Séminaire BOURBAKI Mars 2018
70e année, 2017–2018, no 1146

DISTRIBUTION ASYMPTOTIQUE DES VALEURS PROPRES DES ENDOMORPHISMES DE FROBENIUS
[d'après Abel, Chebyshev, Robinson,...]

par **Jean-Pierre SERRE**

À la mémoire de mon vieil ami Michel Raynaud

INTRODUCTION

Lorsque l'on a une suite d'opérateurs linéaires de rang tendant vers l'infini, on peut s'intéresser à la distribution asymptotique de leurs valeurs propres. C'est ce que nous allons faire ici, dans le cas des endomorphismes de Frobenius des variétés abéliennes (autrement dit, des motifs purs de poids 1).

Fixons un corps fini $\mathbf{F}$, à q éléments. Soit $\mathcal{A}$ l'ensemble des classes d'isogénie de variétés abéliennes sur $\mathbf{F}$ de dimension > 0. Si $A \in \mathcal{A}$, soit $P_A(X)$ le polynôme caractéristique de son endomorphisme de Frobenius. C'est un polynôme unitaire de degré $2 \dim A$, à coefficients dans $\mathbf{Z}$, dont les racines complexes appartiennent au cercle C de centre 0 et de rayon $q^{1/2}$; réciproquement, d'après Honda-Tate ([Ta 69]), tout polynôme ayant ces propriétés provient (à une puissance près, cf. lemme 1.8.1) d'une variété abélienne sur $\mathbf{F}$. Comment se répartissent les racines de P_A quand A varie ?

Pour donner un sens précis à cette question, il est commode d'utiliser le langage des mesures : si $d = 2 \dim A$, écrivons P_A sous la forme $\prod_{i=1}^{d}(X - z_i)$ et définissons une mesure μ_A sur C par $\mu_A = \frac{1}{d}\sum \delta_{z_i}$, où δ_{z_i} désigne la mesure de Dirac en z_i ; c'est une mesure positive de masse 1. Notons $\mathbf{M}^{\mathrm{ab}}$ l'ensemble des mesures sur C qui sont limites (pour la topologie faible de l'espace des mesures, cf. §1.1) d'une suite de μ_A, avec $A \in \mathcal{A}$. Quelles sont les propriétés des mesures $\mu \in \mathbf{M}^{\mathrm{ab}}$, et en particulier quels peuvent être leurs supports ?

Nous répondrons partiellement à cette dernière question, en montrant que *le support d'une mesure de* $\mathbf{M}^{\mathrm{ab}}$ *est, soit fini, soit de capacité* $\geqslant q^{1/4}$, la borne $q^{1/4}$ étant optimale. Nous donnerons aussi des exemples où le support de la mesure est *un ensemble totalement discontinu analogue à l'ensemble triadique de Cantor*. La situation est donc très différente de celle où l'on se limite à des jacobiennes de courbes algébriques : dans ce cas, Tsfasman et Vlăduţ ont montré (cf. [TV 97] et [Se 97]) que l'on n'obtient essentiellement que des mesures à support égal au cercle C, qui ont une densité continue ne s'annulant qu'en un nombre fini de points.

Le texte est formé de deux §§ suivis d'un Appendice.

Le §1 contient les démonstrations des énoncés ci-dessus. Il donne d'abord (§1.2) des théorèmes de structure sur les éléments de $\mathbf{M}^{\mathrm{ab}}$, dans le cadre plus général des entiers algébriques qui sont « totalement » dans un compact fixé de $\mathbf{C}$ (pas nécessairement un cercle). Les démonstrations (§1.4) reposent sur la positivité de certaines intégrales du type $\int \log|Q(x)|\mu(x)$, où Q est un polynôme à coefficients dans $\mathbf{Z}$. Ceci fait, il n'y a plus qu'à appliquer un théorème de Robinson ([Ro 64]) pour obtenir les énoncés indiqués plus haut (§1.8).

Les résultats de cette section avaient été obtenus il y a une vingtaine d'années. Je les avais exposés à diverses occasions, mais je n'en avais jamais publié les démonstrations. Le présent séminaire me donne l'occasion de combler cette lacune. J'ai appris tout récemment que M. Tsfasman venait de rédiger un texte ([Ts 18]) qui couvre une partie des §§1.1 à 1.4.

Le §2 est consacré à la démonstration du théorème de Robinson, une démonstration très intéressante par les différents arguments qu'elle met en jeu : courbes hyperelliptiques, équation de Pell-Abel et polynômes de Chebyshev. Ce § doit beaucoup à l'aide que m'ont apportée J-F. Mestre et A. Bogatyrëv ; je les en remercie vivement.

L'Appendice rassemble quelques définitions et théorèmes standard sur les capacités, tirés principalement des ouvrages de Tsuji [Ts 59] et Ransford [Ra 95].

1. MESURES ASSOCIÉES AUX ENTIERS ALGÉBRIQUES

1.1. Mesures

Les mesures considérées ici sont des mesures de Radon positives sur un espace compact métrisable K, au sens de [INT], chap. III [(1)]. En d'autres termes, ce sont les $\mathbf{R}$-formes linéaires $f \mapsto \mu(f)$ sur l'espace $C(K)$ des fonctions continues réelles f sur K telles que :

(1.1.1) $f \geqslant 0$ sur $K \Rightarrow \mu(f) \geqslant 0$.

On écrit souvent $\int_K f(x)\mu(x)$ ou $\int_K f\mu$, à la place de $\mu(f)$.

La *masse* d'une mesure μ est $\mu(1)$. La *mesure de Dirac* en un point z de K est notée δ_z ; on a $\delta_z(f) = f(z)$.

Nous aurons besoin plus loin d'intégrer des fonctions semi-continues supérieurement F sur K à valeurs dans $\mathbf{R} \cup \{-\infty\}$. Par définition (cf. [INT], chap. IV, §1, appliqué à $-F$ pour transformer « supérieurement » en « inférieurement ») cette intégrale est l'élément de $\mathbf{R} \cup \{-\infty\}$ donné par :

1. Le mode d'exposition de [INT] a été beaucoup critiqué, à la fois à l'intérieur et à l'extérieur de Bourbaki, notamment parce qu'il mêle deux structures différentes : topologie et intégration. Il a cependant l'avantage de s'appliquer parfaitement aux questions d'équipartition dont il est question ici, car ces questions relèvent justement à la fois de la topologie et de l'intégration. Le lecteur que cette question intéresse aura intérêt à lire l'introduction de [Go 03].

(1.1.2) $\int_K F\mu = \inf_{f \geqslant F} \int_K f\mu$,

où la borne inférieure porte sur les $f \in C(K)$ qui majorent F.

Par exemple, si F est la fonction caractéristique d'une partie fermée T de K, le nombre $\int_K F\mu$ est la mesure $\mu(T)$ de T pour μ. Quand $T = \{z\}$ est réduit à un point z, on écrit $\mu(z)$ à la place de $\mu(\{z\})$; c'est la *masse de* μ *en* z. Lorsque tous les points sont de masse nulle, on dit que μ est *diffuse* (« atomless »), cf. [INT], V.5.10.

Dans ce qui suit, nous munirons l'espace des mesures de la *topologie faible* (également appelée *topologie vague*, [INT], chap. III, §1.9) ; c'est celle de la convergence simple : une suite (μ_n) de mesures tend vers une mesure μ si $\mu_n(f) \to \mu(f)$ pour tout $f \in C(K)$. Si F est comme ci-dessus, $\int_K F\mu$ est une fonction semi-continue supérieurement de μ (puisque c'est une borne inférieure de fonctions continues), autrement dit, on a :

(1.1.3) $\int_K F\mu \geqslant \limsup \int_K F\mu_n$ si $\lim \mu_n = \mu$.

En particulier :

(1.1.4) $\int_K F\mu_n \geqslant 0$ pour tout $n \Rightarrow \int_K F\mu \geqslant 0$.

L'espace des mesures positives de masse 1 est compact pour la topologie faible, et métrisable, car c'est une partie fermée de la boule unité du dual de l'espace de Banach $C(K)$, qui est de type dénombrable, cf. [INT], III.1, cor. 3 à la prop. 15.

1.2. Entiers algébriques et mesures associées

À partir de maintenant, K est une partie compacte de $\mathbf{C}$. On va s'intéresser aux entiers algébriques $z \in \mathbf{C}$ dont tous les $\mathbf{Q}$-conjugués appartiennent à K, ce que l'on exprime en disant que z est « *totalement dans* K ».

De façon plus précise, notons Pol_K l'ensemble des polynômes unitaires de degré > 0, à coefficients dans $\mathbf{Z}$, dont toutes les racines appartiennent à K. Si P est un tel polynôme, de degré d et de racines $z_1, \ldots, z_d$, on lui associe la mesure δ_P sur K définie par :

(1.2.1) $\delta_P = \frac{1}{d}(\delta_{z_1} + \cdots + \delta_{z_d})$, i.e. $\delta_P(f) = \frac{1}{d}\sum f(z_i)$ pour tout $f \in C(K)$.

Notons $\mathbf{M}$ (ou $\mathbf{M}_K$ lorsque l'on veut préciser K) l'adhérence pour la topologie faible de la famille des mesures δ_P, où P parcourt Pol_K.

C'est la structure de $\mathbf{M}$ qui nous intéresse. On a tout d'abord :

Proposition 1.2.2. *L'espace* $\mathbf{M}$ *est convexe et compact.*

La compacité résulte de ce que $\mathbf{M}$ est une partie fermée de l'espace des mesures de masse 1 sur K, qui est compact. Pour la convexité, on observe que, si $P_1, \ldots, P_m$ appartiennent à Pol_K, il en est de même de leurs produits $P_1^{a_1} \cdots P_m^{a_m}$ avec $a_i \in \mathbf{N}$, et les δ_P correspondants sont denses dans le simplexe de sommets les δ_{P_i}.

Corollaire 1.2.3. *L'espace* $\mathbf{M}$ *est l'enveloppe convexe fermée de l'ensemble des* δ_P.

Notons Irr_K le sous-ensemble de Pol_K formé des polynômes irréductibles, et soit I_K l'ensemble des δ_P, $P \in \mathrm{Irr}_K$. Les éléments de I_K sont linéairement indépendants, et leur enveloppe convexe fermée est $\mathbf{M}$. Lorsque Irr_K est fini, cela donne la structure de $\mathbf{M}$: c'est le simplexe dont l'ensemble des sommets est I_K.

Supposons Irr_K infini. C'est un ensemble dénombrable. Numérotons ses éléments : $P_1, P_2, \ldots$ Pour tout $n \geqslant 1$, soit $\mathbf{M}_n$ l'enveloppe convexe fermée des $\delta_{P_i}, i \geqslant n$. On a :

(1.2.4) $\mathbf{M} = \mathbf{M}_1 \supset \mathbf{M}_2 \supset \cdots$

Posons :

(1.2.5) $\mathbf{M}_\infty = \bigcap_{n\geqslant 1} \mathbf{M}_n$.

C'est un convexe compact non vide ; il ne dépend pas de la numérotation des éléments de Irr_K.

Théorème 1.2.6. *Soit $\mu \in \mathbf{M}_\infty$, et soit $S = \mathrm{Supp}\,\mu$ son support. Alors* :

(1.2.7) *μ est diffuse* (cf. §1.1).

(1.2.8) *La capacité* $\mathrm{cap}(S)$ *de S est $\geqslant 1$; si elle est égale à 1, alors μ est la mesure d'équilibre de S.*

(1.2.9) *L'ensemble S est réduit au sens de A.4.7.*

(Pour tout ce qui concerne les capacités et les mesures d'équilibre, voir l'Appendice à la fin du texte ; les références à cet Appendice commencent par la lettre A.)

Corollaire 1.2.10 (Fekete-Szegő [FS 55]). *Si* $\mathrm{cap}(K) < 1$, *alors* Irr_K *est fini.*

La démonstration du th. 1.2.6 sera donnée au §1.4.4.

La structure de $\mathbf{M}$ se ramène à celle de $\mathbf{M}_\infty$ par le théorème suivant :

Théorème 1.2.11. *Soit $\mu \in \mathbf{M}$. Il existe une suite et une seule de nombres réels positifs $c_0, c_1, c_2, \ldots$ tels que $\sum_{i\geqslant 0} c_i = 1$, et que* :

(1.2.12) $\mu = \sum_{i\geqslant 1} c_i \delta_{P_i} + \nu$, *avec* $\nu \in c_0 \mathbf{M}_\infty$.

Rappelons que $P_1, P_2, \ldots$ sont les différents éléments de Irr_K, numérotés dans un ordre arbitraire.

La démonstration sera donnée au §1.4.5.

Corollaire 1.2.13. *Si $\mu \in \mathbf{M}$ n'est pas combinaison linéaire d'un nombre fini de δ_{P_i}, la capacité de* $\mathrm{Supp}\,\mu$ *est $\geqslant 1$.*

Si $\nu \neq 0$, cela résulte de (1.2.8) appliqué à $c_0^{-1}\nu$. Si $\nu = 0$, il y a une infinité de c_i qui sont non nuls, et $\mathrm{Supp}\,\mu$ contient les zéros des P_i correspondants ; d'après (1.2.8) appliqué à $\mathrm{Supp}\,\mu$, on a $\mathrm{cap}(\mathrm{Supp}\,\mu) \geqslant 1$.

Remarque. La somme infinie

(1.2.14) $\mu_{\mathrm{at}} = \sum_{i\geqslant 1} c_i \delta_{P_i}$

est une mesure *atomique* ([INT], III.1.3). La formule $\mu = \mu_{\mathrm{at}} + \nu$ donne la décomposition canonique de μ en partie atomique et partie diffuse, cf. [INT] V.5.10, prop. 15. Les th. 1.2.6 et 1.2.11 entraînent :

Théorème 1.2.15. *Soit $\mu \in \mathbf{M}$.*

(i) *$\mu \in \mathbf{M}_\infty \Longleftrightarrow \mu$ est diffuse.*

(ii) *La masse $\mu(z)$ de μ en un point $z \in K$ est 0 si z n'est pas un entier algébrique totalement dans K.*

(iii) *Si $z, z' \in K$ sont deux entiers algébriques conjugués, on a $\mu(z) = \mu(z')$.*

(iv) $\mu \in \mathbf{M}_\infty \Rightarrow \operatorname{Supp}\mu$ *est réduit.*

Remarque sur (ii). Cette propriété exprime une sorte d'*indépendance* des mesures δ_{P_i}, plus forte que la simple indépendance linéaire (le lemme 1.3.1 ci-dessous va dans la même direction). En général, l'enveloppe convexe fermée d'une suite de mesures discrètes contient bien d'autres mesures discrètes. Par exemple, sur $K = [0,1]$, l'enveloppe convexe fermée des mesures δ_z, avec $z \in \mathbf{Q} \cap K$, est l'ensemble de *toutes les mesures positives de masse* 1 *sur* K, y compris les mesures de Dirac en des points irrationnels.

