Autour du théorème de Fekete-Szegö

Pascal Autissier

8 juin 2020

Résumé : Après un rappel de théorie du potentiel, on prouve dans ce cours un théorème de Fekete via la théorie d'Arakelov. On donne ensuite une démonstration "classique" du théorème de Fekete-Szegö. La théorie du potentiel se généralise en fait aux surfaces de Riemann compactes. On explique comment ceci permet d'étendre les énoncés précédents au cas des surfaces arithmétiques. Enfin, on montre un théorème d'équirépartition dû à Bilu et Rumely.

1 Introduction

Soit $\mathcal{K}$ un compact de $\mathbb{C}$. En théorie du potentiel, on associe à $\mathcal{K}$ sa capacité $\gamma(\mathcal{K})$, qui est un réel positif. Ce nombre mesure en quelque sorte la "taille" de $\mathcal{K}$ et est défini de la manière suivante :

D'abord, pour toute mesure de probabilité ν sur $\mathcal{K}$, on considère son **énergie** définie par

$$I(\nu) = -\int_{\mathcal{K}}\int_{\mathcal{K}} \ln|x-y| \mathrm{d}\nu(y)\mathrm{d}\nu(x) \quad ;$$

c'est un élément de $\mathbb{R} \cup \{+\infty\}$.

Définition : On pose $V(\mathcal{K}) = \inf\{I(\nu)\ ;\ \nu \text{ probabilité sur } \mathcal{K}\}$. La **capacité** de $\mathcal{K}$ est le réel $\gamma(\mathcal{K}) = e^{-V(\mathcal{K})}$.

Exemples : La capacité d'un cercle est égale à son rayon. La capacité d'un compact dénombrable est nulle.

Fekete [6] et Fekete-Szegö [7] ont découvert que la capacité de $\mathcal{K}$, bien que de nature analytique, est en fait reliée à la présence d'entiers algébriques dont tous les conjugués sont "près" de $\mathcal{K}$:

Lorsque U est une partie de $\mathbb{C}$, on note ici $\mathcal{Y}(U)$ l'ensemble des $\alpha \in \overline{\mathbb{Z}}$ tels que α et tous ses conjugués (par Galois) soient dans U.

Théorème 1.1 (Fekete 1923) : *Soit $\mathcal{K}$ un compact de $\mathbb{C}$ symétrique par rapport à l'axe réel. On suppose $\gamma(\mathcal{K}) < 1$. Il existe un ouvert U de $\mathbb{C}$ contenant $\mathcal{K}$ tel que $\mathcal{Y}(U)$ soit fini. En particulier $\mathcal{Y}(\mathcal{K})$ est fini.*

Théorème 1.2 (Fekete-Szegö 1955) : *Soit $\mathcal{K}$ un compact de $\mathbb{C}$ symétrique par rapport à l'axe réel. On suppose $\gamma(\mathcal{K}) \geqslant 1$. Pour tout ouvert U de $\mathbb{C}$ contenant $\mathcal{K}$, $\mathcal{Y}(U)$ est infini.*

Remarque : Si U est une partie de $\mathbb{C}$, alors $U^* = \{z \in U \mid \overline{z} \in U\}$ est symétrique par rapport à l'axe réel, et on a $\mathcal{Y}(U^*) = \mathcal{Y}(U)$. L'hypothèse de symétrie est donc naturelle et on peut toujours s'y ramener.

Remarque : Sous les hypothèses du théorème 1.2, $\mathcal{Y}(\mathcal{K})$ peut être vide : si $\mathcal{K}$ est un cercle de centre 0 et de rayon transcendant > 1, alors $\gamma(\mathcal{K}) > 1$ mais $\mathcal{K}$ ne contient aucun nombre algébrique.

Après un rappel de théorie du potentiel, on prouvera le théorème 1.1 via la théorie d'Arakelov sur $\mathbb{P}^1_{\mathbb{Z}}$ (*cf* paragraphe 4). On donnera ensuite une démonstration "classique" du théorème 1.2.

La théorie du potentiel se généralise en fait aux surfaces de Riemann compactes. On expliquera au paragraphe 8 comment ceci permet d'étendre les énoncés précédents au cas des surfaces arithmétiques.

Enfin, dans le cas critique $\gamma(\mathcal{K}) = 1$, on montrera un théorème d'équidistribution dû à Bilu [2] et Rumely [11].

Je remercie le rapporteur pour ses suggestions qui m'ont permis d'améliorer la présentation de ce texte.

2 Théorie du potentiel sur $\mathbb{C}$

Pour tout $p \in \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$, on désigne par δ_p la masse de Dirac en p.

Soit $\mathcal{K}$ un compact de $\mathbb{C}$. Lorsque ν est une mesure de probabilité sur $\mathcal{K}$, on pose

$$\forall x \in \mathbb{C} \quad u_\nu(x) = -\int_{\mathcal{K}} \ln|x-y| \mathrm{d}\nu(y) \; .$$

On a les propriétés suivantes (*cf* chapitre 3 de [9]).

Proposition 2.1 : *Soit ν une probabilité sur $\mathcal{K}$. La fonction u_ν est harmonique sur $\mathbb{C} \smallsetminus \mathcal{K}$, sur-harmonique sur $\mathbb{C}$. Au voisinage de ∞, on a $u_\nu(x) = -\ln|x| + O\Big(\frac{1}{|x|}\Big)$. De plus, on a $\frac{i}{\pi}\partial\overline{\partial}u_\nu = \delta_\infty - \nu$ au sens des courants sur $\mathbb{P}^1(\mathbb{C})$.*

Si $\gamma(\mathcal{K}) > 0$ (*i.e.* si $V(\mathcal{K}) \neq +\infty$), il existe une unique mesure de probabilité $\mu_{\mathcal{K}}$ réalisant l'infimum dans $V(\mathcal{K})$; elle est appelée la **mesure à l'équilibre** de $\mathcal{K}$. La fonction $u_{\mu_{\mathcal{K}}}$ est alors notée $u_{\mathcal{K}}$ et est appelée la **fonction potentiel** de $\mathcal{K}$.

