Dynamique arithmétique

Serge Cantat

Master 2 de mathématiques fondamentales · Université de Rennes 1
Notes prises par Téofil Adamski (version du 11 décembre 2022)

UNIVERSITÉ DE RENNES 1

Sommaire

Première partie

MÉTHODES P-ADIQUES

Chapitre 1
Théorème de Skolem-Mahler-Lech

Dans cette introduction, on fixe un corps k et un entier $m \geqslant 1$. Notons $\mathbf{A}_k^m$ l'espace affine de dimension m sur le corps k. Une application $f\colon \mathbf{A}_k^m \longrightarrow \mathbf{A}_k^m$ est *polynomiale* s'il existe des polynômes $P_1, \ldots, P_m \in k[X_1, \ldots, x_m]$ tels que

$$f(x_1, \ldots, x_m) = (P_1(x_1, \ldots, x_m), \ldots, P_m(x_1, \ldots, x_m)), \qquad (x_1, \ldots, x_m) \in \mathbf{A}_k^m.$$

Le composée de deux applications polynomiales est encore polynomiale. Les éléments inversibles pour la composition, appelés des *automorphismes polynomiaux* de l'espace affine $\mathbf{A}_k^m$, forment un groupe $\mathrm{Aut}(\mathbf{A}_k^m)$.

Exemple. La fonction $x \longmapsto x + x^3$ est une application polynomiale bijective de l'espace affine $\mathbf{A}_{\mathbf{R}}^1$, mais ce n'est pas un automorphisme. En effet, si cette application admettait un inverse g, alors l'identité $f \circ g = g \circ f = \mathrm{id}_{\mathbf{A}_{\mathbf{R}}^1}$ serait également vraie sur $\mathbf{C}$ alors que l'application $f\colon \mathbf{C} \longrightarrow \mathbf{C}$ n'est même pas bijective.

Dans l'exemple précédent, on peut aussi utiliser un argument sur les degrés pour montrer que l'application f n'admet pas d'inverse, mais cet argument ne fonctionne qu'en dimension une.

Exemple. Soit $q \in k[y]$ un polynôme. Alors l'application polynomiale $(x, y) \longmapsto (x + q(y), y)$ est un automorphisme d'inverse $(x, y) \longmapsto (x - q(y), y)$. On remarque ici que le degré des ces polynômes est supérieur à 1.

Soit $W \subset \mathbf{A}_k^m$ une sous-variété algébrique, c'est-à-dire un sous-ensemble défini par des équations polynomiales $Q_i(x_1, \ldots, x_m) = 0$ pour une famille $(Q_i)_{i \in I}$ de polynômes. Soient $x \in \mathbf{A}_k^m$ un point et $f \in \mathrm{Aut}(\mathbf{A}_k^m)$ un automorphisme. On définit l'ensemble

$$\mathrm{Pas}_f(x, W) \coloneqq \{n \in \mathbf{Z} \mid f^n(x) \in W\}.$$

L'*orbite* du point x sous l'action de l'automorphisme f est la suite $(f^n(x))_{n \in \mathbf{N}}$ et l'*orbite totale* est la suite $(f^n(x))_{n \in \mathbf{Z}}$.

Théorème 1.1 *(Skolem-Malher-Lech, Belle-Glioca-Tucken).* Soit k un corps de caractéristique nulle. Soient $W \subset \mathbf{A}_k^m$ une sous-variété algèbrique, $x \in \mathbf{A}_k^m$ un point et $f \in \mathrm{Aut}(\mathbf{A}_k^m)$ un automorphisme. Alors l'ensemble $\mathrm{Pas}_f(x, W)$ est une union finie de progressions arithmétiques.

1.1. Problème du centre

Soit $\sum_{n \geqslant 1} a_n z^n$ une série entière complexe de rayon de convergence strictement positif R. On note f sa somme sur le disque centré en l'origine et de rayon R. Notons $\lambda \coloneqq f'(0) = a_1$. Considérons

l'homothétie $h_\lambda \colon z \in \mathbf{C} \longmapsto \lambda z$. Si $|\lambda| < 1$, alors les orbites de l'application h_λ tendent vers 0. Si $|\lambda| > 1$, alors elles partent à l'infini sauf celle de l'origine.

On suppose que $|\lambda| = 1$. Alors les orbites sont confinées dans les cercles centrés en l'origine. Soit $\theta \in \mathbf{R}/\mathbf{Z}$ l'angle vérifiant $\lambda = e^{2i\pi\theta}$. Si ce dernier appartient à $\mathbf{Q}/\mathbf{Z}$, alors l'application h_λ est d'ordre fini est toute orbite est périodique. Mais s'il appartient à $(\mathbf{R}\setminus\mathbf{Q})/\mathbf{Z}$, alors l'orbite $(h_\lambda^n(z_0))_{n\in\mathbf{N}}$ pour $z_0 \in \mathbf{C}$ est dense dans le cercle centré en l'origine et de rayon $|z_0|$, c'est-à-dire que l'ensemble des réels $n\theta + m$ avec $n \in \mathbf{N}$ et $m \in \mathbf{Z}$ est dense dans $\mathbf{R}$.

Problème. Peut-on trouver une série entière $\sum_{n\in\mathbf{N}} c_n z^n$ de rayon de convergence strictement positif tel que sa somme φ vérifie

(i) $\varphi(0) = 0$;
(ii) $\varphi'(0) = 1$;
(iii) $f \circ \varphi = \varphi \circ h_\lambda$?

Les conditions (i) et (ii) imposent qu'au voisinage de l'origine, l'application φ est un difféomorphisme. La condition (iii) signifie alors que l'application φ conjugue localement les applications f et h_λ. Si on arrive à construire une telle application φ, avec le précédent paragraphe, on comprend parfaitement les orbites de l'application f.

Remarque. Si l'application φ vérifie les points

(i) $\varphi(0) = 0$;
(ii′) $\varphi'(0) \neq 0$;
(iii) $f \circ \varphi = \varphi \circ h_\lambda$,

alors l'application $\varphi \circ h_\beta$ avec $\beta \in \mathbf{C}$ les vérifie encore. Ainsi en choisissant $\beta = 1/\varphi'(0)$, on obtient une application vérifiant les points (i), (ii) et (iii).

Remarque. Lorsque l'angle θ est rationnel et $\lambda \coloneqq e^{2i\pi\theta}$, alors il existe un entier $k \geqslant 1$ tel que $h_\lambda^k = \mathrm{id}$. Par conséquent, si l'application φ existe, alors $f^k = \mathrm{id}$ sur un voisinage de l'origine.

Par exemple, si $f(z) = \lambda z + a_2 z^2 + \cdots + a_d z^d$ est un polynôme de degré $d \geqslant 2$ avec $\lambda = e^{2i\pi\theta}$ et $\theta \in \mathbf{Q}/\mathbf{Z}$, alors une telle application φ n'existe pas. En effet, sinon il existe un entier $k \geqslant 1$ tel que $f^k(z) - z = 0$ pour tout complexe z suffisamment proche de l'origine ce qui est impossible puisque le polynôme $f^k(z) - z$ est de degré d^k.

Théorème 1.2 *(Siegel).* Soit $\theta \in (\mathbf{R} \setminus \mathbf{Q})/\mathbf{Z}$ un angle vérifiant

$$\left|\theta - \frac{p}{q}\right| \geqslant \frac{1}{q^{2+\varepsilon}}$$

pour un réel $\varepsilon > 0$. On suppose que $\lambda = e^{2i\pi\theta}$. Alors l'application φ existe.

Si l'application φ existe, on dit que l'application f est *linéarisable* et que l'application φ est *linéarisante*.

1.2. Ensembles invariants

Théorème 1.3 *(lemme de Scharz).* Soit $h \colon \mathbf{D} \longrightarrow \mathbf{D}$ une application holomorphe telle que $h(0) = 0$. Alors

- $|h'(0)| \leqslant 1$;
- si $|h'(0)| = 1$, alors il existe un nombre $\beta \in \mathbf{C}$ de module 1 vérifiant $h(z) = \beta z$ pour $z \in \mathbf{D}$;
- si $|h'(0)| < 1$, alors $|h(z)| < |z|$ pour $z \in \mathbf{D}$.

Démonstration. On peut écrire $h(z) = \sum_{n\geqslant 1} a_n z^n$ avec rayon de convergence $\geqslant 1$. La fonction g définie par $g(z) = h(z)/z$ est encore une application holomorphe $\mathbf{D} \longrightarrow \mathbf{C}$ et elle vérifie $g(0) = h'(0)$. Pour tout réel $r < 1$ et tout complexe z tel que $|z| = r$, on peut écrire

$$|g(z)| = \frac{|h(z)|}{|z|} \leqslant \frac{1}{r}.$$

Le principe du maximum fournit alors que $|g(z)| \leqslant 1/r$ pour $|z| \leqslant 1$. En faisant $r \longrightarrow 1$, on obtient

$$\forall z \in \mathbf{D}, \qquad |g(z)| \leqslant 1.$$

On obtient alors $|h'(0)| \leqslant 1$. Par ailleurs, si $|h'(0)| = 1$, alors la fonction $|g|$ atteint son maximum sur le disque ouvert $\mathring{\mathbf{D}}$, donc elle est constante ce qui montre le deuxième point. Le troisième point se montre de la même manière. ◇

Proposition 1.4. On suppose $f(z) = \sum_{n\geqslant 1} a_n z^n$ de rayon de convergence strictement positif avec $\lambda \coloneqq a_1 = f'(0) = e^{2i\pi\theta}$. Alors les propriétés suivantes sont équivalentes :

(i) f est linéarisable au voisinage de 0 ;
(ii) il existe un ouvert borné $U \subset \mathbf{D}_{r(f)}$ contenant 0 tel que $f^{-1}(U) = U = f(U)$.

Démonstration. On suppose le point (i). Il suffit de prendre $U = \varphi^{-1}(\mathbf{D}_s)$ pour un réel assez petit $s > 0$.

Réciproquement, on suppose le point (ii). Soit U_0 la composante connexe de U contenant 0. Par le théorème d'uniformisation de Riemann, le revêtement universel de U_0 est un disque $\tilde{U}_0 \simeq \mathbf{D}$ par une difféomorphisme holomorphe.

$$\begin{array}{ccc} U_0 & \longrightarrow & \mathbf{D} \\ {\scriptstyle\pi}\downarrow & \swarrow{\scriptstyle\pi} & \\ U_0 & & \end{array}$$

L'application f induit une application $U \longrightarrow U$ qui permute les composantes connexes et fixe 0, donc on obtient $f(U_0) \subset U_0$. De plus, il existe un unique $\tilde{f}\colon \mathbf{D} \longrightarrow \mathbf{D}$ qui fasse commuter le diagramme suivant.

$$\begin{array}{ccc} \mathbf{D} & \xrightarrow{\tilde{f}} & \mathbf{D} \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ U_0 & \xrightarrow{f} & U_0 \end{array}$$

Alors la fonction $\tilde{f}$ est holomorphe et elle vérifie $\tilde{f}'(0) = f'(0)$ car $\pi'(0) \neq 0$, donc $|\tilde{f}'(0)| = 1$. Par le lemme de Schwarz, on a donc $\tilde{f}(z) = \lambda\,\mathrm{id}$ avec $\lambda \in \mathbf{C}$. On pose alors $\varphi = h_{1/\varphi'(0)} \circ \pi$. ◇

1.3. Phénomène de Cremer

Théorème 1.5 *(Cremer).* Soit $f(z) = \lambda z + a_2 z^2 + \cdots + a_d z^d$ un polynôme de degré d avec $f(0) = 0$ et $\lambda \coloneqq f'(0)$. On suppose que

$$|\lambda^q - 1|^{1/d^q}$$

tend vers 0 le long d'une sous-suite $q_i \longrightarrow +\infty$. Alors la fonction f n'est pas linéarisable.

Remarque. Si $\lambda = e^{2i\pi\theta}$, alors $\lambda^q = e^{2i\pi q\theta}$ et $|\lambda^q - 1| \sim 2\pi\,\mathrm{dist}_{\mathbf{R}/\mathbf{Z}}(q\theta, 0)$.

Exercice 1. On prend $\theta = 10^{-k_1} + \cdots + 10^{-k_n} + \cdots$ avec $k_{j+1}/d^{k_j} \longrightarrow 0$. Montrer que $\lambda = e^{2i\pi\theta}$ vérifie le théorème.

Démonstration. Le cas $\theta \in \mathbf{Q}/\mathbf{Z}$ a déjà été vu. On suppose $\theta \in (\mathbf{R} \setminus \mathbf{Q})/\mathbf{Z}$. Si la fonction f est linéarisable sur un voisinage U de l'origine, alors le seul point périodique de la fonction f dans U est l'origine car l'homothétie h_λ n'a que ce dernier comme point périodique. Donc s'il existe une suite $z_i \longrightarrow 0$ de points périodiques deux à deux distincts, alors la fonction f n'est pas linéarisable.

On cherche donc les points périodiques de période divisant q, c'est-à-dire à résoudre l'équation $f^q(z) = z$. On suppose tout d'abord que $f(z) = \lambda z + a_2 z^2 + \cdots + a_{d-1} z^{d-1} + z^d$. L'équation $f^q(z) - z = 0$ est de la forme $z^{d^q} + \cdots + (\lambda^q - 1)z = 0$, c'est-à-dire $z(z - z_1) \cdots (z - z_{d^q - 1}) = 0$. Les nombres z_j sont les points périodiques de la fonction f de période divisant q et

$$|\lambda^q - 1| = \prod_{j=1}^{d^q - 1} |z_j| \,.$$

Si un nombre z_j réalise le minimum des quantités $|z_i|$, alors

$$|z_j| \leqslant |\lambda^q - 1|^{1/(d^q - 1)},$$

donc on peut trouver une suite de points périodiques qui tend vers 0 par hypothèse. Le cas général se ramène ensuite au cas particulier (voir ci-dessous). ◇

Remarque. Soit $f = \sum_{n \geqslant 1} a_n z^n$ une série de rayon de convergence > 0 avec $a_1 = \lambda = e^{2i\pi\theta} \neq 0$. Soit $\psi = \sum_{n \geqslant 1} a_n z^n$ une série de rayon de convergence > 0 avec $b_1 \neq 0$. Alors le théorème d'inversion locale assure qu'il existe une série entière $\psi^{-1} = \sum_{n \geqslant 1} b'_n z^n$ de rayon de convergence > 1 telle que $\psi \circ \psi^{-1}(z) = \psi^{-1} \circ \psi(z) = z$ au voisinage de 0. On pose $g \coloneqq \psi \circ f \circ \psi^{-1}$. Alors

- $g'(0) = \lambda$;
- la fonction f est linéarisable si et seulement si la fonction g l'est.

Remarque. Dans le groupe des germes de difféomorphismes holomorphes au voisinage de 0

$$\mathrm{Diff}^\omega(\mathbf{C}, 0) \coloneqq \{\sum_{n \geqslant 1} a_n z^n \mid a_1 \neq 0,\ R > 0\},$$

un élément est linéarisable si et seulement sisa classe de conjugaison contient une homothétie.

Application. Soit $f(z) = a_1 z + \cdots + a_d z^d$ un polynôme avec $a_d \neq 0$. Alors sa conjuguée par une homothétie h_μ s'écrit

$$\mu h(hz/\mu) = a_1 a + \cdots + \frac{\mu}{\mu^d} a_d z^d.$$

Si $d \geqslant 2$, on peut alors choisir le complexe μ tel que $a_d = \mu^{d-1}$. Ainsi le polynôme f est conjugué à un polynôme unitaire. Ceci permet de conclure la preuve du théorème de Cremer.

1.4. Seconde version du théorème de Cremer

Définition 1.6. Une partie $\Omega \subset \mathbf{R}/\mathbf{Z}$ est *générique* s'il contient une intersection dénombrable d'ouvert dense de $\mathbf{R}/\mathbf{Z}$.

Exemple. Soit $(\varepsilon(q))_{q \geqslant 1}$ une suite décroissante de réels strictement positifs qui tend vers 0. On considère l'ensemble

$$B \coloneqq \{\theta \in \mathbf{R}/\mathbf{Z} \mid |\theta - r| < \varepsilon(q) \text{ pour une infinité de rationnel } r\}$$

où, pour un élément $\theta \in \mathbf{R}/\mathbf{Z}$, on a posé

$$|\theta - r| \coloneqq \infty\{|\theta - p/q - m| \mid m \in \mathbf{Z}\}.$$

Alors l'ensemble B est générique puisqu'on peut l'écrire

$$B = \bigcap_{q_0 \geqslant 1} B(q_0) \quad \text{avec} \quad B(q_0) \coloneqq \left\{ \theta \in \mathbf{R}/\mathbf{Z} \;\middle|\; \exists q \geqslant q_0,\ \exists p \in \mathbf{Z}^*,\ \left|\theta - \frac{p}{q}\right| < \varepsilon(q_0) \right\}$$

où les ensembles

$$B(q_0) = \bigcup_{\substack{p/q \in \mathbf{Q} \\ q \geqslant q_0}} \left]\frac{p}{q} - \varepsilon(q_0), \frac{p}{q} + \varepsilon(q_0)\right[$$

est un ouvert dense.

Exercice 2. On prend $\varepsilon(q) = 2^{-q!}$. Montrer que tout élément $\theta \in B$ vérifie la propriété de Cremer.

Ainsi la propriété de Cremer est satisfait pour des éléments d'un ensemble générique. On dit que la propriété de Cremer est *générique*.

Théorème 1.7 *(Baire).* Une partie générique $\Omega \subset \mathbf{R}/\mathbf{Z}$ est dense.

On donne maintenant une seconde version, plus forte, du théorème de Cremer.

Théorème 1.8 *(Cremer, version 2).* Il existe un ensemble générique $C \subset \mathbf{R}/\mathbf{Z}$ tel que, pour toute fraction rationnelle $f(z) \coloneqq P(z)/Q(z) \in \mathbf{C}(z)$ de degré au moins 2 et pour tout point fixe z_0 vérifiant $f'(z_0) = e^{2i\pi\theta}$ avec $\theta \in C$, la fonction f n'est pas linéarisable au voisinage du point z_0.

Explications. On considère la fonction f comme une application de l'ensemble $\overline{\mathbf{C}} \coloneqq \mathbf{C} \cup \{\infty\}$ dans lui-même. Par ailleurs, lorsque $z_0 \neq \infty$, on peut calculer la quantité $f'(z_0)$. Mais quand $z_0 = \infty$, on fait le changement de variables $z \longmapsto 1/z$ pour se ramener à $z_0 = 0$. Enfin, la fonction f est linéarisable en un point quelconque z_0 s'il existe un ouvert $U \subset \mathbf{C}$ contenant ce point z_0 et un difféomorphisme $\varphi\colon (U, z_0) \longrightarrow (\mathbf{C}, 0)$ qui est holomorphe sur son image tels que

$$\varphi \circ f \circ \varphi^{-1}(z) = \lambda z, \qquad z \in \operatorname{Im} \varphi$$

avec $\lambda \coloneqq e^{2i\pi\theta}$.

Démonstration. On considère l'ensemble $C \coloneqq B$ avec $\varepsilon(q) = 2^{-q!}$.

• *Étape 1.* L'équation $f(z_0) = z_0$ est une équation de degré $d \geqslant 2$ dont le nombre z_0 est une racine simple puisque $f'(z_0) = \lambda \neq 0$. Ainsi elle admet une autre racine $z_1 \in \overline{\mathbf{C}}$. Maintenant, comme l'action du groupe $\mathrm{PGL}(2, \mathbf{C})$ sur la sphère $\overline{\mathbf{C}}$ est 3-transitive, on peut trouver une homographie

$$h(z) = \frac{az + b}{cz + d}$$

telle que $h(z_0) = z_0$ et $h(\infty) = z_1$. Alors la fonction $g \coloneqq h^{-1} \circ f \circ$ fixe l'origine et envoie l'infini sur cette dernière. De plus, cela reste une fraction rationnelle de degré d et de dérivée λ à l'origine.

On écrit $g(z) = P_1(z)/Q_1(z)$. Comme la fonction g envoie l'infini sur l'origine et comme $g'(0) = \lambda$, cela permet d'écrire

$$g(z) = \frac{a_{d-1}z^{d-1} + \cdots + \lambda z}{b_d z^d + \cdots + 1}.$$

Quitte à conjuguer par l'homothétie h_μ avec $\mu^d = b_d$, on peut supposer que

$$g(z) = \frac{a_{d-1}z^{d-1} + \cdots + \lambda z}{z^d + \cdots + 1} = \frac{P_1(z)}{Q_1(z)}.$$

• *Étape 2.* Pour chaque entier $n \geqslant 1$, on écrit

$$g^n(z) = \frac{P_n(z)}{Q_n(z)} = \frac{*z^{d^n-1} + \cdots + \lambda^n z}{z^{d^n} + \cdots + 1}.$$

En effet, il suffit de vérifier que la fonction g^n est de cette forme par récurrence. On obtient alors

$$\begin{aligned}
g^n(z) = z \quad &\Longleftrightarrow \quad P_n(z) - zQ_n(z) = 0 \\
&\Longleftrightarrow \quad *z^{d^n-1} + \cdots + \lambda^n z - z^{d^n+1} - \cdots - z = 0 \\
&\Longleftrightarrow \quad z \times (*z^{d^n} + \cdots + (1 - \lambda^n)) = 0 \\
&\Longleftrightarrow \quad z\prod_{i=1}^{d^n} = 0 \quad \text{avec} \quad \prod_{i=1}^{d^n} |z_i| = |\lambda^n - 1|\,.
\end{aligned}$$

On conclut alors comme dans la preuve du théorème de Cremer. ◇

Chapitre 2
Nombres p-adiques

2.1. Valeurs absolues, corps valués

Définition 2.1. Une *valeur absolue* sur un corps K est une application $|\cdot| \colon K \longrightarrow \mathbf{R}_+$ vérifiant les points suivants :

(i) pour tout élément $x \in K$, on a $|x| = 0 \Leftrightarrow x = 0$;
(ii) pour tous éléments $x, y \in K$, on a $|xy| = |x|\,|y|$;
(iii) pour tous éléments $x, y \in K$, on a $|x + y| \leqslant |x| + |y|$.

Une valeur absolue $|\cdot|$ est *ultramétrique* si, pour tous éléments $x, y \in K$, on a $|x + y| \leqslant \max(|x|\,, |y|)$.

Exercice 3. Soit $|\cdot|$ une valeur absolue. Montrer que, pour tous éléments $x, y \in K$ tels que $|x| \neq |y|$, on a $|x + y| = \max(|x|\,, |y|)$.

Définition 2.2. Le *groupe des valeurs* est le sous-groupe multiplicatif

$$\{|x| \mid x \in K^\times\} \subset \mathbf{R}_+^*.$$

Si le sous-groupe des valeurs est discrets, alors il est de la forme $q^{\mathbf{Z}}$ pour un réel $q > 0$. Par ailleurs, pour deux éléments $x, y \in K$, on pose $\mathrm{dist}(x, y) \coloneqq |x - y|$. Le *disque ouvert* de centre $c \in K$ et de rayon $r > 0$ est l'ensemble

$$\mathbf{D}_r(c) \coloneqq \{x \in K \mid |x - c| < r\}$$

et le *disque fermé* est l'ensemble

$$\overline{\mathbf{D}}_r(c) \coloneqq \{x \in K \mid |x - c| \leqslant r\}.$$

Enfin, on munit l'ensemble K de la topologie induite par la distance dist.

Exercice 4. Montrer que le groupe des valeurs est discret si et seulement si les disques ouverts sont fermés et inversement. On suppose que la valeur absolue est ultramétrique. Montrer que tout point d'un disque en est un centre.

Si l'espace $(K, |\cdot|)$ n'est pas complet, on peut le compléter par la suite de Cauchy.

Exercice 5. Montrer que le complété K' est un corps dans lequel le corps K est dense et tel que la valeur absolue s'étend en une valeur absolue $K' \longrightarrow \mathbf{R}_+$. Montrer que, si le groupe des valeurs de la valeur absolue initiale est discret, alors le groupe des valeurs de l'extension est le même.

Définition 2.3. Deux valeurs absolues sur le corps K sont *équivalentes* si elles induisent la même topologie.

Exemples. Soient $|\cdot|$ et $|\cdot|'$ deux valeurs absolues sur le corps K. Montrer que les points suivants sont équivalents :

(i) elles sont équivalents ;
(ii) pour tout élément $c \in K$ et tout réel $r > 0$, on a $\mathbf{D}(c,1) = \mathbf{D}'(c,1)$;
(iii) il existe une constante $\alpha \in \mathbf{R}^*$ tel que

$$\forall x \in K', \qquad |x| = |x|'^{\alpha}.$$

2.2. Les valeurs absolues p-adiques sur le corps $\mathbf{Q}$

La valeur absolue usuelle $|\cdot|_\infty$ sur $\mathbf{Q}$ induit le complété $\mathbf{R}$. Introduisons une autre valeur absolue. Soit $\mathscr{P} \subset \mathbf{N}$ l'ensemble des nombres pemiers. On fixe un nombre premier $p \in \mathscr{P}$. Tout entier $a \in \mathbf{Z}^*$ s'écrit sous la forme $a = p^r a'$ avec $p \nmid a'$ et on définit

$$|a|_p := p^{-r} = p^{-v_p(a)}.$$

Pour un rationnel $a/b \in \mathbf{Q}$ avec $a \wedge b = 1$, on pose

$$\left|\frac{a}{p}\right|_q := \frac{|a|_p}{|b|_p} \qquad \text{et} \qquad v_p\Big(\frac{a}{b}\Big) := v_p(a) - v_p(b).$$

Enfin, on décrète $|0|_p = 0$.

Théorème 2.4. L'application $|\cdot|_p \colon \mathbf{Q} \longrightarrow \mathbf{R}_+$ est une valeur absolue ultramétrique sur le corps $\mathbf{Q}$ dont le groupe des valeurs est $p^{\mathbf{Z}}$. Par ailleurs, pour tout rationnel $x \in \mathbf{Q}^*$, on a

$$\prod_{p \in \mathscr{P} \cup \{\infty\}} |x|_p = 1.$$

Démonstration. On vérifie aisément les axiomes (i) et (ii). Pour l'axiome (iii), il suffit de remarquer que, si une puissance p^r divise deux entiers a et c, alors elle divise la somme $a + c$. Autrement dit, cela implique que

$$|a + c|_p \leqslant \max(|a|_p, |c|_p).$$

On généralise ensuite aux rationnels. Donc il s'agit d'une valeur absolue ultramétrique. De plus, son groupe des valeurs est $p^{\mathbf{Z}}$ puisque $|1/p^k|_p = p^k$.

Enfin, vérifions la formule du produit. Soit $a \in \mathbf{Q}^*$. On peut alors l'écrire $a = \pm \prod_{p \in \mathscr{P}} p^{v_p(a)}$ et la multiplicativité de la valeur absolue $|\cdot|_\infty$ donne

$$|a|_\infty = \prod_{p \in \mathscr{P}} |p^{v_p(a)}|_\infty = \prod_{p \in \mathscr{P}} p^{v_p(a)} = \prod_{p \in \mathscr{P}} \frac{1}{|a|_p}. \qquad \diamond$$

2.3. Topologie sur le corps $\mathbf{Q}_p$

On note $\mathbf{Q}_p$ le complété du corps $\mathbf{Q}$ pour la valeur absolue $|\cdot|_p$. On cherche à comprendre la topologie du disque unité $\overline{\mathbf{D}} := \overline{\mathbf{D}}(0,1) \subset \mathbf{Q}_p$. On remarque que, pour tout rationnel $a/b \in \mathbf{Q}$ avec $b \wedge p = 1$, on a $|a/p| \leqslant 1$, donc $a/b \in \overline{\mathbf{D}}$. De plus, on trouve l'inclusion $\mathbf{Z} \subset \overline{\mathbf{D}}$, et donc $\overline{\mathbf{Z}} \subset \overline{\mathbf{D}}$.

Montrons même que $\overline{\mathbf{Z}} = \overline{\mathbf{D}}$. Soit $(x_n)_{n \in \mathbf{N}}$ une suite de $\overline{\mathbf{D}}$ qui converge vers une limite $x \in \overline{\mathbf{D}}$. On pose $r := v_p(x)$. Comme le groupe des valeurs est discret, il existe un entier $n_0 \in \mathbf{N}$ tel que

$$\forall n \geqslant n_0, \qquad |x_n|_p = p^{-r}.$$

Donc $r \geqslant 0$ et $x \in \overline{\mathbf{Z}}$.

Lemme 2.5. Soit $b \in \mathbf{Z}^*$ un entier premier avec p. Alors l'élément $1/b \in \mathbf{Q}_p$ est une limite d'éléments de $\mathbf{N}$.

Démonstration. Comme $b \wedge p = 1$, les entiers b et p^k avec $k \geqslant 1$ sont premiers entre eux, donc il existe deux entiers $q_k, c_k \in \mathbf{Z}$ tel que $bc_k = 1 + q_k p^k$ et on obtient

$$\left|\frac{1}{b} - c_k\right| \leqslant p^{-k} \longrightarrow 0. \qquad \diamond$$

Théorème 2.6. Le disque unité fermé $\mathbf{Z}_p$ de $\mathbf{Q}_p$ est

1. un sous-anneau de $\mathbf{Q}_p$;
2. un sous-ensemble compact de $\mathbf{Q}_p$, homéomorphe à l'ensemble de Cantor $\{0,1,\dots,p-1\}^{\mathbf{N}}$;
3. l'adhérence de $\mathbf{N}$ ou de $\mathbf{Z}$ dans $\mathbf{Q}_p$.

Démonstration.

1. Cela résulte de l'inégalité ultramétrique et de la multiplicativité de la valeur absolue.
2. Soit $(a_n)_{n\in\mathbf{N}}$ une suite entière. Alors la série $\sum a_n p^n$ converge dans $\mathbf{Q}^p$ puisque $|a_n p^n| \leqslant 1/p^n$. Son reste vérifie $|\sum_{n\geqslant N} a_n p^n| \leqslant p^{-N}$. Cela donne une application

$$\Sigma\colon \left|\begin{array}{l} \{0,1,\dots,p-1\}^{\mathbf{N}} \longrightarrow \mathbf{Z}_p, \\ \qquad (a_n)_{n\in\mathbf{N}} \longmapsto \displaystyle\sum_{n=0}^{+\infty} a_n p^n. \end{array}\right.$$

On va voir que c'est un homéomorphisme. Cela conclura puisque l'ensemble $\{0,1,\dots,p-1\}^{\mathbf{N}}$ muni de la topologie produit est un ensemble de Cantor.

