PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

JEAN-PIERRE SERRE

Quelques applications du théorème de densité de Chebotarev

Publications mathématiques de l'I.H.É.S., tome 54 (1981), p. 123-201

<http://www.numdam.org/item?id=PMIHES_1981__54__123_0>

QUELQUES APPLICATIONS DU THÉORÈME DE DENSITÉ DE CHEBOTAREV

par JEAN-PIERRE SERRE

Les applications en question concernent surtout les *formes modulaires* et les *courbes elliptiques*. L'exemple suivant (cf. n° 7.4) est typique :

Soit $f = q \prod_{n=1}^{\infty} (1-q^n)^2(1-q^{11n})^2 = \sum_{n=1}^{\infty} a_n q^n$.

C'est une forme modulaire de poids 2 et de niveau 11 ; elle est associée à la courbe elliptique E d'équation $Y^2 - Y = X^3 - X^2$. Soit Σ_E l'ensemble des nombres premiers p tels que $a_p = 0$; si $p \neq 2$, on a $p \in \Sigma_E$ si et seulement si la réduction de E en p est une courbe elliptique *supersingulière*. Soit x un nombre réel $\geqslant 2$; notons $P_E(x)$ le nombre des $p \in \Sigma_E$ tels que $p \leqslant x$. On sait ([40], IV-13, exerc. 1) que :

(a) $$P_E(x) = o(x/\log x) \quad \text{pour } x \to \infty,$$

autrement dit que Σ_E est *de densité zéro* dans l'ensemble des nombres premiers. Ce résultat est loin d'être optimal : d'après Lang et Trotter ([24]), il est vraisemblable que

($b_?$) $$P_E(x) \sim c_E x^{1/2}/\log x \quad \text{avec } c_E > 0.$$

Nous nous proposons d'*améliorer (a)* — tout en restant, hélas, loin de *($b_?$)* — en prouvant :

(c) $$P_E(x) = O(x/(\log x)^{3/2-\varepsilon}) \quad \text{pour tout } \varepsilon > 0,$$

et, sous l'hypothèse de Riemann généralisée (GRH) :

(d_R) $$P_E(x) = O(x^{3/4}).$$

La majoration *(c)* entraîne :

(c') $$\sum_{p \in \Sigma_E} 1/p < \infty.$$

On déduit de là, et de la multiplicativité de $n \mapsto a_n$, que la série f *n'est pas lacunaire* : si l'on note $M_f(x)$ le nombre des entiers $n \leqslant x$ tels que $a_n \neq 0$, on a

(e) $$M_f(x) \sim \alpha x,$$

où α est un nombre >0 donné par :

$$\alpha = \frac{14}{15} \prod_{p \in \Sigma_E} \left(1 - \frac{1}{p+1}\right) < 0{,}847.$$

Le principe de la démonstration de *(c)* et *(d_R)* est le suivant. Soit ℓ un nombre premier, et soit

$$\rho_\ell : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{Z}_\ell)$$

la représentation ℓ-adique définie par les points de ℓ^m-division de la courbe E ($m = 0, 1, \ldots$). Cette représentation est non ramifiée en dehors de $\{11, \ell\}$. Le groupe $G_\ell = \mathrm{Im}(\rho_\ell)$ est un sous-groupe *ouvert* ([40], [41]) de $\mathbf{GL}_2(\mathbf{Z}_\ell)$; c'est un groupe de Lie ℓ-adique de dimension 4. Si $p \neq 11, \ell$, la *substitution de Frobenius* s_p de p dans G_ℓ est bien définie (à conjugaison près), et l'on sait, d'après Eichler, Shimura et Igusa, que

$$\mathrm{Tr}(s_p) = a_p.$$

La relation $a_p = 0$ équivaut donc à dire que s_p *appartient à la sous-variété* C_ℓ *de* G_ℓ *formée des éléments de trace* 0. Il est immédiat que C_ℓ est *de mesure nulle* dans G_ℓ, ce qui entraîne *(a)* grâce au théorème de Chebotarev « qualitatif » (cf. n° 2.1, th. 1). Pour aller plus loin, et obtenir *(c)* et *(d_R)*, on applique à certains quotients finis de G_ℓ les formes « quantitatives » du théorème de Chebotarev démontrées récemment par Lagarias, Montgomery et Odlyzko ([22], [23]).

La mise en œuvre de la méthode esquissée ci-dessus demande un certain nombre de préliminaires, qui font l'objet des trois premiers paragraphes. Le § 1 contient des majorations de discriminants, d'après Hensel [15]. Le § 2 rappelle les résultats de [22] et [23] sur le théorème de Chebotarev, et les complète sur quelques points. Le § 3 donne des estimations du nombre de points mod ℓ^n d'une variété analytique ℓ-adique : si la dimension de la variété est d, le nombre en question est $O(\ell^{nd})$ pour $n \to \infty$. On passe ensuite (§ 4) aux *extensions à groupe de Galois un groupe de Lie ℓ-adique*. Si G est le groupe de Galois, et C une sous-variété de G stable par conjugaison, on s'intéresse au nombre $\pi_C(x)$ des $p \leqslant x$ dont la substitution de Frobenius dans G appartient à C (je me borne ici, pour simplifier, au cas où le corps de base est $\mathbf{Q}$). On obtient pour $\pi_C(x)$ des majorations analogues à *(c)* et *(d_R)* ci-dessus; dans ces majorations figurent des exposants qui dépendent des dimensions de G et de C comme variétés ℓ-adiques. Le § 5 améliore ces exposants, dans le cas où C ne contient aucune classe de conjugaison finie. C'est grâce à cette amélioration que le membre de droite de *(d_R)* est $O(x^{3/4})$; sinon, on n'obtiendrait que $O(x^{5/6})$.

Le § 6 donne une application du § 4 à la lacunarité des fonctions multiplicatives, et en particulier des coefficients des *fonctions* L attachées à des représentations ℓ-adiques. Si $L(s) = \sum a_n n^{-s}$ est une telle fonction, et si l'on pose

$$M_L(x) = \text{nombre des } n \leqslant x \text{ tels que } a_n \neq 0,$$

on montre que :

(f) $\qquad M_L(x) \sim c_L x/(\log x)^\lambda, \quad$ avec $c_L > 0$,

où λ est un nombre rationnel. On a $0 \leqslant \lambda \leqslant 1 - 1/r^2$, où r est le degré de la représentation ℓ-adique attachée à $L(s)$. La valeur de λ ne dépend que de l'enveloppe algébrique du groupe de Galois ℓ-adique; si cette enveloppe est connexe pour la topologie de Zariski, on a $\lambda = 0$ et $L(s)$ n'est pas lacunaire.

Le § 7 contient les applications aux formes modulaires; il utilise de façon essentielle les représentations ℓ-adiques associées à ces formes par Deligne ([7], [9]). On y trouve des généralisations de *(c)*, *(d_R)* et *(f)* ci-dessus aux formes de poids $\geqslant 2$; on montre en particulier qu'une telle forme n'est pas lacunaire, sauf si elle est combinaison linéaire de formes « de type CM » au sens de Ribet [33] (ces dernières correspondent à $\lambda = 1/2$, avec les notations de *(f)*). Le cas du poids 1, quelque peu différent, est traité séparément; j'ai donné au n° 7.8 un exemple de calcul effectif de la constante c_L de *(f)*, dans un cas où l'exposant λ prend sa valeur maximale, qui est 3/4.

Le dernier paragraphe (§ 8) est consacré aux courbes elliptiques sur $\mathbf{Q}$. Il débute par des résultats analogues à ceux du § 7. Il continue par un théorème de comparaison entre deux courbes elliptiques, d'où l'on déduit finalement ceci :

Soit E une courbe elliptique sur $\mathbf{Q}$, sans multiplication complexe, et soit N_E le produit des nombres premiers en lesquels E a mauvaise réduction. Si p est un nombre premier, soit G_p le groupe de Galois des points de p-division de E. Il existe une constante absolue c telle que, *sous* (GRH), *on ait* $G_p \simeq \mathbf{GL}_2(\mathbf{F}_p)$ *pour tout p tel que*

$$p \geqslant c(\log N_E)(\log\log 2N_E)^3.$$

Cela précise (sous (GRH)...) le théorème, démontré dans [41], suivant lequel on a $G_p \simeq \mathbf{GL}_2(\mathbf{F}_p)$ pour p assez grand.

Comme le montre le résumé ci-dessus, le présent travail consiste essentiellement en une série de *majorations* (c'est plus de l'Analyse que de la Théorie des Nombres, dirait Weil). J'ai essayé de rendre ces majorations aussi précises que possible, au prix de quelques complications de détail (cf. § 5, notamment). Toutefois cette apparente précision ne doit pas faire illusion : *aucun des résultats obtenus n'est optimal*, même pas ceux démontrés sous (GRH). Le lecteur de bonne volonté ne manquera donc pas de problèmes à résoudre.

TABLE DES MATIÈRES

§ 1. Majorations de discriminants

1.1. Notations

Soit K un corps de nombres algébriques, autrement dit une extension finie de $\mathbf{Q}$. On pose :

A_K = anneau des entiers de K,

$n_K = [K : \mathbf{Q}] = [A_K : \mathbf{Z}]$ = degré de K,

Σ_K = ensemble des places ultramétriques de K,

d_K = valeur absolue du discriminant de K.

Si $v \in \Sigma_K$, on identifie v à la valuation discrète normée correspondante (de groupe des valeurs $\mathbf{Z}$), et l'on note $\mathfrak{p}_v$ l'idéal premier de A_K qui correspond à v. Le corps résiduel $A_K/\mathfrak{p}_v$ est un corps fini; on note p_v sa caractéristique, et Nv le nombre de ses éléments. On a

$$Nv = N\mathfrak{p}_v = (p_v)^{f_v},$$

où f_v est le degré résiduel de v. L'indice de ramification e_v de v est défini par $e_v = v(p_v)$; c'est le plus grand entier positif e tel que $\mathfrak{p}_v^e$ divise p_v.

Soit E une extension finie de K, de degré $n = n_E/n_K = [E : K]$. On note $\mathfrak{D}_{E/K}$ (resp. $\mathfrak{d}_{E/K}$) la différente (resp. le discriminant) de l'extension E/K; c'est un idéal $\neq 0$ de A_E (resp. A_K). On a

$$\mathfrak{d}_{E/K} = N_{E/K}(\mathfrak{D}_{E/K}) \quad \text{et} \quad d_E = (d_K)^n N(\mathfrak{d}_{E/K}), \tag{1}$$

cf. par exemple [38], chap. III.

1.2. Estimations locales

Soit E/K comme ci-dessus, et soit $w \in \Sigma_E$ une place ultramétrique de E. Notons v la place de K induite par w, et soit $e_{w/v} = e_w/e_v$ l'indice de ramification de w par rapport à v. On s'intéresse à *l'exposant* $w(\mathfrak{D}_{E/K})$ de l'idéal premier $\mathfrak{p}_w$ dans la différente $\mathfrak{D}_{E/K}$:

Proposition 1. — On a

$$w(\mathfrak{D}_{E/K}) = e_{w/v} - 1 + s_{w/v}, \quad \text{avec } 0 \leqslant s_{w/v} \leqslant w(e_{w/v}).$$

Ce résultat est dû à Hensel [15]; il avait été conjecturé par Dedekind [6]. Rappelons-en brièvement la démonstration (pour plus de détails, voir [38], chap. III, fin du § 6) :

Par des réductions standard (localisation, complétion, etc.), on se ramène à prouver l'énoncé analogue lorsque E et K sont des *corps locaux*, et que E/K est totalement ramifiée, i.e. $e_{w/v}=n$. Si π est une uniformisante de E en w, π satisfait à une *équation d'Eisenstein* $f(\pi)=0$, où $f(X)$ est un polynôme

$$f(X)=a_0X^n+\ldots+a_n,$$

avec $a_i\in K$, $a_0=1$, $v(a_i)\geqslant 1$ pour $i\geqslant 1$ et $v(a_n)=1$.

La différente $\mathfrak{D}_{E/K}$ est engendrée par

$$f'(\pi)=\sum_{0\leqslant i\leqslant n-1}(n-i)a_i\pi^{n-i-1}.$$

Comme $(n-i)a_i$ appartient à K, on a

$$\begin{aligned} w((n-i)a_i\pi^{n-i-1}) &= n-i-1+nv((n-i)a_i) \\ &\equiv -i-1 \pmod n \end{aligned}$$

si $(n-i)a_i\neq 0$. Ainsi, les différents termes non nuls de $f'(\pi)$ ont des valuations *distinctes* (puisque distinctes modulo n). Il en résulte que

$$w(\mathfrak{D}_{E/K})=\operatorname*{Inf}_{0\leqslant i\leqslant n-1} w((n-i)a_i\pi^{n-i-1}).$$

Le terme correspondant à $i=0$ est $n-1+w(n)$; ceux correspondant à $i\geqslant 1$ sont $\geqslant n$. On en conclut que

$$n-1\leqslant w(\mathfrak{D}_{E/K})\leqslant n-1+w(n),$$

d'où le résultat cherché.

Remarque. — Le terme $s_{w/v}$ est la « partie sauvage » de $w(\mathfrak{D}_{E/K})$: il est nul si et seulement si p_v ne divise pas $e_{w/v}$, autrement dit si et seulement si l'extension E/K est « modérée » en w.

Passons maintenant à $\mathfrak{d}_{E/K}$. Soit $v\in\Sigma_K$, de caractéristique résiduelle $p=p_v$; notons v_p la valuation p-adique usuelle du corps $\mathbf{Q}$; on a $v(x)=e_vv_p(x)$ pour tout $x\in\mathbf{Q}$.

Proposition 2. — On a

$$v(\mathfrak{d}_{E/K})\leqslant n-1+ne_v\operatorname*{Sup}_{w\mid v}v_p(e_{w/v}).$$

(Rappelons que $n=[E:K]$, et que $w\mid v$ signifie que v est induite par w, ou encore que w « divise » v.)

La formule $\mathfrak{d}_{E/K}=N_{E/K}(\mathfrak{D}_{E/K})$ montre que

$$v(\mathfrak{d}_{E/K})=\sum_{w\mid v}f_{w/v}w(\mathfrak{D}_{E/K}),\quad\text{avec}\quad f_{w/v}=f_w/f_v.$$

En appliquant la prop. 1, on en déduit

$$v(\mathfrak{d}_{E/K}) = \sum_{w|v} f_{w/v}(e_{w/v}-1) + \sum_{w|v} f_{w/v} s_{w/v} \tag{2}$$
$$\leqslant \sum_{w|v} f_{w/v} e_{w/v} - 1 + \sum_{w|v} f_{w/v} e_w v_p(e_{w/v})$$
$$\leqslant n - 1 + n e_v \operatorname*{Sup}_{w|v} v_p(e_{w/v}),$$

du fait que $n = \sum_{w|v} f_{w/v} e_{w/v}$.

Corollaire. — *On a*

$$v(\mathfrak{d}_{E/K}) \leqslant n - 1 + n e_v \log n/\log p.$$

En effet, pour tout w divisant v, on a $e_{w/v} \leqslant n$ et l'exposant de p dans $e_{u/v}$ est donc $\leqslant \log n/\log p$.

Proposition 3. — *Supposons* E/K *galoisienne, et ramifiée en v. On a alors :*

$$n/2 \leqslant v(\mathfrak{d}_{E/K}) \leqslant n - 1 + n e_v v_p(n).$$

Les places w divisant v sont conjuguées entre elles par le groupe de Galois Gal(E/K). Tous les $e_{w/v}$ sont donc égaux à un même entier e; de même, les $f_{w/v}$ sont égaux à un même entier f, et l'on a $n = efg$, où g est le nombre des w. Puisque e divise n, on a $v_p(e) \leqslant v_p(n)$ et la prop. 2 montre que

$$v(\mathfrak{d}_{E/K}) \leqslant n - 1 + n e_v v_p(e) \leqslant n - 1 + n e_v v_p(n).$$

D'autre part, comme E/K est ramifiée en v, on a $e \geqslant 2$, et la formule (2) ci-dessus montre que

$$v(\mathfrak{d}_{E/K}) \geqslant gf(e-1) \geqslant n(1-1/e) \geqslant n/2.$$

1.3. Estimations globales

On s'intéresse maintenant à la norme $N(\mathfrak{d}_{E/K})$ du discriminant (relatif) de E/K, ainsi qu'aux discriminants (absolus) des corps E et K. D'après (1), on a

$$\log d_E = n \log d_K + \log N(\mathfrak{d}_{E/K}). \tag{3}$$

Notons V(E/K) l'ensemble des $v \in \Sigma_K$ qui sont ramifiés dans E, autrement dit tels que $v(\mathfrak{d}_{E/K}) > 0$. Notons P(E/K) l'ensemble des nombres premiers de la forme p_v, pour $v \in V(E/K)$. Ces ensembles sont finis.

Proposition 4. — *On a*

$$\log N(\mathfrak{d}_{E/K}) \leqslant n_E(1-1/n) \sum_{p \in P(E/K)} \log p + n_E |P(E/K)| \log n.$$

(Si P est un ensemble fini, on note $|P|$ le nombre de ses éléments.)

Compte tenu de (3), on peut reformuler la prop. 4 de la façon suivante :

Proposition 4'. — On a

$$\log d_E \leqslant n \log d_K + n_E(1-1/n) \sum_{p \in P(E/K)} \log p + n_E |P(E/K)| \log n.$$

Démonstration de la prop. 4

Comme $\log Nv = f_v \log p_v$, on a

$$\log N(\mathfrak{d}_{E/K}) = \sum_{v \in V(E/K)} v(\mathfrak{d}_{E/K}) f_v \log p_v, \tag{4}$$

et en appliquant le cor. à la prop. 2, on en déduit

$$\log N(\mathfrak{d}_{E/K}) \leqslant \sum_{v \in V(E/K)} \{(n-1) f_v \log p_v + n f_v e_v \log n\}. \tag{5}$$

Or, pour tout nombre premier p, on a

$$\sum_{p_v = p} f_v e_v = n_K \qquad \text{et} \qquad \sum_{p_v = p} f_v \leqslant n_K.$$

La majoration (5) ci-dessus entraîne donc :

$$\log N(\mathfrak{d}_{E/K}) \leqslant (n-1) n_K \sum_{p \in P(E/K)} \log p + n n_K |P(E/K)| \log n,$$

ce qui établit la prop. 4, vu que $n_E = n n_K$.

Dans le cas galoisien, le terme $|P(E/K)|$ peut être remplacé par 1. De façon plus précise :

Proposition 5. — Supposons E/K *galoisienne. On a alors* :

$$\log N(\mathfrak{d}_{E/K}) \leqslant n_E(1-1/n) \sum_{p \in P(E/K)} \log p + n_E \log n \tag{6}$$

et

$$\log d_E \geqslant \log N(\mathfrak{d}_{E/K}) \geqslant \frac{n}{2} \sum_{v \in V(E/K)} \log Nv. \tag{7}$$

En combinant (4) à la majoration de $v(\mathfrak{d}_{E/K})$ donnée par la prop. 3, on obtient

$$\log N(\mathfrak{d}_{E/K}) \leqslant \sum_{v \in V(E/K)} \{(n-1) f_v \log p_v + n f_v e_v v_{p_v}(n) \log p_v\}.$$

En utilisant les majorations

$$\Sigma f_v \log p_v \leqslant \Sigma f_v e_v \log p_v \leqslant n_K \sum_{p \in P(E/K)} \log p$$

et

$$\Sigma f_v e_v v_{p_v}(n) \log p_v \leqslant n_K \sum_{p \in P(E/K)} v_p(n) \log p \leqslant n_K \log n,$$

on en déduit

$$\log \mathrm{N}(\mathfrak{d}_{\mathrm{E/K}}) \leqslant n_{\mathrm{K}}(n-1) \sum_{p \in \mathrm{P(E/K)}} \log p + n n_{\mathrm{K}} \log n,$$

ce qui équivaut à (6).

L'inégalité

$$\log \mathrm{N}(\mathfrak{d}_{\mathrm{E/K}}) \geqslant \frac{n}{2} \sum_{v \in \mathrm{V(E/K)}} \log \mathrm{N}v$$

résulte de façon analogue de (4), combinée avec la minoration $v(\mathfrak{d}_{\mathrm{E/K}}) \geqslant n/2$ de la prop. 3. Enfin, l'inégalité

$$\log d_{\mathrm{E}} \geqslant \log \mathrm{N}(\mathfrak{d}_{\mathrm{E/K}})$$

résulte de (3).

1.4. Le cas particulier $\mathrm{K} = \mathbf{Q}$

On écrit alors P(E) au lieu de P(E/**Q**); on a $p \in \mathrm{P(E)}$ si et seulement si p divise d_{E}. Les prop. 4 et 5 donnent :

Proposition 6. — Si E *est un corps de nombres de degré n sur* **Q**, *on a*

$$\log d_{\mathrm{E}} \leqslant (n-1) \sum_{p \in \mathrm{P(E)}} \log p + n\,|\mathrm{P(E)}| \log n.$$

Si de plus E *est galoisien sur* **Q**, *on a*

$$\frac{n}{2} \sum_{p \in \mathrm{P(E)}} \log p \leqslant \log d_{\mathrm{E}} \leqslant (n-1) \sum_{p \in \mathrm{P(E)}} \log p + n \log n.$$

Si l'on note δ_{E} le produit des $p \in \mathrm{P(E)}$, autrement dit le plus grand diviseur sans facteur carré de d_{E}, on peut reformuler les inégalités du cas galoisien sous la forme

$$\delta_{\mathrm{E}}^{n/2} \leqslant d_{\mathrm{E}} \leqslant n^n \delta_{\mathrm{E}}^{n-1}.$$

(Ces relations d'inégalité sont même des relations de *divisibilité*, comme le montre la prop. 3.)

Exemple

Soient p un nombre premier, m un entier $\geqslant 1$, et $\mathrm{E} = \mathbf{Q}(\pi)$ avec $\pi^{p^m} = p$. On a $n = p^m$, $\mathrm{P(E)} = \{p\}$ et la différente de E est engendrée par $p^m \pi^{p^m - 1}$; on en conclut que

$$d_{\mathrm{E}} = p^{m p^m + p^m - 1} = n^n p^{n-1},$$

ce qui fournit un exemple où la majoration de la prop. 6 est en fait une *égalité*.

§ 2. Formes effectives du théorème de Chebotarev

2.1. Le théorème de Chebotarev

Soit E/K une extension galoisienne finie de corps de nombres, et soit $G = \mathrm{Gal}(E/K)$. On conserve les notations du § 1; en particulier, on pose

$$n_E = [E : \mathbf{Q}], \quad n_K = [K : \mathbf{Q}], \quad n = [E : K] = n_E/n_K = |G|,$$

et l'on note V(E/K) l'ensemble des places $v \in \Sigma_K$ qui sont ramifiées dans l'extension E.

Si $v \in \Sigma_K$ n'appartient pas à V(E/K), et si $w \in \Sigma_E$ divise v, on note σ_w la *substitution de Frobenius* de w; c'est l'unique élément s de G tel que

$$s(a) \equiv a^{Nv} \pmod{\mathfrak{p}_w} \quad \text{pour tout } a \in A_E.$$

La classe de conjugaison de σ_w ne dépend que de v; on la note σ_v (et l'on se permet de noter également σ_v un élément quelconque de cette classe).

Soient maintenant C une partie de G stable par conjugaison, et Σ_C l'ensemble des $v \in \Sigma_K - V(E/K)$ tels que $\sigma_v \in C$. Le résultat suivant, conjecturé par Frobenius [12], a été démontré par Chebotarev (cf. [1], [47]) :

Théorème 1. — L'ensemble Σ_C est de densité $|C|/|G|$ dans Σ_K.

Précisons ce que nous entendons par « densité ». Si x est un nombre réel $\geqslant 2$, notons $\pi_K(x)$ (resp. $\pi_C(x)$) le nombre des places $v \in \Sigma_K$ (resp. $v \in \Sigma_C$) telles que $Nv \leqslant x$. D'après le « théorème des nombres premiers », appliqué au corps K, on a

$$\pi_K(x) \sim x/\log x \quad \text{pour } x \to \infty. \tag{8}$$

Dire que Σ_C est de densité $\lambda = |C|/|G|$ signifie que

$$\lim_{x \to \infty} \pi_C(x)/\pi_K(x) = \lambda,$$

autrement dit que

$$\pi_C(x) = \lambda x/\log x + o(x/\log x) \quad \text{pour } x \to \infty. \tag{9}$$

(On peut également exprimer le th. 1 en disant que les substitutions de Frobenius sont *équiréparties* dans l'ensemble des classes de conjugaison de G, cf. par exemple [40], Chap. I, App.)

2.2. Une forme effective du théorème de Chebotarev

Il s'agit de préciser le « $o(x/\log x)$ » qui figure dans (9). Avant d'énoncer le résultat, rappelons que la fonction zêta du corps E a au plus un zéro réel positif s tel que

$$1-s \leqslant 1/4 \log d_E;$$

si un tel zéro existe, il est dit *exceptionnel*, et on le note β.

La forme effective du th. 1 démontrée par Lagarias-Odlyzko [23] est la suivante :

Théorème 2. — Il existe des constantes absolues $c_1, c_2, c_3 > 0$ telles que

$$\left|\pi_C(x) - \frac{|C|}{|G|}\operatorname{Li}(x)\right| \leqslant \frac{|C|}{|G|}\operatorname{Li}(x^\beta) + c_1|\widetilde{C}|x\exp(-c_2 n_E^{-1/2}\log^{1/2}x) \tag{10}$$

pour tout $x \geqslant 2$ tel que

$$\log x \geqslant c_3 n_E \log^2 d_E. \tag{11}$$

(Dans (10), $|\widetilde{C}|$ désigne le nombre de classes de conjugaison contenues dans C. Quant au terme $\frac{|C|}{|G|}\operatorname{Li}(x^\beta)$, on le supprime s'il n'y a pas de zéro exceptionnel.)

Rappelons que $\operatorname{Li}(x) = \int_2^x dt/\log t$. Comme $\operatorname{Li}(x) \sim x/\log x$ pour $x \to \infty$, la formule (10) est bien une amélioration de (9).

Remarques

1) Le cas traité dans [23] est celui où C est une classe de conjugaison de G, i.e. $|\widetilde{C}| = 1$. Le cas général s'en déduit par additivité.

2) On pourrait affaiblir sensiblement la condition (11), ce qui renforcerait le théorème. Nous n'en aurons pas besoin : en fait, ce n'est pas le th. 2 lui-même que nous utiliserons dans la suite, mais seulement ses variantes, les ths. 3, 4, 5, 6 ci-après.

3) Insistons sur le fait que les constantes c_1, c_2, c_3 (de même que les $c_4, c_5, \ldots, c_{36}$ introduites plus loin) sont *absolues*, i.e. indépendantes de K, E, C, G, x. De plus, ces constantes sont *effectivement calculables*, au moins en principe. On peut, par exemple, prendre $c_2 = 1/20$.

2.3. Majoration de $\pi_C(x)$

Une telle majoration résulte bien sûr du th. 2, combiné avec le fait que $\beta < 1$ (ou, mieux encore, avec les majorations de β données dans [22] et [45]). On peut également (et c'est ce que nous ferons) utiliser le résultat suivant, dû à Lagarias-Montgomery-Odlyzko ([22], th. (1.4)) :

Théorème 3. — Il existe des constantes absolues c_4 et c_5 telles que

$$\pi_C(x) \leqslant c_4 \frac{|C|}{|G|}\operatorname{Li}(x) \tag{12}$$

pour tout $x \geqslant 3$ *tel que*

$$\log x \geqslant c_5(\log d_E)(\log\log d_E)(\log\log\log 6d_E). \tag{13}$$

Remarques

1) Lorsque $n_E = 1$, i.e. $E = K = \mathbf{Q}$, on convient de supprimer la condition (13), qui n'a pas de sens puisque $d_E = 1$. Lorsque $n_E \geqslant 2$, on a $d_E \geqslant 3$ et il en résulte que $\log d_E$, $\log\log d_E$, et $\log\log\log 6d_E$ sont définis, et >0. (Dans [22], $\log\log\log 6d_E$ est remplacé par $\log\log\log e^{20} d_E$; c'est sans importance.)

2) On aurait pu énoncer (12) avec $x/\log x$ à la place de $\mathrm{Li}(x)$ et « $x \geqslant 2$ » à la place de « $x \geqslant 3$ ».

2.4. Forme effective du théorème de Chebotarev sous (GRH)

Nous entendrons par (GRH) *l'hypothèse de Riemann généralisée*, i.e. l'assertion que la fonction zêta d'un corps de nombres n'a pas de zéro de partie réelle $> 1/2$. Dans ce qui suit, toute formule dépendant de (GRH) porte l'indice « R ».

Cette hypothèse permet de renforcer considérablement les ths. 1 et 2. On a en effet, d'après Lagarias-Odlyzko [23] :

Théorème 4. — *Il existe une constante absolue* $c_6 > 0$ *telle que, sous* (GRH), *on ait*

$$\left|\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x)\right| \leqslant c_6 \frac{|C|}{|G|} x^{1/2}(\log d_E + n_E \log x) \tag{14$_R$}$$

pour tout $x \geqslant 2$.

