Sommes de carrés
D'après Milnor-Husemoller

3 juin 2025

Objectifs :

— Donner quelques compléments sur la multiplicativité, la torsion dans l'anneau de Witt.
— Démontrer que tout entier est somme de quatre carrés à l'aide du théorème de Minkowski.
— Déduire de la formule de Siegel celle de Jacobi donnant le nombre de décompositions d'un entier comme somme de quatre carrés.

1 Multiplicativité

Rappels : Ici, X est un espace quadratique sur un corps $\mathbb{F}$.

Définition 1. X est **multiplicatif** si pour tout r non-nul dans $\mathbb{F}$ représenté par X, il existe un isomorphisme

$$\langle r\rangle \otimes X \cong X.$$

Lemme 2. *Les formes de Pfister sont multplicatives.*

Proposition 3. *Si X est multiplicatif, l'ensemble des éléments représentables par X de F est un sous-groupe de $\mathbb{F}^*$.*

Théorème 4. *Si X est multiplicatif, $(\langle 1\rangle \oplus \langle \alpha\rangle) \otimes X$ l'est aussi (pour tout α dans $\mathbb{F}^*$).*

Corollaire 5. *Soit n un entier naturel. Le produit de deux sommes de 2^n carrés est une somme de 2^n carrés.*

Comme indiqué par Marco, il existe donc des formules universelles pour récrire un produit de sommes de 2, 4, 8, 16 carrés comme sommes du même type. Cependant, en suivant la démonstration du théorème donnée par Milnor, il apparaît que ces formules, qui dépendent de choix d'isomorphismes $aX \cong X$, sont **a priori** non symétriques en les facteurs et susceptibles de faire apparaître des dénominateurs. Elle ne peuvent, a priori, pas être utilisées pour justifier, par exemple, qu'un produit de sommes de 2^n carrés *d'entiers* est une somme de 2^n carrés *d'entiers*. En rang 2, 4 et 8, l'existence des algèbres normées des entiers de Gauss, des quaternions de Hamilton et des octonions permettent d'interpréter une somme carrés comme une valeur d'une norme N multiplicative et d'en déduire des formules valables dans tout anneau :

— Dans l'anneau des entiers de Gauss :

$$\begin{aligned}(a^2+b^2)(A^2+B^2) &= N(a+bi)N(A+Bi)\\ &= N((a+bi)(A+Bi))\\ &= N((aA-bB)+(aB+bA)i)\\ &= (aA-bB)^2+(aB+bA)^2\end{aligned}$$

— Dans l'anneau non commutatif des quaternionsn nous obtenons l'identité d'Euler-Hamilton :

$$\begin{aligned}(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2) =& N(a+bi+jc+kd)N(A+Bi+jC+kD)\\ =& N(a+bi+cj+dk)(A+Bi+Cj+Dk))\\ =& N((aA–bB–cC–dD)+(aB+bA+cD–dC)i+(aC–bD+cA+dB)j+(aD+bC–cB+dA)k)\\ =& (aA-bB-cC-dD)^2+(aB+bA+cD-dC)^2\\ &+(aC-bD+cA+dB)^2+(aD+bC-cB+dA)^2\end{aligned}$$

Proposition 6. *Si α est une somme de 2^n carrés dans $\mathbb{F}$, alors $<1>-<\alpha>$ est de 2^n-torsion dans l'anneau de Witt de $\mathbb{F}$.*

Démonstration. $2^n<\alpha>=<\alpha>(<1>+\cdots+<1>)=<1>+\cdots+<1>=2^n<1>$, vu que $<1>+\cdots+<1>$ est multiplicative par le théorème 4 et représente α par hypothèse. □

Exemple 7. Comme $5=1^2+2^2$,

$$5X^2+5Y^2=(1^2+2^2)(X^2+Y^2)=(X+2Y)^2+(2X-Y)^2$$

ce qui montre que $<5>\oplus<5>$ est isomorphe (sur $\mathbb{Q}$) à $<1>\oplus<1>$ via $(X,Y)\mapsto(X+2Y,2X-Y)$. Ainsi $<1>-<5>$ est de 2-torsion dans l'anneau de Witt de $\mathbb{Q}$.
De même $7=2^2+1^2+1^2+1^2$ et $(A,B,C,D)\mapsto(2A-B-C-D,2B+A+D-C,2C-D+A+B,2D+C-B+A)$ fournit un isomorphisme de $<7>^{\oplus 4}$ dans $<1>^{\oplus 4}$. Ainsi $<1>-<7>$ est de 4-torsion dans l'anneau de Witt de $\mathbb{Q}$.

