

L'OCTOGONE RÉGULIER ET LA SIGNATURE DES FORMES QUADRATIQUES ENTIÈRES NON SINGULIÈRES

par C. BAILLY et M. de J. CABRAL

Avec un Appendice de G. GAHIDE

Les longueurs l_R et L_R des côtés des octogones réguliers inscrits et exinscrits dans un cercle de rayon R vérifient la relation

$$(O) \quad L_R^2 < R \cdot l_R.$$

Cette *inégalité de l'octogone* conduira à une preuve élémentaire de la formule

$$(S) \quad \frac{1}{\sqrt{|\det(B)|}} \sum_{\overline{m} \in \mathcal{D}/\mathcal{R}} \exp(2\pi i Q(m)) = \exp\left(2\pi i \frac{\sigma(Q)}{8}\right)$$

exprimant, comme l'argument (compté en nombre de tours) d'une somme de racines de l'unité, le huitième de la *signature* $\sigma(Q)$ d'une forme quadratique entière non singulière Q , c'est-à-dire de la différence des nombres de valeurs propres positives et négatives d'une matrice symétrique $n \times n$ à coefficients entiers B , de déterminant non nul et paire sur la diagonale.

L'application $Q : \mathbb{Q}^n \rightarrow \mathbb{Q}$ donnée par $Q(x) = \frac{1}{2} x B x^t$ est alors à valeurs entières sur $\mathcal{R} = \mathbb{Z}^n$ et, dans la *formule de la signature* (S) ci-dessus, $\mathcal{D}$ désigne le réseau $B^{-1}(\mathcal{R})$ qui contient $\mathcal{R}$ comme sous groupe d'indice $|\det(B)|$.

Le formalisme de Witt quadratique (cf. [5], [1] ou l'appendice) reconnaît dans le membre de gauche de (S) une racine huitième de l'unité $\gamma(Q)$ déterminée par la classe d'isomorphisme rationnel de la forme quadratique. Cet invariant est multiplicatif pour la somme orthogonale des formes quadratiques et vérifie $\gamma(-Q) = \overline{\gamma(Q)}$.

Comme toute forme quadratique entière est rationnellement isomorphe à une somme orthogonale de formes Q_m de rang 1 données par $Q_m(x) = m x^2$ où m est un entier et, puisque $Q_{k^2 m}$ est, pour tout entier non nul k , isomorphe à Q_m et $\gamma(Q_1) = \frac{1+i}{\sqrt{2}}$, la formule (S) découlera de l'estimation pour m assez grand :

$$(E) \quad |\gamma(Q_m) - \gamma(Q_{m+1})| < |\exp\left(\frac{2\pi i}{8}\right) - 1| = l_1.$$

Posons alors $N = 2m + 1$ et $M = N^2 - 1$. L'identité remarquable

$$(R) \quad \frac{N-1}{2} (x+2y)^2 + (x-(N-1)y)^2 = \frac{N+1}{2} x^2 + (N^2-1)y^2$$

donne un isomorphisme rationnel entre $Q_m \oplus Q_1$ et $Q_{m+1} \oplus Q_M$.

Ainsi par multiplicativité de l'invariant γ pour la somme orthogonale le membre de gauche de (E) est le module de la différence :

$$(D) \quad \gamma(Q_m) - \gamma(Q_{m+1}) = \gamma(Q_M) - \gamma(Q_1).$$

Pour tout réel x notons $e(x) = \exp(2\pi i x)$ et dans la somme de Gauss

$$(\Sigma) \quad \Gamma_N = \sqrt{2M} \gamma(Q_M) = \sum_{k=1-M}^M e\left(\frac{k^2}{4M}\right)$$

écrivons, par division euclidienne par $2N$ l'entier $k = p + 2Nq$, avec reste $-N < p \leq N$ (et quotient q). Ainsi dans chaque terme de Γ_N :

$$e\left(\frac{k^2}{4M}\right) = e\left(\frac{p^2}{4M}\right) e\left(\frac{Npq}{M}\right) e\left(\frac{N^2q^2}{M}\right) = e\left(\frac{p^2}{4M}\right) e\left(\frac{Npq}{M}\right) e\left(\frac{q^2}{M}\right)$$

$$(T_k) \quad e\left(\frac{k^2}{4M}\right) = e\left(\frac{p^2}{4M}\right) e\left(\frac{Npq}{M}\right) + e\left(\frac{p^2}{4M}\right) e\left(\frac{Npq}{M}\right) \left[e\left(\frac{q^2}{M}\right) - 1 \right]$$

on peut faire apparaître une racine de l'unité qui est multiplicative en le quotient. On obtient ainsi, en isolant cette partie multiplicative en q , le partage de la somme de Gauss Γ_N en deux morceaux :

$$\Gamma_N = \Gamma_{N,1} + \Gamma_{N,2}.$$

Avec N^2 à la place de M le premier morceau $\Gamma_{N,1}$ serait, à l'exception des deux termes extrêmes, la somme de Gauss calculant $\gamma(q_{N^2})$ qui, en sommant à p fixé les sommes géométriques $\sum e(\frac{Npq}{N^2})$, vaut $\sqrt{2N^2} \gamma(Q_1)$. Au §3, en sommant de même à reste p fixé les sommes géométriques $\sum e(\frac{Npq}{M})$, la proximité de $M = N^2 - 1$ à N^2 conduira à l'approximation du terme principal :

$$(A) \quad \left| \frac{1}{\sqrt{2M}} [\Gamma_{N,1} - \sqrt{2N^2} \gamma(Q_1)] \right| < \frac{7}{\sqrt{N+1}}.$$

