File:RingGaussSum.tex compil. le 25 février 2017,21:10

Sommes de Gauss sur un anneau fini

Références : notes de P.N. (5 Mai 1993). Koblitz, Introduction to Elliptic Curves and Modular Forms, exercice 9 de la section 2 du chapitre II, page 62 (l'exercice est partiellement corrigé).
Ribenboim, Classical Theory of Algebraic Numbers, en particulier (mais beurk) section 26.1, The Quadratic Character Attached to the Quadratic Field.
Frölich & Taylor, Algebraic Number Theory. En particulier, chap. VI (Cyclotomic Fields), §3 (Quadratic fields revisited).
Loïc Mérel, Nombres Algébriques et Nombres p-adiques (cours préparatoires aux études doctorale 2003-04), `TAN.pdf`
W. Stein, Modular Forms, a Computational Approach, chap. 4, Dirichlet Characters

Objectif

Vous avez dit objectif ? Euh. On veut par exemple étudier des sommes de Gauss quadratiques en liaison avec le caractère de Kronecker χ_D et l'inclusion $\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\sqrt[|D|]{1})$ où D est un discriminant quadratique fondamental.
On veut également s'amuser avec des extensions abéliennes $K/\mathbb{Q}$. Une telle extension abélienne est contenue dans une unique extension cyclotomique minimale :

$$K \subset \mathbb{Q}(\sqrt[m]{1})$$

L'entier m est bien défini si l'on impose $m \not\equiv 2 \bmod 4$ car pour $m = 2m'$ avec m' impair, on a l'égalité $\mathbb{Q}(\sqrt[m]{1}) = \mathbb{Q}(\sqrt[m']{1})$. Cet entier m est le *conducteur cycotomique* de $K/\mathbb{Q}$.
Au niveau des groupes de Galois, on dispose de la surjection canonique qui consiste à restreindre à K un automorphisme de Galois de $\mathbb{Q}(\sqrt[m]{1})$:

$$(\mathbb{Z}/m\mathbb{Z})^\times \overset{\text{can.}}{\simeq} \mathrm{Gal}\left(\mathbb{Q}(\sqrt[m]{1})/\mathbb{Q}\right) \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q})$$

qui fournit une injection (canonique) quand on passe au groupe des caractères

$$\widehat{\mathrm{Gal}(K/\mathbb{Q})} \hookrightarrow \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$$

d'où l'envie d'étudier le groupe de droite : groupe des caractères de Dirichlet modulo m.

Le groupe des inversibles de R/I, R anneau fini

• On note $(\mathbb{U}, \times)$ le groupe multiplicatif des nombres complexes de module 1.

Ici R est un anneau commutatif fini ; il faut par exemple penser à $R = \mathbb{Z}/N\mathbb{Z}$ et/ou à un corps fini.
J'attaque bille en tête, de manière pas très pédagogique, par un lemme. Lemme que je trouve rassurant en ce qui concerne les histoires de caractères (multiplicatifs) primitifs.

Lemme 1.
Pour tout idéal I de R, le morphisme entre groupes multiplicatifs :

$$R^\times \to (R/I)^\times$$

est surjectif de noyau $R^\times \cap (1+I)$. En conséquence, on dispose d'un isomorphisme canonique :

$$(R/I)^\times \overset{\text{can.}}{\simeq} \frac{R^\times}{R^\times \cap (1+I)}$$

Preuve.
► Montrons le d'abord pour $R = \mathbb{Z}/N\mathbb{Z}$. Soit N' un diviseur de N, ce qui permet de considérer $(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/N'\mathbb{Z})^\times$. Considérons $k' \in \mathbb{Z}$ inversible modulo N' que l'on doit relever en un inversible modulo N. On pose (Landau's trick)

$$k = k' + aN' \quad \text{avec} \quad a = \prod_{\substack{p|N \\ p \not| k'}} p$$

Alors $k \equiv k' \bmod N'$. Montrons que k est inversible modulo N en montrant qu'un diviseur premier p de N ne divise pas k via :

$$\begin{array}{l} p \not\mid k' \Longrightarrow p \mid aN' \\ p \mid k' \Longrightarrow p \not\mid aN' \end{array} \qquad \text{donc, dans tous les cas, } p \not\mid k = k' + aN'$$

En effet, dans le cas $p \not\mid k'$, on a $p \mid a$, a fortiori $p \mid aN'$. Dans le second cas $p \mid k'$, on a (par définition de a) $p \not\mid a$ et comme $p \not\mid N'$ (k', N' sont premiers entre eux), on obtient $p \not\mid aN'$.