Remarque 8 (Post exposé)**.** En fait, en choisissant judicieusement les isomorphismes de multiplicativité $\langle r\rangle\otimes X\cong X$ dans la démonstration récursive de Milnor du théorème 4, il est bien possible d'obtenir l'identité d'Euler-Hamilton dans tout corps, donc en particulier dans le corps des fractions d'un anneau et donc, lorsque celui-ci est intègre, dans l'anneau lui-même. D'une manière générale, si $V\mapsto x\circ V$ (resp. $V\mapsto x^{-1}\circ V$) désigne un choix d'isomorphisme de multiplicativité entre $\langle x^2\rangle\otimes X$ (resp. $\langle(1/x^2)\rangle\otimes X$) et X (pour tout x dans X tel que $x^2\neq 0$), il semble que

$$\begin{array}{rcl}\langle x^2+\alpha y^2\rangle\otimes(X\oplus\langle\alpha\rangle\otimes X) & \to & X\oplus\langle\alpha\rangle X\\ (U,V) & \mapsto & (x\circ U-\alpha y^2y^{-1}\circ V, x^2y\circ x^{-1}\circ y^{-1}\circ V+y\circ U)\end{array}$$

fournisse un isomorphisme de multiplicativité, sous réserve que les isométries $x\circ$ et $x^{-1}\circ$ aient été choisies inverses l'unie de l'autre et que $(x^2)^2\circ$ soit la multiplication par x^2. Si de surcroît les $x^{-1}\circ$ et $y\circ$ commutent, cette isométrie se récrit

$$(U,V)\mapsto(x\circ U-\alpha y^2y^{-1}\circ V, x^2x^{-1}\circ V+y\circ U)$$

Dans le cas du passage de $n=1$ à $n=2$ (i.e. $X=\langle 1\rangle\oplus\langle 1\rangle$), X s'identifie à l'anneau de Gauss $\mathbb{F}[i]$ et il est possible de choisir pour $x\circ$ (resp $y\circ$) la multiplication à gauche par x (resp. par y) puis de poser $x^{-1}\circ:=\frac{\bar{x}}{x^2}\circ$ de sorte que les deux contraintes (unité et commutativité) sus-mentionnées soient satisfaites et que l'isométrie prenne la forme

$$(U,V)\mapsto(xU-\alpha\bar{y}V,\bar{x}V+yU).$$

En termes matriciels, si $x=(a,b)$, $x\circ$ a pour matrice

$$\begin{pmatrix}a & b\\ -b & a\end{pmatrix}$$

et il est clair que deux matrices de cette forme commutent (similitudes directes !) et que l'inverse d'une telle matrice est celle de la même forme, associée à $\frac{\bar{x}}{x^2}$. Concrètement, avec $x=(a,b)=a+bi$, $y=(c,d)=c+di$, $U=(A,B)=A+Bi$, $V=(C,D)=C+Di$ et $\alpha=1$,

$$(xU-\alpha\bar{y}V,\bar{x}V+yU)=(aA-bB-cC-dD,aB+bA-cD+dC,aC+bD+cA-dB,aD-bC+cB+dA)$$

et correspond bien au produit des quaternions $A+Bi+Cj+Dk$ et $a+bi+cj+dk$ (dans cet ordre).

Je ne sais toujours pas ce qu'il en est en rang 8 car le produit des quaternions n'est pas commutatif donc la contrainte "$x\circ$ et $y\circ$ commutent" semble impossible à satisfaire "naturellement" pour déduire une éventuelle identité des huit carrés sans dénominateurs de celle d'Euler-Hamilton (passage de $n=2$ à $n=3$ obstrué par la non commutativité du produit quaternionique ?).

2 Théorèmes de Minkowski et de Lagrange

Le deuxième cas de l'exemple est en fait général puisque

Théorème 9. *(Lagrange 1770) Tout entier naturel est la somme de quatre carrés d'entiers.*

2.1 Démonstration via le théorème de Minkowski

Nous allons montrer que le théorème de Lagrange découle du corollaire suivant le théorème de Minkowski déjà évoqué :

Théorème 10. *(Minkowski 1896) Soit L un réseau de $\mathbb{R}^d$. Si $K\subset\mathbb{R}^d$ est un convexe symétrique par rapport à l'origine tel que $\mathrm{Vol}(K)>2^d\mathrm{Vol}(\mathbb{R}^r/L)$ alors K un point non nul de L.*

Corollaire 11. *Soit L un réseau de $\mathbb{R}^d$. Alors L contient un point non nul de norme inférieure ou égale à*

$$2\left(\frac{\mathrm{Vol}(\mathbb{R}^d/L)}{\omega_d}\right)^{1/d}$$

où ω_d désigne le volume la boule unité dans $\mathbb{R}^d$.