1.3. Lemmes de positivité

Les démonstrations des théorèmes du §1.2 sont basées sur la positivité de certaines intégrales portant sur les mesures $\mu \in \mathbf{M}$, les fonctions intégrées étant du type $z \mapsto \log|Q(z)|$, où Q est un polynôme [2] à coefficients dans $\mathbf{Z}$. Noter que, lorsque $Q(z) = 0$, on a $\log|Q(z)| = -\infty$; ainsi $\log|Q|$ est une fonction continue sur K à valeurs dans $\mathbf{R} \cup \{-\infty\}$, et on peut lui appliquer le §1.1.2, ce qui donne un sens aux intégrales de type $\mu(\log|Q|)$.

Lemme 1.3.1. *Soit* $P \in \mathrm{Pol}_K$ *et soit* $Q \in \mathbf{Z}[X]$, $Q \neq 0$.

On a $\delta_P(\log|Q|) = -\infty$ *si* P *et* Q *ont une racine commune, et* $\delta_P(\log|Q|) \geqslant 0$ *sinon.*

Démonstration. Soit d le degré de P et soient $z_1, \ldots, z_d$ ses racines. On a

$$\delta_P(\log|Q|) = \tfrac{1}{d}\textstyle\sum \log|Q(z_i)| = \tfrac{1}{d}\log|\prod Q(z_i)| = \tfrac{1}{d}\log|R|, \tag{1.3.2}$$

où R est le résultant de P et Q ([A IV], §6.6). Comme R est un entier, on a $\log|R| \geqslant 0$ si $R \neq 0$ et $\log|R| = -\infty$ si $R = 0$. D'où (1.3.1), puisque $R = 0$ si et seulement si P et Q ont une racine commune.

Lemme 1.3.3. *Soit* $\mu \in \mathbf{M}_n$, $n \geqslant 1$, *et soit* $Q \in \mathbf{Z}[X]$, $Q \neq 0$. *Supposons que* Q *ne soit divisible par aucun* P_i, $i \geqslant n$. *On a alors* $\mu(\log|Q|) \geqslant 0$.

Démonstration. Lorsque μ est combinaison linéaire finie des $\delta_{P_i}, i \geqslant n$, la positivité de $\mu(\log|Q|)$ résulte de (1.3.1). Le cas général s'en déduit par passage à la limite en utilisant (1.1.4).

Lemme 1.3.4. *On a* $\mu(\log|Q|) \geqslant 0$ *si* $\mu \in \mathbf{M}_\infty$ *et* $Q \in \mathbf{Z}[X], Q \neq 0$.

Cela résulte du lemme précédent, appliqué en prenant n assez grand.

Nous allons maintenant nous occuper d'intégrales doubles (il y a des énoncés analogues pour les intégrales triples, etc. — nous n'en aurons pas besoin).

Lemme 1.3.5. *Soit* μ *une mesure positive sur* K, *soit* $z \in K$, *et soit* $F(x,y)$ *une fonction semi-continue supérieurement sur* $K \times K$, *à valeurs dans* $\mathbf{R} \cup \{-\infty\}$. *On a :*

$$\textstyle\iint_{K\times K} F(x,y)\ \delta_z(x)\mu(y) \;=\; \int_K F(z,y)\ \mu(y). \tag{1.3.6}$$

Démonstration. Lorsque F est continue à valeurs dans $\mathbf{R}$, la formule (1.3.6) est une forme élémentaire du théorème de Lebesgue-Fubini : on la démontre en se ramenant au

2. L'utilisation d'intégrales $\int \log|Q(z)|\mu(z)$ est une technique standard depuis l'application que C. Smyth en a faite pour l'estimation des traces des entiers algébriques totalement positifs, cf. [Sm 84].

cas où $F(x,y)$ est de la forme $f(x)g(y)$. Pour passer de là au cas général, écrivons F comme la borne inférieure d'un ensemble filtrant décroissant $\mathcal{H}$ de fonctions continues $H(x,y)$ à valeurs dans $\mathbf{R}$; lorsque H parcourt $\mathcal{H}$, les fonctions $y \mapsto H(z,y)$ ont pour borne inférieure la fonction $y \mapsto F(z,y)$. On conclut alors par :

$\iint_{K\times K} F(x,y)\delta_z(x)\mu(y) = \inf_{H\in\mathcal{H}} \iint_{K\times K} H(x,y)\ \delta_z(x)\mu(y)$

(par définition)

$$= \inf_{H\in\mathcal{H}} \int_K H(z,y)\mu(y)$$

(puisque H est continue, cf. ci-dessus)

$$= \int_K F(z,y)\mu(y)$$

(d'après le th. 1 de [INT], chap. IV, §1, appliqué à $y \mapsto -F(z,y) + C$, où $C \geqslant \sup_{y\in X} F(z,y)$ — le signe « moins » et la constante C sont dus au fait que Bourbaki traite le cas des fonctions semi-continues inférieurement, à valeurs positives).

Lemme 1.3.7. *Soient $\mu, \nu \in \mathbf{M}_\infty$, et soit $Q \in \mathbf{Z}[X,Y]$, $Q \neq 0$. On a :*

(1.3.8) $\quad \iint_{K\times K} \log|Q(x,y)|\ \mu(x)\nu(y) \geqslant 0.$

Démonstration. Notons $I(\mu,\nu)$ le membre de gauche de (1.3.8). Il a un sens pour tout couple de mesures μ, ν sur K.

Choisissons le couple (δ_P, ν), avec $P \in \mathrm{Irr}_K$; soit d le degré de P, et soient $z_1, \ldots, z_d$ ses racines. Supposons que $P(X)$ ne divise pas $Q(X,Y)$, i.e. que les polynômes $Q(z_i,Y)$ soient $\neq 0$, et posons $H_P(Y) = \prod Q(z_i,Y)$; c'est un polynôme en Y, non nul, et à coefficients entiers. On a :

$$\begin{aligned} I(\delta_P,\nu) &= \iint_{K\times K} \log|Q(x,y)|\ \delta_P(x)\nu(y). \\ &= \tfrac{1}{d}\sum \iint_{K\times K} \log|Q(x,y)|\ \delta_{z_i}(x)\nu(y), \\ &= \tfrac{1}{d}\sum \int_K \log|Q(z_i,y)|\ \nu(y), \text{ d'après (1.3.6)}, \\ &= \tfrac{1}{d}\int_K \log|H_P(y)|\ \nu(y)\ \geqslant 0, \text{ d'après le lemme 1.3.4.} \end{aligned}$$

On déduit de là que $I(\delta_P,\nu) \geqslant 0$ pour tous les $P \in \mathrm{Irr}_K$, sauf ceux qui divisent $Q(X,Y)$. Par combinaisons linéaires et passages à la limite, on en déduit le même résultat pour $I(\mu,\nu)$, avec $\mu \in \mathbf{M}_n$ pour n assez grand. D'où (1.3.8), sous une forme un peu plus précise :

(1.3.9) $\ I(\mu,\nu) \ \geqslant 0$ *si* $\nu \in \mathbf{M}_\infty$ *et* $\mu \in \mathbf{M}_n$ *et si aucun des* $P_i(X), i \geqslant n$, *ne divise* $Q(X,Y)$.

Le cas particulier le plus utile de (1.3.8) est celui où $Q = X - Y$:

Corollaire 1.3.10. *Si $\mu, \nu \in \mathbf{M}_\infty$, on a $\iint_{K\times K} \log|x-y|\mu(x)\nu(y) \geqslant 0$.*

1.4. Démonstration du th. 1.2.6 et du th. 1.2.10

L'énoncé suivant est un cas élémentaire du théorème de décomposition des mesures en partie atomique et partie diffuse ([INT], V.5.10, prop. 15) :

Proposition 1.4.1. *Soit μ une mesure positive sur K, et soit c sa masse en un point $z \in K$. Alors la mesure $\mu - c\delta_z$ est positive.*

Démonstration. Soit f une fonction continue positive sur K. Il nous faut prouver que $\mu(f) \geqslant cf(z)$. Si $f(z) = 1$, cela résulte de la définition de c rappelée au §1.1. Le cas général en résulte par homogénéité.

Corollaire 1.4.2. *Soient μ, z, c comme ci-dessus, avec $c > 0$. Soit F une fonction semi-continue supérieurement sur K, à valeurs dans $\mathbf{R} \cup \{-\infty\}$, et telle que $F(z) = -\infty$. Alors $\mu(F) = -\infty$.*

Démonstration. D'après la prop. 1.4.1, on a $\mu = c\delta_z + \nu$, où ν est une mesure positive ; ainsi, $\nu(F)$ a un sens. On a $\mu(F) = cF(z) + \nu(F) = -\infty + \nu(F) = -\infty$.
[Rappelons que $-\infty + x = -\infty$ pour tout $x \in \mathbf{R} \cup \{-\infty\}$.]

Corollaire 1.4.3. *Si $\mu \in \mathbf{M}_n, n \geqslant 1$, on a $\mu(z) = 0$ pour toute racine z de l'un des polynômes P_i, $i < n$.*

Démonstration. Si l'on avait $\mu(z) > 0$ avec $P_i(z) = 0$ et $i < n$, on aurait $\mu(\log|P_i|) = -\infty$ d'après le cor. 1.4.2, ce qui contredirait le lemme 1.3.3, appliqué à $Q = P_i$.

On va maintenant s'occuper des démonstrations des énoncés du §1.2.

1.4.4. *Démonstration du th. 1.2.6.* Soit $\mu \in \mathbf{M}_\infty$. Si μ avait une masse non nulle en un point $z \in K$, la mesure $\mu \otimes \mu$ aurait une masse non nulle au point (z, z) de $K \times K$; comme la fonction $\log|x - y|$ vaut $-\infty$ en (z, z), le cor. 1.4.2 montrerait que l'intégrale $I(\mu) = \iint_{K\times K} \log|x - y|\mu(x)\mu(y)$ est égale à $-\infty$, ce qui contredirait le cor. 1.3.10, qui dit que $I(\mu) \geqslant 0$. La mesure μ est donc diffuse.

Si S est son support, la positivité de $I(\mu)$ et la caractérisation (A.3.2) de $\operatorname{cap} S$ montrent que $\operatorname{cap}(S) \geqslant 1$; le fait que S soit réduit résulte du cor. A.4.9. Si $\operatorname{cap}(S) = 1$, alors $I(\mu) = 0$ et μ est la mesure d'équilibre de S, vu l'unicité de celle-ci.

1.4.5. *Démonstration du th. 1.2.11.*

Commençons par un résultat partiel :

Proposition 1.4.6. *Soit $n > 0$ et soit $\mu \in \mathbf{M}$.*

(i) *Il existe une famille et une seule de nombres réels positifs $c_0, c_1, \ldots, c_{n-1}$, avec $\sum_{i\geqslant 0} c_i = 1$ telle que $\mu - \sum_{i>0} c_i\delta_{P_i} \in c_0\mathbf{M}_n$.*

(ii) *Soit i tel que $0 < i < n$, et soit $d_i = \deg P_i$. On a $c_i = d_i\mu(z)$ pour toute racine z de P_i.*

Démonstration. Le sous-espace de $\mathbf{M}$ formé des mesures de la forme :

$$c_1\delta_{P_1} + \cdots + c_{n-1}\delta_{P_{n-1}} + c_0\nu, \text{ avec } c_i \geqslant 0,\ \textstyle\sum_{0\leqslant i<n} c_i = 1,\ \nu \in \mathbf{M}_n,$$

est une partie convexe de $\mathbf{M}$ qui est fermée (car image d'un compact) et qui contient tous les $\delta_P, P \in \operatorname{Irr}_K$. C'est donc $\mathbf{M}$, ce qui démontre la partie « existence » de (i).

Si μ est de la forme $c_1\delta_{P_1} + \cdots + c_{n-1}\delta_{P_{n-1}} + c_0\nu$ comme ci-dessus, et si z est l'une des racines de l'un des P_i, on a $\delta_{P_j}(z) = 0$ pour $j \neq i$, $\delta_{P_i}(z) = 1/d_i$ et $\nu(z) = 0$, cf. cor. 1.4.3. D'où (ii) ; l'assertion d'unicité de (i) en résulte.

Corollaire 1.4.7. *Si $\mu \in \mathbf{M}$, on a $\mu \in \mathbf{M}_n$ si et seulement si $\mu(z) = 0$ pour toute racine z de $P_1 \cdots P_{n-1}$.*

Fin de la démonstration du théorème 1.2.11.

Soit $\mu \in \mathbf{M}$. Pour tout $i > 0$, choisissons une racine z de P_i et posons $c_i = d_i\mu(z)$, où $d_i = \deg P_i$. Si $n > 1$, posons $\gamma_n = 1 - \sum_{i<n} c_i$. D'après la prop. 1.4.6, γ_n est $\geqslant 0$, et l'on a :

(1.4.8) $\mu = \sum_{i<n} c_i\delta_{P_i} + \nu_n, \quad \text{avec} \quad \nu_n \in \gamma_n\mathbf{M}_n.$

La série

(1.4.9) $\mu_{\text{at}} = \sum c_i\delta_{P_i}$

est convergente, non seulement pour la topologie faible, mais aussi pour la topologie forte (celle donnée par la norme de l'espace des mesures). Posons $\nu = \mu - \mu_{\text{at}}$. En comparant (1.4.8) et (1.4.9), on obtient :

(1.4.10) $\nu = \lim_{n\to\infty} \nu_n,$

la limite étant prise au sens de la topologie forte. C'est une mesure positive de masse $c_0 = 1 - \sum_i c_i = \lim \gamma_n$. Nous allons voir qu'elle appartient à $c_0\mathbf{M}_\infty$, ce qui démontrera la partie « existence » du th. 1.2.10 (la partie « unicité » résulte de la prop. 1.4.6). C'est clair si $c_0 = 0$, car cela implique que la masse de ν est 0, donc que $\nu = 0$. Supposons $c_0 > 0$. On a

(1.4.11) $c_0^{-1}\nu = \lim_{n\to\infty} c_0^{-1}\nu_n.$

Les masses des mesures positives $(c_0^{-1} - \gamma_n^{-1})\nu_n$ tendent vers 0 pour $n \to \infty$. On peut donc récrire (1.4.11) sous la forme :

(1.4.12) $c_0^{-1}\nu = \lim_{n\to\infty} \gamma_n^{-1}\nu_n.$

On a $\gamma_n^{-1}\nu_n \in \mathbf{M}_n$. Pour tout entier m, on a donc $\gamma_n^{-1}\nu_n \in \mathbf{M}_m$ pour n assez grand, et (1.4.12) entraîne $c_0^{-1}\nu \in \mathbf{M}_m$. Comme ceci est vrai pour tout m, on a $c_0^{-1}\nu \in \mathbf{M}_\infty$, i.e. $\nu \in c_0\mathbf{M}_\infty$, ce qui termine la démonstration du th. 1.2.10.