Exemple : Si $\mathcal{K}$ est le cercle de centre a et de rayon $r > 0$, alors $u_{\mathcal{K}}(z) = -\ln\max(|z-a|, r)$ pour tout $z \in \mathbb{C}$, et $\mu_{\mathcal{K}}$ est la mesure de Haar sur $\mathcal{K}$.

Proposition 2.2 (Frostman) : *On désigne par $\mathcal{D}$ la composante connexe de $\mathbb{P}^1(\mathbb{C}) \smallsetminus \mathcal{K}$ contenant ∞. Supposons $\gamma(\mathcal{K}) > 0$. Alors :*
- Sur $\mathbb{C} \smallsetminus \overline{\mathcal{D}}$, $u_{\mathcal{K}}$ est constante égale à $V(\mathcal{K})$;
- Sur la frontière $\partial\mathcal{D}$, on a $u_{\mathcal{K}} \leqslant V(\mathcal{K})$ avec inégalité stricte seulement sur une réunion dénombrable de compacts de capacité nulle ;
- Sur $\mathcal{D}$, on a en tout point $u_{\mathcal{K}} < V(\mathcal{K})$.

Remarque : Les compacts $\mathcal{K}$ et $\partial\mathcal{D}$ ont même capacité, même mesure à l'équilibre et même fonction potentiel.

Proposition 2.3 : *Soit $x \in \partial\mathcal{D}$. Notons C la composante connexe de $\mathcal{K}$ contenant x. Si $C \neq \{x\}$, alors $\gamma(\mathcal{K}) > 0$, $u_{\mathcal{K}}$ est continue en x et $u_{\mathcal{K}}(x) = V(\mathcal{K})$.*

Définition : On dit que $\mathcal{K}$ est **à bord continu** lorsque $\mathcal{K}$ est la réunion non vide de parties connexes non réduites à un point.

En résumé, si $\mathcal{K}$ est à bord continu, alors $u_{\mathcal{K}}$ est continue sur $\mathbb{C}$ et constante (égale à $V(\mathcal{K})$) sur $\mathcal{K}$.

3 Lien avec l'intersection arithmétique

Si $\widehat{\mathcal{L}}$ est un fibré en droites hermitien (continu) sur $\mathbb{P}^1_{\mathbb{Z}}$ et D un diviseur sur $\mathbb{P}^1_{\mathbb{Z}}$, on désigne par $\mathrm{h}_{\widehat{\mathcal{L}}}(D)$ la hauteur d'Arakelov de D relativement à $\widehat{\mathcal{L}}$ (*cf* cours de C. Soulé [12]). Lorsque $\widehat{\mathcal{L}}$ et $\widehat{\mathcal{M}}$ sont deux fibrés en droites hermitiens admissibles sur $\mathbb{P}^1_{\mathbb{Z}}$, on note $\langle \widehat{\mathcal{L}}.\widehat{\mathcal{M}} \rangle$ leur nombre d'intersection arithmétique (*cf* cours de Chambert-Loir [3]).

Soit $\mathcal{K}$ un compact de $\mathbb{C}$ invariant par conjugaison complexe. On suppose $\mathcal{K}$ à bord continu. On pose $X = \mathbb{P}^1_{\mathbb{Z}}$ et on munit $\mathcal{L} = \mathcal{O}_X([\infty])$ de la métrique continue $\| \ \|$ vérifiant

$$\forall x \in \mathbb{C} \quad \|1(x)\| = \exp[u_{\mathcal{K}}(x) - V(\mathcal{K})] \ , \qquad (*)$$

où 1 désigne la section globale de $\mathcal{L}$ définie par le diviseur $[\infty]$.

Proposition 3.1 : *Posons $\widehat{\mathcal{L}} = (\mathcal{L}, \| \ \|)$. La courbure de $\widehat{\mathcal{L}}$ est égale à $\mu_{\mathcal{K}}$; en particulier $\widehat{\mathcal{L}}$ est admissible. Et on a la formule $\langle \widehat{\mathcal{L}}.\widehat{\mathcal{L}} \rangle = V(\mathcal{K})$.*

Démonstration : On trouve la courbure de $\widehat{\mathcal{L}}$ en appliquant la proposition 2.1.

Montrons la formule. Munissons $\mathcal{L}$ de la métrique $\| \ \|'$ telle que $\|1(x)\|' = \min\Big(\frac{1}{|x|}, 1\Big)$ pour tout $x \in \mathbb{C}$, et posons $\widehat{\mathcal{L}'} = (\mathcal{L}, \| \ \|')$. On vérifie aisément que $\mathrm{h}_{\widehat{\mathcal{L}'}}([\infty]) = 0$. Par ailleurs, la fonction $\varphi = \ln \frac{\| \ \|'}{\| \ \|}$ est continue sur $\mathbb{P}^1(\mathbb{C})$ et vaut $V(\mathcal{K})$ en ∞. D'après la propriété des hauteurs d'Arakelov (*cf* théorème 2.5 de [3]), on a

$$\langle \widehat{\mathcal{L}}.\widehat{\mathcal{L}} \rangle = \mathrm{h}_{\widehat{\mathcal{L}}}([\infty]) - \int_{\mathbb{P}^1(\mathbb{C})} [u_{\mathcal{K}} - V(\mathcal{K})] \mathrm{d}\mu_{\mathcal{K}} = \mathrm{h}_{\widehat{\mathcal{L}}}([\infty]) \ ,$$

puisque la mesure $\mu_{\mathcal{K}}$ est à support dans $\mathcal{K}$ et la fonction $u_{\mathcal{K}}$ vaut $V(\mathcal{K})$ sur $\mathcal{K}$. En outre, on a $\mathrm{h}_{\widehat{\mathcal{L}}}([\infty]) = \mathrm{h}_{\widehat{\mathcal{L}'}}([\infty]) + \varphi(\infty) = V(\mathcal{K})$. D'où le résultat. □