Démonstration du théorème des quatre carrés de Lagrange. Soit p un entier premier. Le principe des paires chaussettes implique l'existence de u et v tels que $u^2+v^2+1=0$ modulo p. Soit L le réseau de $\mathbb{R}^4$ constitué des quadruplets d'entiers (a,b,c,d) tels que $au+bv=c$ et $av-bu=d$ modulo p. L'indice de L dans $\mathbb{R}^4$ est p^2 donc

$$\mathrm{Vol}(\mathbb{R}^4/L)=p^2.$$

D'après le corollaire du théorème de Minkowski, L contient un point (a,b,c,d) non-nul dont le carré de la norme est inférieur à

$$4\left(\frac{\mathrm{Vol}(\mathbb{R}^4/L)}{\omega_4}\right)^{2/4}=\frac{4\sqrt{2}}{\pi}p<2p$$

vu que $\omega_4=\frac{\pi^2}{2}$. Or, le carré de la norme de (a,b,c,d) vérifie aussi

$$0\neq a^2+b^2+c^2+d^2=a^2+b^2+(au+bv)^2+(av-bu)^2\equiv 0 \bmod p$$

donc $a^2+b^2+c^2+d^2=p$ ce qui montre que p est somme de quatre carrés d'entiers. Cette propriété étant stable par produit d'après l'exemple 7, c'est aussi le cas de tout entier naturel. □

2.2 Démonstration via le théorème de Hasse-Minkowski

Serre ([1])) commence par établir que a est représentable par la forme canonique de rang 3 si et seulement si il n'est pas de la forme $4^q(8m-1)$ (résultat dû à Gauss), en s'appuyant le théorème de Hasse-Minkowski (représentabilité sur $\mathbb{Q}$) et un lemme de Cassels-Davenport (passage de $\mathbb{Q}$ à $\mathbb{Z}$), puis passe au cas de rang 4 (Lagrange) en remarquant que dans le cas où a est de la forme $4^q(8m-1)$, $8m-2$ est somme de trois carrés donc $8m-1$ est somme de quatre carrés.

3 Formules de Siegel et de Jacobi

Le théorème de Lagrange assure l'existence de décompositions en somme de quatre carrés mais ne fournit pas le nombre de telles décomposition. Celui-ci est donné par la formule de Jacobi :

Théorème 12. *(Jacobi 1829) Soit n un entier naturel. Le nombre de quadruplets d'entiers relatifs dont la somme des carrés vaut n est égal à*

$$8 \sum_{d|n, 4\nmid d} d$$

Comme proposé dans [4], nous allons déduire le théorème de Jacobi d'une formule due à Siegel, qui pour être énoncée, nécessite d'introduire la notion de densité. Dans la suite, p est un nombre premier (ou ∞).

Définition 13. Soit $f : X \to Y$ une application continue entre espaces topologiques Borel-mesurés et y_0 dans Y. La **densité de f^{-1} en** y_0 est, si elle existe, la limite

$$Df^{-1}(y_0) := \lim_{U \to y_0} Vol(f^{-1}(U))/Vol(U)$$

Exemple 14. Si $f : \mathbb{R}^n \to \mathbb{R}$ est la forme quadratique canonique (qui envoie $(x_1, \cdots, x_n)$ sur $x_1^2 + \cdots + x_n^2$) et source et but sont munis de la mesure de Lebesgue, alors

$$\forall y > 0, \quad Vol(f^{-1}([0, y])) = Vol(\mathbb{B}^n(0, \sqrt{y})) = \omega_n y^{n/2}$$

en notant ω_n le volume de la boule unité dans $\mathbb{R}^n$. Ainsi, pour $y > 0$,

$$Df^{-1}(y) = \lim_{h \to 0^+} \omega_n \frac{(y+h)^{n/2} - (y-h)^{n/2}}{2h} = \frac{d}{dy} \omega_n y^{n/2} = \frac{n}{2} \omega_n y^{n/2-1}.$$

Pour $n = 4$, il vient (vu que $\omega_4 = \pi^2/2$),

$$\boxed{Df^{-1}(y) = \pi^2 y.}$$

Le groupe $\mathbb{Z}_p$ est muni de l'unique mesure de Haar telle que le volume de $p^k \mathbb{Z}_p$ soit égal à p^{-k}. Elle induit une mesure produit sur $\mathbb{Z}_p^n$.