Remarquons que tout entier positif a s'écrit de manière unique sous la forme

$$a = a_0 + a_1 p + \cdots + a_k p^k$$

pour certains entiers $a_i \in \{0,1,\dots,p-1\}$. Ainsi tout entier positif est dans l'image de l'application Σ.

Maintenant, pour toutes suites distincts $(a_n)_{n\in\mathbf{N}}$ et $(b_n)_{n\in\mathbf{N}}$ de $\{0,1,\dots,p-1\}$, on a

$$\Big|\sum_{n=0}^{+\infty} a_n p^n - \sum_{n=0}^{+\infty} b_n p^n\Big| = p^{-n_0}$$

où l'entier n_0 est le premier indice pour lequel $a_{n_0} \neq b_{n_0}$. Cela montre que l'application Σ est continue et injective.

Par continuité et comme $\overline{\mathbf{N}} = \mathbf{Z}_p$, on sait que l'image de l'application Σ est égale à $\mathbf{Z}_p$. Enfin, comme une application continue bijective entre deux compacts est un homéomorphisme, l'application Σ en est un. ◇

Théorème 2.7. L'anneau $\mathbf{Z}_p$ possède un unique idéal maximal, à savoir l'idéal

$$\begin{aligned} \mathbf{Z}_p^0 \coloneqq p\mathbf{Z}_p &= \{x \in \mathbf{Q}_p \mid |x| \leqslant 1/p\} \\ &= \{x \in \mathbf{Q}_p \mid |x| < 1\}. \end{aligned}$$

De plus, l'anneau $\mathbf{Z}_p$ est principal : tout idéal est de la forme $p^k\mathbf{Z}_p$. Enfin, le corps résiduel $\mathbf{Z}_p/\mathbf{Z}_p^0$ est isomorphe au corps $\mathbf{F}_p$ et on a $\mathbf{Z}_p/p^k\mathbf{Z}_p \simeq \mathbf{Z}/p^k\mathbf{Z}$.

Démonstration. Soit $I \subset \mathbf{Z}_p$ un idéal non nul. Soit $s \in \mathbf{N}$ un entier tel que

$$\sup\{|z| \mid z \in I\} = p^{-s}.$$

Cette borne supérieure étant un maximum, on peut trouver un élément $z_0 \in I$ tel que $|z_0| = p^{-s}$. En posant $x_0 \coloneqq z_0/p^s$, on trouve $|x_0| = 1$. Ainsi l'idéal I contient l'élément $z_0 = p^s x_0$ avec $|x_0| = 1$, donc $I \supset p^s(x_0\mathbf{Z}_p) = p^s\mathbf{Z}_p$ car l'élément x_0 est inversible dans $\mathbf{Z}^p$ puisqu'il est de valeur absolue 1. Réciproquement, on montre que $I \subset p^s\mathbf{Z}_p$. D'où $I = p^s\mathbf{Z}^p$

Montrons que $\mathbf{Z}_p/p^k\mathbf{Z}_p \simeq \mathbf{Z}/p^k\mathbf{Z}$. Mais cet isomorphisme est donné par l'application

$$\sum_{n=0}^{+\infty} a_n p^n \longmapsto \sum_{n=0}^{k-1} a_n p^n.$$ ◇

2.4. Premier théorème d'Ostrowski

Définition 2.8. – La *valeur absolue triviale* sur un corps K est la valeur absolue $|\cdot|$ définie par

l'égalité

$$|x| \coloneqq \begin{cases} 0 & \text{si } x = 0, \\ 1 & \text{sinon.} \end{cases}$$

– Une valeur absolue $|\cdot|$ est *archimédienne* si, pour tous éléments $y \in K$ et $x \in K^\times$, il existe un entier $n \in \mathbf{Z}$ tel que $|nx| \geqslant |y|$.

La valeur absolue triviale induit la topologie discrète sur le corps K.

Exercice 6. Montrer qu'une valeur absolue $|\cdot|$ est archimédienne si et seulement si la partie $|\mathbf{N}|$ n'est pas bornée.

Exercice 7. Montrer qu'une valeur absolue ultramétrique $|\cdot|$ est non archimédienne.

Lemme 2.9. Soit $|\cdot|$ une valeur absolue non archimédienne. Alors elle est ultramétrique.

Démonstration. Soient $x, y \in K$ deux éléments tels que $|x| \geqslant |y|$. On souhaite montrer que $|x+y| \leqslant |x|$. La formule du binôme de Newton donne

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k},$$

donc on obtient

$$|x+y|^n \leqslant \sum_{k=0}^{n} \left|\binom{n}{k}\right| |x|^k |y|^{n-k}.$$

Puisque la valeur absolue est non archimédienne, l'ensemble $|\mathbf{N}|$ est borné, donc tout entier positif est de valeur absolue plus petit que 1 car sinon on aurait un entier $a \in \mathbf{N}$ tel que $|a| > 1$ et alors la suite $(|a^n|)_{n \geqslant 1}$ ne serait pas bornée. Ainsi

$$|x+y|^n \leqslant \sum_{k=0}^{n} |x|^k |y|^{n-k} \leqslant (n+1)|x|^n.$$

En prenant la racine n-ième, on trouve alors

$$|x+y| \leqslant (n+1)^{1/n} |x|$$

ce qui, en passant à la limite, donne $|x+y| \leqslant |x|$. ◇

Corollaire 2.10. Une valeur absolue $|\cdot|$ est ultramétrique si et seulement si elle n'est pas archimédienne si et seulement si $|n| \leqslant 1$ pour tout entier $n \in \mathbf{Z}$.

On en vient au théorème principal de cette partie.

Théorème 2.11 *(Ostrowski, 1916).* Soit $|\cdot|$ une valeur absolue non trivial sur $\mathbf{Q}$.

1. Si elle est ultramétrique, alors elle est équivalente à une valeur absolue p-adique pour $p \in \mathscr{P}$.
2. Si elle est archimédienne, alors elle est équivalente à la valeur absolue $|\cdot|_\infty$.

Démonstration. 1. Comme elle est ultramétrique, on a $|n| \leqslant 1$ pour tout entier $n \in \mathbf{Z}$. Mais comme elle est non triviale, il existe un entier $n \neq 0$ tel que $|n| < 1$. Ainsi il existe un nombre premier p tel que $|p| < 1$. Donc l'ensemble $\{m \in \mathbf{Z} \mid |m| < 1\}$ est un idéal propre de $\mathbf{Z}$ et il contient l'idéal maximal $p\mathbf{Z}$ ce qui implique

$$\{m \in \mathbf{Z} \mid |m| < 1\} = p\mathbf{Z}.$$

Notons $s > 0$ l'unique réel tel que $|p| = 1/p^s$. Maintenant, pour tout entier $m \in \mathbf{Z}$, comme

$$m = \pm \prod_{p_i \neq p} p_i^{v_{p_i}(m)} \times p^{v_p(m)},$$

on a

$$|m| = p^{-s v_m(p)} = |m|_p^s.$$

La même égalité est également vraie sur le corps $\mathbf{Q}$ puisque ce dernier est le corps des fractions de l'anneau $\mathbf{Z}$.

2. Montrons que, pour tous entiers $m, n \geqslant 2$, on a
$$|m|^{1/\log m} = |n|^{1/\log n}.$$
On développe l'entier m en base n : on écrit
$$m = a_0 + a_1 n + \cdots + a_r n^r$$
avec $0 \leqslant a_i \leqslant n-1$. Alors $r \log n \leqslant \log m$. Par ailleurs, on a
$$|m| \leqslant \sum_{i=0}^{r} |a_i|\,|m|^i \leqslant n \sum_{i=0}^{r} |n|^i$$
car tout entier positif est plus grand que sa valeur absolue. Mais comme la valeur absolue est archimédienne, on doit nécessairement avoir $|n| \geqslant 1$ sans quoi la valeur absolue serait bornée sur les entiers. Ainsi
$$|m| \leqslant \Big(\sum_{i=1}^{r} |a_i|\Big)|n|^r \leqslant (r+1)n|n|^r \leqslant \left(1 + \frac{\log n}{\log n}\right) n|n|^{\log m/\log n}.$$
Cette dernière inégalité vaut aussi pour les puissances m^k de l'entier m. En prenant ensuite la racine k-ième et en passant à la limite, on obtient l'inégalité
$$|m|^{1/\log m} \leqslant |n|^{1/\log n}.$$
Cela conclut l'égalité par symétrie.

On prend $n = 2$. On définit le réel $s > 0$ tel que $|2| = 2^s$, c'est-à-dire
$$s := \frac{\log |2|}{\log 2} \leqslant 1.$$
Alors pour tout entier $m \in \mathbf{N}$, l'égalité du dernier paragraphe donne
$$|m|^{1/\log m} = |2|^{1/\log 2},$$
c'est-à-dire $|m| = |m|_\infty^s$. ◇

Chapitre 3
Extensions de corps valués complets

3.1. Espaces vectoriels normés

On considère un corps valué complet K.

Définition 3.1. Une *norme* sur un K-espace vectoriel V est une application $\|\cdot\| : V \longrightarrow \mathbf{R}_+$ vérifiant les points suivants :

- $|v| = 0$ si et seulement si $v = 0$;
- $|zv| = |z|\,\|v\|$;
- $\|v + w\| \leqslant \|v\| + \|w\|$

pour tous vecteurs $v, w \in V$ et tout scalaire $z \in K$.

Exemple. Soit $(v_i)_{i\in I}$ une base d'un K-espace vectoriel V. Alors l'application $\|\cdot\|_{\sup}$ définie par

$$\|v\|_{\sup} \coloneqq \max_{i\in I} |a_i| \quad \text{avec} \quad v = \sum_{i\in I} a_i v_i \in V$$

est une norme sur V. Ce K-espace vectoriel normé V est complet lorsqu'il est de dimension finie.

Proposition 3.2. Soit V un K-espace vectoriel de dimension finie. Soit $(v_1, \dots, v_m)$ une base de V. Alors toute norme $\|\cdot\|$ sur V est équivalente à la norme $\|\cdot\|_{\sup}$, c'est-à-dire qu'il existe deux constantes $a, A > 0$ telles que

$$\forall v \in V, \qquad a\|v\|_{\sup} \leqslant \|v\| \leqslant A\|v\|_{\sup}.$$

En particulier, le K-espace vectoriel normé V est complet et l'application

$$\left|\begin{array}{ccc} K^m & \longrightarrow & V, \\ (a_1, \dots, a_m) & \longmapsto & \displaystyle\sum_{j=1}^{m} a_j v_j \end{array}\right.$$

est un homéomorphisme.

Démonstration. Soit $v \in V$ un vecteur qu'on écrit sous la forme $v = \sum_{i=1}^m a_i v_i$. Alors

$$\|v\| \leqslant \sum_{i=1}^{m} |a_i|\,\|v_i\| \leqslant \max_{1\leqslant i\leqslant m} |a_i| \times \sum_{i=1}^{m} \|v_i\| = \|v\|_{\sup} \sum_{i=1}^{m} \|v_i\|\,.$$

En effectuant une récurrence sur l'entier m, montrer qu'il existe une constante $a > 0$ tel que

$$\forall v \in V, \qquad a\|v\|_{\sup} \leqslant \|v\|.$$

Pour $m = 1$, il suffit de poser $a \coloneqq \|v_1\|$. Soit $m \geqslant 2$ un entier. On suppose que l'inégalité est vérifiée pour des K-espaces vectoriels normés de dimension $< m$. Soit $j \in \{1, \dots, m\}$ un indice. Posons

$$W_j \coloneqq \Big\{ \sum_{i=1}^{m} a_i v_i \in V \;\Big|\; a_j = 0 \Big\}.$$

Alors $V = W_j \oplus Kv_j$. Par ailleurs, muni de la norme $\|\cdot\|$, le K-espace vectoriel W_i est complet et donc fermé dans V. Il en va de même pour l'hyperplan affine $W_j + v_j$. Pour la norme $\|\cdot\|_{\sup}$, avec l'hypothèse de récurrence, l'union $F \coloneqq \bigcup_{j=1}^{m}(W_j + v_j)$ est donc un fermé qui ne contient pas l'origine, donc il existe un réel $a > 0$ tel que la boule centrée en l'origine de rayon a n'intersecte pas ce fermé F. Ainsi

$$\forall w \in F, \qquad \|w\| \geqslant a.$$

Soit $v \in V \setminus \{0\}$ un vecteur non nul qu'on écrit sous la forme $v = \sum_{i=1}^{m} a_i v_i$. On choisit un entier j tel que $|a_j| = \|v\|_{\sup}$. On écrit alors

$$v = a_j \Big(v_j + \sum_{i \neq j} \frac{a_i}{a_j} v_i \Big)$$

de telle sorte que

$$\|v\| = |a_j| \left| v_j + \sum_{i \neq j} \frac{a_i}{a_j} v_i \right| \geqslant a\|v\|_{\sup}$$

ce qui conclut. ◇

3.2. Extension de la valeur absolue : unicité

Soient K un corps valué complet et $L : K$ une extension finie. Supposons que la valeur absolue sur K s'étende en une valeur absolue $|\cdot|_L$ sur L. Alors l'application $|\cdot|_L$ est une norme sur le K-espace vectoriel L. D'après ce qui précède, le K-espace vectoriel normé $(L, |\cdot|_L)$ est donc complet et, si la famille $(v_1, \dots, v_m)$ est une K-base de L, alors il existe des constantes $a, A > 0$ telles que

$$\forall v \in L, \qquad a\|v\|_{\sup} \leqslant |v| \leqslant A\|v\|_{\sup}.$$

Plus généralement, pour tout norme $\|\cdot\|$ sur L, il existe des constantes $a, A > 0$ telles que

$$\forall v \in L, \qquad a\|v\| \leqslant |v| \leqslant A\|v\|.$$

Ainsi la valeur absolue $|\cdot|_L$ est donnée par la limite

$$|x|_L \coloneqq \lim_{n \longrightarrow +\infty} \|x^n\|^{1/n}, \qquad x \in L.$$

Remarque. Soit $\sigma \colon L \longrightarrow L$ un automorphisme préservant K. L'application $x \longmapsto \|\sigma(x)\|_L$ est encore une extension de la valeur absolue $|\cdot|_L$. Ainsi l'unicité donne

$$|\sigma(x)|_L = |\sigma|_L, \qquad x \in L.$$

Ainsi le groupe de Galois de l'extension L/K agit par isométries sur L pour la norme $|\cdot|_L$.

3.3. Norme d'un nombre algébrique

Soit $L : K$ une extension finie. Alors elle est algébrique et tout élément $x \in L \setminus \{0\}$ admet un polynôme minimal unitaire $P_x \in K[t]$. Notons d le degré de ce dernier. Alors

- $K(x) = K[x]$;
- le corps $K(x)$ est une extension algébrique de K de degré d ;
- la famille $(1, x, \dots, x^{d-1})$ est une base du K-espace vectoriel $K(x)$.

En effet, les deux premiers points sont clairs et, pour le troisième, pour chaque élément $y \in K[x]\setminus\{0\}$, on montre que l'application

$$\ell_x : \left| \begin{array}{c} K[x] \longrightarrow K[x], \\ z \longmapsto yz \end{array} \right.$$

est bijective.

Remarquons que le polynôme caractéristique de cette dernière application est le polynôme P_x, donc son déterminant est le produit des racines du polynômes P_x comptées avec multiplicité dans une clôture algébrique $\overline{L}$.

Définition 3.3. La *norme* de l'élément x est la quantité

$$\mathrm{Norme}_{K(x):K}(x) \coloneqq \det(\ell_x).$$

Soit $(y_1, \dots, y_m)$ une base du $K(x)$-espace vectoriel L. Alors la famille

$$(y_1, y_1x, \dots, y_1x^{d-1}, \dots, y_m, y_mx, \dots, y_mx^{d-1})$$

est une base du K-espace vectoriel L et, dans cette dernière, la matrice de l'application

$$\ell_{x,L} : \left| \begin{array}{l} L \longrightarrow L, \\ z \longmapsto yz \end{array} \right.$$

est diagonale par blocs égaux à la matrice compagnon du polynôme P_x, donc

$$\det(\ell_{x,L}) = \det(\ell_x)^m.$$

Définition 3.4. La *norme* de l'élément x sur L est la quantité

$$\mathrm{Norme}_{L:K}(x) \coloneqq \det(\ell_{x,L}) = \mathrm{Norme}_{K(x):K}(x)^{[L:K]/\deg(x)}$$

où $\deg(x) \coloneqq \deg(P_x)$.

Application. Soit $|\cdot|$ une valeur absolue sur K qui en fait un corps complet $\overline{K}$ et qui s'étend à ce dernier. Soient $x \in \overline{K} \setminus \{0\}$ un élément et L un corps de rupture du polynôme P_x. On adjoint les racines x_i du polynôme P_x au corps K. On suppose $x_1 = x$. Pour tout indice i, il existe un automorphisme $\sigma \in \mathrm{Gal}(L : K)$ tel que $\sigma(x_1) = x_i$. Alors

$$|x|_{\overline{K}} = |x|_L = |\sigma(x)|_L = |x_i|_L, \qquad x \in L$$

où $|\cdot|_L$ est la restriction de $|\cdot|_{\overline{K}}$ à $L \subset \overline{K}$. Ainsi tous les conjugués de x ont la même valeurs absolue, c'est-à-dire

$$|x_i|_{\overline{K}} = |x|_{\overline{K}}, \qquad \forall i.$$

Mais alors

$$|\mathrm{Norme}_{K(x):K}(x)|_L = \prod_i |x_i|_L = |x|_L^{\deg(x)}.$$

Comme $\mathrm{Norme}_{K(x)/K}(x) = \pm P_x(0) \in K$, on obtient

$$|x|_{\overline{K}} = |\mathrm{Norme}_{K(x):K}(x)|^{1/\deg(x)}.$$

3.4. Corps valués complets archimédiens

Théorème 3.5 *(Ostrowski).* Soit K un corps valué complet archimédien. Alors $K = \mathbf{R}$ ou $\mathbf{C}$ et la valeur absolue $|\cdot|$ est équivalente à la valeur absolue usuelle si $K = \mathbf{R}$ et au module sur $K = \mathbf{C}$.

Démonstration. Comme le corps K est archimédien, il est de caractéristique nulle, donc il existe une injection $\mathbf{Q} \hookrightarrow K$. On suppose que $\mathbf{Q} \subset K$. Alors la valeur absolue sur $\mathbf{Q}$ est équivalente à la valeur absolue usuelle $|\cdot|_\infty$, c'est-à-dire

$$\forall y \in \mathbf{Q}, \qquad |y| = |y|_\infty^s$$

pour un réel $s > 0$. Mais comme le corps K est complet, il contient alors $\mathbf{R}$ et on obtient

$$\forall y \in \mathbf{R}, \qquad |y| = |y|_\infty^s. \tag{$*$}$$

Pour conclure, il suffit de montrer que l'extension $K : \mathbf{R}$ est algébrique. Soit $x \in K \setminus \{0\}$. Considérons la fonction

$$f : \left| \begin{array}{l} \mathbf{C} \longrightarrow \mathbf{R}, \\ z \longmapsto |x^2 + (z + \overline{z})x + z\overline{z}|. \end{array} \right.$$

Elle est continue. De plus, elle tend vers $+\infty$ lorsque $|z|_\infty \longrightarrow +\infty$ en utilisant la relation $(*)$. Par conséquent, la fonction f atteint son minimum m et l'ensemble $M_x \coloneqq \{z \in \mathbf{C} \mid f(x) = m\}$ est un compact de $\mathbf{C}$. Distinguons alors deux cas.

- Si $m = 0$, alors il existe un élément $z_0 \in \mathbf{C}$ tel que $f(z_0) = 0$, donc l'élément x est racine du polynôme $t^2 - (z_0 + \overline{z_0})x + z_0\overline{z_0} \in \mathbf{R}[t]$, donc il est algébrique sur $\mathbf{R}$.
- On suppose $m > 0$. Soit $\varepsilon \in]0, m[$ un réel. Considérons l'élément $z_0 \in M_x$ de module maximal dans M_x et le polynôme

$$P_\varepsilon \coloneqq t^2 - (z_0 + \overline{z_0})x + z_0\overline{z_0} + \varepsilon \in \mathbf{R}[t].$$

Soient $z_1, z_1' \in \mathbf{C}$ les racines de ce dernier. Alors

- soit $z_1 = |z_1'|$,
- soit $z_1, z_1' \in \mathbf{R}$ et on choisit $|z_1|_\infty \geqslant |z_1'|_\infty$.

Dans les deux cas, on obtient $|z_1|_\infty^2 \geqslant z_0\overline{z_0} + \varepsilon$, donc $z_1 \notin M_x$ et $f(z_1) > M$.

Pour un entier $n \geqslant 0$, on considère le polynôme

$$Q(t) \coloneqq (P_\varepsilon(t) - \varepsilon)^n - (-\varepsilon)^n \in \mathbf{R}[t].$$

Alors $Q(z_1) = 0$ et il est de degré $2n$. Ainsi le polynôme Q admet $2n$ racines z_i comptées avec multiplicités qui sont stable par la conjugaison $w \longmapsto \overline{w}$. Alors

$$Q(t) = \prod_{i=1}^{2n}(t - z_i)(t - \overline{z_i}) = \prod_{i=1}^{2n}(t^2 - (z_i + \overline{z_i})t + z_i\overline{z_i}) = \prod_{i=1}^{2n} f(z_i) \geqslant f(z_1)m^{2m-1}.$$

Par ailleurs, on a $|Q(x)| \leqslant f(z_0)^m + |\varepsilon|^m \leqslant m^n + \varepsilon^n$, donc

$$1 < \frac{f(z_1)}{m} \leqslant 1 + \left(\frac{e}{m}\right)^n \xrightarrow[n \longrightarrow +\infty]{} 1$$

ce qui est impossible. Donc $m = 0$ ce qui conclut. ◇

3.5. Lemmes de Hensel

3.5.1. Norme de Gauss et polynômes primitifs

Soit K un corps muni d'une valeur absolue ultramétrique non triviale. On note R son anneau de valuation. Il possède un unique idéal maximal $R^0 \coloneqq \{x \in K \mid |x| < 1\}$. Son *corps résiduel* est le quotient $k \coloneqq R/R^0$.

Définition 3.6. La *norme de Gauss* d'un polynôme $f \coloneqq a_0 + \cdots + a_d t^d \in K[t]$ est la quantité

$$\|f\| \coloneqq \max_{0 \leqslant i \leqslant d} |a_i|.$$

Lemme 3.7 *(Gauss).* Soient $f, g \in K[t]$ deux polynômes. Alors $\|fg\| = \|f\|\,\|g\|$.

Démonstration. On écrit

$$f = a_0 + \cdots + a_d t^d,$$
$$g = b_0 + \cdots + b_e t^e,$$
$$fg = c_0 + \cdots + c_{d+e} t^{d+e}.$$

Alors $|c_k| \leqslant \|f\|\,\|g\|$ ce qui donne $\|fg\| \leqslant \|f\|\,\|g\|$. Montrons l'autre inégalité. Soient i_0 et j_0 les plus petits indices tels que $|a_{i_0}| = \|f\|$ et $|b_{i_0}| = \|g\|$. Alors

$$c_{i_0+j_0} = a_{i_0}b_{j_0} + \sum_{\substack{i+j=i_0+j_0 \\ i<i_0, j<j_0}} a_i b_j.$$

Avec l'ultramétricité, on obtient alors

$$|c_{i_0+j_0}| = |a_{i_0} b_{j_0}| = \|f\| \, \|g\|$$

ce qui conclut. ◇

Définition 3.8. Un polynôme $f \in R[t]$ est primitif sir $\|f\| = 1$, c'est-à-dire si $f \not\equiv 0 \mod R^0$.

3.5.2. Lemme de Hensel

Théorème 3.9 *(lemme de Hensel).* Soit K un corps valué complet ultramétrique dont la valeur absolue est non triviale. soit $f \in R[t]$ un polynôme primitif. Si $\overline{f}(t) = \overline{g}(t)\overline{h}(t)$ dans $k[t]$ où $\overline{g}, \overline{h} \in k[t]$ sont premiers entre eux, alors il existe $g, h \in R[t]$ tel que

- $f(t) = g(t)h(t)$ dans $R[t]$,
- $\deg g = \deg \overline{g}$,
- $g \equiv \overline{g} \mod R^0$ et $h \equiv \overline{h} \mod R^0$.

Démonstration. Notons $d \coloneqq \deg f \geqslant \deg \overline{f}$ et $m \coloneqq \deg g$. Alors $\deg \overline{h} \leqslant d - m$. On choisit des polynômes $g_0, r_0 \in R[t]$ tels que

- $g_0 \equiv \overline{g} \mod R_0$ et $\deg g_0 = m$;
- $g_0 \equiv \overline{g} \mod R_0$ et $\deg h_0 = \deg \overline{h} \leqslant d - m$.

Puisque les polynômes $\overline{g}$ et $\overline{h}$ sont premiers entre eux, il existe deux polynômes $a, b \in R[t]$ tel que

$$a(t)\overline{g}(t) + b(t)\overline{h}(t) \equiv 1 \mod R^0.$$

Alors

$$f - g_0 h_0 \equiv 0 \mod R^0 \qquad \text{et} \qquad a g_0 + b h_0 - 1 \equiv 0 \mod R^0.$$

On choisit alors un élément $\pi \in R^0$ dans ces formules qui soit de valeur absolue maximale. Alors $|\pi| < 1$ et tous les autres coefficients sont de valeurs absolues $\leqslant |\pi|$. On va chercher les polynômes $g, h \in R[t]$ de la forme

$$g = g_0 + \pi p_1 + \pi^2 p_2 + \cdots \qquad \text{et} \qquad h = h_0 + \pi q_1 + \pi^2 q_2 + \cdots$$

avec $p_i \in R[t]$ de degré $\leqslant m - 1$ et $q_i \in R[t]$ de degré $\leqslant d - m$ de sorte que les séries définissant g et h convergeront dans $K[t]$ de degré respectifs $\leqslant m$ et $\leqslant d - m$. On veut que

$$f \equiv g_{n-1} h_{n-1} \mod \pi^n R, \qquad n \geqslant 1$$

où

$$g_n \coloneqq g_0 + \cdots + \pi^n p_n \qquad \text{et} \qquad h_0 \coloneqq h + \cdots + \pi^n h_n.$$

À la limite, on aura $f = gh$. On construit les éléments q_i et p_i en effectuant une récurrence sur n. Pour $n = 1$, c'est clair par construction. On suppose avoir fait la construction à l'ordre $n - 1$. On cherche p_n et q_n tels que les polynômes

$$g_n = g_{n-1} + \pi^n p_n \qquad \text{et} \qquad h_n = h_{n-1} + \pi^n q_n$$

satisfasse la relation demandée. On a

$$g_n h_n \equiv g_{n-1} h_{n-1} + \pi^n (h_{n-1} p_n + g_{n-1} q_n) \mod \pi^{n+1},$$

donc

$$f - g_n h_n \equiv f - g_{n-1} h_{n-1} + \pi^n (h_0 p_n + g_0 q_n) \mod \pi^{n+1}$$

et on veut que $f \equiv g_n g_n \mod \pi^{n+1} R$. Posons alors

$$f_n \coloneqq \frac{f - g_{n-1} h_{n-1}}{\pi^n} \in R[t].$$

En divisant par l'élément π^n, on veut

$$f_n \equiv h_0 p_n + g_0 q_n \mod \pi R.$$

Or on a

$$f_n \equiv a f_n g_0 + b f_n h_0 \mod \pi.$$

Mais les degrés peuvent exploser. Pour pallier ce problème, on effectue une division euclidienne. On note

$$bf_n = s_n g_0 + p_n \quad \text{avec} \quad s_n, p_n \in K[t] \qquad \text{et} \qquad \deg p_n \leqslant m-1.$$

Comme $\deg g_0 = \deg \overline{g} = \deg \overline{g_0}$, le coefficient dominant du polynôme g_0 appartient à $R \setminus R^0$, donc c'est une unité de R. Donc en fait, on a $S_n, p_n \in R[t]$. Alors

$$f_n \equiv a f_n g_0 + s_n g_0 h_0 + p_n h_0 \equiv (a f_n + h_0 s_n) g_0 + p_n h_0 \equiv f_n \mod \pi.$$

On prend alors q_n le polynôme $af_n + h_0 s_n$ auquel on retire tous les monômes $\alpha_i t_i$ pour lesquels $\alpha_i \equiv 0 \mod \pi$. Il suffit alors que montrer que $\deg q_n \leqslant d - m$. Mais $\deg q_n = \deg(q_n \mod \pi)$ et comme $\deg g_0 = m$, $\deg h_0 \leqslant d-m$, $\deg p_n \leqslant m-1$ et $\deg f_n \leqslant d$, on en déduit $\det q_n \leqslant d - m$. ⋄

Corollaire 3.10. Soit K un corps valué complet ultramétrique dont la valeur absolue est non triviale. Soit $f \in R[t]$ un polynôme primitif tel que

- il admette une racine z_0 dans le corps résiduel k ;
- la racine z_0 est simple, c'est-à-dire $f'(z_0) \not\equiv 0 \mod R^0$.

Alors il existe une unique racine $f \in R$ du polynôme f telle que

$$z \equiv z_0 \mod R^0.$$

De plus, elle est simple.

Corollaire 3.11. Soit K un corps valué complet ultramétrique. Soit $f \coloneqq a_0 + \cdots + a_d t^d \in K[t]$ un polynôme irréductible de degré d. Alors

$$\|f\| = \max(|a_0|, |a_d|).$$

En particulier, si $a_d = 1$ et $|a_0| \leqslant 1$, alors $|a_j| \leqslant 1$ pour $i \in [\![0, d]\!]$.

Démonstration. Choisissons j tel que $|a_j| = \|f\| \neq 0$ et divisons f par a_j. Maintenant, on suppose donc que $\|f\| = 1$. En particulier, on a $f \in R[t]$ et f est primitif. On réduit modulo R_0. Si $\|f\| = 1 > \max(|a_0|, |a_d|)$, on aurait $\overline{f}(t) = t^r(a_r + \cdots + a_{d-1} t^{d-r-1})$ où la polynôme dans le facteur a un de ses coefficients qui n'est pas nul. Notons

$$\overline{g}(t) \coloneqq t^r \qquad \text{et} \qquad \overline{h}(t) = a_r + \cdots + a_{d-1} t^{d-r-1}.$$

D'après le lemme de Hensel, il existe g de degré r qui divise f ce qui est impossible. ⋄

Critère d'Eisenstein. Supposons que le groupe des valeurs de la valeur absolue $|\cdot|$ est discret. On peut alors écrire $|K^\times| = |\pi|^{\mathbf{Z}}$ pour un élément $\pi \in R$. Dans ce cas, l'anneau R admet un unique idéal maximal $R^0 \coloneqq \pi R$. Soit $g(t) \coloneqq b_0 + \cdots + b_d t^d \in R[t]$ un polynôme de degré d tel que

- $b_0 \neq 0 \mod \pi^2$;
- $b_j = 0 \mod \pi$ pour $j < d$;
- $b_d \neq 0 \mod \pi$.