Plus simple (vu dans Fröhlich & Taylor). Notons

$$N_2 = \prod_{p \mid N'} p^{v_p(N)}, \qquad N_1 = N/N_2$$

de sorte que $N = N_1 N_2$ avec d'une part $N' \mid N_2$ (ne pas oublier que N' divise N) et N', N_2 ont les mêmes facteurs premiers et d'autre part $N_1 \wedge N_2 = 1$.
Soit $k' \in \mathbb{Z}$ inversible modulo N'. D'après le théorème Chinois, il existe $k \in \mathbb{Z}$ vérifiant :

$$k \equiv \begin{cases} 1 \bmod N_1 \\ k' \bmod N_2 \end{cases}$$

Remarquons que k' est aussi inversible modulo N_2 (car N_2, N' ont les mêmes facteurs premiers). Bilan : k est inversible modulo N_1 et modulo N_2 donc modulo leur produit qui est N ; et bien sûr $k \equiv k' \bmod N'$ car $N' \mid N_2$.

Autre variante : on pourrait le montrer pour D puissance d'un premier (cela devrait être facile car $\mathbb{Z}/D\mathbb{Z}$ est un anneau local) puis montrer que si c'est vérifié pour D_1, D_2 premiers entre eux, alors c'est vrai pour le produit $D_1 D_2$.

▶ Montrons le pour un anneau semi-local i.e. ayant un nombre fini d'idéaux maximaux (cela s'applique donc à un anneau fini). Soient $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ les idéaux maximaux tels que $I \not\subset \mathfrak{m}_j$ ($k = 0$ si $I = R$!). Je dis qu'il n'existe pas d'idéal maximal $\mathfrak{m}$ tel que $I + \mathfrak{m}_1 \cdots \mathfrak{m}_k \subset \mathfrak{m}$ car cela entraînerait $I \subset \mathfrak{m}$ et l'existence d'un j tel que $\mathfrak{m}_j \subset \mathfrak{m}$ puis $\mathfrak{m}_j = \mathfrak{m}$, conduisant à $I \subset \mathfrak{m}_j$, un tantinet contradictoire. Bref $I + \mathfrak{m}_1 \cdots \mathfrak{m}_k = R$. Soit maintenant $x \in R$ inversible modulo I ; alors, par le théorème chinois, il existe y tel que :

$$y \equiv \begin{cases} x \bmod I \\ 1 \bmod \mathfrak{m}_1 \cdots \mathfrak{m}_k \end{cases}$$

Alors $y \equiv x \bmod I$ (ça, c'est sûr) et y est inversible. En effet, imaginons l'existence d'un idéal maximal $\mathfrak{m}$ avec $y \in \mathfrak{m}$. Si $I \subset \mathfrak{m}$, alors $x \in \mathfrak{m}$, et donc dans le quotient R/I, on a $x \in \mathfrak{m}/I$, non tenable car x est inversible dans R/I. Si $I \not\subset \mathfrak{m}$, alors $\mathfrak{m}$ est l'un des $\mathfrak{m}_j$ et donc $y - 1 \in \mathfrak{m}_1 \cdots \mathfrak{m}_k \subset \mathfrak{m}_j$ conduisant à $1 \in \mathfrak{m}_j$.
Quelle horreur.

▶ Vrai aussi pour un anneau résiduellement zéro-dimensionnel i.e. le quotient par son idéal de Jacobson est un anneau zéro-dimensionnel (réduit). Et même pour un anneau local-global.
J'aborde la chose pour un anneau zéro-dimensionnel dans le lemme suivant. □

Lemme 2 (Rigidité de $R^\times \to (R/I)^\times$ pour un anneau zéro-dimensionnel R)**.**
Soit R un anneau zéro-dimensionnel i.e. tout idéal premier est maximal ou encore pour tout $x \in R$, il existe n tel que $x^n \in Rx^{n+1}$. Ceci définit permet d'associer à chaque x un idempotent : c'est l'unique idempotent qui engendre l'idéal $\langle x^n \rangle$ pour n grand. Cf les rappels dans la preuve.
Alors
(i) L'élément $x' = ex + 1 - e$ est inversible dans R.
(ii) Pour tout idéal I tel que x est inversible modulo I, on a $x' \equiv x \bmod I$ et donc x' est un antécédent de $\overline{x}$ dans $R^\times \to (R/I)^\times$.