Proposition 15. *Si f_p est la forme quadratique canonique sur $\mathbb{Z}_p^n$ et $n = 2m$ est pair, alors, pour tout entier a,*

$$Df_p^{-1}(a) = \begin{cases} (1 - s^m)(1 + ps^m + p^2 s^{2m} + \cdots + p^\nu s^{\nu m}) & \text{si } p \text{ est impair} \\ 1 + (-1)^{m/2}(r + r^2 + \cdots + r^{\nu-1} - r^\nu) & \text{si } p = 2 \text{ et } m \text{ est pair} \\ 1 \pm r^{\nu+1} & \text{si } p = 2 \text{ et } m \text{ est impair} \end{cases}$$

où ν est la valuation p-adique de a, $s := p^{-1}\left(\frac{-1}{p}\right)$ et $r := p^{1-m}$.

La démonstration de cette proposition sera (peut-être) donnée à la fin de cette section, nous allons d'abord l'utiliser pour établir la formule de Jacobi comme cas particulier de celle de Siegel.

Soit X un $\mathbb{Z}$-espace muni d'une forme bilinéaire définie positive et $f_p : X \otimes \mathbb{Z}_p \to \mathbb{Z}_p$ la forme quadratique associée (avec la convention $\mathbb{Z}_\infty = \mathbb{R}$.

Théorème 16. *(Siegel 1935 ?, admis) Si X est seul dans son genre et de rang supérieur ou égal à 3, alors*

$$r_X(a) := \text{card}\{x \in X \,/\, f(x) = x \cdot x = a\} = \prod_p Df_p^{-1}(a)$$

pour tout entier a.

Démonstration du théorème de Jacobi. Nous allons appliquer le théorème de Siegel à $\mathbb{Z}^4$ muni de la forme quadratique canonique f en admettant qu'elle est seule dans son genre. Pour $p=\infty$, il a été montré dans l'exemple précédent que la densité associée vérifie

$$Df_p^{-1}(a)=\pi^2 a$$

La proposition 15 (avec ici $m=2$, $s^2=s^m=p^{-2}$ et $ps^m=p^{-1}$) donne, lorsque p est premier impair,

$$Df_p^{-1}(a)=(1-p^{-2})(1+p^{-1}+p^{-2}+\cdots p^{-\nu_p})$$

où ν_p est la valuation p-adique de a. Pour $p=2$, la même proposition fournit (vu que $r=p^{-1}=2^{-1}=1-r$ et $(-1)^{m/2}=-1$)

$$Df_2^{-1}(a)=1-(r+r^2+\cdots+r^{\nu_2-1}-r^{\nu_2})=1+r^{\nu_2}-r\frac{1-r^{\nu_2-1}}{1-r}=r^{\nu_2}+r^{\nu_2-1}=2^{-\nu_2}+2^{-\nu_2+1}.$$

Ainsi, le produit de toutes les densités est le produit d'un facteur qui ne dépend pas de a

$$\pi^2\prod_{p\neq 2}(1-p^{-2})=\frac{4}{3}\pi^2\zeta(2)^{-1}=8$$

par un facteur qui dépend de a, à savoir

$$a(2^{-\nu_2}+2^{-\nu_2+1})\prod_p(1+p^{-1}+p^{-2}+\cdots p^{-\nu_p})=a\sum_{d|a,2^{\nu_2-1}|d}\frac{1}{d}=\sum_{d|a,4\nmid d}d$$

ce qui achève de démontrer la formule de Jacobi.

□

Exemple 17. Le nombre 4 admet 16 décompositions de type $(\pm1)^2+(\pm1)^2+(\pm1)^2+(\pm1)^2$ et 8 de type $0^2+\cdots+(\pm2)^2+\cdots+0^2$ donc $r_4(4)=16+8=24$. Les diviseurs de 4 non divisibles par 4 sont 1 et 2 donc le membre de droite de la formule de Jacobi est bien égal à $8\times(1+2)=24$.

Démonstration de la proposition 15. Il suffit de déterminer le nombre $N_n(a \bmod p^k)$ de solutions de $f(x)=a$ modulo p^k pour k assez grand. Milnor commence par traiter le cas $k=1$ pour établir un premier lemme

Lemme 18. *Soit $n=2m$ un entier pair. Alors,*

$$N_{2m}(u \ mod\ p)=p^{2m-1}(1-s^m)$$

si u est inversible modulo p et

$$N_{2m}(0 \ mod\ p)=p^{2m}s^m+N(u \ mod\ p).$$

en raisonnant par récurrence sur m. Il en déduit (par disjonction de cas) le lemme suivant