Alors le polynôme g est irréductible.

3.6. Extension des valeurs absolues aux extensions algébriques

Théorème 3.12. Soit K un corps valué complet. Soit L une extension algébrique du corps K. Alors la valeur absolue sur K s'étend de manière unique en une valeur absolue sur L. De plus, cette dernière vérifie

$$|x|_L = |\mathrm{Norme}_{K(x):K}(x)|^{1/\deg x}, \qquad x \in L.$$

Enfin, si l'extension $L : K$ est finie, alors le corps valué L est complet et

$$|x|_L = |\mathrm{Norme}_{L:K}(x)|^{1/[L:H]}, \qquad x \in L.$$

Démonstration. Le cas archimédien a déjà été traité : dans ce cas, on obtient $K = \mathbf{R}$ ou $\mathbf{C}$ et on trouve nécessairement $L = \mathbf{R}$ ou $\mathbf{C}$. On suppose désormais que la valeur absolue est ultramétrique.

On sait que l'extension L est l'union des extensions finies $K \subset L' \subset L$. On peut donc supposer que $[L : K] < +\infty$.

Notons R le disque unité fermé de K et R_L la clôture intégrale de R dans L, c'est-à-dire

$$R_L \coloneqq \{x \in L \mid P_x \in R[t]\}.$$

Montrons que

$$R_L = \{x \in L \mid \mathrm{Norme}_{L:K}(x) \in R\}.$$

Pour tout élément $x \in R_L$, on a

$$|\mathrm{Norme}_{L:K}(x)| = |P_x(0)| < 1$$

ce qui montre l'inclusion $\subset$. Réciproquement, soit $x \in R$ un élément tel que $\mathrm{Norme}_{L:K}(x) = |a_0| \in R$ en notant $P_x = a_0 + \cdots + a_d t^d$. Alors le polynôme irréductible $P_x \in K[t]$ vérifie $|a_0| \leqslant 1$ et $a_d = 1$. D'après le corollaire précédent, on obtient alors $\|P_x\| = 1$, c'est-à-dire $P_x \in R[t]$.

On veut montrer que l'expression $|x|_L \coloneqq |\mathrm{Norme}_{L:K}(x)|^{1/[L:H]}$ définit une valeur absolue sur L. Si c'est une valeur absolue, alors elle étend bien celle sur K. Il faut donc montrer que c'est une valeur absolue. La séparation est clair. La multiplicativité vient de la multiplicativité du déterminant. Il reste à établir l'inégalité triangulaire. Quitte à multiplier par y, il suffit de montrer que

$$|x|_L \leqslant 1 \quad \Longrightarrow \quad |x+1|_L \leqslant 1.$$

Mais c'est vrai car la clôture intégrale R_L de R est un sous-anneau de R. En effet, considérons l'application

$$\ell_{1+x} \colon \left| \begin{array}{l} K[t] \longrightarrow K[t], \\ \quad z \longmapsto (1+x)z \end{array} \right.$$

a pour matrice dans la base $(1, t, \ldots, t^{d-1})$

$$\mathrm{Mat}(\ell_{1+x}) = I_n + \mathrm{Mat}(\ell_x),$$

donc son polynôme caractéristique est à coefficients dans R. Comme $1 + x$ annule le polynôme caractéristique, il annule un polynôme à coefficients dans R, donc le polynôme minimal P_{1+x} est à coefficients dans R ce qui conclut. ◇

Remarques.
- Le disque unité fermé (respectivement l'anneau de valuation) de L est la clôture intégrale dans L du disque unité fermé (respectivement l'anneau de valuation) de K.
- Soit p un nombre premier. Alors la valeur absolue p-adique s'étend à la clôture algébrique $\overline{\mathbf{Q}_p}$ du corps $\mathbf{Q}_p$. Mais alors le corps valué $(\overline{\mathbf{Q}_p}, |\cdot|_p)$ n'est pas complet. On note $\mathbf{C}_p$ son complété. Il est algébriquement clos.

Chapitre 4
Fonctions analytiques et théorème de Bell-Poonen

4.1. Algèbre de Tate

Soit K un corps valué complet ultramétrique de caractéristique nulle tel que $K \supset \mathbf{Q}_p$ et $|p| = 1/p$. Notons que ces deux dernières hypothèses peuvent toujours être vérifiée quitte à modifier légèrement la valeur absolue sur K. On note R son anneau de valuation, qui contient $\mathbf{Z}_p$, et k son corps résiduel.

Soit $m \geqslant 1$ un entier. On munit l'espace affine $\mathbf{A}_K^m$ des coordonnées $\underline{x} \coloneqq (x_1, \dots, x_m)$ et de la norme $\|\cdot\|_{\sup}$. Alors

$$R^m = \{\underline{u} \in K \mid \|\underline{u}\|_{\sup} \leqslant 1\}.$$

Soit $f \coloneqq \sum_{I \in \mathbf{N}^m} a_I \underline{x}^I \in K[\underline{x}]$ un polynôme à m-variable où, pour $I \coloneqq (i_1, \dots, i_m) \in \mathbf{N}^m$, on pose

$$\underline{x}^I \coloneqq x_1^{i_1} \cdots x_m^{i_m} \in K[\underline{x}].$$

Sa norme de Gauss vaut alors

$$\|f\| = \max_{I \in \mathbf{N}^m} |a_I|.$$

Il s'agit d'une norme sur $K[\underline{x}]$.

Définition 4.1. L'*algèbre de Tate* est la complétion du K-espace vectoriel norme $K[\underline{x}]$ pour la norme $\|\cdot\|$, qu'on note $K\langle \underline{x} \rangle$.

Tout élément $g \in K\langle \underline{x} \rangle$ est une limite de polynôme $f_n \in K[\underline{x}]$ pour la norme $\|\cdot\|$. En notant

$$f_n = \sum_I a_{n,I} \underline{x}^I,$$

les suites $(a_{n,I})_{n \in \mathbf{N}}$ sont de Cauchy, donc elle converge vers des limites $b_I \in K$. Ces derniers éléments b_I sont canoniquement associé à l'élément g. On pose alors

$$g \coloneqq \sum_I b_I \underline{x}^I.$$

la *série formelle* associée à l'élément g.

Exemple. On prend $f(x) = 1 + px + \cdots + p^n x^n$. Alors

$$\|f_n - f_{n+\ell}\| = \|p^{n+1}x^{n+1} + \cdots + p^{n+\ell}x^{n+\ell}\| = p^{-(n+1)} \longrightarrow 0,$$

donc la suite $(f_n)_{n\in\mathbf{N}}$ est de Cauchy dans $K[\underline{x}]$ pour la norme $\|\cdot\|$, mais elle ne converge pas dans $K[\underline{x}]$. Mais sa limite dans $K\langle\underline{x}\rangle$ est l'élément

$$\sum_{j=0}^{+\infty} p^j x^j.$$

On remarque que $b_I \longrightarrow 0$ dans K lorsque $\mathrm{long}(I) \coloneqq i_1 + \cdots + i_m \longrightarrow +\infty$. En effet, pour un entier fixé n, on a $a_{n,I} = 0$ pour $\mathrm{long}(I) \gg 1$. Réciproquement, si $g(\underline{x}) = \sum_I b_i \underline{x}^I$ est une série formelle telle que $|b_I| \longrightarrow 0$, alors $g \in K\langle\underline{x}\rangle$ en prenant

$$f_n \coloneqq \sum_{\mathrm{long}(I)\leqslant n} b_I \underline{x}^I$$

qui forme une suite de Cauchy. On obtient alors la proposition suivante.

Proposition 4.2. L'algèbre de Tate est

$$K\langle\underline{x}\rangle = \Big\{ \sum_I b_I \underline{x}^I \in K[\![\underline{x}]\!] \;\Big|\; |b_I| \longrightarrow 0 \text{ lorsque } \mathrm{long}(I) \longrightarrow +\infty \Big\}.$$

Théorème 4.3.
1. Un élément $\sum_I b_I \underline{x}^I$ appartient à $K\langle\underline{x}\rangle$ si et seulement si $|b_I| \longrightarrow 0$ si et seulement si la série $\sum b_i \underline{x}^I$ converge uniformément sur le polydisque R^m.
2. Si le corps K est infini, alors
$$\forall g \coloneqq \sum_I b_i \underline{x}^I \in K\langle\underline{x}\rangle, \qquad \max_I |b_I| = \|g\| = \max_{\underline{u}\in R^m} |g(\underline{u})|.$$
3. La norme de Gauss $K\langle\underline{x}\rangle \longrightarrow \mathbf{R}_+$ est multiplicative.

Démonstration.
1. Si $|b_I| \longrightarrow 0$, alors la série converge uniformément grâce à l'inégalité ultramétrique. Réciproquement, si la série converge uniformément, alors la série évaluée en $(1,\ldots,1)$ converge, donc la série $\sum b_I$ converge, donc $|b_I| \longrightarrow 0$.
2. D'abord, l'inégalité ultramétrique donne
$$\max_{\underline{u}\in R^m} |g(\underline{u})| \leqslant \max_I |b_I| \leqslant \|g\|.$$
Réciproquement, on écrit $g(\underline{x}) = \sum_I b_I \underline{x}^I \neq 0$. On choisit un indice J tel que $|b_J| = \|g\|$. On pose alors $h \coloneqq b_J^{-1} g$ de telle sorte que $\|h\| = 1$. On écrit $h(\underline{x}) = \sum_I c_I \underline{x}^I$ avec $c_I \in R$. On veut montrer que $\max_{\underline{u}\in R^m} |h(\underline{u})| = 1$. On réduit l'élément h modulo R^0 et on note $\underline{h}(x) \in k[\underline{x}]$ sa projection. On a $\underline{h} \neq 0$. Comme le corps K est infini, il existe un m-uplet $(\alpha_1,\ldots,\alpha_m) \in R^m$ tel que
$$\underline{h}(\alpha_1,\ldots,\alpha_m) \neq 0 \mod R^0, \quad \text{c'est-à-dire} \quad h(\alpha_1,\ldots,\alpha_m) \notin R^0.$$
Ceci implique $|h(\alpha_1,\ldots,\alpha_m)| = 1$ ce qui conclut.
3. On écrit
$$g(\underline{x}) = \sum a_I \underline{x}^I \qquad \text{et} \qquad h(\underline{x}) = \sum b_I \underline{x}^I.$$
Soit I_0 le plus petit indice pour l'ordre lexicographique tel que $|a_I| = \|g\|$. Soit J_0 le plus petit indice pour l'ordre lexicographique tel que $|a_I| = \|h\|$. On note
$$gh(\underline{x}) = \sum c_I \underline{x}^I.$$
Alors
$$|c_{I_0+J_0}| = \|g\|\,\|h\|.$$
Cela donne $\|g\|\,\|h\| \leqslant \|gh\|$. L'autre inégalité se montre grâce à l'ultramétricité. ◇

Exemple. On prend $m = 1$. Soit $n \geqslant 1$ un entier. On pose
$$B_n(x) \coloneqq \binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!} \in \mathbf{Q}_p[x].$$

Ses coefficients b_i sont de la forme $k_i/n!$ avec $k_i \in \mathbf{N}$, donc

$$|b_i|_p \leqslant \left|\frac{1}{n!}\right|_p.$$

De plus, on a

$$|b_n|_p = \left|\frac{1}{n!}\right|_p.$$

Or

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^\ell} \right\rfloor + \cdots,$$

donc

$$\left\lfloor \frac{n}{p} \right\rfloor \leqslant v_p(n!) \leqslant \frac{n}{p-1}.$$

En particulier, on trouve

$$|b_n|_p \geqslant p^{\lfloor n/p \rfloor}$$

et donc

$$\|B_n\| \geqslant p^{\lfloor n/p \rfloor} \gg 1$$

lorsque $n \gg 1$. Pourtant, on a

$$\max_{u \in \mathbf{Z}_p} |B_n(u)|_p = 1$$

En effet, les éléments $B_n(u)$ avec $u \in \mathbf{N}$ sont des entiers, la fonction B_n est continue et $\overline{\mathbf{N}} = \mathbf{Z}_p$, donc

$$\forall u \in \mathbf{Z}_p, \qquad |B_n(u)|_p \leqslant 1.$$

Comme $B_n(n) = 1$, on en déduit l'égalité.

4.2. Méthode des différences divisées et théorème de Mahler

4.2.1. Le théorème de Newton

Soit $f \in K[t]$ un polynôme de degré d. On suppose qu'on connaît les valeurs $f(0)$, …, $f(d)$. Alors on peut retrouver le polynôme f. On pose $A_0 \coloneqq f(0)$. Considérons l'opérateur de différence Δ défini par

$$\Delta h(t) \coloneqq h(t+1) - h(t).$$

Alors $\Delta f(i) = f(i+1) - f(i)$. On pose

$$A_1 \coloneqq \Delta f(0) \qquad \text{et} \qquad A_j \coloneqq \Delta^j f(0) = \sum_{i=0}^{j} (-1)^i \binom{j}{i} f(j-i).$$

Théorème 4.4 *(Newton).* Si f est un polynôme de degré d à coefficients dans un corps de caractéristique nulle, alors

$$f(x) = \sum_{j=0}^{d} A_j B_j(x) \quad \text{avec} \quad A_j \coloneqq \Delta^j f(0) \quad \text{et} \quad B_j(x) \coloneqq \binom{x}{j}.$$

Démonstration. Les polynômes B_j avec $j \in [\![0, d]\!]$ forment une base de $K[x]_{\leqslant d}$ et ils vérifiant $\Delta B_j = B_{j-1}$. Il s'agit ensuite de trouver la valeur des éléments A_j en composant successivement par l'opérateur Δ. ◇

4.2.2. Le théorème de Mahler

Théorème 4.5 *(Mahler, 1956).* Soit $f \colon \mathbf{Z}_p \longrightarrow \mathbf{Q}_p$ une fonction continue. Soit $(A_m)_{m \geqslant 0}$ la suite

définie par l'égalité

$$A_m \coloneqq \Delta^m f(0) = \sum_{i=0}^{m} (-1)^i \binom{m}{i} f(m-i).$$

Alors $|A_m|_p \longrightarrow 0$ et

$$f(x) = \sum_{m=0}^{+\infty} A_m B_m(x), \qquad x \in \mathbf{Z}_p$$

où la série apparaissant converge uniformément sur $\mathbf{Z}_p$.

Remarque. Une série $\sum a_m B_m(x)$ converge uniformément sur $\mathbf{Z}_p$ si et seulement si $|a_n|_p \longrightarrow 0$.

4.3. Le théorème des zéros isolés

Théorème 4.6. Soit $f(x) \coloneqq \sum_{n=0}^{+\infty} a_n x^n \in K\langle x \rangle$ une application non nulle. Soit N le plus grand entier tel que $|a_N| = \|f\|$. Alors l'application f a au plus N zéros dans R.

Démonstration. On procède par récurrence sur N. Pour $N = 0$, on a

$$|a_0| = \|f\| > |a_j|, \qquad \forall j \geqslant 1.$$

Avec l'inégalité ultramétrique, on obtient alors

$$|f(x)| = |a_0| \neq 0, \forall x \in R.$$

On passe des cas $N' < N$ au cas N. Soit α un zéro de f sur R. Alors

$$\begin{aligned} f(x) &= f(x) - f(\alpha) \\ &= \sum_{n=1}^{+\infty} a_n (x^n - \alpha^n) \end{aligned}$$

avec

$$x^n - \alpha^n = (x-\alpha)(x^{n-1} + x^{n-2}\alpha + \cdots + \alpha^{n-1}),$$

donc

$$\begin{aligned} f(x) &= (x-\alpha) \sum_{n=0}^{+\infty} \sum_{j=0}^{n-1} a_n x^j \alpha^{n-j-1} \\ &= (x-\alpha) \sum_{j=0}^{+\infty} \underbrace{\Big(\sum_{n=j+1}^{+\infty} a_n \alpha^{n-j-1} \Big)}_{b_j} x^j. \end{aligned}$$

Les coefficients b_j vérifient $b_j \in K$ car $|a_n| \longrightarrow 0$ et on a aussi

$$|b_j| \leqslant \max_{n \geqslant j+1} |a_n|, \quad \text{donc} \quad |b_N| < \|f\| \quad \text{et} \quad |b_{N-1}| = |a_N| = \|f\|.$$

Donc l'indice pour la série $\sum b_j x^j$ est $N-1$. Par l'hypothèse de récurrence, elle est donc au plus $N-1$ zéros ce qui conclut. ◇

Corollaire 4.7. Si $\alpha_1, \ldots, \alpha_k \in R$ sont les zéros de $f \in K\langle x \rangle \setminus \{0\}$ dans R, alors

$$f(x) = \prod_{i=1}^{k} (x - \alpha_i) \times g(x) \quad \text{avec} \quad \|g\| \leqslant \|f\|.$$

Corollaire 4.8. Si $f \in K\langle x \rangle$ a une infinité de racines dans R, alors $f = 0$.

4.4. Difféomorphismes et flots analytiques

4.4.1. Difféomorphismes

Définition 4.9. Un *endomorphisme analytique* de R^m est une application

$$\left|\begin{array}{l} R^m \longrightarrow R^m, \\ \underline{x} \longmapsto (f_1(\underline{x}), \dots, f_m(\underline{x})) \end{array}\right.$$

pour des applications $f_i \in R\langle \underline{x} \rangle$

L'ensemble $\mathrm{End}\langle R^m \rangle$ des endomorphismes analytiques est un R-module stable par composition. Les éléments inversibles forment un groupe $\mathrm{Diff}\langle R^m \rangle$.

Lemme 4.10. Soit $g \in K\langle \underline{x} \rangle$. Montrer que l'application $g|_{R^m} : R^m \longrightarrow K$ est $\|g\|$-lipschitzienne.

Démonstration. Pour tous $x, y \in R$, on a

$$\begin{aligned} |x^i - j^i| &= |(x-y)(x^{i-1} + x^{i-2}y + \cdots + y^{i-1})| \\ &\leqslant |x-y| \end{aligned}$$

car $x^{i-1} + x^{i-2}y + \cdots + y^{i-1} \in R$. En dimension deux, on utilise ce qui précède. ◇

Théorème 4.11. Le groupe $\mathrm{End}\langle \mathbf{R}^m \rangle$ agit par transformations 1-lipschitziennes sur R^m et le groupe $\mathrm{Diff}\langle R^m \rangle$ agit par isométries sur R^m.

Application. On prend $K = \mathbf{Q}_p$ et $R = \mathbf{Z}_p$. Soit $f \in \mathrm{Diff}\langle \mathbf{Z}_p^m \rangle$. Les boules de $\mathbf{Z}_p^m$ de rayon p^{-s} sont en bijection avec les classes dans $(\mathbf{Z}_p/p^s\mathbf{Z}_p)^m \simeq (\mathbf{Z}/p^s\mathbf{Z})^m$. On réduit les coefficients de f modulo p^s : l'application $\overline{f}$ est alors polynomiales. De même, on obtient le réduit $\overline{f^{-1}}$ et ce dernier vérifie $\overline{f} \circ \overline{f^{-1}} = \mathrm{Id}$. En fait, on a

$$\hat{f} \in \mathrm{Aut}(\mathbf{A}^m_{\mathbf{Z}/p^s\mathbf{Z}}).$$

En particulier, l'application $\overline{f}$ permute les points de l'espace affine $\mathbf{A}^m(\mathbf{Z}/p^s\mathbf{Z})$ qui a $(p^s)^m$ éléments. Finalement, on obtient une action sur les boules de rayon p^{-s}.

Conséquence. On construit ainsi, pour tout entier $s \geqslant 1$, un homomorphisme

$$\mathrm{Diff}\langle \mathbf{Z}_p^m \rangle \xrightarrow{\theta_s} \mathrm{Aut}(\mathbf{A}^m_{\mathbf{Z}/p^s\mathbf{Z}}) \longrightarrow \mathfrak{S}(\mathbf{A}^m(\mathbf{Z}/p^s\mathbf{Z})).$$

Si $f \in \mathrm{Ker}\,\theta_s$, alors f fixe chaque boule de rayon p^{-s} dans R^m. Ainsi si $f \in \bigcap_{s=1}^{+\infty} \mathrm{Ker}(\theta_s)$, alors f est l'identité.

Définition 4.12. Un groupe G est *résiduellement fini* si, pour tout élément $g \neq 1$, il existe un groupe fini F et un homomorphisme $\Theta : G \longrightarrow F$ tels que $\Theta(g) \neq 1$.

Le groupe $\mathrm{Diff}\langle \mathbf{Z}_p^m \rangle$ est résiduellement fini. Si G est infini et simple, alors il n'est pas résiduellement fini.

Notation. Soit $f, g \in \mathrm{End}\langle R^m \rangle$. On écrit $g = f \mod p^c$ si $\|g - f\| \leqslant p^{-c}$ avec $c > 0$. Par exemple, on a

$$px + 3x^2 + 6x^3 + px^7 = 3x^2 + 6x^3 \mod p.$$

Lemme 4.13. Soient $g, h \in \mathrm{End}\langle x \rangle$ et $f \in \mathrm{Diff}\langle x \rangle$. Alors

1. $\|g \circ h\| \leqslant \|g\|\,\|h\|$;
2. $\|g \circ (\mathrm{Id} + h) - g\| \leqslant \|h\|$;
3. $\|g \circ f\| = \|g\|$;
4. $\|f^{-1} - \mathrm{Id}\| = \|f - \mathrm{Id}\|$.

Démonstration. Les deux premiers points se montrent par le calcul. Les deux derniers s'en déduiront. ◇

Lemme 4.14. Soit $c > 0$. Alors l'ensemble

$$\{f \in \mathrm{Diff}\langle R^m\rangle \mid f = \mathrm{Id} \mod p^c\}$$

est un sous-groupe distingué de $\mathrm{Diff}\langle x\rangle$. De plus, si $f = \mathrm{Id} \mod p^c$, alors

$$f^{p^N} = \mathrm{Id} \mod p^{c+N}.$$

Idée de la preuve. On écrit $f(\underline{x}) = \underline{x} + sh(\underline{x})$ avec $h \in \mathrm{End}\langle R^m\rangle$ et $|s| \leqslant p^{-c}$. Alors

$$\begin{aligned} f \circ f(\underline{x}) &= \underline{x} + sh(\underline{x}) + sh(\underline{x} + sh(\underline{x})) \\ &= \underline{x} + sh(\underline{x}) + sh(\underline{x}) + s^2 h_2(\underline{x}) \quad \text{avec} \quad h_2 \in \mathrm{End}\langle R^m\rangle \\ &= \underline{x} + 2sh(\underline{x}) + s^2 h_2(\underline{x}). \end{aligned}$$

Plus généralement, on obtient

$$f^k(\underline{x}) = \underline{x} + ksh(\underline{x}) + s^2 h_k(\underline{x}).$$

Pour $k = p$, on gagne un facteur p. ◇

4.4.2. Flots analytiques

Soit $\Phi\colon R \longrightarrow \mathrm{Diff}\langle R^m\rangle$ un homomorphisme du groupe additif R dans le groupe pour la composition $\mathrm{Diff}\langle R^m\rangle$. Un tel morphisme est un *flot* paramétré par R. Son action associée est

$$(t, x) \longmapsto \Phi_t(x).$$

Si cette action est analytique au sens de Tate, c'est-à-dire si $\Phi_t(\underline{x}) \in (R\langle t, \underline{x}\rangle)^m$, on dit que le flot est analytique. Son champ de vecteurs associé est

$$X(x) \coloneqq \left.\frac{\partial \Phi_t(x)}{\partial t}\right|_{t=0} \in (R\langle \underline{x}\rangle)^m.$$

4.5. Théorème de Bell-Poonen

Théorème 4.15 *(Bell-Poonen, 2006-2010).* Soit $f \in \mathrm{End}\langle R^m\rangle$ avec $f = \mathrm{Id} \mod p^c$ et $c > 1/(p-1)$. Alors il existe un flot analytique $\Phi\colon R \times R^m \longrightarrow R^m$ tel que

- $\Phi_n(\underline{x}) = f^n(\underline{x})$ pour tout $n \in \mathbf{N}$;
- $\|\Phi_t - \Phi_s\| \leqslant 1/p^{c-1/(p-1)}\,|t - s|$ pour tous $t, s \in R$.

En particulier, on a $f \in \mathrm{Diff}\langle R^m\rangle$ et $f^{-1} = \Phi_{-1}$.

Démonstration. Soit $x \in R$ fixé. Posons $u - n) \coloneqq f^n(x) \in R^m$. On cherche une bourbe $t \in R \longmapsto \Phi_t(x)$ telle que

$$\Phi_n(x) = u(n), \qquad n \in \mathbf{N}.$$

Autrement dit, on cherche à étendre l'application $n \longmapsto u(n)$ en $t \longmapsto \Phi_t(x)$. Pour cela, on utilise la méthode des différences divisées. On a

$$\begin{aligned} u(n+1) - u(n) &= f^{n+1}(x) - f^n(x) \\ &= f^n \circ f(x) - f^n(x). \end{aligned}$$

On introduit l'opérateur

$$\Delta_f\colon h \longmapsto h \circ f - h$$

qui agit sur $\mathrm{End}\langle R^m\rangle$. Comme $f = \mathrm{Id} \mod p^c$, en utilisant les lemmes précédents, on a $\Delta_f h = 0 \mod p^c$ pour tout $h \in \mathrm{End}\langle R^m\rangle$. En itérant, on obtient

$$\|\Delta_f^k h\| \leqslant p^{-kc}, \qquad k \geqslant 1.$$

Pour $h = \mathrm{Id}$, on trouve

$$\|\Delta_f^k \mathrm{Id}\| \leqslant p^{-kc}, \qquad k \geqslant 1. \tag{$*$}$$

Par ailleurs, rappelons que $v_p(k!) \leqslant k/(p-1)$. On définit

$$\Phi_t(\underline{x}) \coloneqq \sum_{k=0}^{+\infty} B_k(t)\Delta_f^k \operatorname{Id}(\underline{x}) = \sum_{k=0}^{+\infty} t(t-1)\cdots(t-k+1)\frac{1}{k!}\Delta_f^k \operatorname{Id}(\underline{x})$$

qui détermine un élément de $(R\langle t, \underline{x}\rangle)^m$ car, grâce à $(*)$, on a

$$\left\| t(t-1)\cdots(t-k+1)\frac{1}{k!}\Delta_f^k \operatorname{Id}(\underline{x}) \right\| \leqslant p^{-k(c-1/(p-1))}.$$

La série $\Phi_t(\underline{x})$ est en fait une somme finie

$$\Phi_t(\underline{x}) = \sum_{k=0}^{n} \binom{n}{k} \Delta_f^k \operatorname{Id}(\underline{x}) = (\operatorname{Id} + \Delta f)^k \operatorname{Id}(\underline{x}) = f^n(\underline{x}).$$

Montrons que l'application Φ est un flot analytique. On a $\Phi_{n+m} = f^{n+m} = f^n \circ f^m = \Phi_n \circ \Phi_m$. Soit $x \in \mathbf{R}$. L'application

$$t \longmapsto \Phi_{t+m}(x) - \Phi_t \circ \Phi_m(x)$$

est nulle pour tout $t \in \mathbf{N}$, donc le théorème des zéros isolés donne

$$\forall t \in R, \qquad \Phi_{t+m}(x) = \Phi_t \circ \Phi_m(x).$$

De la même manière, on trouve

$$\forall t, s \in R, \qquad \Phi_{t+s}(x) = \Phi_t \circ \Phi_s(x).$$

Finalement, on montre que

$$\forall t, s \in R, \qquad \Phi_{t+s} = \Phi_t \circ \Phi_s.$$

Donc l'application Φ est un flot analytique.

Il reste à montrer le second point. En notant $P_k \coloneqq t(t-1)\cdots(t-k+1) \in \mathbf{Z}[t]$ qui est 1-lipschitzien, on a

$$\Phi_t - \Phi_s = \sum_{k=0}^{+\infty} (P_k(t) - P_k(s)) \frac{\Delta_f^k \operatorname{Id}}{k!}$$

et on utilise l'estimation trouvée précédemment. ◇

Exemple. Supposons que le corps K contienne une racine de l'unité ξ d'ordre p. Le polynôme minimal de la racine ξ sur $\mathbf{Q}_p$, avec le critère d'Eisenstein, est le polynôme

$$P(t) \coloneqq t^{p-1} + \cdots + t + 1,$$

donc le polynôme minimal de l'élément $\xi - 1$ est $P(t-1)$ et ce dernier vérifie $P(0+1) = p$. Ainsi, l'extension $\mathbf{Q}_p(\xi) : \mathbf{Q}_p$ est de degré $p-1$ et on calcul

$$\operatorname{Norme}_{\mathbf{Q}_p(\xi):\mathbf{Q}_p}(\xi - 1) = \begin{cases} -2 & \text{si } p = 2, \\ p & \text{si } p \geqslant 3 \end{cases},$$

c'est-à-dire

$$|\xi - 1| = p^{-1/(p-1)}.$$

En prenant $f(\underline{x}) \coloneqq \xi\underline{x}$, on a $f = \operatorname{Id} \mod p^c$ avec $c \coloneqq 1/(p-1)$. Montrons qu'alors le résultat du théorème n'est pas vérifié. Raisonnons par l'absurde et supposons qu'il existe un flot analytique Φ tel que $f = \Phi_1$. Alors

$$\forall n \in \mathbf{Z},\ \forall x \in \mathbf{Z}_p, \qquad \underline{x} = f^{pn}(\underline{x}) = \Phi_{pn}(\underline{x}).$$

Par le théorème des zéros isolés, on trouve alors $\Phi_t = \operatorname{Id}$ pour tout $t \in \mathbf{Z}_p$, donc $f = \operatorname{Id}$ ce qui est impossible.

En effet, on vient aussi d'établir le résultat suivant.

Lemme 4.16. Si $f = \Phi_1$ pour un flot analytique Φ et f est de torsion, c'est-à-dire qu'il existe $\ell \geqslant 1$ tel que $f^\ell = \operatorname{Id}$, alors $f = \operatorname{Id}$.