Preuve.
▶ Rappel : on dispose d'un $n \in \mathbb{N}$ et d'un $a \in R$ tel que $x^n = ax^{n+1}$. On réécrit dans le membre droit $x^{n+1} = x \times x^n = axx^{n+1} = ax^{n+1}$ ce qui donne en tout :

$$x^n = a^2 x^{n+2}$$

Et on recommence :

$$x^n = ax^{n+1} = a^2x^{n+2} = a^3x^{n+3} = \cdots = a^n x^{2n}$$

Bilan : en posant $e = a^n x^n$, on obtient :

$$e^2 = a^{2n}x^{2n} = a^n x^n = e$$

Youpi, un idempotent. On a $e \in \langle x^n \rangle$ et d'autre part, on vérifie que :

$$x^n = ex^n$$

Bilan : $\boxed{\langle x^n \rangle = \langle e \rangle}$
Quant à $x' := ex + 1 - e$, montrons qu'il est bien inversible ; en effet, x' est inversible dans le localisé $R_e = R/\langle 1 - e \rangle$ puisque dans ce localisé e vaut 1 donc x' vaut x et $1 = e = a^n x^n$; et dans le localisé $R_{1-e} = R/\langle e \rangle$, dans lequel e vaut 0, on a x' qui vaut 1. En cas de doute (?) :

$$(ex + 1 - e) \times (ea^n x^{n-1} + 1 - e) = e^2 a^n x^n + 1 - e = e^3 + 1 - e = e + 1 - e = 1$$

Mais il n'y a pas de miracle : x' a été trouvé en écrivant $R = R_e \times R_{1-e}$.
▶ Supposons x inversible modulo I. Comme $x^n(1 - ax) = 0$ et que x est inversible modulo I, on a $ax \equiv 1 \bmod I$ donc $e \equiv 1 \bmod I$. On a donc $x' \equiv x \bmod I$ comme annoncé. □

Caractères additifs

• Un caractère additif ψ sur R est un morphisme de $(R, +)$ dans $(\mathbb{U}, \times)$:

$$\psi(x + y) = \psi(x)\psi(y)$$

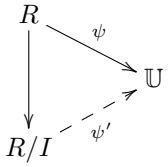
En fait, comme l'anneau est fini, les caractères sont à valeurs dans le sous-groupe $\mathbb{U}_\infty$ constitué des racines n-ièmes de l'unité pour n variable.
Exemple : si $R = \mathbb{Z}/N\mathbb{Z}$, on obtient un caractère additif en prenant une racine primitive N-ème de l'unité et en définissant ψ via :

$$(\star) \qquad \psi : m \bmod N \longmapsto \zeta_N^m$$

Si ψ est un caractère additif, on note, pour $a \in R$, ψ_a le caractère additif obtenu par

$$\psi_a(x) = \psi(ax)$$

• Un caractère additif $\psi : R \to \mathbb{U}$ est dit *primitif* s'il ne transite pas par un caractère additif de R/I pour un idéal I non nul :



Ceci revient à dire que $\psi(I) = 1$ entraîne $I = \{0\}$. En effet, la condition $\psi(I) = 1$ permet de faire passer ψ au quotient modulo I et de définir ψ'.
Le fait que ψ soit primitif est aussi équivalent au fait de dire que $\psi(aR) = 1$ entraîne $a = 0$. Ce qui est équivalent à dire que si ψ_a est le caractère trivial, alors $a = 0$.
Exemple : le caractère $(\star)$ est primitif. Supposons en effet, pour un $a \in \mathbb{Z}$ que $\zeta_N^{ax} = 1$ pour tout $x \in \mathbb{Z}$; alors c'est vrai pour $x = 1$ et donc $N \mid a$ car ζ_N est d'ordre N. En conséquence $a = 0$ dans $\mathbb{Z}/N\mathbb{Z}$.

Caractères multiplicatifs, caractères primitifs

• Un caractère multiplicatif χ sur R est un morphisme multiplicatif $\chi : R^\times \to \mathbb{U}$:

$$\chi(xy) = \chi(x)\chi(y)$$

On le prolonge à R tout entier en posant $\chi(x) = 0$ pour $x \in R \setminus R^\times$. Attention cependant au caractère trivial ε (celui qui vaut 1 sur $R^\times$) qui ne suit pas ce régime : son prolongement est 1 partout.