En faisant intervenir les sommes, à quotient q fixé, de $r = 1 - N$ à p de $e(\frac{Npq}{M})$ on obtiendra au §4 pour le second morceau $\Gamma_{N,2}$ la majoration

$$(M) \quad \left| \frac{1}{\sqrt{2M}} \Gamma_{N,2} \right| < \frac{24}{\sqrt{M}} + \frac{\pi^2}{16}.$$

Comme le membre de droite de (D) est

$$\gamma(Q_M) - \gamma(Q_1) = \frac{1}{\sqrt{2M}} [\Gamma_N - \sqrt{2N^2} \gamma(Q_1)] + \frac{1}{\sqrt{M}(N + \sqrt{M})} \gamma(Q_1),$$

on tire alors de ces estimations (A) et (M) l'estimation explicite :

$$(EE) \quad \begin{aligned} |\gamma(Q_m) - \gamma(Q_{m+1})| &< \frac{\pi^2}{16} + \frac{24}{\sqrt{M}} + \frac{7}{\sqrt{N+1}} + \frac{1}{2M} \\ &< \left(\frac{\pi}{4}\right)^2 + \frac{20}{\sqrt{m+1}}. \end{aligned}$$

Ainsi, puisque la longueur d'un segment extérieur au cercle unité est inférieure à son angle visuel $\frac{\pi}{4} < L_1$, l'inégalité de l'octogone donnera l'estimation (E) pour m assez grand. $\square$

En 1995, classifiant les formes quadratiques rationnelles d'une manière alternative (cf. [5] ou l'appendice) à la présentation classique (cf. [6]), un conférencier, peu scrupuleux mais naïf, déduisait la formule de la signature (S) de l'estimation (E). Sa preuve, esquissée à la fin de la dernière conférence devant une salle désertée, s'appuyait malheureusement sur

$$\left| \frac{1}{\sqrt{2m}} e\left(\frac{k^2}{4m}\right) - \frac{1}{\sqrt{2(m+1)}} e\left(\frac{k^2}{4(m+1)}\right) \right| < \frac{1}{\sqrt{m(m+1)}(\sqrt{2(m+1)} + \sqrt{2m})}.$$

Cette supercherie (pour $k = m$, le membre de gauche dépasse $\frac{1}{2\sqrt{m+1}}$!) n'a pas échappé à l'un des derniers auditeurs de ces trois conférences Institut Fourier-I.R.E.M., Monsieur Lachouque. Il ne manquait pas de citer cette escroquerie pour nous signaler le danger qu'il y a à « oublier les arguments » et son espoir que quelqu'un, un jour, puisse donner de l'estimation (E) une preuve élémentaire mais correcte.

Cet article n'existerait donc pas sans Monsieur Lachouque qui a suscité le problème et permis sa résolution en nous enseignant les rudiments de géométrie du §1 et la douzaine de relations trigonométriques que l'on trouvera au §2.

Remercions aussi Caroline Chauffin et Chantal Fayolle qui ont su, à différents moments de l'élaboration de ce travail, nous prêter une oreille attentive et amicale et excuser nos escapades lors de la rédaction finale.

1. L'inégalité de l'octogone.

PROPOSITION. — *Le rayon r du cercle inscrit dans un octogone régulier est supérieur à la moyenne arithmétique de la longueur l de ses côtés et du rayon R de son cercle exinscrit*

$$r > \frac{l + R}{2}.$$

Démonstration. — Désignons par O le centre de l'octogone et par I le milieu d'un de ses côté AB . Introduisons le point J de OI qui voit ce côté AB sous un angle droit. Ainsi le triangle JAB est isocèle de hauteur la moitié de son hypoténuse :

$$JI = \frac{1}{2}AB = \frac{1}{2}l.$$

La droite OI étant la bissectrice de l'angle $\widehat{AOB}$ on a

$$\widehat{AOJ} = \widehat{AOI} = \frac{1}{2}\widehat{AOB} = \frac{\pi}{8},$$

d'autre part l'angle en A du triangle OJA vaut

$$\widehat{OAJ} = \left(\frac{\pi}{2} - \frac{\pi}{8}\right) - \frac{\pi}{4} = \frac{\pi}{8}.$$

Ce triangle OJA est donc isocèle et $OJ = JA > \frac{1}{2}OA$. Ainsi

$$r = OI = OJ + JI = OJ + \frac{1}{2}l > \frac{1}{2}(OA + l) = \frac{1}{2}(R + l).$$