Application. On prend $K = \mathbf{Q}_p$. Notons

$$\beta\colon \mathrm{Diff}\langle \mathbf{Z}_p^m\rangle \xrightarrow{\theta_2} \mathrm{Aut}(\mathbf{A}^m_{\mathbf{Z}/p^s\mathbf{Z}}) \longrightarrow \mathfrak{S}(\mathbf{A}^m(\mathbf{Z}/p^s\mathbf{Z}))$$

la composée de θ_2 et de l'inclusion. Alors son noyau $\mathrm{Ker}\,\beta$ est d'indice fini, majorée par $(p^{2m})!$. Pour tout $f \in \mathrm{Ker}\,\beta$, on a $f(0) = 0 \mod p^2$. De plus, soit $f \in \mathrm{Ker}\,\beta$. Alors sa différentielle en 0 est une matrice $df_0 \mod p$ de $\mathrm{GL}_m(\mathbf{Z}/p\mathbf{Z})$. On obtient un homomorphisme

$$\mathrm{Ker}\,\beta \longrightarrow \mathrm{GL}_m(\mathbf{Z}/p\mathbf{Z})$$

Soit $\mathrm{Diff}^0\langle \mathbf{Z}_p^m\rangle$ le noyau de ce morphisme. Un élément $f \in \mathrm{Diff}^0\langle \mathbf{Z}_p^m\rangle$ s'écrit alors sous la forme

$$f(\underline{x}) = A_0 + A_1(\underline{x}) + A_2(\underline{x}) + \cdots$$

où chaque fonction $A_j\colon \mathbf{A}^m \longrightarrow \mathbf{A}^m$ est polynomiale homogène de degré j à coefficients dans R et elles vérifient

$$A_0 = 0 \mod p^2 \qquad \text{et} \qquad A_1 = \mathrm{Id} \mod p.$$

En conjuguant par la multiplication par p, on trouve alors

$$\begin{aligned}\frac{1}{p}f(p\underline{x}) &= \frac{A_0}{p} + A_1(\underline{x}) + \cdots + p^{j-1}A_j(\underline{x}) + \cdots \\ &= 0 + \mathrm{Id}(\underline{x}) \mod p.\end{aligned}$$

Ainsi la fonction $\frac{1}{p}f(px)$ vérifie les hypothèses du théorème de Bell-Poonen. En particulier, elle est dans un flot.

Corollaire 4.17. Soit $f \in \mathrm{Diff}^0\langle \mathbf{Z}_p^m\rangle$ un élément avec torsion. Alors $f = \mathrm{Id}$.

Chapitre 5
Orbites des automorphismes de l'espace affine

Objectif. On va énoncer des faits de base sur la structure des sous-groupes de $\mathrm{Aut}(\mathbf{A}^m_{\mathbf{C}})$ et sur l'orbite d'un élément $f \in \mathrm{Aut}(\mathbf{A}^m_{\mathbf{C}})$.

5.1. Théorème de prolongement de Lech

Lemme 5.1. Soit $P \in \mathbf{Z}[t]$ un polynôme non constant. Alors il existe une infinité de nombre premier p tel que le polynôme P ait une racine dans $\mathbf{F}_p$.

Démonstration. Sinon il existe des nombres premiers $p_1, \ldots, p_k$ tels que

$$\forall n \in \mathbf{Z}, \qquad P(n) = \pm \prod_{i=1}^{k} p_i^{v_i(n)}.$$

Comptons les valeurs entières du polynôme P dans $[-M, M]$ avec $M \gg 1$. Si $|P(n)| \leqslant M$, alors

$$2^{v_1(n)+\cdots+v_k(n)} \leqslant \prod_{i=1}^{k} p_i^{v_i(n)} \leqslant M,$$

donc

$$\sum_{i=1}^{k} v_i(n) \leqslant \frac{\log M}{\log 2}.$$

On a donc au plus $(\log M/\log 2)^k$ choix possibles, donc les valeurs entières du polynôme P dans $[-M, M]$ forment un ensemble de cardinal au plus $2(\log M/\log 2)^k$. Par ailleurs, avec $d := \deg P$, on a $P(n) \simeq c_d n^d$ pour n assez grand, donc les valeurs entières du polynôme P dans $[-M, M]$ forment également un ensemble de cardinal au moins $\varepsilon_0 M^{1/d}$ pour un réel $\varepsilon > 0$ ce qui est impossible. ◇

Théorème 5.2 *(Lech).* Soient K une extension de type fini de $\mathbf{Q}$ et S une partie finie de $K \setminus \{0\}$. Alors il existe un nombre premier p et un plongement $\iota\colon K \hookrightarrow \mathbf{Q}_p$ tel que $\iota(S) \subset \mathbf{Z}_p$. En effet, les tels nombres premiers p forment un ensemble de densité positive parmi les nombres premiers, c'est-à-dire qu'il existe un réel $\varepsilon_0 > 0$ tel que

$$\forall B \gg 1, \qquad \frac{\sharp\{p \in \mathscr{P} \mid p \leqslant B,\ p \text{ convient}\}}{\sharp\{p \in \mathscr{P} \mid p \leqslant B\}} \geqslant \varepsilon_0.$$

Démonstration. On traite d'abord un premier cas. On suppose que l'extension $K : \mathbf{Q}$ est transcendante, c'est-à-dire qu'on peut écrire $K = \mathbf{Q}(t_1, \ldots, t_s)$ où les éléments t_i ne vérifient pas de

relations algébriques entre eux. Comme l'ensemble $\mathbf{Z}_p$ n'est pas dénombrable, on peut trouver des nombres transcendants $\tau_1, \dots, \tau_s \in \mathbf{Z}_p$ tels que $\mathbf{Q}(\tau_1, \dots, \tau_s) \simeq \mathbf{Q}(t_1, \dots, t_s)$.

Ensuite, on suppose que l'extension $K : \mathbf{Q}$ est algébrique (primitive). On l'écrit $K = \mathbf{Q}(\alpha)$ avec un élément algébrique $\alpha \in K$. Soit $P_\alpha \in \mathbf{Z}[t]$ son polynôme minimal (il n'est pas forcément unitaire). Son discriminant D est alors un entier non nul. Avec le lemme, on choisit un nombre premier $p > D$ tel que le polynôme P_α admette une racine dans $\mathbf{F}_p$. Une telle racine est simple car $D \not\equiv 0 \mod p$. Avec le lemme de Hensel, le polynôme P_α admet donc une racine dans $\alpha' \in \mathbf{Z}_p$. On considère alors le plongement qui envoie la racine α sur la racine α'.

Traitons maintenant le cas général. L'extension K est une extension algébrique d'une extension transcendante pure de $\mathbf{Q}$, c'est-à-dire qu'on peut écrire $\mathbf{Q} \subset L \coloneqq \mathbf{Q}(t_1, \dots, t_s) \subset K$ où la première extension est transcendante pure et la seconde algébrique. D'après le théorème de l'élément primitif, il existe un élément $\alpha \in K$ tel que $K = L(\alpha)$. Notons $P_\alpha \in \mathbf{Z}[t_1, \dots, t_s][x]$ son polynôme minimal sur L qui n'est pas forcément unitaire. Soit $D \in \mathbf{Z}[t_1, \dots, t_s]$ son discriminant. Tout élément $s \in S$ s'écrit sous la forme $s = G_s(\alpha)$ avec $G_s \in L[x]$. On choisit $B_s \in L$ tel que $B_s G_s \in \mathbf{Z}[t_1, \dots, t_s][x]$. Notons R_S le résultant des polynômes $B_s G_s$ et P_α. Comme $s \neq 0$, on a $R_s \neq 0$. On choisit un s-uplet $(a_1, \dots, a_s) \in \mathbf{Z}^s$ tel que

- $D(a_1, \dots, a_s) \neq 0$;
- le polynôme $P_\alpha(a_1, \dots, a_s)$ ne soit pas constant ;
- $R_s(a_1, \dots, a_s) \neq 0$ pour tout $s \in S$;
- $B_s(a_1, \dots, a_s) \neq 0$ pour tout $s \in S$.

On choisit un nombre premier p tel que les égalités précédentes restent vraie modulo p (il suffit de prendre un nombre premier $p > |D(a_1, \dots, a_s)|$) et tel que le polynôme $P_\alpha(a_1, \dots, a_s)$ ait une racine modulo p. On choisit des éléments $\tau_1, \dots, \tau_s \in \mathbf{Z}_p$ tels que l'extension $\mathbf{Q}(\tau_1, \dots, \tau_s) \subset \mathbf{Q}_p$ soit transcendante pure de degré s. On définit le plongement $\iota_L \colon L \longrightarrow \mathbf{Q}_p$ par l'égalité

$$\iota(t_i) = a_i + p\tau_i, \qquad i \in [\![1, s]\!].$$

Il envoie le polynôme P_α sur le polynôme $P_\alpha(a_1 + p\tau_1, \dots, a_s + p\tau_s)$. Alors modulo p, le discriminant de ce dernier est non nul, donc $\operatorname{disc}(P_\alpha(a_1, \dots, a_s)) \neq 0$ et le polynôme $P_\alpha(\alpha_1, \dots, \alpha_s)$ a une racine modulo p, donc le polynôme $P_\alpha(a_1, \dots, a_s)$ a une racine $\hat{\alpha} \in \mathbf{Z}_p$. On étend alors le plongement ι_L en le plongement $\iota \colon L(\alpha) \longrightarrow \mathbf{Q}_p$ en posant $\iota(\alpha) = \hat{\alpha}$.

Montrons alors que $\iota(S) \subset \mathbf{Z}_p$. On sait que $|B_s(a_i + p\tau_i)|_p = 1$ et $B_s G_s(\hat{\alpha}) \neq 0 \mod p$, donc $|B_s G_s(\hat{\alpha})|_p = 1$, donc $|G_s(a_i + p\tau_i)(\hat{\alpha})|_p = 1$ ce qui termine la preuve. ◇

Théorème 5.3 *(Tits, Brouillard & Gelender).* Soit A un anneau intègre de type fini. Soit $S \subset A$ une partie infinie. Alors il existe un corps valué complet localement compact K et un plongement d'anneaux $\iota \colon A \longrightarrow K$ tels que la partie $|\iota(S)|$ ne soit pas bornée.

5.2. Résiduellement fini, virtuellement sous torsion

Définition 5.4. Un groupe G vérifie *virtuellement* une propriété (P) s'il existe un sous-groupe $H \subset G$ d'indice fini vérifiant la propriété (P).

Théorème 5.5 *(Bass, Lubotzky).* Soient K un corps de caractéristique nulle et Γ un sous-groupe de type fini de $\operatorname{Aut}(\mathbf{A}^m_K)$. Alors

1. le groupe Γ est résiduellement fini ;
2. il est virtuellement sans torsion

Démonstration. Soit $S \subset \Gamma$ une partie finie symétrique engendrant le groupe Γ. Soit C_S l'ensemble fini des coefficients non nuls des formules de éléments $g \in S$. Alors $\Gamma \subset \operatorname{Aut}(\mathbf{A}^m_{K_0})$ où le corps K_0 est celui engendré par l'ensemble C_S. Grâce au théorème, il existe un plongement $\iota \colon K_0 \longrightarrow \mathbf{Q}_p$ qui envoie l'ensemble C_S sur le boule $\mathbf{Z}_p$. On obtient alors un homomorphisme de groupes injectif

$$\Gamma \hookrightarrow \operatorname{Aut}(\mathbf{A}^m_{\mathbf{Z}_p})$$

On peut donc supposer que $\Gamma \subset \operatorname{Aut}(\mathbf{A}^m_{\mathbf{Z}_p}) \subset \operatorname{Diff}\langle \mathbf{Z}^m_p \rangle$. Mais on a déjà vu que ce dernier groupe était résiduellement fini et virtuellement sans torsion. ◇

Exemple. Le groupe $\mathrm{GL}_m(\mathbf{Z})$ est résiduellement fini et virtuellement sans torsion.

Lemme 5.6 *(Makowski).* Le noyau de la réduction modulo 3 est sans torsion.

5.3. Théorème d'arithméticité des temps de passage

Théorème 5.7 *(Bell, 2006).* Soient K un corps de caractéristique nulle et $f \in \mathrm{Aut}(\mathbf{A}^m_K)$ un automorphisme. Soit $W \subset \mathbf{A}^m_K$ une sous-variété algébrique. Alors l'ensemble $\mathrm{Pas}_f(x, W)$ est une union finie de progressions arithmétiques.

Démonstration. Soit C l'ensemble des coefficients de f, de f^{-1}, des coordonnées de x et les coefficients d'un système fini d'équations $P_i(\underline{x}) = 0$ avec $i \in [\![1, k]\!]$ définissant W. Soit K_0 le corps engendré par C. On peut alors trouver un plongement $\iota\colon K_0 \longrightarrow \mathbf{Q}_p$ tel que $\iota(C) \subset \mathbf{Z}_p$. On a

$$\mathrm{Pas}_f(x, W) = \{n \in \mathbf{Z} \mid \forall i,\ P_i(f^n(x)) = 0\}.$$

En appliquant ι, l'ensemble $\mathrm{Pas}_f(x, W)$ reste inchangé. On peut donc supposer que tout est à coefficients dans $\mathbf{Z}_p$.

On conjugue f par $T_x\colon z \longmapsto z + x$ pour ramener x en 0. Ensuite, on change $T_x^{-1} \circ f \circ T_x$ en un itéré $(T_x^{-1} \circ f \circ T_x)^N$ pour que $T_x^{-1} \circ f \circ T_x \in D \subset \mathrm{Diff}\langle \mathbf{Z}_p^m \rangle$ avec

$$D \coloneqq \{g \in \mathrm{Diff}\langle \mathbf{Z}_p^m \rangle \mid g(0) = 0,\ dg_0 = \mathrm{Id} \mod p\}.$$

On pose $g \coloneqq h^{-1} \circ T_x^{-1} \circ f \circ T_x \circ h$ où h est l'homothétie de rapport p. Alors g est donc un flot analytique Φ_t. Le nouvel ensemble algébrique V est définie par les équations $Q_i(\underline{z}) \coloneqq P_i(p\underline{z} + x) = 0$.

On étudie ainsi l'ensemble

$$\mathrm{Pas}_g(0, V) = \{n \in \mathbf{Z} \mid \forall i,\ Q_i(\Phi_n(0)) = 0\}.$$

D'après le théorème de Strassner, soit l'ensemble $\mathrm{Pas}_g(0, V)$ est fini, soit il est égal à $\mathbf{Z}$ ce qui conclut le théorème pour g. On a donc montré le théorème pour $\mathrm{Pas}_{f^N}(x, W)$, donc aussi pour $\mathrm{Pas}_{f^N}(x, f^{-j}(W))$. Mais

$$\mathrm{Pas}_f(x, W) = \bigcup_{j=0}^{N-1} (N \,\mathrm{Pas}_{f^N}(x, f^{-j}(W)) + j)$$

ce qui permet de conclure le cas général. ◇

Remarque. Les raisons des progressions arithmétique divisent l'indice D de D dans $\mathrm{Diff}\langle \mathbf{Z}_p^m \rangle$.

5.4. Applications

Existe-t-il un automorphisme $f \in \mathrm{Aut}(\mathbf{A}^m_{\mathbf{Z}})$ qui agit transitivement sur l'ensemble $\mathbf{A}^m(\mathbf{Z})$? Pour $m = 1$, la réponse est oui : il suffit de prendre $f(z) = z + 1$. Mais la réponse est non lorsque $m \geqslant 2$.

Théorème 5.8 *(Bell-Glioca-Satians).* Soient K un corps de caractéristique nulle, $f \in \mathrm{Aut}(\mathbf{A}^m_K)$ un automorphisme, $\xi \in K[x_1, \ldots, x_m]$ un polynôme et $x \in \mathbf{A}^m(K)$ un point. Si l'ensemble

$$\{n \in \mathbf{Z} \mid \xi(f^n(x)) = a\}$$

est fini pour tout élément $a \in K$, alors leurs cardinaux sont uniformément bornés.

Théorème 5.9. Soit $m \geqslant 1$ un entier. Alors il existe un entier $q(m) \in \mathbf{N}$ tel que, pour tout automorphisme $f \in \mathrm{Aut}(\mathbf{A}^m_{\mathbf{Z}})$ et tout point $x \in \mathbf{A}^m(\mathbf{Z})$, si x est périodique pour f, alors sa période est $\leqslant q(m)$.

Chapitre 6

Valeurs absolues sur les extensions finies d'un corps valué

Soit $z := [z_0 : \ldots : z_m] \in \mathbf{P}^m(\mathbf{Q})$ un point de l'espace projectif de dimension m. On peut l'écrire sous la forme $z = [Z_0 : \ldots : Z_m]$ pour des entiers $Z_i \in \mathbf{Z}$ sans facteurs commun et non égaux à ± 1. La *hauteur* du point z est la quantité

$$h(z) := \log(\max(|Z_1|, \ldots, |Z_m|)).$$

On va se poser deux questions :

- comment étendre cette définition à l'espace projectif $\mathbf{P}^m(\overline{\mathbf{Q}})$?
- comment se comporte la quantité $h(z)$ quand on change z en $f(z)$ pour une fonction polynomiale $f : \mathbf{P}^m_{\overline{\mathbf{Q}}} \longrightarrow \mathbf{P}^m_{\overline{\mathbf{Q}}}$?

6.1. Places

Définition 6.1. Une *place* d'un corps K est une classe d'équivalence de valeurs absolues non triviales sur K. L'ensemble des places est noté M_K. Pour une place $v \in M_K$, on note $|\cdot|_v$ un de ses représentants

Exemple. L'ensemble $M_{\mathbf{Q}}$ est constitué des classes des valeurs absolues $|\cdot|_p$ pour un nombre premier p et de la classe de la valeur absolue $|\cdot|_\infty$.

Soient $L : K$ une extension de corps et $w \in M_L$ une place. Alors la restriction de la valeur absolue $|\cdot|_v$ à K détermine une valeur absolue sur K et donc une place sur K. On obtient alors une application $v \in M_L \longmapsto w \in M_K$ et on note $w \mid v$.

6.2. Théorème de l'élément primitif

Soient $L : K$ une extension finie et $\overline{K}$ une clôture algébrique de K. Un *plongement* de L dans $\overline{K}$ est un morphisme de corps $\iota : L \longrightarrow \overline{K}$ qui est l'identité sur K. Comme l'extension $L : K$ est finie, on peut écrire $L = K(\alpha_1, \ldots, \alpha_r)$ pour des éléments $\alpha_i \in L$. Le *degré séparable* de l'extension $L : K$, noté $[L : K]_{\text{sep}}$ est le nombre de plongements de L dans $\overline{K}$: comme le degré, cette notion est multiplicative.

Proposition 6.2. Si $L = K(\alpha)$ et $P \in K[t]$ est le polynôme minimal de α, alors tout plongement doit envoyer α sur une racine de P dans $\overline{K}$ et il est uniquement déterminé par ce choix. En

particulier, on a

$$[L : K]_{\text{sep}} \leqslant \deg P = [L : K].$$

Avec la multiplicativité, on en déduit l'inégalité

$$[L : K]_{\text{sep}} \leqslant [L : K]$$

pour toute extension finie $L : K$. L'extension est *séparable* si on a égalité. Ainsi l'extension $L : K$ est sépable si et seulement si le polynôme minimal de tout élément $\alpha \in L$ est scindé simple sur $\overline{K}$.

Théorème 6.3 *(de l'élément primitif).* Soient K un corps et L une extension finie de K. Alors il existe un élément $\xi \in L$ tel que $L = K(\xi)$ si et seulement si le nombre d'extensions intermédiaires entre K et L est fini. En particulier, la condition est vérifiée lorsque l'extension $L : K$ est séparable.

Un tel élément ξ est appelé un *élément primitif*.

Démonstration. Si K est fini, alors L l'est aussi, donc $L^\times$ est un groupe cyclique, donc un générateur ξ de ce dernier convient. On suppose désormais que K est infini.

On suppose qu'il n'existe qu'un nombre fini d'extensions intermédiaires entre K et L. On veut que montrer que, si $\alpha, \beta \in L$, le corps $K(\alpha, \beta)$ est primitif. Mais si $K(\alpha + c_1\beta) = K(\alpha + c_2\beta)$ avec $c_1 \neq c_2$, alors $K(a + c_1\beta) = K(\alpha, \beta)$ car $(c_1 - c_2)\beta \in K(a + c_1\beta)$. Comme il n'y a qu'un nombre fini d'extension intermédiaire et que K est infini, on peut trouver deux tels éléments c_1 et c_2. On conclut alors par récurrence.

Réciproquement, on suppose que $L = K(\xi)$. Soit $P \in K[t]$ le polynôme minimal de ξ. Soit K' une extension intermédiaire. Soit $Q \in K'[t]$ le polynôme de ξ sur K'. Alors $Q \mid P$ dans $K'[t]$ et donc dans $L[t]$. Il n'existe donc qu'un nombre fini de Q possible. Maintenant, un tel polynôme Q étant donné, on associe l'extension intermédiaire K'_0 engendré par les coefficients de Q. Alors $K'_0 \subset K'$. De plus, comme Q est irréductible sur K'_0, donc $[L : K'_0] = \deg Q = [L : K']$, donc $K'_0 = K'$. Ainsi le choix de Q détermine le choix de K' ce qui conclut.

On suppose que l'extension $L : K$ est séparable. Soient $\iota_j \colon L \longrightarrow \overline{K}$ les plongements. Supposons que $L = K(\alpha, \beta)$. On cherche un $\xi \in K(\alpha, \beta)$ tel que

$$[K(\xi) : K] = [L : K].$$

On le cherche sous la forme $\xi = \alpha + c\beta$. En prenant c évitant les valeurs $(\iota_i(\alpha) - \iota_j(\alpha))/(\iota_i(\beta) - \iota_j(\beta))$, cela fonctionne. ◇

6.3. Extensions de valeurs absolues aux extensions primitives

Soient $v \in M_K$ une place et $L = K(\xi)$ une extension primitive. Notons $K_v \supset K$ la complété pour la valeur absolue $|\cdot|_v$ et $\overline{K_v} \supset \overline{K}$ sa clôture algébrique. On veut étendre $|\cdot|_v$ à L. Soit $P \in K[t]$ le polynôme minimal de ξ.

Remarque. Si $\iota \colon L \longrightarrow \overline{K_v}$ est un plongement de L dans $\overline{K_v}$, alors on peut composer la valeur absolue $|\cdot|_v$ avec ι

$$|x|_w \coloneqq |\iota(x)|_v$$

qui définit une valeur absolue sur L qui coïncide avec $|\cdot|_v$ sur K.

L'image de ι est contenu dans $\overline{K} \subset \overline{K_v}$. L'image de $P(t)$ par ι est $P(t)$, mais vu comme un polynôme de $K_v[t]$, il peut se factoriser. On écrit

$$P(t) = P_1(t)^{k_1} \cdots P_s(t)^{k_s}$$

sa factorisation dans $K_v[t]$. De plus, $\iota(\xi)$ est une racine de P dans $\overline{K}$, donc son polynôme minimal est l'un des P_i, donc l'image de L coïncide avec l'extension associée à ce P_i dans $\overline{K_v}$ qu'on note $K_i \coloneqq K_v[t]/(P_i)$. Cette dernière est une extension finie de K_v de degré $\deg P_i$. Soit L_w le complété pour $|\cdot|_w$. Alors ι s'étend $(L_w, |\cdot|_w) \longrightarrow (K_i, |\cdot|_v)$ comme un morphisme de corps isométrique. L'image de L_w contient K_v et $t \mod P_i$, donc $\iota(L_w) = K_i$

Remarque. Réciproquement, soit $|\cdot|_w$ une valeur absolue sur L qui étend $|\cdot|_v$ sur K. On note L_w le complété de L pour $|\cdot|_w$. Alors $L_w \supset K_v$, donc $L_w \supset K_v(\xi)$ et donc $L_w = K_v(\xi)$ car

$K_v(\xi) \supset K(\xi) = L$ est dense dans L_w et $K_v(\xi)$ est une extension finie, donc fermée et complète dans K_v. Le polynôme minimal de ξ sur K_v est un diviseur irréductible de P dans $K_v[t]$, donc c'est l'un des P_i. Donc $L_W \simeq K_v[t]/(P_i)$.

Des deux remarques, on en déduit que toute valeur absolue $|\cdot|_v$ sur K s'étend à L. Toute extension est donnée par image réciproque de la valeur absolue $|\cdot|_v$ sur $\overline{K_v}$ par un plongement $\iota\colon L \longrightarrow \overline{K_v}$. Autrement dit, pour tous $v \in M_K$ et $w \in M_L$, il existe un plongement $\iota\colon L \longrightarrow \overline{K_v}$ tel que $|\cdot|_w = |\iota(\cdot)|_v$.

Exemple. On prend $L = \mathbf{Q}(\sqrt{5}) \subset \mathbf{R}$. On cherche à étendre la valeur absolue usuelle $|\cdot|_\infty$ sur $\mathbf{Q}$. Son complété est $\mathbf{R}$. Le polynôme minimal de $\sqrt{5}$ est $P(t) \coloneqq t^2 - 5$. Sur $\mathbf{R}$, on a

$$P(t) = (t - \sqrt{5})(t + \sqrt{5}).$$

Il y a 2 plongements possibles de L dans R : celui qui envoie t sur $+\sqrt{5}$, noté ι_1, et celui qui envoie t sur $-\sqrt{5}$, noté ι_2. Alors

$$\iota_2 = \iota_1 \circ \sigma \quad \text{avec} \quad \sigma(a + b\sqrt{5}) = a - b\sqrt{5}.$$

Alors

$$|a + b\sqrt{5}|_{w_1} = |\iota_1(a + b\sqrt{5})|_\infty = |a + b\sqrt{5}|_\infty,$$
$$|a + b\sqrt{5}|_{w_2} = |\iota_2(a + b\sqrt{5})|_\infty = |a - b\sqrt{5}|_\infty.$$

Exemple. On prend $L = \mathbf{Q}(i)$. Alors $\mathbf{Q}_\infty = \mathbf{R}$ et le polynôme $P(t) \coloneqq t^2 + 1$ est encore irréductible sur $\mathbf{R}$. On obtient les deux valeurs absolues

$$|a + ib|_\infty \qquad \text{et} \qquad |a - ib|_\infty$$

qui se trouvent être la même.

Conséquence. Si $L : K$ est une extension finie séparable et si $v \in M_K$, alors

$$\sum_{\substack{w \in M_L \\ w|v}} [L_w : K_v] = [L : K].$$

Démonstration. En effet, les k_i sont égaux à 1 car l'extension est séparable et on peut donc écrire

$$\begin{aligned} \sum [L_w : K_v] &= \sum \deg P_i \\ &= \deg P \\ &= [L : K]. \end{aligned}$$

◇

Conséquence. Soient $L : K$ une extension galoisienne de groupe de Galois G et $|\cdot|_v$ une valeur absolue sur K. Alors G permute transitive les extensions $|\cdot|_w$ et $|\cdot|_v$: pour toute valeur absolue $|\cdot|_w$ et $|\cdot|_{w'}$ de $|\cdot|_v$, il existe $\sigma \in G$ tel que $|\sigma(\cdot)|_w = |\cdot|_{w'}$.

6.4. Corps cyclotomiques

Soient $p \geqslant 3$ un nombre premier et ξ une racine de l'unité d'ordre p. Son polynôme minimal sur le corps $\mathbf{Q}$ est

$$P(t) \coloneqq t^{p-1} + t^{p-2} + \cdots + 1.$$

En effet, il annule bien la racine ζ et il est irréductible sur $\mathbf{Q}$ en appliquant le critère d'Eisenstein au polynôme $P(t+1)$. On écrit $P(t) = P_1(t) \cdots P_r(t)$ avec $r \coloneqq (p-1)/2$ dans $\mathbf{R}[X]$ où chaque polynôme P_i est de degré 2.

Exemple. Dans le cas $p = 5$, on a $P_1(t) = t^2 - 2\cos(\frac{2\pi}{5})t + 1$ et on calcul de même $P_2(t)$.

Il y a donc r extensions K_i de degrés locaux 2. Un élément du groupe de Galois σ_k est uniquement déterminé par l'image de ζ qui est une puissance ζ^k.

Exemple. Par exemple, si $p = 5$ et $\sigma_2(\xi) = \xi^2$, alors un élément

$$a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 + a_4\xi^4$$

est envoyé sur l'élément

$$a_0 + a_1\xi^2 + a_2\xi^4 + a_3\xi + a_4\xi^3.$$

Le deuxième automorphisme est la conjugaison σ_4.

De manière général, le groupe de Galois est d'ordre $p-1$ et il existe r valeurs absolues distinctes qui étendent la valeur absolue triviale de $\mathbf{Q}$ à L.

Exemple. On considère la valeur absolue p-adique. Le critère d'Eisenstein s'applique encore dans l'anneau $\mathbf{Z}_p$: le polynôme $P(t)$ est irréductible dans $\mathbf{Q}_p[t]$, donc il existe une unique extension de la valeur absolue p-adique à une extension $\mathbf{Q}(\xi) = \mathbf{Q}[t]/(P)$ et le groupe de Galois agit par isométries.

Comment étendre la valeur absolue $|\cdot|_q$ de $\mathbf{Q}$ à L pour $q \neq p$? Soient $\mathbf{F}_q$ le corps fini à q éléments et $\mathbf{F}_{q^s}$ une extension de degré s. Alors cette dernière question un élément d'ordre p si et seulement si $p \mid q^s - 1$, c'est-à-dire $q^s \equiv 1 \mod p$. Les points suivants sont équivalents :

- le corps $\mathbf{F}_{q^r}$ contient un élément d'ordre p ;
- l'entier r est l'ordre de l'élément q dans $(\mathbf{Z}/p\mathbf{Z})^\times$.

On choisit un entier r comme cela. Considérons l'automorphisme de Frobenius

$$\varphi\colon \left| \begin{array}{l} \mathbf{F}_{q^r} \longrightarrow \mathbf{F}_{q^r}, \\ \quad z \longmapsto z^q \end{array} \right. .$$

Il est d'ordre $r = [\mathbf{F}_{q^r} : \mathbf{F}_q]$ et ses points fixes sont exactement les éléments du corps $\mathbf{F}_q$. Donc le groupe cyclique engendré par l'automorphisme φ est d'ordre r et coincide donc avec le groupe de Galois $\mathrm{Gal}(\mathbf{F}_{q^r} : \mathbf{F}_q)$.