Ce résultat est démontré dans [23] sous la forme un peu plus faible suivante :

$$\left|\pi_C(x) - \frac{|C|}{|G|}\mathrm{Li}(x)\right| \leqslant c_7\left\{\log d_E + \frac{|C|}{|G|} x^{1/2}(\log d_E + n_E \log x)\right\}, \tag{15$_R$}$$

valable lorsque C est une classe de conjugaison. En fait, le terme parasite $c_7 \log d_E$ peut être supprimé de cette formule. En effet, si l'on examine la démonstration de [23], on voit que ce terme provient de la majoration du bas de la p. 424 :

$$\sum_{p \text{ ram.}} \log \mathrm{N}p \leqslant \log d_L \quad (\text{où } L = E), \tag{16}$$

autrement dit :

$$\sum_{v \in V(E/K)} \log \mathrm{N}v \leqslant \log d_E. \tag{17}$$

Or, d'après la prop. 5 du n° 1.3, on peut remplacer (16) et (17) par :

$$\sum_{v \in V(E/K)} \log \mathrm{N}v \leqslant \frac{2}{|G|} \log d_E. \tag{18}$$

Ce changement a pour effet, dans les formules (3.18), (7.4) et (9.1) de [23], de remplacer $(\log x)(\log d_L)$ par $\frac{1}{|G|}(\log x)(\log d_L)$. On en déduit (15_R) avec $\log d_E$ remplacé par $\frac{1}{|G|}\log d_E$, et ce terme peut alors être absorbé par le terme $\frac{|C|}{|G|}x^{1/2}\log d_E$. Cela établit (14_R) dans le cas où C est une classe de conjugaison; le cas général s'en déduit par additivité.

Remarques

1) Bien entendu, pour prouver (14_R), il n'est pas nécessaire de supposer que (GRH) soit vraie : il suffit (et il faut...) que la fonction zêta *du corps* E *considéré* n'ait pas de zéro de partie réelle $>1/2$. Le même genre de remarque s'applique aux autres énoncés démontrés par la suite sous (GRH).

2) D'après J. Oesterlé (cf. [30]) la constante c_6 peut être prise égale à 2, et l'on peut l'abaisser à $1/3$ si l'on suppose $x \geqslant c_8$, avec c_8 assez grand. Dans le cas particulier $E = K = \mathbf{Q}$, $C = G = \{1\}$, où $\pi_C(x)$ est la fonction standard $\pi(x) = |\{p; p \leqslant x\}|$, on trouvera des résultats encore plus précis dans Schoenfeld [36].

3) Il peut être utile d'écrire le terme d'erreur de (14_R) sous une forme qui ne fasse intervenir que la ramification de E/K. Comme au § 1, notons P(E/K) l'ensemble des nombres premiers p tels que E/K soit ramifiée en au moins une place de K divisant p. D'après les formules (3) et (6) du n° 1.3, on a

$$\log d_E \leqslant n \log d_K + n_E \log n + n_E \sum_{p \in P(E/K)} \log p. \tag{19}$$

En portant dans (14_R), cela donne :

$$\left|\pi_C(x) - \frac{|C|}{|G|}\operatorname{Li}(x)\right| \leqslant c_6 |C| n_K x^{1/2}\left\{\log x + \log n + \frac{1}{n_K}\log d_K + \sum_{p \in P(E/K)} \log p\right\}. \tag{20_R}$$

2.5. Non-nullité de $\pi_C(x)$, sous (GRH)

Théorème 5. — Il existe une constante absolue $c_9 > 0$ telle que, sous (GRH), *on ait*

$$\pi_C(x) \geqslant 1 \quad \textit{si } C \neq \emptyset \tag{21_R}$$

pour tout $x \geqslant 2$ tel que

$$x \geqslant c_9 (\log d_E)^2. \tag{22_R}$$

Ce théorème est énoncé dans [23], qui en donne une esquisse de démonstration. D'après J. Oesterlé [30], on peut prendre $c_9 = 70$.

Remarques

1) L'application directe du th. 4 donnerait un résultat un peu moins fort : on serait conduit à remplacer (22_R) par l'inégalité plus restrictive

$$x \geqslant c_{10} (\log d_E)^2 (\log\log d_E)^4. \tag{23_R}$$

Ce léger affaiblissement n'aurait pas grande importance pour la suite.

2) On peut se demander si l'exposant 2 dans (22_R) est optimum. Peut-être est-il possible de le remplacer par $1+\varepsilon$, pour tout $\varepsilon>0$? Dans le cas où $K=\mathbf{Q}$, $E=\mathbf{Q}(\sqrt[m]{1})$, la question est équivalente à la suivante, déjà posée par S. Chowla [4] : est-il vrai que le plus petit nombre premier dans une progression arithmétique de raison m est $O(m^{1+\varepsilon})$?

3) Le th. (1.1) de [22] donne une condition, indépendante de (GRH), qui permet d'affirmer que $\pi_C(x)\geqslant 1$ si $C\neq\emptyset$; cette condition est :

$$x\geqslant 2(d_E)^{c_{11}}, \tag{24}$$

où c_{11} est une constante absolue. Malheureusement, (24) est trop restrictive pour les applications que nous avons en vue.

Supposons maintenant que $K=\mathbf{Q}$. Identifions $\Sigma_{\mathbf{Q}}$ à l'ensemble des nombres premiers, et notons σ_p la substitution de Frobenius de p. On a alors :

Théorème 6. — Soient E *une extension galoisienne de* $\mathbf{Q}$ *de degré fini n, et* S *un ensemble fini de nombres premiers tel que* $E/\mathbf{Q}$ *soit non ramifiée en dehors de* S. *Supposons* (GRH) *vérifiée. Pour toute classe de conjugaison* C *de* $G=\mathrm{Gal}(E/\mathbf{Q})$, *il existe un nombre premier* $p\notin S$, *tel que* $\sigma_p\in C$ *et que*

$$p\leqslant c_{12}n^2(\log n+\sum_{q\in S}\log q)^2, \tag{25$_R$}$$

où c_{12} *est une constante absolue.*

(La démonstration montrera que l'on peut prendre $c_{12}=4c_9$, donc $c_{12}=280$ d'après [30].)

Cet énoncé se déduit du th. 5 de la manière suivante :

Soit $P=P(E)$ l'ensemble des $p\in\Sigma_{\mathbf{Q}}$ en lesquels E est ramifiée. On a $P\subset S$ par hypothèse. Distinguons deux cas :

(a) $P=S$.

Le th. 5 montre qu'il existe $p\notin S$ tel que $\sigma_p\in C$ et

$$p\leqslant c_9(\log d_E)^2.$$

Or, d'après la prop. 6 du n° 1.4, on a

$$\log d_E\leqslant n(\log n+\sum_{q\in S}\log q).$$

D'où :

$$p\leqslant c_9n^2(\log n+\sum_{q\in S}\log q)^2,$$

ce qui prouve (25_R) avec c_{12} remplacé par c_9.

(b) $P\neq S$.

Soit D le produit des nombres premiers q appartenant à $S-P$, et soit F l'unique corps quadratique tel que $d_F=D$ si D est impair, et $d_F=2D$ si D est pair; on a

$F=\mathbf{Q}(\sqrt{\pm D})$ dans le premier cas et $F=\mathbf{Q}(\sqrt{\pm D/2})$ dans le second, le signe $\pm$ étant choisi tel que $\pm D \equiv 1 \pmod 4$ et $\pm D/2 \equiv 3 \pmod 4$ respectivement. Comme E est non ramifié en les facteurs premiers de d_F, les corps E et F sont linéairement disjoints. Leur composé $E'=E.F$ est galoisien, de groupe de Galois $G'=G\times\{\pm 1\}$. Comme d_E et d_F sont premiers entre eux, on a

$$d_{E'}=(d_F)^n(d_E)^2. \tag{26}$$

En particulier, P(E') est égal à S; l'extension $E'/\mathbf{Q}$ est ramifiée en tous les nombres premiers q appartenant à S. Le th. 5, appliqué à $E'/\mathbf{Q}$ et à $C\times\{\pm 1\}$, montre alors qu'il existe $p\notin S$ avec $\sigma_p\in C$ et

$$p \leqslant c_9(\log d_{E'})^2. \tag{27_R}$$

D'après (26), on a

$$\log d_{E'}=n\log d_F+2\log d_E,$$

d'où, en appliquant la prop. 6 du n° 1.4 à E :

$$\log d_{E'} \leqslant n\log d_F+2n(\log n+\sum_{q\in P}\log q).$$

Comme d'autre part $d_F \leqslant D^2$, on a

$$n\log d_F \leqslant 2n\log D \leqslant 2n\sum_{q\in S-P}\log q.$$

On en déduit

$$\log d_{E'} \leqslant 2n(\log n+\sum_{q\in S}\log q),$$

et en portant dans (27_R) on obtient bien (25_R), avec $c_{12}=4c_9$.

2.6. Variantes : les fonctions $\pi_\varphi(x)$ et $\tilde{\pi}_\varphi(x)$

(Les résultats de ce numéro et du suivant ne seront utilisés qu'au § 5.)

Les $\pi_\varphi(x)$

Revenons aux notations du n° 2.1. Soit φ une *fonction centrale* (i.e. invariante par conjugaison) sur le groupe de Galois G. Si $x\geqslant 2$, nous poserons

$$\pi_\varphi(x)=\sum_{Nv\leqslant x}\varphi(\sigma_v), \tag{28}$$

la sommation étant étendue aux $v\in\Sigma_K-V(E/K)$ avec $Nv\leqslant x$, et σ_v désignant la substitution de Frobenius de v.

Soient $C_1, \ldots, C_h$ les différentes classes de conjugaison de G, et $\lambda_1, \ldots, \lambda_h$ les valeurs prises par φ sur ces classes. On a

$$\pi_\varphi(x)=\sum_{1\leqslant i\leqslant h}\lambda_i\pi_{C_i}(x). \tag{29}$$

Ainsi, tout résultat sur les $\pi_{C_i}(x)$ en entraîne un pour les $\pi_\varphi(x)$. Par exemple, (9) donne :

$$\pi_\varphi(x) = m(\varphi)x/\log x + o(x/\log x) \quad \text{pour } x \to \infty, \tag{30}$$

où

$$m(\varphi) = \frac{1}{|G|}\sum_{s\in G}\varphi(s) = \sum_{1\leqslant i\leqslant h}\lambda_i|C_i|/|G|. \tag{31}$$

De même, le th. 3 entraîne

$$|\pi_\varphi(x)| \leqslant c_4 m(|\varphi|)\,\mathrm{Li}(x) \tag{32}$$

pour tout $x \geqslant 3$ satisfaisant à (13), et le th. 4 entraîne sous (GRH) :

$$|\pi_\varphi(x) - m(\varphi)\,\mathrm{Li}(x)| \leqslant c_6 m(|\varphi|)x^{1/2}(\log d_E + n_E \log x). \tag{33$_R$}$$

Les $\widetilde{\pi}_\varphi(x)$

Pour définir $\widetilde{\pi}_\varphi(x)$, on a besoin d'étendre la définition de σ_v au cas où v est *ramifiée* dans l'extension E/K. Cela se fait de la manière suivante (cf. [38], II) : on choisit une place w de E divisant v, et l'on définit σ_v comme le *générateur canonique* du groupe D_w/I_w où D_w (resp. I_w) est le groupe de décomposition (resp. d'inertie) de w dans G. Si $m \in \mathbf{Z}$, on *définit* $\varphi(\sigma_v^m)$ par la formule (cf. Artin [1]) :

$$\varphi(\sigma_v^m) = \frac{1}{|I_w|}\sum_{s\to\sigma_v^m}\varphi(s), \tag{34}$$

la somme étant étendue à tous les $s \in D_w$ dont l'image dans D_w/I_w est égale à la m-ième puissance de σ_v (du fait que φ est centrale, cette expression ne dépend pas du choix de w) ; la notation est justifiée par le fait que, lorsque v est non ramifiée dans E/K, $\varphi(\sigma_v^m)$ est simplement la valeur de φ sur la classe de conjugaison de σ_v^m.

Avec ces notations, la définition de $\widetilde{\pi}_\varphi(x)$ est :

$$\widetilde{\pi}_\varphi(x) = \sum_{Nv^m\leqslant x}\frac{1}{m}\varphi(\sigma_v^m), \tag{35}$$

la somme étant étendue aux couples (v, m) où v est un élément de Σ_K et m un entier $\geqslant 1$ tels que $Nv^m \leqslant x$.

[*Exemple.* — Si $\varphi = 1$, $\widetilde{\pi}_\varphi(x)$ n'est autre que la classique fonction

$$\pi_K(x) + \frac{1}{2}\pi_K(x^{1/2}) + \frac{1}{3}\pi_K(x^{1/3}) + \ldots]$$

L'intérêt des $\widetilde{\pi}_\varphi(x)$ provient des deux propriétés suivantes :

i) $\widetilde{\pi}_\varphi(x) - \pi_\varphi(x)$ est « négligeable » ;
ii) $\widetilde{\pi}_\varphi(x)$ est invariant par « induction » et « extension ».

Précisons ces deux points :

i) *Estimation de* $\widetilde{\pi}_\varphi(x)-\pi_\varphi(x)$

Posons

$$||\varphi||=\operatorname*{Sup}_{s\in G}|\varphi(s)|. \tag{36}$$

Proposition 7. — Il existe une constante absolue c_{15} *telle que*

$$|\widetilde{\pi}_\varphi(x)-\pi_\varphi(x)|\leqslant c_{15}||\varphi||\left(\frac{1}{n}\log d_E+n_K x^{1/2}\right). \tag{37}$$

On peut supposer que $||\varphi||=1$. Dans (35), les termes relatifs à $m=1$ et $v\notin V(E/K)$ donnent $\pi_\varphi(x)$. On en conclut que

$$|\widetilde{\pi}_\varphi(x)-\pi_\varphi(x)|\leqslant A+B,$$

où $A=\sum_{v\in V(E/K)} 1$ et $B=\sum_{Nv^m\leqslant x;\, m\geqslant 2} 1/m$. Comme $\log Nv\geqslant\log 2$ pour tout v, on déduit de (18) que

$$A\leqslant\sum_{v\in V(E/K)}\log Nv/\log 2\leqslant\frac{2}{n}\log d_E/\log 2,$$

i.e.
$$A\leqslant c_{13}\left(\frac{1}{n}\log d_E\right)\quad\text{avec } c_{13}=2/\log 2.$$

On a d'autre part

$$B=\frac{1}{2}\pi_K(x^{1/2})+\frac{1}{3}\pi_K(x^{1/3})+\ldots+\frac{1}{m}\pi_K(x^{1/m})$$

où m est le plus grand entier tel que $x^{1/m}\geqslant 2$. En utilisant la majoration triviale

$$\pi_K(x)\leqslant n_K x,$$

on en déduit

$$B\leqslant n_K\left(\frac{1}{2}x^{1/2}+\frac{1}{3}x^{1/3}+\ldots+\frac{1}{m}x^{1/m}\right)$$

$$\leqslant n_K\left(\frac{1}{2}x^{1/2}+x^{1/3}\log m\right)\leqslant c_{14}n_K x^{1/2}.$$

D'où (37), avec $c_{15}=\operatorname{Sup}(c_{13},c_{14})$; un calcul numérique facile montre d'ailleurs que l'on peut prendre $c_{15}=c_{13}=2/\log 2$.

Corollaire 1. — On a

$$|\widetilde{\pi}_\varphi(x)-\pi_\varphi(x)|\leqslant c_{15}m(|\varphi|)(\log d_E+n_E x^{1/2}). \tag{38}$$

Cela résulte de l'inégalité $||\varphi||\leqslant nm(|\varphi|)$.

Corollaire 2. — *Quitte à augmenter* c_4 *et* c_6, *les estimations* (30), (32) *et* (33_R) *ci-dessus restent valables lorsqu'on y remplace* $\pi_\varphi(x)$ *par* $\widetilde{\pi}_\varphi(x)$.

(Bien entendu, dans le cas de (33_R), on suppose en outre que (GRH) est vérifiée.)

Pour (30), cela résulte de (37) et de $x^{1/2} = o(x/\log x)$.

Pour (33_R), cela résulte de (38) et du fait que

$$\log d_E + n_E x^{1/2} \leqslant c_{16} x^{1/2} (\log d_E + n_E \log x)$$

avec $c_{16} = 1/\log 2$.

Pour (32), on vérifie que

$$\log d_E + n_E x^{1/2} \leqslant c_{17} x^{1/2} \log x \leqslant c_{18} \operatorname{Li}(x)$$

pour tout $x \geqslant 3$ satisfaisant à (13); cela se fait par un calcul sans difficulté, en tenant compte de l'inégalité de Minkowski

$$\log d_E \geqslant c_{19} n_E \quad \text{si } n_E > 1,$$

avec $c_{19} > 0$ (par exemple $c_{19} = \frac{1}{2} \log 3$).

Remarque. — Dans la suite, on supposera les constantes c_4 et c_6 choisies telles que (32) et (33_R) soient valables aussi bien pour $\widetilde{\pi}_\varphi(x)$ que pour $\pi_\varphi(x)$.

ii) *Propriétés d'invariance des fonctions* $\widetilde{\pi}_\varphi(x)$

Ces propriétés se déduisent des propriétés analogues pour les fonctions L d'Artin. Soient en effet χ un caractère de G et $L(s, \chi)$ la série L attachée à χ et à l'extension E/K, cf. [1]. Le développement en série de Dirichlet du logarithme de $L(s, \chi)$ est ([1], p. 296) :

$$\log L(s, \chi) = \sum_{v, m} \chi(\sigma_v^m) N v^{-ms}/m, \tag{39}$$

où v parcourt Σ_K et m les entiers $\geqslant 1$. (Précisons qu'il s'agit de la branche du logarithme dans le demi-plan $\operatorname{Re}(s) > 1$ qui tend vers 0 quand $s \to \infty$.)

Si l'on écrit ce développement sous la forme

$$\log L(s, \chi) = \sum_{n=1}^{\infty} a_n(\chi) n^{-s}, \tag{40}$$

on voit que

$$\widetilde{\pi}_\chi(x) = \sum_{n \leqslant x} a_n(\chi); \tag{41}$$

autrement dit, $\widetilde{\pi}_\chi(x)$ est la *fonction sommatoire* des coefficients de $\log L(s, \chi)$. Toute identité entre fonctions L donne une identité entre les $\widetilde{\pi}$ correspondantes. En particulier :

Proposition 8. — (a) *Soient* H *un sous-groupe de* G, φ_H *une fonction centrale sur* H, *et* $\varphi_G = \operatorname{Ind}_H^G \varphi_H$ *la fonction centrale sur* G *déduite de* φ_H *par induction. On a*

$$\widetilde{\pi}_{\varphi_G}(x) = \widetilde{\pi}_{\varphi_H}(x) \quad \textit{pour tout } x \geqslant 2. \tag{42}$$

(b) *Soient* N *un sous-groupe distingué de* G, $\varphi_{G/N}$ *une fonction centrale sur* G/N *et* φ *la fonction centrale sur* G *obtenue en composant* $\varphi_{G/N}$ *avec* $G \to G/N$. *On a*

$$\tilde{\pi}_{\varphi_G}(x) = \tilde{\pi}_{\varphi_{G/N}}(x) \quad \textit{pour tout } x \geqslant 2. \tag{43}$$

Par linéarité, il suffit de prouver (a) lorsque φ_H, donc aussi φ_G, est un *caractère*; dans ce cas, (42) résulte de (41) et du fait bien connu ([1], p. 297) que $L(s, \varphi_G) = L(s, \varphi_H)$. De même, (b) résulte de l'égalité $L(s, \varphi_G) = L(s, \varphi_{G/N})$.

Remarque

En combinant les prop. 7 et 8, on voit que les fonctions π_φ sont « presque » invariantes par induction et extension.

2.7. La propriété (R_k)

Soit C une partie de G stable par conjugaison, et soit k un nombre >0. Nous dirons que C *satisfait à la propriété* (R_k) si :

(R_k) — *Pour tout* $s \in C$, *il existe un sous-groupe* H *de* G *contenant* s, *et un sous-groupe distingué* U *de* H *tels que* :

(a) $|U| \geqslant k$;

(b) *tout élément de la forme* us, *avec* $u \in U$, *est conjugué de* s *dans* H.

Exemples

1) Supposons que $G = \mathbf{GL}_r(\mathbf{F}_q)$, et que tous les éléments de C soient *réguliers* et *déployés*, autrement dit possèdent r valeurs propres distinctes dans $\mathbf{F}_q$. Tout $s \in C$ peut alors se mettre sous forme diagonale, et l'on peut prendre pour H (resp. U) le groupe trigonal (resp. trigonal strict) supérieur; on en conclut que C satisfait à (R_k), avec $k = q^{r(r-1)/2}$.

2) Supposons que C satisfasse à la condition suivante :

(R'_k) — *Pour tout* $s \in C$, *il existe un sous-groupe abélien* A *de* G *normalisé par* s *tel que le groupe des éléments de la forme* $a^{-1}sas^{-1}$, *où* a *parcourt* A, *soit d'ordre* $\geqslant k$.

Alors C satisfait à (R_k). En effet, si s et A sont comme ci-dessus, on prend pour H le groupe engendré par s et A, et pour U le groupe des éléments de la forme $a^{-1}sas^{-1}$, avec $a \in A$. Il est clair que les conditions (a) et (b) de (R_k) sont satisfaites.

La propriété (R_k) permet de « *gagner un facteur* k » dans les th. 3 et 4. De façon plus précise :

Théorème 7. — *Supposons que* C *satisfasse à* (R_k). *Alors* :

(i) *Pour tout* $x \geqslant 3$ *tel que*

$$\log x \geqslant \frac{1}{k} c_5 (\log d_E)(\log\log d_E)(\log\log\log 6 d_E) \tag{44}$$

on a

$$\pi_C(x) \leqslant c_4 \frac{|C|}{|G|} \mathrm{Li}(x), \tag{45}$$

où c_4 et c_5 sont les constantes absolues introduites plus haut (cf. th. 3 et Remarque suivant le cor. 2 à la prop. 7).

(ii) *Sous* (GRH), *on a, pour tout* $x \geqslant 2$,

$$\left| \pi_C(x) - \frac{|C|}{|G|} \mathrm{Li}(x) \right| \leqslant \frac{1}{k} c_{21} \frac{|C|}{|G|} x^{1/2} (\log d_E + n_E \log x), \tag{46$_R$}$$

où c_{21} est une constante absolue.

(Noter la présence du facteur $1/k$ dans (44) et (46$_R$).)

Par additivité, il suffit de prouver ce théorème lorsque C est la classe de conjugaison d'un élément s. Choisissons alors H et U satisfaisant aux conditions (a) et (b) de (R_k). Notons φ_G la fonction caractéristique de la classe C; on a

$$\varphi_G(g) = \begin{cases} 1 & \text{si } g \in C, \text{ i.e. si } g \text{ est conjugué à } s \\ 0 & \text{sinon.} \end{cases}$$

Soit C_H la classe de conjugaison de s dans H. Posons

$$\lambda = |C|\,|C_H|^{-1}|H|\,|G|^{-1},$$

et soit φ_H la fonction sur H qui vaut λ sur C_H et o ailleurs. On vérifie facilement que

$$\varphi_G = \mathrm{Ind}_H^G \varphi_H.$$

Soit de même $C_{H/U}$ la classe de conjugaison dans H/U de l'image de s, et soit $\varphi_{H/U}$ la fonction sur H/U qui vaut λ sur $C_{H/U}$ et o ailleurs. D'après la partie (b) de (R_k), C_H est l'image réciproque de $C_{H/U}$ par la projection $H \to H/U$; il en résulte que φ_H est la composée de $\varphi_{H/U}$ et de $H \to H/U$. En appliquant la prop. 8, on obtient alors

$$\tilde{\pi}_{\varphi_G}(x) = \tilde{\pi}_{\varphi_H}(x) = \tilde{\pi}_{\varphi_{H/U}}(x) \quad \text{pour tout } x \geqslant 2. \tag{47}$$

Notons E′ et K′ les sous-corps de E fixés par U et H respectivement. L'extension E′/K′ est galoisienne de groupe de Galois H/U. De plus, comme $[E : E'] = |U| \geqslant k$, il résulte de la formule (3) du n° 1.3 que l'on a

$$\log d_{E'} \leqslant \frac{1}{k} \log d_E. \tag{48}$$

La condition

$$\log x \geqslant \frac{1}{k} c_5 (\log d_E)(\log\log d_E)(\log\log\log 6 d_E) \tag{44}$$

entraîne donc

$$\log x \geqslant c_5 (\log d_{E'})(\log\log d_{E'})(\log\log\log 6 d_{E'}); \tag{49}$$

en appliquant le cor. 2 à la prop. 7 à l'extension E′/K′, on en déduit

$$\widetilde{\pi}_{\varphi_{H/U}}(x) \leqslant c_4 m(\varphi_{H/U})\,\mathrm{Li}(x). \tag{50}$$

Mais il est clair que $m(\varphi_{H/U}) = m(\varphi_H) = m(\varphi_G) = |C|/|G|$. On peut donc récrire (50) sous la forme

$$\widetilde{\pi}_{\varphi_{H/U}}(x) \leqslant c_4 \frac{|C|}{|G|}\,\mathrm{Li}(x). \tag{51}$$

Comme $\pi_C(x) \leqslant \widetilde{\pi}_{\varphi_G}(x) = \widetilde{\pi}_{\varphi_{H/U}}(x)$, ceci démontre (45).

Supposons maintenant (GRH) satisfaite. En appliquant le cor. 2 à la prop. 7 à l'extension E′/K′, et tenant compte de (47) et (48), on obtient

$$|\widetilde{\pi}_{\varphi_G}(x) - \frac{|C|}{|G|}\,\mathrm{Li}(x)| \leqslant \frac{1}{k} c_6 \frac{|C|}{|G|} x^{1/2}(\log d_E + n_E \log x). \tag{52$_R$}$$

D'autre part, la prop. 7 montre que

$$|\pi_C(x) - \widetilde{\pi}_{\varphi_G}(x)| \leqslant c_{15}\left(\frac{1}{n}\log d_E + n_K x^{1/2}\right).$$

Pour obtenir (46$_R$), il suffit donc de prouver l'existence d'une constante absolue c_{20} telle que

$$\frac{1}{n}\log d_E + n_K x^{1/2} \leqslant \frac{1}{k} c_{20} \frac{|C|}{|G|} x^{1/2}(\log d_E + n_E \log x) \tag{53}$$

pour tout $x \geqslant 2$. Or c'est immédiat : on peut prendre par exemple $c_{20} = 1/\log 2$, comme on le voit en remarquant que $n_E/n_K = n$, et que $|C| \geqslant |U| \geqslant k$.

§ 3. Réduction mod ℓ^n des variétés ℓ-adiques

A partir de maintenant, et jusqu'au § 6 inclus, la lettre ℓ désigne un nombre premier fixé.

3.1. La notion de M-dimension

Soit N un entier $\geqslant 0$. Soit $X=(\mathbf{Z}_\ell)^N$ le produit de N copies de $\mathbf{Z}_\ell$; c'est une variété analytique ℓ-adique de dimension N (cf. [2], [39]). Si n est un entier $\geqslant 0$, on pose

$$X_n = X/\ell^n X = \mathbf{Z}/\ell^n\mathbf{Z}\times\ldots\times\mathbf{Z}/\ell^n\mathbf{Z} \text{ (N facteurs)};$$

l'espace compact X est limite projective des ensembles finis X_n.

Soit Y une partie fermée de X. Notons Y_n l'image de Y dans X_n; c'est la « réduction de Y mod ℓ^n ». On a

$$Y = \varprojlim Y_n \quad \text{(puisque Y est fermée)}$$

et

$$|Y_n| \leqslant |X_n| = \ell^{nN}.$$

Soit d un nombre réel $\geqslant 0$. Nous dirons que Y *est de* M-*dimension* $\leqslant d$ (ce que nous écrirons $\dim_M Y \leqslant d$) *si*

$$|Y_n| = O(\ell^{nd}) \quad \textit{pour } n\to\infty. \tag{54}$$

Ainsi, un point est de M-dimension $\leqslant 0$, et tout sous-espace de X est de M-dimension $\leqslant N$.

Cette définition peut aussi se présenter en termes de *mesures de* ε-*voisinages*, à la Minkowski (d'où l'emploi de la lettre « M ») :

Munissons X de la *distance* $||x-y|| = 1/\ell^n$, où n est le plus grand entier $\geqslant 0$ tel que $x\equiv y \pmod{\ell^n}$. Les points de X à distance $\leqslant 1/\ell^n$ de Y forment une partie ouverte compacte $Y(n)$ de X (c'est l'image réciproque de Y_n par la projection $X\to X_n$). Si $\mu_X = dx_1\ldots dx_N$ désigne la mesure de Haar de X, normalisée de telle sorte que sa masse totale soit 1, on a

$$\mu_X(Y(n)) = |Y_n|/|X_n| = \ell^{-nN}|Y_n|. \tag{55}$$

La propriété (54) revient donc à dire que

$$\mu_X(Y(n)) = O(\ell^{n(d-N)}) \quad \text{pour } n\to\infty, \tag{56}$$

ou encore que *la mesure d'un* ε-*voisinage de* Y *est* $O(\varepsilon^{N-d})$ *quand* $\varepsilon\to 0$.

Proposition 9. — *Soient* N' *un entier* $\geqslant 0$, $X'=(\mathbf{Z}_\ell)^{N'}$ *et*

$$\varphi : X' \to X$$

une application analytique ℓ*-adique de* X' *dans* X (cf. [2], § 4). *Soient* Y' *une partie fermée de* X' *et* Y *son image par* φ. *Si* $\dim_M Y' \leqslant d$, *on a* $\dim_M Y \leqslant d$.