□

Un octogone régulier exinscrit à un cercle de rayon R est homothétique dans une homothétie de centre le centre du cercle et de rapport $\frac{R}{r}$ d'un octogone inscrit dans ce cercle. D'où, puisque la proposition $r > \frac{1}{2}(R + l)$ implique, par l'inégalité de la moyenne géométrique, $r^2 > Rl$, l'inégalité de l'octogone :

$$L^2 = \left(\frac{R}{r}l\right)^2 = R \frac{Rl}{r^2} l < R \frac{Rl}{Rl} l = Rl.$$

□

2. Quelques relations et inégalités trigonométriques.

Le point d'argument $2\pi i x$ sur le cercle trigonométrique U est

$$(i) \quad e(x) = \exp(2\pi i x) = c(x) + i s(x) \quad \text{où}$$

$$c(x) = \frac{1}{2}(e(x) + e(-x)), \quad \text{et} \quad s(x) = \frac{1}{2i}(e(x) - e(-x))$$

sont ses coordonnées réelles. Comme $e(2x) - 1 = e(x) 2i s(x)$ on a

$$(ii) \quad |e(2x) - 1| = 2 |s(x)|.$$

La longueur $2\pi |x|$ de l'arc de U joignant 1 à $e(x)$ étant au moins la distance de $e(x)$ à l'axe réel, on a pour tout réel x les majorations en module :

$$(iii) \quad |s(x)| \leq 2\pi |x|$$

$$(iii') \quad |e(x) - 1| \leq 2\pi |x|.$$

Ainsi, puisque $1 - c(2x) = 2s(x)^2$, on a pour tout réel y l'encadrement

$$(iv) \quad 0 \leq 1 - c(y) \leq 2\pi^2 y^2.$$

Soit $\alpha(x)$, pour $0 < x \leq \frac{1}{4}$, l'arc réalisant la distance de i à l'axe réel sur un cercle orthogonal à l'axe réel et faisant en i un angle de $2\pi x$ avec l'axe imaginaire. Sa longueur est $\frac{2\pi x}{s(x)}$. L'arc concave $\alpha(y)$ étant, si $\frac{1}{4} \geq y > x > 0$, extérieur à $\alpha(x)$, la fonction $\frac{x}{s(x)}$ est croissante sur $]0, \frac{1}{4}]$, ainsi sur cet intervalle, on a la minoration

$$(v) \quad 4x \leq s(x).$$

La fonction c est positive et décroît sur $[0, \frac{1}{4}]$. Comme $c(\frac{1}{8}) = s(\frac{1}{8}) = \sqrt{\frac{1}{2}}$, il vient

$$(vi) \quad 4\sqrt{2} c(x) x \leq s(x).$$

Si N et p sont des entiers et x est non entier les sommes géométriques

$$T_{N,x}(p) = \sum_{k=1-N}^p e(kx) = e((1-N)x) \frac{e((p+N)x) - 1}{e(x) - 1} = \frac{e(px) - e(-Nx)}{1 - e(-x)}$$

sont nulle pour $p = -N$ et les doubles de leurs parties réelles

$$(vii) \quad C_{N,x}(p) = \sum_{k=1-N}^p 2c(kx) = \frac{\nu_{N,x}(p)}{|1 - e(x)|^2} = \frac{\nu_{N,x}(p)}{4s(\frac{x}{2})^2}$$

où les réels $\nu_{N,x}(p)$, somme de huit racines de l'unité, vérifient

$$(viii) \quad |\nu_{N,x}(p)| \leq 8$$

de plus,

$$(ix) \quad C_{N,x}(p) - C_{N,x}(-p) = \frac{4s(px)s(x)}{4s(\frac{x}{2})^2} = 2s(px) \frac{c(\frac{x}{2})}{s(\frac{x}{2})}.$$

Si N est impair et x non entier, la somme symétrique $T_{\frac{N+1}{2},x}(\frac{N-1}{2})$ vaut

$$S_N(x) = \sum_{q=\frac{1-N}{2}}^{\frac{N-1}{2}} e(qx) = \frac{e(\frac{N-1}{2}x) - e(-\frac{N+1}{2}x)}{1 - e(-x)}$$

$$(x) \quad S_N(x) = 1 + 2 \sum_{q=1}^{\frac{N-1}{2}} c(qx) = \frac{s(\frac{Nx}{2})}{s(\frac{x}{2})}.$$

Notons enfin que l'on obtient par récurrence sur l'entier positif p les formules :

$$(xi') \quad \sum_{k=1}^{p-1} k = \frac{p(p-1)}{2}$$

$$(xi'') \quad \sum_{k=1}^{p-1} k^2 = \frac{p(p-1)(2p-1)}{6}.$$

En particulier

$$(xi) \quad \sum_{k=1}^{\frac{N-1}{2}} k^2 = \frac{N(N^2-1)}{24}.$$

D'où, si θ est non demi-entier, d'après (x) pour $x = 2\theta$ et (iv) pour $y = 2q\theta$, l'encadrement

$$(xii) \quad N \left[1 - \frac{2\pi^2}{3} (N^2 - 1) \theta^2 \right] \leq \frac{s(N\theta)}{s(\theta)} \leq N.$$

Les relations (xii) et (iii') donnent la majoration

$$(8) \quad |A_N - \sqrt{2N^2} \gamma(Q_1)| \\ \leq \frac{2\pi^2}{3} (N^2 - 1) N \frac{1}{4M^2} + 2\pi \frac{1}{4M} N = \frac{\pi(\pi+3)}{6} \frac{N}{M}.$$