1.5. Deux exemples : le cercle unité et l'intervalle $[-2, 2]$

Prenons pour K le cercle unité C_1, i.e. l'ensemble des $z \in \mathbf{C}$ de module 1. Les entiers algébriques totalement dans K sont les racines de l'unité, cf. [Kr 57]. Les éléments de Irr_K sont les polynômes cyclotomiques Φ_n, $n = 1, 2, \ldots$ La capacité de K est 1 ; d'après (1.2.8), cela montre que le seul élément de $\mathbf{M}_\infty$ est la mesure d'équilibre μ_K de K, qui n'est autre que la mesure de masse 1 invariante par rotation, autrement dit la mesure $\frac{1}{2\pi}d\varphi$, si l'on écrit les éléments de K comme $z = e^{i\varphi}$. D'après le th. 1.2.10, tout élément μ de $\mathbf{M}$ s'écrit de façon unique sous la forme

(1.5.1) $\mu = c_0\mu_K + \sum_{n=1}^{\infty} c_n\delta_{\Phi_n},$

où les c_i sont des nombres réels positifs tels que $\sum_{n=0}^{\infty} c_n = 1$.

On peut montrer que l'application $\mu \mapsto (c_n)_{n\geqslant 1}$ est un homéomorphisme de $\mathbf{M}$ sur le sous-espace du cube infini $[0,1]\times[0,1]\times\cdots$ formé des (c_n) tels que $\sum_{n\geqslant 1} c_n \leqslant 1$.

Noter que l'application $\mathbf{M}\to[0,1]$ donnée par $\mu\mapsto c_n$ est continue si $n>0$, mais ne l'est pas si $n=0$; la coordonnée c_0 ne joue pas le même rôle que les autres. D'ailleurs le sous-espace du cube infini formé des $(c_n)_{n\geqslant 0}$ de somme 1 n'est pas fermé.

Du cercle C_1 on passe à l'intervalle $I=[-2,2]$ par $z\mapsto z+\overline{z}$, cf. A.6. Les entiers algébriques totalement dans I sont les $z+\overline{z}$, où z est une racine de l'unité. On a une bijection naturelle des polynômes irréductibles correspondants, d'où aussi un isomorphisme de M_{C_1} sur M_I. L'unique élément de $\mathbf{M}_{\infty,I}$ est la mesure d'équilibre $\mu_I=\frac{1}{\pi}\frac{dx}{\sqrt{4-x^2}}$.

Remarque. Au lieu de prendre $K=I$, comme nous venons de le faire, on pourrait choisir pour K n'importe quel ensemble compact contenant I et s'intéresser à l'espace $\mathbf{M}_{K,I}$ formé des $\mu\in\mathbf{M}_K$ *dont le support est contenu dans* I. A priori, cet espace pourrait être strictement plus grand que $\mathbf{M}_I$ – cela se produit dans d'autres cas. Mais cela ne se produit pas ici : on a $\mathbf{M}_{K,I}=\mathbf{M}_I$; cela se voit en remarquant que, comme $\mathrm{cap}(I)=1$, la seule mesure diffuse de $\mathbf{M}_{K,I}$ est μ_I. Même chose pour le cercle C_1.

1.6. Les sous-ensembles de R et le théorème de Robinson

On suppose maintenant que K *est un intervalle fermé de* $\mathbf{R}$. Lorsque la longueur ℓ de K est <4, sa capacité est <1, et Irr_K est fini, cf. cor. 1.2.10. Lorsque $\ell=4$ et que les extrémités de K sont dans $\mathbf{Z}$, on se ramène par translation au cas $K=[-2,2]$ que l'on vient de traiter : l'ensemble Irr_K est infini, et $\mathbf{M}_\infty$ est réduit à un élément, la mesure d'équilibre de K. Lorsque $\ell=4$, et que les extrémités de K ne sont pas dans $\mathbf{Z}$, on ignore (autant que je sache) si Irr_K est fini ou infini.

Écartons ces cas, et *supposons* $\ell>4$. D'après Robinson ([Ro 62]), Irr_K est infini. Ce remarquable résultat a été généralisé deux ans plus tard par l'auteur lui-même ([Ro 64]) sous la forme suivante :

Théorème 1.6.1 (Robinson). *Soit E la réunion d'un ensemble fini d'intervalles de* $\mathbf{R}$. *Supposons* $\mathrm{cap}\,E>1$. *Alors* Irr_E *est infini.*
(Autrement dit, il existe une infinité d'entiers algébriques totalement dans E.)

La démonstration fera l'objet du §2.

Noter que ce résultat est l'analogue sur $\mathbf{R}$ d'un théorème de Fekete-Szegő ([FS 55]) sur $\mathbf{C}$:

(1.6.2) *Soit E un compact de* $\mathbf{C}$ *de capacité* $\geqslant 1$, *invariant par conjugaison. Pour tout voisinage U de E dans* $\mathbf{C}$, *il existe une infinité d'entiers algébriques qui sont totalement dans U.*

(Noter aussi que, si $E\subset\mathbf{R}$, les entiers algébriques en question ne sont pas nécessairement dans $\mathbf{R}$; ils en sont « arbitrairement voisins », ce qui n'est pas suffisant pour ce qui nous intéresse.)

Nous allons maintenant donner deux applications du th. 1.6.1 aux mesures $\mu \in \mathbf{M} = \mathbf{M}_K$. Tout d'abord :

Théorème 1.6.3. *Soit E une partie compacte de K de capacité* 1, *et soit μ_E sa mesure d'équilibre. On a $\mu_E \in \mathbf{M}_\infty$.*

[Rappelons que K est un intervalle de longueur > 4, donc de capacité > 1.]

Démonstration. Si $n > 0$, notons E_n l'ensemble des points de K dont la distance à E est $\leqslant 1/n$. On a $E \neq K$, donc E_n est distinct de E. On a $\operatorname{cap} E_n > 1$; sinon, d'après la prop. A.4.1, on aurait $\operatorname{cap}(E_n - E) = 0$, ce qui est impossible car $E_n - E$ contient un intervalle non vide. D'autre part, E_n est une réunion finie d'intervalles (et même d'intervalles de longueur $\geqslant 1/n$). D'après le th. 1.6.1, Irr_{E_n} est infini. Il existe donc une mesure $\mu_n \in \mathbf{M}_\infty$ dont le support est contenu dans E_n. Une sous-suite des μ_n converge vers une mesure $\mu \in \mathbf{M}_\infty$; le support E' de μ est contenu dans E, donc de capacité $\leqslant 1$. D'après (1.2.8), cela entraîne $\operatorname{cap}(E') = 1$ et $\mu = \mu_{E'}$. Comme $I(\mu) = 0$ (cf. (A.3.1) pour la définition de $I(\mu)$), on a $\mu = \mu_E$, d'où $\mu_E \in \mathbf{M}_\infty$.

Exemple. Ceci s'applique notamment aux intervalles de longueur 4 contenus dans K : les mesures d'équilibre correspondantes appartiennent à $\mathbf{M}_\infty$.

Le théorème suivant décrit la structure des supports des mesures $\mu \in \mathbf{M}_\infty$:

Théorème 1.6.4. *Soit S un compact de K. Pour que S soit le support d'une mesure appartenant à $\mathbf{M}_\infty$, il faut et il suffit que les deux conditions suivantes soient satisfaites* :

(i) $\operatorname{cap}(S) \geqslant 1$.

(ii) *S est réduit, au sens de* A.4.7.

Démonstration. La nécessité des conditions (i) et (ii) a déjà été démontrée (th. 1.2.6). Reste à voir la suffisance. Prouvons d'abord :

Lemme 1.6.5. *La condition* (i) *entraîne que S est réunion finie de sous-espaces compacts de capacité 1.*

Démonstration du lemme. Par compacité, il suffit de montrer que tout point $s \in S$ est contenu dans l'intérieur d'une partie compacte de S de capacité 1. Si t est un nombre réel $\geqslant 0$, notons S_t l'ensemble des points $z \in S$ tels que $|z - s| \leqslant t$, et posons $f(t) = \operatorname{cap}(S_t)$.

La fonction f est continue. En effet :

Elle est *continue à droite* ; sinon, il existerait $t_0 \geqslant 0$ et $c > 0$ tel que $f(t) \geqslant f(t_0) + c$ pour tout $t > t_0$; cela contredirait (A.5.2), appliqué à la suite des compacts $S_{t_0+1/n}$.

Elle est *continue à gauche* ; sinon, il existerait $t_1 > 0$ et $c > 0$ tel que $f(t) \leqslant f(t_1) - c$ pour tout $t < t_1$. La capacité de l'ouvert B réunion des S_t pour $t < t_1$ serait strictement plus petite que celle de S_{t_1}, ce qui contredirait (A.5.4), puisque $S_{t_1} - B$ a au plus deux éléments, donc est de capacité 0.

D'autre part f est croissante et l'on a $f(0) = 0$, et $f(t) = \operatorname{cap}(S) \geqslant 1$ pour t assez grand. Il existe donc une valeur de t pour laquelle $f(t) = 1$. L'ensemble S_t répond à la question.

Fin de la démonstration du th. 1.6.4. D'après le lemme, on a $S = \cup_{i=1}^m E_i$, où les E_i sont de capacité 1. Soit μ_i la mesure d'équilibre de E_i, et soit $\mu = \frac{1}{m} \sum \mu_i$. D'après

le th. 1.6.3, on a $\mu_i \in \mathbf{M}_\infty$ pour tout i, donc aussi $\mu \in \mathbf{M}_\infty$. Soit $S_i = \operatorname{Supp} \mu_i$, et soit $S' = \operatorname{Supp} \mu = \cup S_i$. D'après le cor. A.4.6, les $E_i - S_i$ sont de capacité 0 ; il en est donc de même de leur réunion ([Ra 95], th. 3.2.3 — cela résulte aussi de (A.5.4)) ; comme $S - S'$ est contenu dans cette réunion, il est aussi de capacité 0. La prop. A.4.1 entraîne alors que S' contient $\operatorname{Supp}(\mu_S)$, qui est égal à S puisque S est réduit. On a donc $S = S' = \operatorname{Supp}(\mu)$.

Un exemple.

Soit *E l'ensemble triadique de Cantor* dans $[0, 1]$: ensemble des $\sum_{n=1}^{\infty} \varepsilon_n 3^{-n}$, avec $\varepsilon_n \in \{0, 2\}$. Soit $\gamma = \operatorname{cap}(E)$. D'après [RR 07] et [LSN 17], il est vraisemblable que $\gamma = 0,22094\ldots$ [On trouvera dans [Ro 64], §2 et [Ra 95], th. 5.3.7, une démonstration simple du fait que γ est > 0, et même qu'il est $\geqslant 1/9$.]

L'ensemble E est réduit. Cela résulte de la prop. A.4.8 ; en effet, tout ouvert non vide de E contient un sous-ensemble déduit de E par homothétie par une puissance de $1/3$ suivie d'une translation ; un tel ouvert n'est donc pas de capacité 0.

Ainsi, on peut appliquer le th. 1.6.4 à un multiple λE de E, avec $\lambda > 1/\gamma$, par exemple $\lambda > 9$. Le compact K contient un tel sous-espace si sa longueur est assez grande.

L'intérêt de cet exemple est que la mesure $\mu \in \mathbf{M}_\infty$ ainsi obtenue *a un support qui est de mesure* 0 *pour la mesure de Lebesgue dx* ; ainsi, μ et dx sont des mesures *étrangères*, au sens de [INT], chap. V, §5.7 ; en particulier, μ n'est de la forme $\varphi(x)dx$ pour aucune fonction intégrable φ sur K.

Problèmes

On aimerait avoir davantage de renseignements sur les mesures qui appartiennent à $\mathbf{M}_\infty$. Par exemple :

(1.6.6) Les mesures données par le th. 1.6.3 (autrement dit, celles de support de capacité 1) sont des *points extrémaux* de $\mathbf{M}_\infty$. Y en a-t-il d'autres ?

Si ce sont les seules, alors, par un théorème de Choquet ([INT], chap. IV, §7), on pourrait obtenir tout élément de $\mathbf{M}_\infty$ à partir d'elles, en prenant des barycentres.

(1.6.7) Soit I un intervalle fermé, et soit ν_I sa mesure de Lebesgue (normalisée pour être de masse 1). Est-il possible que ν_I appartienne à $\mathbf{M}_\infty$?

1.7. Les sous-ensembles d'un cercle centré en 0

On suppose maintenant que K est *un cercle C de centre* 0 *et de rayon $r > 1$, avec* $r^2 \in \mathbf{N}$.

Le cas qui nous intéressera par la suite est celui où $r^2 = q$, avec $q = |\mathbf{F}|$, comme dans l'introduction. Pour le cas plus général où une puissance entière de r est dans $\mathbf{N}$, voir [Ro 69], §2.

Soit $I = [-2r, 2r]$. Si $z \in \mathbf{C}$, posons $f(z) = z + \overline{z}$. Nous obtenons ainsi une application continue surjective $f : C \to I$; si $a \in I$, l'image réciproque de a est formée des racines de l'équation $z^2 - az + r^2 = 0$ (on voit ainsi que, si a est un entier algébrique, il en est de même de z). Cette application va nous permettre *d'identifier les ensembles*

$\mathrm{Irr}_C, \mathbf{M}_C, \mathbf{M}_{C,\infty}$ *avec les ensembles correspondants pour* I. Cela provient des propriétés suivantes de f :

1.7.1. *Comportement vis-à-vis des mesures*

L'application $\mu \mapsto f(\mu)$ est un isomorphisme de l'espace des mesures sur C invariantes par conjugaison sur l'espace des mesures sur I.

1.7.2. *Comportement vis-à-vis de la capacité*

Si E est un compact de C stable par conjugaison, soit E_I son image par f. D'après la prop. A.6.1, on a :

(1.7.3) $\mathrm{cap}(E) = r^{1/2}\,\mathrm{cap}(E_I)^{1/2}$.

