nabla} f \cdot \overrightarrow{n}(\theta) \frac{\mathrm{d}l}{r} \\ &= \frac{1}{2\pi r} \iint_{B(0,r)} \overrightarrow{\nabla} \cdot \overrightarrow{\nabla} f \cdot ds. \end{aligned}$$

□

Example B.1 Le F be a holomorphic function on an open subset $D \in \mathbb{C}$. Then for $p > 0$, $|F|^p$ and $\log|F|$ are sub-harmonic. Indeed, it is enough to prove this claim on the open set $\{F \neq 0\}$. Since locally F^p (*resp.* $\log F$) has a holomorphic branch, we can verify the continuity and apply Cauchy's formula. Then we conclude by using the triangular inequality for integrals (by considering the real part *resp.*).

Proposition B.1 Let f, g be two super-harmonic function on U. Then $\min(f, g)$ is also super-harmonic on U.

Proof. The minimum of two l.s.c. functions is still a l.s.c. function. Then we conclude by verifying the super-mean property. □

Theorem B.1 (Minimum principle for super-harmonic functions). Let $D \subset \mathbb{C}$ be a connected and bounded open subset. Let f be a non-constant super-harmonic function on D such that

$$\liminf_{z \to \zeta} f(z) \geq m, \quad \forall \zeta \in \partial D$$

Then $f(z) > m$ for all $z \in D$. Thus, no non-constant super-harmonic function on a connected open set (not necessarily bounded) reaches its minimum.

Proof. The idea of the proof is to use the super-mean property and an open-closed set argument.

Firstly, we extend $f(z)$ to all points $\zeta \in \partial D$ by $\tilde{f}(\zeta) = \liminf_{z \to \zeta} f(z)$ and $\tilde{f}|_D = f$. So $\tilde{f}$ is a l.s.c. function on $\overline{D}$ and super-harmonic on D. Since $D \subset \mathbb{C}$ is bounded and $\overline{D}$ is compact, $\tilde{f}$ reaches its minimum $m' = \min_{\overline{D}} \tilde{f}$ on $\overline{D}$ (Prop. A.2).

Since f is l.s.c., the set $\{f = m'\} = \{f \leq m'\}$ is closed in D. On the other hand, for all $\zeta_0 \in D$ verifying $f(\zeta_0) = m'$, we have for some $\delta > 0$ and all $r \in]0, \delta]$,

$$m' = f(\zeta_0) \geq \frac{1}{2\pi} \int_0^{2\pi} f(\zeta_0 + re^{i\theta}) \, \mathrm{d}\theta \geq m'$$

By Prop. A.3, for all $r \in]0, \delta]$, $\theta \in [0, 2\pi]$, we have $f(\zeta_0 + re^{i\theta}) = f(\zeta_0) = m'$, *i.e.* $f \equiv m'$ in a neighborhood of ζ_0, which shows that $\{f = m'\}$ is an open subset of D. Thus, $\{f \leq m'\} = \{f = m'\}$ is open-closed in D; it is not D since f is non-constant, so it is empty because D is connected, *i.e.* $f(z) > m'$, $\forall z \in D$.

On the other hand, since m' is effectively reached by $\tilde{f}$, there exists $\zeta_0 \in \overline{D} \backslash D = \partial D$ such that $\tilde{f}(\zeta_0) = m'$. By definition of $\tilde{f}$ and the hypothesis in the statement of the theorem (finally!), we have

$$\tilde{f}(\zeta_0) = \liminf_{z \to \zeta_0} f(z) \geq m$$

. So that $m' \geq m$. Then we conclude that $f(z) > m$, $\forall z \in D$. □

Corollary B.1 (Maximum principle for potentials). Let μ be a finite positive measure with compact support. If $U^\mu(z) \leq M$ for all $z \in \mathrm{supp}(\mu)$, then it holds for all $z \in \mathbb{C}$.

Proof. Let $K = \mathrm{supp}(\mu)$. Let us define $f(z) := -U^\mu(z)$, which is a harmonic function, *a fortiori* super-

harmonic on $\mathbb{C}\backslash K$. It is non-constant and converges to $+\infty$ when $z \to \infty$. For all $\zeta_0 \in \partial K$, we have

$$\liminf_{z\to\zeta_0} f(z) \geq -M. \tag{4}$$

Then f reaches its minimum if there exists $z \in \mathbb{C}$ such that $U^\mu(z) > M$.