4 Théorème de Fekete

Théorème 4.1 : *Soit $\mathcal{K}$ un compact de $\mathbb{C}$ invariant par conjugaison complexe. On suppose $\gamma(\mathcal{K}) < 1$. Soit R un réel $> \gamma(\mathcal{K})$. Il existe $P \in \mathbb{Z}[X]$ de degré $d \geqslant 1$ tel que $\forall z \in \mathcal{K}$ $|P(z)| < R^{d/2}$.*

Démonstration : On peut bien sûr se placer dans le cas $R \leqslant 1$. Quitte à agrandir le compact $\mathcal{K}$ (on le recouvre par un nombre fini de petites boules fermées), on peut le supposer à bord continu. Considérons $X = \mathbb{P}^1_{\mathbb{Z}}$ et munissons $\mathcal{L} = \mathcal{O}_X([\infty])$ de la métrique $\| \ \|$ vérifiant $(*)$. Le théorème de Hilbert-Samuel arithmétique (*cf* cours de H. Chen [4]) permet d'estimer le quotient V_n du covolume du réseau $\Gamma(X, \mathcal{L}^{\otimes n})$ par le volume de la boule $\left\{ s \in \Gamma(X, \mathcal{L}^{\otimes n})_{\mathbb{R}} \ \middle| \ \max_{X(\mathbb{C})} \|s\| \leqslant 1 \right\}$:

$$\ln V_n = -\big\langle \widehat{\mathcal{L}}.\widehat{\mathcal{L}} \big\rangle \frac{n^2}{2} + o(n^2) \ .$$

En posant $\varepsilon = \dfrac{1}{2} \ln \dfrac{R}{\gamma(\mathcal{K})}$, le théorème de Minkowski fournit un entier $n \geqslant 1$ et une section $s \in \Gamma(X, \mathcal{L}^{\otimes n}) \smallsetminus \{0\}$ tels que

$$\max_{X(\mathbb{C})} \|s\| \leqslant 2 V_n^{1/(n+1)} < \exp\Big(-\big\langle \widehat{\mathcal{L}}.\widehat{\mathcal{L}} \big\rangle \frac{n}{2} + \varepsilon n \Big) = R^{n/2} \ .$$

La section s définit un polynôme $P \in \mathbb{Z}[X]$ non nul de degré $d \leqslant n$. Alors pour tout $z \in \mathcal{K}$, on a $|P(z)| = \|s(z)\| < R^{n/2} \leqslant R^{d/2}$ (ce qui implique $d \geqslant 1$). □

On en déduit le théorème de Fekete de la manière suivante.

Démonstration de 1.1 : D'après le théorème 4.1, il existe $P \in \mathbb{Z}[X]$ non nul tel que $|P(z)| < 1$ pour tout $z \in \mathcal{K}$. Considérons l'ouvert $U = \{z \in \mathbb{C} \mid |P(z)| < 1\}$, qui contient donc $\mathcal{K}$. Soit $\alpha \in \mathcal{Y}(U)$; notons $\alpha_1, \cdots, \alpha_n$ ses conjugués. La norme $P(\alpha_1) \cdots P(\alpha_n)$ de $P(\alpha)$ est un entier de valeur absolue < 1, donc est nulle. D'où $P(\alpha) = 0$. On en conclut que $\mathcal{Y}(U)$ est contenu dans l'ensemble fini des racines de P. □

Remarquons que l'inégalité du théorème 4.1 est en fait presque optimale :

Proposition 4.2 : *Soit n un entier $\geqslant 1$; désignons par $\mathcal{C}$ le cercle de centre $\dfrac{1}{n}$ et de rayon $\dfrac{1}{n^2}$. Pour tout $P \in \mathbb{Z}[X]$ non nul de degré d, on a $\max_{\mathcal{C}} |P| \geqslant \gamma(\mathcal{C})^{d/2}$.*

Démonstration : Le polynôme $nX - 1$ est irréductible dans $\mathbb{Z}[X]$. On peut donc factoriser P sous la forme $P = (nX - 1)^k Q$ avec $k \in \{0, \cdots, d\}$ et $Q \in \mathbb{Z}[X]$ de degré

$d-k$ vérifiant $Q\Big(\dfrac{1}{n}\Big) \neq 0$. On a alors

$$\begin{aligned} \max_{\mathcal{C}} |P| = \frac{1}{n^k} \max_{\mathcal{C}} |Q| \quad &\geqslant \quad \frac{1}{n^k}\Big|Q\Big(\frac{1}{n}\Big)\Big| \qquad \text{(principe du maximum)} \\ &\geqslant \quad \frac{1}{n^k}\frac{1}{n^{d-k}} = \gamma(\mathcal{C})^{d/2}\ . \quad \square \end{aligned}$$

5 Théorème de Fekete-Szegö

On aura besoin du résultat suivant de théorie du potentiel :

Proposition 5.1 : *Soit $\mathcal{K}$ un compact non vide de $\mathbb{C}$. Soit U un ouvert de $\mathbb{C}$ contenant $\mathcal{K}$. Il existe $P \in \mathbb{C}[X]$ unitaire de degré $k \geqslant 1$ tel que $\forall z \in \mathbb{C} \setminus U\ |P(z)| > \gamma(\mathcal{K})^k$.*

Si $\mathcal{K}$ est invariant par conjugaison complexe, alors on peut imposer à P d'être à coefficients réels.