(1.7.4) Si $\mathrm{cap}(E) > 0$, l'image par f de la mesure d'équilibre μ_E est la mesure d'équilibre μ_{E_I}.

1.7.5. *Comportement vis-à-vis des entiers algébriques — cf.* [Ro 69], §2

Si $P \in \mathrm{Irr}_C$ il existe un unique $P_I \in \mathrm{Irr}_I$ dont les racines sont les images par f des racines de P, et l'on obtient ainsi une bijection $\mathrm{Irr}_C \to \mathrm{Irr}_I$. On a $\deg P_I = \frac{1}{2}\deg P$, sauf lorsque r est entier et $P(X) = X \pm r$ auquel cas $P_I(X) = X \pm 2r$. De plus, on a :

(1.7.6) $f(\delta_P) = \delta_{P_I}$.

Ces propriétés entraînent :

Proposition 1.7.7. *L'application* $\mu \mapsto f(\mu)$ *définit un isomorphisme de* $\mathbf{M}_C$ *sur* $\mathbf{M}_I$ *qui transforme* $\mathbf{M}_{C,\infty}$ *en* $\mathbf{M}_{I,\infty}$.

En appliquant à I les théorèmes 1.6.4 et 1.6.3, on obtient :

Théorème 1.7.8. *Soit* E *une partie fermée de* C *invariante par conjugaison.*

(i) *Pour que* E *soit le support d'une mesure appartenant à* $\mathbf{M}_{C,\infty}$*, il faut et il suffit que* E *soit réduit et* $\mathrm{cap}(E) \geqslant r^{1/2}$.

(ii) *Il existe des ensembles* E *satisfaisant à* (i) *de mesure de Lebesgue* 0.

(iii) *Si* $\mathrm{cap}(E) = r^{1/2}$*, on a* $\mu_E \in \mathbf{M}_{C,\infty}$.

[Noter le remplacement de 1 par $r^{1/2}$, dû à (1.7.3).]

1.8. Application aux variétés abéliennes

Comme on l'a dit dans l'introduction, à toute variété abélienne $A \neq 0$ sur un corps $\mathbf{F}$ à q éléments, on associe le polynôme caractéristique P_A de son endomorphisme de Frobenius. Ses valeurs propres se trouvent sur le cercle C de centre 0 et de rayon $r = q^{1/2}$.

Lemme 1.8.1. *Soit* $P \in \mathrm{Irr}_C$*. Il existe un entier* $m > 0$ *et une variété abélienne* A *sur* $\mathbf{F}$ *tels que* $P_A = P^m$.

Cela résulte du théorème de Honda-Tate, cf. [Ta 69], §1, Remarque 2.

Comme $\delta_{P^m} = \delta_P$, on déduit de là :

Proposition 1.8.2. *L'enveloppe convexe fermée* $\mathbf{M}^{\mathrm{ab}}$ *des* δ_A *est égale à* $\mathbf{M}_C$.

On peut donc appliquer à $\mathbf{M}^{\mathrm{ab}}$ les résultats du § précédent ; noter que $r^{1/2}$ est ici $q^{1/4}$; la capacité du support d'une mesure appartenant à $\mathbf{M}_\infty^{\mathrm{ab}}$ est donc $\geqslant q^{1/4}$.

À titre de curiosité, voici un exemple de mesure appartenant à $\mathbf{M}_\infty^{\mathrm{ab}}$: on choisit un intervalle $I = [a, b]$, contenu dans $[-q^{1/2}, q^{1/2}]$ et de longueur 2 ; soit C_I l'ensemble des points $z = x + iy \in C$ tels que $x \in I$. Il résulte de (1.7.3) que $\mathrm{cap}(C_I) = q^{1/4}$, de sorte que la mesure d'équilibre μ de C_I appartient à $\mathbf{M}_\infty^{\mathrm{ab}}$ d'après le th. 1.7.8. Sur la « moitié supérieure » de C_I (celle où $y \geqslant 0$), on a $\mu = \frac{1}{2\pi} \frac{dx}{\sqrt{(b-x)(x-a)}}$; idem pour l'autre moitié.

2. DÉMONSTRATION DU THÉORÈME DE ROBINSON

2.1. Résumé de la démonstration

Il s'agit de démontrer le th. 1.6.1. On se donne des nombres réels

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

en nombre $2g + 2, g \geqslant 0$. Pour chaque $j = 0, \ldots, g$, soit $E_j = [a_j, b_j]$ et soit $E = \cup_j E_j$. On doit prouver que, si $\mathrm{cap}(E) > 1$, il existe une infinité d'entiers algébriques qui sont totalement contenus dans E.

La méthode est la suivante :

On commence par traiter un cas particulier, celui que nous appellerons *de Pell-Abel*, cf. §2.2 ; dans ce cas, on verra au §2.4 qu'il existe, pour un certain entier $r \geqslant 1$, un polynôme unitaire $P(x)$ de degré r, à coefficients réels, dont les racines sont distinctes et appartiennent à E ; de plus, sur chaque E_j, ce polynôme oscille entre $-M$ et M (avec $M > 0$) de façon analogue à celle des polynômes de Chebyshev usuels sur $[-2, 2]$. On a $\mathrm{cap}(E) = M/2$, de sorte que $M > 2$.

L'étape suivante consiste à rétrécir E et à modifier P, arbitrairement peu, de telle sorte que l'on ait encore $\mathrm{cap}(E) > 1$, et que les coefficients de P soient rationnels (§2.6) ; de là, on parvient à un polynôme à coefficients *entiers*, dont les racines sont dans E (§2.7) ; on obtient ainsi des polynômes de degré arbitrairement grands, ce qui démontre le th. 1.6.1 dans le cas considéré. Il reste à ramener le cas général à celui-là en prouvant que, en rétrécissant arbitrairement peu E, il devient du type de Pell-Abel (§2.8).

La démonstration résumée ci-dessus est essentiellement celle de Robinson ([Ro 64]). Il en existe une autre, due à R. Rumely, qui est plus longue, mais qui donne un résultat plus général : elle s'applique à des courbes algébriques de genre quelconque et elle permet d'imposer aux points rationnels de ces courbes des conditions, non seulement archimédiennes, mais aussi p-adiques. Je renvoie à [Ru 13] pour les énoncés (voir notamment, Introduction, th. 0.4 et App.B, th.B.18), ainsi que pour l'historique du sujet, et notamment le rôle de D. Cantor ([Ca 69], [Ca 80]), qui a été le premier à donner des énoncés de ce type.

2.2. Courbes hyperelliptiques et équation de Pell-Abel

Soit k un corps de caractéristique $\neq 2$, et soit $D(x) \in k[x]$ un polynôme unitaire de discriminant $\neq 0$, et de degré pair $2g+2, g \geqslant 0$. L'équation $y^2 = D(x)$ définit une courbe hyperelliptique affine C_D^{aff} de genre g ; sa complétée C_D s'obtient en lui ajoutant deux points à l'infini, que nous noterons ∞_+ et ∞_- ; ils sont caractérisés par le fait que y/x^{g+1} prend la valeur 1 au premier et -1 au second.

L'algèbre affine de C_D^{aff} est un $k[x]$-module libre de base $\{1, y\}$. Ses éléments inversibles sont de la forme :

(2.2.1) $f = P + yQ$, avec $P, Q \in k[x]$ et $P^2 - DQ^2 = c$, avec $c \in k^\times$.

On supposera que P et Q sont non nuls (cela revient à éliminer le cas $f \in k^\times$), et on les normalisera en demandant que ce soient des polynômes unitaires. On appellera *degré* de f le degré de P. L'équation $P^2 - DQ^2 = c$ est l'analogue pour $k[x]$ de l'équation dite « de Pell » pour $\mathbf{Z}$. Il est raisonnable de l'appeler *l'équation de Pell-Abel*, car elle apparaît pour la première fois dans Abel ([Ab 26]) où elle est étudiée à l'aide de fractions continues, comme dans le cas de $\mathbf{Z}$.

On trouve aussi dans la littérature le nom d'*équation d'Abel-Chebyshev* : elle avait en effet été retrouvée, et utilisée, par Chebyshev ([Ch 54]), à propos d'un problème de mécanique [3].

Une différence importante avec l'équation usuelle de Pell est que *l'équation de Pell-Abel n'a pas toujours de solution.*

De façon plus précise, soit r un entier $\geqslant 1$. Il y a équivalence entre :

(2.2.2) *L'équation (2.2.1) a une solution de degré r.*

(2.2.3) *Le diviseur $r(\infty_- - \infty_+)$ de la courbe C_D est linéairement équivalent à 0.*

[C'est immédiat : il suffit de vérifier qu'une fonction rationnelle f sur C_D de diviseur $r(\infty_- - \infty_+)$ est nécessairement de la forme $f = P + yQ$, comme dans (2.2.1).]

On peut reformuler (2.2.3) de la manière suivante : si J désigne la jacobienne de C_D, le diviseur $\infty_- - \infty_+$ définit un point P_∞ de $J(k)$, et (2.2.3) signifie que $rP_\infty = 0$, autrement dit que P_∞ est un point d'ordre fini divisant r. Lorsque $g = 0$, c'est le cas car $J = 0$, et l'on trouve pour P, Q les polynômes de Chebyshev usuels (de première et seconde espèce, respectivement), avec une normalisation un peu différente ; c'est aussi le cas (pour r bien choisi) lorsque $g \geqslant 1$ et k est un corps fini. Par contre, si $g \geqslant 1$ et si $\text{car}(k) = 0$, il est facile de construire des exemples où P_∞ est d'ordre infini, ce qui entraîne que l'équation de Pell-Abel n'a pas de solution.

3. Problème (important pour les constructeurs de locomotives) : comment utiliser certains quadrangles articulés (les *mécanismes de Chebyshev*) pour transformer aussi bien que possible un mouvement circulaire en un mouvement rectiligne, et inversement ? C'est en essayant d'optimiser le « aussi bien que possible » que Chebyshev a été conduit aux polynômes qui portent son nom, ainsi qu'à l'équation $P(x)^2 - D(x)Q(x)^2 = c$. Le lecteur curieux trouvera sur internet des reproductions (avec vidéo) de certains de ces mécanismes.

[Une autre façon de formuler ceci est d'introduire la *Jacobienne généralisée* $J_{\mathfrak{m}}$ de C_D relative au conducteur $\mathfrak{m} = \infty_- + \infty_+$. On a une suite exacte $1 \to \mathbf{G}_m \to J_{\mathfrak{m}} \to J \to 1$, qui montre que $J_{\mathfrak{m}}$ est une extension de J par le groupe multiplicatif $\mathbf{G}_m$; la classe de cette extension dans $\mathrm{Ext}(J, \mathbf{G}_m) \simeq J(k)$ est P_∞, au signe près. Dire que P_∞ est d'ordre fini signifie donc que $J_{\mathfrak{m}}$ *est isogène à* $J \times \mathbf{G}_m$, ou encore que le 1-motif mixte de la courbe C_D^{aff} est scindé.]

2.3. Le cas réel : la forme de troisième espèce canonique

Nous allons maintenant supposer que $k = \mathbf{R}$ et que le polynôme $D(x)$ a pour racines les a_j, b_j du §2.1 :

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

Ainsi $D(x)$ est $\leqslant 0$ si $x \in E$ et > 0 sinon. Les points réels de la courbe C_D correspondent donc aux $x \in \mathbf{P}_1(\mathbf{R}) - \overset{\circ}{E}$.

Soit $A \in \mathbf{R}[x]$ un polynôme unitaire de degré g ; on lui associe la forme différentielle $\eta_A = \frac{A(x)dx}{y}$ sur C_D. Cette forme est holomorphe ailleurs qu'en l'infini ; elle a un pôle simple en ∞_+ et ∞_-, avec résidus -1 et $+1$ respectivement ; c'est une « forme de 3-ème espèce ». Changer A revient à lui ajouter une forme de première espèce, puisque celles-ci ont pour base les $x^j dx/y, 0 \leqslant j < g$. On en déduit *qu'il existe un choix et un seul de* A *tel que les périodes réelles de* η_A *soient nulles*, autrement dit qui vérifie les conditions :

(2.3.2) $\int_{b_{j-1}}^{a_j} \frac{A(x)}{\sqrt{D(x)}}\, dx = 0$ pour $j = 1, \ldots, g$.

[Dans cette formule, ainsi que dans les suivantes, si t est réel $\geqslant 0$, nous notons $\sqrt{t}$ sa racine carrée $\geqslant 0$; si $t < 0$, nous définissons $\sqrt{t}$ comme $i \cdot \sqrt{-t}$.]

Le polynôme A déterminé par ces conditions sera noté R, et la forme η_R sera appelée la *forme de 3-ème espèce canonique*, et notée simplement η. La formule (2.3.2), appliquée à R, montre que, dans chaque intervalle intermédiaire $T_j = [b_{j-1}, a_j]$, l'intégrale de $\frac{R(x)}{\sqrt{-D(x)}}$ est nulle ; cela entraîne que $R(x)$ change de signe dans T_j, donc s'annule en au moins un point. Comme le nombre des j est égal au degré de R, on obtient :

(2.3.4) *Le polynôme* $R(x)$ *a une racine et une seule dans chaque* T_j*, et n'a aucune autre racine (réelle ou complexe).*

Les changements de signe de R se font donc dans les « trous » T_j. Cela montre que R garde un signe constant sur chaque E_j. Comme $R(x)$ est $\geqslant 0$ pour x assez grand, on en déduit, par récurrence descendante sur j :

(2.3.5) *On a* $R(x) \geqslant 0$ *sur* E_j *si* $g - j$ *est pair et* $R(x) \leqslant 0$ *sinon.*

On va maintenant s'intéresser aux « périodes imaginaires » de η, qui sont égales à $2\eta_j$, avec :

(2.3.6) $\eta_j = \int_{a_j}^{b_j} \frac{R(x)}{\sqrt{D(x)}}\, dx$, $j = 0, 1, \ldots, g$.

Leurs parties réelles sont nulles.

Proposition 2.3.7. *Il existe des signes* $\varepsilon_j \in \{-1, 1\}$ *tels que l'on ait :*

(2.3.8) $\sum_{0 \leqslant j \leqslant g} \varepsilon_j \eta_j = i\pi$.