De plus, comme le corps $\mathbf{F}_{q^r}$ contient un élément x d'ordre p, il contient ses puissances x, x^2, …, x^{p-1} et donc toutes les racines primitives p-ièmes de $\overline{\mathbf{F}_q}$. Si x^j est une telle racine, son orbites sous le morphisme φ est $\{x^j, \dots, x^{q^r j}\}$ et, comme q est inversible modulo p, ces puissances sont deux à deux distinctes et il y en a r. On obtient alors une factorisation

$$P(t) = P_1(t) \cdots P_k(t)$$

avec $k = (p-1)/r$ et chaque polynôme P_i ont pour racine une orbite du morphisme φ. Ceci est la décomposition en facteurs irréductibles dans $\mathbf{F}_q[t]$.

Passons à $\mathbf{Q}_q[t]$. Comme $P \in \mathbf{Z}[t] \subset \mathbf{Z}_q[t]$, le lemme de Hensel fournit la décomposition en facteurs irréductible $P = \tilde{P}_1 \cdots \tilde{P}_k$ dans $\mathbf{Z}_q[t]$ et donc dans $\mathbf{Q}_q[t]$. Il existe donc $k = (p-1)/r$ extensions de la valeurs absolue $|\cdot|_q$ au corps $L \coloneqq \mathbf{Q}(t)/(P)$. Chaque extension $(L, |\cdot|_w)$ est isomorphe au corps $\mathbf{Q}_q[t]/(\tilde{P}_j)$ pour un unique indice j.

6.5. La formule du produit

Soient K un corps et $|\cdot|_v$ une valeur absolue sur K. Soit L une extension finie séparable de K. On peut l'écrire $L = K(\xi)$. La valeur absolue $|\cdot|_v$ s'étend en un nombre fini de valeurs absolues $|\cdot|_w$ à L. Ces extensions sont construites par le plongement $L \longrightarrow \overline{K_v}$.

Si $|\cdot|_w$ est une valeur absolue sur L, alors sa restriction à K détermine une valeur absolue sur K. Notons-la $|\cdot|_v$ où $w \mid v$. Alors $K_v \subset L_w$. Soit P_j le polynôme minimal de ξ sur K_v. Alors $L_w = K_v[t]/(P_j)$, donc la valeur absolue $|\cdot|_v$ s'étend de manière unique à L et l'extension est $|\cdot|_w$ et

$$|\xi|_w = |\mathrm{Norme}_{L_w:K_v}(\xi)|_v^{1/[L_w:K_v]} = |P_j(0)|_w^{1/\deg P_j}.$$

donc

$$\prod_{w|v} |\xi|_w^{[L_w:K_v]} = \prod_{j=1}^{k} |P_j(0)|_v = |P(0)|_v = |\mathrm{Norme}_{L:K}(\xi)|^{[L:K]}.$$

De manière équivalente, on obtient

$$\frac{1}{[L:K]}\sum_{w|v}[L_w:K_v]\log|\xi|_v=\log|\mathrm{Norme}_{L:K}(\xi)|_v\,.$$

Proposition 6.4. Pour tout élément $x\in L$, on a

$$\prod_{w|v}|x|_w^{[L_w:K_v]}=|\mathrm{Norme}_{L:K}(x)|_v^{[L:K]}.$$

Démonstration. On introduit l'extension intermédiaire $K\subset K(x)\leqslant L$. ◇

On peut appliquer tout cela aux corps de nombres, c'est-à-dire aux extensions finies de $\mathbf{Q}$.

Proposition 6.5 *(formule du produit).* Soit L une extension finie de $\mathbf{Q}$. Soit $x\in L\setminus\{0\}$ un élément. Alors

$$\prod_{w\in M_L}|x|_w^{[L_w:\mathbf{Q}_w]}=1.$$

Démonstration. La proposition précédente et la formule du produit dans $\mathbf{Q}$ donnent

$$\begin{aligned}\prod_{w\in M_L}|x|_w^{[L_w:\mathbf{Q}_w]}&=\prod_{p\in\mathscr{P}\cup\{\infty\}}\prod_{w|p}|x|_w^{[L_w:\mathbf{Q}_w]}\\&=\prod_{p\in M_{\mathbf{Q}}}|\mathrm{Norme}_{L:\mathbf{Q}}(x)|_v^{[L:\mathbf{Q}]}=1.\end{aligned}$$

◇

Deuxième partie

HAUTEURS ET HAUTEURS CANONIQUES

Chapitre 7

Hauteur d'un point de l'espace projectif, hauteur d'un polynôme

7.1. Hauteur d'un point de l'espace projectif

Soit $z \coloneqq [z_0 : \ldots : z_m] \in \mathbf{P}^m(\overline{\mathbf{Q}})$. On pose

$$h(z) \coloneqq \frac{1}{[K : \mathbf{Q}]} \sum_{v \in M_K} [K_v : \mathbf{Q}_v] \log(\max(|z_1|_v, \ldots, |z_m|_v))$$

pour une extension finie $K \supset \mathbf{Q}$ contenant les éléments z_i. Cette définition

(a) ne dépend pas du choix des éléments z_i ;
(b) ne dépend pas du choix de l'extension finie K.

Le point (a) est clair puisque multiplier par un nombre λ les coordonnées revient à rajouter le terme

$$\frac{1}{[K : \mathbf{Q}]} \sum_{v \in M_K} [K_v : \mathbf{Q}_v] \log |\lambda|_v = 0.$$

Pour le point (b), il faut que, si K est remplacé par une extension finie $\mathbf{Q} \subset K \subset L$, alors la quantité $h(z)$ calculée dans L est la même que celle calculée dans L car on a la relation

$$\forall x \in K,\ \forall v \in M_K, \qquad \prod_{w|v} |x|_w^{[L_w : K_v]} = |x|_v^{[L:K]}$$

et la multiplicativité des degrés.

Par ailleurs, la quantité $h(z)$ est une somme finie. En effet, en utilisant le point (a), on peut se ramener au cas où les éléments z_j sont des entiers algébriques. Dans ce cas, pour toute place v, on a $|z_j|_v \leqslant 1$ et la somme

$$\sum_{p \in \mathscr{P}} \sum_{v|p} \cdots$$

qui intervient dans $h(z)$ ne porte que sur les nombres premiers p qui divise l'un des nombres $\mathrm{Norme}_{K:\mathbf{Q}}(z_i)$.

Exemple. On considère le point

$$z \coloneqq \left[\frac{3}{4} : \frac{1}{\sqrt{5}} : 2\right] = [3\sqrt{5} : 4 : 8\sqrt{5}] \in \mathbf{P}^2(\overline{\mathbf{Q}}).$$

Pour tout nombre premier p et toute valeur absolue $|\cdot|_v$ étant la valeur absolue $|\cdot|_p$, on a

$$|3\sqrt{5}|_v, |4|_v, |8\sqrt{5}|_v \leqslant 1$$

car les trois nombres sont des entiers algébrique. En effet, par exemple, on a $|3|_v = 1$ si $v \mid p$ avec $p \wedge 3 = 1$ et $= 1/3$ si $p \mid 3$. De même pour $\left|\sqrt{5}\right|_v$. Donc $\left|3\sqrt{5}\right|_v \leqslant 1$. Ainsi pour tout nombre premier p, le maximum des trois valeurs absolues est 1 si $v \mid p$. Donc la somme est finie. Avec $K = \mathbf{Q}(\sqrt{5})$, on calcul ainsi

$$h(z) = \frac{1}{[K : \mathbf{Q}]} \sum_{v|\infty} [K_v : \mathbf{Q}_v] \log(\max(|3\sqrt{5}|_v, |4|_v, |8\sqrt{5}|_v)).$$

Or il existe deux plongements $K \hookrightarrow \mathbf{R}$, donc

$$\begin{aligned} h(z) &= \frac{1}{2} \sum_{\text{2 choix}} [\mathbf{R} : \mathbf{R}] \log(8\sqrt{5}). \\ &= \log(8\sqrt{5}) \end{aligned}$$

Ainsi les quantités $h(z)$ définissent une fonction $\mathbf{P}^m(\overline{\mathbf{Q}}) \longrightarrow \mathbf{R}_+$. Elle est invariante par permutation des coordonnées.

Si $x = (x_1, \ldots, x_m) \in \mathbf{A}^m(\overline{\mathbf{Q}})$, on pose $h(x) \coloneqq h([1 : x_1 : \ldots : x_m])$. Pour $x \in \overline{\mathbf{Q}} \simeq \mathbf{A}^1(\overline{\mathbf{Q}})$, en notant K un corps de nombres qui contient x, on a

$$\begin{aligned} h(x) &= \frac{1}{[K : \mathbf{Q}]} \sum_{v \in M_K} [K_v : \mathbf{Q}_v] \log(\max(1, |x|_v)) \\ &= \frac{1}{[K : \mathbf{Q}]} \sum_{v \in M_K} [K_v : \mathbf{Q}_v] \log^+ |x|_v. \end{aligned}$$

Lemme 7.1. Soit $K/\mathbf{Q}$ une extension galoisienne contenant les éléments z_i. Soit $\sigma \in \mathrm{Gal}(K : \mathbf{Q})$. Alors $h(\sigma(z)) = h(z)$ avec $\sigma(z) \coloneqq [\sigma(z_0) : \ldots : \sigma(z_m)]$.

Démonstration. On remarque que l'automorphisme σ permute les extensions $|\cdot|_v$ de la valeur absolue $|\cdot|_v$ pour tout nombre premier p. ◇

Théorème 7.2 *(Kronecker).* Un nombre algébrique $\xi \in \overline{\mathbf{Q}}^\times$ est une racine de l'unité si et seulement si $h(\xi) = 0$.

Démonstration. On suppose que $\xi^N = 1$. Alors $|\xi|_v = 1$ pour tout v, donc $h(\xi) = 0$. Réciproquement, on suppose que le nombre ξ est de hauteur nulle. Soit $P \in \mathbf{Q}[t]$ son polynôme minimal. Soit $\xi_1 = \xi$, …, ξ_d ses racines dans $\overline{\mathbf{Q}}$. Le groupe $\mathrm{Gal}(\overline{\mathbf{Q}} : \mathbf{Q})$ permute transitivement les nombres ξ_i, donc $h(\xi_i) = 0$ pour tout i. Comme

$$h(\xi_i) = \frac{1}{[K : \mathbf{Q}]} \sum_{v \in M_K} [K_v : \mathbf{Q}_v] \log^+ |\xi_i|_v,$$

on en déduit que $|\xi_i|_v \leqslant 1$ pour tout $v \in M_K$. Donc les coefficients du polynôme $P = \prod_{i=1}^d (t - \xi_i)$ sont des nombres rationnels a_i et également des fonctions symétriques en les éléments ξ_i à coefficients entiers, donc $|a_i|_v \leqslant 1$ pour toute $v \in M_K$ ultramétrique, c'est-à-dire $|a_i|_p \leqslant 1$ pour tout p premier, donc $a_i \in \mathbf{Z}$ et $P \in \mathbf{Z}[t]$. Ainsi le nombre ξ est un entier algébrique. Par ailleurs, on a $|\xi_j|_v \leqslant 1$ pour tout j et $v \mid \infty$, donc $|\xi_j^N|_v \leqslant 1$ pour tout j, $N \geqslant 1$ et $v \mid \infty$. Alors le polynôme minimal P_N de ξ^N appartient à $\mathbf{Z}[t]$ de degré $\leqslant d$ et ses coefficients sont des fonctions symétriques en les éléments ξ_i^N à coefficients entiers, donc ils sont uniformément majorés indépendamment de N. Donc il n'y a qu'un nombre fini de P_N possibles. Ainsi les éléments ξ^N pour $N \geqslant 1$ ne prennent qu'un nombre fini de valeurs, donc il existe $N < N'$ tel que $\xi^N = \xi^{N'}$ ce qui donne $\xi^{N-N'} = 1$. ◇

La hauteur h est souvent qualifiée de logarithmique ou d'additive.

7.2. Hauteur d'un polynôme

Le *mesure de Mahler logarithmique* d'un polynôme $P \in \mathbf{C}[t] \setminus \{0\}$ est la quantité

$$m(P) \coloneqq \int_0^1 \log|P(e^{2i\pi\theta})| \, \mathrm{d}\theta.$$

Elle est bien définie car la fonction $t \longmapsto \log t$ est intégrable sur chaque intervalle $]0, \varepsilon]$ avec $\varepsilon > 0$. Par convention, on pose $m(0) \coloneqq -\infty$. La *mesure de Malher* est la quantité $M(P) \coloneqq \exp(m(P))$.

Théorème 7.3 *(formule de Jensen).* Si $P(t) = a_d \prod_{i=1}^{d}(t - z_i)$ est un polynôme non nul, alors

$$m(P) = \log|a_d| + \sum_{i=1}^{n} \log^+|z_i|\,.$$

Démonstration. On écrit

$$\log|P(e^{2i\pi\theta})| = \log|a_d| + \sum_{j=1}^{d} \log\left|e^{2i\pi\theta} - z_j\right|,$$

donc il s'agit de montrer que

$$\forall w \in \mathbf{C}, \qquad \int_0^1 \log\left|e^{2i\pi\theta} - z_j\right| = \log^+|w|\,.$$

Si $|w| > 1$, la fonction

$$u\colon w \in \overline{\mathbf{D}} \longmapsto \log|z - w|$$

est harmonique, donc sa moyenne sur le cercle unité est égale à sa valeur au centre $\log|w|$. Si $|w|\,1$, on remarque que

$$\log\left|e^{2i\pi\theta} - w\right| = \log\left|1 - we^{-2i\pi\theta}\right|$$

et on est ramené au cas précédent, donc la moyenne sur le cercle unité est égale à $\log 1 = 0 = \log^+|w|$. Si $|w| = 1$, il suffit d'appliquer le théorème de convergence dominée. ◇

Théorème 7.4. Si $P \in \mathbf{Z}[t]$ est le polynôme minimal non unitaire de $x \in \overline{\mathbf{Q}}$, alors

$$h(x) = \frac{m(P)}{\deg P}.$$

Démonstration. Soit K une extension finie galoisienne de $\mathbf{Q}$ contenant toutes les racines de P. Dans cette extension, on note $P = a\sum_{i=1}^{d}(t - z_i)$.

D'abord, pour toute place $v \in M_K^F$, on remarque que $\|P\|_v = 1$. Mais la norme de Gauss est multiplicative, on obtient

$$\|P\|_v = |a|_v \prod_{i=1}^{d} \max(1, |z_i|_v),$$

donc

$$0 = \log|a|_v + \sum_{i=1}^{d} \log^+|z_i|_v.$$

Soit $\sigma \in G \coloneqq \mathrm{Gal}(K : \mathbf{Q})$ un élément du groupe de Galois. On sait que $h(\sigma(x)) = h(x)$, que G permute les racines de P et que $|G| = [K : \mathbf{Q}]$. Ainsi dans la liste $(\sigma(x))_{\sigma\in G}$, on trouve toutes les racines z_i répétées exactement $[K : \mathbf{Q}]/d$ fois. On obtient alors

$$[K : \mathbf{Q}]^2 h(x) = \sum_{v\in M_K} [K_v : \mathbf{Q}_v] \sum_{\sigma\in G} \log^+|\sigma(x)|_v.$$

Soit $v \mid p$ avec $p \in M_{\mathbf{Q}}$. Alors

$$\sum_{\sigma\in G} \log^+|\sigma(x)|_v = \frac{[K : \mathbf{Q}]}{d} \sum_{i=1}^{d} \log^+|z_i|_p.$$

Avec ces deux dernières égalités, on trouve

$$[K : \mathbf{Q}]^2 h(x) = \frac{[K : \mathbf{Q}]}{d} \sum_{v\in M_K} [K_v : \mathbf{Q}_v] \sum_{i=1}^{d} \log^+|z_i|_v.$$

On prend $p=\infty$. Si $v\in M_K^\infty$, alors

$$\sum_{i=1}^d \log^+|z_i|_v = \sum_{i=1}^d \log^+|z_i|$$

et

$$\sum_{v|\infty}[K_v:\mathbf{R}] = [K:\mathbf{Q}].$$

On obtient alors

$$\frac{[K:\mathbf{Q}]}{d}\sum_{v\in M_K^\infty}[K_v:\mathbf{Q}_v]\sum_{i=1}^d \log^+|z_i|_v = \frac{[K:\mathbf{Q}]^2}{d}\sum_{i=1}^d \log^+|z_i|.$$

Par ailleurs, avec la formule du produit, on a

$$\begin{aligned}\sum_{v\in M_K^F}[K_v:\mathbf{Q}_v]\sum_{i=1}^d \log^+|z_i| &= -\sum_{v\in M_K^F}[K_v:\mathbf{Q}_v]\log|a_d|_v\\ &= \sum_{v\in M_K^\infty}[K_v:\mathbf{Q}_v]\log|a_d|_\infty\\ &= [K:\mathbf{Q}]\log|a_d|,\end{aligned}$$

donc

$$\frac{[K:\mathbf{Q}]}{d} = \frac{[K:\mathbf{Q}]^2}{d}\log|a_d|.$$

Ceci conclut. ◇

Corollaire 7.5. Soit $x\in\overline{\mathbf{Q}}$. Alors

$$\frac{1}{\deg x}\log|\mathrm{Norme}_{\mathbf{Q}(x):\mathbf{Q}}(x)| \leqslant h(x).$$

7.3. Théorème de finitude de Northcott

7.3.1. Comparaison de normes

La mesure multiplicative de Malher vérifie

$$M(P) = \lim_{p\to 0}\left(\int_0^1 |P(e^{2i\pi\theta})|^p\,\mathrm{d}\theta\right)^{1/p}.$$

Pour un polynôme $P\coloneqq\sum_{i=0}^d a_i t^i$, on pose

$$\|P\|_{\ell^\infty} = \max(|a_1|,\dots,|a_d|).$$

On a également la norme L^1 ou L^2 sur le cercle unité. Par exemple, la seconde s'écrit

$$\|P\|_{\mathrm{L}^2(\mathbf{S}^1,\mathrm{d}\theta)} = \left(\int_0^1 |P(e^{2i\pi\theta})|^2\,\mathrm{d}\theta\right)^{1/2}.$$

La formule de Poisson donne

$$\begin{aligned}\|P\|_{\mathrm{L}^2(\mathbf{S}^1,\mathrm{d}\theta)} &\leqslant \Big(\sum_{i=0}^d |a_i|^2\Big)^{1/2}\\ &\leqslant \sqrt{d+1}\|P\|_{\ell^\infty}.\end{aligned}$$

Lemme 7.6. Pour tout polynôme complexe $P=\sum_{i=0}^d a_i t^i$, on a

$$\binom{d}{\lfloor d/2\rfloor}^{-1}\|P\|_{\ell^\infty} \leqslant M(P) \leqslant \|P\|_{\mathrm{L}^2(\mathbf{S}^1,\mathrm{d}\theta)}.$$

Démonstration. Montrons d'abord la première inégalité. On suppose que $a_d \neq 0$. On a

$$\left|\frac{a_{d-r}}{a_d}\right| \leqslant \sum_{j_1<\cdots<j_k} |z_{j_1}\cdots z_{j_d}|$$

où les z_i sont les racines de P de telle sorte que

$$\left|\frac{a_{d-r}}{a_d}\right| \leqslant \binom{d}{r}\prod_{i=1}^{d}\max(1,|z_i|),$$

donc

$$|a_{d-r}| \leqslant a_d\binom{d}{\lfloor d/2\rfloor}\prod_{i=1}^{d}\max(1,|z_i|) = \binom{d}{\lfloor d/2\rfloor}M(P).$$

Passons à la seconde. En utilisant la concavité du logarithme et l'inégalité de Cauchy-Schwarz, on trouve

$$M(P) = \exp\int_0^1 \log|P(e^{2i\pi\theta})|\,\mathrm{d}\theta \leqslant \int_0^1 |P(e^{2i\pi\theta})|\,\mathrm{d}\theta \leqslant \|P\|_{\mathrm{L}^2(\mathbf{S}^1,\mathrm{d}\theta)}.$$ ◇

Définition 7.7. Le *degré* d'un point $z \coloneqq [z_0 : \cdots : z_m] \in \mathbf{P}^m(\overline{\mathbf{Q}})$ est le petit degré $[K : \mathbf{Q}]$ d'un corps de nombres K tel que $z = [w_0 : \cdots : w_m]$ pour des éléments $w_i \in K$.

7.3.2. Le théorème

Théorème 7.8 *(Northcott).* Soit $B \geqslant 0$ un réel. Alors l'ensemble des points $x \in \overline{\mathbf{Q}}$ (resp. $z \in \mathbf{P}^m(\overline{\mathbf{Q}})$) tels que

$$\deg z \leqslant B \qquad \text{et} \qquad h(z) \leqslant B$$

est fini.

Démonstration. Soit $x \in \overline{\mathbf{Q}}$ un point tel que $\deg z \leqslant B$ et $h(z) \leqslant B$. Soit $P \in \mathbf{Z}[t]$ le polynôme minimal de x qu'on note $P = \sum_{i=0}^{d} a_i t^i$. D'après le lemme, on a

$$\max_{1\leqslant i\leqslant d}|a_i| \leqslant \binom{B}{\lfloor B/2\rfloor}\exp(B\times B).$$

Ainsi le degré de P est les coefficients $|a_i|$ sont bornées par une fonction de B, donc il y a un nombre fini d'éléments x possibles.

Donnons l'idée dans le cas projectif. On peut procéder avec les étapes suivantes :

1. on recouvre l'espace projectif $\mathbf{P}^m(\overline{\mathbf{Q}})$ par les espaces affines $\mathbf{A}^m(\overline{\mathbf{Q}}) \coloneqq \{z_i \neq 0\}$;
2. on utiliser la première partie du théorème pour montrer que l'ensemble
$$\{(x_1,\ldots,x_m) \in \mathbf{A}^m(\overline{\mathbf{Q}}) \mid \forall i \in [\![1,n]\!],\ \deg x_i \leqslant B \text{ et } h(x_i) \leqslant B\}$$
3. et on conclut. ◇

Remarque. On fixe un corps de nombres K. On cherche à estimer la quantité

$$\sharp\{z \in \mathbf{P}^m(K) \mid h(z) \leqslant B\} \in \mathbf{N}$$

lorsque $n \longrightarrow +\infty$.

Exemple. Pour $K = \mathbf{Q}$, soit $z \coloneqq [z_1 : \cdots : z_m] \in \mathbf{P}^m(\overline{\mathbf{Q}})$ un point où les nombres z_i sont entiers et globalement premiers entre eux. Alors $h(z) \leqslant B$ si et seulement si $\max_{1\leqslant i\leqslant m}|z_i| \leqslant \exp(B)$. Dans le cas $n = 1$, il s'agit de dénombrer les couples d'entiers (x, y) de taille $\leqslant \exp(B)$ tel que $x \wedge y = 1$. Lorsque $B \longrightarrow +\infty$, on a l'estimation

$$\sharp\{z \in \mathbf{P}^m(\overline{\mathbf{Q}}) \mid h(z) \leqslant B\} \sim \frac{2^m}{\zeta(m+1)}e^{(m+1)B}.$$

Chapitre 8
Hauteur canonique

8.1. Endomorphisme

Définition 8.1. Soit K un corps. Un *endomorphisme* de $\mathbf{P}^m_K$ est la donnée de m polynômes homogènes $f_i \in K[x_0 : \cdots : x_m]$ de même degré d tels

$$\{(z_0, \ldots, z_m) \in \overline{K}^{m+1} \mid \forall i,\ f_i(z_0, \ldots, z_m) = 0\} = \{0\}.$$

On pose alors

$$f[x_0 : \cdots : x_m] \coloneqq [f_0(x_0, \ldots, x_m) : \cdots : f_m(x_0, \ldots, x_m)].$$

Le *degré* de f est l'entier d.

Remarques.
- On a $\deg(f \circ g) = \deg f \times \deg g$.
- Soit $H \subset \mathbf{P}^m_{\overline{K}}$ un hyperplan projectif, c'est-à-dire un sous-ensemble d'équation $\sum_{i=0}^m a_i x^i = 0$ avec $a_i \in \overline{K}$. L'ensemble $f^{-1}(H)$ est une hypersurface algébrique de degré d. Soit $L \subset \mathbf{P}^m_{\overline{K}}$ une droite projective. Alors
$$\sharp L \cap f^{-1}(H) = \deg f$$
compté avec multiplicité.
- Soit $z \in \mathbf{P}^m(\overline{K})$. Alors
$$\sharp f^{-1}(z) = (\deg f)^m$$
compté avec multiplicité.

Exemples.
- Les endomorphismes de degré 1 forment un groupe isomorphe à $\mathrm{PGL}_{n+1}(K)$.
- Les endomorphismes de $\mathbf{P}^1_K$ de degré d sont exactement les fractions rationnelles $f \in K(z)$ de degré d. Par exemple, si
$$f(z) = \frac{z^2 - 2}{z^3 + 1},$$
alors avec $z = x/y$, on a
$$f[x, y] = f[z : 1] = [z^2 - 2 : z^3 + 3] = [x^2 y - 2y^3 : x^3 + y^3].$$
Réciproquement, si
$$s[x : y : z]) = [yz : zx : xy],$$
alors
$$s \circ s[x : y : z] = [zxxy : xyyz : yzzx] = (xyz)[x : y : z].$$
Ici, la première égalité de la remarque ne marche plus car les coordonnées définissant l'endomorphisme s ont des zéros communs.

8.2. Points périodiques

Théorème 8.2. Soit $f\colon \mathbf{P}^m_K \longrightarrow \mathbf{P}^m_K$ un endomorphisme de degré $d \geqslant 2$. Soit $N \geqslant 1$ un entier. Alors l'ensemble des points périodiques de f de période N dans $\mathbf{P}^m(\overline{K})$ est fini.

Démonstration. On prend d'abord $m = 1$. Montrons que l'équation $f^N(z) = z$ admet un nombre fini de solutions. L'endomorphisme f est une fraction rationnelle de degré d, donc l'endomorphisme f^N en est une de degré d^N. On note $f^N = P_N/Q_N$ avec $P_N, Q_N \in K(z)$. De la sorte, l'équation $f^N(z) = z$ se réécrit $P_N(z) = zQ_N(z)$ qui admet au plus $d^N + 1$ racines, donc il y a au plus $d^N + 1$ points périodique de période N.

Donnons l'idée de la preuve en dimension quelconque. Quitte à remplacer f par f^N, il s'agit de montrer que f n'a qu'un nombre fini de points fixes dans $\mathbf{P}^m(\overline{K})$. On note $f = [f_0 : \cdots : f_m]$. Le problème équivaut à résoudre le système

$$f_i i(z_1, \ldots, z_m) = z_i w^{d-1}, \qquad i \in [\![1, m]\!]$$

pour un élément $w \in \overline{K} \setminus \{0\}$. D'une part, ce système définit une sous-variété algébrique $F \subset \mathbf{P}^{m+1}_K$. D'autre part, il n'a pas de solution tel que $w = 0$, c'est-à-dire $F \cap \{w = 0\} = \emptyset$. Ensuite, on utilise le théorème suivant. ◇

Théorème 8.3. Une variété algébrique de $\mathbf{P}^m_{\overline{K}}$ évitant un hyperplan est un ensemble fini.

Corollaire 8.4. Si f est un endomorphisme de $\mathbf{P}^m_{\overline{\mathbf{Q}}}$ de degré $\geqslant 2$, alors les points de $\mathbf{P}^m(\mathbf{C})$ qui sont périodiques pour f sont contenus dans $\mathbf{P}^m(\overline{\mathbf{Q}})$

8.3. Hauteur canonique

Théorème 8.5 *(Northcott, Tate).* Soit f un endomorphisme de $\mathbf{P}^m_{\overline{\mathbf{Q}}}$ de degré $d \geqslant 1$. Alors

1. il existe une constante $c(f) > 0$ telle que
$$|d \times h(z) - h(f(z))| \leqslant c(f), \qquad z \in \mathbf{P}^m(\overline{\mathbf{Q}})\ ;$$
2. pour tout point $z \in \mathbf{P}^m(\overline{\mathbf{Q}})$, la limite
$$\hat{h}(z) \coloneqq \lim_{n \to +\infty} \frac{1}{d^n} h(f^n(z))$$
existe. L'application obtenue $\hat{h}\colon \mathbf{P}^m(\overline{\mathbf{Q}})$ vérifie
$$|h(z) - \hat{h}(z)| \leqslant C(f) \coloneqq \frac{c(f)}{d-1}, \qquad z \in \mathbf{P}^m(\overline{\mathbf{Q}})\ ;$$
3. pour tout point $z \in \mathbf{P}^m(\overline{\mathbf{Q}})$, on a $\hat{h}(f(z)) = d\hat{h}(z)$;
4. un point $z \in \mathbf{P}^m(\overline{\mathbf{Q}})$ possède une orbite finie si et seulement si $\hat{h}(z) = 0$ si et seulement si la suite $(h(f^n(z))_{n \geqslant 1})$ est bornée. Si l'orbite est infinie, alors cette dernière suit croît exponentiellement vite.

Définition 8.6. L'application $\hat{h}$ est la *hauteur canonique* associée à l'endomorphisme f.

Corollaire 8.7. Si $z \in \mathbf{P}^m(\mathbf{Q})$ et f est définie sur $\mathbf{Q}$, alors l'image de la suite $(f^n(z))_{n \geqslant 0}$ n'est pas l'espace projectif tout entier $\mathbf{P}^m(\mathbf{Q})$.

Démonstration du théorème. On écrit $f = [f_0 : \cdots : f_m]$ avec $f_i = \sum_{|I|=d} a_{i,I} \underline{x}^I$. Soit K un corps contenant les z_i avec $z = [z_0 : \cdots : z_m]$. Soit $L \supset K$ un corps contenant les $a_{i,I}$. On a

$$h(z) = \frac{1}{[L : \mathbf{Q}]} \sum_{w \in M_L} [L_w : \mathbf{Q}_w] \log(\max_{0 \leqslant i \leqslant m} |z_i|_w).$$

Si w n'est pas archimédienne, alors

$$|f_i(z_0, \ldots, z_m)| \leqslant \max_I \left|a_{i,I} \underline{z}^I\right|_w$$

$$\leqslant B_w(\max|z_i|_w)^d \quad \text{avec} \quad B_w \coloneqq \max_{i,I}|a_{i,I}|^w.$$

Si $w \mid \infty$, alors

$$|f_i(z_0,\dots,z_m)| \leqslant \binom{d+m}{d} B_w \max_{i,I}|a_{i,I}|^w.$$

On obtient donc

$$\begin{aligned} h(f(z)) &= \frac{1}{[L:\mathbf{Q}]}\sum_{w\in M_L}[L_w:\mathbf{Q}_w]\log(\max_{0\leqslant i\leqslant m}|f_1(z_0,\dots,z_m)|_w) \\ &\leqslant dh(z) + \frac{1}{[L:\mathbf{Q}]}\sum_{w\in M_L}[L_w:\mathbf{Q}_w]\log(\max_{i,I}|a_{i,I}|_w) + \frac{1}{[L:\mathbf{Q}]}\sum_{w\in M_L}[L_w:\mathbf{Q}_w]\log\binom{d+m}{d} \\ &\leqslant dh(z) + c_1(f) \quad \text{avec} \quad c_1(f) \coloneqq \frac{1}{[L:\mathbf{Q}]}\sum_{w\in M_L}[L_w:\mathbf{Q}_w]\log(\max_{i,I}|a_{i,I}|_w) + \log\binom{d+m}{d}. \end{aligned}$$

Montrons l'autre inégalité. On utilise le théorème suivant.