Lemme 19. *Si $a=p^\nu u$ avec u premier avec p et $k\geq\nu$, alors*

$$N(a \ mod\ p^k)=p^{(2m-1)k}(1-s^m)(1+ps^m+p^2s^{2m}+\cdots+p^\nu s^{\nu m}).$$

dont découle la proposition vu que les $x+p^k\mathbb{Z}_p^n$ partitionnent $f_p^{-1}(a+p^k\mathbb{Z}_p)$ lorsque x varie dans l'ensemble des solutions de $f(x)=a$ modulo p^k :

$$Df_p^{-1}(a)=\lim_k \mathrm{Vol}(f_p^{-1}(a+p^k\mathbb{Z}_p))/\mathrm{Vol}(p^k\mathbb{Z}_p)=\lim_k N(a \bmod p^k)p^{-kn}/p^{-k}=(1-s^m)(1+ps^m+p^2s^{2m}+\cdots+p^\nu s^{\nu m})$$

□

Il reste ainsi à établir les deux lemmes techniques.

Démonstration du lemme 18. Pour $n = 1$, il s'agit de dénombrer les solutions de $x^2 = a \bmod p$, il y en a $\left(\frac{a}{p}\right) + 1$. Le cas $n = 2$ découle du cas $n = 1$ car

$$\begin{aligned} N_2(a \bmod p) &= \sum_{x+y=a \bmod p} N_1(x)N_1(y) \\ &= \sum_{x+y=a \bmod p} 1 + \left(\frac{x}{p}\right) + \left(\frac{y}{p}\right) + \left(\frac{xy}{p}\right) \\ &= p + 0 + 0 + \sum_x \left(\frac{x(a-x)}{p}\right) \\ &= p + \left(\frac{-x^2}{p}\right) \sum_{x\neq 0} \left(\frac{1-a/x}{p}\right) \\ &= p + \left(\frac{-x^2}{p}\right) \sum_{x\neq 0} \left(\frac{1-a/x}{p}\right) \\ &= \begin{cases} p(1-s) & \text{si } a \neq 0 \\ p^2 s + p(1-s) & \text{si } a = 0. \end{cases} \end{aligned}$$

L'hérédité s'établit de façon similaire :

$$N_{2m+2}(u \bmod p) = \sum_{x+y=a} N_{2m}(x \bmod p)N_2(y \bmod p) = \cdots$$

□

Remarque 20. Avant d'aborder la démonstration du lemme 19, il peut être judicieux de se convaincre qu'étant donnée un solution ξ dans $\mathbb{F}_p$ de la congruence

$$\xi^2 = a \bmod p,$$

il existe une unique solution x dans $\mathbb{Z}_p$ de l'équation

$$x^2 = a$$

telle que $x \equiv \xi \bmod p$.

Démonstration du lemme 19. Soit $n := 2m$ un entier pair et p un nombre premier impair. Il s'agit de déterminer le nombre $N_{2m}(a \bmod p^k)$ de solutions dans $(\mathbb{Z}/p\mathbb{Z})^n$ de

$$x_1^2 + \cdots + x_n^2 \equiv a \mod p^k \qquad (*)$$

Écrivons a sous la forme $a = p^\nu u$ avec u inversible.

— Si ν est nulle, toute solution de

$$\xi_1^2 + \cdots + \xi_n^2 = u \mod p$$

est différente du n-uplet nul et donne lieu à exactement $p^{(n-1)(k-1)}$ solutions de $(*)$, qui en a donc $N_{2m}(u)p^{(n-1)(k-1)} = p^{(2m-1)k}(1 - s^m)$.

— Si $\nu = 1$, toute solution de $(*)$ est l'un des $p^{(n-1)(k-1)}$ relèvements d'une des $N_{2m}(0) - 1$ solutions *non nulles* de

$$\xi_1^2 + \cdots + \xi_n^2 = 0 \mod p$$

et il y en a donc

$$\begin{aligned} (N_{2m}(0) - 1)p^{(n-1)(k-1)} &= N_{2m}(u)p^{(n-1)(k-1)} + (p^n s^m - 1)p^{(n-1)(k-1)} \\ &= p^{(2m-1)k}(1 - s^m) + p^{(2m-1)k}(ps^m - p^{1-n}) = \quad p^{(2m-1)k}(1 - s^m)(1 + ps^m) \end{aligned}$$

vu que $ps^{2m} = p^{1-n}$.