• Exemple de caractère multiplicatif : le power residue symbol (Ireland & Rosen, chap. 14, The Stickelberger Relation and The Eisenstein Reciprocity Law, §2, p. 203). Considérons l'anneau cyclotomique $\mathbb{Z}[\sqrt[n]{1}]$ et un idéal premier $\mathfrak{p}$ avec $n \notin \mathfrak{p}$ i.e. si $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$, tel que $p \not| n$. Alors :

$$\mathbb{Z}[\sqrt[n]{1}]/\mathfrak{p} = \mathbb{F}_p[\sqrt[n]{1}] = \mathbb{F}_p(\overline{\zeta_n}) = \mathbb{F}_q \qquad \text{avec} \qquad \dim_{\mathbb{F}_p} \mathbb{F}_q = \text{ordre de } p \text{ dans } (\mathbb{Z}/n\mathbb{Z})^\times$$

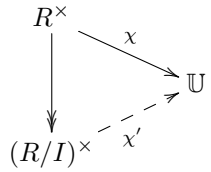
Puisque $\overline{\zeta_n}$ est d'ordre n dans $\mathbb{F}_q^*$, on a $n \mid q-1$ et on dispose d'un isomorphisme canonique :

$$\mathbb{U}_n \xrightarrow{\simeq} U_n\big(\mathbb{Z}[\sqrt[n]{1}]/\mathfrak{p}\big)$$

Ainsi, pour $x \in \mathbb{Z}[\sqrt[n]{1}] \setminus \mathfrak{p}$, on peut considérer $x^{\frac{q-1}{n}}$, qui appartient à $U_n\big(\mathbb{Z}[\sqrt[n]{1}]/\mathfrak{p}\big)$ et que l'on peut remonter en une vraie racine n-ième de $\mathbb{U}_n$. On obtient ainsi un caractère multiplicatif d'ordre n que l'on prolonge à 0 :

$$\mathbb{Z}[\sqrt[n]{1}]/\mathfrak{p} \ni x \longmapsto \left(\frac{x}{\mathfrak{p}}\right)_n \in \mathbb{U}_n \cup \{0\}$$

• Un caractère multiplicatif $\chi : R \to \mathbb{U}$ est dit *primitif* s'il ne transite pas par un caractère multiplicatif de R/I pour un idéal I non nul :



Ceci revient à dire que $\chi\big(R^\times \cap (1+I)\big) = 1$ entraîne $I = \{0\}$. En effet, la condition $\chi\big(R^\times \cap (1+I)\big) = 1$ dit que χ passe au quotient "modulo I" pour former un caractère χ' sur $(R/I)^\times$, ce qui fait que I est bien nul.
En conséquence, dire que χ est primitif signifie que pour tout idéal non nul I, il existe

$$x_0 \in R^\times, \qquad x_0 \equiv 1 \bmod I, \qquad \chi(x_0) \neq 1$$

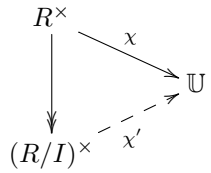
Ou encore, pour tout $a \neq 0$, il existe

$$x_0 \in R^\times, \qquad x_0 \equiv 1 \bmod a, \qquad \chi(x_0) \neq 1$$

Ainsi un caractère multiplicatif $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{U}$ est primitif si pour tout diviseur strict N' de N, il existe $x_0 \in \mathbb{Z}$, inversible modulo N, tel que $x_0 \equiv 1 \bmod N'$ et $\chi(x_0) \neq 1$.

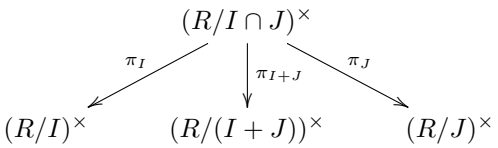
Conducteur d'un caractère multiplicatif : un début

Soit $\chi : R^\times \to \mathbb{U}$ un caractère multiplicatif fixé. On étudie à quelle condition, pour un idéal I, χ "passe au quotient modulo I". Attention à cette terminologie qui signifie l'existence de χ'.



Ceci revient à dire que $\chi\big(R^\times \cap (1+I)\big) = 1$.