Théorème 8.8 *(des zéros de Hilbert).* Soient K un corps et $\overline{K}$ une clôture algébrique de K. Soient $g, g_1, \dots, g_k \in K[x_1,\dots,x_\ell]$. On suppose que g s'annule identiquement sur l'ensemble $V_{\overline{K}}(g_1,\dots,g_k)$. Alors il existe un entier $N \geqslant 1$ et des polynômes $\varphi_i \in K[x_1,\dots,x_\ell]$ tels que

$$g(\underline{x})^N = \sum_{i=1}^k \varphi_i(\underline{x})g_i(\underline{x}).$$

De plus, si les g_i sont homogènes, alors les φ_i peuvent être pris homogènes.

Les polynômes $f_0,\dots,f_m \in L[x_0,\dots,x_m]$ s'annulent simultanément dans $\overline{L}^{m+1}$ à l'origine uniquement. Avec les notations du théorème, on a $V \coloneqq V_{\overline{L}}(g_0,\dots,f_m) = \{0\}$. Donc les fonctions coordonnées x_i avec $i \in [\![0,m]\!]$ s'annulent identiquement sur V. En appliquant le théorème, il existe un entier $N \geqslant 1$ et des polynômes homogènes $\varphi_{i,j} \in L[x_0,\dots,x_m]$ de degré $N-d$ tels que

$$x_i^N = \sum_{j=0}^m \varphi_{i,j}(\underline{x})f_j(\underline{x}). \qquad (*)$$

On veut majorer $dh(z) \leqslant h(f(z)) + c_2(f)$. Pour cela, on utilise l'égalité $(*)$ pour $|z_i|_w^N$: les $\varphi_{i,j}$ contribuent pour $\leqslant (N-d)h(z) + e(f)$ pour une constante $e(f)$ ne dépendant que des $\varphi_{i,j}$ et donc que de f. On trouve alors

$$Nh(z) \leqslant (N-d)h(z) + h(f(z)) + c_2(f)$$

ce qui se simplifie et donne ce qu'on veut.

Montrons le deuxième point. Avec le premier point, on peut écrire

$$\frac{1}{d}h(f(z)) = h(z) + r(z)$$

avec $|r(z)| \leqslant c(f)/d$. On obtient alors

$$\begin{aligned} \frac{1}{d^2}h(f^2(z)) &= \frac{1}{d}h(f(z)) + \frac{1}{d}r(f(z)) \\ &= h(z) + r(z) + \frac{1}{d}r(f(z)). \end{aligned}$$

En itérant, on trouve

$$h(f^n(z)) = h(z) + \sum_{i=0}^{n-1}\frac{r\circ f^n(z)}{d^i}$$

où la série à droite converge uniformément et sa somme est majoré par

$$c(f)/d \times (1 + 1/d + 1/d^2 + \dots) \leqslant c(f)/(d-1).$$

Le troisième point a déjà été fait. Il reste le quatrième point. Si l'orbite de z est finie, alors la quantité $h(f^n(z))$ avec $n \geqslant 1$ ne prend qu'un nombre fini de valeurs, donc la suite $(h(f^n(z))/d^n)_{n\geqslant 0}$

tend vers zéro, donc $\hat{h}(z) = 0$. Réciproquement, on suppose $\hat{h}(z) = 0$. Alors la suite $(h(f^n(z)))_{n\geqslant 0}$ est bornée par $c(f)/(d-1)$ et $f^n(z) \in \mathbf{P}^m(L)$ pour un corps de nombres L. Par le théorème de finitude de Northcott, la suite $(f^n(z))_{n\geqslant 0}$ ne prend qu'un nombre fini de valeurs. ◇

Chapitre 9
Topologie de Zariski dans l'espace affine

Dans cette partie, on souhaite montrer l'alternative de Tits.

Théorème 9.1 *(alternative de Tits).* Soient K un corps de caractéristique nulle et $m \geqslant 1$ un entier. Soit $\Gamma \subset \mathrm{GL}_m(K)$ un groupe. Alors le groupe Γ contient ou bien un groupe abélien non libre ou bien un sous-groupe d'indice fini résoluble.

9.1. Définition

On fixe un corps K. On note $\mathrm{V}(K) \coloneqq \mathbf{A}^m(K)$ l'espace affine de dimension m et $K[V]$ l'ensemble des fonctions polynomiales. Pour une partie $E \subset \mathrm{V}(K)$, on pose l'idéal

$$\mathscr{I}(E) \coloneqq \{P \in K[V] \mid \forall z \in E,\ P(z) = 0\}.$$

Pour une partie $J \subset K[V]$, on pose

$$\mathscr{Z}(J) \coloneqq \{z \in \mathrm{V}(K) \mid \forall P \in J,\ P(z) = 0\}.$$

Un *fermé de Zariski* est une partie de la forme $\mathscr{Z}(J)$ pour un idéal $J \subset K[V]$. Comme l'anneau $K[V]$ est noethérien, tout fermé est défini par un nombre fini d'équations. Les fermés de Zariski définissent une topologie sur l'espace affine $\mathrm{V}(K)$.

Remarque. Toute application polynomiale $\mathbf{A}^m_K \longrightarrow \mathbf{A}^n_K$ est continue pour la topologie de Zariski.

Attention, la topologie sur $\mathbf{A}^{m+m'}(K)$ n'est pas la topologie produit sur $\mathbf{A}^m(K) \times \mathbf{A}^{m'}(K)$. En effet, on prend $m = m' = 1$. Les fermés de $\mathbf{A}^1(K)$ sont l'ensemble vide, l'espace tout entier et les parties finis : il y a donc beaucoup plus de fermés dans $\mathbf{A}^m(K) \times \mathbf{A}^{m'}(K)$.

Notation. Pour une partie $E \subset \mathrm{V}(K)$, on note $\overline{E}$ ou $\mathrm{Zar}(K)$ son adhérence.

9.2. Topologie induite et connexité

Exemple. La partie $\mathbf{Z} \subset \mathbf{A}^1(\mathbf{R})$ est dense. Plus généralement, toute partie infinie de $\mathbf{A}^1(K)$ est dense et connexe.

9.3. Irréductibilité

Une partie $E \subset \mathrm{V}(K)$ est irréductible si elle n'est pas la réunion de deux parties fermés non vides distinctes de E. Une partie irréductible est connexe. La réciproque est fausse : deux droites

qui se coupent forment un ensemble réductible non connexe.

Exemple. On considère la courbe $C \subset \mathbf{A}^2(\mathbf{R})$ d'équation $y^2 = x(x-1)(x+1)$. Elle a deux composantes connexes pour la topologie usuelle. Mais pour la topologie de Zariski, elle est irréductible.

Proposition 9.2.
1. Une partie $E \subset \mathrm{V}(K)$ est irréductible si et seulement si l'intersection de deux ouverts non vides de E est non vides.
2. Tout ouvert non vide d'une partie irréductible est dense.
3. Une partie est irréductible si et seulement si tout ouvert non vide est connexe.

Exercice 8.
1. Une partie $E \subset \mathrm{V}(K)$ est irréductible si et seulement si l'idéal $\mathscr{I}(E)$ est premier.
2. Une partie $E \subset \mathrm{V}(K)$ admet un nombre fini de composantes irréductibles.
3. Les composantes connexes sont des unions de composantes irréductibles.

9.4. Dimension

On suppose que le corps K est algébriquement clos. La *dimension* d'une sous-variété irréductible $W \subset \mathrm{V}(K)$, c'est-à-dire un fermé irréductible, est la longueur maximale d'une chaîne

$$\emptyset \subsetneq W_0 \subsetneq \cdots \subsetneq W_\ell = W$$

formées de sous-variétés irréductibles. De manière équivalente, c'est de longueur maximale d'une chaîne d'idéaux premiers dans l'anneau $K[W] \coloneqq K[V]/\mathscr{I}(V)$ des fonctions régulières sur W ou c'est le degré de transcendance du corps $\operatorname{Frac} K[W]$ sur K.

9.5. Groupes linéaires

Soit V un K-espace vectoriel de dimension m. En considérant $\mathrm{End}(V) \simeq \mathbf{A}^{m^2}(K)$, le groupe $\mathrm{GL}(V)$ est un ouvert de Zariski et le groupe $\mathrm{SL}(V)$ un fermé. Les applications

$$(g,h) \in \mathrm{End}(V) \times \mathrm{End}(V) \longmapsto gh \in \mathrm{End}(V) \qquad \text{et} \qquad g \in \mathrm{SL}(V) \longmapsto g^{-1} \in \mathrm{SL}(V)$$

sont polynomiales. On dit alors que le groupe $\mathrm{SL}(V)$ est un groupe algébrique linéaire.

Montrons qu'il en est de même pour le groupe $\mathrm{GL}(V)$. On plonge le groupe $\mathrm{GL}(V)$ dans l'espace vectoriel $\mathrm{End}(V \oplus L)$ pour une droite L par l'application

$$g \longmapsto \begin{pmatrix} g & 0 \\ 0 & 1/\det g \end{pmatrix}.$$

La fonction $1/\det g$ devient alors polynomiale. Avec cette structure, le groupe $\mathrm{GL}(V)$ devient un groupe algébrique linéaire. En particulier, les applications $(g,h) \longmapsto gh$ et $g \longmapsto g^{-1}$ sont continues.

Proposition 9.3. Soit $\Gamma \subset \mathrm{GL}(V)$ un sous-groupe. Soit Γ^0 la composante irréductible de Γ contenant l'élément neutre Id_V. Alors
1. les composantes connexes de Γ coïncident avec ses composantes irréductibles ;
2. le groupe Γ agit par conjugaison (respectivement par translation) sur lui-même et cette action permute les composantes de Γ, l'action par conjugaison préserve la composante Γ^0 ;
3. la composante Γ^0 est un sous-groupe distingué de Γ.

Vocabulaire. La composante Γ^0 est la *composante neutre*.

Démonstration. Soient $\Gamma_1, \ldots, \Gamma_\ell \subset \Gamma$ les composantes irréductibles. Le groupe Γ agit sur lui-même par translation. Pour $g \in \Gamma$, l'application $L_g \colon h \longmapsto gh$ est continue pour la topologie de Zariski, donc elle permet les composantes irréductibles. Soit $x \in \Gamma_1$ qui n'appartient à aucune autre composante. Soit $z \in \Gamma$ tel que $zx \in \Gamma_i$. Alors $L_z(x) \in \Gamma_i$ et $L_z(x)$ n'appartient à aucune autre composante connexe, donc $L_z(\Gamma_1) = \Gamma_1$. Par transitivité de l'action par translation, les composantes sont donc disjointes. Ainsi les composantes irréductibles sont les composantes connexes.

Pour le deuxième point, pour $g \in G$, l'application $h \longmapsto ghg^{-1}$ est continue et elle fixe l'identité, donc elle fixe la composante Γ^0.

Montrons que la composante Γ^0 est un sous-groupe. L'application $g \longmapsto g^{-1}$ est continue, donc elle permute les composantes. Mais comme elle fixe l'identité, elle préserve la composante Γ^0. De même, la composante Γ est stable par produit. ◇

Théorème 9.4. Soient $\Gamma \subset \mathrm{GL}(V)$ un sous-groupe et G son adhérence. Alors

1. l'ensemble G est un sous-groupe de $\mathrm{GL}(V)$;
2. le groupe $[\Gamma, \Gamma]$ est dense dans $[G, G]$;
3. le groupe Γ est abélien (respectivement nilpotent ou résoluble) si et seulement si le groupe G l'est ;
4. si $\Gamma_0 \subset \Gamma$ est un sous-groupe distingué, alors $\overline{\Gamma_0}$ est distingue dans G.

Démonstration.

1. L'application $g \longmapsto g^{-1}$ envoie Γ sur lui-même et elle est continue, donc elle envoie G sur lui-même. Par ailleurs, l'application $(g, h) \longmapsto gh$ envoie Γ^2 sur Γ et elle est continue. Or Γ^2 est dense dans G^2, donc le groupe G est stable par produit.
2. Soit H un groupe. On note $C_k(H)$ l'ensemble des produits de k commutateurs. Alors
$$[H, H] = \bigcup_{k \geqslant 1} C_k(H).$$
Remarquons que $C_1(\Gamma)$ est dense dans $C_1(G)$: c'est le même argument qu'au point 1. Une récurrence immédiate montre alors que $C_k(\Gamma)$ est dense dans $C_k(G)$. Ainsi
$$[G, G] = \bigcup_{k \geqslant 1} C_k(G) \leqslant \overline{\bigcup_{k \geqslant 1} C_k(\Gamma)} = \overline{[\Gamma, \Gamma]}.$$
3. Si Γ est abélien, alors $[\Gamma, \Gamma] = \{\mathrm{Id}_V\}$, donc $[G, G] = \overline{[\Gamma, \Gamma]} = \{\mathrm{Id}_V\}$, donc G est abélien. La réciproque est claire. ◇

Exemple. Soit θ un nombre irrationnel. Soit $f \in \mathrm{GL}_2(\mathbf{R})$ la rotation d'angle $2\pi\theta$. Alors l'adhérence du groupe $f^{\mathbf{Z}}$ est le groupe $\mathrm{SO}_2(\mathbf{R})$.

Chapitre 10

Groupes linéaires : propriétés élémentaires

10.1. Irréductibilité et théorème de Burnside

Soient K un corps et $m \geqslant 1$ un entier. Soient $\Gamma \subset \mathrm{GL}_m(K)$ un sous-groupe et $A \subset \mathrm{End}_m(K)$ une sous-algèbre. On dit que le sous-groupe Γ (ou la sous-algèbre A) agit de manière *réductible* sur K^m s'il existe un sous-espace vectoriel propre et non nul $W \subset K^m$ qui est invariant par le groupe Γ (ou par l'algèbre A).

Exemple. Le groupe $\mathrm{SO}_2(\mathbf{R})$ agit irréductiblement sur $\mathbf{R}^2$.

Théorème 10.1 *(Burnside).* Soit K un corps. Soit $A \subset \mathrm{End}_m(K)$ une sous-algèbre dont l'action sur $\overline{K}^m$ est irréductible. Alors $A = \mathrm{End}_m(K)$.

Démonstration. • *Préliminaire.* L'intersection des noyaux $\operatorname{Ker} a$ avec $a \in A$ est A-invariant, donc elle est nulle par irréductibilité. Soit $x \in K^* \setminus \{0\}$. L'ensemble $A(x) \coloneqq \{a(x) \mid a \in A\}$ est un sous-espace vectoriel qui est A-invariant et n'est pas nul, donc $A(x) = K^m$. Soit ξ une forme linéaire non nulle. L'intersection des noyaux $\operatorname{Ker}(\xi \circ a)$ avec $a \in A$ est également nulle. On en déduit l'égalité $A^*\xi \coloneqq \{\xi \circ a \mid a \in A\} = (K^m)^*$.

• *Un cas particulier.* D'abord, on suppose que le corps K est algébriquement clos. Il suffit de montrer que l'algèbre A contient un endomorphisme de rang 1. En effet, si un endomorphisme $g \in A$ est de rang 1, les endomorphismes $b \circ g \circ a$ et $a, b \in A$ décrivent tous les endomorphismes de rang au plus 1. Soit r le minimum des rangs des endomorphismes $g \in A \setminus \{0\}$. Si $r = 1$, c'est fini. On suppose $r \geqslant 2$ et on va trouver une contradiction. On choisit un endomorphisme g de rang r. Comme $r \geqslant 2$, il existe deux vecteurs $x_1, x_2 \in K^n$ tel que la famille $(g(x_1), g(x_2))$ soit libre. On choisit un endomorphisme $a \in A$ tel que $a \circ g(x_1) = x_2$. Les vecteurs $g \circ a \circ g(x_1) = g(x_2)$ et $g(x_1)$ sont alors linéairement indépendants de telle sorte que

$$\forall \alpha \in K, \qquad g \circ a \circ g - \alpha g \in A \setminus \{0\}\,.$$

On considère le sous-espace vectoriel $g(K^m)$ qui est stable par les endomorphismes $g - \alpha \operatorname{Id}_{K^m}$ avec $\alpha \in K$. Il existe un vecteur propre $w \in g(K^m)$ de l'endomorphisme $g \circ a$ pour une certaine valeur propre β. Ainsi l'endomorphisme $g \circ a - \beta \operatorname{Id}_{K^m}$ a une image de codimension strictement positive. Donc l'endomorphisme $g \circ a \circ g - \beta g \in A \setminus \{0\}$ a une image de dimension strictement plus petite que le rang r ce qui est contradictoire.

• *Le cas général.* Comme l'action de A sur $\overline{K}^m$ est irréductible, la sous-algèbre de $\mathrm{End}_m(\overline{K})$ engendrée par A est égale à tout d'après le cas particulier. Ainsi l'algèbre A contient m^2 linéairement indépendants, donc elle contient une base de $\mathrm{End}_m(K)$, donc elle est égale à $\mathrm{End}_m(K)$. ◇

10.2. Éléments et groupes unipotents

Un élément $f \in \mathrm{GL}_m(K)$ est *unipotent* si sa seule valeur propre dans $\overline{K}$ est le neutre 1, c'est-à-dire si son polynôme caractéristique vaut $(t-1)^m$. Il est *virtuellement unipotent* s'il existe un entier $n > 0$ tel que l'élément f^n soit unipotent. Un sous-groupe de $\mathrm{GL}_m(K)$ est unipotent si tous ses éléments le sont. Il est virtuellement unipotent s'il contient un groupe unipotent d'indice fini.

Théorème 10.2. Soient K un corps de caractéristique nulle et $\Gamma \subset \mathrm{GL}_m(K)$ un sous-groupe de type fini. Alors

1. le groupe Γ contient un sous-groupe d'indice fini dont les éléments virtuellement unipotents sont unipotents ;
2. si le groupe Γ est unipotent, alors il est conjugué à un groupe de matrices triangulaires supérieures comportant des 1 sur la diagonale ;
3. si tous les éléments du groupe Γ sont virtuellement unipotents, il existe un sous-groupe $\Gamma_0 \subset \Gamma$ d'indice fini nilpotent.

Démonstration. 1. Soit $S \subset \Gamma$ une partie génératrice et symétrique. Soit R l'anneau engendré par l'ensemble $C \subset K$ des coefficients des matrices $s \in S$. On pose $L \coloneqq \operatorname{Frac} R \subset K$. D'après le théorème de plongement de Lech, il existe un nombre premier p et un plongement $\iota \colon L \longrightarrow \mathbf{Q}_p$ tel que $\iota(C) \subset \mathbf{Z}_p$. Cela donne un morphisme injectif $\iota \colon \Gamma \longrightarrow \mathrm{GL}_m(\mathbf{Z}_p)$. On pose

$$\Gamma_0 \coloneqq \{g \in \Gamma \mid \iota(g) = \mathrm{Id} \mod p,\ \iota(g) = \mathrm{Id} + pB,\ B \in \mathrm{End}_m(\mathbf{Z}_p)\}.$$

Soit $g \in \Gamma_0$ un élément. Alors le théorème de Bell-Poonen assure qu'on peut écrire $\iota(g) = \Phi_1$ pour un flot analytique Φ_t. Si l'élément g avait une valeur propre $\alpha \in \overline{K} \setminus \{1\}$ qui est une racine de l'unité, alors on trouverait une vecteur propre associé $w \in \overline{K}^m$ et un entier $\ell \geqslant 1$ tels que

$$\forall v \in \overline{K}w, \qquad g^\ell(v) = v.$$

Dans $\overline{K}w$, tous les vecteurs $v \neq 0$ sont périodiques de période l'ordre de α. D'après le théorème des zéros isolés, on en déduit que $\Phi_t = \mathrm{Id}$, donc $g(v) = v$, donc $\alpha = 1$ ce qui est impossible. Ainsi tous les éléments de Γ_0 sont unipotents.

2. On suppose que tout élément de Γ est unipotent. On effectue une récurrence sur m. Lorsque $m = 1$, c'est terminé. On suppose le résultat vrai en dimension $\leqslant m-1$. Pour tout élément $f \in \Gamma$, on a $\operatorname{tr} f = m = \operatorname{tr} \mathrm{Id}$, donc $\operatorname{tr}(f - \mathrm{Id}) = 0$ et même $\operatorname{tr}((f-\mathrm{Id}) \circ h) = 0$ pour $h \in \Gamma$ et donc pour $h \in \overline{K}[\Gamma]$. Ainsi l'algèbre engendrée par Γ n'est pas tout. Par le théorème de Burnside, la représentation de Γ dans $\mathrm{GL}_m(\overline{K})$ est réductible sur $\overline{K}$, donc il existe un sous-espace vectoriel invariant $W \subset \overline{K}^m$ tel que $1 \leqslant \dim W \leqslant m-1$. Il existe donc un élément $w \neq 0$ de W tel que

$$\forall g \in \Gamma, \qquad g(w) = w$$

par l'hypothèse de récurrence, donc l'ensemble $F \coloneqq \{w \mid \forall g \in \Gamma,\ g(w) = w\}$ est un sous-espace vectoriel non nul sur $\overline{K}$ et donc sur K, donc il existe $v \neq 0 \in K^m$ tel que

$$\forall g \in \Gamma, \qquad g(v) = v.$$

Le quotient $Q \coloneqq K^m/Kv$ est un espace vectoriel de dimension $m-1$. De plus, le groupe Γ agit linéairement sur K, donc il existe une base $(q_1, \dots, q_{m-1})$ de Q dans laquelle les éléments de Γ sont donnés par des matrices triangulaires supérieures. Alors la famille $(v, \tilde{q}_1, \dots, \tilde{q}_{m-1})$ avec $\tilde{q}_i = q_i \mod Kv$ est une base dans laquelle les matrices des éléments de Γ sont triangulaires supérieures. ◇

Théorème 10.3. Soit $\Gamma \subset \mathrm{GL}_m(K)$ un sous-groupe qui n'est pas virtuellement résoluble. Alors il existe un élément de Γ ayant une valeur propre qui n'est pas une racine de l'unité.

Cet énoncé est faux en caractéristique positive. Il résulte du lemme suivant.

Lemme 10.4. Soit $\Gamma \subset \mathrm{GL}_m(K)$ un sous-groupe.

- Si tous les sous-groupes de type fini de Γ sont virtuellement résolubles, alors Γ l'est aussi.
- Si tous les sous-groupes de type fini de Γ sont résolubles, alors Γ l'est aussi.

Exemple. Les mêmes énoncés ne marchent plus en remplaçant « résoluble » par « nilpotent ». On considère le groupe affine $\mathrm{Aff}(\mathbf{R}^2) = \mathrm{GL}_2(\mathbf{R}) \ltimes \mathbf{R}^2$. C'est un sous-groupe de $\mathrm{GL}_3(\mathbf{R})$. On considère le sous-groupe Γ engendré par

- les rotations d'angle appartenant à $2\pi\mathbf{Q}$;
- la translation de vecteur $(1, 0)$.

Soit $\Gamma_0 \subset \Gamma$ un sous-groupe de type fini. On a la suite existe

$$\mathbf{R}^2 \longrightarrow \mathrm{Aff}(\mathbf{R}^2) \longrightarrow \mathrm{GL}_2(\mathbf{R}).$$

Ainsi on a un morphisme $\Gamma_0 \longrightarrow \mathrm{SO}(2)$ dont l'image sont les roations d'angles $2\pi\mathbf{Q}$, donc la partie linéaire de Γ_0 est un groupe fini (à indice fini près, le sous-groupe Γ_0 est abélien). Ainsi tout sous-groupe de type fini de Γ est virtuellement abélien et donc virtuellement nilpotent. Pourtant, le sous-groupe Γ n'est pas virtuellement nilpotent.

Démonstration. Soit G l'adhérence de Zariski de Γ dans $\mathrm{GL}_m(\overline{K})$. Il suffit de supposer que le groupe G est irréductible et de montrer qu'il est résoluble.

Soient $E \subset \overline{K}^N$ une partie et W son adhérence de Zariski. Alors il existe une partie dénombrable de E dont l'adhérence est W. On considère l'idéal $\mathscr{J}(E)$. Il vaut

$$\mathscr{J}(E) = \bigcup_{d \in \mathbf{N}} \mathscr{J}(E, d) \quad \text{avec} \quad \mathscr{J}(E, d) \coloneqq \{f \in \overline{K}[\underline{x}] \mid \deg f \leqslant d \text{ et } \forall x \in E,\ f(x) = 0\}.$$

Par dimension finie, pour tout entier $d \geqslant 0$, il existe $a_1, \ldots, a_{k(d)} \in E$ tel que

$$\mathscr{J}(E, d) = \{f \in \overline{K}[\underline{x}] \mid \deg f \leqslant d \text{ et } \forall i \leqslant k(d),\ f(a_i) = 0\}.$$

Alors il suffit de prendre l'ensemble

$$F \coloneqq \bigcup_{d \in \mathbf{N}} \{a_1, \ldots, a_{k(d)}\}.$$

Avec cette remarque, il existe un sous-groupe dénombrable $\Gamma_0 \subset \Gamma$ tel que $G = \overline{\Gamma_0}$. On écrit $\Gamma_0 = \bigcup_{i=1}^{+\infty} \Gamma_i$ comme une union croissante de sous-groupes de type fini. Les composantes neutres $\overline{\Gamma_i}^0$ forment une suite croissante de fermés de Zariski irréductibles dans G. Le nombre de termes distincts de cette suite est alors bornés par la dimension de G, il existe un entier j tel que $\overline{\Gamma_i}^0 = G$ car $\overline{\Gamma_i}^0 \subset \overline{\Gamma_i} \subset G$. Par hypothèse, le sous-groupe Γ_j est de type fini et donc virtuellement résoluble, donc il existe un sous-groupe $\Lambda \subset \Gamma_j$ d'indice fini résoluble. Ceci implique que $\overline{\Lambda} = G$ car G est irréductible. Ainsi le groupe G est résouble. ◇

Chapitre 11

Éléments proximaux

11.1. Points fixes attractifs

Soient X un espace topologique et $g\colon X \longrightarrow X$ une application continue. Un point fixe $x \in X$ de l'application g est *attractif* s'il existe un voisinage U du point x tel que

$$\forall y \in E, \qquad g^n(y) \longrightarrow x.$$

Dans ce cas, le bassin d'attraction du point x est l'ensemble

$$\mathrm{Bas}(x) \coloneqq \{y \in X \mid \lim_{n \longrightarrow +\infty} g^n(y) = x\}.$$

Exemple. Soit K un corps valué complet. On considère une homothétie de rapport $\lambda \in K$ avec $|\lambda| < 1$. Alors l'origine est un point fixe attractif et son bassin et le corps K tout entier.

Exemple. Soit $f(z) = \lambda z + a_1 z^2 + \cdots + a_d z^d$ un polynôme complexe tel que $f(0) = 0$ at $|\lambda| < 1$. Alors l'origine est un point fixe attractif de la fonction f. Son bassin est un sous-ensemble borné et ouvert de $\mathbf{C}$ et dont le bord est (typiquement) fractal.

11.2. Proximalité

Soit K un corps valué complet. Soit V un K-espace vectoriel normé de dimension $m < +\infty$ (on prend la norme associée à une base par exemple). On peut munir l'ensemble $\mathbf{P}(V \otimes_K \overline{K})$ d'une distance définie par l'égalité

$$d(X, Y) = \inf\{\|\tilde{x} - \tilde{y}\| \mid \tilde{x}, \tilde{y} \in V \otimes_K \overline{K},\ \|\tilde{x}\| = \|\tilde{y}\| = 1,\ [\tilde{x}] = X,\ [\tilde{y}] = Y\}.$$

Remarque. L'ensemble $\mathbf{P}(V)$ devient un espace métrique complet. De plus, si le corps K est local (c'est-à-dire localement compact), alors l'espace métrique $\mathbf{P}(V)$ est compact.

Soit $g \in \mathrm{End}(V)$ un endomorphisme et $\lambda > 0$ un réel. On note $V_\lambda(g)$ le plus grand sous-espace vectoriel g-invariant tel que toute valeur propre $\alpha \in \overline{K}$ de l'endomorphisme g sur le sous-espace vectoriel $V_\lambda(g)$ vérifie $|\alpha| = \lambda$. Pour exemple, pour $\lambda = 0$, on retrouve le noyau de l'endomorphisme g.

On classe les valeurs propres α_i pour que $\lambda_1 \coloneqq |\alpha_1| \geqslant \cdots \geqslant \lambda_m \coloneqq |\alpha_m|$. La valeur propre λ_1 est alors le rayon spectral de l'endomorphisme g, c'est aussi la limite de la suite $(\|g^n\|^{1/n})_{n \in \mathbf{N}^*}$. Posons $V^+(g) \coloneqq V_{\lambda_1}(g)$ et $m^+(g) \coloneqq \dim V^+(g)$, puis $V^<(g) \coloneqq \bigoplus_{\lambda < \lambda_1} V_\lambda(g)$ où la somme est faite sur les nombres distincts λ_i.

Définition 11.1. L'endomorphisme g est *proximal* sur $\mathbf{P}(V)$ si l'une des conditions équivalentes suivantes est vérifiée :

(i) $\lambda_1 > \lambda_2$;
(ii) $m^+(g) = 1$.
Si c'est le cas, alors $\alpha_1 \in K$ et $V^+(g) \subset V$.

Si $g \in \mathrm{GL}(V)$, alors l'endomorphisme g agit par transformation linéaire projective sur $\mathbf{P}(V)$ et les conditions (i) et (ii) sont équivalentes au point suivant :

(iii) l'endomorphisme g admet un point fixe attractive $x^+(g) \in \mathbf{P}(V)$. Alors
$$x^+(g) \in \mathbf{P}(V^+(g)) \qquad \text{et} \qquad \mathrm{Bas}(x^+(g)) = \mathbf{P}(V) \setminus \mathbf{P}(V^<(g)).$$

Remarque. On suppose $g \in \mathrm{GL}(V)$. Alors l'endomorphisme g est proximal si et seulement si l'une des conditions suivantes sont vérifiées :

- pour tout scalaire $\beta \in K \setminus \{0\}$, l'endomorphisme βg est proximal ;
- pour tout entier $n \geqslant 1$, l'endomorphisme g^n est proximal ;
- pour toute extension $K \subset L \subset \overline{K}$, l'endomorphisme g est proximal si $\mathbf{P}(V \otimes_K L)$.