Démonstration. Notons S la variété analytique complexe $C_D(\mathbf{C})$, vue comme une surface de Riemann au-dessus de $\mathbf{P}_1(\mathbf{C}) = \mathbf{C} \cup \{\infty\}$ via l'application $(x, y) \mapsto x$. C'est un revêtement quadratique, ramifié seulement aux points a_j, b_j. Ce revêtement est non ramifié (c'est un vrai revêtement, au sens de la Topologie) au-dessus de $U = \mathbf{P}_1(\mathbf{C}) - E$. Notons $\tilde{E}_j$ l'image réciproque de E_j dans S, et soit $\tilde{E}$ la réunion des $\tilde{E}_j$. L'image réciproque $\tilde{U}$ de U dans S est égale à $S - \tilde{E}$. Un calcul sur les groupes fondamentaux montre que *le revêtement $\tilde{U} \to U$ est trivial.*

[En termes plus traditionnels, cela signifie que l'on peut définir y comme une fonction méromorphe sur U, par prolongement analytique à partir de l'une de ses deux valeurs possibles en un point de U.]

Il en résulte que $\tilde{U}$ a deux composantes connexes ; nous noterons $\tilde{U}_+$ celle qui contient le point ∞_+ ; définition analogue pour $\tilde{U}_-$. L'adhérence S_+ de $\tilde{U}_+$ est $\tilde{U}_+ \cup \tilde{E}$; c'est une surface à bord (une « pièce », dit Bourbaki [FRV], 11.1.2), dont le bord est la réunion des $g+1$ cercles $\tilde{E}_j$. Si l'on définit de manière analogue S_-, on voit que S peut s'obtenir à partir de S_+ et S_- en collant leurs bords.

On notera que l'orientation naturelle de $\tilde{U}_+$ (comme variété analytique complexe) définit une orientation sur chacune des composantes $\tilde{E}_{j+}$ de son bord ; cela donne un sens à une intégrale du type $\int_{\tilde{E}_{j+}} \omega$. Lorsque ω est de première espèce, la formule de Cauchy [4] ([FRV], 11.2.5) donne :

$\sum_j \int_{\tilde{E}_{j+}} \omega = 0$.

Un argument analogue, appliqué à η et à $\tilde{U}_+$ dont on a retiré un petit disque autour de ∞_+, donne :

(2.3.9) $\sum_j \int_{\tilde{E}_{j+}} \eta = -2i\pi$,

du fait que le résidu de η au point ∞_+ est -1.

On passe de (2.3.9) à (2.3.8) en remarquant que, pour tout j, l'intégrale $\int_{\tilde{E}_{j+}} \eta$ est égale à $\pm 2\eta_j$, le signe « $\pm$ » provenant du fait que l'on n'essaie pas de préciser les orientations.

2.4. L'équation de Pell-Abel dans le cas du §2.3 – énoncé des résultats

On conserve les hypothèses du §2.3, et l'on suppose en outre que, pour un certain entier $r \geqslant 1$, il existe une solution (P, Q) de degré r de l'équation $P^2 - DQ^2 = c$, avec $c \in \mathbf{R}^\times$. La constante c est positive, car c'est le carré de la valeur de P en l'un quelconque des points a_j, b_j. Nous la noterons M^2, avec $M > 0$. On a donc :

(2.4.1) $P^2 - DQ^2 = M^2$.

Supposons x réel ; on a $D(x) \leqslant 0$ si et seulement si $x \in E$; cela entraîne :

(2.4.2) $|P(x)| \leqslant M \iff x \in E$ ou $Q(x) = 0$.

[En fait, le th. 2.4.4 ci-dessous entraîne que $Q(x) \neq 0$ si $x \notin E$. On peut donc supprimer « ou $Q(x) = 0$ » dans (2.4.2).]

4. Cas particulier de la formule de Stokes en dimension 2.

De plus :

(2.4.3) $|P(x)| = M \iff$ x est, soit une racine de Q, soit l'un des a_j, b_j.

En ce qui concerne les racines des polynômes P, Q, la propriété la plus importante pour la suite est la partie (i) du théorème suivant :

Théorème 2.4.4. (i) *Les racines des polynômes P et Q sont réelles, simples, et appartiennent à E.*

(ii) *Soit $f = P + yQ$, cf. §2.2.1. On a $df/f = r\eta$, où η est la forme de troisième espèce canonique définie au §2.3.*

En fait, on aura besoin d'autres résultats, à savoir :

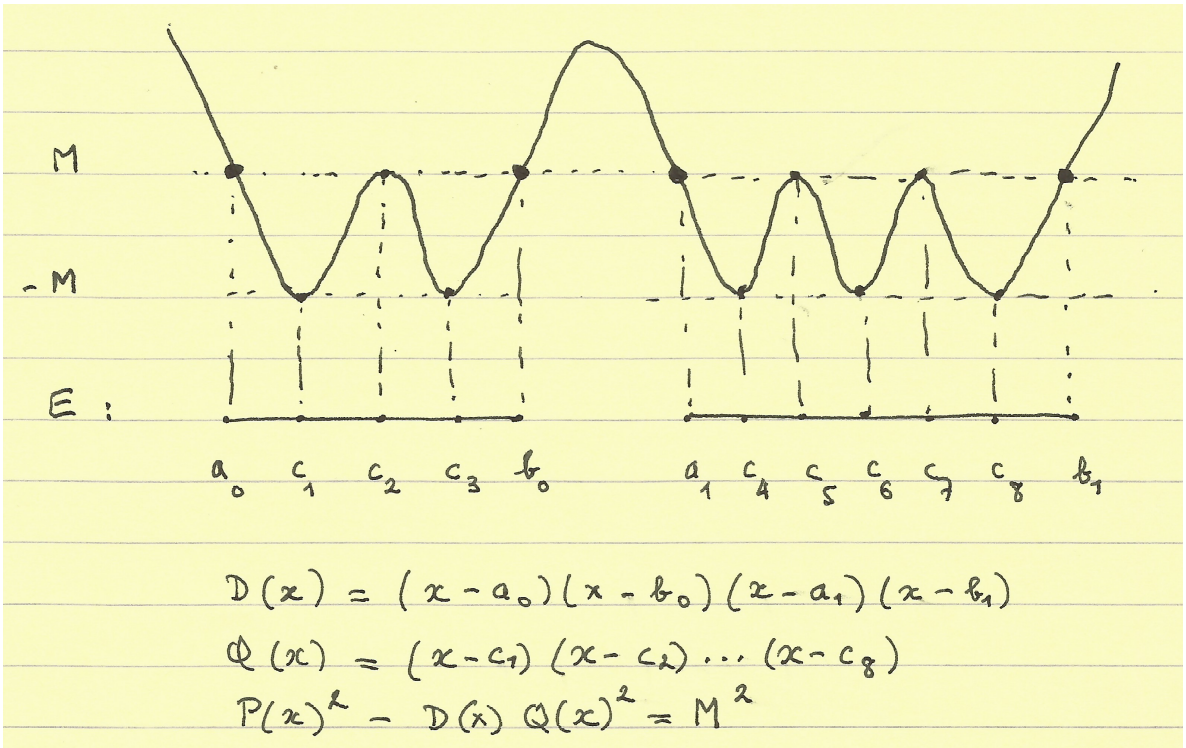
Théorème 2.4.5. *Pour $j = 0, \dots, g$, soit $r_j = r|\eta_j|/\pi$, où η_j est la j-ième demi-période imaginaire de η, cf. (2.3.6). Alors :*

(2.4.6) *Les r_j sont des entiers > 0, de somme r.*

(2.4.7) *Le nombre de racines de P dans E_j est r_j; le nombre de racines de Q dans l'intérieur de E_j est $r_j - 1$.*

(2.4.8) *Les racines de Q qui sont contenues dans l'intérieur de E_j divisent E_j en r_j sous-intervalles; dans chacun d'eux, le polynôme P est, soit strictement croissant, soit strictement décroissant, de valeurs extrêmes M et $-M$.*

La figure ci-dessous indique à quoi ressemble le graphe de P dans le cas où $g = 1, r_1 = 4, r_2 = 6, r = 10$, les racines de Q étant notées $c_1, \dots, c_8$. Les 10 sous-intervalles sont $[a_0, c_1], [c_1, c_2], \dots, [c_8, b_1]$.



Autres propriétés :

Théorème 2.4.9. (i) $dP/dx = rQ(x)R(x)$, *où* R *est le polynôme de degré* g *défini au §2.3.*

(ii) *Le polynôme* P *est le* r*-ième polynôme de Chebyshev* (au sens du §A.2) *du compact* E.

(iii) $\mathrm{cap}(E) = (M/2)^{1/r}$.

[Dans le cas de la figure ci-dessus, on a $R(x) = x - \gamma$, où γ est le point de $[b_0, a_1]$ où P est maximum.]

Les démonstrations des trois théorèmes ci-dessus sont données au §2.5 ci-dessous.

Remarque historique. Il n'est pas facile de dire à qui ces théorèmes sont dus. L'une des difficultés est qu'ils sont rarement énoncés explicitement, et, du coup, ils ne sont pas démontrés en détail. La plus ancienne référence que j'aie pu trouver est celle de Robinson [Ro 64]. Il y a eu ensuite Peherstorfer ([Pe 90]), Sodin-Yuditskii ([SY 92]), Bogatyrëv ([Bo 99] et [Bo 05]), et sans doute d'autres. Il est toutefois possible que l'école russe, descendante de Chebyshev et Zolotarëv, et en particulier N.I. Akhiezer, ait été familière avec ces résultats dès les années 1930.

2.5. Démonstrations des énoncés du §2.4

Démonstration du th. 2.4.4 (ii). Soit $f = P + yQ$; les seuls pôles de df/f sont les points ∞_+ et ∞_-, qui sont des pôles simples de résidus $-r$ et r respectivement. Pour prouver que $df/f = r\eta$, il nous suffit donc de prouver que les périodes réelles de df/f sont nulles.

Si $j = 1, \ldots, g$, choisissons une détermination de y sur l'intervalle $T_j = [b_{j-1}, a_j]$, par exemple $y(x) = \sqrt{D(x)}$; cela permet de voir f comme une fonction $f(x)$ sur T_j. Cette fonction est réelle, et ne s'annule pas ; comme $|f(b_{j-1})| = M = |f(a_j)|$, on en conclut que $f(b_{j-1}) = f(a_j) = \varepsilon M$, avec $\varepsilon = \pm 1$; le signe de f est donc ε sur T_j La fonction $\log(\varepsilon f)$ prend les mêmes valeurs aux extrémités de T_j. Cela entraîne que l'intégrale sur T_j de sa dérivée est 0 ; comme cette dérivée est df/f, cela signifie que la j-ième période réelle de df/f est nulle.

Remarque. Soit $\varphi(x) = \log(\varepsilon f(x)/M)$. On a $f(x) = \varepsilon M e^{\varphi(x)}$; si $f_1 = P - yQ$, le fait que $f_1 f = M^2$ montre que $f_1(x) = \varepsilon M e^{-\varphi(x)}$. Comme $P = (f + f_1)/2$ et $yQ = (f - f_1)/2$, cela donne :

(2.5.1) *On a* $P(x) = \varepsilon M \cosh(\varphi(x))$ *et* $y(x)Q(x) = \varepsilon M \sinh(\varphi(x))$ *si* $x \in T_j = [b_{j-1}, a_j]$.

Comme φ est une « primitive » de $df/f = rR(x)dx/y(x)$, on obtient donc une expression explicite de P et Q en termes de $R(x)$, lequel peut se calculer en résolvant un système linéaire d'équations de type $g \times g$.

Démonstration du th. 2.4.9 (i). Les formules (2.5.1) montrent que, sur T_j, on a :

$$\begin{aligned} dP(x) &= y(x)Q(x)d\varphi(x) \;=\; y(x)Q(x)df(x)/f(x) \\ &= ry(x)Q(x)R(x)dx/y(x) \;=\; rQ(x)R(x)dx. \end{aligned}$$

La formule $\frac{dP}{dx} = rQR$ du th. 2.4.9 (i) est donc vraie sur T_j, donc partout, puisque c'est une identité entre polynômes.

Démonstration du th. 2.4.5 et du th. 2.4.4 (i).

[La méthode est essentiellement la même que pour le th. 2.4.4 (ii), à cela près que le groupe multiplicatif $\mathbf{R}^\times$ est remplacé par le cercle unité C_1.]

Considérons l'un des intervalles E_j, $j = 0, \ldots, g$. Posons $y_1(x) = \sqrt{-D(x)}$, qui est à valeurs réelles $\geqslant 0$, et choisissons comme détermination de y la fonction $iy_1(x)$. Comme ci-dessus, on peut voir $f(x) = P(x) + iy_1(x)Q(x)$ comme une fonction sur E_j ; cette fonction est à valeurs complexes et de module M. On peut donc l'écrire sous la forme $f(x) = Me^{i\vartheta(x)}$, où $\vartheta(x)$ est bien défini mod 2π. On peut relever $\vartheta : E_j \to \mathbf{R}/2\pi\mathbf{Z}$ en une fonction continue $\theta : E_j \to \mathbf{R}$, qui est bien déterminée si on lui impose sa valeur en a_j ; comme $f(a_j) = \pm M$, cette valeur est de la forme $c_0\pi$, avec $c_0 \in \mathbf{Z}$; la valeur de f en b_j est alors $c_1\pi$ avec $c_1 \in \mathbf{Z}$. On a :

(2.5.2) $\quad P(x) = M\cos(\theta(x))$ et $y_1(x)Q(x) = M\sin(\theta(x))$.

De plus :

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

Soit $r_j = |c_1 - c_0|$; c'est un entier > 0. Comme $df/f = r\eta$, la formule ci-dessus montre que, au signe près, $r_j i\pi$ est la j-ième demi-période imaginaire de $r\eta$. On a donc $r_j = r|\eta_j|/\pi$, avec les notations de (2.3.3). D'après (2.3.5), il existe des signes $\pm$ tels que :

(2.5.3) $\quad \sum_j \pm r_j = r$.

Noter que la dérivée de $\theta(x)$ ne s'annule pas, donc $\theta(x)$ est strictement croissante (resp. décroissante) si $c_0 < c_1$ (resp. si $c_1 < c_0$). Or, si une variable croît strictement entre deux multiples entiers $u\pi$ et $v\pi$, son cosinus s'annule un nombre de fois égal à $v - u$, et son sinus s'annule $v - u - 1$ fois en dehors des extrémités. On en conclut que *le nombre de racines de P dans E_j est r_j et que le nombre analogue pour Q dans l'intérieur de E_j est $r_j - 1$*. Comme P a au plus r racines, on a donc :

(2.5.4) $\quad \sum_j r_j \leqslant r$.