Avec (iii) pour les numérateurs des fractions dans les termes de B_N et (v) pour leurs dénominateurs (car, dans (6), on a $\frac{Np}{2M} < \frac{1}{4}$) on obtient la majoration

$$(9) \quad |B_N| \leq 2 \sum_{p=1}^{\frac{N-1}{2}} 2\pi \frac{p}{2M} \frac{2M}{4Np} = \frac{\pi}{2} \frac{N-1}{N} < \frac{\pi}{2}.$$

On opère de même sur l'expression (7') de C_N , puisqu'alors on a $\frac{Nb-1}{2M} < \frac{1}{4}$:

$$(10) \quad |C_N| \leq 2 \sum_{b=1}^{\frac{N-1}{2}} 2\pi \frac{N-b}{2M} \frac{2M}{4(Nb-1)} \leq \pi \frac{N-1}{N} \sum_{b=1}^{\frac{N-1}{2}} \frac{1}{b - \frac{1}{N}} \\ = \pi \frac{N-1}{N} \left[\sum_{b=1}^k \frac{1}{b - \frac{1}{N}} + \sum_{b=k+1}^{\frac{N-1}{2}} \frac{1}{b - \frac{1}{N}} \right] \\ \leq \pi \frac{N-1}{N} \left[\frac{N}{N-1} k + \left(\frac{N-1}{2} - k \right) \frac{N}{N-1} \frac{1}{k+1 + \frac{k}{N-1}} \right]$$

d'où, en prenant pour $k = \lfloor \sqrt{\frac{N-1}{2}} \rfloor$ la partie entière de $\sqrt{\frac{N-1}{2}}$, la majoration

$$(11) \quad |C_N| \leq \pi \sqrt{2} \sqrt{N-1}.$$

De (3), (8), (9) et (11) on tire par inégalité triangulaire :

$$(12) \quad \left| \frac{1}{\sqrt{2M}} [\Gamma_{N,1} - \sqrt{2N^2} \gamma(Q_1)] \right| \\ \leq \frac{1}{\sqrt{2M}} \left[\frac{\pi(\pi+3)}{6} \frac{N}{M} + \frac{\pi}{2} + \pi \sqrt{2} \sqrt{N-1} + 2 \right] \\ = \frac{\pi}{\sqrt{2(N+1)}} \left[\frac{\pi+3}{6} \frac{N}{M \sqrt{N-1}} + \frac{1}{2\sqrt{N-1}} + \sqrt{2} + \frac{2}{\pi \sqrt{N-1}} \right]$$

soit, puisque $N = 2m + 1 \geq 3$ et $\pi \leq 4$ l'approximation (A) de l'introduction.

4. Estimation du second morceau $\Gamma_{N,2}$.

Notons $\tilde{\Gamma}_{N,2}$ la somme des seconds termes de (T_k) étendue à tous les entiers $k = p + 2Nq$ où p et q vérifient $-N < p \leq N$ et $\frac{1-N}{2} \leq q \leq \frac{N-1}{2}$ et

$$(13) \quad \Gamma_{N,2}(q) = \sum_{p=1-N}^N e\left(\frac{p^2}{4M}\right) 2c\left(\frac{Npq}{M}\right) \left[e\left(\frac{q^2}{M}\right) - 1\right].$$

Le second morceau $\Gamma_{N,2}$ s'écrit alors

$$(14) \quad \Gamma_{N,2} = \tilde{\Gamma}_{N,2} - R_{N,2} = \sum_{q=1}^{\frac{N-1}{2}} \Gamma_{N,2}(q) - R_{N,2}$$

où l'excédent $R_{N,2}$ est maintenant de module au plus 4 :

$$(15) \quad |R_{N,2}| \leq 4.$$

Posons $C_N^q(p) = C_{N, \frac{Nq}{M}}(p)$. Comme $\frac{Nq}{M}$ est non entier, cette somme se calcule par la formule (vii) et celle qui la précède, en particulier nulle pour $p = -N$. En reportant dans (13) la valeur $2c\left(\frac{Npq}{M}\right) = C_N^q(p) - C_N^q(p-1)$ nous avons :

$$(16) \quad \Gamma_{N,2}(q) = \sum_{p=1-N}^N e\left(\frac{p^2}{4N}\right) [C_N^q(p) - C_N^q(p-1)] \left[e\left(\frac{q^2}{M}\right) - 1\right]$$

donc en réordonnant suivant les $C_N^q(p)$ et posant :

$$\begin{aligned} D_N^q &= e\left(\frac{N^2}{4M}\right) C_N^q(N) \left[e\left(\frac{q^2}{M}\right) - 1\right] \\ &= ie\left(\frac{1}{4M}\right) 2s\left(\frac{N^2q}{M}\right) \frac{c\left(\frac{Nq}{2M}\right)}{s\left(\frac{Nq}{2M}\right)} \left[e\left(\frac{q^2}{M}\right) - 1\right] \end{aligned}$$