Proposition 11.2. 1. Pour tout entier $m' \leqslant m$, l'ensemble $\{g \in \mathrm{End}(V) \mid m^+(g) \leqslant m'\}$ est un ouvert de l'espace $\mathrm{End}(V)$ muni de la norme subordonnée.
2. L'ensemble des endomorphismes proximaux est un ouvert de l'espace $\mathrm{End}(V)$ muni de la norme subordonnée.
3. Un endomorphisme $g \in \mathrm{End}(V)$ est proximal si et seulement s'il existe une suite scalaire $(c_n)_{n\in\mathbf{N}}$ telle que la suite $(c_n g^n)_{n\in\mathbf{N}}$ converge dans $\mathrm{End}(V)$ vers un projecteur de rang 1.

Démonstration. 1. On a $\{g \in \mathrm{End}(V) \mid m^+(g) \leqslant m'\} = \{g \in \mathrm{End}(V) \mid \lambda_1(g) > \lambda_{m'+1}(g)\}$. Par continuité des racines, cet ensemble est un ouvert.
2. On prend $m' = 1$.
3. On suppose que l'endomorphisme g est proximal. On prend $c_n = \alpha_1^{-1}$. Il suffit ensuite de remarquer que $V = V^+(g) \oplus V^<(g)$: la suite $(c_n g^n)_{n\in\mathbf{N}}$ converge alors vers le projecteur sur la droite $V^+(g)$. Réciproquement, on suppose qu'il existe une suite scalaire $(c_n)_{n\in\mathbf{N}}$ telle que la suite $(c_n g^n)_{n\in\mathbf{N}}$ converge dans $\mathrm{End}(V)$ vers un projecteur de rang 1. Alors les endomorphismes $c_n g^n$ avec $n \gg 1$ sont proximaux par le point 1. Ceci assure que les endomorphismes g^n sont proximaux, donc l'endomorphisme g est proximal. ◇

11.3. Puissances extérieures

Soient $k \in \{1, \dots, \dim V\}$ un entier et $g \in \mathrm{End}(V)$ un endomorphisme. Notons $\bigwedge^k g$ l'application induit sur l'espace vectoriel $\bigwedge^k V$. Ses valeurs propres sont les scalaires $\mu_I \coloneqq \alpha_{i_1} \cdots \alpha_{i_k}$ pour un multi-indice $I = (i_1, \dots, i_k)$ avec $i_1 > \cdots > i_k$. Si $k < m^+(g)$, alors l'endomorphisme $\bigwedge^k g$ n'est pas proximal. Si $k = m^+(g)$, alors il l'est.

11.4. Ping-pong

Il s'agit d'une technique pour produire des groupes libres non abéliens dans l'ensemble des bijections d'un ensemble donné.

Théorème 11.3. Soient X un ensemble et $f, g \in \mathfrak{S}(X)$ deux bijections de X. Soient $A, B \subset X$ deux parties telles que
(i) $A \cap V = \emptyset$ et $A \neq \emptyset$;
(ii) $f^n(A) \subset B$ pour tout $n \in \mathbf{Z}^*$;
(iii) $g^n(B) \subset A$ pour tout $n \in \mathbf{Z}^*$.
Alors les applications f et g engendrent un groupe libre de rang 2.

Démonstration. Soit w un mot réduit en les symboles f et g. On peut l'écrire sous la forme

$$w = f^{m_1} g^{n_1} \cdots g^{n_{k-1}} f^{m_k}$$

avec tous les entiers m_i et n_i non nuls sauf peut être m_1 ou m_k. On va montrer que w définie une bijection de X différente de l'identité. On peut conjuguer le mot w par une puissance de f pour que $m_1 m_k \neq 0$. Alors le mot w ne peut être l'identité car il envoie un élément de A sur un élément de B et inversement. ◇

Exemple. On prend $f \coloneqq \operatorname{diag}(\alpha, 1/\alpha) \in \mathrm{SL}_2(\mathbf{R})$ et g conjuguée à $\operatorname{diag}(\beta, 1/\beta)$. On suppose que $|\alpha|, |\beta| > 1$. On note $\alpha(f)$ et $\omega(f)$ des vecteurs propres de f associé à α et $1/\alpha$. On note A un petit voisinage compact contenant $\alpha(g)$ et $\omega(g)$ et B un petit voisinage compact contenant $\alpha(f)$ et $\omega(f)$. Par compacité de A, il existe un entier $N \geqslant 1$ tel que

$$\forall\, |n| \geqslant N, \qquad f^n(A) \subset B.$$

En particulier, on a

$$\forall n \in \mathbf{Z} \setminus \{0\}, \qquad (f^N)^n(A) \subset B.$$

De même, il existe un entier $M \geqslant 1$ tel que

$$\forall n \in \mathbf{Z} \setminus \{0\}, \qquad (g^M)^n(B) \subset A.$$

Ainsi le groupe engendré par les matrices f^N et g^M est bien un groupe libre de rang 2.

Corollaire 11.4. Soient $f, g \in \mathrm{GL}(V)$ deux automorphismes tels que

(i) les automorphismes f et f^{-1} soient proximaux ;
(ii) les automorphismes g et g^{-1} soient proximaux ;
(iii) les quatre éléments $x^+(f)$, $x^+(f^{-1})$, $x^+(g)$ et $x^+(g^{-1})$ soient distincts ;
(iv) on ait $\emptyset = \{x^+(f), x^+(g)\} \cap \mathbf{P}(V^<(g)) \sqcup \mathbf{P}(V^<(g^{-1}))$ et de même si on permute le rôle des automorphismes f et g.

Alors ils engendrent un groupe libre de rang 2.

Théorème 11.5. Soit K un corps local. Soit V un K-espace vectoriel de dimension finie $m \geqslant 2$. Soit $\Gamma \subset \mathrm{GL}(V)$ un sous-groupe connexe pour la topologie de Zariski et agissant irréductiblement sur V. On suppose que ce dernier contient un élément proximal. Alors

1. il contient un élément f qui est proximal et tel que son inverse soit proximal ;
2. il contient un groupe libre de rang 2.

Démonstration. 1. On munit l'espace vectoriel V d'une base et de la norme associée. Soit $g \in \Gamma$ un élément proximal. Il existe une suite d'entiers n_i, une suite d'éléments c_{n_i} et d_{n_i} de $K^\times$ tels que

- n_i est croissante et tend vers $+\infty$;
- $c_{n_i} g^{n_i}$ tend vers un projecteur π de rang 1 ;
- $c_{n_i} g^{-n_i}$ tend vers un projecteur endomorphisme non nul σ.

Pour cela, on a déjà vu comment avoir les deux premiers points. Pour le troisième point, on choisit $|d_n| = \|g^{-n}\|^{-1}$. Par ce choisit, on trouve un élément $d_n g^{-n} \in \mathrm{End}(V)$ de la sphère unité qui est compact (puisque le corps K est compact), donc on peut extraire une sous-suite qui converge vers un endomorphisme σ qui est donc de norme 1 et donc non nul.

On considère les deux conditions suivantes portant sur un couple $(h_1, h_2) \in \Gamma \times \Gamma$:

- $h_1(\operatorname{Im}\pi) \not\subset \operatorname{Ker}\sigma$;
- $h_2(\sigma(h_1(\operatorname{Im}\pi))) \not\subset \operatorname{Ker}\pi$.

La condition $h_1(\operatorname{Im}\pi) \subset \operatorname{Ker}\sigma$ est fermée pour la topologique de Zariski, donc son complémentaire est un ouvert de Γ pour la topologie de Zariski induite. De même, la paire des conditions précédentes définies un ouvert de Zariski de $\Gamma \times \Gamma$. Cet ouvert est non vide. En effet, si $h_1(\operatorname{Im}\pi) \subset \operatorname{Ker}\sigma$, alors le sous-espace vectoriel $W \coloneqq \operatorname{Vect}(h(\operatorname{Im}\pi))_{h\in\Gamma}$ est inclus dans $\operatorname{Ker}\sigma$, non nul de de dimension $< m$, invariant par Γ ce qui contredirait l'irréductible de l'action de Γ. Un tel élément h_1 étant fixé, le sous-espace vectoriel $L_1 \coloneqq \sigma(h_1(\operatorname{Im}\pi))$ est

une droite. La seconde condition se réécrit alors $h_2(L_1) \not\subset \operatorname{Ker}\varphi$ et un tel élément h_2 existe par le même argument. Comme le groupe Γ est connexe pour la topologie de Zariski, il est irréductible, donc les deux conditions précédentes définissant un ouvert dense de $\Gamma \times \Gamma$.

On fixe un couple $(h_1, h_2) \in \Gamma \times \Gamma$ vérifiant ces conditions. On pose $g_n \coloneqq h_2 g^{-n} h_1 g^n$. Alors $c_{n_i} d_{n_i} g_{n_i} \longrightarrow h_2 \sigma h_1 \pi$ où l'endomorphisme $h_2 \sigma h_1 \pi$ est un multiple d'un projecteur de rang 1, donc c'est proximal. Ainsi comme l'ensemble des endomorphismes proximaux est un ouvert, pour $i \gg 1$, l'endomorphisme g_{n_i} est proximal. Mais $g_n^{-1} = g^{-n} h_1^{-1} g^n g_2^{-1}$ et $c_n d_n g_n^{-1} \longrightarrow \sigma h_1^{-1} \pi h_2^{-1}$. Donc si

- $h_1^{-1}(\operatorname{Im}\pi) \not\subset \operatorname{Ker}\sigma$,
- $h_2^{-1}(\sigma(h_1^{-1}(\operatorname{Im}\pi))) \not\subset \operatorname{Ker}\pi$,

alors pour $i \gg 1$, l'endomorphisme $g_{n_i}^{-1}$ est encore proximal. Il reste à montrer qu'il existe un couple (h_1, h_2) satisfait les quatre points précédents. Mais les deux dernières conditions définissant aussi un ouvert non vide de $\Gamma \times \Gamma$. Par irréductibilité, ces deux ouverts sont denses et s'intersectent donc. L'élément $f = g_{n_i}$ convient alors.

2. On veut trouver deux éléments $f, g \in \Gamma$ qui engendrent un groupe libre de rang 2. D'après le premier point, il existe un élément $f \in \Gamma$ qui soit proximal sur $\mathbf{P}(V)$ et tel que son inverse le soit aussi. On va le conjuguer par un élément $h \in \Gamma$ pour construit l'élément $g \coloneqq hfh^{-1}$ qui sera proximal et d'inverse proximal tel que la technique du ping-pong s'applique au couple (f, g). Les conditions gênantes sont

$$\begin{aligned} h^{\pm}(x^+(f)) &\in \{x^+(f), x^+(f^{-1})\}, \\ h^{\pm}(x^+(f^{-1})) &\in \{x^+(f), x^+(f^{-1})\}, \\ h^{\pm}(x^+(f)) &\in \mathbf{P}(V^<(f)) \cup \mathbf{P}(V^<(f^{-1})), \\ h^{\pm}(x^+(f^{-1})) &\in \mathbf{P}(V^<(f)) \cup \mathbf{P}(V^<(f^{-1})). \end{aligned}$$

notées (1), (2), (3) et (4). Si (1) est satisfaite pour tout $h \in \Gamma$, alors l'orbite de la droite $x^+(f)$ est fini ce qui contredit l'hypothèse d'irréductibilité forte. De plus, la condition

$$h^{\pm}(x^+(f)) \notin \{x^+(f), x^+(f^{-1})\}$$

est ouvert en topologie de Zariski, donc elle forme un ouvert dense. De même pour les conditions (2), (3) et (4). On peut donc trouver un tel élément h. ◇

Exercice 9.

1. Soit $\Gamma \subset \mathrm{GL}(V)$ un sous-groupe tel que son adhérence de Zariski $\overline{\Gamma}$ soit connexe. Soit $\Gamma_0 \subset \Gamma$ un sous-groupe d'indice fini. Montrer que $\overline{\Gamma_0} = \overline{\Gamma}$.
2. On dit que l'action de Γ sur V est *fortement irréductible* si l'orbite de tout sous-espace $W \subset V$ de dimension entre 1 et $m-1$ est infini. Autrement dit, si tout sous-groupe $\Gamma_0 \subset \Gamma$ d'indice fini agit irréductiblement sur V. On suppose que le groupe Γ est connexe et que son action est irréductible. Montrer qu'il est fortement irréductible.

Chapitre 12
L'alternative de Tits

Théorème 12.1 *(alternative de Tits).* Soient K un corps de caractéristique nulle et $m \geqslant 1$ un entier. Soit $\Gamma \subset \mathrm{GL}_m(K)$ un groupe. Alors le groupe Γ contient ou bien un groupe abélien non libre ou bien un sous-groupe d'indice fini résoluble.

Ce théorème est faux en caractéristique positive. On prend le corps $\overline{\mathbf{F}_p}$. Soit $F \subset \mathrm{GL}_m(\overline{\mathbf{F}_p})$ une partie finie. Alors $F \subset \mathrm{GL}_m(L)$ pour une certaine extension finie $L = \mathbf{F}_q$ de $\mathbf{F}_p$. Alors le groupe engendré $\langle F \rangle$ par la partie F est un élément de $\mathrm{GL}_m(\mathbf{F}_q)$ qui est fini. Donc il n'existe pas de partie finie non vide engendrant un groupe libre. Pourtant, le groupe $\mathrm{GL}_m(\overline{\mathbf{F}_p})$ n'est pas virtuellement résoluble si $m \geqslant 2$.

Par contre, l'alternative de Tits reste valable en caractéristique positive si on ne considère que des groupes de type fini. On connaît aussi une version forte du théorème.

Théorème 12.2 *(Breuillard).* Pour toute dimension $m \geqslant 1$, il existe une constante $B(m) \in \mathbf{N}^*$ vérifiant la propriété suivante : pour tout corps K et toute partie finie symétrique $F \subset \mathrm{GL}_m(K)$, ou bien le groupe engendré par F est virtuellement résoluble ou bien il existe deux éléments $f, g \in F^{B(m)}$, produit de $B(m)$ éléments de F, qui engendrent un groupe libre de rang 2.

On va montrer l'alternative de Tits grâce aux étapes suivantes.

12.1. Première étape : variation sur le théorème de Kronecker

Lemme 12.3. Soit L une extension de type fini de $\mathbf{Q}$. Soit $\alpha \in L$ un élément qui n'est pas une racine de l'unité. Alors il existe un corps local $(L_v, |\cdot|_v)$ et un plongement $\tau \colon L \longrightarrow L_v$ tels que $|\tau(\alpha)|_v \neq 1$.

Démonstration. • *Premier cas.* On suppose que l'extension est algèbre. D'après le théorème de Kronecker, il existe une valeur absolue $|\cdot|_v$ sur L telle que $|\alpha|_v \neq 1$. On considère le complété L_v et le plongement naturel $L \longrightarrow L_v$.

• *Deuxième cas.* On ne suppose plus que l'extension L est un corps de nombres, mais on suppose que l'élément α est algébrique. Posons $L' \coloneqq \mathbf{Q}(\alpha)$. C'est une extension algébrique. D'après le premier cas, il existe une valeur absolue $|\cdot|'_v$ sur L' tel que $|\alpha|'_v \neq 1$. Notons L'_v le complété de L' pour cette valeur absolue. On se donne une famille maximale $(t_1, \ldots, t_r)$ d'éléments de L définissant une extension transcendante pure $L'(t_1, \ldots, t_r) \subset L$. Alors le corps L est une extension algébrique finie de $L'(t_1, \ldots, t_r)$. Comme le corps L_v n'est pas dénombrable, il contient des éléments algébriquement indépendants $s_1, \ldots, s_r \in L'_v$ sur L'. Ainsi il existe une extension finie L_v de L'_v et un plongement $\iota \colon L \longrightarrow L_v$ qui étend le plongement$L'(t_1, \ldots, t_r) \longrightarrow L'_v$.

• *Troisième cas.* On suppose que l'élément α est transcendant sur $\mathbf{Q}$. On choisit une famille maximale $(t_1 = \alpha, t_2, \ldots, t_r)$ d'éléments algébriquement indépendantes sur $\mathbf{Q}$. Il existe $s_1, \ldots, s_r \in \mathbf{C}$

algébriquement indépendants sur $\mathbf{Q}$ tels que $|s_1|_\infty \neq 1$. On considère l'isomorphisme

$$\left|\begin{array}{l}\mathbf{Q}(t_1,\dots,t_r) \longrightarrow \mathbf{Q}(s_1,\dots,s_r),\\ \qquad\qquad t_i \longmapsto s_i.\end{array}\right.$$

On peut l'étendre en un plongement $\iota\colon L \longrightarrow \mathbf{C}$ et on prend alors $(L_v, |\cdot|_v) = (\mathbf{C}, |\cdot|_\infty)$. ◇

12.2. Deuxième étape : changement du groupe Γ

On suppose que le groupe Γ n'est pas virtuellement résoluble. Il existe des sous-groupe de type fini de Γ qui ne sont pas virtuellement résolubles. On remplace le groupe Γ par un tel sous-groupe. Le but est de construire un groupe libre non abélien dans Γ. Soit S une partie génératrice symétrique de Γ. Soit R l'anneau engendré par les coefficients des éléments de S. Soit $L \coloneqq \operatorname{Frac} R$. C'est une extension de type fini de $\mathbf{Q}$. Soit $\overline{L}$ sa clôture algébrique. Quitte à remplacer le groupe Γ par un sous-groupe d'indice fini, on peut supposer qu'il est connexe pour la topologie de Zariski. Ainsi son adhérence $G \subset \mathrm{GL}_n(\overline{L})$ est connexe et donc irréductible pour la topologie de Zariski. Le groupe dérivé $[G,G]$ est encore connexe. En effet, l'ensemble $C_1(G)$ est l'image d'un connexe par une application continue, donc il est connexe. Ainsi le groupe $C_1(G)^k$ est connexe, donc $C_k(G)$ est connexe. Ceci permet de conclure que le groupe $[G,G] = \bigcup_{k\geqslant 1} C_k(G)$ est connexe car les éléments de l'intersection sont connexes et ont un élément commun. De plus, on sait que $[\Gamma,\Gamma]$ est dense dans $[G,G]$ et donc connexe.

Remarque. Attention, le groupe $[\Gamma,\Gamma]$ n'est plus nécessairement de type fini.

Remarque. Le groupe $[\Gamma,\Gamma]$ n'est pas virtuellement résoluble. En effet, soit $\Lambda \subset [\Gamma,\Gamma]$ un sous-groupe. Alors son adhérence est égale à $[G,G]$. Si Λ était résoluble, alors le groupe $[G,G]$ le serait et donc G aussi et donc Γ aussi.

12.3. Troisième étape

Il existe un élément $f \in [\Gamma,\Gamma]$ ayant une valeur propre α qui n'est pas une racine de l'unité. Par le lemme précédent, il existe un plongement $\iota\colon L \longrightarrow L_v$ dans un corps local L_v tel que $|\iota(\alpha)|_v \neq 1$. Ici l'élément α appartient à $\overline{L}$, mais on a étendu le plongement ι en un plongement $\overline{L} \longrightarrow \overline{L_v}$. On note encore Γ l'image de Γ dans $\mathrm{GL}_m(L_v)$. Maintenant, le sous-groupe $[\Gamma,\Gamma] \subset \mathrm{GL}_m(L_v)$ contient un élément f qui a une valeur propre α avec $|\alpha|_v > 1$ (quitte à remplacer f par f^{-1}).

On considère l'espace vectoriel $W \coloneqq \bigwedge^k (L_v)^m$ où $k \coloneqq m^+(f)$. Alors $\bigwedge^k \Gamma$ devient un sous-groupe de $\mathrm{GL}(W)$ et $\bigwedge^k f$ devient un élément proximal sur $\mathbf{P}(W)$. Notons α_1 la valeur propre de $\bigwedge^k f$ de valeur absolue maximale. Supposons que la représentation de $[\Gamma,\Gamma]$ sur W ne soit pas irréductible. Alors on peut trouver un sous-espace non nul et propre $W' \subset W$ qui est $[\Gamma,\Gamma]$-invariant. On regarde les représentations induites sur W' et W/W' et on recommence. En un nombre fini d'étapes, on trouve une suite de sous-espaces vectoriels $\{0\} \subsetneq W_1 \subsetneq \cdots \subsetneq W_\ell \subsetneq W_{\ell+1} = W$ tels que la représentation de Γ sur chaque uotient W_{i+1}/W_i soit irréductible.

Notons W' l'unique quotient W_{i+1}/W_i dans lequel l'endomorphisme $\bigwedge^k f|_{W_{i+1}/W_i}$ a la valeur propre α. Montrons que $\dim W' \geqslant 2$. Raisonnons par l'absurde et supposons le contraire. Sinon $\dim W' = 1$, donc $\mathrm{GL}(W')$ est commutatif, donc $\bigwedge^k f \in \bigwedge^k[\Gamma,\Gamma]$ serait l'identité ce qui est impossible car $|\alpha|_v > 1$.

Par ailleurs, le groupe $\bigwedge^k \Gamma|_{W'} \subset \mathrm{GL}(W')$ est connexe et donc irréductible. En effet, l'application

$$\left|\begin{array}{l}\Gamma \subset \mathrm{GL}_m(\overline{L}) \longrightarrow \mathrm{GL}(W),\\ \qquad\qquad f \longmapsto \bigwedge^k f\end{array}\right.$$

est un homéomorphisme algébrique. Comme le groupe Γ est connexe, il en va de même du groupe $\bigwedge^k \Gamma$. On a également un homéomorphisme algébrique $\Gamma \longrightarrow \mathrm{GL}(\bigwedge^k \overline{L_v}^m)$. Enfin, la reste de $\bigwedge^k \Gamma$ à W_{i+1} puis à W' est donnée par un homéomorphisme algébrique, donc l'image est connexe.

Soient Γ' l'image de Γ dans $\mathrm{GL}(W')$ et f' l'image de f dans $\mathrm{GL}(W')$. Alors on a montré les propriétés suivantes :

- $\dim W' \geqslant 2'$;
- f' est proximale sur $\mathbf{P}(W')$;
- Γ' est connexe ;
- Γ' agit de manière irréductible.

Par le théorème précédent, le groupe Γ'contient deux éléments g' et h' engendrent un groupe libre de rang 2. On prend $g, h \in \Gamma$ tels que $\bigwedge^k g|_{W'} = g'$ et $\bigwedge^k h|_{W'} = h'$. Alors g et h engendrent un groupe libre de rang 2.

12.4. Application

Soit Γ un groupe de type fini. Soit S une partie génératrice finie symétrique. On considère le graphe de Cayley G de Γ dont les sommets sont les éléments de Γ et où deux sommets $g, h \in \Gamma$ sont reliés si et seulement s'il existe $s \in S$ tel que $gs = h$.

Pour $N \in \mathbf{N}$, on note $V_S(N)$ le cardinal de la boule de centre e et de rayon N. Quel est le comportement asymptotique de la quantité $V_S(N)$?

Corollaire 12.4. Si Γ est un groupe linéaire de type fini, alors ou bien $V_S(N)$ est équivalent à une expression polynomiale en N ou bien il l'est à une expression exponentielles en N.

Pourtant, il existe des groupes à croissance intermédiaire.

Chapitre 13
Théorème d'Erdös et Turán

Théorème 13.1 *(Baker, de Marco).* Soient $f, g \in \mathbf{C}[z]$ deux polynômes de degré $\geqslant 2$. S'ils ont une infinité de points périodiques communs, alors ils ont un itéré commun.

Théorème 13.2 *(de Marco, Krieger, Ye).* Si $f(x) = z^2 + c$ et $g(z) = z^2 + d$ ont 10^{82} points périodiques communs, alors $f = g$.

Le point de départ de ces deux résultats est le fait suivant : si on a une infinité de points périodiques communs, alors on a exactement les mêmes points périodiques et le même ensemble de Julia. Pour montrer ce fait, on utilise un théorème d'équidistribution des points périodiques.

Théorème 13.3 *(d'équidistribution de Bilu).* Soit $(\alpha_n)_{n\in\mathbf{N}}$ une suite de nombres algébriques tels que $\deg \alpha_n \longrightarrow +\infty$ et $h(\alpha_n) \longrightarrow 0$. Alors la suite de mesures de probabilité

$$\mu_n \coloneqq \frac{1}{\deg \alpha_n} \sum_{\beta} \delta_\beta$$

où les β sont les conjugués de α_n tend vers la mesure $\mathrm{d}\theta$ sur le cercle unité $\mathbf{S}^1$

13.1. Limites de mesures de probabilité

Soit X un espace métrique compact. Notons $\mathrm{Proba}(X)$ l'ensemble des mesures de probabilité sur X. C'est un ensemble convexe compact pour la topologie faible, c'est-à-dire que, si μ_n est une suite de mesures de probabilité, alors il existe une sous-suite μ_{n_i} et une mesure de probabilité telles que, pour toute fonction continue $\xi\colon X \longrightarrow \mathbf{R}$, on ait

$$\int_X \xi(x)\,\mathrm{d}\mu_{n_i}(x) \longrightarrow \int_X \xi(x)\,\mathrm{d}\mu(x).$$

Soit $P \in \mathbf{C}[t]$ un polynôme de degré d. Notons $z_1, \ldots, z_d \in \mathbf{C}$ ses racines. Alors

$$\mu_P \coloneqq \frac{1}{d} \sum_{i=1}^{d} \delta_{z_i}$$

est une mesure de probabilité sur $\mathbf{C}$ et donc sur $\mathbf{P}^1(\mathbf{C}) = \mathbf{C} \cup \{\infty\}$.

13.2. Mesure de Mahler et distance au cercle unité

Soit $P = a_d t^d + \cdots + a_0 \in \mathbf{C}[t]$ un polynôme. Rappelons que sa mesure de Mahler est

$$m(P) = \int_0^1 \log|P(e^{2i\pi\theta})| \, \mathrm{d}\theta.$$

On pose également

$$m^+(P) = \int_0^1 \log^+|P(e^{2i\pi\theta})| \, \mathrm{d}\theta.$$

Supposons $a_0 \neq 0$ et utilisons $m(P) = m(t^d P(1/t))$. En notant z_i les racines de P, la formule de Jensen donne

$$m(P) = \log|a_0| + \sum_{i=1}^{d} \log^+\left|\frac{1}{z_i}\right|.$$

En combinant avec l'égalité

$$m(P) = \log|a_0| + \sum_{i=1}^{d} \log^+|z_i|,$$

on trouve

$$m(P) = \log\sqrt{|a_0 a_d|} + \frac{1}{2}\sum_{i=1}^{d} \log(\max(|z_i|, |1/z_i|)).$$

Posons $\tilde{P} \coloneqq P/\sqrt{|a_0 a_d|}$. Alors

$$m(\tilde{P}) = \frac{1}{2}\sum_{i=1}^{d} \log(\max(|z_i|, |1/z_i|)).$$

Soit $\rho > 1$. On note $\delta_P(\rho)$ la proportion des racines de P en dehors de l'anneau $\{\rho^{-1} < |\cdot| < \rho\}$, c'est-à-dire

$$\delta_P(\rho) = \frac{\sharp\{i \mid |z_i| > \rho \text{ ou } |z_i| < 1/\rho\}}{\deg P}.$$

Alors

$$\frac{1}{2}\log(\rho) \times \sharp\{i \mid |z_i| > \rho \text{ ou } |z_i| < 1/\rho\} \leqslant m(\tilde{P}),$$

donc

$$\frac{1}{2}\log(\rho)\delta_P(\rho) \leqslant \frac{m(\tilde{P})}{\deg \tilde{P}}.$$

Proposition 13.4. Soit $(P_n)_{n\in\mathbf{N}}$ une suite de polynômes complexes telle que $m(\tilde{P}_n) = o(\deg P_n)$. Alors toute valeur d'adhérence de la suite $(\mu_{P_n})_{n\in\mathbf{N}}$ de mesures de probabilité sur $\mathbf{P}^1(\mathbf{C})$ est une mesure de probabilité supportée par le cercle $\mathbf{S}^1$.

13.3. Observation de Schur

Soit $P \in \mathbf{C}[t]$ un polynôme de degré d ne s'annulant pas en l'origine. On écrit ses racines $z_j \in \mathbf{C}$ sous la forme $z_j = |z_j| \, e^{2i\pi\theta_j}$. Posons

$$Q(t) \coloneqq \prod_{j=1}^{d}(t - e^{2i\pi\theta_j}).$$

Lemme 13.5 *(Schur).*
1. Pour tout complexe z de module 1, on a $|Q(z)| \leqslant |\tilde{P}(z)|$.
2. On a $\|Q\|_{\mathrm{L}^\infty(\mathbf{S}^1)} \leqslant \|\tilde{P}\|_{\mathrm{L}^\infty(\mathbf{S}^1)}$.
3. On a $m(Q) \leqslant m(\tilde{P})$ et $m^+(Q) \leqslant m^+(\tilde{P})$.

Démonstration. Montrons uniquement le premier point. On calcule

$$|\tilde{P}(z)|^2 = \left|\frac{a_d}{a_0}\right| \prod_{j=1}^{d} |z - z_j|^2.$$

Or

$$a_d \prod_{j=1}^{d} (0 - z_j) = P(0) = a_0,$$

donc

$$\left|\frac{a_d}{a_0}\right| = \frac{1}{\prod_{j=1}^{d} |z_i|}$$

si bien que

$$\begin{aligned}
|\tilde{P}(z)|^2 &= \prod_{j=1}^{d} \frac{|z - z_j|^2}{|z_j|} \\
&= \prod_{j=1}^{d} \left| \frac{z}{\sqrt{|z_j|}} - \frac{z_j}{\sqrt{|z_j|}} \right|^2 \\
&= \prod_{j=1}^{d} \left| \frac{z}{\sqrt{|z_j|}} - \sqrt{|z_j|} e^{2i\pi\theta_j} \right|^2 \\
&\geqslant |Q(z)|^2 = \prod_{j=1}^{d} |z - e^{2i\pi\theta_j}|^2.
\end{aligned}$$

Il suffit donc de montrer que, pour tout réel $r \neq 0$, tout angle θ et tout complexe z de module 1, on a l'inégalité

$$\left| \frac{z}{r} - r e^{2i\pi\theta} \right|^2 \geqslant |z - e^{2i\pi\theta}|^2$$

ce qui n'est pas trop dur. ◇

Si $m^+(\tilde{P}_n) = o(\deg P_n)$, alors $m^+(Q_n) = o(\deg Q_n)$.