Démonstration : La première partie de l'énoncé se déduit aisément du théorème 5.5.8 de [9].

Montrons la deuxième partie : on suppose donc $\mathcal{K}$ invariant par conjugaison complexe. Quitte à réduire l'ouvert U, on peut le supposer symétrique par rapport à l'axe réel. D'après la première partie, il existe $P_0 \in \mathbb{C}$ unitaire de degré $k' \geqslant 1$ tel que $|P_0(z)| > \gamma(\mathcal{K})^{k'}$ pour tout $z \in \mathbb{C} \setminus U$. Considérons le polynôme $P \in \mathbb{R}[X]$ caractérisé par la propriété $\forall z \in \mathbb{C}\ P(z) = P_0(z)\overline{P_0(\overline{z})}$. Alors P est unitaire de degré $k = 2k'$. Et pour tout $z \in \mathbb{C} \setminus U$, on a $|P(z)| = |P_0(z)||P_0(\overline{z})| > \gamma(\mathcal{K})^{2k'} = \gamma(\mathcal{K})^k$. $\square$

Théorème 5.2 : *Soit $\mathcal{K}$ un compact de $\mathbb{C}$ invariant par conjugaison complexe. On suppose $\gamma(\mathcal{K}) \geqslant 1$. Soit U un ouvert de $\mathbb{C}$ contenant $\mathcal{K}$. Il existe $P \in \mathbb{Z}[X]$ unitaire de degré $d \geqslant 1$ tel que $\forall z \in \mathbb{C} \setminus U\ |P(z)| > \gamma(\mathcal{K})^d$.*

Démonstration : La proposition 5.1 fournit un $P_0 \in \mathbb{R}[X]$ unitaire de degré $k \geqslant 1$ tel que $|P_0(z)| > \gamma(\mathcal{K})^k$ pour tout $z \in \mathbb{C} \setminus U$. Par compacité de $\mathbb{P}^1(\mathbb{C}) \setminus U$, on a $\inf\limits_{\mathbb{C}\setminus U} |P_0| > \gamma(\mathcal{K})^k$. On approche P_0 par un $P_1 \in \mathbb{Q}[X]$ unitaire de degré k de telle sorte qu'il existe un réel $R > \gamma(\mathcal{K})^k$ vérifiant $\forall z \in \mathbb{C} \setminus U\ |P_1(z)| \geqslant R$.

Pour tout entier $n \geqslant -1$, désignons par $\mathbb{Q}[X]_n$ l'espace des polynômes à coefficients rationnels de degré $\leqslant n$. Posons $T = \max\limits_{z \in \mathbb{C}\setminus U} \sum\limits_{b=0}^{k-1} \dfrac{|z|^b}{|P_1(z)|}$. Observant que $R > 1$, on choisit un entier $v \geqslant 1$ tel que $R^v \geqslant \dfrac{RT}{R-1}$.

L'idée est maintenant de trouver un $n \geqslant v$ et un $P \in \mathbb{Z}[X]$ vérifiant

$$P_1^n - P \in \sum_{a=0}^{n-v-1} \sum_{b=0}^{k-1} \Big[-\frac{1}{2}, \frac{1}{2}\Big] P_1^a X^b\ .$$

Le polynôme P_1 s'écrit $P_1 = X^k + \dfrac{1}{q}Q$ avec $Q \in \mathbb{Z}[X]$ de degré $\leqslant k-1$ et q entier $\geqslant 1$.

Pour tout entier $n \geqslant 1$, on a $P_1^n = \sum_{j=0}^{n} \frac{\mathrm{C}_n^j}{q^j} X^{(n-j)k} Q^j$.

On choisit un entier n multiple de $(vk)!q^{vk}$ et tel que $\left(\frac{R}{\gamma(\mathcal{K})^k}\right)^n > 2$. Pour tout $j \in \{1, \cdots, vk\}$, $\frac{\mathrm{C}_n^j}{q^j}$ est alors un entier. En posant

$$F = \sum_{j=0}^{vk} \frac{\mathrm{C}_n^j}{q^j} X^{(n-j)k} Q^j \quad \text{et} \quad G = \sum_{j=vk+1}^{n} \frac{\mathrm{C}_n^j}{q^j} X^{(n-j)k} Q^j \ ,$$

on a donc $P_1^n = F + G$ avec $F \in \mathbb{Z}[X]$ unitaire de degré $d = nk$ et $G \in \mathbb{Q}[X]_{d-vk-1}$.

On construit 3 suites (c_j), (G_j), (H_j) par récurrence descendante sur j :
On commence par poser $G_{d-vk-1} = G \in \mathbb{Q}[X]_{d-vk-1}$. Soit $j \in \{0, \cdots, d-vk-1\}$. Écrivons j sous la forme $j = ak + b$ avec $0 \leqslant a \leqslant n - v - 1$ et $0 \leqslant b \leqslant k - 1$. Le coefficient de degré j de G_j s'écrit $c_j + \delta_j$ avec c_j entier et $|\delta_j| \leqslant \frac{1}{2}$. On pose alors $H_j = \delta_j P_1^a X^b$ et $G_{j-1} = G_j - c_j X^j - H_j$, de sorte que $H_j \in \mathbb{Q}[X]_j$ et $G_{j-1} \in \mathbb{Q}[X]_{j-1}$. Remarquons que $|H_j(z)| \leqslant \frac{1}{2}|z|^b |P_1(z)|^a$ pour tout $z \in \mathbb{C}$.