car $N^2 = M + 1$, et d'après la relation (ix), puisque $C_N^q(-N) = 0$ donc

$$(17) \quad D_N^q = ie\left(\frac{1}{4M}\right) 2s\left(\frac{q}{M}\right) \frac{c\left(\frac{Nq}{2M}\right)}{s\left(\frac{Nq}{2M}\right)} \left[e\left(\frac{q^2}{M}\right) - 1\right]$$

nous obtenons, puisque $C_N^q(-N) = 0$, la relation

$$\begin{aligned} \Gamma_{N,2}(q) &= D_N^q + \sum_{p=1-N}^{N-1} \left[e\left(\frac{p^2}{4M}\right) - e\left(\frac{(p+1)^2}{4M}\right) \right] C_N^q(p) \left[e\left(\frac{q^2}{M}\right) - 1 \right] \\ (18) \quad \Gamma_{N,2}(q) &= D_N^q \\ &\quad + \sum_{p=1-N}^{N-1} e\left(\frac{p^2}{4M}\right) \left[1 - e\left(\frac{p}{2M}\right) e\left(\frac{1}{4M}\right) \right] C_N^q(p) \left[e\left(\frac{q^2}{M}\right) - 1 \right]. \end{aligned}$$

Ainsi $\Gamma_{N,2} = \tilde{\Gamma}_{N,2} - R_{N,2} = D_N + E_N + F_N + G_N - R_{N,2}$ où pour $X = D, E, F, G$ on a noté $X_N = \sum_{q=1}^{\frac{N-1}{2}} X_N^q$, avec, si $\nu_N^q(p) = \nu_{N, \frac{Nq}{M}}(p)$, les X_N^q donnés par (17) ci-dessus et (19), (20), (21) ci-dessous :

$$\begin{aligned} E_N^q &= \sum_{p=1-N}^{N-1} e\left(\frac{p^2}{4M}\right) \left[1 - e\left(\frac{1}{4M}\right) \right] C_N^q(p) \left[e\left(\frac{q^2}{M}\right) - 1 \right] \\ (19) \quad E_N^q &= \sum_{p=1-N}^{N-1} e\left(\frac{p^2}{4M}\right) \left[1 - e\left(\frac{1}{4M}\right) \right] \frac{\nu_N^q(p)}{4s\left(\frac{Nq}{2M}\right)^2} \left[e\left(\frac{q^2}{M}\right) - 1 \right] \end{aligned}$$

$$F_N^q = \sum_{p=1}^{N-1} e\left(\frac{p^2}{4M}\right) e\left(\frac{1}{4M}\right) 2 \left[1 - c\left(\frac{p}{2M}\right) \right] C_N^q(p) \left[e\left(\frac{q^2}{M}\right) - 1 \right]$$

$$\begin{aligned} (20) \quad F_N^q &= \sum_{p=1}^{N-1} e\left(\frac{p^2}{4M}\right) e\left(\frac{1}{4M}\right) \\ &\quad 2 \left[1 - c\left(\frac{p}{2M}\right) \right] \frac{\nu_N^q(p)}{4s\left(\frac{Nq}{2M}\right)^2} \left[e\left(\frac{q^2}{M}\right) - 1 \right] \end{aligned}$$

$$\begin{aligned} G_N^q &= \sum_{p=1}^{N-1} e\left(\frac{p^2}{4M}\right) e\left(\frac{1}{4M}\right) \\ &\quad \left[1 - e\left(\frac{-p}{2M}\right) \right] [C_N^q(-p) - C_N^q(p)] \left[e\left(\frac{q^2}{M}\right) - 1 \right] \end{aligned}$$

$$\begin{aligned} (21) \quad G_N^q &= \sum_{p=1}^{N-1} e\left(\frac{p^2}{4M}\right) e\left(\frac{1}{4M}\right) \\ &\quad \left[1 - e\left(\frac{-p}{2M}\right) \right] - 2s\left(\frac{Npq}{M}\right) \frac{c\left(\frac{Nq}{2M}\right)}{s\left(\frac{Nq}{2M}\right)} \left[e\left(\frac{q^2}{M}\right) - 1 \right]. \end{aligned}$$

Pour majorer les modules des X_N il nous suffit de sommer en q les majorations des X_N^q obtenues en utilisant les inégalités du §1 :

Pour D_N on enfile sur (17) les inégalités (iii), (vi) et (iii') puis (xi) :

$$(22) \quad |D_N| \leq 2 \sum_{q=1}^{\frac{N-1}{2}} 2\pi \frac{q}{M} \frac{1}{4\sqrt{2}} \frac{2M}{Nq} 2\pi \frac{q^2}{M} = \frac{2\sqrt{2}}{MN} \pi^2 \sum_{q=1}^{\frac{N-1}{2}} q^2 = \frac{\pi^2 \sqrt{2}}{12}.$$

Pour E_N on enfile sur (19) les inégalités (iii'), (viii), (v) et (iii') :

$$(23) \quad |E_N| \leq \sum_{q=1}^{\frac{N-1}{2}} \sum_{p=1-N}^N 2\pi \frac{1}{4M} \frac{8 \cdot 4M^2}{4 \cdot 16N^2 q^2} 2\pi \frac{q^2}{M} \\ = \frac{\pi^2}{2N^2} 2N \frac{N-1}{2} < \frac{\pi^2}{2}.$$