13.4. Théorème d'Erdös et Turán pour les angles

Lemme 13.6. 1. Les coefficients de Fourier de la fonction 1-périodique

$$\xi : \theta \longmapsto \log|e^{2i\pi\theta} - 1|$$

sont

$$\hat{\xi}(k) = 0 \qquad \text{et} \qquad \hat{\xi}(k) = -|2k|^{-1}, \qquad k \neq 0.$$

2. Pour tout angle φ et tout entier $k \neq 0$, on a

$$e^{2i\pi k\varphi} = -2\,|k| \int_0^1 e^{2i\pi k\theta} \log|e^{2i\pi\theta} - e^{2i\pi\varphi}|\,\mathrm{d}\theta.$$

On applique le second point avec $\varphi = \theta$ puis on somme sur j si bien qu'on trouve

$$\sum_{j=1}^{d} e^{2i\pi k\theta_j} = -2\,|k| \int_0^1 e^{2i\pi k\theta} \log|Q(e^{2i\pi\theta})|\,\mathrm{d}\theta.$$

Après division par d du membre de gauche, on obtient

$$\frac{1}{d} \sum_{j=1}^{d} e^{2i\pi k\theta_j} = \frac{1}{d} \sum_{j=1}^{d} \langle \delta_{e^{2i\pi\theta_j}}, \xi_k \rangle \quad \text{avec} \quad \xi_k(\theta) = e^{2i\pi k\theta},$$

donc

$$\frac{1}{d}\sum_{j=1}^{d} e^{2i\pi k\theta_j} = \int_{\mathbf{S}^1} \xi_k \,\mathrm{d}\mu_Q = \hat{\mu}_Q(-k).$$

Par ailleurs, la formule de Jensen donne

$$\int_0^1 \log|Q(e^{2i\pi\theta})|\,\mathrm{d}\theta = 0.$$

On en déduit

$$\begin{aligned}\left|\int_0^1 e^{2i\pi k\theta}\log|Q(e^{2i\pi\theta})|\,\mathrm{d}\theta\right| &\leqslant \int_0^1 |\log|Q(e^{2i\pi\theta})||\,\mathrm{d}\theta \\ &\leqslant 2\int_0^1 \log^+|Q(e^{2i\pi\theta})|\,\mathrm{d}\theta.\end{aligned}$$

D'où

$$|\hat{\mu}_Q(-k)| \leqslant 4\,|k|\,\frac{m^+(Q)}{\deg Q} \leqslant 4\,|k|\,\frac{m^+(\tilde{P})}{\deg P}.$$

On obtient la proposition suivante.

Proposition 13.7. Soit $(P_n)_{n\in\mathbf{N}}$ une suite de polynômes complexes telle que $m^+(\tilde{P}_n) = o(\deg P_n)$ et $P_n(0) \neq 0$. Alors la suite $(\mu_{P_n})_{n\in\mathbf{N}}$ de mesures de probabilité sur $\mathbf{S}^1$ définie par l'égalité

$$\mu_n \coloneqq \frac{1}{\deg P_n}\sum_{j=1}^{\deg P_n} \delta_{e^{2i\pi\theta_j(n)}},$$

où les $\theta_j(n)$ sont les angles des racines de P_n, converge vers la mesure $\mathrm{d}\theta$.

Démonstration du théorème d'équidistribution de Bilu. Soit $\mu \in \mathrm{Proba}(\mathbf{S}^1)$ une valur d'adhérence de la suite $(\mu_n)_{n\in\mathbf{N}}$. On note $\mu_{n_i} \longrightarrow \mu$. On veut montrer que $\mu = \mathrm{d}\theta$. Calculons les coefficients de Fourier de la mesure μ. On a

$$\hat{\mu}(k) = \int_0^1 \xi_k(e^{2i\pi\theta})\,\mathrm{d}\mu(\theta) = \lim_{i\longrightarrow+\infty}\int_0^1 \xi_k(e^{2i\pi\theta})\,\mathrm{d}\mu_{n_i}(\theta).$$

Mais pour $k \neq 0$, on a

$$\begin{aligned}\left|\int_0^1 \xi_k(e^{2i\pi\theta})\,\mathrm{d}\mu_{n_i}(\theta)\right| &= |\hat{\mu}_{Q_{n_i}}(-k)| \\ &\leqslant 4\,|k|\,\frac{m^+(\tilde{P}_{n_i})}{\deg P_{n_i}} \longrightarrow 0.\end{aligned}$$

On en déduit que $\hat{\mu}(k) = 0$ pour $k \neq 0$ et $\hat{\mu}(0) = 1$. Ainsi la mesure μ a les mêmes coefficients de Fourier que la mesure $\mathrm{d}\theta$, donc ces deux mesures sont les mêmes. ◇

13.5. Le théorème d'Erdös et Turán

Théorème 13.8. Soit $(P_n)_{n\in\mathbf{N}}$ une suite de polynômes complexes telle que $m^+(\tilde{P}_n) = o(\deg P_n)$ et $P_n(0) \neq 0$. Alors $\mu_{P_n} \longrightarrow \mathrm{d}\theta$.

Démonstration. On prend une valeur d'adhérence μde la suite $(\mu_{P_n})_{n\in\mathbf{N}}$ dans $\mathrm{Proba}(\mathbf{P}^1(\mathbf{C}))$. Par la première proposition, son support est inclus dans $\mathbf{S}^1$. On veut montrer que $\hat{\mu}(k) = 0$ pour $k \neq 0$ ce qui conclura. On prend $\xi_k(z) = z^k/|z|^k$. Soit $\varphi\colon \mathbf{R}_+ \longrightarrow [0,1]$ une fonction telle que

- $\varphi(s) = 0$ si $s > \rho$ et $s < 1/\rho$;
- $\varphi(s) = 1$ si $2/(1+\rho) < s < (1+\rho)/2$.

On pose $\eta_k(z) = \xi_k(z)\varphi(|z|)$. Alors

$$\hat{\mu}(-k) = \int_{\mathbf{P}^1(\mathbf{C})} \eta_k \,\mathrm{d}\mu$$

$$= \lim_{i \longrightarrow +\infty} \int_{\mathbf{P}^1(\mathbf{C})} \eta_k \, \mathrm{d}\mu_{n_i}$$
$$= \mathrm{O}(\rho) \qquad \text{si } k \neq 0.$$

◇

13.6. Discriminant et inégalité d'Hadamard

Soient $P = \sum_{i=0}^{d} a_i t^i$ et $Q = \sum_{j=0}^{d'} b_j t^j$ deux polynômes. On considère leur résultant $\mathrm{Res}(P, Q)$. C'est un polynôme à les variables a_i et b_j à coefficients entiers, de degré d' par rapport aux variables a_i et homogène de degré d par rapport aux variables b_j. Il existe deux polynômes Φ et Ψ tels que

$$\Phi P + \Psi Q = \mathrm{Res}(P, Q).$$

Le discriminant du polynôme P est la quantité

$$\mathrm{Disc}(P) \coloneqq a_d^{2d-2} \sum_{i<j} (z_i - z_j)^2. \qquad (*)$$

où les nombres z_j sont les racines du polynômes P répétées avec multiplicité. Il vérifie

$$a_d \, \mathrm{Disc}(P) = (-1)^{d(d-1)/2} \, \mathrm{Res}(P, P').$$

Lemme 13.9. Soit P un polynôme de degré $d \geqslant 1$ à coefficients complexes de discriminant non nul. Alors

$$\log |\mathrm{Disc}(P)| \leqslant d \log d + (2d-2) m(P).$$

Démonstration. D'après la formule $(*)$, le discriminant est le carré du déterminant de Vandermonde des z_i fois a_d^{2d-2}. Notons V la matrice de Vandermonde. On a

$$\Big(\sum_{j=0}^{d-1} |z_i^j|^2 \Big)^{1/2} \leqslant (d \max(1, |z_i|)^{2d-2})^{1/2}.$$

L'inégalité d'Hadamard donne alors

$$|\det V| \leqslant \prod_{j=0}^{d-1} (d \max(1, |z_i|)^{2d-2})^{1/2},$$

donc

$$|\mathrm{Disc}\, P| \leqslant |a_d|^{2d-2} d^d \prod_{i=0}^{d-1} \max(1, |z_i|)^{2d-2}$$
$$\leqslant d^d M(P)$$

et on passe ensuite au logarithme. ◇

Exemple. Lorsque $P = t^d - 1$, on trouve le cas d'égalité.

13.7. Énergie et analyse de Fourier

13.7.1. Énergie potentielle

Soient $K \subset \mathbf{C}$ un compact et μ une mesure de probabilité supportée par la partie K. L'*énergie* de la mesure μ est la quantité

$$\acute{\mathrm{E}}\mathrm{n}(\mu) \coloneqq \iint_{K \times K} - \log |z - w| \, \mathrm{d}\mu(z) \, \mathrm{d}\mu(w)$$

et son *énergie restreinte* est la quantité

$$\acute{\mathrm{E}}\mathrm{n}^0(\mu) \coloneqq \iint_{K \times K \setminus \Delta} - \log |z - w| \, \mathrm{d}\mu(z) \, \mathrm{d}\mu(w)$$

où l'ensemble $\Delta \subset K \times K$ désigne la diagonale.

Exemple. On prend

$$\mu = \sum_{i=1}^{d} m_i \delta_{z_i}.$$

Alors

$$\text{Én}^0(\mu) = \sum_{i \neq j} m_i m_j \log \frac{1}{|z_i - z_j|}.$$

13.7.2. Analyse de Fourier

Soient μ et ν deux probabilités supportés par le cercle $\mathbf{S}^1$. On note $\mu * \nu$ leur convolution définie par l'égalité

$$\int_{\mathbf{S}^1} \xi(z)\, \mathrm{d}(\mu * \nu)(z) = \int_{\mathbf{S}^1} \int_{\mathbf{S}^1} \xi(zw)\, \mathrm{d}\mu(z)\, \mathrm{d}\nu(w).$$

On note $\hat{\mu}(k)$ ses coefficients de Fourier, c'est-à-dire

$$\hat{\mu}(k) = \int_{\mathbf{S}^1} z^{-k}\, \mathrm{d}\mu(z).$$

En notant $\sigma(z) = \overline{z}$, la mesure image $\mu' \coloneqq \sigma_* \mu$ est encore une probabilité supportée par le cercle $\mathbf{S}^1$ et ses coefficients de Fourier satisfont $\hat{\mu}'(k) = \hat{\mu}(-k)$. Comme $\widehat{\mu * \nu}(k) = \hat{\mu}(k)\hat{\nu}(k)$, on trouve

$$\widehat{\mu * \mu'}(k) = |\hat{\mu}(k)|^2.$$

13.7.3. Application

Proposition 13.10. L'énergie d'une mesure μ supportée par le cercle $\mathbf{S}^1$ vaut

$$\text{Én}(\mu) = \sum_{k \in \mathbf{Z}^*} \frac{|\hat{\mu}(k)|^2}{2\,|k|}.$$

En particulier, son énergie est nulle si et seulement si $\mu = \mathrm{d}\theta$.

Démonstration. Notons $\zeta(z) = -\log|z-1|$. On écrit

$$\begin{aligned}
\text{Én}(\mu) &= \iint -\log|z-w|\, \mathrm{d}\mu(z)\, \mathrm{d}\mu(w) \\
&= \iint -\log|zw^{-1} - 1|\, \mathrm{d}\mu(z)\, \mathrm{d}\mu(w) \\
&= \iint \xi(zz')\, \mathrm{d}\mu(z)\, \mathrm{d}\mu'(z') \\
&= \int \xi(z)\, \mathrm{d}(\mu * \mu)(z) \\
&= \sum_{k \in \mathbf{Z}} \hat{\xi}(k) \widehat{\mu * \mu'}(k) \\
&= \sum_{k \in \mathbf{Z}^*} \frac{|\hat{\mu}(k)|^2}{2\,|k|}.
\end{aligned}$$

◇

13.7.4. Semi-continuité inférieure

Lemme 13.11. Soit $(\mu_n)_{n \in \mathbf{N}}$ une suite de mesure supportées par un compact $K \subset \mathbf{C}$. On suppose qu'elle tend vers une mesure μ pour la convergence faible. Alors

$$\text{Én}(\mu) \leqslant \liminf_{n \longrightarrow +\infty} \text{Én}(\mu_n).$$

Démonstration. Soit $M > 0$ un réel. On pose

$$\ell_M : t \geqslant 0 \longmapsto \min(M, -\log|t|).$$

Alors

$$\text{Én}(\mu_n) \geqslant \iint -\ell_M(|z-w|)\,\mathrm{d}\mu_n(z)\,\mathrm{d}\mu_n(w).$$

Comme $\mu_n \longrightarrow \mu$, on a $\mu_n \otimes \mu_n \longrightarrow \mu \otimes \mu$. Comme la fonction ℓ_M est continue, on trouve

$$\iint -\ell_M(|z-w|)\,\mathrm{d}\mu_n(z)\,\mathrm{d}\mu_n(w) \longrightarrow \iint -\ell_M(|z-w|)\,\mathrm{d}\mu(z)\,\mathrm{d}\mu(w).$$

On en déduit que

$$\liminf_{n\longrightarrow+\infty} \text{Én}(\mu_n) \geqslant \iint -\ell_M(|z-w|)\,\mathrm{d}\mu(z)\,\mathrm{d}\mu(w).$$

Or $\ell_M(t) \longrightarrow -\log|t|$ lorsque $M \longrightarrow +\infty$, donc le théorème de convergence monotone assure que

$$\iint -\ell_M(|z-w|)\,\mathrm{d}\mu(z)\,\mathrm{d}\mu(w) \longrightarrow \text{Én}(\mu)$$

ce qui conclut le lemme. ◇

13.8. Théorème d'équidistribution de Bilu

Théorème 13.12. Soit $(P_n)_{n\geqslant 1}$ une suite de polynômes à coefficients complexes de degré respectifs d_n. On note

$$P_n(t) = a_{d_n}(n)t^{d_n} + \cdots + a_0(n).$$

Soit $\{z_1(n), \ldots, z_{d_n}(n)\}$ l'ensemble des racines du polynômes P_n répétées avec multiplicité. Supposons que

1. $\liminf_{n\longrightarrow+\infty} \frac{1}{d_n}\log|a_0(n)| \geqslant 0$ et $\liminf_{n\longrightarrow+\infty} \frac{1}{d_n}\log|a_{d_n}(n)| \geqslant 0$;
2. $\liminf_{n\longrightarrow+\infty} \frac{1}{d_n^2}\log|\mathrm{Disc}(P_n)| \geqslant 0$;
3. $\limsup_{n\longrightarrow+\infty} \frac{1}{d_n} m(P_n) = 0$;
4. $d_n \longrightarrow +\infty$.

Alors la suite $(\mu_n)_{n\geqslant 1}$ définie par l'égalité

$$\mu_n \coloneqq \frac{1}{d_n}\sum_{j=1}^{d_n} \delta_{z_j(n)}$$

converge vers la mesure $\mathrm{d}\theta$ sur le cercle $\mathbf{S}^1$.

Démonstration. Quitte à extraire, on peut supposer que la suite $(\mu_n)_{n\geqslant 1}$ converge vers une mesure μ dans $\mathrm{Proba}(\hat{\mathbf{C}})$. La compacité de l'espace projectif $\overline{\mathbf{C}}$ conclura.

• *Première étape.* Montrons que la mesure μ est portée par le cercle $\mathbf{S}^1$. D'après la formule de Jensen, on a

$$\frac{1}{d_n} m(P_n) = \frac{1}{d_n}\log|a_{d_n}(n)| + \frac{1}{d_n}\sum_{i=1}^{d_n} \log^+|z_i(n)|\,.$$

Avec les hypothèses 2 et 3, on trouve

$$\frac{1}{d_n}\log|a_{d_n}(n)| \longrightarrow 0 \qquad \text{et} \qquad \frac{1}{d_n}\sum_{i=1}^{d_n} \log^+|z_i(n)| \longrightarrow 0.$$

On utilise maintenant $m(P_n) = m(t^{d_n}P_n(1/t))$, on trouve

$$\frac{1}{d_n}\log|a_0(n)| \longrightarrow 0 \qquad \text{et} \qquad \frac{1}{d_n}\sum_{i=1}^{d_n} \log^+\left|\frac{1}{z_i(n)}\right| \longrightarrow 0.$$

Ainsi on trouve

$$\frac{1}{d_n} m(\tilde{P}_n) \longrightarrow 0.$$

Par le proposition d'Erdös-Turán, on pose $A(\rho) \coloneqq \{1/\rho < |\cdot| < \rho\}$ et $\delta_{P_n}(\rho)$ la proportion des racines de P_n hors de $A(\rho)$, on trouve

$$\log(\rho)\delta_{P_n}(\rho) \leqslant \frac{2}{f_n}(m(P_n) - \frac{1}{2}\log|a_0(n)a_{d_n}(n)|) \longrightarrow 0.$$

Donc le support de la mesure μ est inclus dans l'ensemble $\bigcap_{\rho>1} A(\rho) \subset \mathbf{S}^1$.

• *Deuxième étape.* Montrons que l'énergie restreinte de la mesure μ_n tend vers zéro. On a

$$\frac{1}{d_n^2}\log|\mathrm{Disc}(P_n)| \leqslant \frac{\log d_n}{d_n} + \frac{2d_n-2}{d_n}\frac{m(P_n)}{d_n}.$$

Avec la deuxième hypothèse, on en déduit alors

$$\frac{1}{d_n^2}\log|\mathrm{Disc}(P_n)| \longrightarrow 0.$$

Mais

$$\log|\mathrm{Disc}(P_n)| = \frac{2d_n-2}{d_n}\frac{1}{d_n}\log|a_{d_n}(n)| + \frac{1}{d_n^2}\sum_{i\neq j}\log|z_i - z_j|$$

avec

$$\frac{2d_n-2}{d_n}\frac{1}{d_n}\log|a_{d_n}(n)| \longrightarrow 0.$$

D'où

$$\acute{\mathrm{E}}\mathrm{n}^0(\mu_n) \longrightarrow 0.$$

• *Troisième étape.* Montrons que $\acute{\mathrm{E}}\mathrm{n}(\mu) = 0$ ce qui conclura. Soit $M > 0$ un réel. On considère toujours la fonction ℓ_M. Remarquons que

$$\forall z, w \in \mathbf{C}, \qquad \log|z-w| \leqslant \log^+|z| + \log^+|w| + \log 2.$$

On peut donc écrire

$$M \geqslant \ell_M(|z-w|) \geqslant -(\log^+|z| + \log^+|w| + \log 2).$$

Soient $r > 1$ un réel et $\varphi\colon \mathbf{R}_+ \longrightarrow [0,1]$ une fonction continue telle que

- $\varphi(t) = 1$ si $0 \leqslant t \leqslant r$;
- $\varphi(t) = 0$ si $t \geqslant 2r$.

La fonction $(z,w) \longmapsto \varphi(|z|)\varphi(|w|)\ell_M(|z-w|)$ est continue sur $\overline{\mathbf{C}} \times \overline{\mathbf{C}}$. On peut écrire

$$\begin{aligned}
\acute{\mathrm{E}}\mathrm{n}^0(\mu_n) &\geqslant \frac{1}{d_n^2}\sum_{i\neq j}\ell_M(|z_i(n) - z_j(n)|) \\
&= \iint_{\overline{\mathbf{C}}\times\overline{\mathbf{C}}} \ell_M(|z-w|)\,\mathrm{d}\mu_n(z)\,\mathrm{d}\mu_n(w) - \frac{M}{d_n} \\
&= \iint_{\overline{\mathbf{C}}\times\overline{\mathbf{C}}} (\varphi(|z|) + 1 - \varphi(|z|))(\varphi(|w|) + 1 - \varphi(|w|))\ell_M(|z-w|)\,\mathrm{d}\mu_n(z)\,\mathrm{d}\mu_n(w) - \frac{M}{d_n} \\
&= I_1(n) + I_2(n) + I_3(n) - \frac{M}{d_n}
\end{aligned}$$

avec

$$\begin{aligned}
I_1(n) &\coloneqq \iint \varphi(|z|)\varphi(|w|)\ell_M(|z-w|)\,\mathrm{d}\mu_n(z)\,\mathrm{d}\mu_n(w) \\
&\longrightarrow \iint \ell_M(|z-w|)\,\mathrm{d}\mu(z)\,\mathrm{d}\mu(w), \\
I_2(n) &\coloneqq 2\iint (1-\varphi(|z|))\varphi(|w|)\ell_M(|z-w|)\,\mathrm{d}\mu_n(z)\,\mathrm{d}\mu_n(w) \\
&\geqslant -2\int_{\overline{\mathbf{C}}\setminus D_r}\int_{\overline{\mathbf{C}}} \log(2r) + \log^+|w|\,\mathrm{d}\mu_n(z)\,\mathrm{d}\mu_n(w) \\
&\geqslant -2\mu_n(\overline{\mathbf{C}} - D_r)\log(2r) - 2\mu_n(\overline{\mathbf{C}}\setminus\mathbf{D}_r)\int_{\mathbf{C}}\log^+|w|\,\mathrm{d}\mu_n(w).
\end{aligned}$$

Or $\mu_n(\overline{\mathbf{C}} - D_r) \leqslant \delta_{P_n}(r) \longrightarrow 0$ et

$$\int_{\mathbf{C}} \log^+ |w| \, \mathrm{d}\mu_n(w) = \frac{1}{d_n} \sum_{i=1}^{d_n} \log^+ |z_i(n)| = \frac{1}{d_n} m(P_n) - \frac{1}{d_n} \log |a_{d_n}(n)| \longrightarrow 0.$$

D'où $\liminf_{n \longrightarrow +\infty} I_2(n) \longrightarrow 0$. Enfin, on trouve

$$I_3(n) \coloneqq \iint (1 - \varphi(|z|))(1 - \varphi(|w|)) \ell_M(|z - w|) \, \mathrm{d}\mu_n(z) \, \mathrm{d}\mu_n(w)$$

et, par le même argument, l'inégalité $\liminf_{n \longrightarrow +\infty} I_3(n) \geqslant 0$. Par passage à la limite, on en déduit

$$\liminf_{n \longrightarrow +\infty} \text{Én}^0(\mu_n) \geqslant \iint_{\mathbf{S}^1 \times \mathbf{S}^1} \ell_M(|z - w|) \, \mathrm{d}\mu(z) \, \mathrm{d}\mu(w).$$

En faisant $M \longrightarrow +\infty$, on trouve alors $\text{Én}(\mu) \leqslant 0$ et donc $\text{Én}(\mu) = 0$. ◇

Chapitre 14
Compléments

14.1. Théorie de potentiel sur C

Soit μ une mesure de probabilité sur $\mathbf{C}$ à support compact. Son *potentiel* créé en un point $z \in \mathbf{C}$ est la quantité

$$P_\mu(z) \coloneqq \int_{\mathbf{C}} \log|z-w| \,\mathrm{d}\mu(w).$$

Il vérifie

$$\text{Én}(\mu) = -\int_{\mathbf{C}} P_\mu(z) \,\mathrm{d}\mu(z).$$

On fixe un compact $K \subset \mathbf{C}$. Une mesure $\mu \in \text{Proba}(K)$ est une *mesure équilibre* de K si elle réalise le minimum $\text{Én}(K)$ des énergies $\text{Én}(\mu)$ avec $\mu \in \text{Proba}(K)$. Le compact K est *polaire* si $\text{Én}(K) = +\infty$. Les ensembles polaires jouent le rôle des ensembles négligeables dans la théorie du potentiel. Un ensemble $E \subset \mathbf{C}$ est polaire si tous ses compacts le sont.

Remarque. Un ensemble polaire est de mesure de Lebesgue nulle. Si $\text{Én}(\mu) < +\infty$ et E est polaire, alors $\mu(E) = 0$.

Exercice 10. Montrer qu'il existe toujours des mesures d'équilibres.

Théorème 14.1 *(Frostman).* Soient $K \subset \mathbf{C}$ un compact et $\nu \in \text{Proba}(K)$ une mesure d'équilibre. Alors

1. $P_\nu(z) \geqslant -\text{Én}(K)$ pour tout $z \in \mathbf{C}$;
2. $P_\nu = -\text{Én}(K)$ sur K privé de l'ensemble polaire
$$E \coloneqq \bigcup_{n \geqslant 1} \{z \in K \mid p_\nu(z) \geqslant -\text{Én}(K) + 1/n\}$$
où chaque ensemble de cette intersection est un compact polaire contenu dans ∂K ;
3. en particulier, on a $P_\nu = -\text{Én}(K)$ sur K privé d'un ensemble de mesure de Lebesgue nulle ;
4. si K n'est pas polaire, alors la mesure d'équilibre est unique.

Exemple. Si K est le cercle unité, alors $\nu = \mathrm{d}\theta$. Son potentiel est $p_\nu(z) = \log^+|z|$.

On suppose que K n'est pas polaire. Sa *fonction de Green* est

$$g_K(z) = p_{\nu_K}(z) + \text{Én}(K)$$

et sa *capacité* est

$$\text{cap}(K) \coloneqq e^{-\text{Én}(K)}.$$

Exercice 11. Montrer que

$$g_K(z) = \log \frac{|z|}{\operatorname{cap} K} + \mathrm{O}\Big(\frac{1}{|z|}\Big).$$

Proposition 14.2.
1. On a $\operatorname{cap}(K) \geqslant 0$.
2. On a $\operatorname{cap}(K) \subset \operatorname{cap}(K')$ si $K \subset K'$.
3. On a $\operatorname{cap}(aK + b) = |\alpha| \operatorname{cap}(K)$.
4. On a $\operatorname{cap}(\mathbf{D}_r) = r$.
5. Si $f \in \mathbf{C}[z]$, alors $\operatorname{cap}(f^{-1}(K)) = (\operatorname{cap}(K)/|a_d|)^{1/d}$ où a_d est le coefficient dominant de f.

Pour un compact K, on pose

$$\operatorname{diam}^n(K) \coloneqq \sup\Big\{ \Big(\prod_{i<j} |w_i - w_j|\Big)^{2/n(n-1)} \;\Big|\; w_1, \dots, w_n \in K \Big\}.$$

Théorème 14.3 *(Fekete-Szegö).* La suite $(\operatorname{diam}^n(K))_{n\in\mathbf{N}^*}$ converge vers $\cap(K)$.

14.2. Équidistribution arithémtique

Théorème 14.4. Soit $K \subset \mathbf{C}$ un compact symétrique par rapport à l'axe réel. Alors $\operatorname{cap}(K) \geqslant 1$ si et seulement si, pour tout ouvert $U \subset \mathbf{C}$ tel que $K \subset U$ et tout entier $d \geqslant 1$, il existe un entier algébrique α de degré $\geqslant d$ dont tous les conjugués galoisiens soient dans U.

Soit $K \subset \mathbf{C}$ un compact non polaire. Soit $\alpha \in \overline{\mathbf{Q}}$ un nombre algébrique de degré d. On considère son polynôme minimal $P_\alpha \in \mathbf{Z}[t]$. On pose

$$h_K(\alpha) \coloneqq \frac{1}{d}\Big(\log|a_d| + \sum_{j=1}^{d} g_k(z_j)\Big)$$

où les complexes z_i sont les racînes du polynômes P_α.

Exercice 12.
1. Si $L/\mathbf{Q}$ est une extension qui contient α, alors
$$h_K(\alpha) = \frac{1}{[L:\mathbf{Q}]}\Big(\sum_{v\in M_L^{\mathrm{fini}}} [L_v : \mathbf{Q}_v] \log^+|\alpha|_v + \sum_{\sigma\colon L\hookrightarrow\mathbf{C}} g_K(\sigma(\alpha))\Big).$$
2. Il existe une constante $C_K \geqslant 0$ telle que $|h - h_K| \leqslant C_K$ sur $\overline{\mathbf{Q}}$.

Théorème 14.5 *(Bilu-Rumely).* Soient $K \subset \mathbf{C}$ un compact et $(\alpha_n)_{n\in\mathbf{N}}$ une suite de nombres algébriques tels que
- $h_K(\alpha_n) \longrightarrow 0$;
- $\deg \alpha_n \longrightarrow +\infty$;
- $\operatorname{cap}(K) = 1$.

Alors

$$\frac{1}{\deg\alpha_n} \sum_{j=1}^{\deg\alpha_n} \delta_{z_j(n)} \longrightarrow \nu_K$$

où les complexes $z_j(n)$ sont les conjugués du nombre α_n.

14.3. Itération de polynômes

Soit $f \in \mathbf{C}[t]$ un polynôme de degré $d \geqslant 2$. On pose

$$K_f \coloneqq \{z \in \mathbf{C} \mid \text{la suite } (f^n(z))_{n\in\mathbf{N}} \text{ est bornée}\}.$$

Ce compact vérifie $f^{-1}(K_f) = K_f$. Son *ensemble de Fatou* est le complémentaire $F(f) \coloneqq \overline{\mathbf{C}} \setminus \partial K_f$. C'est un ensemble où localement la suite $(f^n)_{n\in\mathbf{N}}$ forment une famille équicontinue (plus difficile).

Théorème 14.6. On suppose que le polynôme f est unitaire. Alors

1. $\mathrm{cap}(K_f) = 1$;
2. la fonction de Green g_{K_f} vérifie
$$g_{K_f}(z) = \lim_{n \longrightarrow +\infty} \frac{1}{\deg f^n} \log^+ |f^n(z)| \ ;$$
3. la mesure ν_{K_f} est f-invariante, c'est-à-dire
$$f_* \nu_{K_f} = \nu_{K_f}.$$

Théorème 14.7 *(Brolin-Lyubich-Mañé).*

1. Pour tout $w \in \mathbf{C}$ privé d'au plus un point q, on a
$$\frac{1}{\deg f^n} \sum_{f^n(z)=w} \delta_z \longrightarrow \nu_{K_f}.$$
2. On a
$$\frac{1}{\deg f^n} \sum_{f^n(z)=z} \delta_z \longrightarrow \nu_{K_f}.$$

14.4. Polynômes à coefficients algébriques

Soit $f \in \overline{\mathbf{Q}}[t]$ un polynôme unitaire à coefficients algébriques. Alors
$$h_{K_f}(\alpha) = \hat{h}_f(\alpha), \qquad \forall \alpha \in \overline{\mathbf{Q}}.$$

Corollaire 14.8. Soient $f, g \in \overline{\mathbf{Q}}[t]$ deux polynômes de degré $\geqslant 2$ ayant une infinité de points périodiques communs. Alors $\nu_{K_f} = \nu_{K_g}$ et $K_f = K_g$.