Now we should prove (4). Let $r > 0$. We have

$$f(\zeta) - f(z) = \int \log \frac{|\zeta - t|}{z - t} \, \mathrm{d}\mu(t) = \left(\int_{K\cap B(\zeta_0,r)} + \int_{K\setminus B(\zeta_0,r)} \right) \log \frac{|\zeta - t|}{|z - t|} \, \mathrm{d}\mu(t).$$

Let us choose $\zeta = \zeta(z) \in \arg\min_{\zeta\in K} |\zeta - z|$. Then for all $t \in K$, we have

$$\frac{|\zeta - t|}{|z - t|} = \frac{|\zeta - z| + |z - t|}{|z - t|} \leq \frac{|t - z| + |z - t|}{|z - t|} = 2.$$

We derive that

$$\int_{K\cap B(\zeta_0,r)} \log \frac{|\zeta - t|}{|z - t|} \, \mathrm{d}\mu(t) \leq 2\mu(B(\zeta_0, r)).$$

On the other hand, when $z \to \zeta_0$, we have $\zeta \to \zeta_0$. So,

$$\int_{K\setminus B(\zeta_0,r)} \log \frac{|\zeta - t|}{|z - t|} \, \mathrm{d}\mu(t) \to \mu(B(\zeta_0, r)^c) \times \log(1) = 0.$$

The assumption on $U^\mu(z)$ implies that $f(\zeta) \geq -M > -\infty$. By passing to the limit $z \to \zeta_0$, we have

$$\liminf_{z\to\zeta_0} f(z) \geq -M - 2\mu(B(\zeta_0, r)). \tag{5}$$

Since $f \geq -M$ on K by hypothesis, we have $f > -\infty$ everywhere on $\mathbb{C}$ by the definition of $f = -U^\mu(z)$. So

$$\lim_{r\to 0} \mu(B(\zeta_0, r)) = \mu(\{\zeta_0\}) = 0.$$

Combining with (5), we conclude the proof of (4). □

We state the following theorem which generalizes the minimum principle:

Theorem B.2 (Generalized minimum principle). Let $D \subset \overline{\mathbb{C}}$ be a connected open set such that $\mathrm{Cap}(\partial D) > 0$. Let f be a non-constant super-harmonic function, lower-bounded in D, verifying *quasi-almost everywhere* in D the inequality :

$$\liminf_{z\to\zeta} f(z) \geq m.$$

Then we have $f(z) > m$ for all $z \in D$.

A proof of the theorem can be found in [10], Theorem 3.6.9.

Proposition B.2 (Backward-pulling by holomorphic mapping). Let f be a non-constant holomorphic function on a connected open subset $D \subset \mathbb{C}$. Let $D' = f(D)$ (a connected open set as well). Then for any (sub-, super-)harmonic function $u : D' \to \mathbb{R}$, $u \circ f$ is also (sub-, super-)harmonic.

A proof of the proposition can be found ([10], Corollary 2.4.3).

This proposition allows us to extend the definition of (sub-, super-)harmonic functions to the Riemann sphere $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$:

Definition B.2 **((Super-, sub-)harmonic function on Riemann sphere).** A function $f(z)$ defined on a neighborhood of ∞ (∞ included) is said to be *(sub-,super-)harmonic on a neighborhood of* ∞ if $f(1/z)$ is (sub-, super-)harmonic at point 0. A function $f : \overline{\mathbb{C}} \supset D \to \mathbb{R}$ is said to be *(sub-,super-)harmonic* if all points of D have a neighborhood where f is *(sub-,super-)harmonic*.

C
SOME TECHNICAL PROOFS

C.1 Proof of proposition 2.6

Proposition C.1 Let $K \subset \mathbb{C}$ be a compact subset with $\mathrm{Cap}(K) > 0$. If Ω_K verifies the cone condition, then Ω_K is regular.