Puisque φ est analytique, φ est Lipschitzienne. Il existe donc un entier $m \geqslant 0$ tel que

$$||\varphi(x)-\varphi(y)|| \leqslant \ell^m ||x-y|| \quad \text{pour } x, y \in X'.$$

Si n est un entier $\geqslant 0$, on a

$$x \equiv y \pmod{\ell^{n+m}} \Rightarrow \varphi(x) \equiv \varphi(y) \pmod{\ell^n}.$$

L'application φ définit donc par passage au quotient une application $\varphi_n : X'_{n+m} \to X_n$, et l'on a $Y_n = \varphi_n(Y'_{n+m})$, d'où

$$|Y_n| \leqslant |Y'_{n+m}| = O(\ell^{(n+m)d}) = \ell^{md} O(\ell^{nd}) = O(\ell^{nd}),$$

ce qui prouve bien que $\dim_M Y \leqslant d$.

La prop. 9 montre en particulier que la notion de M-dimension est *invariante* par tout automorphisme analytique de X.

Extension aux variétés analytiques ℓ*-adiques*

Soit Ω une variété analytique ℓ-adique compacte, de dimension N en tout point, et soit Y une partie fermée de Ω. Choisissons un recouvrement ouvert (U_i) de Ω formé de « boules ℓ-adiques » de dimension N (de sorte que chaque U_i est analytiquement isomorphe à $(\mathbf{Z}_\ell)^N$). Nous dirons que Y *est de* M-*dimension* $\leqslant d$ s'il en est ainsi de tous les $Y \cap U_i$; d'après la prop. 9, cette définition est indépendante du recouvrement (U_i) choisi.

3.2. Ensembles *d*-paramétrables et sous-espaces analytiques

On suppose maintenant que d est un entier $\geqslant 0$.

Une partie Y de $X=(\mathbf{Z}_\ell)^N$ est dite *d-paramétrable* s'il existe une famille finie d'applications analytiques

$$\varphi_i : (\mathbf{Z}_\ell)^d \to X$$

telle que Y soit *réunion des images des* φ_i.

En appliquant la prop. 9 avec $Y'=X'=(\mathbf{Z}_\ell)^d$, on obtient :

Proposition 10. — *Si* Y *est d-paramétrable, on a* $\dim_M Y \leqslant d$.

(Un résultat analogue vaut dans le cas réel, cf. par exemple Federer [11], p. 274.)

Corollaire. — *Toute sous-variété analytique* (lisse) *de* X, *fermée et de dimension* $\leqslant d$ *en tout point, est de* M-*dimension* $\leqslant d$.

En effet, il est clair qu'une telle variété est d-paramétrable (c'est même une *somme disjointe de boules* de dimension $\leqslant d$, cf. [39]).

On peut se demander si l'hypothèse de lissité peut être supprimée, autrement dit si le corollaire ci-dessus reste valable pour des *sous-espaces analytiques* de X, ayant éventuellement des singularités. La réponse est affirmative :

Théorème 8. — *Tout sous-espace analytique fermé de* X, *de dimension* $\leqslant d$, *est de* M-*dimension* $\leqslant d$.

Soit Y un tel sous-espace. On va montrer par récurrence sur d que Y est *d-paramétrable*, de sorte qu'on peut lui appliquer la prop. 10. Le cas $d=0$ est trivial, Y étant réduit à un ensemble fini. Supposons $d \geqslant 1$.

Le *théorème de résolution des singularités* (Hironaka [16], p. 161) est applicable localement à Y, du fait que l'anneau local des séries convergentes à coefficients dans $\mathbf{Q}_\ell$ est *excellent* ([10]). Le passage du local au global ne présente pas de difficulté puisqu'on dispose de recouvrements arbitrairement fins par des ouverts compacts. On en conclut qu'il existe un sous-espace analytique fermé Y^s de Y, de dimension $\leqslant d-1$, et un éclatement $\theta : \tilde{Y} \to Y$, où :

a) $\tilde{Y}$ est une variété lisse compacte partout de dimension d;
b) θ est une application analytique;
c) la restriction de θ à $\tilde{Y} - \theta^{-1}(Y^s)$ est un isomorphisme de $\tilde{Y} - \theta^{-1}(Y^s)$ sur $Y - Y^s$.

Vu l'hypothèse de récurrence, Y^s est $(d-1)$-paramétrable, donc aussi d-paramétrable. D'autre part, les propriétés *a)* et *b)* entraînent que $\theta(\tilde{Y})$ est d-paramétrable. D'après *c)*, Y est réunion de Y^s et de $\theta(\tilde{Y})$; donc Y est d-paramétrable.

Remarque

Le principe de la démonstration ci-dessus (utilisation de la résolution des singularités) m'a été indiqué par Michel Raynaud; je l'en remercie vivement. Il était souhaitable d'avoir une démonstration plus élémentaire, ne serait-ce que pour pouvoir l'appliquer à des corps locaux d'égale caractéristique. Cela vient d'être fait par J. Oesterlé (à paraître), au moyen d'une généralisation des invariants $N_a(f, r)$ introduits par Robba [34] dans le cas des hypersurfaces.

La même question se pose sur $\mathbf{R}$: si K est une partie compacte d'un sous-espace analytique de dimension $\leqslant d$ de $\mathbf{R}^N$, peut-on prouver élémentairement (i.e. sans résolution des singularités) que le volume des ε-voisinages de K est $o(\varepsilon^{N-d})$ quand $\varepsilon \to 0$?

Exemple : hypersurfaces algébriques

Soit $F(T_1, \ldots, T_N)$ un polynôme non identiquement nul, à coefficients dans $\mathbf{Z}_\ell$. Prenons pour Y *l'ensemble des zéros* de F, i.e. l'ensemble des points $x=(x_1, \ldots, x_N)$

de $(\mathbf{Z}_\ell)^N$ tels que $F(x)=0$. Si n est un entier $\geqslant 0$, Y_n est la partie de $X_n=(\mathbf{Z}/\ell^n\mathbf{Z})^N$ obtenue en réduisant $Y \bmod \ell^n$; si l'on note $\widetilde{Y}_n$ l'ensemble des $x\in X_n$ tels que $F(x)\equiv 0 \pmod{\ell^n}$, on a $Y_n\subset\widetilde{Y}_n$ mais il n'y a pas égalité en général (on peut simplement dire que Y_n est l'image de $\widetilde{Y}_{n+k}$ dans $\widetilde{Y}_n$, pour k assez grand).

Le th. 8 s'applique à Y, avec $d=N-1$. D'où :

Corollaire. — *On a* $|Y_n|=O(\ell^{n(N-1)})$ *pour* $n\to\infty$.

(En fait, la méthode d'Oesterlé-Robba citée plus haut donne $|Y_n|\leqslant \deg(F)\ell^{n(N-1)}$ pour tout $n\geqslant 0$, ce qui est bien plus précis.)

L'énoncé analogue pour $|\widetilde{Y}_n|$ est inexact, comme le montrent des exemples simples. Toutefois, il n'est pas difficile de prouver que

$$|\widetilde{Y}_n|=O(\ell^{n(N-\delta)}), \quad \text{avec } \delta=1/\deg(F). \tag{57}$$

La variation de $|\widetilde{Y}_n|$ avec n a été étudiée par Igusa ([17], [18]) qui a notamment montré que *la série formelle* $\sum_{n=0}^{\infty}|\widetilde{Y}_n|\,t^n$ *est une fonction rationnelle de* t; j'ignore si un résultat analogue vaut pour les $|Y_n|$.

3.3. Compléments

(Les résultats de ce numéro ne seront pas utilisés dans la suite.)

Revenons au cas où Y est une sous-variété fermée *lisse* de $X=(\mathbf{Z}_\ell)^N$, de dimension d en tout point. D'après le cor. à la prop. 10, on a

$$|Y_n|=O(\ell^{nd}) \quad \text{pour } n\to\infty.$$

Nous allons préciser ce résultat (cf. th. 9 ci-après).

Remarquons d'abord que le plongement de Y dans X munit Y d'une *mesure canonique* μ_Y, analogue à *l'élément d'aire* du cas réel : si $I=\{i_1,\ldots,i_d\}$, avec $i_1<i_2<\ldots<i_d$, est une partie à d éléments de $[1, N]$, notons $\omega_{Y,I}$ la forme différentielle induite sur Y par $dx_{i_1}\wedge\ldots\wedge dx_{i_d}$, et notons $\mu_{Y,I}$ la mesure positive $\bmod(\omega_{Y,I})$ associée à $\omega_{Y,I}$ au sens de Bourbaki [2], § 10.1. La *mesure canonique* de Y est alors définie par

$$\mu_Y=\operatorname*{Sup}_I(\mu_{Y,I}), \tag{58}$$

où I parcourt les parties à d éléments de l'intervalle $[1, N]$.

[Autre définition de μ_Y : si $y\in Y$, l'espace tangent T_yY à Y en y est un $\mathbf{Q}_\ell$-sous-espace vectoriel de $T_yX=(\mathbf{Q}_\ell)^N$, donc possède un $\mathbf{Z}_\ell$-réseau canonique, à savoir $T_yY\cap(\mathbf{Z}_\ell)^N$. Le fibré tangent à Y est ainsi muni d'un champ localement constant de réseaux (analogue ℓ-adique d'un ds^2). La mesure μ_Y est la mesure associée à la puissance extérieure d-ième de ce champ.]

Soit maintenant

$$\text{vol}(Y) = \mu_Y(Y) \tag{59}$$

la masse totale de la mesure μ_Y.

Théorème 9. — *On a* $|Y_n| = \text{vol}(Y)\ell^{nd}$ *pour n assez grand.*

(La situation est analogue à celle du cas réel, où le volume du ε-voisinage d'une variété lisse compacte est un *polynôme en* ε, pour ε assez petit, cf. par exemple H. Weyl [49].)

Commençons par vérifier le théorème dans un certain nombre de cas :

Cas (i). — Y est la sous-variété de $(\mathbf{Z}_\ell)^N$ définie par les équations

$$x_{d+1} = \varphi_{d+1}(x_1, \ldots, x_d)$$
$$\cdots$$
$$x_N = \varphi_N(x_1, \ldots, x_d)$$

où les φ_i $(d < i \leqslant N)$ sont des séries formelles en $x_1, \ldots, x_d$ à coefficients dans $\mathbf{Z}_\ell$ tendant vers 0 (séries « restreintes »). La mesure μ_Y est alors égale à $dx_1 \ldots dx_d$ et sa masse totale est 1. On a $|Y_n| = \ell^{nd}$ pour tout $n \geqslant 0$, et le th. 9 est bien vérifié dans ce cas.

Cas (ii). — C'est le cas que l'on déduit du cas (i) par une *permutation* des coordonnées $(x_1, \ldots, x_N)$; il est clair que le th. 9 est encore vérifié.

Cas (iii$_m$), *avec m entier* $\geqslant 0$. — C'est le cas où Y est de la forme

$$Y = y + \ell^m Y_m,$$

où y est un point de $(\mathbf{Z}_\ell)^N$ et où Y_m est une sous-variété de $(\mathbf{Z}_\ell)^N$ du type (ii) ci-dessus.

La variété Y est alors contenue dans la classe de y mod ℓ^m i.e. dans une boule de rayon $1/\ell^m$. On a $\text{vol}(Y) = \ell^{-md}$, $|Y_n| = 1$ pour $n \leqslant m$ et $|Y_n| = \ell^{d(n-m)}$ si $n \geqslant m$. D'où

$$Y_n = \text{vol}(Y)\ell^{nd} \quad \text{si } n \geqslant m,$$

et le th. 9 est encore vérifié.

Pour établir le th. 9 dans le cas général, il suffit donc de démontrer le résultat suivant :

Proposition 11. — *Si m est assez grand, l'intersection de* Y *avec toute classe* mod ℓ^m *est, soit vide, soit du type* (iii$_m$) *ci-dessus.*

(En d'autres termes, Y est *somme disjointe* de sous-variétés ouvertes compactes du type (iii$_m$).)

Ce résultat est essentiellement connu, au moins dans le cas algébrique (il intervient dans les travaux de A. Néron et M. Artin, par exemple). Rappelons sa démonstration :

Quitte à décomposer Y en somme disjointe de sous-variétés ouvertes compactes, on peut supposer qu'il existe une partie I à d éléments de $[1, N]$ telle que $\mu_Y = \mu_{Y,I}$, cf. (58); après permutation des coordonnées, on peut supposer que $I = [1, d]$. Le fait

que $\mu_Y = \mu_{Y,I}$ équivaut alors à dire que, pour tout $y \in Y$, l'espace tangent $T_y Y$ est le sous-espace de $T_y X = (\mathbf{Q}_\ell)^N$ défini par un système d'équations linéaires

$$x_{d+1} = a_{d+1,1} x_1 + \ldots + a_{d+1,d} x_d$$
$$\ldots$$
$$x_N = a_{N,1} x_1 + \ldots + a_{N,d} x_d$$

dont les coefficients a_{ij} *appartiennent à* $\mathbf{Z}_\ell$. Si l'on prend y pour origine, cela signifie que, au voisinage de $y = 0$, la variété Y est définie par un système d'équations de la forme

$$x_{d+1} = a_{d+1,1} x_1 + \ldots + a_{d+1} x_d + \psi_{d+1}(x_1, \ldots, x_d)$$
$$\ldots$$
$$x_N = a_{N,1} x_1 + \ldots + a_{N,d} x_d + \psi_N(x_1, \ldots, x_d)$$

où les ψ_i sont des séries convergentes ne contenant que des termes de degrés $\geqslant 2$. Lorsque l'on fait le changement de variables $x_i = \ell^m z_i$ (de façon à se placer dans la boule de rayon $1/\ell^m$ centré en y), ces équations s'écrivent

$$z_i = \sum_j a_{i,j} z_j + \psi_{i,m}(z_1, \ldots, z_d) \qquad (d < i \leqslant N;\ 1 \leqslant j \leqslant d)$$

et l'on vérifie tout de suite que, si m est assez grand, les coefficients des $\psi_{i,m}$ *appartiennent à* $\mathbf{Z}_\ell$ *et tendent vers* 0. L'intersection de Y et de la boule de rayon $1/\ell^m$ est donc de type (iii_m). Ceci s'applique à tout point de Y. La prop. 11 en résulte par un argument de compacité.

Remarques

1) La démonstration montre en outre que, si n est assez grand, les *fibres* de l'application $Y_{n+1} \to Y_n$ sont des espaces affines sur $\mathbf{Z}/\ell\mathbf{Z}$ de dimension d; en particulier, elles ont toutes ℓ^d éléments.

2) Le nombre vol(Y) est de la forme a/ℓ^m, avec $a \in \mathbf{Z}$ et m entier $\geqslant 0$. Son image dans $\mathbf{Z}/(\ell-1)\mathbf{Z}$ par réduction mod$(\ell-1)$ *ne dépend que de la variété* ℓ*-adique* Y, et pas de son plongement dans $(\mathbf{Z}_\ell)^N$; c'est *l'invariant* de Y défini dans [39].

Le cas singulier

Supprimons l'hypothèse de lissité sur Y, i.e. supposons seulement que Y soit un *sous-espace analytique* fermé de X, de dimension $\leqslant d$, ayant éventuellement des singularités. Notons Y^{reg} l'ensemble des points en lesquels Y est lisse de dimension d. La mesure canonique μ_Y est définie sur Y^{reg}, et l'on prouve sans grande difficulté que c'est une *mesure bornée*. Cela permet de définir le volume de Y par la formule

$$\mathrm{vol}(Y) = \mu_Y(Y^{reg}). \tag{60}$$

En appliquant le th. 9 aux sous-variétés ouvertes compactes de Y^{reg}, on voit que

$$\liminf_{n \to \infty} |Y_n|/\ell^{nd} \geqslant \mathrm{vol}(Y). \tag{61}$$

En fait, on a le résultat plus précis suivant

$$\lim_{n \to \infty} |Y_n|/\ell^{nd} = \mathrm{vol}(Y); \tag{62}$$

c'est ce que vient de prouver J. Oesterlé (à paraître). Il est probable que l'on a même :

$$(6_{3?}) \qquad |Y_n| = \mathrm{vol}(Y)\ell^{nd} + O(\ell^{n\delta}) \quad \text{avec } \delta < d;$$

cela devrait pouvoir se démontrer en utilisant l' « inégalité de Lojasiewicz » ℓ-adique.

(Signalons, à titre de curiosité, que vol(Y) *est un nombre rationnel.* Cela se déduit du résultat suivant, que l'on démontre, à la Igusa, en utilisant la résolution des singularités : si α est une forme différentielle analytique de degré d sur une variété ℓ-adique lisse compacte de dimension d, la masse totale de la mesure mod(α) *est un nombre rationnel.*)

Généralisations

Les résultats de ce paragraphe restent valables lorsque l'on remplace $\mathbf{Q}_\ell$ par n'importe quel corps local à corps résiduel fini, cf. J. Oesterlé, *loc. cit.*

§ 4. Majorations de $\pi_C(x)$ dans le cas ℓ-adique

4.1. Énoncé du théorème

Soient :

K un corps de nombres algébriques, de degré fini n_K;
S une partie finie de l'ensemble Σ_K des places ultramétriques de K;
G un groupe de Lie ℓ-adique compact, de dimension $N \geqslant 1$ (pour tout ce qui concerne les groupes de Lie ℓ-adiques, voir [3], [26]);
C une partie fermée de G, stable par conjugaison;
E une extension galoisienne infinie de K, de groupe de Galois G, non ramifiée en dehors de S.

Si $v \in \Sigma_K - S$, on note σ_v la substitution de Frobenius de v relativement à l'extension E/K; c'est un élément de G, défini à conjugaison près. Comme au § 2, on note Σ_C l'ensemble des $v \in \Sigma_K - S$ tels que $\sigma_v \in C$; si $x \geqslant 2$, on note $\pi_C(x)$ le nombre des $v \in \Sigma_C$ tels que $Nv \leqslant x$. On va donner une *majoration asymptotique* de $\pi_C(x)$:

Théorème 10. — *Soit d un nombre réel tel que* $0 \leqslant d < N$. *Supposons que* $\dim_M C \leqslant d$ (au sens du n° 3.1). *Posons* $\alpha = (N-d)/N$. *Alors* :

(i) *On a*

$$\pi_C(x) = O(\mathrm{Li}(x)/\varepsilon(x)^{\alpha}) \quad \textit{pour } x \to \infty, \tag{64}$$

avec

$$\varepsilon(x) = (\log x)(\log\log x)^{-2}(\log\log\log x)^{-1}, \quad x \geqslant 16. \tag{65}$$

(ii) *Sous* (GRH), *on a*

$$\pi_C(x) = O(\mathrm{Li}(x)/\varepsilon_R(x)^{\alpha}) \quad \textit{pour } x \to \infty, \tag{66$_R$}$$

avec

$$\varepsilon_R(x) = x^{1/2}(\log x)^{-2}. \tag{67}$$

La démonstration sera donnée aux n^{os} 4.3 et 4.4 ci-après.

Corollaire 1. — *Pour tout* $\varepsilon > 0$, *on a*

$$\pi_C(x) = O(x/(\log x)^{1+\alpha-\varepsilon}) \tag{68}$$

et, sous (GRH),

$$\pi_C(x) = O(x^{1-\alpha/2+\varepsilon}). \tag{69$_R$}$$

Cela résulte du théorème, compte tenu de $\mathrm{Li}(x) \sim x/\log x$ et de

$$\varepsilon(x)^{-1} = O((\log x)^{-1+\delta}) \quad \text{pour tout } \delta > 0 \tag{70}$$

$$\varepsilon_R(x)^{-1} = O(x^{-1/2+\delta}) \quad \text{pour tout } \delta > 0. \tag{71}$$

Corollaire 2. — La série $\sum_v 1/\mathrm{N}v$, *étendue aux* $v \in \Sigma_C$, *est convergente.*

Cela résulte de (68), et de la convergence de la série de terme général $1/n(\log n)^\rho$ pour $\rho > 1$.

Remarques

1) On verra au § 5 que l'on peut, dans certains cas, renforcer le th. 10 en remplaçant l'exposant α par un exposant β un peu plus grand.

2) Les constantes cachées dans la notation « O » de (64) et (66$_R$) dépendent des données K, S, G, C, d; ce ne sont pas des constantes absolues.

Exemple. — Supposons que C soit un *sous-espace analytique* de G d'intérieur vide. D'après le th. 8, on a $\dim_M C \leqslant N-1$. On peut donc appliquer le th. 10 avec $d = N-1$ et $\alpha = 1/N$.

4.2. Préparatifs

Soit $\mathfrak{g}$ l'algèbre de Lie de G. C'est un $\mathbf{Q}_\ell$-espace vectoriel de dimension N, sur lequel G opère par la représentation adjointe. On sait (cf. par exemple [3], chap. III, § 7) que l'application logarithme

$$\log_G : G \to \mathfrak{g}$$

est un *isomorphisme local*. Comme G est compact, il existe un $\mathbf{Z}_\ell$-réseau $\mathfrak{g}(o)$ de $\mathfrak{g}$ stable par la représentation adjointe. Quitte à remplacer $\mathfrak{g}(o)$ par un multiple $\ell^r\mathfrak{g}(o)$, avec r assez grand, on peut supposer que :

a) $\mathfrak{g}(o)$ est stable par $(x, y) \mapsto \ell^{-2}[x, y]$ (donc aussi par la « loi de Hausdorff », cf. [3], *loc. cit.*);

b) il existe un sous-groupe ouvert distingué G(o) de G tel que la restriction de $\log_G$ à G(o) définisse un isomorphisme de G(o) sur $\mathfrak{g}(o)$, muni de la loi de Hausdorff.

Choisissons de tels $\mathfrak{g}(o)$ et G(o). Pour tout entier $n \geqslant o$, posons $\mathfrak{g}(n) = \ell^n\mathfrak{g}(o)$ et notons G(n) l'ensemble des $s \in G(o)$ tels que $\log_G s \in \mathfrak{g}(n)$. On vérifie tout de suite que G(n) est un sous-groupe ouvert distingué de G. Si l'on pose

$$G_n = G/G(n),$$

on a

$$|G_n| = a\ell^{nN} \quad \text{avec } a = (G : G(o)) = |G_0|. \tag{72}$$

Soit C_n l'image de C par la projection $G \to G_n$. L'hypothèse $\dim_M C \leqslant d$ se traduit par :

$$|C_n| = O(\ell^{nd}) \quad \text{pour } n \to \infty, \tag{73}$$

ou, ce qui revient au même vu (72),

$$|C_n|/|G_n| = O(1/|G_n|^{\alpha}) \quad \text{pour } n \to \infty. \tag{74}$$

Soit E_n l'ensemble des éléments de E fixés par $G(n)$. L'extension E_n/K est galoisienne, de groupe de Galois G_n. D'après la formule (19) du n° 2.4, on a

$$\log d_{E_n} \leqslant |G_n|(\log d_K + n_K \log |G_n| + \sum_{p \in S_{\mathbf{Q}}} \log p), \tag{75}$$

où $S_{\mathbf{Q}}$ désigne l'ensemble des nombres premiers p tels qu'il existe $v \in S$ divisant p. En particulier :

$$\log d_{E_n} \leqslant |G_n|(O(1) + n_K \log |G_n|) \leqslant (n_K + o(1))|G_n| \log |G_n| \tag{76}$$

pour $n \to \infty$.

Remarque. — En utilisant un théorème de Sen [37], on peut prouver :

$$\log d_{E_n} \leqslant \frac{1}{N}|G_n|(O(1) + n_K \log |G_n|) \quad \text{pour } n \to \infty, \tag{76'}$$

ce qui améliore (76) par un facteur N.

4.3. Démonstration du théorème 10 (i)

Le principe de la démonstration est celui-ci : pour x donné, on choisit un entier $n = n(x)$ convenable, et l'on majore $\pi_{C_n}(x)$ (qui est relatif à l'extension finie E_n/K de groupe de Galois G_n) grâce au th. 3 du n° 2.3. Compte tenu de l'inégalité évidente

$$\pi_C(x) \leqslant \pi_{C_n}(x), \tag{77}$$

on en déduit bien une majoration de $\pi_C(x)$.

De façon plus précise, choisissons un nombre réel $b > 0$ tel que

$$bc_5 n_K < 1, \tag{78}$$

où c_5 est la constante absolue introduite au n° 2.3. Vu (72), si x est assez grand, il existe un entier positif $n = n(x)$ et un seul tel que

$$b\ell^{-N}\varepsilon(x) < |G_n| \leqslant b\varepsilon(x), \tag{79}$$

à savoir $n = [\log(a^{-1}b\varepsilon(x))/N \log \ell]$.

Nous allons voir qu'avec ce choix de n, on a

$$\log x \geqslant c_5(\log d_{E_n})(\log\log d_{E_n})(\log\log\log 6d_{E_n}) \tag{80}$$

pourvu que x soit assez grand. En effet, on déduit de (76) et (79) que

$$\log d_{E_n} \leqslant (n_K + o(1))b\varepsilon(x) \log \varepsilon(x)$$
$$\leqslant (n_K + o(1))b(\log x)(\log\log x)^{-1}(\log\log\log x)^{-1}$$

d'où $$\log\log d_{E_n} \leqslant (1 + o(1)) \log\log x$$

et $$\log\log\log 6d_{E_n} \leqslant (1 + o(1)) \log\log\log x.$$

En multipliant ces inégalités, on obtient

$$c_5(\log d_{E_n})(\log\log d_{E_n})(\log\log\log 6d_{E_n}) \leqslant (bc_5 n_K + o(1)) \log x,$$

ce qui entraîne (80) pour x assez grand puisque $bc_5 n_K < 1$.

Ceci fait, on applique le th. 3 du n° 2.3 à l'extension E_n/K et l'on obtient

$$\pi_{C_n}(x) \leqslant c_4 |C_n| |G_n|^{-1} \mathrm{Li}(x). \tag{81}$$

Vu (74) et (79), on a $|C_n|/|G_n| = O(\varepsilon(x)^{-\alpha})$. D'où

$$\pi_{C_n}(x) = O(\mathrm{Li}(x)/\varepsilon(x)^{\alpha}), \tag{82}$$

ce qui démontre le th. 10 (i), compte tenu de (77).

Remarque. — La démonstration ci-dessus montre que le choix de la fonction $\varepsilon(x)$ est imposé par la forme de la condition (13) du th. 3. Si par exemple on pouvait remplacer (13) par

$$\log x \geqslant c_{22} \log d_E,$$

on pourrait prendre pour $\varepsilon(x)$ la fonction $(\log x)(\log\log x)^{-1}$.

4.4. Démonstration du théorème 10 (ii)

On procède de manière analogue : si x est assez grand, il existe un unique entier positif $n = n(x)$ tel que

$$\ell^{-N} \varepsilon_R(x) < |G_n| \leqslant \varepsilon_R(x). \tag{83}$$

D'après le th. 4 du n° 2.4, on a, sous (GRH),

$$\pi_{C_n}(x) \leqslant |C_n| |G_n|^{-1} \{\mathrm{Li}(x) + c_6 x^{1/2} \log d_{E_n} + c_6 [E_n : \mathbf{Q}] x^{1/2} \log x\}. \tag{84$_R$}$$

Vu (83) et (74), on a

$$|C_n| |G_n|^{-1} = O(\varepsilon_R(x)^{-\alpha}).$$

D'autre part, (83) et (76) entraînent :

$$x^{1/2} \log d_{E_n} = O(x^{1/2} \varepsilon_R(x) \log \varepsilon_R(x)) = O(x(\log x)^{-1}) = O(\mathrm{Li}(x))$$

et $$[E_n : \mathbf{Q}] x^{1/2} \log x = O(\varepsilon_R(x) x^{1/2} \log x) = O(x(\log x)^{-1}) = O(\mathrm{Li}(x)).$$

En portant ces majorations dans (84$_R$), on en déduit

$$\pi_{C_n}(x) = O(\mathrm{Li}(x)/\varepsilon_R(x)^{\alpha}), \tag{85$_R$}$$

ce qui démontre le th. 10 (ii), compte tenu de (77).

4.5. Un exemple

Lorsque C est réduit à un seul élément, le th. 10 s'applique avec $d=0$ et $\alpha=1$; sous (GRH), il implique que

$$(86_R) \qquad \pi_C(x)=O(x^{1/2}\log x) \quad \text{pour } x\to\infty.$$

Nous allons voir que cette borne n'est pas loin d'être optimale.

Prenons pour K un corps quadratique imaginaire. Supposons (afin de simplifier les notations) que ℓ se décompose dans K en deux places distinctes λ et $\bar{\lambda}$, que le nombre de classes de K soit 1, et que K ne contienne pas de racine de l'unité $\neq\pm 1$ (exemple : $K=\mathbf{Q}(\sqrt{-163})$ et $\ell=41$). Si $v\in\Sigma_K$, choisissons un générateur z_v de l'idéal $\mathfrak{p}_v$, et posons $\omega(v)=z_v/\bar{z}_v$; comme z_v est défini au signe près, $\omega(v)$ est indépendant du choix de z_v. On a $\omega(v)\in K^*$; comme la place λ définit un plongement de K dans $\mathbf{Q}_\ell$, on peut identifier $\omega(v)$ à un élément de $\mathbf{Q}_\ell^*$. On a $\omega(v)\in\mathbf{Z}_\ell^*$ si v ne divise pas ℓ, i.e. si $v\neq\lambda,\bar{\lambda}$. D'après la théorie du corps de classes, il existe une extension abélienne E/K, de groupe de Galois $G=\mathbf{Z}_\ell^*$, qui est non ramifiée en dehors de $S=\{\lambda,\bar{\lambda}\}$ et telle que, pour tout $v\in\Sigma_K-S$, la substitution de Frobenius σ_v de v soit égale à $\omega(v)$. Prenons $C=\{1\}$, de sorte que Σ_C est formé des places v de K qui sont *complètement décomposées* dans l'extension E. On a $v\in\Sigma_C$ si et seulement si $z_v=\bar{z}_v$; il est facile de voir que cela équivaut à dire que $\mathfrak{p}_v$ est un idéal premier *de degré* 2, autrement dit engendré par un nombre premier p_v qui est inerte dans $K/\mathbf{Q}$. Comme $Nv=p_v^2$, on en déduit que $\pi_C(x)$ est égal au nombre des $p\leqslant x^{1/2}$ tels que $\left(\frac{p}{K/\mathbf{Q}}\right)=-1$. D'où :

$$(87) \qquad \pi_C(x)\sim x^{1/2}/\log x \quad \text{pour } x\to\infty.$$

La majoration (86_R) est donc *optimale en ce qui concerne l'exposant de x* (mais probablement pas en ce qui concerne l'exposant de $\log x$).