On pose finalement $P = F + \sum_{j=0}^{d-vk-1} c_j X^j$; c'est un polynôme à coefficients entiers, unitaire de degré d.

Par construction, on obtient $G_{-1} = 0$ puis $G = G_{d-vk-1} = \sum_{j=0}^{d-vk-1} (c_j X^j + H_j)$. Il en découle la relation $P_1^n - P = \sum_{j=0}^{d-vk-1} H_j$. Soit $z \in \mathbb{C} \setminus U$. Alors on a

$$\begin{aligned} |P_1(z)^n - P(z)| &\leqslant \frac{1}{2}\Big(\sum_{b=0}^{k-1} |z|^b\Big)\Big(\sum_{a=0}^{n-v-1} |P_1(z)|^a\Big) \\ &\leqslant \frac{T}{2}|P_1(z)| \sum_{a=0}^{n-v-1} \frac{|P_1(z)|^{n-1}}{R^{n-1-a}} \leqslant \frac{T|P_1(z)|^n}{2R^{v-1}(R-1)} \leqslant \frac{1}{2}|P_1(z)|^n \ . \end{aligned}$$

On en déduit que $|P(z)| \geqslant \frac{1}{2}|P_1(z)|^n \geqslant \frac{R^n}{2} > \gamma(\mathcal{K})^d$. $\square$

Prouvons maintenant le théorème de Fekete-Szegö.

Démonstration de 1.2 : D'après le théorème 5.2, il existe $P \in \mathbb{Z}[X]$ unitaire de degré $d \geqslant 1$ tel que $|P(z)| > 1$ pour tout $z \in \mathbb{C} \setminus U$. Soit n un entier $\geqslant 1$. On note Φ_n le n-ième polynôme cyclotomique et on choisit une racine α_n du polynôme unitaire $\Phi_n \circ P$. Pour tout conjugué β de α_n, $P(\beta)$ est une racine de l'unité, donc de module 1 ; en particulier $\beta \in U$. On en déduit que α_n est un élément de $\mathcal{Y}(U)$. En outre $P(\alpha_n)$ est d'ordre n dans le groupe $\mathbb{C}^*$. Les $(\alpha_n)_{n \geqslant 1}$ sont donc distincts deux à deux. $\square$

6 Théorie du potentiel sur les courbes

Soit M une surface de Riemann compacte connexe, munie d'une forme volume μ de masse totale 1.

Soit p un point de M. Rappelons que la **fonction de Green** pour p est l'unique fonction g_p de classe C^∞ sur $M \setminus \{p\}$ telle que :
- Dans une carte (U, z) contenant p, on ait $g_p = -\ln|z - z(p)| + \varphi$, où φ est C^∞ sur U ;
- Sur $M \setminus \{p\}$, on ait $\dfrac{i}{\pi}\partial\overline{\partial} g_p = \mu$;
- On ait $\displaystyle\int_M g_p \mu = 0$.

Pour tout $(x, y) \in M^2$ tel que $x \neq y$, on pose $g(x, y) = g_x(y)$. La fonction g ainsi définie est de classe C^∞ sur $M \times M \setminus \Delta$, où Δ désigne la diagonale de $M \times M$. Et on a $g(x, y) = g(y, x)$ pour tout $(x, y) \in M^2 \setminus \Delta$.

Pour tout $(p, x, y) \in M^3$ tel que $y \neq p$, on pose $[x, y]_p = \exp[g(x, p) + g(y, p) - g(x, y)]$. Ceci mesure la "pseudo-distance" entre x et y (c'est l'analogue de la distance induite par la valeur absolue sur $\mathbb{C}$; le point p joue le rôle de ∞).

Fixons maintenant un compact $\mathcal{K}$ de M et un point p de $M \setminus \mathcal{K}$. Lorsque ν est une mesure de probabilité sur $\mathcal{K}$, on pose

$$\forall x \in M \quad u_\nu(x) = -\int_{\mathcal{K}} \ln[x, y]_p \mathrm{d}\nu(y) \ .$$

On a les propriétés suivantes (*cf* chapitre 3 de [10]).

Proposition 6.1 : *Soit ν une probabilité sur $\mathcal{K}$. La fonction u_ν est harmonique sur $M \setminus (\mathcal{K} \cup \{p\})$, sur-harmonique sur $M \setminus \{p\}$. Au voisinage de p, on a $u_\nu = -g_p + \varphi$ avec φ de classe C^∞ au voisinage de p et nulle en p. De plus, on a $\dfrac{i}{\pi}\partial\overline{\partial} u_\nu = \delta_p - \nu$ au sens des courants sur M.*

On définit ensuite l'**énergie** de ν :

$$I(\nu) = \int_{\mathcal{K}} u_\nu \mathrm{d}\nu = -\int_{\mathcal{K}}\int_{\mathcal{K}} \ln[x, y]_p \mathrm{d}\nu(y)\mathrm{d}\nu(x) \ .$$

Définition : On pose $V_p(\mathcal{K}) = \inf\{I(\nu) \ ; \ \nu \text{ probabilité sur } \mathcal{K}\}$. La **capacité** de $\mathcal{K}$ par rapport à p est le réel $\gamma_p(\mathcal{K}) = e^{-V_p(\mathcal{K})}$.