En comparant (2.5.3) et (2.5.4), on voit que tous les signes de (2.5.3) sont des signes $+$, de sorte que l'on a $\sum r_j = r$, et l'on voit aussi que P n'a pas d'autres racines que celles qui sont dans les E_j et que celles-ci sont des racines simples (ce dernier point résulte aussi de la formule $dP/dx = rQR$ du th. 2.4.9 (i)). Le même argument montre que Q n'a pas d'autres racines que celles contenues dans l'intérieur de E. Cela achève la démonstration de 2.4.4 (i), (2.4.6) et (2.4.7). Pour (2.4.8), on remarque que, dans un sous-intervalle $[\alpha, \beta]$ du type de (2.4.8), la dérivée de P est $\neq 0$ en tout point x tel que $\alpha < x < \beta$: cela résulte de la formule $\frac{dP}{dx} = rQR$ et du fait que R ne s'annule pas sur les E_j, cf. (2.3.4).

Démonstration du th. 2.4.9 (ii) : P est un polynôme de Chebyshev.

On démontre d'abord :

Lemme 2.5.5. *Soit $q \in \mathbf{R}[x]$ tel que $|q(x)| < M$ pour tout $x \in E$. Le polynôme $P - q$ a au moins r racines dans E.*

Démonstration. Soit $[\alpha, \beta]$ un sous-intervalle de type (2.4.8) ; on a $P(\alpha) = -P(\beta) = \pm M$; l'hypothèse faite sur q entraîne que le polynôme $P-q$ a le même signe que P en α et en β ; il a donc au moins une racine dans l'intervalle ouvert $]\alpha, \beta[$; d'où le lemme, puisque le nombre des sous-intervalles est r.

Démonstration du th. 2.4.9 (ii).

Soit q le polynôme de Chebyshev de E de degré r ; le fait qu'il soit unique montre que ses coefficients sont réels. Si l'on avait $q \neq P$, on aurait $\sup_{x\in E} |q(x)| < M$. D'après le lemme ci-dessus, le polynôme $P - q$ a au moins r racines ; comme il est de degré $< r$, ce n'est possible que s'il est nul, ce qui contredit l'hypothèse faite sur q.

Démonstration du th. 2.4.9 (iii) : calcul de $\mathrm{cap}(E)$.

On a vu ci-dessus que, dans tout intervalle E_j, le polynôme P a r_j zéros. Le même argument montre, pour tout $z \in [-M, M]$, distinct de $\pm M$, l'équation $P(x) = z$ a r_j solutions dans E_j, donc n'a aucune solution dans $\mathbf{C} - E$ puisque $r = \sum r_j$; lorsque $z = \pm M$, cet énoncé est également vrai (il résulte par exemple de $P^2 - M^2 = DQ^2$). D'où :

(2.5.6) *L'image réciproque de $[-M, M]$ par $P : \mathbf{C} \to \mathbf{C}$ est E.*

Comme la capacité de $[-M, M]$ est $M/2$, la formule (A.5.7) montre que $\mathrm{cap}(E) = (M/2)^{1/r}$.

Autre démonstration : on verra au §2.7 que, pour tout entier $n > 0$, l'équation de Pell-Abel pour D, de degré rn, a une solution P_n, Q_n, M_n avec $M_n = M^n 2^{1-n}$. Avec les notations de (A.2), cela entraîne que $c_{rn}(E) = M_n$. D'après (A.2.1), on a :

$\mathrm{cap}(E) = \lim_{n\to\infty} c_{rn}(E)^{1/rn} = \lim_n (M_n)^{1/rn} = M^{1/r} \lim_n 2^{(1-n)/rn} = (M/2)^{1/r}$.

2.6. Comment remplacer les coefficients réels par des coefficients rationnels

On conserve les notations E, D, P, Q, r, M des §§ ci-dessus. On désire démontrer :

Proposition 2.6.1. *Pour tout M' tel que $0 < M' < M$ il existe E' et P' [5] tels que le sextuplet $E', D', P', 1, r, M'$ ait les mêmes propriétés que E, D, P, Q, r, M, et en outre :*

(2.6.2) *On a $P' \in \mathbf{Q}[x]$ et $E' \subset E$.*

[Autrement dit, on peut modifier P, sans augmenter E, et en diminuant M à volonté, de telle sorte que ses coefficients soient dans $\mathbf{Q}$.]

Démonstration.

Soient $u_1 < u_2 < \cdots < u_{2r}$ les racines de $P(x)^2 = M'^2$. D'après (2.5.5), les u_i sont distincts et appartiennent à l'intérieur de E ; de façon plus précise, pour tout j impair, l'intervalle $[u_j, u_{j+1}]$ est contenu dans l'intérieur du j-ième sous-intervalle de E au sens

5. On aura soin de ne pas confondre P' avec la dérivée dP/dx de P.

de (2.4.8). Si P' est assez voisin de P (au sens de la topologie naturelle de l'espace des polynômes unitaires de degré r), la même propriété vaut pour les racines de $u'_1, \cdots, u'_{2r}$ de $P' - M'$ et $P' + M'$, et les relations d'ordre entre racines de $P' - M'$ et racines de $P' + M'$ sont les mêmes que pour P. Choisissons un tel P' qui soit à coefficients dans $\mathbf{Q}$. Posons $Q' = 1$ et $D' = P'^2 - M'^2$; l'équation de Pell-Abel $P'^2 - D'Q'^2 = M'^2$ est satisfaite. On a $D' = \prod(x - u'_i)$. L'ensemble E' des points où D' est $\leqslant 0$ est la réunion des $[u_j, u_{j+1}]$, j impair. Il est contenu dans E (et même dans l'intérieur de E) : les conditions (2.6.2) sont donc satisfaites.

Corollaire 2.6.3. *On peut choisir E' et P' de telle sorte que M' soit rationnel et que* $\mathrm{cap}(E) - \mathrm{cap}(E')$ *soit aussi petit que l'on veut.*

C'est clair, puisque $\mathrm{cap}(E') = (M'/2)^{1/r}$ d'après le th. 2.4.9 (iii) appliqué à E'.

Remarque. Le compact E' a r composantes connexes, et chacune d'elles contient une racine de P' et une seule ; le genre de la courbe hyperelliptique correspondante est en général $> g$.

2.7. Comment remplacer les coefficients rationnels par des coefficients entiers

Reprenons les notations et hypothèses des §§ 2.3, 2.4, en supposant en outre que M *et les coefficients de P sont rationnels.* Posons $\lambda = M/2$; d'après le th. 2.4.9 (ii), on a $\mathrm{cap}(E) = \lambda^{1/r}$. On va démontrer :

Théorème 2.7.1. *Supposons* $\mathrm{cap}(E) > 1$, *autrement dit $\lambda > 1$. Il existe une suite de polynômes unitaires, à coefficients entiers, de degrés tendant vers l'infini, dont toutes les racines sont simples et appartiennent à E.*

Corollaire 2.7.2. *Il existe une infinité d'entiers algébriques qui appartiennent totalement à E.*

[Autrement dit, le th. 1.6.1 est vrai pour E.]

Démonstration (d'après [Ro 64], §6, dont nous adoptons les notations).

Le point de départ consiste à utiliser la solution donnée (P, Q, λ) de l'équation de Pell-Abel pour en fabriquer d'autres de degré nr pour tout $n \geqslant 1$: il suffit d'élever $P + yQ$ à la puissance n, et de regrouper les termes. On trouve :

$$(P + yQ)^n = 2^{n-1}(P_n + yQ_n) \quad \text{et} \quad P_n^2 - DQ_n^2 = 4\lambda^{2n},$$

où P_n et Q_n sont unitaires de degrés nr et $nr - g - 1$, respectivement.

Pour $n = 2$, cela donne :

$$(P + yQ)^2 = 2(P_2 + yQ_2), \text{ avec } P_2 = P^2 - 2\lambda^2 \text{ et } Q_2 = PQ.$$

Pour n arbitraire, la formule analogue est :

$$P_n(x) = \lambda^n T_n(P(x)/\lambda), \tag{2.7.3}$$

où T_n est le n-ième polynôme de Chebyshev, cf. (A.2.2) ; cela se démontre, par exemple, en se plaçant dans un sous-intervalle, et en remarquant que, d'après (2.5.2), on a $P(x) = 2\lambda\cos(\theta(x))$ et $P_n(x) = 2\lambda^n\cos(n\theta(x))$.

Nous aurons besoin d'une formule pour T_n qui mette en évidence les propriétés de divisibilité de ses coefficients. Robinson donne la suivante (démontrée dans [Ro 62], §2) :

(2.7.4) $T_n(X) = X^n + \sum_{k=1}^{[n/2]} (-1)^k \frac{n}{k} \binom{n-k-1}{k-1} X^{n-2k}$.

D'où :

(2.7.5) $P_n(x) = P(x)^n + \sum_{k=1}^{[n/2]} (-1)^k \frac{n}{k} \binom{n-k-1}{k-1} \lambda^{2k} P(x)^{n-2k}$.

Cela peut s'écrire en abrégé :

(2.7.6) $P_n(x) = x^{nr} + \sum_{k>0} \alpha_k x^{nr-k}$,

où, pour chaque $k > 0$, α_k est un polynôme à coefficients dans $\mathbf{Q}$ en n, en λ, et en les coefficients de P ; comme λ et les coefficients de P sont rationnels, on voit que α_k *est un polynôme en* n*, à coefficients dans* $\mathbf{Q}$*, et de terme constant* 0.

Posons

(2.7.7) $C = \sup_{x \in E}(1 + |x| + \cdots + |x|^{r-1})$.

Choisissons un entier $\ell > 0$ tel que :

(2.7.8) $\lambda^\ell(\lambda - 1) \geqslant C/2$.

C'est possible puisque $\lambda > 1$.

Choisissons un entier $m \geqslant 1$ tel que, pour $k = 1, \ldots, \ell r$, les α_k, considérés comme polynômes en n, soient à coefficients dans $\frac{1}{m}\mathbf{Z}$.

Lemme 2.7.9. *Pour tout* $n > 0$ *divisible par* m*, il existe* $q \in \mathbf{R}[x]$*, de degré* $< nr$*, tel que* :

(i) $|q(x)| < 2\lambda^n$ *pour tout* $x \in E$.

(ii) *Les coefficients de* $P_n - q$ *sont des entiers.*

Ce lemme entraîne le th. 2.7.1 : en effet, le polynôme $P_n - q$ est à coefficients entiers, et, d'après le lemme 2.5.5, appliqué à P_n, il a nr racines distinctes contenues dans E.

Démonstration du lemme 2.7.9.

Il s'agit de modifier P_n pour que ses coefficients deviennent entiers. On remarque d'abord que les ℓr premiers coefficients $\alpha_1, \ldots, \alpha_{\ell r}$ sont entiers ; cela provient du fait que n est un multiple de m. Il suffit donc de prendre pour q un polynôme de degré $\leqslant nr - \ell r - 1$. On utilise pour cela la base formée [6] des $x^j P_k(x)$, avec $0 \leqslant j < r$ et $0 \leqslant k < n - \ell$. On écrit q sous la forme $q(x) = \sum_{j,k} c_{jk}\ x^j P_k(x)$, et l'on choisit les coefficients c_{jk} entre $-1/2$ et $1/2$, et tels que $P - q$ soit à coefficients dans $\mathbf{Z}$. Pour tout $x \in E$, on a :

$$|q(x)| \leqslant \tfrac{1}{2} \sum_{j,k} |x|^j 2\lambda^k \leqslant C \sum_{k=0}^{k=n-\ell-1} \lambda^k \leqslant C \frac{\lambda^{n-\ell}-1}{\lambda-1} < C \frac{\lambda^{n-\ell}}{\lambda-1}.$$

D'où $|q(x)| < 2\lambda^n$, d'après (2.7.8).

6. Il ne faut surtout pas utiliser la base naturelle $1, x, x^2, \ldots, x^{nr-\ell r-1}$, qui conduirait à une majoration inutilisable de $|q(x)|$.

2.8. Comment ramener le cas général au cas de Pell-Abel

Fixons $g \geqslant 0$. Soit U l'ouvert de $\mathbf{R}^{2g+2}$ formé des $(a_0, b_0, a_1, \ldots, b_g)$ tels que $a_0 < b_0 < \cdots < b_g$. Si $u = (a_0, \ldots, b_g)$ appartient à U, notons E_u le compact correspondant :

$$E_u = [a_0, b_0] \cup \cdots \cup [a_g, b_g].$$

Disons que *u est de type PA* si l'équation de Pell-Abel correspondante a une solution de degré > 0. Soit U_{PA} l'ensemble des u de ce type.

Théorème 2.8.1. *U_{PA} est dense dans U.*

Cet énoncé permet d'achever la démonstration du th. 1.6.1. En effet, soit $u = (a_0, \ldots, b_g)$ un élément de U tel que $\mathrm{cap}(E_u) > 1$. D'après la prop. A.7.1, tous les $v \in U$ suffisamment voisins de u sont tels que $\mathrm{cap}(E_v) > 1$. D'après le th. 2.8.1, on peut choisir $v \in U_{PA}$ avec $E_v \subset E_u$ et $\mathrm{cap}(E_v) > 1$. Grâce au cor. 2.6.3, on peut aussi supposer que l'équation de Pell-Abel $P^2 - DQ^2 = M^2$ pour E_v a une solution avec $P \in \mathbf{Q}[x]$ et $M \in \mathbf{Q}$; le cor. 2.7.2 montre alors que Irr_{E_v} est infini, donc aussi Irr_{E_u}, ce qui démontre le th. 1.6.1.

Démonstration du th. 2.8.1 (d'après [La 16]).

Si $u \in U$, soit J_u la jacobienne de la courbe hyperelliptique C_u associée à E_u. La composante neutre $J_u(\mathbf{R})^0$ de $J_u(\mathbf{R})$ est un tore de dimension g, que l'on peut identifier à $\mathbf{R}^g/\mathbf{Z}^g$, après un choix convenable (précisé dans [La 16]) de bases pour les formes de première espèce, et pour les cycles réels. L'image de $\infty_- - \infty_+$ dans $J_u(\mathbf{R})$ appartient à $J_u(\mathbf{R})^0$; d'où un élément $\vartheta(u) \in \mathbf{R}^g/\mathbf{Z}^g$. Cela définit une application analytique réelle (cf. [La 16]) $\vartheta : U \to \mathbf{R}^g/\mathbf{Z}^g$; comme U est simplement connexe, on peut la relever en une application continue $\theta : U \to \mathbf{R}^g$. On a :

(2.8.2) $u \in U_{PA} \iff \theta(u) \in \mathbf{Q}^g$.