Des exemples analogues existent avec $d=0$ et N arbitrairement grand. Par contre, lorsque $d>0$, je ne connais aucun cas où la majoration du th. 10 (ii) (ni celle du th. 12 (ii)) soit essentiellement optimale. Il est fort possible que l'on ait en fait

$$(88_?) \qquad \pi_C(x)=O(x^{1/2}/\log x) \quad \text{pour } x\to\infty,$$

lorsque C est un sous-espace analytique de dimension $d<N$, mais je ne vois pas comment le démontrer, même sous (GRH).

4.6. Généralisation

La démonstration du th. 10 fait intervenir de façon essentielle la « tour » d'extensions galoisiennes E_n/K définie au n° 4.2. Plus généralement, considérons une *famille d'extensions galoisiennes finies* $(E_\lambda/K)_{\lambda\in\Lambda}$; si $\lambda\in\Lambda$, soit $G_\lambda=\mathrm{Gal}(E_\lambda/K)$ et soit C_λ une

partie de G_λ stable par conjugaison; soit α un nombre réel tel que $0<\alpha\leqslant 1$. Faisons les hypothèses suivantes :

(a) *(Répartition des degrés)*. Il existe un nombre $L>0$ tel que tout intervalle de $\mathbf{R}_+$ de longueur L contienne au moins un $\log|G_\lambda|$.

(b) *(Croissance des discriminants)*. Il existe un nombre $M>0$ tel que

$$\log d_{E_\lambda} \leqslant M|G_\lambda| \log|G_\lambda| \quad \text{pour tout } \lambda\in\Lambda. \tag{89}$$

(c) *(Taille des C_λ)*. Il existe un nombre $P>0$ tel que

$$|C_\lambda|/|G_\lambda| \leqslant P/|G_\lambda|^\alpha \quad \text{pour tout } \lambda\in\Lambda. \tag{90}$$

Posons alors

$$\pi_C(x) = \operatorname{Inf} \pi_{C_\lambda}(x) \quad (x\geqslant 2), \tag{91}$$

où $\pi_{C_\lambda}(x)$ est défini comme au n° 2.1 (relativement à l'extension finie E_λ/K).

Théorème 11. — (i) *On a*

$$\pi_C(x) = O(\mathrm{Li}(x)/\varepsilon(x)^\alpha) \quad \textit{pour } x\to\infty. \tag{92}$$

(ii) *Sous* (GRH), *on a*

$$\pi_C(x) = O(\mathrm{Li}(x)/\varepsilon_R(x)^\alpha) \quad \textit{pour } x\to\infty. \tag{93_R}$$

(Les fonctions $\varepsilon(x)$ et $\varepsilon_R(x)$ sont celles définies dans l'énoncé du th. 10.)

La démonstration est essentiellement la même que celle du th. 10. Pour (i), on choisit un nombre $b>0$ tel que

$$bMc_5<1. \tag{94}$$

D'après (a), si x est assez grand, il existe un $\lambda=\lambda(x)$ tel que

$$e^{-L}b\varepsilon(x)\leqslant|G_\lambda|\leqslant b\varepsilon(x). \tag{95}$$

Comme au n° 4.3, on déduit de (95) et (89) que

$$c_5(\log d_{E_\lambda})(\log\log d_{E_\lambda})(\log\log\log 6d_{E_\lambda}) \leqslant (bMc_5+o(1))\log x,$$

d'où, grâce à (94),

$$\log x \geqslant c_5(\log d_{E_\lambda})(\log\log d_{E_\lambda})(\log\log\log 6d_{E_\lambda})$$

pour x assez grand. En appliquant le th. 3 du n° 2.3, on en déduit

$$\pi_{C_\lambda}(x) \leqslant c_4\,\mathrm{Li}(x)|C_\lambda|/|G_\lambda|;$$

compte tenu de (90) et (95), cela donne

$$\pi_{C_\lambda}(x) = O(\mathrm{Li}(x)/\varepsilon(x)^\alpha),$$

d'où (92).

Sous (GRH), on raisonne de même, en choisissant $\lambda=\lambda(x)$ de telle sorte que

$$e^{-L}\varepsilon_R(x)\leqslant|G_\lambda|\leqslant\varepsilon_R(x). \tag{96}$$

Un calcul analogue à celui du n° 4.4 montre alors que

$$x^{1/2}\log d_{E_\lambda}+[E_\lambda : \mathbf{Q}]x^{1/2}\log x = O(\mathrm{Li}(x)),$$

et en appliquant le th. 4 du n° 2.4, on en déduit

$$\pi_{C_\lambda}(x) = O(\mathrm{Li}(x)\,|\,C_\lambda\,|/|\,G_\lambda\,|) = O(\mathrm{Li}(x)/\varepsilon_R(x)^\alpha),$$

d'où (93_R).

Exemples

1) Le th. 11, appliqué aux extensions E_n/K du n° 4.2, redonne le th. 10 (noter que le « $\pi_C(x)$ » du th. 11 ne diffère du « $\pi_C(x)$ » du th. 10 que par $O(1)$).

2) Prenons pour Λ l'ensemble des nombres premiers. Supposons que $|G_\lambda|$ soit de l'ordre de grandeur de λ^N, avec $N>0$, et que E_λ soit non ramifiée en dehors des places divisant λ et de celles appartenant à un ensemble fini fixe. Les conditions (a) et (b) sont alors satisfaites : c'est immédiat pour (a), et pour (b) cela résulte de la formule (19) du n° 2.4. Ceci s'applique notamment aux extensions galoisiennes fournies par les points de division d'ordre premier d'une courbe elliptique définie sur K; nous reviendrons là-dessus au § 8.

§ 5. Majorations améliorées

5.1. Énoncé du théorème

Les notations sont les mêmes qu'aux nos 4.1 et 4.2. En particulier, $\mathfrak{g}$ désigne l'algèbre de Lie du groupe de Lie ℓ-adique G. Si $s \in G$, on note $\mathrm{Ad}(s)$ l'automorphisme de $\mathfrak{g}$ induit par l'automorphisme intérieur $\mathrm{Int}(s) : t \mapsto sts^{-1}$ de G. On pose

$$r(s) = \mathrm{rg}(\mathrm{Ad}(s) - 1) = \dim \mathrm{Im}(\mathrm{Ad}(s) - 1). \tag{97}$$

Si $Z_G(s)$ désigne le centralisateur de s dans G, et $\mathfrak{z}_G(s)$ son algèbre de Lie, on a (cf. [3], p. 234, prop. 8)

$$\mathfrak{z}_G(s) = \mathrm{Ker}(\mathrm{Ad}(s) - 1). \tag{98}$$

On en déduit

$$r(s) = N - \dim \mathfrak{z}_G(s) = \dim G/Z_G(s) = \dim \mathrm{Cl}(s), \tag{99}$$

où $\mathrm{Cl}(s)$ désigne la classe de conjugaison de s dans G; en effet, d'après [3], p. 108, prop. 14, $\mathrm{Cl}(s)$ est une sous-variété lisse compacte de G, isomorphe à l'espace homogène $G/Z_G(s)$.

Théorème 12. — *Soient* C *une partie fermée de* G, *stable par conjugaison, et* d *un nombre réel tel que* $0 \leqslant d < N$ *et* $\dim_M C \leqslant d$. *Posons*

$$r = \operatorname*{Inf}_{s \in C} r(s) \quad \text{et} \quad \beta = (N - d)/(N - r/2). \tag{100}$$

Alors :

(i) *On a*

$$\pi_C(x) = O(\mathrm{Li}(x)/\varepsilon(x)^{\beta}) \quad \text{pour } x \to \infty. \tag{101}$$

(ii) *Sous* (GRH), *on a*

$$\pi_C(x) = O(\mathrm{Li}(x)/\varepsilon_R(x)^{\beta}) \quad \text{pour } x \to \infty. \tag{102_R}$$

La démonstration sera donnée aux nos 5.3 et 5.4 ci-après.

Remarque. — Comme r est $\geqslant 0$, on a $\beta \geqslant (N - d)/N = \alpha$. Le th. 12 *contient* donc le th. 10 comme cas particulier; il *l'améliore* si $\beta > \alpha$, i.e. si $r \geqslant 1$, autrement dit *si aucune des classes de conjugaison contenues dans* C *n'est finie*. Pour qu'on ait intérêt à appliquer le th. 12, il faut notamment que C ne rencontre pas le centre de G.

Exemple. — Si C est réduit à une seule classe de conjugaison $\mathrm{Cl}(s)$, on peut prendre $d = \dim C = r(s)$ et $\beta = (N - d)/(N - d/2)$.

5.2. Préparatifs

Comme au n° 4.2, on choisit un $\mathbf{Z}_\ell$-réseau $\mathfrak{g}(0)$ de $\mathfrak{g}$ et un sous-groupe ouvert distingué $G(0)$ de G tels que

a) $\mathfrak{g}(0)$ est stable par $(x,y)\mapsto \ell^{-2}[x,y]$;

b) l'application $\log_G$ définit un isomorphisme de $G(0)$ sur $\mathfrak{g}(0)$, muni de la loi de Hausdorff

$$x\,\mathrm{H}\,y = x+y+\frac{1}{2}[x,y]+\ldots, \qquad \text{cf. [3], [26].} \tag{103}$$

On note $\exp_G$ l'isomorphisme réciproque $\mathfrak{g}(0)\to G(0)$.

Si n est un entier $\geqslant 0$, on pose

$$\mathfrak{g}(n)=\ell^n\mathfrak{g}(0), \quad G(n)=\exp_G \mathfrak{g}(n), \quad G_n=G/G(n), \tag{104}$$

et l'on note C_n l'image de C dans G_n.

Proposition 12. — Il existe un nombre $c>0$ tel que, pour tout $n\geqslant 0$, C_n jouisse de la propriété $R_{k(n)}$ du n° 2.7, avec

$$k(n)=c\ell^{nr/2}. \tag{105}$$

(Rappelons que $r=\operatorname{Inf}_{s\in C} r(s)=\operatorname{Inf}_{s\in C} \mathrm{rg}(\mathrm{Ad}(s)-1)$, cf. (100).)

On va démontrer un peu plus, à savoir que C_n jouit de la propriété $(R'_{k(n)})$ du n° 2.7. Pour cela, il suffit de construire pour tout $n\geqslant 0$ un sous-groupe abélien distingué A_n de G_n ayant la propriété suivante :

(106) *Pour tout $s\in C_n$, le groupe des éléments de la forme $a^{-1}sas^{-1}$, où a parcourt A_n, est d'ordre $\geqslant c\ell^{nr/2}$, avec $c>0$ ne dépendant ni de s ni de n.*

Définition de A_n

Soit $m=[n/2]$ la partie entière de $n/2$. Nous prendrons pour A_n *l'image de* $G(m+1)$ *dans* G_n par la projection $G\to G_n$. On a $A_n=\{1\}$ si $n=0$ ou 1. Si $n\geqslant 2$, A_n est isomorphe à $G(m+1)/G(n)$, lui-même isomorphe à $\mathfrak{g}(m+1)/\mathfrak{g}(n)$ muni de la loi de Hausdorff. Mais la majoration ℓ-adique des coefficients de la série de Hausdorff ([3], p. 67) montre que, si $x,y\in\mathfrak{g}(a)$ pour un entier $a\geqslant 0$, on a

$$x\,\mathrm{H}\,y\equiv x+y \pmod{\mathfrak{g}(2a)}.$$

Comme $2(m+1)\geqslant n$, il en résulte que la loi de Hausdorff sur $A_n=\mathfrak{g}(m+1)/\mathfrak{g}(n)$ est simplement *l'addition*; on obtient ainsi un isomorphisme canonique

$$A_n\simeq \ell^{m+1}\mathfrak{g}(0)/\ell^n\mathfrak{g}(0)=\mathfrak{g}(0)/\ell^{n-m-1}\mathfrak{g}(0). \tag{107}$$

En particulier, A_n est *abélien*. Il est clair qu'il est distingué dans G_n.

Vérification de la propriété (106)

Soit $s \in C_n$; notons également s un représentant de cet élément dans C. Comme

$$\log_G \circ \mathrm{Int}(s) = \mathrm{Ad}(s) \circ \log_G,$$

l'isomorphisme (107) transforme l'automorphisme $\mathrm{Int}(s)$ de A_n en l'automorphisme $\mathrm{Ad}(s)$ de $g(o)/\ell^{n-m-1}g(o)$. Le groupe $A_{n,s}$ des éléments $a^{-1}sas^{-1}$ $(a \in A_n)$ est donc isomorphe au sous-groupe de $g(o)/\ell^{n-m-1}g(o)$ formé par les $\mathrm{Ad}(s)a - a$, où a parcourt $g(o)/\ell^{n-m-1}g(o)$. Si l'on note $L(s)$ l'image de l'endomorphisme $\mathrm{Ad}(s) - 1$ de $g(o)$, on voit ainsi que $A_{n,s}$ *est isomorphe à* $L(s)/(L(s) \cap \ell^{n-m-1}g(o))$. Il nous faut prouver

(108) $$|A_{n,s}| \geqslant c\ell^{nr/2}, \quad \text{avec } c > o.$$

Or on a le lemme suivant :

Lemme 1. — Soit Ω *un ensemble compact d'endomorphismes d'un* $\mathbf{Z}_\ell$*-module* L *libre de rang* N, *et soit* $r = \inf_{\omega \in \Omega} \mathrm{rg}(\omega)$. *Il existe un nombre* $c(\Omega) > o$ *tel que*

$$|\mathrm{Im}(\omega)/(\mathrm{Im}(\omega) \cap \ell^q L)| \geqslant c(\Omega)\ell^{qr},$$

pour tout $\omega \in \Omega$ *et tout entier* $q \geqslant o$.

Soit $\omega \in \Omega$. Comme $\mathrm{rg}(\omega) \geqslant r$, les r premiers *facteurs invariants* de ω sont $\neq o$. On peut les écrire sous la forme

$$\ell^{m_1(\omega)}, \ldots, \ell^{m_r(\omega)}, \quad \text{avec} \quad o \leqslant m_1(\omega) \leqslant \ldots \leqslant m_r(\omega).$$

Il existe une $\mathbf{Z}_\ell$-base $(e_i(\omega))_{1 \leqslant i \leqslant N}$ de L telle que $\mathrm{Im}(\omega)$ soit engendré par les $\ell^{m_i(\omega)}e_i(\omega)$, $1 \leqslant i \leqslant r$, et par des multiples (éventuellement nuls) des $e_j(\omega)$, $r < j \leqslant N$. Dans le quotient

$$\mathrm{Im}(\omega)/(\mathrm{Im}(\omega) \cap \ell^q L),$$

les $e_i(\omega)$, $1 \leqslant i \leqslant r$, engendrent un sous-groupe qui est somme directe de groupes cycliques d'ordres $\ell^{\mathrm{Sup}(0, q - m_i(\omega))}$. Il en résulte que

$$|\mathrm{Im}(\omega)/(\mathrm{Im}(\omega) \cap \ell^q L)| \geqslant \prod_{i=1}^{i=r} \ell^{q - m_i(\omega)} = c(\omega)\ell^{qr},$$

où $c(\omega) = \prod_{i=1}^{i=r} \ell^{-m_i(\omega)}$. Mais les $m_i(\omega)$ sont des fonctions *localement constantes* de ω; cela se voit par récurrence sur i, en utilisant le fait que $\ell^{m_1(\omega) + \ldots + m_i(\omega)}$ est la plus grande puissance de ℓ qui divise la puissance extérieure i-ième de ω. Comme Ω est compact, il en résulte que les $m_i(\omega)$ sont bornés et la borne inférieure des $c(\omega)$ est $> o$. D'où le lemme.

On applique le lemme 1 au module $L = g(o)$, en prenant pour Ω l'ensemble des $\mathrm{Ad}(s) - 1$, pour $s \in C$. On en déduit

$$|A_{n,s}| \geqslant c(\Omega)\ell^{(n-m-1)r},$$

et comme $n - m \geqslant n/2$, cela donne bien (108) avec $c = \ell^{-r}c(\Omega)$. Cela achève la démonstration de la prop. 12.

5.3. Démonstration du théorème 12 (i)

On procède comme pour le th. 10 (i), à cela près que l'on utilise le th. 7 à la place du th. 3 :

Soit b un nombre réel >0 tel que

(109) $\qquad bc_5 n_K(1-r/2N)^{-2}<1.$

Vu (72) et (105), on a

(110) $\qquad |G_n|/k(n)=ac^{-1}\ell^{r(N-r/2)}.$

Il résulte de (110) que, si x est assez grand, il existe un unique entier positif $n=n(x)$ tel que

(111) $\qquad b\ell^{-(N-r/2)}\varepsilon(x)<|G_n|/k(n)\leqslant b\varepsilon(x).$

On en déduit

(112) $\qquad |G_n|=O(\varepsilon(x)^\gamma) \quad \text{et} \quad |G_n|^{-1}=O(\varepsilon(x)^{-\gamma}),$

avec

(113) $\qquad \gamma=1/(1-r/2N).$

De (112) on tire

(114) $\qquad \log|G_n|\leqslant(\gamma+o(1))\log\log x.$

D'où, d'après (76) :

(115) $\qquad \log d_{E_n}\leqslant(\gamma n_K+o(1))|G_n|\log\log x,$

et en particulier

(116) $\qquad \log d_{E_n}=O(\varepsilon(x)^\gamma\log\log x),$

d'où

(117) $\qquad \log\log d_{E_n}\leqslant(\gamma+o(1))\log\log x$

et

(118) $\qquad \log\log\log 6d_{E_n}\leqslant(1+o(1))\log\log\log x.$

En combinant (111), (115), (117) et (118), on obtient

$$\frac{1}{k(n)}(\log d_{E_n})(\log\log d_{E_n})(\log\log\log 6d_{E_n})\leqslant(b\gamma^2 n_K+o(1))\log x.$$

Vu (109), ceci entraîne

$$\frac{1}{k(n)}c_5(\log d_{E_n})(\log\log d_{E_n})(\log\log\log 6d_{E_n})\leqslant\log x$$

pour x assez grand. En appliquant la prop. 12 et le th. 7 (i), on en déduit

$$\pi_{C_n}(x) \leqslant c_4 |C_n| \, |G_n|^{-1} \operatorname{Li}(x). \tag{119}$$

D'après (74) et (112), on a

$$|C_n| \, |G_n|^{-1} = O(|G_n|^{-\alpha}) = O(\varepsilon(x)^{-\alpha\gamma}) = O(\varepsilon(x)^{-\beta}).$$

L'inégalité (119) entraîne donc

$$\pi_{C_n}(x) = O(\operatorname{Li}(x)/\varepsilon(x)^{\beta}), \tag{120}$$

ce qui démontre le th. 12 (i), compte tenu de (77).

5.4. Démonstration du théorème 12 (ii)

Si x est assez grand, il existe un unique entier positif $n=n(x)$ tel que

$$\ell^{-(N-r/2)} \varepsilon_R(x) < |G_n|/k(n) \leqslant \varepsilon_R(x). \tag{121}$$

On en déduit, comme au n° 5.3,

$$|C_n| \, |G_n|^{-1} = O(\varepsilon_R(x)^{-\beta}). \tag{122}$$

D'autre part, la prop. 12 et le th. 7 (ii) entraînent, sous (GRH) :

$$\pi_{C_n}(x) \leqslant |C_n| \, |G_n|^{-1} \{\operatorname{Li}(x) + c_{21} k(n)^{-1} x^{1/2} (\log d_{E_n} + [E_n : \mathbf{Q}] \log x)\}. \tag{123$_R$}$$

D'après (76), on a

$$\log d_{E_n} = O(|G_n| \log |G_n|) = O(|G_n| \log x).$$

D'où

$$\begin{aligned} k(n)^{-1} x^{1/2} (\log d_{E_n} + [E_n : \mathbf{Q}] \log x) &= O(k(n)^{-1} |G_n| x^{1/2} \log x) \\ &= O(\varepsilon_R(x) x^{1/2} \log x), \quad \text{cf. (121)} \\ &= O(x/\log x) = O(\operatorname{Li}(x)). \end{aligned}$$

L'inégalité (123$_R$) entraîne donc :

$$\pi_{C_n}(x) = O(|C_n| \, |G_n|^{-1} \operatorname{Li}(x)) = O(\operatorname{Li}(x)/\varepsilon_R(x)^{\beta}), \quad \text{cf. (122)}. \tag{124$_R$}$$

Compte tenu de (77), cela démontre le th. 12 (ii).

§ 6. Non-lacunarité de certains produits eulériens

Comme dans les paragraphes précédents, la lettre K désigne un corps de nombres de degré fini n_K. On note M_K l'ensemble des idéaux $\neq 0$ de l'anneau A_K. La multiplication des idéaux fait de M_K un monoïde multiplicatif; l'élément neutre A_K de ce monoïde sera également noté 1.

6.1. Annulation de fonctions multiplicatives

Soit R un anneau commutatif intègre, et soit $a : M_K \to R$ une fonction *multiplicative*, autrement dit une fonction satisfaisant aux deux conditions suivantes :

$$a(1) = 1;$$

$$a(\mathfrak{m}\mathfrak{m}') = a(\mathfrak{m})a(\mathfrak{m}') \quad \text{si } \mathfrak{m}, \mathfrak{m}' \in M_K \text{ sont premiers entre eux.}$$

(Lorsque $K = \mathbf{Q}$, M_K s'identifie au monoïde $\mathbf{N}^*$ des entiers ≥ 1, et les conditions ci-dessus expriment bien que la fonction $n \mapsto a(n)$ est « multiplicative » au sens usuel.)

Nous nous intéresserons dans ce qui suit à la nullité, ou non-nullité, de $a(\mathfrak{m})$. Si x est un nombre réel ≥ 0, nous poserons

$$M_a(x) = \text{nombre des } \mathfrak{m} \in M_K \text{ tels que } a(\mathfrak{m}) \neq 0 \text{ et } N\mathfrak{m} \leq x; \tag{125}$$

$$P_a(x) = \text{nombre des } v \in \Sigma_K \text{ tels que } a(\mathfrak{p}_v) = 0 \text{ et } Nv \leq x. \tag{126}$$

(Rappelons que $N\mathfrak{m}$ désigne la norme de l'idéal $\mathfrak{m}$, et que $Nv = N\mathfrak{p}_v$, où $\mathfrak{p}_v$ est l'idéal premier de A_K défini par la place v, cf. n° 1.1.)

Le comportement asymptotique de la fonction P_a détermine presque celui de la fonction M_a. De façon plus précise :

Théorème 13. — Supposons que l'on ait

$$P_a(x) = \lambda x/\log x + O(x/(\log x)^{1+\delta}) \quad \textit{pour } x \to \infty \tag{127}$$

avec $0 \leq \lambda < 1$ *et* $\delta > 0$. *On a alors*

$$M_a(x) \sim \gamma_a x/(\log x)^{\lambda} \quad \textit{pour } x \to \infty \tag{128}$$

où γ_a *est une constante* > 0.

La démonstration sera donnée au n° 6.2.

Remarques

1) D'après (127), λ est la *densité* (au sens du n° 2.1) de l'ensemble des v tels que $a(\mathfrak{p}_v)=0$. On suppose $\lambda<1$.

2) La condition (127) peut être remplacée par la condition plus faible suivante :

(127′) $$P_a(x)=\lambda x/\log x+\omega(x),$$

avec $$|\omega(x)|=o(x/\log x) \quad \text{et} \quad \int_2^\infty |\omega(x)|x^{-2}dx<\infty.$$

3) Le th. 13 montre que le comportement de *a sur les idéaux premiers* $\mathfrak{p}_v$ suffit à déterminer l'ordre de grandeur de M_a, à la multiplication près par la constante γ_a. Par contre, γ_a dépend des valeurs de a sur les puissances des $\mathfrak{p}_v$.

4) Le cas le plus intéressant pour la suite est celui où $\lambda=0$. La condition (127′) ci-dessus revient alors à dire que l'intégrale $\int_2^\infty P_a(x)x^{-2}dx$ est convergente, ou, ce qui revient au même :

(127″) $$\sum_{a(\mathfrak{p}_v)=0} 1/Nv<\infty.$$

Le th. 13 affirme que

(129) $$M_a(x)\sim\gamma_a x \quad \text{avec } \gamma_a>0.$$

Si $M_1(x)$ désigne le nombre des $\mathfrak{m}\in M_K$ tels que $N\mathfrak{m}\leqslant x$, on sait (Dedekind [6], § 184) que $M_1(x)\sim\gamma_1 x$, où γ_1 est le résidu de la fonction zêta du corps K. Vu (129), on a donc

(130) $$M_a(x)/M_1(x)\to\gamma_a/\gamma_1 \quad \text{pour } x\to\infty.$$

Convenons de dire qu'une partie A de M_K est *de densité* α si le nombre des $\mathfrak{m}\in A$ tels que $N\mathfrak{m}\leqslant x$ est égal à $\alpha M_1(x)+o(x)$ pour $x\to\infty$. On peut alors reformuler (130) de la manière suivante :

Théorème 14. — Si (127″) *est satisfaite, l'ensemble des* $\mathfrak{m}\in M_K$ *tels que* $a(\mathfrak{m})\neq 0$ *a une densité* >0.

Pour une démonstration directe de ce théorème, voir n° 6.3.

6.2. Démonstration du théorème 13

Si $\mathfrak{m}\in M_K$, posons :

$$a^0(\mathfrak{m})=\begin{cases}0 & \text{si} \quad a(\mathfrak{m})=0\\ 1 & \text{si} \quad a(\mathfrak{m})\neq 0.\end{cases}$$

La fonction $a^0: M_K\to\{0,1\}$ ainsi définie est *multiplicative* du fait que R est intègre. Il est clair que $P_a=P_{a^0}$ et $M_a=M_{a^0}$. Il suffit donc de démontrer le th. 13 *lorsque* $a=a^0$, autrement dit *lorsque la fonction a ne prend que les valeurs* 0 *et* 1.

Supposons que ce soit le cas. Considérons la série de Dirichlet

$$\varphi(s)=\sum_{\mathfrak{m}} a(\mathfrak{m})\mathrm{N}\mathfrak{m}^{-s}, \tag{131}$$

qui converge dans le demi-plan $\mathrm{Re}(s)>1$. Si l'on écrit cette série sous la forme

$$\varphi(s)=\sum_{n=1}^{\infty} b(n)n^{-s}, \quad \text{avec} \quad b(n)=\sum_{\mathrm{N}\mathfrak{m}=n} a(\mathfrak{m}), \tag{132}$$

on a

$$\mathrm{M}_a(x)=\sum_{n\leqslant x} b(n), \tag{133}$$

autrement dit $\mathrm{M}_a(x)$ est la *fonction sommatoire* des coefficients de $\varphi(s)$.

La multiplicativité de la fonction a entraîne celle de la fonction b. On peut donc écrire $\varphi(s)$ comme *produit eulérien*

$$\varphi(s)=\prod_p \varphi_p(s),$$

avec

$$\varphi_p(s)=1+\sum_{n=1}^{\infty} b(p^n)p^{-ns}=\prod_{v\mid p}\left(1+\sum_{n=1}^{\infty} a(\mathfrak{p}_v^n)\mathrm{N}v^{-ns}\right). \tag{134}$$

Lemme 2. — *On a*

$$\sum_{\mathrm{N}v\leqslant x} a(\mathfrak{p}_v)=(1-\lambda)x/\log x+O(x/(\log x)^{1+\delta}), \tag{135}$$

avec $\delta>0$.

En effet, puisque $a(\mathfrak{p}_v)=0$ ou 1, on a

$$\mathrm{P}_a(x)=\sum_{\mathrm{N}v\leqslant x}(1-a(\mathfrak{p}_v))=\pi_{\mathrm{K}}(x)-\sum_{\mathrm{N}v\leqslant x} a(\mathfrak{p}_v), \tag{136}$$

où $\pi_{\mathrm{K}}(x)$ est le nombre des places v telles que $\mathrm{N}v\leqslant x$, cf. n° 2.1. D'après le théorème des nombres premiers « avec reste » (cf. par exemple n° 2.2, th. 2), on a

$$\pi_{\mathrm{K}}(x)=x/\log x+O(x/(\log x)^2). \tag{137}$$

En combinant (136), (137) et (127), on obtient (135).

Lemme 3. — *On a*

$$\sum_{p\leqslant x} b(p)=(1-\lambda)x/\log x+O(x/(\log x)^{1+\delta}), \tag{138}$$

avec $\delta>0$.

(Précisons que, dans (138), la sommation porte sur les nombres *premiers* $p\leqslant x$.)

Par définition, on a $b(p)=\sum_{\mathrm{N}v=p} a(\mathfrak{p}_v)$. On a donc

$$\sum_{\mathrm{N}v\leqslant x} a(\mathfrak{p}_v)=\sum_{p\leqslant x} b(p)+\Sigma' a(\mathfrak{p}_v),$$

où la somme Σ' porte sur les places v *de degré* $f_v \geqslant 2$ (i.e. telles que Nv ne soit pas un nombre premier), avec $Nv \leqslant x$. Le nombre de telles places est évidemment $O(x^{1/2}/\log x)$. On en conclut que

$$\sum_{Nv \leqslant x} a(\mathfrak{p}_v) = \sum_{p \leqslant x} b(p) + O(x^{1/2}/\log x),$$

et (138) résulte donc de (135).