Pour F_N on enfile sur (20) les inégalités (iv), (viii), (v) et (iii') puis (xi'') :

$$(24) \quad |F_N| \leq \sum_{q=1}^{\frac{N-1}{2}} \sum_{p=1}^{N-1} 2\pi^2 \frac{p^2}{4M^2} \frac{8 \cdot 4M^2}{4 \cdot 16N^2 q^2} 2\pi \frac{q^2}{M} \\ = \sum_{q=1}^{\frac{N-1}{2}} \sum_{p=1}^{N-1} \frac{\pi^3 p^2}{N^2 M} = \frac{\pi^3 N(N-1)(2N-1)}{6N^2 M} \frac{N-1}{2} < \frac{\pi^3}{6}.$$

Pour G_N enfin, on enfile sur (21) les inégalités (iii'), (vi) et (iii') :

$$|G_N| \leq \sum_{q=1}^{\frac{N-1}{2}} \sum_{p=1}^{N-1} 2\pi \frac{p}{2M} 2 \frac{2M}{4\sqrt{2}Nq} 2\pi \frac{q^2}{M} = \sum_{q=1}^{\frac{N-1}{2}} \sum_{p=1}^{N-1} \pi^2 \sqrt{2} \frac{pq}{NM}$$

donc, d'après la formule (xi'), ce « gros » terme admet la majoration :

$$(25) \quad |G_N| \leq \frac{\pi^2 \sqrt{2}}{NM} \frac{N(N-1)}{2} \frac{1}{2} \frac{N+1}{2} \frac{N-1}{2} \\ = \frac{\pi^2 \sqrt{2}(N-1)}{16} \leq \sqrt{2M} \frac{\pi^2}{16}.$$

Ainsi de (22), (23), (24), (25) et (15) on tire par l'inégalité triangulaire :

$$(26) \quad \left| \frac{1}{\sqrt{2M}} \Gamma_{N,2} \right| \leq \frac{1}{\sqrt{2M}} \left[\frac{\pi^2}{12} (\sqrt{2} + 6 + 2\pi) + \sqrt{2M} \frac{\pi^2}{16} + 4 \right]$$

d'où, puisque $\pi \leq 4$ et $\sqrt{2} \geq 1$, la majoration (M) de l'introduction.

Appendice.

Le formalisme des groupes de Witt

1. Soit A un anneau commutatif.

Une *forme quadratique* sur un A -module M de type fini à valeurs dans un A -module K est une application $q : M \rightarrow K$ qui est

(i) homogène de degré 2 (pour tout m de M et a de A on a $q(am) = a^2 q(m)$);

et telle que, en notant $b(m, n) = m \cdot n = q(m+n) - q(m) - q(n)$:

(ii) l'application $b : M \times M \rightarrow K$ est bilinéaire.

On dit que s est la *forme bilinéaire sous-jacente* à la forme quadratique.

Le dièse $b^\sharp : M \rightarrow \text{Hom}_A(M, K)$ de b est l'application qui à n de M associe l'application linéaire $b^\sharp(n)$ envoyant tout m de M sur $b(m, n)$. Une forme quadratique est *non dégénérée* si $b^\sharp$ est un isomorphisme de M sur $\text{Hom}_A(M, K)$.

On suppose désormais les formes quadratiques non dégénérées et soit que $A = K$ est un corps soit que M est un groupe abélien fini, $A = \mathbb{Z}$ et $K = \mathbb{Q}/\mathbb{Z}$. Un tel couple (M, q) sera appelé *espace quadratique*, ou *q-espace*, sur le corps K dans le premier cas et *module d'enlacement quadratique*, ou *qe-module* dans le second.

Deux éléments $n, m \in M$ sont dit *orthogonaux* pour la forme bilinéaire b si $b(n, m) = 0$. L'*orthogonal* d'un sous-module $S \subset M$ est le sous-module $S^\perp = \{m \in M \mid \forall s \in S \text{ on a } b(s, m) = 0\}$ formé des éléments orthogonaux à tous les éléments de S , c'est le noyau de la composée $\iota_S^* \circ b^\sharp$ du dièse et de l'application de restriction à S .

Tout *qe-module* est somme orthogonale de ses composantes p -primaires.

Un sous-module $I \subset M$ sur lequel la forme quadratique q s'annule est dit *q-isotrope*. Une forme quadratique est dite *anisotrope* si le sous-module nul 0 est le seul sous-module *q-isotrope*.

2. On dit qu'un sous-module $L \subset M$ est un *Lagrangien quadratique* de la forme quadratique q s'il est isotrope ($q(L) = 0$) et égal à son orthogonal ($L = L^\perp$).

Une forme quadratique est *neutre* si elle possède un Lagrangien quadratique. Un *q-espace neutre* est de dimension paire $d = 2k$ et est

isomorphe au q -espace hyperbolique $(V^* \oplus V, h_V)$ sur un espace vectoriel V de dimension k qui à $(f, v) \in V^* \oplus V$ associe $h_V(f, v) = f(v)$. Un q -module neutre a pour nombre d'éléments un carré mais, cette fois sa classe d'isomorphisme n'est pas déterminée par son nombre d'éléments.