Proof. We shall prove that for all $\zeta_0 \in \partial\Omega_K$,

$$\lim_{z\to\zeta_0} g_K(z,\infty) = 0$$

(i) First, let $\chi(z)$ be a positive super-harmonic function defined on a non-empty connected open set $\Omega_0 = \Omega_K \cap B(\zeta_0,\delta)$ such that

$$A = \inf\left\{\chi(z) : z \in \Omega_K, \frac{\delta}{2} < |z-\zeta_0| < \delta\right\} > 0$$

$$\lim_{z\to\zeta_0} \chi(z) = 0.$$

Since $g_K(\cdot,\infty)$ is bounded on Ω_0 (Thm. 2.6), one can find a large enough $M > 0$ such that $MA > g_K(\cdot,\infty)$ on Ω_0; thus for all $\zeta \in \Omega_K \cap \partial B(\zeta_0,\delta)$, we have

$$\liminf_{z\to\zeta}(M\chi(z) - g_K(z,\infty)) \geq 0;$$

we also deduce that $M\chi - g_K(\cdot,\infty)$ is *bounded from below* on Ω_0. Also, because χ is positive, for all $\zeta \in \partial\Omega_K$ such that $|\zeta-\zeta_0| \leq \delta$, we have

$$\liminf_{z\to\zeta} \chi(z) \geq 0,$$

then we have *q.-a.e.* in $\partial\Omega_K$,

$$\liminf_{z\to\zeta}(M\chi(z) - g_K(z,\infty)) \geq 0.$$

On the other hand, χ is super-harmonic on Ω_0, so $M\chi - g_K(\cdot,\infty)$ is super-harmonic because $g_K(\cdot,\infty)$ is harmonic. Observing that

$$\partial\Omega_0 \subset \{\zeta \in \partial\Omega_K : |\zeta-\zeta_0| \leq \delta\} \cup \{\zeta \in \Omega_K : |\zeta-\zeta_0| = \delta\}$$

and that (Prop. 2.4(c)) $\mathrm{Cap}(\partial\Omega_0) = \mathrm{Cap}(\overline{\Omega_0}) > 0$ since Ω_0 is open and non-empty (Cor. 2.3(a)). By applying the generalized minimum principle on Ω_0, we have for all $z \in \Omega_0$,

$$M\chi(z) - g_K(z,\infty) \geq 0,$$

therefore,

$$0 = \lim_{z\to\zeta_0} M\chi(z) \geq \limsup_{z\to\zeta_0} g_K(z,\infty) \geq 0$$

$$\lim_{z\to\zeta_0} g_K(z,\infty) = 0.$$

(ii) Let χ be a positive super-harmonic function on $\Omega_1 = \Omega_K \cap B(\zeta_0,\delta) \neq \emptyset$ such that

$$A = \inf\left\{\chi(z) : z\in\Omega_K, \frac{\delta}{2} < |z-\zeta_0| < \delta\right\} > 0$$

$$\lim_{z\to\zeta_0} \chi(z) = 0$$

For $z\in\Omega_K$, define

$$\tilde{\chi}(z) = \begin{cases} \min\left(\frac{\chi(z)}{A}, 1\right) & z\in\Omega_1 \\ 1 & z\in\Omega_K\backslash\Omega_1 \end{cases}$$

By definition, $0 < \tilde{\chi} \leq 1$. As the minimum of two super-harmonic functions, $\tilde{\chi}$ is also super-harmonic on Ω_1; $\tilde{\chi}\equiv 1$ is super-harmonic on $\Omega_K \cap \{|z-\zeta_0| > \frac{\delta}{2}\}$; therefore, $\tilde{\chi}$ is super-harmonic on Ω_K. Furthermore, we have

$$\lim_{z\to\zeta_0} \tilde{\chi}(z) = 0.$$

Take $R > 2\delta$ large enough such that $\partial\Omega_K \subset B(\zeta_0,R)$, then $\Omega_0 = \Omega_K \cap B(\zeta_0,R) \neq \emptyset$ is *connected* because Ω_K is *connected*. Also, we have

$$\inf\left\{\chi(z) : z\in\Omega_K, \frac{R}{2} < |z-\zeta_0| < R\right\} = 1 > 0.$$

We have reduced our proof to the case (i) with $(\chi,\delta) := (\tilde{\chi},R)$.

(iii) For all $\zeta_0\in\partial\Omega_K$, we shall prove the existence of such a function χ as in (ii) (for some $\delta>0$). We can take the composition of a Möbius transformation and an analytic branch of $\Re(1/\log w), |w|<1$.