Lemme 4. — *On a*

$$\sum_p b(p)p^{-s} = (1-\lambda)\log 1/(s-1) + \varepsilon_1(s), \tag{139}$$

pour s *réel* >1, *où* $\varepsilon_1(s)$ *est continue en* $s=1$.

Posons

$$B(x) = \sum_{p \leqslant x} b(p).$$

On a

$$\sum_p b(p)p^{-s} = \int_2^\infty x^{-s}\,dB(x) = -\int_2^\infty B(x)\,d(x^{-s}) = s\int_2^\infty B(x)x^{-1-s}\,dx.$$

D'après le lemme précédent, on a

$$B(x) = (1-\lambda)x/\log x + \rho(x),$$

avec $\rho(x) = O(x/(\log x)^{1+\delta})$, $\delta > 0$. D'où :

$$\sum_p b(p)p^{-s} = (1-\lambda)s\int_2^\infty x^{-s}(\log x)^{-1}\,dx + s\int_2^\infty \rho(x)x^{-1-s}\,dx.$$

Le terme $s\int_2^\infty \rho(x)x^{-1-s}\,dx$ est continu en $s=1$. Pour prouver le lemme 4, il suffit donc de vérifier que l'intégrale

$$I(s) = \int_2^\infty x^{-s}(\log x)^{-1}\,dx$$

est de la forme $\log 1/(s-1) + \varepsilon_2(s)$, où $\varepsilon_2(s)$ est continue en $s=1$; cela ne présente pas de difficultés [on peut par exemple faire le changement de variable $x = e^{u/(s-1)}$; on en déduit que $I(s) = E_1((s-1)\log 2)$, avec $E_1(z) = \int_z^\infty u^{-1}e^{-u}\,du$; on utilise ensuite le fait connu que $E_1(z) = -\gamma - \log z + O(z)$ pour $z \to 0$, où γ désigne la constante d'Euler].

Lemme 5. — *Il existe une constante* $u > 0$ *telle que*

$$\varphi(s) \sim u/(s-1)^{1-\lambda} \quad \textit{pour } s \to 1 \quad (s \text{ réel} > 1). \tag{140}$$

D'après (134), on a

$$\log \varphi(s) = \sum_p \log \varphi_p(s) = \sum_p b(p)p^{-s} + \varepsilon_3(s),$$

où $\varepsilon_3(s)$ est continue pour $s=1$ (et même prolongeable analytiquement dans le demi-plan $\mathrm{Re}(s)>1/2$). Vu (139), cela donne

$$\log \varphi(s)=(1-\lambda)\log 1/(s-1)+\varepsilon_4(s),$$

où $\varepsilon_4(s)$ est continue en $s=1$. D'où (140), avec $u=\exp \varepsilon_4(1)$.

Lemme 6. — *On a*

$$\sum_{n\leqslant x} b(n)/n \sim u(\log x)^{1-\lambda}/\Gamma(2-\lambda) \quad \textit{pour } x\to\infty. \tag{141}$$

Cela résulte du lemme 5, et d'un théorème taubérien de Hardy-Littlewood ([13], th. 16 et [14], th. D).

Lemme 7. — *On a*

$$M_a(x) \sim (1-\lambda)\frac{x}{\log x}\sum_{n\leqslant x} b(n)/n \quad \textit{pour } x\to\infty. \tag{142}$$

Cela résulte du lemme 3 et de la multiplicativité de la fonction b, d'après Wirsing [50], Hilfssatz 2, p. 93.

En combinant les lemmes 6 et 7, on obtient

$$M_a(x) \sim \gamma_a x/(\log x)^{\lambda},$$

avec

$$\gamma_a=(1-\lambda)u/\Gamma(2-\lambda)=u/\Gamma(1-\lambda), \tag{143}$$

ce qui achève la démonstration du th. 13.

Remarques

1) Lorsqu'on remplace l'hypothèse (127) par l'hypothèse plus faible (127'), les énoncés des lemmes 2 et 3 doivent être modifiés de façon évidente. Le reste de la démonstration s'applique sans changement.

2) A la place du théorème taubérien de Hardy-Littlewood, on aurait pu utiliser un théorème de Wirsing sur les fonctions multiplicatives ([50], Satz 1).

6.3. Démonstration directe du théorème 14

Dans le cas où $\lambda=0$ (th. 14), on peut éviter de recourir à un théorème taubérien. Voici comment on procède :

On part de l'hypothèse :

$$\sum_{a(\mathfrak{p}_v)=0} 1/\mathrm{N}v<\infty. \tag{127''}$$

Comme au n° 6.2, on suppose que a ne prend que les valeurs 0 et 1. Soit $c : \mathrm{M_K} \to \mathbf{Z}$ la fonction multiplicative caractérisée par la propriété

$$a(\mathfrak{m}) = \sum_{\mathfrak{m}' \mid \mathfrak{m}} c(\mathfrak{m}') \quad \text{pour tout } \mathfrak{m} \in \mathrm{M_K}. \tag{144}$$

D'après la formule d'inversion de Möbius, on a

$$c(\mathfrak{p}_v^n) = a(\mathfrak{p}_v^n) - a(\mathfrak{p}_v^{n-1}) = \begin{cases} 1 & \text{si} \quad a(\mathfrak{p}_v^n) = 1 \quad \text{et} \quad a(\mathfrak{p}_v^{n-1}) = 0 \\ 0 & \text{si} \quad a(\mathfrak{p}_v^n) = a(\mathfrak{p}_v^{n-1}) \\ -1 & \text{si} \quad a(\mathfrak{p}_v^n) = 0 \quad \text{et} \quad a(\mathfrak{p}_v^{n-1}) = 1 \end{cases} \tag{145}$$

pour tout $v \in \Sigma_\mathrm{K}$ et tout $n \geqslant 1$.

Posons

$$\alpha_v = 1 + \sum_{n=1}^{\infty} c(\mathfrak{p}_v^n)/\mathrm{N}v^n = (1 - 1/\mathrm{N}v)(1 + \sum_{n=1}^{\infty} a(\mathfrak{p}_v^n)/\mathrm{N}v^n). \tag{146}$$

On a

$$\alpha_v = \begin{cases} 1 + O(1/\mathrm{N}v^2) & \text{si} \quad a(\mathfrak{p}_v) = 1 \\ 1 - 1/\mathrm{N}v + O(1/\mathrm{N}v^2) & \text{si} \quad a(\mathfrak{p}_v) = 0. \end{cases}$$

Vu (127''), cela entraîne que le produit infini

$$\alpha = \prod_v \alpha_v \tag{147}$$

est absolument convergent, et égal à $\sum_{\mathfrak{m}} c(\mathfrak{m})/\mathrm{N}\mathfrak{m}$. Comme les α_v sont >0, il en est de même de α.

D'autre part, la formule (144) entraîne

$$\mathrm{M}_a(x) = \sum_{\mathfrak{m}} c(\mathfrak{m}) \mathrm{M}_1(x/\mathrm{N}\mathfrak{m}), \tag{148}$$

où $\mathrm{M}_1(x)$ désigne le nombre des $\mathfrak{m} \in \mathrm{M_K}$ tels que $\mathrm{N}\mathfrak{m} \leqslant x$, cf. n° 6.1, Remarque 4. Or on a

$$\mathrm{M}_1(x) = \gamma_1 x + \psi(x) \quad \text{avec} \quad \psi(x) = o(x), \tag{149}$$

où γ_1 est le résidu de la fonction zêta de K. On en déduit

$$\begin{aligned} \mathrm{M}_a(x) &= \sum_{\mathfrak{m}} (\gamma_1 c(\mathfrak{m}) x/\mathrm{N}\mathfrak{m} + c(\mathfrak{m}) \psi(x/\mathrm{N}\mathfrak{m})) \\ &= \gamma_1 \alpha x + \sum_{\mathfrak{m}} c(\mathfrak{m}) \psi(x/\mathrm{N}\mathfrak{m}). \end{aligned} \tag{150}$$

Utilisant la convergence absolue de la série $\sum c(\mathfrak{m})/\mathrm{N}\mathfrak{m}$, et le fait que $\psi(x) = o(x)$, on montre facilement que

$$\sum_{\mathfrak{m}} c(\mathfrak{m}) \psi(x/\mathrm{N}\mathfrak{m}) = o(x) \quad \text{pour } x \to \infty.$$

Vu (150), on a donc

$$M_a(x) \sim \gamma_1 \alpha x \quad \text{pour } x \to \infty, \tag{151}$$

ce qui démontre le th. 14, et prouve en même temps que la densité de l'ensemble des $\mathfrak{m} \in M_K$ tels que $a(\mathfrak{m}) \neq 0$ est égale à α.

6.4. Relations avec le § 4

Revenons aux notations du n° 4.1, i.e. considérons une extension galoisienne E/K, dont le groupe de Galois G est un groupe de Lie ℓ-adique, et qui est non ramifiée en dehors d'une partie finie S de Σ_K; soit C une partie fermée de G stable par conjugaison, et soit Σ_C l'ensemble des $v \in \Sigma_K - S$ tels que la substitution de Frobenius σ_v de v appartienne à C.

Nous dirons que C est *liée* à la fonction multiplicative a si :

$$a(\mathfrak{p}_v) = 0 \Leftrightarrow v \in \Sigma_C \quad (\text{pour } v \in \Sigma_K - S). \tag{152}$$

Proposition 13. — Supposons que C *soit un sous-ensemble analytique fermé du groupe de Lie* G, *et que* $C \neq G$. *Soit* μ *la mesure de Haar de* G *normalisée de telle sorte que sa masse totale soit* 1. *Alors, si* C *et a sont liés au sens ci-dessus, la condition*

$$P_a(x) = \lambda x/\log x + o(x/(\log x)^{1+\delta}) \tag{127}$$

du th. 13 est satisfaite, avec $\lambda = \mu(C)$ *et* $\delta > 0$.

Si $\pi_C(x)$ désigne le nombre des places $v \in \Sigma_C$ telles que $Nv \leqslant x$, la relation (152) entraîne

$$\pi_C(x) \leqslant P_a(x) \leqslant \pi_C(x) + |S|,$$

d'où

$$P_a(x) = \pi_C(x) + O(1). \tag{153}$$

Tout revient donc à démontrer que

$$\pi_C(x) = \lambda x/\log x + O(x/(\log x)^{1+\delta}) \quad \text{avec } \delta > 0. \tag{154}$$

Soit C_1 l'intérieur de C, et soit $C_2 = C - C_1$. Du fait que C est analytique, C_1 est fermé. Il en résulte que C_1 et C_2 sont des parties fermées disjointes, et l'on a

$$\pi_C(x) = \pi_{C_1}(x) + \pi_{C_2}(x). \tag{155}$$

Comme l'intérieur de C_2 est vide, on a $\dim C_2 < \dim G$, et le cor. 1 au th. 10 du n° 4.1 montre que

$$\pi_{C_2}(x) = O(x/(\log x)^{1+\delta}) \tag{156}$$

avec $\delta > 0$, par exemple $\delta = 1/(N+1)$, où $N = \dim G$. D'autre part, tout ensemble analytique d'intérieur vide est de mesure nulle; c'est là un résultat élémentaire (cf. [2], § 10.1.2 ainsi que [40], p. 1.8, exerc.) que l'on peut déduire, par exemple, du « Vor-

bereitungssatz » (bien entendu, c'est aussi une conséquence du th. 8 du n° 3.2). On a donc $\mu(C_2)=0$, d'où

(157) $$\mu(C)=\mu(C_1).$$

Comme C_1 est ouvert et fermé dans G, il existe un sous-groupe ouvert distingué U de G tel que C_1 soit réunion de classes modulo U, i.e. soit image réciproque d'un sous-ensemble C_U du groupe quotient G/U. On a

(158) $$\mu(C_1)=|C_U|/(G:U).$$

Soit E_U le sous-corps de E fixé par U. L'extension E_U/K est galoisienne, et son groupe de Galois est le groupe fini G/U. En appliquant le théorème de Chebotarev (sous la forme du th. 2 du n° 2.2, par exemple) à E_U/K et à C_U, on obtient :

(159) $$\pi_{C_1}(x)=\pi_{C_U}(x)=\lambda x/\log x+O(x/(\log x)^2),$$

avec $\lambda=|C_U|/(G:U)=\mu(C_1)=\mu(C)$. En combinant (156) et (159) on obtient (154), ce qui achève la démonstration.

Corollaire 1. — Il existe un nombre $\gamma_a>0$ *tel que*

(128) $$M_a(x)\sim\gamma_a x/(\log x)^\lambda \quad \textit{pour } x\to\infty.$$

Cela résulte du th. 13, et du fait que $\lambda=\mu(C)$ est <1 puisque $C\neq G$.

Corollaire 2. — Les deux propriétés suivantes sont équivalentes :

(i) *l'intérieur de* C *est vide*;

(ii) *l'ensemble des* $\mathfrak{m}\in M_K$ *tels que* $a(\mathfrak{m})\neq 0$ *a une densité* >0.

En effet, (i) équivaut à $C_1=\emptyset$, i.e. $C_U=\emptyset$, i.e. $\lambda=0$.

6.5. Exemple : série L attachée à une représentation ℓ-adique

Soit E/K comme ci-dessus. Donnons-nous un plongement du groupe $G=\mathrm{Gal}(E/K)$ dans un *groupe linéaire* $\mathbf{GL}_r(F)$, où F est une extension finie de $\mathbf{Q}_\ell$, et r un entier $\geqslant 1$. Si $\overline{K}$ est une clôture algébrique de K, l'homomorphisme

$$\mathrm{Gal}(\overline{K}/K)\to\mathrm{Gal}(E/K)=G\to\mathbf{GL}_r(F)$$

sera noté ρ. Lorsque $F=\mathbf{Q}_\ell$, ρ est une « représentation ℓ-adique de K », au sens de [40], chap. I.

Les polynômes $P_v(T)$

Si $v\in\Sigma_K-S$, on *définit* P_v par la formule

(160) $$P_v(T)=\det(1-T\sigma_v);$$

cela a un sens, puisque σ_v est un élément de $G\subset\mathbf{GL}_r(F)$, défini à conjugaison près. Le polynôme P_v est de degré r; ses coefficients appartiennent à F.

Si $v \in S$, on *choisit* un polynôme P_v, de degré $\leqslant r$, à coefficients dans F, tel que $P_v(0) = 1$.

La série L *attachée à* ρ

C'est une série *formelle* de Dirichlet relativement à K, au sens de Weil [48]. Elle est définie par le produit eulérien

$$L(s) = \sum_{\mathfrak{m}} a(\mathfrak{m}) N\mathfrak{m}^{-s} = \prod_{v} L_v(s), \tag{161}$$

où

$$L_v(s) = 1/P_v(Nv^{-s}). \tag{162}$$

Les coefficients $a(\mathfrak{m})$ de L sont caractérisés par :

(163) $\mathfrak{m} \mapsto a(\mathfrak{m})$ est une fonction multiplicative à valeurs dans F;

$$1/P_v(T) = 1 + \sum_{n=1}^{\infty} a(\mathfrak{p}_v^n) T^n \quad \text{pour tout } v \in \Sigma_K. \tag{164}$$

Vu (160), ceci entraîne :

$$a(\mathfrak{p}_v) = \operatorname{Tr} \sigma_v \quad \text{pour tout } v \in \Sigma_K - S. \tag{165}$$

L'ensemble C

On définit C comme l'ensemble des $s \in G$ tels que $\operatorname{Tr}(s) = 0$, la trace étant relative au plongement donné de G dans $\mathbf{GL}_r(F)$. Il est clair que C est un sous-espace analytique fermé de G, stable par conjugaison, et distinct de G (puisque l'élément neutre n'appartient pas à C). La formule (165) montre que C est *lié* à la fonction multiplicative a, au sens du n° 6.4. Les conditions de la prop. 13 sont donc satisfaites; vu le cor. 1 à cette proposition, on a :

Proposition 14. — *Soit* $\lambda = \mu(C)$ *la mesure de* C. *Il existe un nombre* $\gamma_a > 0$ *tel que*

$$M_a(x) \sim \gamma_a x/(\log x)^{\lambda} \quad \textit{pour } x \to \infty. \tag{128}$$

On verra ci-après que $\lambda \leqslant 1 - 1/r^2$.

Corollaire. — *Si* $\lambda = 0$, *i.e. si l'intérieur de* C *est vide, la densité de l'ensemble des* $\mathfrak{m}$ *tels que* $a(\mathfrak{m}) \neq 0$ *est* > 0.

(En d'autres termes, la série formelle $\sum a(\mathfrak{m}) N\mathfrak{m}^{-s}$ a « beaucoup » de termes $\neq 0$: ce n'est pas une série « lacunaire ».)

Calcul de $\lambda = \mu(C)$

On va voir que C ne dépend que de *l'enveloppe algébrique* du groupe G. Rappelons d'abord ce qu'est cette enveloppe : c'est le plus petit sous-groupe algébrique H de $\mathbf{GL}_r$ dont le groupe des points H(F) contienne G (c'est aussi, si l'on préfère, *l'adhérence* de G dans $\mathbf{GL}_r$ pour la topologie de Zariski). Soit H_1 la composante neutre de H, et soit Φ

le groupe fini H/H_1; si $\varphi\in\Phi$, notons H_φ son image réciproque dans H, et notons G_φ l'intersection de G et H_φ; on vérifie facilement que G_φ est dense dans H_φ pour la topologie de Zariski.

Proposition 15. — Soit Ψ l'ensemble des $\psi\in\Phi=H/H_1$ tels que l'on ait $\mathrm{Tr}(s)=0$ pour tout $s\in H_\psi$. On a alors

$$C_1=\bigcup_{\psi\in\Psi} G_\psi.$$

(Rappelons que C_1 désigne l'intérieur de C, cf. n° 6.4.)

Corollaire 1. — On a $\lambda=|\Psi|/|\Phi|$.

En effet, la prop. 15 montre que

$$\lambda=\mu(C_1)=\sum_{\psi\in\Psi}\mu(G_\psi)=|\Psi|\mu(G_1)=|\Psi|.(G:G_1)^{-1}=|\Psi|/|\Phi|.$$

Corollaire 2. — Si l'enveloppe algébrique H de G est connexe, on a $\lambda=0$, et la série L attachée à ρ n'est pas lacunaire (au sens du cor. à la prop. 14).

En effet, si H est connexe, on a $H=H_1$, $|\Phi|=1$ et $|\Psi|=0$.

Démonstration de la prop. 15

Si $\psi\in\Psi$, G_ψ est contenu dans C; comme G_ψ est ouvert dans G, il en résulte que G_ψ est contenu dans C_1. Reste à montrer que, si $\varphi\in\Phi-\Psi$, l'ensemble $C_\varphi=C\cap G_\varphi$ a un intérieur vide. Supposons que ce ne soit pas le cas, et soit g un point intérieur à C_φ. Il existe un sous-groupe ouvert distingué U de G_1 tel que C_φ contienne gU. Soit H_U l'adhérence de U pour la topologie de Zariski. On a $H_U\subset H_1$, et, comme U est d'indice fini dans G_1, H_U est d'indice fini dans H; vu le fait que H_1 est connexe, ceci entraîne $H_U=H_1$. L'adhérence de gU pour la topologie de Zariski est donc $gH_1=H_\varphi$. Comme la trace s'annule sur gU, et que c'est une fonction polynomiale, elle s'annule sur tout H_φ, ce qui contredit l'hypothèse $\varphi\in\Phi-\Psi$.

Proposition 16. — On a $\lambda\leqslant 1-1/r^2$.

Vu le cor. 1 à la prop. 15, on est ramené à prouver :

Lemme 8. — Si H est un sous-groupe algébrique de $\mathbf{GL}_r$ (sur un corps de caractéristique zéro), *de composante neutre H_1, et si l'on définit $\Phi=H/H_1$, Ψ et $\lambda=|\Psi|/|\Phi|$ comme ci-dessus, on a*

$$\lambda\leqslant 1-1/r^2. \tag{166}$$

Le *principe de Lefschetz* permet de supposer que le corps de base est $\mathbf{C}$. On peut également supposer (quitte à remplacer la représentation $H\to\mathbf{GL}_r$ par sa semi-simplifiée) que H est un groupe *réductif*. Soit alors U un sous-groupe compact maximal du groupe complexe $H(\mathbf{C})$; si $\varphi\in\Phi$, posons $U_\varphi=U\cap H_\varphi$. On sait que $U_1=U\cap H_1$ est connexe,

et que U_φ est une classe modulo U_1; le groupe U/U_1 s'identifie à $\Phi = H/H_1$. Notons C(U) l'ensemble des éléments de U de trace 0, et posons $C(U)_\varphi = U_\varphi \cap C(U)$ pour tout $\varphi \in \Phi$. On a $C(U)_\psi = U_\psi$ si $\psi \in \Psi$; par contre, si $\varphi \in \Phi - \Psi$, un argument analogue à celui utilisé dans la démonstration de la prop. 15 montre que $C(U)_\varphi$ est un sous-ensemble analytique (réel) fermé de U_φ, d'intérieur vide, et que sa mesure est nulle. Si μ est la mesure de Haar de U, normalisée de telle sorte que sa masse totale soit 1, on a

$$\mu(C(U)) = \sum_{\psi \in \Psi} \mu(U_\psi) = |\Psi| \mu(U_1) = |\Psi| / |\Phi| = \lambda. \tag{167}$$

D'après la théorie des caractères des groupes compacts, l'intégrale

$$\int_U |\mathrm{Tr}(s)|^2 \mu(s)$$

est égale à la dimension du commutant de U (ou de H, cela revient au même) dans l'algèbre $\mathbf{M}_r(\mathbf{C})$ des matrices. En particulier, on a

$$\int_U |\mathrm{Tr}(s)|^2 \mu(s) \geqslant 1. \tag{168}$$

Mais $\mathrm{Tr}(s)$ est 0 sur C(U), et est majoré en valeur absolue par r sur $U - C(U)$. On a donc, d'après (167)

$$\int_U |\mathrm{Tr}(s)|^2 \mu(s) \leqslant \mu(U - C(U)) r^2 \leqslant (1 - \lambda) r^2. \tag{169}$$

En combinant (168) et (169), on obtient (166).

Remarque

Pour que λ soit *égal à* $1 - 1/r^2$ (ce qui conduit à une série L « aussi lacunaire que possible »), il faut et il suffit que les deux conditions suivantes soient satisfaites :

(i) la représentation $H \to \mathbf{GL}_r$ est *absolument irréductible*;

(ii) l'image PH de H dans le groupe projectif $\mathbf{PGL}_r$ est un *groupe fini d'ordre* r^2.

(Cela se voit en reprenant la démonstration ci-dessus, et en déterminant dans quel cas on a égalité dans (168) et (169).)

Des exemples de tels groupes existent pour toute valeur de r. On peut notamment prendre pour PH le produit d'un groupe abélien d'ordre r par lui-même; il y a également des exemples non abéliens, cf. Iwahori-Matsumoto [19], fin du § 5.

Lorsque $r = 2$, la valeur maximum de λ est $3/4$, et cette valeur est atteinte si et seulement si le groupe PH est un groupe non cyclique d'ordre 4; on en verra un exemple au n° 7.8.

Problème

Y a-t-il des résultats analogues à ceux de cette section pour les séries L attachées par Langlands aux représentations cuspidales des groupes réductifs — même lorsque ces séries L ne correspondent pas à des représentations ℓ-adiques? Cela me paraît probable; la question est liée aux conjectures de Langlands [25], p. 210 (conjectures qui visent à introduire des groupes « H » et « U » analogues à ceux du lemme 8 ci-dessus).

§ 7. Applications aux formes modulaires

7.1. Notations

Soient :

N et k des entiers $\geqslant 1$ (le « niveau » et le « poids »);

$\Gamma_0(N)$ le sous-groupe de $\mathbf{SL}_2(\mathbf{Z})$ formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que $c \equiv 0 \pmod{N}$;

$\omega : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$ un caractère mod N tel que $\omega(-1) = (-1)^k$.

Nous noterons $M(N, k, \omega)$ (resp. $S(N, k, \omega)$) l'espace des *formes modulaires* (resp. formes modulaires paraboliques) *de type* (k, ω) sur $\Gamma_0(N)$, cf. par exemple [9], [27], [44]; c'est un espace vectoriel complexe de dimension finie. Rappelons que, si $f \in M(N, k, \omega)$, on a

$$f\left(\frac{az+b}{cz+d}\right) = \omega(d)(cz+d)^k f(z) \quad \text{pour tout} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N). \tag{170}$$

De plus, f admet un développement en série

$$f(z) = \sum_{n=0}^{\infty} a_n(f) q^n, \quad \text{où } q = e^{2\pi i z}, \tag{171}$$

qui converge pour tout z tel que $\mathrm{Im}(z) > 0$; les $a_n(f)$ sont appelés les *coefficients* de f; on a $a_0(f) = 0$ si f est parabolique.

Opérateurs de Hecke

Si p est un nombre premier, et si $f \in M(N, k, \omega)$, on pose :

$$f \mid U_p = \Sigma a_{pn}(f) q^n \quad \text{si } p \mid N, \tag{172}$$

$$f \mid T_p = \Sigma a_{pn}(f) q^n + \omega(p) p^{k-1} \Sigma a_n(f) q^{pn} \quad \text{si } p \nmid N. \tag{173}$$

On a $f \mid U_p \in M(N, k, \omega)$ et $f \mid T_p \in M(N, k, \omega)$, cf. [27]. Les opérateurs U_p et T_p ainsi définis commutent entre eux, et laissent stable le sous-espace $S(N, k, \omega)$ des formes paraboliques. Leurs valeurs propres sont des entiers algébriques (cf. [9], prop. 2.7 ainsi que Shimura [44], § 3.5).

7.2. Valeurs propres des opérateurs de Hecke : énoncé du théorème

Soit f une forme modulaire non identiquement nulle, appartenant à $M(N, k, \omega)$. Supposons que f soit *fonction propre des* T_p, $p \nmid N$, avec pour valeurs propres a_p :

$$f \mid T_p = a_p f \quad (p \nmid N). \tag{174}$$

Supposons en outre que :

(a) le poids k de f est $\geqslant 2$;

(b) f est *parabolique*;

(c) f n'est pas de type CM au sens de Ribet (i.e. il n'existe pas de corps quadratique imaginaire L tel que $a_p = 0$ pour tout p qui est inerte dans L, cf. [33], § 3).

Soit d'autre part $h(T)$ un polynôme à coefficients complexes, et soit $\Sigma_{f,h}$ l'ensemble des $p \nmid N$ tels que

$$a_p = h(p). \tag{175}$$

Si x est un nombre réel $\geqslant 2$, posons

$$P_{f,h}(x) = \text{nombre des } p \leqslant x \text{ appartenant à } \Sigma_{f,h}. \tag{176}$$

(Par exemple, pour $h = 0$, $P_{f,0}(x)$ est le nombre des $p \leqslant x$ tels que $p \nmid N$ et $a_p = 0$.)

Nous allons voir que la fonction $P_{f,h}(x)$ est « petite » lorsque $x \to \infty$, autrement dit que la relation (175) est « peu souvent » vérifiée. De façon plus précise :

Théorème 15. — Sous les hypothèses (a), (b) et (c) ci-dessus, on a

$$P_{f,h}(x) = O(\mathrm{Li}(x)/\varepsilon(x)^{1/4}) \quad \textit{pour } x \to \infty, \tag{177}$$

et, sous (GRH),

$$P_{f,h}(x) = O(\mathrm{Li}(x)/\varepsilon_R(x)^{1/4}) \quad \textit{pour } x \to \infty, \tag{178$_R$}$$

où $\varepsilon(x)$ *et* $\varepsilon_R(x)$ *sont les fonctions définies par les formules* (65) *et* (67) *du n°* 4.1.

De plus, lorsque $h = 0$, *l'exposant* 1/4 *de* (177) *et* (178$_R$) *peut être remplacé par* 1/2.

La démonstration sera donnée au n° 7.3.

Compte tenu des formules :

$$\varepsilon(x) = (\log x)(\log\log x)^{-2}(\log\log\log x)^{-1} \tag{65}$$

et

$$\varepsilon_R(x) = x^{1/2}(\log x)^{-2}, \tag{67}$$

le th. 15 entraîne :

Corollaire 1. — On a

$$P_{f,h}(x) = O(x/(\log x)^{5/4-\delta}) \quad \textit{pour tout } \delta > 0, \tag{179}$$

et, sous (GRH),

$$P_{f,h}(x) = O(x^{7/8}(\log x)^{1/2}). \tag{180$_R$}$$

De même, pour $h = 0$:

Corollaire 2. — On a

$$P_{f,0}(x) = O(x/(\log x)^{3/2-\delta}) \quad \textit{pour tout } \delta > 0, \tag{181}$$

et, sous (GRH),

$$(182_R) \qquad P_{f,0}(x) = O(x^{3/4}).$$

Remarques

1) Si $\deg(h) \geqslant k/2$, l'ensemble $\Sigma_{f,h}$ des p tels que $a_p = h(p)$ est *fini*, autrement dit, on a $P_{f,h}(x) = O(1)$. Cela résulte de la majoration

$$(183) \qquad |a_p| \leqslant 2p^{k/2-\delta},$$

avec $\delta > 0$ ($\delta = 1/8$ d'après Kloosterman [20], $\delta = 1/5$ d'après Rankin [32], et finalement $\delta = 1/2$ d'après Deligne [8], th. 8.2). Le th. 15 n'a donc d'intérêt que si $\deg(h) \leqslant (k-1)/2$.