Deux formes $q_1 : M_1 \rightarrow K$ et $q_2 : M_2 \rightarrow K$ sont liées par la relation de Witt si leur «différence orthogonale» $q = q_1 \oplus -q_2 : M_1 \oplus M_2 \rightarrow K$, qui à $m = (m_1, m_2) \in M_1 \oplus M_2$ associe $q(m) = q_1(m_1) - q_2(m_2)$, est neutre.

Cette relation de Witt est une relation d'équivalence compatible avec la somme orthogonale. La somme orthogonale induit sur l'ensemble quotient une structure de groupe abélien. On note ce groupe $WQ(K)$ dans le premier cas et $WQ(\mathbb{Q}, \mathbb{Z})$ dans le second, ce sont le groupe de Witt quadratique du corps K et le groupe de Witt-Pontryaguine quadratique.

Par la décomposition d'un q -module en somme orthogonale de ses composantes p -primaires, ce dernier est isomorphe à la somme directe des groupes de Witt-Pontryaguine quadratiques des p -groupes :

$$WQ(\mathbb{Q}, \mathbb{Z}) = \oplus WQ_p(\mathbb{Q}, \mathbb{Z})$$

La relation de Witt est impliquée par l'isomorphisme et réciproquement :

Toute forme quadratique est Witt-équivalente à une forme quadratique anisotrope et la classe d'isomorphisme d'une forme quadratique anisotrope est déterminée par sa classe de Witt.

Tout q -espace est somme orthogonale d'un de ses représentants anisotropes et d'une forme neutre, d'où le Théorème de Witt :

Deux formes quadratiques sur un corps K sont isomorphes si et seulement si elles ont même dimension et même classe de Witt.

3. Un réseau dans l'espace vectoriel M d'un q -espace rationnel est un sous-groupe de type fini $\mathcal{R}$ de M engendrant M comme espace vectoriel.

Il est dit entier si les valeurs de la forme q sur $\mathcal{R}$ sont entières. Un réseau entier $\mathcal{R}$ est inclus dans son réseau dièse

$$\mathcal{R}^\# = \{m \in M \mid \forall r \in \mathcal{R} \text{ on a } b(r, m) \in \mathbb{Z}\}$$

et on a un enlacement quadratique $(\mathcal{R}^\#/\mathcal{R}, q_{\mathcal{R}})$ où $q_{\mathcal{R}} : \mathcal{R}^\#/\mathcal{R} \rightarrow \mathbb{Q}/\mathbb{Z}$ est la forme $q_{\mathcal{R}}(r + L) = q(r) + \mathbb{Z}$ induite par q .

La classe de Witt de $q_{\mathcal{R}}$ dans le groupe de Witt-Pontryaguine quadratique ne dépend que de celle de (M, q) dans le groupe de Witt quadratique rationnel, cette association définissant un morphisme dit *bord quadratique* :

$$\partial_q : WQ(\mathbb{Q}) \rightarrow WQ(\mathbb{Q}, \mathbb{Z})$$

dont le noyau, formé des classes d'espaces quadratiques (M, q) possédant un réseau entier $\mathcal{R}$ *unimodulaire*, c'est-à-dire égal à son dièse $\mathcal{R}^\sharp$, est le groupe de Witt quadratique unimodulaire $WQ(\mathbb{Z})$.

4. On opère de même, avec les formes bilinéaires symétriques non dégénérées.

Si B est la matrice dans une base de la forme bilinéaire symétrique b d'un b -espace de dimension d alors la classe de $(\bar{d}, [(-1)^{\frac{d(d-1)}{2}} \det(B)])$ dans $D(K)$ ne dépend que de la classe de Witt de b et définit un morphisme $\delta : W(K) \rightarrow D(K)$ dit *discriminant total* qui est déjà surjectif sur les b -espaces de rang au plus 2.

Ainsi d'après le théorème de Chevalley, *tout b -espace de rang supérieur à deux sur un corps fini est isotrope* (cf. [6] p. 12-14), le discriminant total est un isomorphisme dans le cas d'un corps fini. En particulier en ce cas $W(K)$ a 2 éléments si la caractéristique de K est 2 et 4 éléments sinon. Ainsi le groupe de Witt-Pontryaguine, isomorphe à la somme directe $\oplus W(\mathbb{Z}/p\mathbb{Z})$, est de 4-torsion.

En général tout espace bilinéaire anisotrope se diagonalise, c'est-à-dire est somme orthogonale d'espaces de rang un isomorphes à $\langle a \rangle = (K \times K, (x, y) \mapsto axy)$ où $a \in K^*$ est un élément inversible de K . La classe de a modulo les carrés ne dépendant que de la classe d'isomorphisme de $\langle a \rangle$, le groupe de Witt de K est engendré par les classes $[\langle a \rangle]$ où a parcourt un système de représentants de K^* modulo les carrés K^{**} .