— si $\nu \geq 2$ il y a deux types de solutions : $p^{(2m-1)k}(1-s^m)(1+ps^m)$ qui proviennent de relèvements de solutions non-nulle modulo p et celles qui sont nulles modulo p et s'écrivent donc sous la forme

$$(x_1, \cdots, x_n) = (py_1, \cdots, py_n).$$

Les y_i sont uniquement déterminés modulo p^{k-1} et il faut et il suffit que $(y_1, \cdots, y_n)$ soit l'un des p^n relèvements modulo p^{k-1} d'une des solutions de

$$z_1^2 + \cdots + z_n^2 = up^{\nu-2} \mod p^{k-2}$$

qui sont au nombre de $N_{2m}(up^{\nu-2} \bmod p^{k-2})$. L'hérédité en découle comme suit

$$\begin{aligned} N_{2m}(up^\nu \bmod p^k) =& p^{(2m-1)k}(1-s^m)(1+ps^m) + p^n N_{2m}(up^{\nu-2} \bmod p^{k-2}) \\ =& p^{(2m-1)k}(1-s^m)(1+ps^m) + p^n p^{(2m-1)(k-2)}(1-s^m)(1+ps^m + \cdots p^{\nu-2}s^{m(\nu-2)}) \\ =& p^{(2m-1)k}(1-s^m)(1+ps^m + p^{2-n}(1+ps^m + \cdots p^{\nu-2}s^{m(\nu-2)})) \end{aligned}$$

qui se récrit comme voulu car pour tout i, $(ps^m)^{i+2} = p^2 s^{2m}(ps^m)^i = p^{2-n}p^i s^{mi}$.

□

Remarque 21. La formule de Jacobi peut également être démontrée en introduisant la fonction θ du même nom et exprimant θ^4 en fonction de la série d'Eisenstein de poids 2, en s'appuyant sur la formule "k/12" (voir Colmez VII.6) satisfaite par les formes modulaires.

4 Autres formules de Siegel

4.1 Formules de masse

Lorsque X n'est pas seul dans son genre, celui-ci ne contient néanmoins qu'un nombre fini de classes d'isomorphisme distinctes (car des formes de même genre ont même déterminant). Si X_1, ..., X_g des représentants de ces classes et posons

$$w_i := \frac{|O(X_i)|^{-1}}{\sum_{j=1}^g |O(X_j)|^{-1}}$$

pour tout i dans $\{1, \cdots, g\}$.

Théorème 22. *(Siegel 1851, voir [4]) Pour tout entier naturel non nul a,*

$$\sum_{i=1} w_i r_{X_i}(a) = \prod_p Df_p^{-1}(a)$$

Cet énoncé admet une généralisation matricielle qui permet en particulier de calculer la masse $M = \sum_{j=1}^g |O(X_j)|^{-1}$.
Une formule analogue, appelée formule de Minkowski-Siegel, se trouve dans le cours d'arithmétique de Serre [1] :

Théorème 23. *Soit $n = 8k$ un entier divisible par 8 et C_n l'ensemble des classes d'isomorphisme d'espaces quadratiques sur $\mathbb{Z}$ définis positifs, pairs et de rang n. Alors,*

$$\sum_{E \in C_n} |O(E)|^{-1} = \frac{B_{2k}}{8k} \prod_{j=1}^{4k-1} \frac{B_j}{4j}$$

où B_i est le i-ème nombre de Bernoulli ($B_1 = 1/6$, $B_2 = 1/30$, $B_3 = 1/42$, $B_4 = 1/30$...).

Corollaire 24. *C_8 est réduit à Γ_8 et $C_{16} = \{\Gamma_{16}, \Gamma_8 \oplus \Gamma_8\}$*

Démonstration. L'ordre du groupe d'automorphismes de Γ_8 est égal à $2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$ (c.f. Bourbaki *Groupes et alg. de Lie*, chap. VI, par. 4) et coïncide avec l'inverse du membre de droite dans la formule de Siegel, donc la somme apparaissant dans le membre de gauche n'a qu'un terme.. □

Il existe également une formule générale qui dénombre (avec poids) le nombre de représentations d'une forme par un genre : elle se spécialise pour donner les différentes formules présentées jusqu'ici. Voir les cours de Serre au collège de France (en particulier le résumé [2]).

4.2 Formes modulaires, fonctions theta

Dans cette section, H désigne le demi-plan de Poincaré constitué des nombres complexes de partie imaginaire strictement posiitive et G le groupe $\mathrm{PSL}_2(\mathbb{Z})$, qui agit sur H via

$$g.z := \frac{az+b}{cz+d}$$

pour tout z dans H et $g := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans G.

Théorème 25. *Un domaine fondamental de l'action de G sur H est $D := \{z \in H \,/\, |z| \geq 1$ et $|\mathrm{Re}(z)| \leq 1/2\}$. Le groupe G est engendré par les éléments S et T définis par*

$$T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Démonstration. Faire un dessin. Voir [1]. □

Le théorème 23 précédent admet un analogue en termes de fonctions theta et de séries d'Eisenstein. Pour l'énoncer, il faut introduire la notion de forme modulaire.