Lemme 3.
Pour deux idéaux I, J de R, on considère le diagramme :



Alors :

$$\ker \pi_{I+J} = \ker \pi_I \ker \pi_J$$

Preuve.
Par définition, $\ker \pi_I$ est constitué des $\overline{x} \in (R/I \cap J)^\times$ tels que $x \equiv 1 \bmod I$. Idem pour les autres noyaux. Il est clair que $\ker \pi_I \subset \ker \pi_{I+J}$. D'où l'inclusion $\ker \pi_{I+J} \supseteq \ker \pi_I \ker \pi_J$.
Pour l'inclusion réciproque, soit $x \in R$ tel que x soit inversible modulo $I \cap J$ et $x \in \ker \pi_{I+J}$ i.e. $x \equiv 1 \bmod I + J$. On écrit $x = 1 + i + j$ avec $i \in I$, $j \in J$, puis

$$x = 1 + i + j = (1 + i)(1 + j) - ij \equiv yz \bmod I \cap J \qquad \text{avec} \qquad y = 1 + i, \quad z = 1 + j$$

Puisque $x \equiv yz \bmod I \cap J$ et que x est inversible modulo $I \cap J$, il en est de même de y et z. Merci Flip-Flop. Et l'on a :

$$y \equiv 1 \bmod I, \qquad z \equiv 1 \bmod J$$

Et l'égalité $\overline{x} = \overline{y}\,\overline{z}$ prouve que $x \in \ker \pi_I \ker \pi_J$.

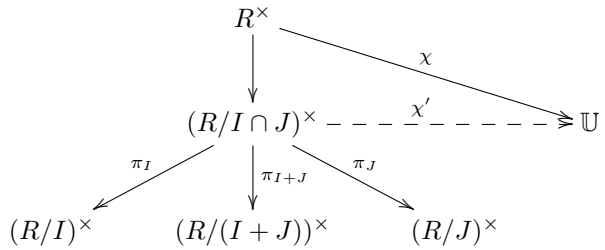
Bizarre : on aurait un résultat plus fort avec IJ au lieu de $I \cap J$. □

Lemme 4 (Passage au quotient d'un caractère multiplicatif)**.**
Soit $\chi : R^\times \to \mathbb{U}$ un caractère multiplicatif. On suppose que pour deux idéaux I, J de R, χ passe au quotient modulo ces idéaux, ce qui signifie :

$$\chi\big(R^\times \cap (1 + I)\big) = 1, \qquad \chi\big(R^\times \cap (1 + J)\big) = 1$$

Alors χ passe au quotient modulo $I + J$.

Preuve.
On considère le diagramme suivant :



Explication : puisque χ passe au quotient modulo I, il passe au quotient modulo $I \cap J$. D'où le caractère multiplicatif χ' sur le dessin.
Mais χ' passe au quotient modulo I et modulo J. Ceci signifie, avec les notations du lemme précédent, que χ' est trivial sur $\ker \pi_I$ et $\ker \pi_J$. Donc, il est trivial sur leur produit qui est $\ker \pi_{I+J}$. Et donc χ' passe au quotient modulo $I + J$. Et il en est de même de χ □

Cela devrait être encore plus direct. Cela me paraît bizarre de passer par cet intermédiaire $I \cap J$.

Definition 1 (conducteur d'un caractère multiplicatif)**.**
Soit $\chi : R^\times \to \mathbb{U}$ un caractère multiplicatif. Le conducteur de χ est le plus grand idéal I tel que l'on ait l'égalité $\chi\big(R^\times \cap (1 + I)\big) = 1$. Ou encore, c'est l'idéal constitué des $a \in R$ tels que :

$$\chi\big(R^\times \cap (1 + aR)\big) = 1 \qquad c.a.d \qquad R^\times \cap (1 + aR) \subset \operatorname{Ker} \chi$$

On aimerait un point de vue qui soit plus direct. C'est l'objet de la section suivante.

L'idéal conducteur : une autre approche

On vise l'énoncé suivant dans lequel il n'y a pas de caractére multiplicatif.

Théorème 1. *Soient I, J deux idéaux d'un anneau zéro-dimensionnel R. Alors :*

$$\big(R^\times \cap (1 + I)\big) \cdot \big(R^\times \cap (1 + J)\big) = R^\times \cap (1 + I + J)$$

Une fois ce résultat établi, il est clair, pour un caractère multiplicatif $\chi : R^\times \to \mathbb{U}$ que

$$[R^\times \cap (1+I) \subset \ker\chi \quad \text{et} \quad R^\times \cap (1+J) \subset \ker\chi] \quad \Rightarrow \quad R^\times \cap \big(1+I+J)\big) \subset \ker\chi$$

Et donc que l'ensemble des $a \in R$ tels que $R^\times \cap (1+aR) \subset \mathrm{Ker}\,\chi$ est un idéal : the so called conductor of χ.