Si $\gamma_p(\mathcal{K}) > 0$, il existe une unique mesure de probabilité $\mu_{\mathcal{K},p}$ réalisant l'infimum dans $V_p(\mathcal{K})$; elle est appelée la **mesure à l'équilibre** de $\mathcal{K}$ par rapport à p. On pose alors $g_{\mathcal{K},p}(x) = V_p(\mathcal{K}) - u_{\mu_{\mathcal{K},p}}(x)$ pour tout $x \in M \setminus \{p\}$. La fonction $g_{\mathcal{K},p}$ et la mesure $\mu_{\mathcal{K},p}$ ne dépendent pas du choix de μ.

Proposition 6.2 : *On note $\mathcal{D}_p$ la composante connexe de $M \setminus \mathcal{K}$ contenant p. Supposons $\gamma_p(\mathcal{K}) > 0$. Alors :*

- Sur $M \setminus \overline{\mathcal{D}_p}$, $g_{\mathcal{K},p}$ est nulle ;
- Sur $\partial\mathcal{D}_p$, on a $g_{\mathcal{K},p} \geqslant 0$ avec inégalité stricte seulement sur une réunion dénombrable de compacts de capacité nulle ;
- Sur $\mathcal{D}_p$, on a en tout point $g_{\mathcal{K},p} > 0$.

Proposition 6.3 : *Soit $x \in \partial\mathcal{D}_p$. Désignons par C la composante connexe de $\mathcal{K}$ contenant x. Si $C \neq \{x\}$, alors $\gamma_p(\mathcal{K}) > 0$, $g_{\mathcal{K},p}$ est continue en x et $g_{\mathcal{K},p}(x) = 0$.*

Définition : On dit que $\mathcal{K}$ est **à bord continu** lorsque $\mathcal{K}$ est la réunion non vide de parties connexes non réduites à un point.

Pour toute partie finie Z de $M \setminus \mathcal{K}$, on posera

$$g_{\mathcal{K},Z} = \sum_{p \in Z} g_{\mathcal{K},p} \ , \quad \mu_{\mathcal{K},Z} = \sum_{p \in Z} \mu_{\mathcal{K},p} \quad \text{et} \quad \delta_Z = \sum_{p \in Z} \delta_p \ .$$

7 Points entiers

Soit K un corps de nombres. On note G_K l'ensemble des plongements $\sigma : K \hookrightarrow \mathbb{C}$. Soit X une surface arithmétique sur O_K, *i.e.* un schéma intègre, régulier, projectif et plat sur O_K, tel que la fibre générique X_K soit une courbe géométriquement irréductible sur K.

Remarque : Soit Y un fermé intègre de X. On a deux possibilités :
- Y est plat et surjectif sur $B = \mathrm{Spec}(O_K)$; Y est alors dit **horizontal** ;
- Y est au-dessus d'un point fermé de B ; Y est alors dit **vertical**.

Définition : Soit V un ouvert de X. Un **point entier** sur V est un fermé E intègre horizontal (de X) de dimension 1 contenu dans V. E est alors affine : $E = \mathrm{Spec}(A)$, avec un ordre A d'un corps de nombres $k(E)$.

Exemple : L'ensemble des points entiers sur $\mathbb{P}^1_{\mathbb{Z}} \setminus [\infty]$ est en bijection naturelle avec l'ensemble des entiers algébriques modulo l'action du groupe de Galois absolu de $\mathbb{Q}$.

Définition : Soient $\widehat{\mathcal{L}}$ un fibré en droites hermitien (continu) sur X et E un point entier sur X. La **hauteur normalisée** de E relativement à $\widehat{\mathcal{L}}$ est le réel

$$\mathrm{h}'_{\widehat{\mathcal{L}}}(E) = \frac{\mathrm{h}_{\widehat{\mathcal{L}}}(E)}{[k(E):K]} \ .$$

Rappelons qu'à tout diviseur d'Arakelov continu $\widehat{D} = (D, g_0)$ sur X, on associe le fibré en droites $\mathcal{O}_X(D)$ muni de la métrique continue $\| \ \|$ telle que $\|1_D(x)\| = e^{-g_0(x)}$ pour tout $x \in X(\mathbb{C}) \setminus |D_{\mathbb{C}}|$, où 1_D désigne la section rationnelle de $\mathcal{O}_X(D)$ définie par le diviseur D. On note $\widehat{\mathcal{O}}_X(D, g_0)$ ce fibré en droites hermitien (continu) sur X.

Lorsque $\widehat{D}_1$ et $\widehat{D}_2$ sont deux diviseurs d'Arakelov admissibles sur X, on désignera par $\langle \widehat{D}_1.\widehat{D}_2 \rangle$ leur nombre d'intersection arithmétique (*cf* cours de Chambert-Loir [3]).

8 Théorèmes de Rumely

Soient K un corps de nombres et X une surface arithmétique sur O_K. On se donne un fermé Z de X purement de dimension 1 tel que $Z(\mathbb{C})$ ne soit pas vide, et un compact $\mathcal{K}$ de $X(\mathbb{C})$ invariant par conjugaison complexe. On suppose que pour tout $\sigma \in G_K$, le compact $\mathcal{K}_\sigma = X_\sigma(\mathbb{C}) \cap \mathcal{K}$ est à bord continu et est disjoint de $Z_\sigma(\mathbb{C})$. On suppose aussi chaque $X_\sigma(\mathbb{C})$ munie d'une forme volume de masse totale 1. On utilise les notations du paragraphe 6.

Notons $Z_1, \cdots, Z_r$ les composantes irréductibles de Z, avec $Z_1, \cdots, Z_q$ horizontales et $Z_{q+1}, \cdots, Z_r$ verticales. Pour tout $i \in \{1, \cdots, q\}$, on désigne par $g_{\mathcal{K},i}$ la fonction sur $X(\mathbb{C})$ égale à $g_{\mathcal{K}_\sigma, Z_{i\sigma}}$ sur chaque $X_\sigma(\mathbb{C})$ et on pose $\widehat{Z}_i = (Z_i, g_{\mathcal{K},i})$. Pour tout $i \in \{q+1, \cdots, r\}$, on pose $\widehat{Z}_i = (Z_i, 0)$.