Définition 26. Une **forme (resp fonction) modulaire** de poids $2k$ est une fonction holomorphe (resp. méromorphe) f sur le demi plan de Poincaré H et en ∞ telle que

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{2k} f(z) \qquad \forall z \in H\,, \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G.$$

Une telle forme modulaire est dite **parabolique** lorsque $f(\infty) = 0$.

Remarque 27. L'équation fonctionnelle est équivalente à $f(z+1) = 1$ et $f(-1/z) = z^{2k} f(z)$ en vertu du théorème 25.

Définition 28. Soit k un entier naturel strictement supérieur à 1. La **série d'Eisenstein d'indice** k, notée G_k, est définie par

$$G_k(z) := \sum_{(m,n) \neq (0,0)} \frac{1}{(mz+n)^{2k}}.$$

Les séries d'Eisenstein sont une source de formes modulaires :

Proposition 29. *Pour tout entier naturel $k > 1$, G_k est une forme modulaire de poids $2k$ et $G_k(\infty) = 2\zeta(2k)$.*

Démonstration. Pour la convergence, se ramener à D et remarquer que $|mz+n|^2 \geq |mj-n|^2$ pour déduire la convergence normale de G_k sur D de la convergence de $\sum 1/|\gamma|^s$ pour $s > 2$. □

Les formes modulaires sont assez contraintes :

Théorème 30 (théorème k/6 ou k/12)**.** *Soit f une fonction modulaire non nulle de poids $2k$. Alors,*

$$\nu_\infty(f) + \frac{1}{2}\nu_i(f) + \frac{1}{3}\nu_j(f) + \sum_{x \in H/G \setminus \{i,j\}} \nu_x(f) = \frac{k}{6}$$

où $\nu_x(f)$ désigne l'orde de f en x.

Démonstration. Intégrer $\frac{1}{2i\pi}\frac{df}{f}$ sur le bord du domaine fondamental D et appliquer le théorème des résidus. □

Corollaire 31. *Pour $k < 0$ et $k = 1$, l'espace vectoriel des formes modulaires de poids k est réduit à la forme nulle.*
Pour k dans $\{0, 2, 3, 4, 5\}$, l'espace vectoriel des formes modulaires de poids $2k$ est unidimensionnel (donc engendré par G_k) et toute forme parabolique est nulle.

Remarque 32. En fait, toute forme modulaire est un polynôme en G_2 et G_3.

Le développement des séries d'Eisenstein au voisinage de l'infini est donné par la proposition suivante

Proposition 33. *Soit k un entier non nul. Alors,*

$$G_k = 2\zeta(2k)E_k$$

où

$$E_k(q) := 1 + \frac{(-1)^k 4k}{Bk} \sum_{m \geq 1} \sigma_{2k-1}(m) q^m$$

avec $\sigma_t(m) := \sum_{d|m} d^t$ pour tout m..

Démonstration. Exprimer $\pi \text{cotan} \pi z$ de deux façons différentes puis différentier plusieurs fois la relation obtenue. □

Définition 34. Soit Γ un espace quadratique sur $\mathbb{Z}$. La **fonction theta** associée à Γ, notée θ_Γ, est définie par

$$\theta_\Gamma(z) := \sum_{x \in \Gamma} q^{(x \cdot x)/2} = \sum_x \mathrm{e}^{\pi i z (x \cdot x)} = \sum_{m=0}^{+\infty} r_\Gamma(m) q^m$$

pour tout z dans le demi plan de Poincaré, où $q := e^{2i\pi z}$ et $r_\Gamma(m)$ est le nombre de représentations de $2m$ par Γ.

Théorème 35. *Si Γ est égal à son dual et pair, alors sa dimension est divisible par 8 et la fonction θ_Γ est modulaire de poids $n/2$. En conséquence, il existe f_Γ parabolique telle que*

$$\theta_\Gamma = E_k + f_\Gamma$$

avec $k = n/4$.