2) La majoration (178_R), même avec l'exposant $1/4$ remplacé par 1, n'est probablement pas la meilleure possible. Des arguments heuristiques basés sur l'ordre de grandeur de $a_p - h(p)$ suggèrent les conjectures suivantes (cf. [42], § 4.11, ainsi que Lang-Trotter [24]) :

$$(184_?) \qquad P_{f,h}(x) = O(x^{1/2}/\log x) \quad \text{si } k = 2,$$

$$(185_?) \qquad P_{f,h}(x) = O(\log\log x) \quad \text{si } k = 3,$$

$$(186_?) \qquad P_{f,h}(x) = O(1) \quad \text{si } k \geqslant 4.$$

3) Les hypothèses *(a)*, *(b)*, *(c)* sont *nécessaires* pour la validité de (177), ou même simplement de $P_{f,h}(x) = o(x/\log x)$. De façon plus précise, si l'une de ces hypothèses n'est pas satisfaite, on peut choisir le polynôme $h(T)$ de telle sorte que

$$P_{f,h}(x) \sim Cx/\log x \quad \text{avec} \quad C > 0$$

(autrement dit $\Sigma_{f,h}$ a une densité >0). On prend en effet :

$$h(T) = \begin{cases} 0 \text{ ou } 2 & \text{si } k = 1, \\ 1 + T^{k-1} & \text{si } f \text{ n'est pas parabolique}, \\ 0 & \text{si } f \text{ est de type CM}. \end{cases}$$

7.3. Démonstration du th. 15

i) *Représentations ℓ-adiques attachées à f* (cf. [7], [9], [33])

Soit F un corps de nombres contenant les a_p et les $\omega(p)$ pour $p \nmid N$: il en existe, cf. par exemple [9], § 2. Soit λ une place ultramétrique de F de degré 1, i.e. telle que le complété F_λ de F en λ s'identifie à un corps ℓ-adique $\mathbf{Q}_\ell$; le choix d'une telle place revient à plonger F dans $\mathbf{Q}_\ell$, ce qui permet d'identifier les a_p et les $\omega(p)$ à des éléments de $\mathbf{Q}_\ell$. D'après Deligne ([7], voir aussi [9], th. 6.1) il existe une représentation linéaire continue

$$\rho_\ell : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(F_\lambda) = \mathbf{GL}_2(\mathbf{Q}_\ell)$$

qui jouit des propriétés suivantes :

(i) ρ_ℓ est semi-simple;

(ii) ρ_ℓ est non ramifiée en dehors des facteurs premiers de $N\ell$ (nous dirons aussi « non ramifiée en dehors de $N\ell$ »);

(iii) si $p \nmid N\ell$, la substitution de Frobenius $\rho_\ell(\sigma_p)$ (qui est définie, à conjugaison près, grâce à (ii)), est telle que :

$$\text{Tr } \rho_\ell(\sigma_p) = a_p \tag{187}$$

et

$$\det \rho_\ell(\sigma_p) = \omega(p)p^{k-1}. \tag{188}$$

De plus, ces propriétés caractérisent ρ_ℓ, à équivalence près.

Proposition 17. — *Le groupe* $G_\ell = \text{Im}(\rho_\ell)$ *est un sous-groupe* ouvert *de* $\mathbf{GL}_2(\mathbf{Q}_\ell)$.

Soit $\mathfrak{g}_\ell$ l'algèbre de Lie du groupe ℓ-adique G_ℓ. C'est une sous-algèbre de l'algèbre de Lie $\mathfrak{gl}_2 = \mathbf{M}_2(\mathbf{Q}_\ell)$. D'après Ribet [33], prop. 4.4, $\mathfrak{g}_\ell$ est irréductible, et non abélienne; elle contient donc la sous-algèbre $\mathfrak{sl}_2$ de $\mathfrak{gl}_2$ formée des éléments de trace 0. On a $\mathfrak{g}_\ell \neq \mathfrak{sl}_2$, car sinon l'image de G_ℓ par l'homomorphisme $\det : \mathbf{GL}_2(\mathbf{Q}_\ell) \to \mathbf{Q}_\ell^*$ serait un groupe fini, ce qui est incompatible avec (188). On a donc $\mathfrak{g}_\ell = \mathfrak{gl}_2$, d'où la prop. 17.

ii) *Démonstration du th. 15 : cas général*

Choisissons F, λ et ℓ comme ci-dessus. Soit E_ℓ la sous-extension de $\overline{\mathbf{Q}}$ fixée par $\text{Ker}(\rho_\ell)$. L'extension $E_\ell/\mathbf{Q}$ est galoisienne, et son groupe de Galois s'identifie au groupe $G_\ell = \text{Im}(\rho_\ell)$. Vu la prop. 17, G_ℓ est un groupe de Lie ℓ-adique de dimension 4. On va lui appliquer le th. 10 du § 4.

Remarquons d'abord que l'on peut supposer que les coefficients du polynôme $h(T)$ appartiennent à F (sinon, l'ensemble $\Sigma_{\ell,h}$ serait fini). Soit e l'ordre du caractère ω; posons $m = (k-1)e$. Si U et T sont deux indéterminées, il existe un polynôme H(U, T), à coefficients dans F, tel que

$$\text{H}(\text{U}, \text{T}^m) = \prod_{w \in \mu_m} (\text{U} - h(w\text{T})), \tag{189}$$

où w parcourt le groupe μ_m des racines m-ièmes de l'unité; cela se voit en remarquant que le membre de droite de (189) est invariant par $\text{T} \mapsto w\text{T}$ (pour $w \in \mu_m$). Soit C le sous-espace de G_ℓ formé des matrices s telles que

$$\text{H}(\text{Tr}(s), \det(s)^e) = 0. \tag{190}$$

Il est clair que C est un sous-espace analytique fermé de G_ℓ, stable par conjugaison, et sans point intérieur, donc de dimension $\leqslant 3$. De plus, si $p \in \Sigma_{\ell,h}$ et $p \neq \ell$, la substitution de Frobenius $s_p = \rho_\ell(\sigma_p)$ *appartient à* C. On a en effet

$$\text{Tr}(s_p) = a_p = h(p) \quad \text{et} \quad \det(s_p)^e = p^{(k-1)e} = p^m,$$

d'où

$$\text{H}(\text{Tr}(s_p), \det(s_p)^e) = \text{H}(h(p), p^m) = \prod_w (h(p) - h(wp)) = 0.$$

On a donc

$$\Sigma_{f,h} \subset \Sigma_C \cup \{\ell\},$$

où Σ_C est défini comme au § 4 (relativement à l'ensemble S formé des diviseurs premiers de $N\ell$). D'où, avec les notations du n° 4.1 :

$$P_{f,h}(x) \leqslant \pi_C(x) + 1, \tag{191}$$

et en appliquant le th. 10 avec $\alpha = (4-3)/4 = 1/4$, on obtient le résultat cherché.

iii) *Démonstration du th. 15 : le cas* $h = 0$

On procède de manière analogue, en définissant C comme l'ensemble des $s \in G_\ell$ tels que $\mathrm{Tr}(s) = 0$. Si H_ℓ désigne l'intersection de G_ℓ avec le groupe des homothéties, C est stable par multiplication par H_ℓ, donc est image réciproque d'une partie C′ du groupe quotient $G'_\ell = G_\ell / H_\ell$. Le groupe G'_ℓ est un groupe de Lie ℓ-adique de dimension 3; c'est un sous-groupe ouvert du groupe $\mathbf{PGL}_2(\mathbf{Q}_\ell)$. La partie C′ est une sous-variété fermée de dimension $\leqslant 2$ (c'est l'ensemble des éléments d'ordre 2 de G'_ℓ). De plus, tous les éléments de C′ sont *réguliers* dans G'_ℓ : avec les notations du n° 5.1, on a $r(s) = 2$ pour tout $s \in C'$. On peut donc appliquer le th. 12 du § 5 au couple (G'_ℓ, C'), avec $r = 2$ et $\beta = (3-2)/(3-2/2) = 1/2$. D'où le résultat cherché, compte tenu de l'inégalité

$$P_{f,0}(x) \leqslant \pi_{C'}(x) + 1. \tag{192}$$

7.4. Non-lacunarité des formes modulaires — cas des fonctions propres des opérateurs de Hecke

Si $f = \Sigma a_n(f) q^n$ est une forme modulaire, et x un nombre réel $\geqslant 1$, nous poserons :

$$M_f(x) = \text{nombre des entiers } n \text{ tels que } 1 \leqslant n \leqslant x \text{ et } a_n(f) \neq 0. \tag{193}$$

Théorème 16. — Soit f un élément non nul de $M(N, k, \omega)$. *Supposons que f soit fonction propre des opérateurs* U_p *et* T_p, *que f ne soit pas de type* CM *au sens de* [31], *et que le poids k de f soit* $\geqslant 2$. *Il existe alors un nombre* $\alpha > 0$ *tel que*

$$M_f(x) \sim \alpha x \quad \textit{pour } x \to \infty. \tag{194}$$

En d'autres termes, l'ensemble des entiers n tels que $a_n(f) \neq 0$ a une *densité* α qui est > 0.

Démonstration

L'hypothèse faite sur f entraîne $a_1(f) \neq 0$, cf. par exemple [27]. Quitte à multiplier f par une constante, on peut donc supposer que $a_1(f) = 1$. On sait alors *(loc. cit.)* que, si l'on pose $a_p = a_p(f)$, on a

$$f \mid U_p = a_p f \quad \text{pour } p \mid N \quad \text{et} \quad f \mid T_p = a_p f \quad \text{pour } p \nmid N.$$

De plus, la fonction $n \mapsto a_n(f)$ est *multiplicative*. Distinguons deux cas :

a) *f est parabolique*

D'après le cor. 2 au th. 15, le nombre des $p \leqslant x$ tels que $a_p = 0$ est $O(x/(\log x)^{1+\delta})$, avec $\delta > 0$, par exemple $\delta = 1/3$. Le th. 13 du n° 6.1 s'applique donc à $n \mapsto a_n(f)$, avec $K = \mathbf{Q}$ et $\lambda = 0$; on obtient ainsi (194).

b) *f n'est pas parabolique*

C'est alors une série d'Eisenstein, et il existe un caractère χ mod N tel que

$$a_p = \chi(p) + \chi^{-1}(p)\omega(p)p^{k-1} \quad \text{si } p \nmid N.$$

Comme $k \geqslant 2$, cette formule montre que $a_p \neq 0$ pour tout p tel que $p \nmid N$, et l'on conclut comme ci-dessus. [Si S est l'ensemble des $p \mid N$ tels que $a_p = 0$, on peut montrer que $a_n(f) = 0$ si et seulement si l'un des facteurs premiers de n appartient à S; on a $M_f(x)\alpha = x + O(1)$, avec $\alpha = \prod_{p \in S}(1 - p^{-1})$.]

Calcul de la densité $\alpha = \lim_{x \to \infty} . x^{-1} M_f(x)$

Posons

$$a_n^0 = \begin{cases} 1 & \text{si } a_n(f) \neq 0 \\ 0 & \text{si } a_n(f) = 0 \end{cases} \tag{195}$$

et

$$\alpha_p = (1 - p^{-1})(1 + \sum_{m=1}^{\infty} a_{p^m}^0 / p^m). \tag{196}$$

D'après le n° 6.3, on a

$$\alpha = \prod_p \alpha_p. \tag{197}$$

Tout revient à calculer les α_p. Distinguons deux cas :

i) $p \mid N$

La formule $a_{p^m} = (a_p)^m$ entraîne

$$\alpha_p = \begin{cases} 1 - p^{-1} & \text{si } a_p = 0 \\ 1 & \text{si } a_p \neq 0. \end{cases} \tag{198}$$

ii) $p \nmid N$

Si β_p et γ_p sont tels que

$$1 - a_p T + \omega(p)p^{k-1}T^2 = (1 - \beta_p T)(1 - \gamma_p T),$$

on a

$$\begin{aligned} a_{p^m} &= \beta_p^m + \beta_p^{m-1}\gamma_p + \ldots + \gamma_p^m \\ &= (\beta_p^{m+1} - \gamma_p^{m+1})/(\beta_p - \gamma_p) \quad \text{si } \beta_p \neq \gamma_p. \end{aligned} \tag{199}$$

On en déduit que $a_{p^m} \neq 0$ sauf si β_p/γ_p est une racine de l'unité d'ordre $r(p) \geqslant 2$ et $m \equiv -1 \pmod{r(p)}$. D'où :

$$\alpha_p = \begin{cases} 1 \text{ si } \beta_p/\gamma_p = 1, \text{ ou si } \beta_p/\gamma_p \text{ n'est pas une racine de l'unité;} \\ 1-(p-1)/(p^{r(p)}-1) \text{ si } \beta_p/\gamma_p \text{ est une racine de l'unité d'ordre } r(p) \geqslant 2. \end{cases} \tag{200}$$

En particulier, $a_p = 0 \Leftrightarrow r(p) = 2 \Leftrightarrow \alpha_p = 1 - 1/(p+1)$.

Exemples

Je me borne à deux exemples où le caractère ω est égal à 1 (ce qui entraîne que k est pair), et où les coefficients de f appartiennent à $\mathbf{Z}$. On voit alors facilement que $r(p) \geqslant 3$ n'est possible que si :

a) $p = 2$, $a_2 = \pm 2^{k/2}$, auquel cas $r(2) = 4$ et $\alpha_2 = 14/15$;

b) $p = 3$, $a_3 = \pm 3^{k/2}$, auquel cas $r(3) = 6$ et $\alpha_3 = 363/364$.

Exemple 1 : $k = 2$, $N = 11$, $f = q\prod_{m=1}^{\infty}(1-q^m)^2(1-q^{11m})^2 = \eta^2(z)\eta^2(11z)$

On a $a_2 = -2$, $a_3 = -1$ et $a_{11} = -1$. D'où $\alpha_2 = 14/15$, $\alpha_3 = \alpha_{11} = 1$, et, pour $p \neq 2, 3, 11$, $\alpha_p = 1$ si $a_p \neq 0$ et $\alpha_p = 1 - 1/(p+1)$ si $a_p = 0$. La densité α des $n \geqslant 1$ pour lesquels $a_n(f) \neq 0$ est donc

$$\alpha = \prod_p \alpha_p = \frac{14}{15} \prod_{a_p = 0} \left(1 - \frac{1}{p+1}\right). \tag{201}$$

On trouvera dans Lang-Trotter [24], p. 267, la liste des $p \leqslant 2\,590\,717$ tels que $a_p = 0$. Ceux $\leqslant 40\,000$ sont : $p = 19$, 29, 199, 569, 809, 1 289, 1 439, 2 539, 3 319, 3 559, 3 919, 5 519, 9 419, 9 539, 9 929, 11 279, 11 549, 13 229, 14 489, 17 239, 18 149, 18 959, 19 319, 22 279, 24 359, 27 529, 28 789, 32 999, 33 029, 36 559.

Vu (201), on en déduit $\alpha < 0{,}847$. Il est *probable* que $\alpha \geqslant 0{,}845$, mais, pour le prouver, il conviendrait d'avoir une borne *explicite* (et non triviale) du nombre des $p \leqslant x$ tels que $a_p = 0$.

Exemple 2 : $k = 12$, $N = 1$, $f = \Delta = q\prod_{m=1}^{\infty}(1-q^m)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$

On a $\tau(2) = -24$ et $\tau(3) = 252$. D'où $\alpha_2 = \alpha_3 = 1$ et $\alpha_p = 1$ si $\tau(p) \neq 0$, $\alpha_p = 1 - 1/(p+1)$ si $\tau(p) = 0$. La densité α des n pour lesquels $\tau(n) \neq 0$ est donc :

$$\alpha = \prod_{\tau(p)=0} \left(1 - \frac{1}{p+1}\right). \tag{202}$$

En fait, on conjecture que $\tau(n) \neq 0$ pour tout $n \geqslant 1$, et l'on sait qu'il en est bien ainsi pour $n \leqslant 10^{15}$.

[Si τ s'annule, le plus petit entier p tel que $\tau(p)=0$ est un nombre premier; de plus, les congruences satisfaites par $\tau(p)$ montrent que p est de la forme $h\mathrm{M}-1$, avec $\mathrm{M}=2^{14}3^7 5^3 7^2 691$, et que $\left(\frac{p}{23}\right)=-1$, cf. [46]. Or les valeurs $h=1, 2, 3, 4, 5$ sont impossibles car $h\mathrm{M}-1$ n'est pas premier (il est divisible par 1 249, 79, 11, 4 789 et 131 respectivement); les valeurs $h=6, 7$ ne conviennent pas non plus, car $h\mathrm{M}-1$ est alors résidu quadratique mod 23; on a donc $h\geqslant 8$, d'où $p\geqslant 8\mathrm{M}-1>10^{15}$.]

Ainsi, il est *probable* que $\alpha=1$. D'après le th. 16, on a en tout cas $\alpha>0$; ici encore, pour avoir une minoration effective de α, il conviendrait d'avoir une borne explicite du nombre des $p\leqslant x$ tels que $\tau(p)=0$; c'est en principe faisable, mais je ne l'ai pas fait.

7.5. Formes de type CM

Soit $f\in \mathrm{M}(\mathrm{N}, k, \omega)$, $f\neq 0$. Supposons que f soit fonction propre des U_p et T_p, que $k\geqslant 2$, et que f soit de type CM.

Proposition 18. — Sous les hypothèses ci-dessus, il existe un nombre $\alpha>0$ tel que

$$\mathrm{M}_f(x)\sim \alpha x/(\log x)^{1/2} \quad \textit{pour } x\to\infty. \tag{203}$$

Comme pour le th. 16, on peut supposer que $a_1(f)=1$, auquel cas la fonction $n\mapsto a_n(f)$ est multiplicative. Soit L l'extension quadratique de $\mathbf{Q}$ associée à f, cf. Ribet [33]. Il résulte de [33] que, pour $p\nmid \mathrm{N}$, on a $a_p(f)=0$ si et seulement si p est inerte dans l'extension $\mathrm{L}/\mathbf{Q}$. Le nombre des $p\leqslant x$ tels que $a_p(f)=0$ est donc égal à $\frac{1}{2}x/\log x+O(x/(\log x)^2)$ pour $x\to\infty$. En appliquant le th. 13 avec $\mathrm{K}=\mathbf{Q}$ et $\lambda=1/2$, on obtient (203).

Remarque

L'emploi de la méthode de Landau ([42], th. 2.8) conduit à un résultat plus précis : la fonction $\mathrm{M}_f(x)$ possède un *développement asymptotique*

$$\mathrm{M}_f(x)=\frac{x}{(\log x)^{1/2}}(\alpha+\alpha_1/\log x+\dots).$$

7.6. Non-lacunarité des formes modulaires en poids $\geqslant 2$

Rappelons d'abord que l'espace $\mathrm{M}(\mathrm{N}, k, \omega)$ des formes de type (k, ω) sur $\Gamma_0(\mathrm{N})$ se décompose en somme directe

$$\mathrm{M}(\mathrm{N}, k, \omega)=\mathrm{S}(\mathrm{N}, k, \omega)\oplus \mathrm{E}(\mathrm{N}, k, \omega), \tag{204}$$

où $\mathrm{S}(\mathrm{N}, k, \omega)$ est le sous-espace des formes paraboliques, et $\mathrm{E}(\mathrm{N}, k, \omega)$ le sous-espace des séries d'Eisenstein. Cette décomposition est stable par les U_p et les T_p.

Soit $\mathfrak{M}=\mathfrak{M}(\mathrm{N}, \omega)$ l'ensemble des diviseurs positifs M de N tels que le conducteur de ω divise M. Si $\mathrm{M}\in\mathfrak{M}$, soit ω_M le caractère mod M qui coïncide avec ω sur les entiers premiers à N, et soit P_M l'ensemble des formes primitives (« newforms », cf. Li [27])

de niveau M et de type (k, ω_M); si $f \in P_M$, on suppose f normalisée de telle sorte que $a_1(f) = 1$. Soit d un diviseur positif de N/M; si $f \in P_M$, la forme modulaire f_d définie par

$$f_d(z) = f(dz)$$

appartient à $S(N, k, \omega)$. De plus, les formes f_d (pour M parcourant $\mathfrak{M}$, $f \in P_M$ et d diviseur de N/M) forment une *base* du **C**-espace vectoriel $S(N, k, \omega)$, cf. [27]. Nous noterons $S_{cm}(N, k, \omega)$ (resp. $S_{cm}^{non}(N, k, \omega)$) le sous-espace de $S(N, k, \omega)$ engendré par les f_d où f est de type CM (resp. n'est pas de type CM). On a

$$S(N, k, \omega) = S_{cm}^{non}(N, k, \omega) \oplus S_{cm}(N, k, \omega). \tag{205}$$

Ici encore, cette décomposition est stable par les U_p et les T_p : cela résulte des formules suivantes, valables pour tout $M \in \mathfrak{M}$, tout $f \in P_M$ et tout diviseur positif d de N/M :

$$f_d | T_p = a_p(f) f_d \quad \text{si } p \nmid N, \tag{206}$$

$$f_d | U_p = \begin{cases} f_{d/p} & \text{si } p | d, \\ a_p(f) f_d & \text{si } p \nmid d \text{ et } p | M, \\ a_p(f) f_d - \omega_M(p) p^{k-1} f_{dp} & \text{si } p \nmid dM \text{ et } p | N. \end{cases} \tag{207}$$

En combinant (204) et (205), on obtient :

$$M(N, k, \omega) = S_{cm}^{non}(N, k, \omega) \oplus S_{cm}(N, k, \omega) \oplus E(N, k, \omega). \tag{208}$$

Théorème 17. — *Soit* $f \in M(N, k, \omega)$, *avec* $k \geqslant 2$.

(i) *Si* $f \notin S_{cm}(N, k, \omega)$, *on a*

$$M_f(x) \asymp x \quad \textit{pour } x \to \infty. \tag{209}$$

(ii) *Si* $f \in S_{cm}(N, k, \omega)$ *et* $f \neq 0$, *on a*

$$M_f(x) \asymp x/(\log x)^{1/2} \quad \textit{pour } x \to \infty. \tag{210}$$

Rappelons que $M_f(x)$ désigne le nombre des entiers n tels que $1 \leqslant n \leqslant x$ et $a_n(f) \neq 0$; quant à la notation « $\varphi \asymp \psi$ », elle équivaut à « $\varphi = O(\psi)$ et $\psi = O(\varphi)$ », cf. par exemple Bourbaki, *Fonct. var. réelle*, chap. V, § 1, déf. 2.

Corollaire. — *Si* $f \notin S_{cm}(N, k, \omega)$ *et* $k \geqslant 2$, *l'ensemble des n tels que* $a_n(f) \neq 0$ *a une densité inférieure qui est* > 0.

Ce n'est qu'une reformulation de (i).

Remarque. — Ce corollaire est notamment applicable lorsque $N = 1$ et $f \neq 0$; en effet, il n'existe pas de forme de niveau 1 de type CM. Même chose lorsque N est un nombre premier congru à 1 mod 4.

Démonstration du th. 17

Il est clair que $M_f(x) = O(x)$, et la prop. 18 montre que

$$M_f(x) = O(x/(\log x)^{1/2}) \quad \text{si } f \in S_{cm}(N, k, \omega). \tag{211}$$

Pour prouver le th. 17, il suffit donc d'établir que :

$$\lim.\inf_{x\to\infty} x^{-1}M_f(x) > 0 \quad \text{si } f \notin S_{cm}(N, k, \omega)$$

et

$$\lim.\inf_{x\to\infty} x^{-1}M_f(x)(\log x)^{1/2} > 0 \quad \text{si } f \in S_{cm}(N, k, \omega),\ f \neq 0.$$

Posons :

$$R_0 = \text{ensemble des } f \text{ tels que } \lim.\inf_{x\to\infty} x^{-1}M_f(x) = 0$$

$$R_{1/2} = \text{ensemble des } f \text{ tels que } \lim.\inf_{x\to\infty} x^{-1}M_f(x)(\log x)^{1/2} = 0.$$

Il s'agit de montrer que $R_0 = S_{cm}(N, k, \omega)$ et $R_{1/2} = 0$. Soit $\mathfrak{H}$ la $\mathbf{C}$-algèbre d'endomorphismes de $M(N, k, \omega)$ engendrée par les U_p et les T_p.

Lemme 9. — Les ensembles R_0 *et* $R_{1/2}$ *sont stables par* $\mathfrak{H}$.

Les formules (172) et (173) montrent que, si $g = f|U_p$ ou $f|T_p$, on a

$$M_g(x) \leqslant M_f(px) + M_f(x/p) \leqslant 2M_f(mx) \quad \text{pour tout } m \geqslant p. \tag{212}$$

En itérant cette formule, et en tenant compte de l'inégalité

$$M_{g+h}(x) \leqslant M_g(x) + M_h(x), \tag{213}$$

on en déduit que, pour tout $A \in \mathfrak{H}$, il existe des entiers c_A et m_A strictement positifs tels que

$$M_{Af}(x) \leqslant c_A M_f(m_A x) \quad \text{pour tout } f \in M(N, k, \omega). \tag{214}$$

Si $f \in R_0$, il existe une suite x_α tendant vers $+\infty$ telle que $x_\alpha^{-1}M_f(x_\alpha) \to 0$. Si l'on pose $y_\alpha = m_A^{-1}x_\alpha$, la formule (214) montre que $y_\alpha^{-1}M_{Af}(y_\alpha) \to 0$. On a donc $Af \in R_0$, ce qui prouve que R_0 est stable par $\mathfrak{H}$. On raisonne de même pour $R_{1/2}$.

Ce lemme étant établi, revenons à la démonstration du th. 17 (i). On a vu que R_0 *contient* $S_{cm}(N, k, \omega)$, et il s'agit de prouver qu'il y a *égalité*. Supposons donc que f appartienne à R_0, mais pas à $S_{cm}(N, k, \omega)$. Écrivons f sous la forme

$$f = g + h, \quad \text{avec} \quad g \in S_{cm}^{non}(N, k, \omega) \oplus E(N, k, \omega) \quad \text{et} \quad h \in S_{cm}(N, k, \omega).$$

On a $M_g(x) \leqslant M_f(x) + M_h(x)$. Comme $M_h(x) = o(x)$ d'après (211), et que

$$\lim.\inf x^{-1}M_f(x) = 0,$$

on a $\lim.\inf x^{-1}M_g(x) = 0$, d'où $g \in R_0$. Par hypothèse, g est $\neq 0$. Le sous-$\mathfrak{H}$-module $\mathfrak{H}g$ engendré par g contient un sous-module simple Σ; comme $\mathfrak{H}$ est une algèbre commutative, Σ est de dimension 1 sur $\mathbf{C}$. Si f' est un élément non nul de Σ, f' est vecteur propre des U_p et des T_p; comme f' est contenu dans $\mathfrak{H}g$, le lemme 9 montre que f' appartient à R_0, i.e. que $\lim.\inf x^{-1}M_{f'}(x) = 0$. Mais f' est contenu dans $S_{cm}^{non}(N, k, \omega) \oplus E(N, k, \omega)$ donc n'est pas de type CM; d'après le th. 16, $x^{-1}M_{f'}(x)$ a une limite >0 quand $x \to \infty$. Cette contradiction montre que $R_0 = S_{cm}(N, k, \omega)$ d'où le th. 17 (i).

La partie (ii) du th. 17 se démontre de la même manière : si $R_{1/2}$ est $\neq 0$, l'argument ci-dessus montre qu'il contient un $f' \neq 0$ qui est vecteur propre des U_p et des T_p; un tel f' contredit la prop. 18 s'il est de type CM, et le th. 16 s'il ne l'est pas. On a donc bien $R_{1/2} = 0$.

Questions

1) Peut-on donner un *développement asymptotique* de $M_f(x)$? En particulier, est-il vrai que $x^{-1}M_f(x)$ *a une limite* pour $x \to \infty$? La même question se pose pour $x^{-1}M_f(x)(\log x)^{1/2}$ lorsque f appartient à $S_{cm}(N, k, \omega)$.

2) (« Lacunes »). Supposons $f \neq 0$. Pour tout entier $n \geqslant 1$, notons $i_f(n)$ le plus grand entier $\geqslant 0$ tel que

$$a_{n+i}(f) = 0 \quad \text{pour tout } i \text{ tel que } 0 < i \leqslant i_f(n).$$

Si $f \notin S_{cm}(N, k, \omega)$ et $k \geqslant 2$, le th. 17 (i) entraîne :

$$i_f(n) = O(n) \quad \text{pour } n \to \infty. \tag{215}$$

Peut-on améliorer cette majoration, et prouver par exemple :

$$i_f(n) = O(n/(\log n)^m) \quad \text{pour tout } m \geqslant 0, \tag{216?}$$

ou même :

$$i_f(n) = O(n^\delta) \quad \text{avec } \delta < 1 \text{ ?} \tag{217?}$$

3) Y a-t-il des résultats analogues pour les formes de poids $\geqslant 2$ (non nécessairement entier) sur d'autres sous-groupes de $\mathbf{SL}_2(\mathbf{Z})$, ou plus généralement d'autres groupes fuchsiens ? Voir là-dessus Knopp-Lehner [21], qui contient un certain nombre d'exemples.

7.7. Formes paraboliques de poids 1

Dans ce numéro, on suppose que le poids k est égal à 1 ; pour simplifier, on ne considère que des formes paraboliques (il y a des résultats analogues pour les séries d'Eisenstein).