On pose finalement $a_{ij} = \langle \widehat{Z}_i . \widehat{Z}_j \rangle$ pour tout $(i,j) \in \{1, \cdots, r\}^2$.

Lorsque U est une partie de $X(\mathbb{C})$, on note ici $\mathcal{Y}(U)$ l'ensemble des points entiers E sur $X \setminus Z$ tels que $E(\mathbb{C}) \subset U$. Rumely ([10] théorème 6.3.1) a établi la généralisation suivante du théorème de Fekete :

Théorème 8.1 (Rumely 1989) : *On suppose qu'il existe* $(\lambda_1, \cdots, \lambda_r) \in \mathbb{R}_+^r$ *vérifiant* $\displaystyle\sum_{i=1}^{r} \sum_{j=1}^{r} \lambda_i a_{ij} \lambda_j > 0$. *Il existe un ouvert* U *de* $X(\mathbb{C})$ *contenant* $\mathcal{K}$ *tel que* $\mathcal{Y}(U)$ *soit fini.*

Démonstration : Par densité, on peut supposer que $(\lambda_1, \cdots, \lambda_r) \in \mathbb{Q}_+^{*r}$. Choisissons un entier $m \geqslant 1$ tel que $m\lambda_i$ soit entier pour tout $i \in \{1, \cdots, r\}$. Posons

$$D = \sum_{i=1}^{r} m\lambda_i Z_i \quad \text{et} \quad g_0 = \sum_{i=1}^{q} m\lambda_i g_{\mathcal{K},i} \ .$$

On pose aussi $\widehat{\mathcal{L}} = \widehat{\mathcal{O}}_X(D, g_0)$ et $\varepsilon = \dfrac{\langle \widehat{\mathcal{L}} . \widehat{\mathcal{L}} \rangle}{4 \deg(\mathcal{L}_K)}$. Remarquons que $\varepsilon > 0$ par hypothèse.

On considère l'ouvert $U = \left\{ x \in X(\mathbb{C}) \;\middle|\; g_0(x) < \dfrac{\varepsilon}{[K : \mathbb{Q}]} \right\}$, qui contient donc $\mathcal{K}$. Soit E un point entier sur $X \setminus Z$ tel que $E(\mathbb{C}) \subset U$. Par définition des hauteurs d'Arakelov, on a

$$\mathrm{h}_{\widehat{\mathcal{L}}}(E) = \langle D.E \rangle_{\text{fini}} + \sum_{p \in E(\mathbb{C})} g_0(p) = \sum_{p \in E(\mathbb{C})} g_0(p) < \varepsilon [k(E) : K] \ ,$$

où $\langle D.E \rangle_{\text{fini}}$ désigne le nombre d'intersection de D et E au-dessus des places finies. On vient ainsi de vérifier que $\mathrm{h}'_{\widehat{\mathcal{L}}}(E) < \varepsilon$ pour tout $E \in \mathcal{Y}(U)$. Or d'après le corollaire de Hilbert-Samuel arithmétique (*cf* lemme 7.4 de [3]), X n'admet qu'un nombre fini de points entiers E tels que

$$\mathrm{h}'_{\widehat{\mathcal{L}}}(E) < \frac{\langle \widehat{\mathcal{L}} . \widehat{\mathcal{L}} \rangle}{2 \deg(\mathcal{L}_K)} - \varepsilon = \varepsilon \ .$$

En particulier $\mathcal{Y}(U)$ est fini. □

Rumely a également montré l'extension suivante du théorème de Fekete-Szegö (*cf* théorème 6.3.2 de [10]) :

Théorème 8.2 (Rumely 1989) : *On suppose que* $\sum_{i=1}^{r}\sum_{j=1}^{r}\lambda_i a_{ij}\lambda_j < 0$ *pour tout* $(\lambda_1,\cdots,\lambda_r)\in\mathbb{R}_+^r\smallsetminus\{0\}$. *Pour tout ouvert* U *de* $X(\mathbb{C})$ *contenant* $\mathcal{K}$, $\mathcal{Y}(U)$ *est infini.*

9 Équidistribution dans le cas critique

Lorsque α est un nombre algébrique, on note ici d_α son degré et $\mathrm{O}(\alpha)$ l'ensemble des conjugués de α.

Rumely [11], généralisant un théorème de Bilu [2], a obtenu le résultat d'équirépartition suivant :

Théorème 9.1 (Bilu, Rumely) : *Soit* $\mathcal{K}$ *un compact de* $\mathbb{C}$ *symétrique par rapport à l'axe réel. On suppose* $\mathcal{K}$ *à bord continu et* $\gamma(\mathcal{K})=1$. *Soit* $(\alpha_n)_{n\geqslant 1}$ *une suite d'entiers algébriques distincts deux à deux vérifiant : pour tout ouvert* U *de* $\mathbb{C}$ *contenant* $\mathcal{K}$, *il existe* n_0 *tel que* $\mathrm{O}(\alpha_n)\subset U$ *pour tout* $n\geqslant n_0$. *Alors la suite de mesures* $\left(\frac{1}{\mathrm{d}_{\alpha_n}}\delta_{\mathrm{O}(\alpha_n)}\right)_{n\geqslant 1}$ *converge faiblement vers* $\mu_{\mathcal{K}}$, *ce qui signifie que pour toute* $f:\mathbb{P}^1(\mathbb{C})\to\mathbb{R}$ *continue, on a*

$$\lim_{n\to+\infty}\frac{1}{\mathrm{d}_{\alpha_n}}\sum_{\beta\in\mathrm{O}(\alpha_n)}f(\beta)=\int_{\mathbb{C}}f\mathrm{d}\mu_{\mathcal{K}}\ .$$