Démonstration. Admettons que n est divisible par 8 et montrons que θ_Γ est modulaire de poids $n/2$ i.e.

$$\theta_\Gamma(-1/z) = z^{n/2} \theta_\Gamma(z)$$

pour tout z dans le demi-plan de Poincaré H. Comme les deux membres sont holomorphes, il suffit d'établir cette égalité pour tout z de la forme it avec $t > 0$. Dans ce cas,

$$\begin{aligned}
\theta_\Gamma(z) =& \theta_\Gamma(it) \\
=& \sum_{x\in\Gamma} \mathrm{e}^{-\pi t(x\cdot x)} \\
=& \sum_{x\in\sqrt{t}\Gamma} \mathrm{e}^{-\pi(x\cdot x)} \\
=& \frac{1}{\mathrm{Vol}(\mathbb{R}^n/\sqrt{t}\,\Gamma)} \sum_{y\in(\sqrt{t}\Gamma)'} \mathrm{e}^{-\pi(y\cdot y)} \qquad \text{(Formule de Poisson)} \\
=& t^{-n/2} \sum_{y\in(1/\sqrt{t})\Gamma} \mathrm{e}^{-\pi(y\cdot y)} \\
=& t^{-n/2} \sum_{y\in\Gamma} \mathrm{e}^{-\pi(y\cdot y)/t} \\
=& t^{-n/2}\theta_\Gamma(i/t) \\
=& z^{-n/2}\theta_\Gamma(-1/z).
\end{aligned}$$

Le fait que $f_\Gamma := \theta_\Gamma - E_k$ soit parabolique résulte du fait que $\theta_\Gamma(\infty) = 1 = E_k(\infty)$. □

Corollaire 36. *Soit m un entier. Si $\Gamma = \Gamma_8$, alors*

$$r_\Gamma(m) = 240\sigma_3(m)$$

et si $\Gamma = \Gamma_{16}$ ou $\Gamma = \Gamma_8 \oplus \Gamma_8$, alors

$$r_\Gamma(m) = 480\sigma_7(m).$$

Démonstration. D'après le corollaire du théorème 30, la seule forme parabolique de poids 4 est la forme nulle donc

$$\theta_{\Gamma_8} = E_2$$

d'où

$$\sum_{m=0}^{+\infty} r_{\Gamma_8}(m)q^m = 1 + \frac{8}{B_2}\sum_{m=1}^{+\infty}\sigma_3(m)q^m = 1 + 240\sum_{m=1}^{+\infty}\sigma_3(m)q^m.$$

et la première égalité voulue s'obtient en identifiant les coefficients de q^m dans chaque développement. L'argument reste valable lorsque $n = 16$ et fournit la deuxième égalité. L'argument □

Exemple 37. $r_{\Gamma_8}(1) = 240\sigma_3(1) = 240$ ce qui signifie que Γ_8 contient exactement 240 vecteurs de norme minimale égale à $\sqrt{2}$.

Remarque 38. Le terme d'erreur f_Γ n'est en général pas nul mais Siegel a montré que la somme pondérée des f_Γ l'est i.e.

$$\sum_{\Gamma\in C_n} w_\gamma\theta_\Gamma = E_k$$

avec $k = n/4$ et en utilisant les notations de la formule de masse de Minkowski-Siegel présentée dans la section précédente.

La fonction theta associée à la somme des carrées n'est que quasi-modulaire (modulaire par rapport à un sous groupes de $SL_2(\mathbb{Z})$: la méthode s'appliquerait pour obtenir la formule de Jacobi mais il faudrait surmonter un certain nombre de difficultés techniques qui ont eu raison de la volonté de l'orateur.

5 Weil-Siegel

Weil a généralisé à d'autres groupes les formules de Siegel. Le membre de droite s'exprime comme un volume adélique (lien avec la théorie du corps de classe qui correspond au cas du groupe GL_1) et l'égalité équivaut au fait que le nombre de Tamagawa du groupe considéré vaut 1 (ou 2 ?). Voir les cours de Serre au Collège de France (1981-1982), notamment le résumé [2] et les notes d'Osterlé [3].

Voir l'exposé de Lurie, qui propose une approche pour obtenir une formule de masse pour les classes d'isomorphismes de fibrés sur une courbe définie sur une corps de fonctions $\mathbb{F}_p(T)$. Cette stratégie lui a permis de démontrer, avec Gaitsgory, la conjecture de Weil (Tamagawa=2) dans le cas des corps de fonctions, voir [6].

Références

[1] Jean-Pierre Serre *Cours d'arithmétique*, 1970

[2] Jean-Pierre Serre `https://www.college-de-france.fr/sites/default/files/media/document/2023-03/1982-1983_serre.pdf` 1982

[3] Jean-Pierre Serre `https://www.numdam.org/item/CJPS_1982__4_.pdf` 1982

[4] John Willard Milnor et Dale Husemoller *Symmetric bilinear forms*, Springer, 1973

[5] Colmez Pierre *Eléments d'analyse et d'algèbre (et de théorie des nombres)*, Editions Ecole Polytechnique, 2009

[6] Jacob Lurie, Dennis Gaitsgory `https://people.math.harvard.edu/~lurie/papers/tamagawa-abridged.pdf`