Comme $\mathbb{R}^*/(\mathbb{R}^*)^2 = \{-1, +1\}$ tout espace quadratique réel (M, q) est isomorphe à une somme orthogonale de u copies de $\langle 1 \rangle$ et de v copies de $\langle -1 \rangle$, la différence $s = u - v$ ne dépend que de la classe de Witt de (M, q) et réalise l'*isomorphisme de signature*

$$s : W(\mathbb{R}) \rightarrow \mathbb{Z}$$

du groupe de Witt des réels sur les entiers.

Un morphisme entre deux corps induit un morphisme de leurs groupes de Witt, d'où le morphisme dit de *signature*

$$\sigma : W(\mathbb{Q}) \rightarrow W(\mathbb{R}) \xrightarrow{s} \mathbb{Z}$$

on montre simultanément que sa restriction à $W(\mathbb{Z})$ est un isomorphisme et que le bord $\partial_b : W(\mathbb{Q}) \rightarrow W(\mathbb{Q}, \mathbb{Z}) \simeq \oplus W(\mathbb{Z}/p\mathbb{Z})$ est surjectif. D'où la forme faible du théorème de Hasse-Minkowski :

Le morphisme (σ, ∂_q) est un isomorphisme du groupe de Witt des rationnels sur le produit des entiers par le groupe de Witt-Pontryaguine.

5. On note

$$V(\mathbb{Q}, \mathbb{Z}) = \text{Ker}(\sigma : W(\mathbb{Q}, \mathbb{Z}) \longrightarrow W(\mathbb{Q}, \mathbb{Z})),$$

le noyau du morphisme d'oubli.

Si L est un lagrangien bilinéaire d'un représentant (M, q) d'un élément de $V(\mathbb{Q}, \mathbb{Z})$ alors la restriction de q à L est linéaire donc donnée par le produit par un élément $\omega \in M$ bien défini modulo L et dont la valeur $q(\omega)$ est d'ordre 8 et ne dépend pas de son choix. Ce procédé réalise un isomorphisme de $V(\mathbb{Q}, \mathbb{Z})$ sur le groupe cyclique des éléments d'ordre 8 de $\mathbb{Q}/\mathbb{Z}$.

Comme $\langle 1 \rangle \oplus \langle 1 \rangle$ et $\langle 2 \rangle \oplus \langle 2 \rangle$ sont rationnellement isomorphes la classe de la forme quadratique rationnelle associée à $\langle 1 \rangle \oplus \langle -2 \rangle$ est d'ordre 2 dans le groupe de Witt quadratique $WQ(\mathbb{Q})$ et son bord scinde le facteur $o_2 : WQ_2(\mathbb{Q}, \mathbb{Z}) \rightarrow W_2(\mathbb{Q}, \mathbb{Z}) \simeq W(\mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$ de o correspondant aux groupes 2-primaires, ainsi l'oubli o est scindé, puisqu'il est un isomorphisme sur l'autre facteur, correspondant aux groupes d'ordre impair.

En particulier, le groupe de Witt-Pontryaguine $W(\mathbb{Q}, \mathbb{Z})$ étant tué par 4, le groupe de Witt-Pontryaguine quadratique $WQ(\mathbb{Q}, \mathbb{Z})$ est tué par 8.

Soit (M, q) un qe -module alors la somme de Gauss normalisée

$$\gamma(q) = \frac{1}{\sqrt{\#M}} \sum_{m \in M} \exp(2\pi i q(m))$$

est une racine de l'unité qui ne dépend que de la classe de Witt de (M, q) . Son ordre est un diviseur de 8 et l'application $\gamma : WQ(\mathbb{Q}, \mathbb{Z}) \rightarrow \mu_8$ ainsi définie est un morphisme de groupe induisant un isomorphisme sur $V(\mathbb{Q}, \mathbb{Z})$.

BIBLIOGRAPHIE

Les titres [2], [3] ne renvoient pas au texte mais précisent, tout comme [1] et [4], les commentaires historiques de la version française du résumé.

- [1] J. BARGE, J. LANNES, F. LATOUR et P. VOGEL, Appendice de Λ -Sphères, Annales scientifiques de l'École Normale Supérieure, 4^e série, t. 7, fasc. 4 (1974), 494-505.
- [2] H. BRAUN, Geschlechter quadratischer Formen, Journal für die reine und angewandte Mathematik, 182 (1940), 36.
- [3] K. CHANDRASEKHARAN, Elliptic functions, Grundlehren der mathematischen Wissenschaften, 281, Chap IX Springer Verlag, 1985.

- [4] J. MILNOR et D. HUSEMOLLER, Symmetric bilinear forms, *Ergebnisse der Mathematik und ihrer Grenzgebiete*, B. 73, Springer Verlag, 24-26 et Appendix 4, 1973.
- [5] C. MOSER, Cours de quadratique : Formes et Topologie, rédaction de [7], à paraître (paraît-il) aux Publication de l'I.R.E.M.
- [6] J.-P. SERRE, Cours d'arithmétique, P.U.F, 1970.
- [7] Formes quadratiques et topologie, trois conférences, Tradition orale, 1995.

Manuscrit reçu le 9 octobre 2002,
accepté le 12 novembre 2002.

Catherine BAILLY et Maria de Jesus CABRAL,
Rua da Amendoeira 29
1100-023 Lisboa (Portugal).