En effet, $\theta(u) \in \mathbf{Q}^g \iff \vartheta(u)$ est d'ordre fini dans $\mathbf{R}^g/\mathbf{Z}^g$.

Ainsi, le th. 2.8.1 équivaut à dire que *l'image réciproque de $\mathbf{Q}^g$ par $\theta : U \to \mathbf{R}^g$ est dense dans U*. On va voir que cela provient simplement du fait que $\mathbf{Q}^g$ est dense dans $\mathbf{R}^g$. Il faut d'abord « rappeler » quelques faits élémentaires :

Intermède topologique.

Proposition 2.8.3. *Soit $f : X \to Y$ une application entre espaces topologiques. Soit Y' une partie dense de Y. Si f est une application ouverte, $f^{-1}(Y')$ est dense dans X.*
[Rappelons que f est dite *ouverte* si l'image par f de tout ouvert de X est un ouvert de Y ; cela n'entraîne pas que f soit continue.]

Démonstration. Soit V un ouvert non vide de X. Alors $f(V)$ est un ouvert non vide de Y ; il rencontre donc Y', d'où $V \cap f^{-1}(Y') \neq \varnothing$, ce qui montre que $f^{-1}(Y')$ est dense dans X.

Nous allons appliquer ceci aux variétés analytiques réelles :

Proposition 2.8.4. *Soit $f : X \to Y$ un morphisme de variétés analytiques réelles de dimension finie. Supposons que X soit connexe, et qu'il existe $x \in X$ en lequel f est une submersion. Soit Y' une partie dense de Y. Alors $f^{-1}(Y')$ est dense dans X.*

[Rappelons que f est une submersion en x signifie que l'application tangente à f en x est surjective.]

Démonstration. Soit F l'ensemble des points de X en lesquels f n'est pas une submersion ; c'est un sous-ensemble analytique fermé de X : il est défini localement par l'annulation d'un nombre fini d'équations analytiques. Soit $\overset{\circ}{F}$ l'intérieur de F. Le classique « principe du prolongement analytique » dit que $\overset{\circ}{F}$ est fermé. Comme il est ouvert, et que X est connexe, c'est, soit $\varnothing$, soit X. Or ce n'est pas X, puisqu'il ne contient pas x. C'est donc $\varnothing$, autrement dit $X - F$ est dense dans X. Comme la restriction de f à $X - F$ est une submersion, c'est une application ouverte. La prop. 2.8.3 entraîne que $(X - F) \cap f^{-1}(Y')$ est dense dans $X - F$, donc aussi dans X.

Fin de la démonstration du th. 2.8.1

Pour démontrer le th. 2.8.1, il suffirait, d'après la prop. 2.8.4, d'exhiber un élément u de U, en lequel l'application $\theta : U \to \mathbf{R}^g$ est une submersion. Malheureusement, ce n'est pas facile pour $g > 1$. Dans [La 16], Lawrence procède autrement : il définit une variété U' qui contient U, ainsi que certains points « dégénérés » ; l'application θ se prolonge à U', et il montre qu'elle est une submersion en certains des points dégénérés. Je renvoie à [La 16] pour plus de détails. *Grosso modo*, les points dégénérés qu'il utilise correspondent à des suites $a_0 < b_0 = a_1 < b_1 = a_2 < \cdots < b_{g-1} = a_g < b_g$. La courbe hyperelliptique de genre g est remplacée par une courbe de genre 0 ayant g points doubles ; sa jacobienne généralisée est un groupe de type multiplicatif de dimension g dont le groupe des points réels est compact.

Remarque. On trouvera une autre démonstration du th. 2.8.1 dans [Ro 64] et dans [ACZ 18].

APPENDICE. FASCICULE DE RÉSULTATS SUR LES CAPACITÉS

Soit K une partie compacte de $\mathbf{C}$. La *capacité* $\mathrm{cap}(K)$ de K (parfois appelée *capacité logarithmique*, ou bien *diamètre transfini*) est un nombre réel $\geqslant 0$, défini de l'une des trois façons équivalentes A.1, A.2, A.3 données ci-dessous. Cette notion a été introduite en 1923-1924 par Fekete ([Fe 23]) et Szegő ([Sz 24]), sans doute inspirés par des résultats antérieurs de Stieltjes ([St 85]) et de Schur ([Sc 18]). On en trouvera une étude détaillée dans Tsuji ([Ts 59], chap. III) et Ransford ([Ra 95], chap. 3-4-5).

A.1. La capacité définie au moyen de discriminants [7]

Si $n > 1$, posons :

(A.1.1) $d_n(K) = \sup_{x_1,\dots,x_n \in K} \prod_{i \neq j} |x_i - x_j|^{1/n(n-1)}$.

[Lorsque $n = 2$, $d_n(K)$ est le *diamètre* de K, au sens habituel.]

On a $d_2(K) \geqslant d_3(K) \geqslant \cdots$. Lorsque K est fini, on convient que $d_n(K) = 0$ si $n > |K|$.

La capacité de K est définie par :

(A.1.2) $\mathrm{cap}(K) = \inf_n d_n(K) = \lim_{n\to\infty} d_n(K)$.

Elle est souvent notée $d_\infty(K)$.

A.2. La capacité, à la Chebyshev

Si $n > 0$, soit $c_n(K) = \inf_P \|P\|^{1/n}$, où P parcourt l'ensemble des polynômes unitaires de degré n à coefficients dans $\mathbf{C}$, et $\|P\|$ est la borne supérieure de $|P|$ sur K. Pour chaque $n \leqslant \mathrm{card}(K)$, il existe un unique P (cf. [Ts 59], th. III.23) tel que $\|P\| = c_n(K)^n$: c'est le *n-ième polynôme de Chebyshev* de K.

On a :

(A.2.1) $\mathrm{cap}(K) = \inf_n c_n(K)^{1/n} = \lim_{n\to\infty} c_n(K)^{1/n}$.

Exemple. Prenons pour K le segment $[-2, 2]$; il est bien connu que le n-ième polynôme de Chebyshev de K est le polynôme T_n caractérisé par

(A.2.2) $T_n(t + t^{-1}) = t^n + t^{-n}$,

ou, ce qui revient au même :

(A.2.3) $T_n(2\cosh x) = 2\cosh nx$ et $T_n(2\cos\theta) = 2\cos n\theta$.

On a $\|T_n\|_K = 2$; d'après (A.2.1), cela entraîne $\mathrm{cap}(K) = 1$. Ce résultat peut aussi se déduire de (A.1.2), et de la détermination des $d_n(K)$ due à Stieltjes et Schur, cf. [St 85] et [Sc 18], §1, Satz I.

La mesure d'équilibre de K (au sens de A.4 ci-dessous) est :

(A.2.4) $\mu_K = \frac{1}{\pi} \frac{dx}{\sqrt{4-x^2}}$;

cela résulte de la prop. A.6.1, et du fait que la mesure d'équilibre d'un cercle est l'unique mesure de masse 1 invariante par rotation.

Par homothétie, on déduit de $\mathrm{cap}([-2, 2]) = 1$ que *la capacité d'un intervalle de longueur ℓ est égale à $\ell/4$.*

---

7. Dans les énoncés ci-dessous, on suppose K non vide ; lorsque K est vide, et plus généralement quand K est fini, on a $\mathrm{cap}(K) = 0$.

A.3. Une variante de A.1, en termes de mesures

Soit μ une mesure positive sur K. Posons :

(A.3.1) $I(\mu) = \iint_{K\times K} \log|x-y|\mu(x)\mu(y)$.

C'est, soit $-\infty$, soit un nombre réel. Soit $v(K) = \sup_\mu I(\mu)$, où μ parcourt l'ensemble des mesures positives de masse 1 à support dans K. On a :

(A.3.2) $\operatorname{cap}(K) = e^{v(K)}$,

et en particulier $\operatorname{cap}(K) = 0$ si et seulement si $I(\mu) = -\infty$ pour tout μ à support dans K.

Le fait que les définitions A.1, A.2 et A.3 de $\operatorname{cap}(K)$ sont équivalentes est dû à Fekete et Szegő, cf. [Fe 23], [Sz 24], [FS 55], ainsi que [Ra 95], th. 5.5.2 et th. 5.5.4. La terminologie « diamètre transfini » provient de A.1 et celle de « capacité logarithmique » de A.3. Noter que, du point de vue de la théorie des capacités de Choquet, c'est $v(K) = \log\operatorname{cap}(K)$, et non $\operatorname{cap}(K)$, qui mériterait le nom de « capacité », cf. [Ch 58].

A.3.3. *Extension de la notion de compacité aux ensembles non compacts.*

Soit Y une partie bornée de $\mathbf{C}$. On appelle *capacité intérieure* (ou simplement « capacité ») de Y, la borne supérieure des $\operatorname{cap}(K)$ lorsque K parcourt les sous-espaces compacts de Y ; on la note encore $\operatorname{cap}(Y)$. En particulier, Y est dit *de capacité* 0 (« ensemble polaire » : « polar set » dans [Ra 95]) si $\operatorname{cap}(K) = 0$ pour toute partie compacte K de Y.

A.4. Mesure d'équilibre

Lorsque K est un compact de capacité > 0, il existe une unique mesure positive μ de masse 1 telle que $I(\mu) = \log\operatorname{cap}(K)$, cf. [Ra 95], th. 3.7.6. On l'appelle la *mesure d'équilibre* de K, et on la note μ_K. C'est une mesure diffuse (cela résulte du cor. 1.4.2). Son support $\operatorname{Supp}(\mu_K)$ n'est pas toujours égal à K ; ainsi, lorsque K est un disque, le support de μ_K est le cercle qui borde ce disque. Lorsque K est contenu dans $\mathbf{R}$, K et $\operatorname{Supp}(\mu_K)$ ne diffèrent que par un ensemble de capacité 0. De façon plus précise :

Proposition A.4.1. *Soit K une partie compacte de $\mathbf{R}$ de capacité > 0. Soit K' une partie fermée de K. Les propriétés suivantes sont équivalentes* :

(A.4.2) $\operatorname{cap}(K') = \operatorname{cap}(K)$.

(A.4.3) $K' \supset \operatorname{Supp}(\mu_K)$.

(A.4.4) $K - K'$ *est de capacité* 0 (au sens de A.3.3).

Corollaire A.4.5. $\operatorname{Supp}(\mu_K)$ *est la plus petite partie fermée de K ayant même capacité que K.*

Corollaire A.4.6. *L'ensemble* $K - \operatorname{Supp}(\mu_K)$ *est de capacité* 0.

Démonstration de la prop. A.4.1.

(A.4.2) ⇒ (A.4.3). Si $\mathrm{cap}(K') = \mathrm{cap}(K)$, on a $I(\mu_{K'}) = I(\mu_K)$, d'où $\mu_{K'} = \mu_K$ en vertu de l'unicité de la mesure d'équilibre de K ; cela entraîne $\mathrm{Supp}(\mu_{K'}) = \mathrm{Supp}(\mu_K)$, d'où $K' \supset \mathrm{Supp}(\mu_K)$.

(A.4.3) ⇒ (A.4.4). D'après [Ts 59], th. III.31, l'ensemble $K - \mathrm{Supp}(\mu_K)$ est de capacité 0. Il en est a fortiori de même de $K - K'$ si K' contient $\mathrm{Supp}(\mu_K)$.

(A.4.4) ⇒ (A.4.2). Cela résulte de A.5.4 ci-dessous.

A.4.7. Disons que K est *réduit* si $K = \mathrm{Supp}(\mu_K)$. La prop. A.4.1 entraîne :

Proposition A.4.8. *Soit K une partie compacte de $\mathbf{R}$ de capacité > 0. Les propriétés suivantes sont équivalentes* :

(i) *K est réduit.*

(ii) *Aucune partie fermée de K, distincte de K, n'a la même capacité que K.*

(iii) *Aucune partie ouverte non vide de K n'est de capacité* 0.

Corollaire A.4.9. *Soit μ une mesure positive à support compact sur $\mathbf{R}$, telle que $I(\mu) > -\infty$. Alors* $\mathrm{Supp}(\mu)$ *est réduit.*

Démonstration. Soit $K = \mathrm{Supp}(\mu)$. Si K n'était pas réduit, d'après la prop. A.4.8, il existerait un ouvert non vide U de K de capacité 0. D'après le th. III.7 de [Ts 59], on aurait $\mu(U) = 0$, ce qui contredirait le fait que U est contenu dans $\mathrm{Supp}(\mu)$.

A.5. Quelques propriétés de la capacité

(A.5.1) (*Linéarité*) $\mathrm{cap}(\lambda K) = |\lambda| \,\mathrm{cap}(K)$ pour tout $\lambda \in \mathbf{C}$.

(A.5.2) (*Continuité pour les suites décroissantes*) Soit K_n une suite décroissante de compacts de $\mathbf{C}$. On a $\mathrm{cap}(\cap K_n) = \inf_n \mathrm{cap}(K_n)$, cf. [Ra 95], th. 5.1.3 (a).

(A.5.3) Soient $K_1, K_2 \subset \mathbf{C}$ deux compacts, et soit d leur distance. On a :

$$\mathrm{cap}(K_1 \cup K_2) \geqslant \mathrm{cap}(K_1)^{1/4} \,\mathrm{cap}(K_2)^{1/4} d^{1/2}.$$

Cela se démontre en appliquant (A.1.1) avec n pair, en choisissant de façon optimale $n/2$ points dans K_1 et $n/2$ points dans K_2.

(A.5.4) Soient B_1 et B_2 deux parties boréliennes bornées de $\mathbf{C}$. Si B_2 est de capacité 0, on a $\mathrm{cap}(B_1 \cup B_2) = \mathrm{cap}(B_1)$, cf. [Ts 59], th. III.18.

(A.5.5) (*Continuité pour les suites croissantes*) Soit K_n une suite croissante de compacts et soit K l'adhérence de $\cup_n K_n$. On suppose que K est borné (donc compact) et que $\mathrm{cap}(K - \cup K_n) = 0$. Alors $\mathrm{cap}(K) = \sup \mathrm{cap}(K_n)$.

Démonstration.

D'après [Ra 95], th. 5.1.3 (b), on a $\mathrm{cap}(\cup_n K_n) = \sup \mathrm{cap}(K_n)$. On applique (A.5.4) à $B = K, B_1 = \cup_n K_n$ et $B_2 = K - \cup_n K_n$.

(A.5.6) Soit K un compact contenu dans $\mathbf{R}$, et soit $\mathrm{mes}(K)$ sa mesure de Lebesgue. On a $\mathrm{cap}(K) \geqslant \mathrm{mes}(K)/4$, cf. [Ra 95], th. 5.3.2.