Pour prouver le théorème (1), on va étudier le problème suivant. Partant de l'hypothèse :

$$x = 1+a+b \qquad x \text{ inversible dans } R,\ a,b \in R$$

écrire :

$$x = yz \quad \text{avec} \quad \begin{cases} y \equiv 1 \bmod a \\ z \equiv 1 \bmod b \end{cases}$$

Il est clair que le théorème sera conséquence de ce résultat.
• On donne une première réponse en supposant que $1+a$ vérifie la « bascule zéro-dimensionnelle locale » : $1+a$ est nilpotent ou $1+a$ est inversible. Il suffit de prendre

$$\begin{bmatrix} y \\ z \end{bmatrix} = \begin{bmatrix} x \\ 1 \end{bmatrix} \text{ si } 1+a \text{ est nilpotent,} \qquad \begin{bmatrix} y \\ z \end{bmatrix} = \begin{bmatrix} 1+a \\ (1+a)^{-1}x \end{bmatrix} \text{ si } 1+a \text{ est inversible}$$

Explications. Dans les deux cas, on a bien $x = yz$. Dans le premier cas, $1+a$ étant nilpotent, on obtient d'une part que a est inversible et d'autre part que b l'est aussi puisque $b = x-(1+a)$ et que la somme d'un inversible et d'un nilpotent est inversible. Ce qui fait que les demandes $y \equiv 1 \bmod a$ et $z \equiv 1 \bmod b$ sont automatiquement vérifiées.
Dans le second cas, il est clair que $y = 1+a$ satisfait $y \equiv 1 \bmod a$. Quant à $z = (1+a)^{-1}x$, que se passe-t-il modulo b i.e. modulo $x = 1+a$? Et bien, z vaut 1, ce qui était souhaité.

• L'assemblage. On rappelle que pour tout élément c d'un anneau zéro-dimensionnel, il existe $n \in \mathbb{N}$ tel que $\langle c^n\rangle = \langle e\rangle$ où e est un idempotent. Cette égalité d'idéaux se traduit par :

$$c^n = c^n e, \qquad e = qc^n \text{ pour un certain } q$$

Alors $c' = ec + 1 - e$ est inversible. En effet, dans la branche $e = 0$, on a $c' = 1$, d'inverse 1 ; et dans la branche $e = 1$, on a $c' = c$ qui est bien inversible puisque $\langle c^n\rangle = \langle e\rangle = \langle 1\rangle$; dans cette branche, son inverse est qc^{n-1}. On peut expliciter l'inverse de c' en assemblant :

$$c'^{-1} = (1-e)\times 1 + e \times qc^{n-1}$$

Et en calculant avec la régle :

$$\big((1-e)\alpha + e\beta\big)\big((1-e)\alpha' + e\beta'\big) = (1-e)\alpha\alpha' + e\beta\beta'$$

on vérifie que l'on a bien $c'c'^{-1} = 1$.
Ici, pour produire globalement y, z à partir du terrain local :

$$\begin{bmatrix} y \\ z \end{bmatrix} = \begin{bmatrix} x \\ 1 \end{bmatrix} \text{ si } 1+a \text{ est nilpotent,} \qquad \begin{bmatrix} y \\ z \end{bmatrix} = \begin{bmatrix} 1+a \\ (1+a)^{-1}x \end{bmatrix} \text{ si } 1+a \text{ est inversible}$$

il faut inverser $1+a$. On va considérer son peudo-inverse u :

$$u = (1-e)\times 1 + e \times q(1+a)^{n-1} \qquad \text{où} \qquad \begin{array}{l} (1+a)^n = (1+a)^n e, \qquad e = q(1+a)^n \\ e \text{ idempotent, traduisant } \langle e\rangle = \langle (1+a)^n\rangle \end{array}$$

On propose donc :

$$\begin{aligned} y &= (1-e)x + e(1+a) \\ z &= (1-e)1 + eux = 1 - e + e\big((1-e)\times 1 + e \times q(1+a)^{n-1}\big)x \\ &= 1 - e + eq(1+a)^{n-1}x \end{aligned}$$