Fonctions propres des opérateurs de Hecke

Soit f un élément non nul de $S(N, 1, \omega)$. Supposons que f soit fonction propre des T_p, $p \nmid N$, avec pour valeurs propres a_p. On sait ([9], [43]) qu'il existe alors une représentation irréductible continue

$$\rho : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{C})$$

qui est non ramifiée en dehors de N, et telle que

$$\mathrm{Tr}\, \rho(\sigma_p) = a_p \quad \text{et} \quad \det \rho(\sigma_p) = \omega(p) \quad \text{pour tout } p \nmid N. \tag{218}$$

Ces propriétés caractérisent ρ à isomorphisme près.

Le groupe $G = \mathrm{Im}(\rho)$ est un sous-groupe fini de $\mathbf{GL}_2(\mathbf{C})$. Son image PG dans $\mathbf{PGL}_2(\mathbf{C}) = \mathbf{GL}_2(\mathbf{C})/\mathbf{C}^*$ est isomorphe à l'un des groupes suivants :

groupe diédral $\mathbf{D}_n$ d'ordre $2n$ $(n \geqslant 2)$,

groupe alterné $\mathfrak{A}_4$,

groupe symétrique $\mathfrak{S}_4$,

groupe alterné $\mathfrak{A}_5$.

Nous dirons, suivant les cas, que f est *de type* $\mathbf{D}_n$, $\mathfrak{A}_4$, $\mathfrak{S}_4$ *ou* $\mathfrak{A}_5$; les types $\mathfrak{A}_4$, $\mathfrak{S}_4$ et $\mathfrak{A}_5$ sont parfois appelés « exotiques ».

Si PG_2 désigne l'ensemble des éléments d'ordre 2 du groupe PG (images des éléments de G de trace 0), nous poserons

$$\lambda = |\mathrm{PG}_2|/|\mathrm{PG}|. \tag{219}$$

On a

$$\lambda = \begin{cases} 1/2 + 1/2n & \text{si} \quad \mathrm{PG} \simeq \mathbf{D}_n \quad (n \text{ pair} \geqslant 2) \\ 1/2 & \text{si} \quad \mathrm{PG} \simeq \mathbf{D}_n \quad (n \text{ impair} \geqslant 3) \\ 3/8 & \text{si} \quad \mathrm{PG} \simeq \mathfrak{S}_4 \\ 1/4 & \text{si} \quad \mathrm{PG} \simeq \mathfrak{A}_4 \text{ ou } \mathfrak{A}_5. \end{cases} \tag{220}$$

Théorème 18. — *Soit f un élément non nul de* $\mathrm{S}(\mathrm{N}, 1, \omega)$. *Supposons f fonction propre des opérateurs* U_p *et* T_p. *Il existe alors un nombre* $\alpha > 0$ *tel que*

$$\mathrm{M}_f(x) \sim \alpha x/(\log x)^{\lambda} \quad \textit{pour} \quad x \to \infty, \tag{221}$$

où λ *est défini par les formules* (219) *et* (220) *ci-dessus.*

Ce résultat est démontré dans [42], th. 4.2, qui donne même un développement asymptotique pour $\mathrm{M}_f(x)$. On peut aussi le déduire du th. 13 du n° 6.1, en remarquant que l'ensemble des p tels que $a_p = 0$ est *frobénien* ([42], (1.4)) de densité λ.

Remarque. — Les formes les moins « lacunaires » sont les formes de type exotique, pour lesquelles λ est $< 1/2$. Les plus lacunaires sont celles de type $\mathbf{D}_2$, où $\lambda = 3/4$ (cf. fin du n° 6.5); pour un exemple explicite (et le calcul de la constante α correspondante), voir n° 7.8 ci-après.

Cas général

Revenons à la base (f_d) de $\mathrm{S}(\mathrm{N}, 1, \omega)$ définie au n° 7.6. Si ν est un nombre donné, avec $0 < \nu < 1$, notons $\mathrm{S}^{\nu}(\mathrm{N}, 1, \omega)$ le sous-espace de $\mathrm{S}(\mathrm{N}, 1, \omega)$ qui a pour base les f_d tels que l'invariant λ de f soit égal à ν. On a évidemment

$$\mathrm{S}(\mathrm{N}, 1, \omega) = \bigoplus_{\nu} \mathrm{S}^{\nu}(\mathrm{N}, 1, \omega). \tag{222}$$

Si l'on pose

$$\mathrm{S}_{\mu}(\mathrm{N}, 1, \omega) = \bigoplus_{\nu \geqslant \mu} \mathrm{S}^{\nu}(\mathrm{N}, 1, \omega), \tag{223}$$

on obtient une *filtration décroissante* de l'espace $S(N, 1, \omega)$; on a

$$S_{1/4}(N, 1, \omega) = S(N, 1, \omega) \quad \text{et} \quad S_\mu(N, 1, \omega) = 0 \quad \text{si} \quad \mu > 3/4.$$

Un élément $f \neq 0$ de $S(N, 1, \omega)$ est dit *de filtration* λ s'il appartient à $S_\lambda(N, 1, \omega)$, et s'il n'appartient pas à $S_\mu(N, 1, \omega)$ pour $\mu > \lambda$.

Théorème 19. — Si f est un élément non nul de $S(N, 1, \omega)$ de filtration λ, on a

$$M_f(x) \asymp x/(\log x)^\lambda \quad \textit{pour } x \to \infty. \tag{224}$$

Le th. 18 entraîne que $M_f(x) = O(x/(\log x)^\lambda)$, et il faut montrer que

$$\lim.\inf x^{-1} M_f(x) (\log x)^\lambda > 0.$$

On procède comme pour la démonstration du th. 17. On pose :

$$R_\lambda = \text{ensemble des } f \text{ tels que } \lim.\inf x^{-1} M_f(x) (\log x)^\lambda = 0.$$

Si $S_\lambda^+(N, 1, \omega)$ désigne la réunion des $S_\mu(N, 1, \omega)$ pour $\mu > \lambda$, on a $R_\lambda \supset S_\lambda^+(N, 1, \omega)$, et il s'agit de prouver qu'il y a *égalité*. Or R_λ jouit des deux propriétés suivantes :

(i) $f \in R_\lambda$ et $g \in S_\lambda^+(N, 1, \omega) \Rightarrow f + g \in R_\lambda$ (immédiat);
(ii) R_λ est stable par l'algèbre $\mathfrak{H}$ engendrée par les U_p et les T_p (cela se démontre comme le lemme 9, en utilisant (214)).

En combinant (i) et (ii) on en déduit (cf. démonstration du th. 17) que, si R_λ est distinct de $S_\lambda^+(N, 1, \omega)$, il contient un élément non nul f' qui est vecteur propre des U_p et des T_p et qui appartient à la somme directe des $S^\nu(N, 1, \omega)$ pour $\nu \geqslant \lambda$. Un tel f' contredit le th. 18. On a donc bien $R_\lambda = S_\lambda^+(N, 1, \omega)$, ce qui démontre le th. 19.

7.8. Exemple : $f = q \prod_{m=1}^{\infty} (1 - q^{12m})^2 = \eta^2(12z)$

On a :

$$f = q - 2q^{13} - q^{25} + 2q^{37} + q^{49} + 2q^{61} - 2q^{73} - 2q^{97} - 2q^{109} + q^{121} + 2q^{157} + 3q^{169} - 2q^{181} + 2q^{193} - 2q^{229} - 2q^{241} - \dots$$

La forme f est une forme parabolique de poids 1, de niveau $N = 2^4 3^2$ et de caractère ω tel que $\omega(p) = (-1)^{(p-1)/2}$ si $p \geqslant 5$. Elle est fonction propre des U_p ($p = 2, 3$) et des T_p ($p \geqslant 5$). La représentation correspondante est de type $\mathbf{D}_2$; elle est décrite dans [43], p. 242-244. L'exposant λ est égal à 3/4. D'après le th. 18, on a

$$M_f(x) \sim \alpha x/(\log x)^{3/4}, \quad \text{avec } \alpha > 0. \tag{225}$$

Nous allons calculer α :

Proposition 19. — On a

$$\alpha = \{2^{-1} 3^{-7} \pi^6 \log(2 + \sqrt{3})\}^{1/4} A^{1/2} / \Gamma(1/4), \tag{226}$$

avec $A = \prod_{p \equiv 1 \pmod{12}} (1 - p^{-2})$.

Un calcul approché de A, basé sur $p \leqslant 25\,000$, donne $A = 0{,}992\,44\ldots$ Comme $\Gamma(1/4) = 3{,}625\,609\,9\ldots$ et $\log(2+\sqrt{3}) = 1{,}316\,957\ldots$, on en déduit :

$$\alpha = 0{,}201\,54\ldots \tag{226'}$$

Démonstration de la prop. 19

L'extension galoisienne correspondant au groupe $PG \simeq \mathbf{D}_2$ est le corps des racines 12-ièmes de l'unité $E = \mathbf{Q}(\sqrt{-1}, \sqrt{3})$, cf. [43], p. 243. On en déduit que, pour $p \geqslant 5$, la valeur propre a_p de T_p est $\neq 0$ si et seulement si p est totalement décomposé dans $E/\mathbf{Q}$, i.e. si $p \equiv 1 \pmod{12}$. D'autre part, les valeurs propres de U_2 et U_3 sont nulles. On déduit de là que $a_n(f)$ est $\neq 0$ si et seulement si $v_p(n) = 0$ pour $p = 2, 3$ et $v_p(n) \equiv 0 \pmod 2$ pour tout $p \equiv 5, 7$ ou $11 \pmod{12}$.

Posons alors, comme au n° 6.2 :

$$\varphi(s) = \sum_{n=1}^{\infty} a_n^0(f) n^{-s},$$

où $a_n^0(f)$ est égal à 0 ou 1 suivant que $a_n(f)$ est 0 ou $\neq 0$. Vu ce qui précède, on a :

$$\varphi(s) = \prod_p \varphi_p(s), \tag{227}$$

avec

$$\varphi_p(s) = \begin{cases} 1 & \text{si} \quad p = 2 \text{ ou } 3, \\ 1/(1-p^{-s}) & \text{si} \quad p \equiv 1 \pmod{12} \\ 1/(1-p^{-2s}) & \text{si} \quad p \equiv 5, 7 \text{ ou } 11 \pmod{12}. \end{cases} \tag{228}$$

D'après le lemme 5 du n° 6.2, il existe une constante $u > 0$ telle que

$$\varphi(s) \sim u/(s-1)^{1/4} \quad \text{pour } s \to 1 \ (s \text{ réel} > 1), \tag{229}$$

et d'après (143) on a

$$\alpha = u/\Gamma(1/4). \tag{230}$$

Tout revient donc à calculer u.

Soit $\zeta_E(s)$ la fonction zêta du corps E. On a

$$\zeta_E(s) = \prod_p \zeta_{E,p}(s),$$

avec

$$\zeta_{E,p}(s) = \begin{cases} 1/(1-p^{-2s}) & \text{si} \quad p = 2 \text{ ou } 3 \\ 1/(1-p^{-s})^4 & \text{si} \quad p \equiv 1 \pmod{12} \\ 1/(1-p^{-2s})^2 & \text{si} \quad p \equiv 5, 7, 11 \pmod{12}. \end{cases} \tag{231}$$

En comparant (228) et (231), on voit que

$$\varphi(s)^4 = \zeta_E(s)\psi(s), \tag{232}$$

avec

$$\psi(s) = \prod_{p=2,3} (1-p^{-2s}) \prod_{p \equiv 5, 7, 11 \pmod{12}} (1-p^{-2s})^{-2}. \tag{233}$$

La fonction ψ est holomorphe et non nulle en $s=1$. Si κ désigne le résidu de $\zeta_E(s)$ en $s=1$, la formule (232) montre que

$$\varphi(s)\sim(\kappa\psi(1))^{1/4}/(s-1)^{1/4} \quad \text{pour } s\to 1,$$

d'où

$$u=(\kappa\psi(1))^{1/4}. \tag{234}$$

Le résidu κ se calcule sans difficulté : on a

$$\kappa=L_\omega(1)L_\chi(1)L_{\chi\omega}(1), \tag{235}$$

où $L_\omega(s)$, $L_\chi(s)$ et $L_{\omega\chi}(s)$ sont les fonctions L associées aux trois corps quadratiques $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{3})$ et $\mathbf{Q}(\sqrt{-3})$. On trouve

$$L_\omega(1)=\pi/4, \quad L_\chi(1)=(\log(2+\sqrt{3}))/\sqrt{3} \quad \text{et} \quad L_{\omega\chi}(1)=\pi/3\sqrt{3},$$

d'où :

$$\kappa=\frac{\pi^2}{36}\log(2+\sqrt{3}). \tag{236}$$

On a d'autre part

$$\psi(1)=(1-1/4)(1-1/9)\prod_{p\equiv 5,\,7,\,11 \pmod{12}}(1-p^{-2})^{-2},$$

d'où, en multipliant par A^{-2} :

$$\begin{aligned}\psi(1)A^{-2}&=(1-1/4)^3(1-1/9)^3\prod_p(1-p^{-2})^{-2}\\&=(3/4)^3(8/9)^3(\pi^2/6)^2,\end{aligned}$$

i.e.

$$\psi(1)=2\cdot 3^{-5}\pi^4A^2.$$

En combinant cette égalité avec (234) et (236), on obtient

$$u^4=2^{-1}3^{-7}\pi^6A^2\log(2+\sqrt{3}),$$

d'où le résultat cherché, d'après (230).

§ 8. Applications aux courbes elliptiques

8.1. Notations et rappels (cf. [24], [28], [31], [40], [41])

Soit E une courbe elliptique sur $\mathbf{Q}$.

On note S_E l'ensemble des nombres premiers en lesquels E a mauvaise réduction; c'est un ensemble fini, qui est non vide d'après un théorème de Šafarevič ([35], voir aussi Ogg [31]).

Si p est un nombre premier n'appartenant pas à S_E, on note $\tilde{E}(p)$ la réduction de E en p, π_p l'endomorphisme de Frobenius de $\tilde{E}(p)$, et a_p la trace de π_p; on a

$$a_p = 1 + p - A_p(E), \tag{237}$$

où $A_p(E)$ est le nombre de points de $\tilde{E}(p)$ sur le corps $\mathbf{F}_p$.

Si n est un entier $\geqslant 1$, on note E_n le groupe des points $x \in E(\bar{\mathbf{Q}})$ tels que $nx = 0$; l'action de $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ sur E_n définit un homomorphisme continu

$$\varphi_n : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(E_n) \simeq \mathbf{GL}_2(\mathbf{Z}/n\mathbf{Z}).$$

Soit $S_{E,n}$ la réunion de S_E et de l'ensemble des diviseurs premiers de n. L'homomorphisme φ_n est non ramifié en dehors de $S_{E,n}$; si $p \notin S_{E,n}$, on a

$$\mathrm{Tr}\ \varphi_n(\sigma_p) \equiv a_p \pmod{n} \quad \text{et} \quad \det \varphi_n(\sigma_p) \equiv p \pmod{n}, \tag{238}$$

où σ_p désigne la substitution de Frobenius de p.

Si ℓ est un nombre premier, les représentations φ_{ℓ^m} définissent par passage à la limite une représentation ℓ-adique

$$\rho_\ell : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \varprojlim \mathrm{Aut}(E_{\ell^m}) \simeq \mathbf{GL}_2(\mathbf{Z}_\ell).$$

Cette représentation est non ramifiée en dehors de $S_{E,\ell}$, et l'on a, d'après (238) :

$$\mathrm{Tr}\ \rho_\ell(\sigma_p) = a_p \quad \text{et} \quad \det \rho_\ell(\sigma_p) = p \quad \text{si } p \notin S_{E,\ell}. \tag{239}$$

Lorsque E n'a pas de multiplication complexe, i.e. lorsque $\mathrm{End}_{\bar{\mathbf{Q}}} E = \mathbf{Z}$, le groupe $G_\ell = \mathrm{Im}(\rho_\ell)$ est *ouvert* dans $\mathbf{GL}_2(\mathbf{Z}_\ell)$, et l'on a $G_\ell = \mathbf{GL}_2(\mathbf{Z}_\ell)$ pour tout ℓ sauf un nombre fini (cf. [41]).

8.2. Nombre des $p \leqslant x$ tels que a_p ait une valeur donnée

Soit $h \in \mathbf{Z}$. Si x est un nombre réel $\geqslant 2$, posons

$$P_{E,h}(x) = \text{nombre des } p \leqslant x \text{ tels que } p \notin S_E \text{ et } a_p = h. \tag{240}$$

Théorème 20. — Supposons que E *n'ait pas de multiplication complexe. On a alors*

$$P_{E,h}(x) = O(\mathrm{Li}(x)/\varepsilon(x)^{1/4}) \quad \textit{pour } x \to \infty, \tag{241}$$

et, sous (GRH) :

$$P_{E,h}(x) = O(\mathrm{Li}(x)/\varepsilon_R(x)^{1/4}) \quad \textit{pour } x \to \infty, \tag{242$_R$}$$

où $\varepsilon(x)$ *et* $\varepsilon_R(x)$ *sont les fonctions définies au* n° 4.1.

De plus, lorsque $h \neq \pm 2$, *on peut remplacer l'exposant* 1/4 *de* (241) *et* (242$_R$) *par* 1/3, *et lorsque* $h = 0$, *on peut le remplacer par* 1/2.

En particulier :

Corollaire 1. — Si $h \neq \pm 2$, *on a*

$$P_{E,h}(x) = O(x/(\log x)^{4/3-\delta}) \quad \textit{pour tout } \delta > 0, \tag{243}$$

et, sous (GRH),

$$P_{E,h}(x) = O(x^{5/6}/(\log x)^{1/3}). \tag{244$_R$}$$

Corollaire 2. — On a

$$P_{E,0}(x) = O(x/(\log x)^{3/2-\delta}) \quad \textit{pour tout } \delta > 0, \tag{245}$$

et, sous (GRH),

$$P_{E,0}(x) = O(x^{3/4}). \tag{246$_R$}$$

Démonstration du th. 20

C'est essentiellement la même que celle du th. 15 :

i) *Cas général*

On choisit un nombre premier ℓ. On applique le th. 10 du n° (4.1) au groupe de Galois $G_\ell = \mathrm{Im}(\rho_\ell)$, et à la partie $C_{\ell,h}$ de G_ℓ formée des éléments $s \in G_\ell$ tels que $\mathrm{Tr}(s) = h$. Avec les notations du n° (4.1), on a $\dim G_\ell = 4$, $\dim C_{\ell,h} = 3$, d'où $\alpha = 1/4$, et l'on obtient le résultat cherché.

ii) *Le cas* $h \neq 0, 2, -2$

On choisit ℓ de la manière suivante :

ii$_1$) $\ell = 2$ si h est de la forme $\pm 2^m$, $m = 0$ ou $m \geqslant 2$;
ii$_2$) $\ell =$ facteur premier impair de h sinon.

On définit G_ℓ et $C_{\ell,h}$ comme dans le cas i).

Lemme 10. — Pour tout $s \in C_{\ell,h}$, *on a* $\mathrm{Tr}(s)^2 - 4\det(s) \neq 0$.

Supposons que $\mathrm{Tr}(s)^2 = 4\det(s)$. Comme $\mathrm{Tr}(s) = h$, et que $\det(s)$ est une unité ℓ-adique, on en conclut que $v_\ell(h) = v_\ell(2)$, où v_ℓ désigne la valuation ℓ-adique. Mais c'est impossible :

dans le cas ii_1), on a $v_\ell(2) = 1$ et $v_\ell(h) \neq 1$,
dans le cas ii_2), on a $v_\ell(2) = 0$ et $v_\ell(h) \geq 1$.

D'où le lemme.

Ainsi, pour tout $s \in C_{\ell,h}$, les valeurs propres de s sont distinctes : l'élément s est « régulier » dans $\mathbf{GL}_2$, et la dimension $r(s)$ de sa classe de conjugaison est égale à 2. On peut alors appliquer le th. 12 du n° 5.1 avec

$$\beta = (4-3)/(4-2/2) = 1/3,$$

et l'on a bien remplacé l'exposant 1/4 par 1/3.

iii) *Le cas* $h = 0$

On procède comme dans le cas i), mais l'on remplace le groupe G_ℓ par son image G'_ℓ dans $\mathbf{PGL}_2(\mathbf{Z}_\ell)$, qui est un groupe de Lie de dimension 3, cf. n° 7.3, iii). Cela a pour effet de remplacer $C_{\ell,0}$ par l'ensemble C'_ℓ des éléments de G'_ℓ d'ordre 2; comme les éléments de C'_ℓ sont réguliers dans $\mathbf{PGL}_2$, on peut appliquer le th. 12 du n° 5.1, avec

$$\beta = (3-2)/(3-2/2) = 1/2.$$

D'où le résultat cherché.

Remarques

1) A la place de la représentation ℓ-adique ρ_ℓ (avec ℓ fixé), on peut utiliser les représentations φ_ℓ (avec ℓ variable) à valeurs dans les groupes $\mathbf{GL}_2(\mathbf{F}_\ell)$. Grâce au th. 11 du n° 4.6, on obtient ainsi les formules (241) et (242_R) du th. 20, avec le même exposant $\alpha = 1/4$. Toutefois, je ne sais pas obtenir par cette méthode les améliorations de α données ci-dessus pour $h \neq \pm 2$.

2) Le th. 20 s'étend aux courbes elliptiques définies sur un corps de nombres quelconque. La démonstration est la même.

3) Disons que l'entier h est *permis* (pour la courbe E) si, pour tout $n \geq 1$, il existe $s \in \mathrm{Im}(\varphi_n)$ tel que $\mathrm{Tr}(s) \equiv h \pmod{n}$. Par exemple, 2 et 0 sont permis (prendre pour s l'élément neutre, et la conjugaison complexe, respectivement); 1 n'est pas toujours permis.

Si h n'est pas permis, la formule (238) montre que $a_p \neq h$ pour tout p assez grand; on a $P_{E,h}(x) = O(1)$.

Par contre, si h est permis, il est vraisemblable que $P_{E,h}(x)$ *tend vers l'infini* avec x. Lang et Trotter ([24]) ont même conjecturé que

$$(247_?) \qquad P_{E,h}(x) \sim C_h(E)\, x^{1/2}/\log x \quad \text{pour } x \to \infty,$$

où $C_h(E)$ est un nombre >0 dont on trouvera la valeur dans [24]. La majoration de $P_{E,h}(x)$ donnée par le th. 20 n'est donc probablement pas optimale, même sous (GRH), et même dans le cas le plus favorable, qui est $h=0$ (cas « supersingulier »).

4) Soit K un corps quadratique imaginaire. Notons $P_{E,K}(x)$ le nombre des $p\leqslant x$, $p\notin S_E$, tels que le corps $\mathbf{Q}(\pi_p)$ engendré par l'endomorphisme de Frobenius de $\tilde{E}(p)$ soit isomorphe à K. Dans [24], Lang et Trotter conjecturent que

$$(248_?) \qquad P_{E,K}(x)\sim C_K(E)\,x^{1/2}/\log x, \quad \text{avec } C_K(E)>0.$$

Cette conjecture semble au moins aussi difficile que la précédente — elle-même analogue au classique problème des nombres premiers de la forme $1+n^2$. A défaut de la démontrer, on peut se demander si l'on peut donner une *majoration* non triviale de $P_{E,K}(x)$ pour $x\to\infty$. Il en est bien ainsi. On peut prouver que :

$$(249) \qquad P_{E,K}(x)=O(x/(\log x)^\gamma) \quad \text{avec } \gamma>1,$$

et, sous (GRH) :

$$(250_R) \qquad P_{E,K}(x)=O(x^\delta) \quad \text{avec } \delta<1.$$

La démonstration combine des arguments de style « Chebotarev » avec une technique de crible à la Selberg; elle est trop longue pour être donnée ici.

8.3. Comparaison de deux courbes elliptiques

Soient E et E′ deux courbes elliptiques sur $\mathbf{Q}$. Nous conservons pour E les notations S_E, a_p, E_n, φ_n, ρ_ℓ définies au n° 8.1, et nous utilisons pour E′ les notations analogues $S_{E'}$, a'_p, E'_n, φ'_n et ρ'_ℓ. Deux cas sont possibles :

(a) les représentations ℓ-adiques ρ_ℓ et ρ'_ℓ sont isomorphes (pour un ℓ, ou pour tout ℓ, cela revient au même, cf. [40], p. IV-15); on a alors $S_E=S_{E'}$ et $a_p=a'_p$ pour tout $p\notin S_E$;

(b) les représentations ρ_ℓ et ρ'_ℓ ne sont pas isomorphes; l'ensemble des p tels que $a_p\neq a'_p$ est alors de densité >0 ([40], *loc. cit.*).

Le cas *(a)* se produit lorsque E et E′ sont $\mathbf{Q}$-isogènes. On conjecture qu'il ne se produit que dans ce cas, mais on ne sait le démontrer que lorsque E ou E′ a des multiplications complexes, ou lorsque l'invariant modulaire de E ou E′ n'appartient pas à $\mathbf{Z}$ ([40], p. IV-14).

Théorème 21. — Supposons que l'on soit dans le cas (b), i.e. que l'ensemble des p tels que $a_p\neq a'_p$ *soit infini. Soit* S *un ensemble fini de nombres premiers contenant* S_E *et* $S_{E'}$; *posons* $N_S=\prod_{\ell\in S}\ell$.

Soit $p = p(E, E', S)$ *le plus petit nombre premier n'appartenant pas à* S *tel que* $a_p \neq a'_p$. *Sous* (GRH), *on a alors*

$$(251_R) \qquad p \leqslant c_{34}(\log N_S)^2(\log\log 2N_S)^{12},$$

où c_{34} *est une constante absolue.*

(Noter que $N_S \geqslant 2$, puisque S contient S_E, qui est non vide; par suite $\log N_S$ et $\log\log 2N_S$ sont >0.)

On peut reformuler le th. 21 en disant que, sous (GRH), si l'on vérifie que $a_p = a'_p$ pour tout $p \notin S$ satisfaisant à (251_R), alors $a_p = a'_p$ pour tout $p \notin S_E = S_{E'}$.

Démonstration du th. 21

Commençons par deux lemmes élémentaires :

Lemme 11. — *Il existe une constante absolue* $c_{23} > 0$ *telle que*

$$(252) \qquad \sum_{\ell \leqslant x} \log \ell \geqslant c_{23}\, x \quad \textit{pour tout} \quad x \geqslant 2.$$

(Précisons que la sommation porte sur les nombres *premiers* ℓ qui sont $\leqslant x$.)

Ce lemme résulte du théorème des nombres premiers — ou même simplement de la version plus faible due à Chebyshev.

Lemme 12. — *Si* n *est un entier* >0, *il existe un nombre premier* ℓ *tel que*

$$(253) \qquad n \not\equiv 0 \pmod{\ell} \quad \textit{et} \quad \ell \leqslant c_{24} \log 2n,$$

où c_{24} *est une constante absolue.*

Prenons $c_{24} = \mathrm{Sup}(2/\log 2,\ 1/c_{23})$. Si le nombre premier cherché ℓ n'existait pas, n serait divisible par tous les $\ell \leqslant x$, où $x = c_{24} \log 2n$. On aurait alors $n \geqslant \prod_{\ell \leqslant x} \ell$, i.e.

$$\log n \geqslant \sum_{\ell \leqslant x} \log \ell.$$

Par hypothèse, on a $x \geqslant c_{24} \log 2 \geqslant 2$, et le lemme 11 montre que

$$\sum_{\ell \leqslant x} \log \ell \geqslant c_{23} x = c_{23} c_{24} \log 2n \geqslant \log 2n.$$

On aurait donc $\log n \geqslant \log 2n$, ce qui est absurde.

(Les valeurs optimales de c_{23} et c_{24} sont $c_{23} = \frac{1}{3}\log 2$ et $c_{24} = 2/\log 2$.)

Revenons à la démonstration du th. 21. Il s'agit de majorer le nombre premier $p = p(E, E', S)$. Par hypothèse, l'entier $n = |a_p - a'_p|$ est >0. Choisissons un nombre premier ℓ satisfaisant à la condition (253) du lemme 12. On a :

$$(254) \qquad a_p \not\equiv a'_p \pmod{\ell}$$

et

$$(255) \qquad \ell \leqslant c_{24} \log(2\,|a_p - a'_p|).$$

D'après un théorème de Hasse, on a

(256) $$|a_p| \leqslant 2p^{1/2} \quad \text{et} \quad |a'_p| \leqslant 2p^{1/2}$$

d'où

(257) $$|a_p - a'_p| \leqslant 4p^{1/2}.$$

Vu (255), cela entraîne

(258) $$\ell \leqslant c_{24} \log 8p^{1/2} \leqslant c_{25} \log p,$$

où c_{25} est une constante absolue >0. En particulier, on a

(259) $$\ell \neq p$$

sauf si p est inférieur à une constante absolue c_{26} (auquel cas il n'y a rien à démontrer).