En particulier, $\mathrm{cap}(K) = 0$ entraîne $\mathrm{mes}(K) = 0$. La réciproque est fausse : l'ensemble triadique de Cantor dans $[0,1]$ est de mesure nulle, mais sa capacité est au moins $1/9$, cf. §1.6.

(A.5.7) Soit $f \in \mathbf{C}[X]$ un polynôme unitaire de degré $r \geqslant 1$.
On a $\mathrm{cap}(f^{-1}K) = \mathrm{cap}(K)^{1/r}$ pour tout compact K de $\mathbf{C}$, cf. [Ra 95], th. 5.2.5.

(A.5.8) (*Capacité de la réunion de deux intervalles de même longueur*)

Soient $a, b \in \mathbf{R}$ avec $0 < a < b$, et soit $E = [-b,-a] \cup [a,b]$. On a :

$\mathrm{cap}(E) = \frac{1}{2}\sqrt{b^2 - a^2}$.

Cela résulte de (A.5.7) appliqué à $f = X^2$ et $K = [a^2, b^2]$, de sorte que $f^{-1}K = E$.

A.6. Capacité des sous-ensembles d'un cercle

L'énoncé suivant est analogue à (A.5.7) :

Proposition A.6.1. *Soit C un cercle de centre 0 et de rayon r. Soit $I = [-2r, 2r]$, et soit $f : C \to I$ l'application $z \mapsto z + \overline{z}$. Soit K un compact de I et soit $K_C = f^{-1}(K)$.*

(i) *On a* $\mathrm{cap}(K_C) = r^{1/2}\,\mathrm{cap}(K)^{1/2}$.

(ii) *Supposons* $\mathrm{cap}(K) \neq 0$. *On a $f(\mu_{K_C}) = \mu_K$, où μ_K et μ_{K_C} sont les mesures d'équilibre de K et de K_C, cf. A.4.*

La notation $f(\mu_{K_C})$ désigne *l'image* de la mesure μ_{K_C} par l'application f.

Corollaire A.6.2. *La capacité d'un cercle de rayon r est égale à r.*

Cela résulte de (i) appliqué à $K = I, K_C = C$.

Démonstration de la prop. A.6.1.

Quitte à faire une homothétie, on peut supposer $r = 1$; alors C est le cercle unité $|z| = 1$, et $I = [-2, 2]$. On peut aussi supposer que $\mathrm{cap}(K) > 0$.

Soit ν une mesure positive sur C, invariante par la conjugaison complexe $z \mapsto \overline{z}$. Soit ν' l'image de ν par f ; c'est une mesure sur I, de même masse que ν. Soient $I(\nu)$ et $I(\nu')$ les intégrales définies dans (A.3.1), autrement dit :

$I(\nu) = \iint_{C\times C} \log|z_1 - z_2|\nu(z_1)\nu(z_2)$

et

$I(\nu') = \iint_{I\times I} \log|x - y|\nu'(x)\nu'(y)$.

Lemme A.6.3. *On a $I(\nu') = 2I(\nu)$.*

Démonstration du lemme.

Posons $A(z_1, z_2) = \log|z_1 - z_2| + \log|\overline{z}_1 - z_2|$. Comme ν est invariante par conjugaison, on a

(A.6.4) $\iint_{C\times C} A(z_1, z_2)\nu(z_1)\nu(z_2) = 2I(\nu)$.

Soient $x = f(z_1) = z_1 + \overline{z}_1$ et $y = f(z_2)$. Un calcul simple montre que :

(A.6.5) $|(z_1 - z_2)(\overline{z}_1 - z_2)| = |z_1 + \overline{z}_1 - (z_2 + \overline{z}_2)| = |x - y|$,

d'où :

(A.6.6) $A(z_1, z_2) = \log|x - y|$.

Ainsi, la fonction $A(z_1, z_2)$ est la composée de $f \times f : C \times C \to I \times I$ et de la fonction $\log|x-y|$ sur $I \times I$.
Comme $\nu' \otimes \nu'$ est l'image de $\nu \otimes \nu$ par $f \times f$, on en déduit :

(A.6.7) $\iint_{C\times C} A(z_1, z_2)\nu(z_1)\nu(z_2) = \iint_{I\times I} \log|x-y|\nu'(x)\nu'(y) = I(\nu')$.

Le lemme résulte de (A.6.4) et (A.6.7).

Fin de la démonstration de la prop. A.6.1.

L'application $\nu \mapsto \nu'$ donne une bijection entre les mesures positives de masse 1 sur K_C qui sont invariantes par conjugaison, et les mesures positives de masse 1 sur K.

Soit μ_K la mesure d'équilibre de K ; on a $I(\mu_K) = c$, avec $c = \log \operatorname{cap}(K)$. Si ν est la mesure correspondante sur K_C, le lemme A.6.3 montre que $I(\nu) = c/2$, d'où $\operatorname{cap}(K_C) \geqslant \operatorname{cap}(K)^{1/2}$. Si cette inégalité était stricte, on aurait $I(\mu_{K_C}) > c/2$; comme la mesure $I(\mu_{K_C})$ est canonique, elle est invariante par conjugaison, et elle correspondrait à une mesure ν' sur K telle que $I(\nu') > c$, contrairement à la définition de c. On a donc $\operatorname{cap}(K_C) = \operatorname{cap}(K)^{1/2}$, ce qui démontre (i). On voit en outre que ν est la mesure d'équilibre de K_C, ce qui démontre (ii).

A.7. Une propriété de continuité pour les réunions finies d'intervalles fermés de R

Soit $a = \{a_1, \ldots, a_n\}$ une suite strictement croissante de nombres réels, en nombre n pair, et posons :

$$E_a = [a_1, a_2] \cup [a_3, a_4] \cup \cdots \cup [a_{n-1}, a_n].$$

Proposition A.7.1. *La capacité de E_a dépend continûment de a.*

Démonstration. Soit $d = \inf a_{i+1} - a_i$. Si ε est > 0 et $< d/2$, notons a'_ε la suite des $a_i + (-1)^i\varepsilon$ et a''_ε la suite des $a_i - (-1)^i\varepsilon$. On a :

$$E_{a''_\varepsilon} \subset E_a \subset E_{a'_\varepsilon}.$$

La continuité de $\operatorname{cap}(E_a)$ équivaut à dire que $\operatorname{cap}(E_a)$ est la borne inférieure des $\operatorname{cap}(E_{a'_\varepsilon})$ ainsi que la borne supérieure des $\operatorname{cap}(E_{a''_\varepsilon})$, ce qui résulte respectivement de (A.5.2) et (A.5.5).

A.8. Calculs effectifs de capacités

Le calcul de la capacité d'un compact K donné est un problème difficile. On trouvera dans [Ra 95, p. 135] une liste de quelques cas connus. Signalons par exemple celui d'un arc de cercle, de rayon r et d'angle α, avec $0 \leqslant \alpha \leqslant 2\pi$: c'est $r\sin(\alpha/4)$; cela se déduit de la prop. A.6.1 appliquée à $K = [2r\cos(\alpha/2), 2r]$. Voir aussi [RR 07] et [LSN 17] pour des calculs approchés, sur ordinateur.

Pour les sous-espaces de $\mathbf{R}$, un cas particulièrement intéressant est celui où K est réunion disjointe de segments fermés. Le cas de deux segments a été traité par Akhiezer : [Ak 30] et [Ak 32] ; le résultat s'exprime en termes de fonctions thêta à la Jacobi. Pour le cas général, voir Bogatyrëv [Bo 99], Peherstorfer-Schiefermayr [PS 99] et Bogatyrëv-Grigoriev [BG 17].

RÉFÉRENCES

[Ab 26] N.H. Abel, *Sur l'intégration de la forme différentielle* $\rho dx/\sqrt{R}$, *R et* ρ *étant des fonctions entières*[8], J. Crelle 1 (1826), 105-144 (= *Oe*, XI).

[ACZ 18] Y. André, P. Corvaja & U. Zannier, *The Betti map associated to a section of an abelian scheme* (with an Appendix by Z. Gao), à paraître.

[Ak 30] N.I. Akhiezer (= Achieser = Achyeser), *Sur les polynomes de Tchebyscheff pour deux segments*, C.R.A.S. 191 (1930), 754-756.

[Ak 32] —— , *Über einige Funktionen welche in zwei gegebenen Intervallen am wenigsten von Null abweichen* I, Izv. Akad. Nauk SSSR (1932), 1163-1202 ; II, III, *ibid.* (1933), 499-536.

[A IV] N. Bourbaki, *Algèbre. Chapitres* IV-VII, Masson, 1981 ; traduction anglaise, *Algebra* II, Springer-Verlag, 2003.

[BG 17] A. Bogatyrëv & O.A. Grigoriev, *Closed formula for the capacity of several aligned segments*, Proc. Inst. Steklov Math. 298 (2017), 60-67.

[Bo 99] A. Bogatyrëv, *Effective computations of Chebyshev polynomials for several intervals* (en russe), Math. Sbornik 190 (1999), 15-50 ; traduction anglaise, Sbornik, Mathematics 190 (1999), 1571-1605.

[Bo 05] —— , *Extremal Polynomials and Riemann Surfaces* (en russe), MCCME, Moscou, 2005 ; traduction anglaise, Springer-Verlag, 2012.

[Ca 69] D. Cantor, *On approximation by polynomials with algebraic integer coefficients*, Proc. Symposia Pure Math. 12, AMS, 1969, 1-13.

[Ca 80] —— , *On an extension of the definition of transfinite diameter and some applications*, J. Crelle 316 (1980), 160-207.

[Ch 54] P.L. Tchebychef (= Chebyshev), *Théorie des mécanismes connus sous le nom de parallélogrammes*, Mém. Acad. Sci. Pétersb. 7 (1854), 539-568 (= *Oe* I, 111-143).

[Ch 58] G. Choquet, *Capacitabilité en potentiel logarithmique*, Bull. Acad. Royale Belg. Cl. Sci., 44 (1958), 321-326.

[Fe 23] M. Fekete, *Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten*, Math. Zeit. 17 (1923), 228-249.

[FRV] N. Bourbaki, *Fascicule de Résultats des Variétés*, Hermann, Paris, 1971.

[FS 55] M. Fekete & G. Szegő, *On algebraic equations with integral coefficients whose roots belong to a given point set*, Math. Zeit. 63 (1955), 158-172.

[Go 03] R. Godement, *Analyse Mathématique* IV : *Intégration et théorie spectrale, analyse harmonique, le jardin des délices modulaires*, Springer-Verlag, 2003 ; traduction anglaise, *Analysis* IV, Springer-Verlag, 2015

[INT] N. Bourbaki, *Intégration. Chapitres* I-V, seconde édition, Hermann, Paris, 1967 ; traduction anglaise, *Integration* I, Springer-Verlag, 2004.

8. Le texte original, écrit en français, est celui reproduit dans les *Oeuvres* ; celui du journal de Crelle est une traduction en allemand, due probablement à Crelle.

[Kr 57] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, J. Crelle 53 (1857), 173-175 (= *Werke* I, 103-108).

[La 16] B. Lawrence, *A density result for real hyperelliptic curves*, C.R.A.S. 354 (2016), 1219-1224.

[LSN 17] J. Liesen, O. Sète & M.M.S. Nasser, *Fast and accurate computation of the logarithmic capacity of compact sets*, Comp. Methods Funct. Theory 17 (2017), 689-713.

[Pe 90] F. Peherstorfer, *On Bernstein-Szegő orthogonal polynomials on several intervals*, Siam J. Math. Anal. 21 (1990), 461-482.

[PS 99] F. Peherstorfer & K. Schiefermayr, *Description of extremal polynomials on several intervals and their computation* I, II, Acta Math. Hung. 83 (1999), 71-102 & 103-128.

[Ra 95] T. Ransford, *Potential Theory in the Complex Plane*, London Math. Soc., Students Texts 28, 1995.

[RR 07] T. Ransford & J. Rostand, *Computation of capacity*, Math. Comp. 76 (2007), 1499-1520.

[Ro 62] R.M. Robinson, *Intervals containing infinitely many sets of conjugate algebraic integers*, in *Studies in Mathematical Analysis and Related Topics* : *Essays in honor of George Pólya*, Stanford 1962, 305-315.

[Ro 64] —— , *Conjugate algebraic integers in real point sets*, Math. Zeit. 84 (1964), 415-427.

[Ro 69] —— , *Conjugate algebraic integers on a circle*, Math. Zeit. 110 (1969), 41-51.

[Ru 14] R. Rumely, *Capacity Theory with Local Rationality - The strong Fekete-Szegő theorem on curves*, A.M.S. Surveys 193, 2013.

[Sc 18] I. Schur, *Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten*, Math. Zeit. 1 (1918), 377-402 (= *Gesam. Abh.* II, 32).

[Se 97] J-P. Serre, *Répartition asymptotique des valeurs propres de l'opérateur de Hecke* T_p, J.A.M.S. 10 (1997), 75-102 (= *Oe.* IV, 170).

[Sm 84] C. Smyth, *Totally positive algebraic integers of small trace*, Ann. Inst. Fourier 33 (1984), 1-28.

[SY 92] M.L. Sodin & P.M. Yuditskii, *Functions which deviate least from zero on closed subsets of the real axis* (en russe), Algebra i Analiz 4 (1992), 1-61 ; traduction anglaise, St. Petersburg Math. J. 4 (1993), 201-249.

[St 85] T.J. Stieltjes, *Sur quelques théorèmes d'algèbre*, C.R.A.S. 100 (1885), 439-440 (= *Oe.* I, 440-441).

[Sz 24] G. Szegő, *Bermerkungen über einer Arbeit von Herrn M. Fekete* : *Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten*, Math. Zeit. 21 (1924), 203-208.

[Ta 69] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini*, Sém. Bourbaki 1968/1969, n° 352 (= LNM 175 (1971), 95-110 = *Coll. Papers* I, 32).

[Ts 18] M. A. Tsfasman, *Serre's theorem and measures corresponding to abelian varieties over finite fields*, à paraître.

[Ts 59] M. Tsuji, *Potential Theory in Modern Function Theory*, Maruzen, Tokyo, 1959 ; seconde édition, Chelsea, New York, 1975.

[TV 97] M.A. Tsfasman & S.G. Vlăduţ, *Asymptotic properties of zeta functions*, J. Math. Sci. (New York) 84 (1997), 1445-1467.

Jean-Pierre SERRE

Collège de France
3 rue d'Ulm
75005 Paris
E-mail : `serre@noos.fr`