More precisely, since the cone condition is verified, one can choose $\zeta_1 \neq \zeta_0$ such that the segment $[\zeta_0,\zeta_1] \subset \mathbb{C}\backslash\Omega_K$. Then take

$$\chi(z) = \Re\left(1\Big/\log\frac{z-\zeta_0}{z-\zeta_1}\right), \quad z\in\Omega_K, \left|\frac{z-\zeta_0}{z-\zeta_1}\right| < 1$$

for some well-chosen δ. Taking Prop. B.2 into account, the verification of this construction will be direct. □

Remark C.1 Notice that it is only in step (iii) that we have used the cone condition, which aimed at constructing a pair (δ,χ) for (ii); therefore, without the cone condition, if one can construct a pair (δ,χ) for all $\zeta_0\in\partial\Omega_K$ verifying the conditions in (ii), then Ω_K is still regular.

C.2 Proof of theorem 2.8

Theorem C.1 Let $K_1, K_2 \subset \mathbb{C}$ be two non-empty compact subsets. Let $f : \Omega_{K_1} \cup \{\infty\} \to \Omega_{K_2} \cup \{\infty\}$ be a non-constant holomorphic mapping such that $f(\infty) = \infty$. Then,

(a) $|A_f| \operatorname{Cap}(K_1)^{n_f} \geq \operatorname{Cap}(K_2)$.

(b) If we assume in addition :

(i) $\operatorname{Cap}(K_2) > 0$;

(ii) $f^{-1}(\infty) = \{\infty\}$;

(iii) Ω_{K_2} is regular;

(iv) f can be continuously extended to the boundaries $\partial\Omega_{K_1} \to \partial\Omega_{K_2}$.

Then, $\operatorname{Cap}(K_1)>0$, Ω_{K_1} is regular and

$$g_{K_1}(\cdot, \infty) = \frac{1}{n_f} g_{K_2}(f(\cdot), \infty)$$

$$|A_f| \operatorname{Cap}(K_1)^{n_f} = \operatorname{Cap}(K_2).$$

Proof. (a). We can assume that $\operatorname{Cap}(K_2) > 0$ without loss of generality. Then $g_{K_2}(\cdot, \infty) > 0$ is harmonic on Ω_{K_2}. So that $g_{K_2}(f(\cdot), \infty) > 0$ is super-harmonic (Prop. B.2) on Ω_{K_1} (and it is harmonic if $f^{-1}(\infty) = \{\infty\}$). Furthermore, we have $g_{K_2}(w, \infty) = \log|w| + V_{K_2} + o(1)$ when $w \to \infty$. Then,

$$g_{K_2}(f(z), \infty) = \log|f(z)| + V_{K_2} + o(1) = n_f \log|z| + \log|A_f| + V_{K_2} + o(1), \quad z \to \infty$$

Assume first that $\operatorname{Cap}(K_1) > 0$. Let us define

$$h(z) := g_{K_2}(f(z), \infty) - n_f g_{K_1}(z, \infty).$$

Then h is super-harmonic on Ω_{K_1}, and even on $\Omega_{K_1} \cup \{\infty\}$ if we remove this isolated singularity by defining

$$h(\infty) := \log|A_f| + V_{K_2} - n_f V_{K_1}.$$

According to Thm. 2.6, $\lim_{z\to\zeta} g_{K_1}(z, \infty) = 0$ for *quasi-almost every* $\zeta \in \partial\Omega_{K_1}$. So, we have for *quasi-almost every* $\zeta \in \partial\Omega_{K_1}$

$$\liminf_{z\to\zeta} h(z) \geq 0.$$

Besides, we have seen that $h(z)$ in bounded on a neighborhood of ∞; beyond this neighborhood , $g_{K_1}(\cdot, \infty)$ is bounded. Thus $h(z)$ is lower-bounded. So, the generalized minimun principle implies that either $h(z) \equiv 0$ or $h(z) > 0$ on Ω_{K_1}. In particular,

$$h(\infty) = \log|A_f| + V_{K_2} - n_f V_{K_1} \geq 0.$$

Henceforth, we no longer assume $\operatorname{Cap}(K_1) > 0$. For $\epsilon > 0$, let $K_1^\epsilon = \{z \in \mathbb{C} : \operatorname{dist}(z, K_1) \leq \epsilon\}$, which has non-empty interior. Thus, $\operatorname{Cap}(K_1^\epsilon) > 0$ according to Cor. 2.3(a). Then we have $|A_f| \operatorname{Cap}(K_1^\epsilon)^{n_f} \geq \operatorname{Cap}(K_2)$ by previous arguments. Applying Prop. 2.4(d) to the sequence $(K_1^{1/n})$, we have