Les représentations

$$\varphi_\ell : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_\ell) \quad \text{et} \quad \varphi'_\ell : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_\ell)$$

associées aux courbes E et E', ainsi qu'au nombre premier ℓ, définissent un homomorphisme

$$\psi_\ell : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_\ell) \times \mathbf{GL}_2(\mathbf{F}_\ell).$$

Soit $G_\ell \subset \mathbf{GL}_2(\mathbf{F}_\ell) \times \mathbf{GL}_2(\mathbf{F}_\ell)$ l'image de ψ_ℓ et soit C_ℓ le sous-ensemble de G_ℓ formé des couples (s, s') tels que $\mathrm{Tr}(s) \neq \mathrm{Tr}(s')$. Si q est un nombre premier n'appartenant pas à $S_\ell = S \cup \{\ell\}$, la représentation ψ_ℓ est non ramifiée en q, et l'on peut parler de la substitution de Frobenius de q :

$$\psi_\ell(\sigma_q) = (\varphi_\ell(\sigma_q), \varphi'_\ell(\sigma_q));$$

c'est un élément de G_ℓ, défini à conjugaison près; nous le noterons (s_q, s'_q). Vu (238), on a

$$\mathrm{Tr}(s_q) \equiv a_q \pmod{\ell} \quad \text{et} \quad \mathrm{Tr}(s'_q) \equiv a'_q \pmod{\ell}.$$

Il en résulte que (s_q, s'_q) *appartient à* C_ℓ *si et seulement si l'on a*

(260) $$a_q \equiv a'_q \pmod{\ell}.$$

D'après (254) et (259), cette condition est satisfaite si $q = p$. On a donc $(s_p, s'_p) \in C_\ell$, ce qui montre que C_ℓ *est non vide.*

Soit maintenant H_ℓ l'intersection de G_ℓ avec le groupe des homothéties (λ, λ), où λ parcourt $\mathbf{F}_\ell^*$. Il est clair que C_ℓ est stable par H_ℓ, donc est image réciproque d'une partie non vide C'_ℓ du groupe quotient $G'_\ell = G_\ell / H_\ell$.

Lemme 13. — On a $|G'_\ell| < 2\ell^6$.

L'homomorphisme canonique

$$G_\ell \to \mathbf{GL}_2(\mathbf{F}_\ell) \times \mathbf{GL}_2(\mathbf{F}_\ell) \to \mathbf{PGL}_2(\mathbf{F}_\ell) \times \mathbf{PGL}_2(\mathbf{F}_\ell)$$

a pour noyau l'intersection $\tilde{H}_\ell$ de G_ℓ avec le groupe des (λ, μ), où λ et μ parcourent $\mathbf{F}_\ell^*$. Il est clair que $\tilde{H}_\ell$ contient H_ℓ. D'autre part, si $(s, s') \in G_\ell$, on a $\det(s) = \det(s')$ d'après

(238); il en résulte que, si $(\lambda, \mu) \in \widetilde{H}_\ell$, on a $\lambda^2 = \mu^2$, d'où $\lambda = \pm\mu$; cela montre que $(\widetilde{H}_\ell : H_\ell) = 1$ ou 2. D'où :

$$|G_\ell/H_\ell| \leqslant 2|G_\ell/\widetilde{H}_\ell| \leqslant 2\,|\mathbf{PGL}_2(\mathbf{F}_\ell)|^2 \leqslant 2(\ell^3-\ell)^2 < 2\ell^6,$$

ce qui démontre le lemme.

[On a en fait $|G'_\ell| \leqslant (\ell^3-\ell)^2 < \ell^6$, mais la majoration ci-dessus nous suffira.]

Lemme 14. — *Sous* (GRH), *il existe* $q \notin S_\ell$ *tel que* $a_q \equiv a'_q \pmod{\ell}$ *et*

$$(261_R) \qquad q \leqslant c_{27}\ell^{12}(\log \ell + \log N_S)^2,$$

où c_{27} *est une constante absolue.*

Soit L le sous-corps de $\overline{\mathbf{Q}}$ fixé par le noyau de l'homomorphisme

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to G_\ell \to G'_\ell.$$

L'extension $L/\mathbf{Q}$ est galoisienne, de groupe de Galois G'_ℓ. Elle est non ramifiée en dehors de S_ℓ. Appliquons alors le th. 6 du n° 2.5 à cette extension, et à une classe de conjugaison de G'_ℓ contenue dans C'_ℓ. On en conclut, sous (GRH), qu'il existe un nombre premier $q \notin S_\ell$ dont la substitution de Frobenius appartient à C'_ℓ, et qui satisfait à l'inégalité

$$(262_R) \qquad q \leqslant c_{12}n^2(\log n + \log N_S + \log \ell)^2,$$

où $n = [L : \mathbf{Q}] = |G'_\ell|$. La première propriété équivaut à

$$a_q \equiv a'_q \pmod{\ell},$$

on l'a vu. Quant à la majoration (262_R), combinée avec l'inégalité $n < 2\ell^6$ du lemme 13, elle entraîne bien (261_R) si c_{27} est assez grand.

Si q satisfait aux conditions du lemme 14, on a évidemment $a_q \neq a'_q$. Vu la minimalité de p, cela entraîne $p \leqslant q$, d'où, d'après (261_R) :

$$(263_R) \qquad p \leqslant c_{27}\ell^{12}(\log \ell + \log N_S)^2.$$

Mais, d'après (258), on a $\ell \leqslant c_{25} \log p$. L'inégalité (263_R) entraîne donc

$$(264_R) \qquad p \leqslant c_{28}(\log p)^{12}(\log\log p + \log N_S)^2,$$

où c_{28} est une constante absolue >0.

Il reste maintenant à déduire (251_R) de (264_R). Cela ne présente pas de difficulté. En divisant les deux membres de (264_R) par $(\log p)^{14}$, on obtient

$$(265_R) \qquad p/(\log p)^{14} \leqslant c_{29}(1 + \log N_S)^2 \leqslant c_{30}(\log 2N_S)^2.$$

Comme $x^{1/2} \leqslant c_{31}x/(\log x)^{14}$ pour $x \geqslant 2$, cela implique

$$(266_R) \qquad p^{1/2} \leqslant c_{32}(\log 2N_S)^2$$

d'où

$$(267_R) \qquad \log p \leqslant c_{33} \log\log 2N_S;$$

en portant dans (264_R), cela donne

$$p \leqslant c_{28}(c_{33})^2(\log\log 2N_S)^{12}(\log c_{33}+\log\log\log 2N_S+\log N_S)^2,$$

d'où

$$p \leqslant c_{34}(\log\log 2N_S)^{12}(\log N_S)^2$$

si c_{34} est assez grand.

Variantes

L'exposant 12 de (251_R) provient de l'exposant 6 du lemme 13, lui-même égal à la dimension du groupe $\mathbf{PGL}_2\times\mathbf{PGL}_2$. On peut l'abaisser si l'on sait que l'image de G_ℓ dans $\mathbf{PGL}_2(\mathbf{F}_\ell)\times\mathbf{PGL}_2(\mathbf{F}_\ell)$ est sensiblement plus petite que le groupe entier. Par exemple :

Théorème 21'. — Supposons que E' *se déduise de* E *par « torsion » au moyen d'un caractère quadratique, i.e. que* $a'_p/a_p=\pm 1$ *pour tout* $p\notin S$. *Sous les hypothèses du th. 21, on a alors :*

(268_R) $$p \leqslant c_{35}(\log N_S)^2(\log\log 2N_S)^6,$$

où c_{35} *est une constante absolue.*

L'hypothèse signifie qu'il existe un caractère continu

$$\varepsilon : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \{\pm 1\}$$

tel que $\varphi'_n(g)=\varepsilon(g)\varphi_n(g)$ pour tout $g\in\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ et tout $n\geqslant 1$. L'image de G_ℓ par l'homomorphisme

$$G_\ell \to \mathbf{GL}_2(\mathbf{F}_\ell)\times\mathbf{GL}_2(\mathbf{F}_\ell) \to \mathbf{PGL}_2(\mathbf{F}_\ell)\times\mathbf{PGL}_2(\mathbf{F}_\ell)$$

est contenue dans le *sous-groupe diagonal* de $\mathbf{PGL}_2(\mathbf{F}_\ell)\times\mathbf{PGL}_2(\mathbf{F}_\ell)$; son ordre est $<\ell^3$. Comme dans la démonstration du lemme 13 on déduit de là que $|G'_\ell|<2\ell^3$; le lemme 14 est alors valable avec ℓ^{12} remplacé par ℓ^6 (et c_{27} remplacé par une autre constante absolue) ; il en est de même de (263_R) et (264_R), et l'on en déduit (268_R) par le même argument que ci-dessus.

Remarques

1) Des arguments analogues montrent que, si E (resp. E et E') a des multiplications complexes, l'exposant 12 peut être remplacé par 8 (resp. par 4).

2) A la place de l'équation $a_p=a'_p$, on aurait pu considérer une équation plus générale, par exemple

(269) $$F(p, a_p, a'_p)=0 \quad (\text{pour } p\notin S),$$

où F est un polynôme à trois variables. On aurait obtenu le résultat suivant :

ou bien $F(p, a_p, a'_p)=0$ *pour tout* $p\notin S$,
ou bien il existe une infinité de $p\notin S$ *tels que* $F(p, a_p, a'_p)\neq 0$, *et, si l'on appelle* p_F *le plus petit de ceux-là, on a, sous* (GRH),

(270_R) $$p_F \leqslant c(F)(\log N_S)^2(\log\log 2N_S)^{14},$$

où $c(F)$ *est un nombre* >0 *qui ne dépend que de* F. Si de plus F est isobare (la première variable étant de poids 2, et les deux autres de poids 1), l'exposant 14 peut être remplacé par 12.

Il y a des résultats analogues pour trois (ou quatre...) courbes elliptiques, ou pour des systèmes rationnels de représentations ℓ-adiques (cf. [40]) qui satisfont à une « conjecture de Weil » semblable à (236). Dans chaque cas, on trouve une borne en

$$(\log N_S)^2(\log\log N_S)^{2d},$$

où d est la dimension (comme groupe algébrique) du groupe de Galois qui intervient.

3) Il serait intéressant d'obtenir une majoration effective de $p=p(E, E', S)$ qui n'utilise pas (GRH). Je n'y suis pas parvenu.

8.4. Groupes de Galois des points de ℓ-division

Supposons E *sans multiplication complexe*. Comme on l'a rappelé au n° 8.1, les représentations ℓ-adiques

$$\rho_\ell : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{Z}_\ell)$$

sont surjectives pour ℓ assez grand. Nous allons préciser ce résultat.

Posons

$$N_E = \prod_{\ell \in S_E} \ell. \tag{271}$$

Théorème 22. — *Sous* (GRH), *on a* $\mathrm{Im}(\rho_\ell)=\mathbf{GL}_2(\mathbf{Z}_\ell)$ *pour tout nombre premier* ℓ *tel que*

$$\ell \geqslant c_{36}(\log N_E)(\log\log 2N_E)^3, \tag{272$_R$}$$

où c_{36} *est une constante absolue.*

De façon plus précise, on va montrer, sous (GRH), que ρ_ℓ est surjectif pour tout ℓ satisfaisant aux deux conditions suivantes :

$$\ell \geqslant 19 \quad \text{et} \quad \ell \neq 37, \tag{273}$$

$$\ell \geqslant 2(c_{35})^{1/2}(\log N_E)(\log\log 2N_E)^3, \tag{274$_R$}$$

où c_{35} est la constante du th. 21′.

Le lemme suivant permet de se ramener au groupe

$$G_\ell = \mathrm{Im}(\varphi_\ell) \subset \mathbf{GL}_2(\mathbf{F}_\ell).$$

Lemme 15. — *Supposons* $\ell \geqslant 5$. *On a* $G_\ell=\mathbf{GL}_2(\mathbf{F}_\ell)$ *si et seulement si* $\mathrm{Im}(\rho_\ell)=\mathbf{GL}_2(\mathbf{Z}_\ell)$.

Posons $\Gamma_\ell=\mathrm{Im}(\rho_\ell)$; l'image de Γ_ℓ dans $\mathbf{GL}_2(\mathbf{F}_\ell)$ par réduction modulo ℓ est G_ℓ. Cela montre que $\Gamma_\ell=\mathbf{GL}_2(\mathbf{Z}_\ell) \Rightarrow G_\ell=\mathbf{GL}_2(\mathbf{F}_\ell)$. Posons d'autre part

$$\Gamma_\ell^1=\Gamma_\ell \cap \mathbf{SL}_2(\mathbf{Z}_\ell) \quad \text{et} \quad G_\ell^1=G_\ell \cap \mathbf{SL}_2(\mathbf{F}_\ell).$$

Ces groupes sont les noyaux des homomorphismes

$$\det : \Gamma_\ell \to \mathbf{Z}_\ell^* \quad \text{et} \quad \det : G_\ell \to \mathbf{F}_\ell^*;$$

ces homomorphismes sont surjectifs, d'après (239). Il s'ensuit que la réduction modulo ℓ applique Γ_ℓ^1 *sur* G_ℓ^1. Si l'on suppose que $G_\ell=\mathbf{GL}_2(\mathbf{F}_\ell)$, on a $G_\ell^1=\mathbf{SL}_2(\mathbf{F}_\ell)$, et, pour

$\ell \geqslant 5$, le lemme 3 de [40], p. IV-23, montre que $\Gamma_\ell^1 = \mathbf{SL}_2(\mathbf{Z}_\ell)$, d'où $\Gamma_\ell = \mathbf{GL}_2(\mathbf{Z}_\ell)$, ce qui achève de prouver le lemme 15.

Nous n'avons donc à nous occuper que du groupe $G_\ell \subset \mathbf{GL}_2(\mathbf{F}_\ell)$. Notons PG_ℓ l'image de ce groupe dans le groupe projectif $\mathbf{PGL}_2(\mathbf{F}_\ell)$. Pour prouver que $G_\ell = \mathbf{GL}_2(\mathbf{F}_\ell)$, il suffit de montrer que PG_ℓ est égal à $\mathbf{PGL}_2(\mathbf{F}_\ell)$, ou même seulement que PG_ℓ *contient* le groupe $\mathbf{PSL}_2(\mathbf{F}_\ell)$ (qui est un sous-groupe simple, d'indice 2, de $\mathbf{PGL}_2(\mathbf{F}_\ell)$). Or on sait (cf. par exemple [41], § 2) que tout sous-groupe H de $\mathbf{PGL}_2(\mathbf{F}_\ell)$ ne contenant pas $\mathbf{PSL}_2(\mathbf{F}_\ell)$ possède l'une des propriétés suivantes :

(i) H est contenu dans un sous-groupe de Borel de $\mathbf{PGL}_2(\mathbf{F}_\ell)$;
(ii) H est contenu dans un sous-groupe de Cartan non déployé C_ℓ de $\mathbf{PGL}_2(\mathbf{F}_\ell)$;
(iii) H est isomorphe à $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$;
(iv) H est contenu dans le normalisateur N_ℓ d'un sous-groupe de Cartan C_ℓ de $\mathbf{PGL}_2(\mathbf{F}_\ell)$, et n'est pas contenu dans C_ℓ.

Nous allons éliminer ces diverses possibilités :

Lemme 16. — Le cas (i) *est impossible si ℓ satisfait à* (273).

Cela résulte d'un théorème de Mazur [29], compte tenu de ce que E n'a pas de multiplication complexe.

Lemme 17. — Le cas (ii) *est impossible pour $\ell \geqslant 3$.*

Cela résulte de ce que G_ℓ contient un élément de valeurs propres 1 et -1, à savoir celui défini par la conjugaison complexe (cf. [41], § 5.2 iii)).

Lemme 18. — Le cas (iii) *est impossible pour $\ell \geqslant 17$.*

On a vu ci-dessus que $H = PG_\ell$ n'est pas contenu dans le sous-groupe $\mathbf{PSL}_2(\mathbf{F}_\ell)$ de $\mathbf{PGL}_2(\mathbf{F}_\ell)$. Or $\mathfrak{A}_4$ et $\mathfrak{A}_5$ sont contenus dans $\mathbf{PSL}_2(\mathbf{F}_\ell)$, et il en est de même de $\mathfrak{S}_4$ si $\ell \equiv \pm 1 \pmod 8$. Reste à éliminer le cas où $H \simeq \mathfrak{S}_4$ et $\ell \equiv \pm 3 \pmod 8$. Cela se fait au moyen du résultat suivant (cf. [28], p. 36) :

Lemme 18'. — Le groupe d'inertie de $H = PG_\ell$ en ℓ contient un élément d'ordre $\geqslant (\ell - 1)/4$.

(Lorsque $\ell > 17$, ce lemme montre que H contient un élément d'ordre > 4, donc n'est pas isomorphe à $\mathfrak{S}_4$; le cas $\ell = 17$ est exclu grâce au fait que $17 \equiv 1 \pmod 8$.)

Pour prouver le lemme 18', on distingue deux cas :

a) L'invariant modulaire j de E *n'est pas entier en ℓ.*

Il existe alors une extension de degré $\leqslant 2$ du corps $\mathbf{Q}_\ell$ sur laquelle E devient une « courbe de Tate », cf. [41], § 1.12. On en déduit *(loc. cit.)* que le groupe d'inertie modérée de H en ℓ contient un sous-groupe cyclique d'ordre $\geqslant (\ell - 1)/2$.

b) L'invariant modulaire j de E *est entier en ℓ.*

Il y a bonne réduction « potentielle », cf. [41], § 5.6. Comme $\ell \neq 2, 3$, cela entraîne l'existence d'une extension finie K de $\mathbf{Q}_\ell$, avec indice de ramification e égal

à 1, 2, 3, 4 ou 6, sur laquelle E a bonne réduction; de plus, le cas $e=6$ peut être ramené par « torsion » au moyen d'un caractère quadratique au cas $e=3$ (noter que la « torsion » ne change pas le groupe PG_ℓ). On peut donc supposer que $e\leqslant 4$.

Identifions alors E (sur l'anneau des entiers de K) à une cubique $y^2=x^3+Ax+B$ à discriminant inversible, et soit

$$[\ell](t)=\ell t+\ldots+a_\ell t^\ell+\ldots \qquad (\text{avec } t=x/y)$$

la série formelle donnant la multiplication par ℓ dans le groupe formel défini par E (cf. [41], § 1.11). Soit $f=v_K(a_\ell)$ la valuation du coefficient a_ℓ. Il y a trois possibilités :

b_1) $f=0$.

La réduction de E est de hauteur 1. Il résulte alors de [41], prop. 11, que le groupe d'inertie de H en ℓ contient un élément d'ordre $(\ell-1)/e'$, où $e'=(e,\ell-1)\leqslant 4$.

b_2) $1\leqslant f<e\ell/(\ell+1)$.

La réduction de E est de hauteur 2, et le polygone de Newton de $[\ell](t)$ est formé de deux segments de pentes distinctes, à savoir $(e-f)/(\ell-1)$ et $f/(\ell^2-\ell)$. Comme la seconde de ces pentes n'est pas ℓ-entière, cela entraîne que le groupe d'inertie de G_ℓ en ℓ contient un élément d'ordre ℓ, et il en est de même de $H=PG_\ell$.

b_3) $f\geqslant e\ell/(\ell+1)$.

La réduction de E est de hauteur 2, et le polygone de Newton de $[\ell](t)$ est formé d'un seul segment de pente $e/(\ell^2-1)$. D'après [41], prop. 10, les caractères de l'inertie modérée (sur le corps de base K) qui interviennent dans E_p sont les puissances e-ièmes des deux caractères fondamentaux de niveau 2, au sens de [41]. On en déduit que le groupe d'inertie de H en ℓ contient un élément d'ordre $(\ell+1)/e''$, où $e''=(\ell+1,e)\leqslant 4$. Cela achève la démonstration du lemme 18′.

Reste le cas (iv) :

Lemme 19. — Sous (GRH), *le cas* (iv) *est impossible si ℓ satisfait à* (274_R) *et* $\ell\geqslant 5$.

Supposons que ℓ satisfasse à (iv), i.e. soit contenu dans le normalisateur N_ℓ d'un sous-groupe de Cartan C_ℓ, sans être contenu dans C_ℓ. Soit ε le caractère d'ordre 2 de $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ défini par

$$\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})\to G_\ell\to PG_\ell\to N_\ell\to N_\ell/C_\ell\simeq\{\pm 1\}.$$

D'après [41], p. 317, ε est *non ramifié en dehors de* S_E. De plus, si l'on identifie comme d'ordinaire ε à un caractère de Dirichlet, on a

$$(275) \qquad a_p\equiv 0 \pmod{\ell} \quad \text{pour tout } p\notin S_E \text{ tel que } \varepsilon(p)=-1,$$

cf. [41], p. 317, (c_5).

Soit alors E′ la courbe elliptique déduite de E par torsion au moyen de ε. Du fait

que ε est non ramifié en dehors de S_E, la courbe E′ a bonne réduction en dehors de S_E. Avec les notations du n° 8.3, on a

(276) $\qquad a'_p = \varepsilon(p)a_p \quad$ pour tout $\quad p \notin S_E$.

De plus, il existe des p tels que $a'_p \neq a_p$: sinon, en effet, on aurait $a_p = 0$ pour tout p tel que $\varepsilon(p) = -1$, et cela contredirait l'hypothèse que E n'a pas de multiplication complexe (cf. th. 20 par exemple). On peut donc appliquer le th. 21′ aux courbes E et E′, avec $S = S_E$. On en déduit, sous (GRH), qu'il existe un nombre premier $p \notin S_E$ tel que :

(277_R) $\qquad a'_p \neq a_p$

et

(278_R) $\qquad p \leqslant c_{35}(\log N_E)^2(\log\log 2N_E)^6$.

La propriété (277_R) équivaut à $\varepsilon(p) = -1$ et $a_p \neq 0$. Vu (275), il en résulte que ℓ divise a_p. Comme $a_p \neq 0$, cela entraîne $\ell \leqslant |a_p|$, d'où

(279_R) $\qquad \ell < 2p^{1/2}$, d'après (256).

Compte tenu de (278_R), on obtient

$$\ell < 2(c_{35})^{1/2}(\log N_E)(\log\log 2N_E)^3,$$

ce qui contredit (274_R), et achève la démonstration.

Questions

1) Peut-on démontrer un résultat analogue au th. 22 *sans supposer* (GRH) ?

2) La condition $\ell \geqslant 41$ *suffit-elle* à assurer que ρ_ℓ est surjectif?

3) Peut-on étendre le th. 22 aux courbes elliptiques définies sur *un corps de nombres* quelconque ?

BIBLIOGRAPHIE

[1] E. Artin, Über eine neue Art von L-Reihen, *Hamb. Abh.*, **3** (1923), 89-108 (= *Coll. Papers*, 105-124).

[2] N. Bourbaki, *Variétés différentielles et analytiques. Fascicule de résultats*, Paris, Hermann, 1971.

[3] N. Bourbaki, *Groupes et Algèbres de Lie*, chapitre II : « Algèbres de Lie libres »; chapitre III : « Groupes de Lie », Paris, Hermann, 1972.

[4] S. Chowla, On the least prime in an arithmetic progression, *J. Indian Math. Soc.*, **1** (1934), 1-3.

[5] R. Dedekind, Über die Diskriminanten endlicher Körper, *Gött. Abh.*, **29** (1882), 1-56 (= *Ges. Math. Werke*, I, 351-397).

[6] R. Dedekind, *Vorlesungen über Zahlentheorie von P. G. Lejeune-Dirichlet*, 4e éd., Braunschweig, 1893 (réimpr. : New York, Chelsea, 1968).

[7] P. Deligne, Formes modulaires et représentations ℓ-adiques, Sém. Bourbaki 1968-1969, exposé 355, *Lecture Notes in Math.*, **179**, Springer-Verlag, 1971, 139-172.

[8] P. Deligne, La conjecture de Weil, I, *Publ. Math. I.H.E.S.*, **43** (1974), 273-307.

[9] P. Deligne et J.-P. Serre, Formes modulaires de poids 1, *Ann. Sci. E.N.S.*, 4e série, **7** (1974), 507-530.

[10] J. DIEUDONNÉ et A. GROTHENDIECK, Critères différentiels de régularité pour les localisés des algèbres analytiques, *J. of Algebra*, **5** (1967), 305-324.
[11] H. FEDERER, *Geometric Measure Theory*, Berlin, Springer-Verlag, 1969.
[12] G. F. FROBENIUS, Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe, *Sitz. Akad. Berlin* (1896), 689-703 (= *Ges. Abh.*, II, 719-733).
[13] G. H. HARDY et J. E. LITTLEWOOD, Tauberian theorems concerning power series and Dirichlet series whose coefficients are positive, *Proc. London Math. Soc.*, 2e série, **13** (1914), 174-191 (= G. H. HARDY, *Coll. Papers*, VI, 510-527).
[14] G. H. HARDY et J. E. LITTLEWOOD, Some theorems concerning Dirichlet series, *Messenger of Math.*, **43** (1914), 134-147 (= G. H. HARDY, *Coll. Papers*, VI, 542-555).
[15] K. HENSEL, Über die Entwicklung der algebraischen Zahlen in Potenzreihen, *Math. Ann.*, **55** (1902), 301-336.
[16] H. HIRONAKA, Resolution of singularities of an algebraic variety over a field of characteristic zero, *Ann. of Math.*, **79** (1964), 109-326.
[17] J. IGUSA, Complex Powers and Asymptotic Expansions II, *J. Crelle*, **278-279** (1975), 307-321.
[18] J. IGUSA, Some observations on higher degree characters, *Amer. J. of Math.*, **99** (1977), 393-417.
[19] N. IWAHORI et H. MATSUMOTO, Several remarks on projective representations of finite groups, *J. Fac. Sci. Univ. Tokyo*, **10** (1964), 129-146.
[20] H. D. KLOOSTERMAN, Asymptotische Formeln für die Fourierkoeffizienten ganzer Modulformen, *Hamb. Abh.*, **5** (1927), 338-352.
[21] M. I. KNOPP et J. LEHNER, *Gaps in the Fourier series of automorphic forms* (à paraître).
[22] J. C. LAGARIAS, H. L. MONTGOMERY et A. M. ODLYZKO, A Bound for the Least Prime Ideal in the Chebotarev Density Theorem, *Invent. Math.*, **54** (1979), 271-296.
[23] J. C. LAGARIAS et A. M. ODLYZKO, Effective Versions of the Chebotarev Density Theorem, *Algebraic Number Fields* (A. Fröhlich edit.), New York, Academic Press, 1977, 409-464.
[24] S. LANG et H. TROTTER, Frobenius Distributions in GL_2-Extensions, *Lect. Notes in Math.*, **504**, Springer-Verlag, 1975.
[25] R. P. LANGLANDS, Automorphic representations, Shimura varieties and motives. Ein Märchen, *Proc. Symp. Pure Math.*, **33**, Amer. Math. Soc., 1979, t. 2, 205-246.
[26] M. LAZARD, Groupes analytiques p-adiques, *Publ. Math. I.H.E.S.*, **26** (1965), 1-219.
[27] W. LI, Newforms and Functional Equations, *Math. Ann.*, **212** (1975), 285-315.
[28] B. MAZUR, Modular curves and the Eisenstein ideal, *Publ. Math. I.H.E.S.*, **47** (1978), 33-186.
[29] B. MAZUR, Rational Isogenies of Prime Degree, *Invent. Math.*, **44** (1978), 129-162.
[30] J. ŒSTERLÉ, Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée, *Astérisque*, **61** (1979), 165-167.
[31] A. OGG, Abelian curves of 2-power conductor, *Proc. Camb. Phil. Soc.*, **62** (1966), 143-148.
[32] R. RANKIN, Contribution to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions, I, II, *Proc. Camb. Phil. Soc.*, **35** (1939), 351-372.
[33] K. RIBET, Galois Representations attached to Eigenforms with Nebentypus, *Lect. Notes in Math.*, **601**, Springer-Verlag, 1977, 17-52.
[34] P. ROBBA, Lemmes de Schwarz et lemmes d'approximations p-adiques en plusieurs variables, *Invent. Math.*, **48** (1978), 245-277.
[35] I. ŠAFAREVIČ, Corps de nombres algébriques (en russe), *Proc. Int. Congr. Math.*, Stockholm (1962), 163-176 (trad. anglaise : *Amer. Math. Transl.* (2), vol. 31 (1963), 25-39).
[36] L. SCHŒNFELD, Sharper Bounds for the Chebyshev Functions $\theta(x)$ and $\psi(x)$, II, *Math. of Comp.*, **30** (1976), 337-360.
[37] S. SEN, Ramification in p-adic Lie Extensions, *Invent. Math.*, **17** (1972), 44-50.
[38] J.-P. SERRE, *Corps locaux*, Paris, Hermann, 1980, 3e éd. (trad. anglaise, *Local Fields*, GTM 67, Springer-Verlag, 1979).
[39] J.-P. SERRE, Classification des variétés analytiques p-adiques compactes, *Topology*, **3** (1965), 409-412.
[40] J.-P. SERRE, *Abelian ℓ-adic representations and elliptic curves*, New York, Benjamin Publ., 1968.
[41] J.-P. SERRE, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.*, **15** (1972), 259-331.
[42] J.-P. SERRE, Divisibilité de certaines fonctions arithmétiques, *L'Ens. Math.*, **22** (1976), 227-260.

[43] J.-P. SERRE, Modular forms of weight one and Galois representations, *Algebraic Number Theory* (A. Fröhlich edit.), New York, Academic Press, 1977, 193-268.

[44] G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. Japan, vol. 11, Princeton Univ. Press, 1971.

[45] H. STARK, Some effective cases of the Brauer-Siegel theorem, *Invent. Math.*, **23** (1974), 135-152.

[46] H. P. F. SWINNERTON-DYER, On ℓ-adic representations and congruences for coefficients of modular forms, *Lecture Notes in Math.*, **350**, Springer-Verlag, 1973, 1-55.

[47] N. TSCHEBOTAREFF, Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören, *Math. Ann.*, **95** (1926), 191-228.

[48] A. WEIL, Zeta-functions and Mellin transforms, *Proc. Bombay Coll. on Alg. Geometry*, Bombay, Tata Institute, 1968, 409-426 (= *Œuvres Sci.*, III, 179-196).

[49] H. WEYL, On the volume of tubes, *Amer. J. of Math.*, **61** (1939), 461-472 (= *Ges. Abh.*, III, 658-669).

[50] E. WIRSING, Das asymptotische Verhalten von Summen über multiplikative Funktionen, *Math. Ann.*, **143** (1961), 75-102.

Collège de France,
Paris.

Manuscrit reçu le 14 juillet 1981.