Démonstration : On pose $X=\mathbb{P}^1_{\mathbb{Z}}$ et $\widehat{\mathcal{L}}=\widehat{\mathcal{O}}_X([\infty],-u_{\mathcal{K}})$. D'après la proposition 3.1, la courbure de $\widehat{\mathcal{L}}$ vaut $\mu_{\mathcal{K}}$, et on a $\langle\widehat{\mathcal{L}}.\widehat{\mathcal{L}}\rangle=0$. Pour tout $n\geqslant 1$, notons E_n l'adhérence de Zariski de α_n dans X, de sorte que E_n est un point entier sur $X\smallsetminus[\infty]$.

Soit ε un réel >0. Appliquons l'hypothèse à l'ouvert $U=\{x\in X(\mathbb{C})\mid u_{\mathcal{K}}(x)>-\varepsilon\}$: il existe n_0 tel que $\mathrm{O}(\alpha_n)\subset U$ pour tout $n\geqslant n_0$. On a alors, pour tout $n\geqslant n_0$:

$$0\leqslant \mathrm{h}_{\widehat{\mathcal{L}}}(E_n)=\langle[\infty].E_n\rangle_{\mathrm{fini}}-\sum_{\beta\in E_n(\mathbb{C})}u_{\mathcal{K}}(\beta)=-\sum_{\beta\in\mathrm{O}(\alpha_n)}u_{\mathcal{K}}(\beta)<\varepsilon[k(E_n):\mathbb{Q}]\ .$$

On vient ainsi de montrer que $\mathrm{h}'_{\widehat{\mathcal{L}}}(E_n)$ converge vers 0 lorsque n tend vers $+\infty$. On conclut par le théorème d'équidistribution (*cf* théorème 8.4 de [3]). □

On peut en fait étendre cet énoncé au cas des surfaces arithmétiques (*cf* proposition 4.7.1 de [1]) :

On reprend les notations du paragraphe 8 concernant K, X, Z, $\mathcal{K}$, les $\widehat{Z}_i$, les a_{ij}. On note de plus $\mu_{\mathcal{K},i}$ la mesure sur $X(\mathbb{C})$ égale, sur chaque $X_\sigma(\mathbb{C})$, à $\mu_{\mathcal{K}_\sigma,Z_{i\sigma}}$.

Proposition 9.2 : *On suppose qu'il existe* $(\lambda_1, \cdots, \lambda_r) \in \mathbb{R}_+^r$ *tel que*

$$\sum_{i=1}^{r}\sum_{j=1}^{r}\lambda_i a_{ij}\lambda_j = 0 \quad \textit{et que} \quad d = \sum_{i=1}^{q}\lambda_i[k(Z_i):K] > 0 \ .$$

Soit $(E_n)_{n\geqslant 1}$ *une suite de points entiers sur* $X \smallsetminus Z$ *distincts deux à deux vérifiant : pour tout ouvert* U *de* $X(\mathbb{C})$ *contenant* $\mathcal{K}$*, il existe* n_0 *tel que* $E_n(\mathbb{C}) \subset U$ *pour tout* $n \geqslant n_0$*. Posons* $e_n = [k(E_n) : K]$ *pour tout* $n \geqslant 1$*. Alors la suite de mesures* $\left(\frac{1}{e_n}\delta_{E_n(\mathbb{C})}\right)_{n\geqslant 1}$ *converge faiblement vers* $\frac{1}{d}\sum_{i=1}^{q}\lambda_i\mu_{\mathcal{K},i}$*.*

Observons que la mesure $\frac{1}{d}\sum_{i=1}^{q}\lambda_i\mu_{\mathcal{K},i}$ ne dépend pas du choix de $(\lambda_1, \cdots, \lambda_r)$.

Références

[1] *P. Autissier :* Points entiers sur les surfaces arithmétiques. Journal für die reine und angewandte Math. **531** (2001), p. 201-235.

[2] *Y. Bilu :* Limit distribution of small points on algebraic tori. Duke Math. Journal **89** (1997), p. 465-476.

[3] *A. Chambert-Loir :* Arakelov geometry, heights, equidistribution, and the Bogomolov conjecture. Ce volume (2020).

[4] *H. Chen :* Introduction aux théorèmes de Hilbert-Samuel arithmétiques. Ce volume (2020).

[5] *R. Dujardin :* Some problems of arithmetic origin in rational dynamics. Ce volume (2020).

[6] *M. Fekete :* Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten. Math. Zeitschrift **17** (1923), p. 228-249.

[7] *M. Fekete, G. Szegö :* On algebraic equations with integral coefficients whose roots belong to a given point set. Math. Zeitschrift **63** (1955), p. 158-172.

[8] *P.M. Gruber, C.G. Lekkerkerker.* Geometry of numbers (second edition). North-Holland Math. Library **37** (1987).

[9] *T. Ransford :* Potential theory in the complex plane. LMS Student Texts **28** (1995).

[10] *R. Rumely :* Capacity theory on algebraic curves. Lecture Notes in Math. **1378** (1989).

[11] *R. Rumely :* On Bilu's equidistribution theorem. Contemporary Math. **237** (1999), p. 159-166.

[12] *C. Soulé :* Arithmetic intersection. Ce volume (2020).

Pascal Autissier. I.M.B., université de Bordeaux, 351, cours de la Libération, 33405 Talence cedex, France.

pascal.autissier@math.u-bordeaux.fr