$$|A_f| \operatorname{Cap}(K_1)^{n_f} \geq \operatorname{Cap}(K_2)$$

(b). We have $\mathrm{Cap}(K_1) > 0$ by (a). By the continuous extension theorem, we have that $\lim_{z\to\zeta_0} f(z)$ exists and belongs to Ω_{K_2} for all $\zeta_0 \in \partial\Omega_{K_1}$. So the regularity of Ω_{K_2} implies that

$$\lim_{z\to\zeta_0} g_{K_2}(f(z),\infty) = 0, \quad \forall \zeta_0 \in \partial\Omega_{K_1}$$

We keep the notations of (a). We remind that $h(z)$ is bounded on a neighborhood U of ∞; The conditions (ii) and (iv) imply that $f(U)$ is included in the complementary of a neighborhood of ∞ in Ω_{K_2}. Then $g_{K_2}(f(\cdot),\infty)$ is bounded in $\Omega_{K_1}\backslash U$. We have then shown that $h(z)$ is a harmonic function which is bounded on $\Omega_{K_1} \cup \{\infty\}$ and verifies

$$\lim_{z\to\zeta} h(z) = 0.$$

for *quasi-almost every* $\zeta \in \partial\Omega_{K_1}$. By the generalized minimum principle applied to h and to $-h$, we have $h(z) \equiv 0$, in particular $h(\infty) = 0$. So, we have

$$V_{K_1} = \frac{1}{n_f}(\log|A_f| + V_{K_2})$$

$$\mathrm{Cap}(K_1) = \left(\frac{\mathrm{Cap}(K_2)}{|A_f|}\right)^{1/n_f}.$$

□

REFERENCES

[1] Marc Hindry : Géométrie arithmétique. *In Cahiers du séminaire d'histoire des mathématiques 2e série*, volume 3, pages 79–84. 1993.

[2] G. Rémond : Conjectures uniformes sur les variétés abéliennes. *Quart.,J. Math.(to appear)*, 2017.

[3] Bertrand et Waldschmidt : Quelques travaux récents en théorie des nombres transcendants. *In Mémoires de la S. M. F. 2e série*, volume 2, pages 107–119. 1980.

[4] Pierre Deligne : La conjecture de weil : I. *Publications Mathématiques de l'IHÉS*, 43:273–307, 1974.

[5] J.-P. Serre : Distribution asymptotique des valeurs propres des endomorphismes de Frobenius [d'après Abel, Chebyshev, Robinson, ...]. *Séminaire Bourbaki*, n° 1146, 2018.

[6] Valérie Flammang, Georges Rhin et Qiang wu : The totally real algebraic integers with diameter less than 4. *Moscow Journal of Combinatorics and Number Theory*, 1, 01 2011.

[7] Edward B Saff et Vilmos Totik : *Logarithmic potentials with external fields*, volume 316. Springer Science & Business Media, 2013.

[8] Robert Mayans : The chebyshev equioscillation theorem. *The Journal of Online Mathematics and Its Applications*, 6, 2006.

[9] Jean-Benoît Bost : *Introduction to Compact Riemann Surfaces, Jacobians, and Abelian Varieties*, pages 64–211. Springer Berlin Heidelberg, Berlin, Heidelberg, 1992.

[10] T. Ransford : *Potential theory in the complex plane*, volume 28. Cambridge University Press, 1995.

[11] E. B. Saff : Logarithmic potential theory with applications to approximation theory. *Surveys in Approximation Theory, 5 (2010), 165–200.*

[12] J. I. Burgos Gil et R. Menares : Equidistribución, teoría del potencial y aplicaciones aritméticas. Notes de cours.

[13] M. Tsuji : *Potential theory in modern function theory*, volume 4. Chelsea Publ. Co., New York, 1975.

[14] M. Fekete et G. Szegö : On algebraic equations with integral coefficients whose roots belong to a given point set. *Mathematische Zeitschrift*, 63(1):158–172, 1955.

[15] T. Ransford : Computation of logarithmic capacity. *Computational Methods and Function Theory*, 10(2):555–578, 2011.