Et cela fonctionne globalement car cela fonctionne dans chaque composante. Vérifions le tout de même. D'abord, le produit yz qui doit être égal à x :

$$yz = (1-e)x + eq(1+a)^n x = (1-e)x + e^2 x = (1-e)x + ex = x$$

Vérifions $y = 1 \bmod a$. Travaillons modulo a ; on a $y = (1-e)x + e$; et comme $\langle e\rangle = \langle (1+a)^n\rangle = \langle 1\rangle$, donc $e = 1$ et il reste $y = 1$ (modulo a, bien entendu).
Vérifions $z = 1 \bmod b$. Travaillons modulo b i.e. modulo $x = 1+a$; on a $z = 1 - e + eq(1+a)^n = 1 - e + e^2 = 1$.

Le calcul du produit de sommes de Gauss $G_\psi(\chi)G_\psi(\overline{\chi})$

Théorème 2.
*Soient ψ, χ deux caractères sur R, ψ étant additif, χ étant multiplicatif, les deux **primitifs**. On définit la somme de Gauss :*

$$G_\psi(\chi) = \sum_{x \in R} \psi(x)\chi(x)$$

Alors :

$$\boxed{G_\psi(\chi)G_\psi(\overline{\chi}) = \chi(-1) \times \#R}$$

Quelques lemmes techniques

Lemme 5.
Soit ψ un caractère additif non trivial. Alors :

$$\sum_{x \in R} \psi(x) = 0$$

Preuve.
Soit $x_0 \in R$ tel que $\psi(x_0) \neq 1$. Comme $x \mapsto x_0 + x$ est une bijection de R sur lui-même

$$\sum_{x \in R} \psi(x) = \sum_{x \in R} \psi(x_0 + x) = \psi(x_0) \sum_{x \in R} \psi(x) \qquad \text{i.e.} \qquad \big(1 - \psi(x_0)\big) \sum_{x \in R} \psi(x) = 0$$

D'où la chute puisque $\psi(x_0) \neq 1$. □

Lemme 6.
*Soit χ un caractère multiplicatif **primitif**. Alors pour tout idéal non nul I et pour tout $a \in R$:*

$$\sum_{x \equiv a \bmod I} \chi(x) = 0$$

Preuve.
Soit $x_0 \in R^\times$ tel que $x_0 \equiv 1 \bmod I$ et $\chi(x_0) \neq 1$, dont l'existence est assurée par le fait que χ est primitif et I non nul.
La multiplication par x_0 induit une bijection de $a+I$ sur lui-même, ceci étant dû au fait que $x_0 \equiv 1 \bmod I$.
On peut donc écrire :

$$\sum_{x \equiv a \bmod I} \chi(x) = \sum_{x \equiv a \bmod I} \chi(x_0 x) = \chi(x_0) \sum_{x \equiv a \bmod I} \chi(x)$$

c'est-à-dire :

$$\big(1 - \chi(x_0)\big) \sum_{x \equiv a \bmod I} \chi(x) = 0$$

Et donc la somme est bien nulle puisque $\chi(x_0) \neq 1$. □

Remarque : il est fondamental de supposer I non nul. Car lorsque $I = \{0\}$, la somme se réduit à $\chi(a)$, et il n'est pas raisonnable d'obtenir $\chi(a) = 0$ (pour tout a).

Lemme 7. *Soit χ un caractère multiplicatif **primitif**. Alors pour tout caractère additif ψ et tout élément b **non inversible**, on a :*

$$\sum_{x \in R} \chi(x)\psi(bx) = 0$$

Preuve. Introduisons l'idéal

$$I = \{x \in R \mid bx = 0\}$$

Cet idéal n'est pas réduit à 0 ; en effet, si c'était le cas, b serait régulier, donc, puisque l'anneau est fini, inversible, ce qui n'est pas le cas.
On va pouvoir appliquer le lemme précédent en sommant sur chaque classe modulo I i.e. on va montrer que chaque sous-somme est nulle :

$$S_a := \sum_{x \equiv a \bmod I} \chi(x)\psi(bx)$$

Pour $x \equiv a \bmod I$, on a $x - a \in I$ donc, par définition de I, $b(x-a) = 0$ i.e. $bx = ba$. Si bien la somme S_a vaut :

$$S_a = \sum_{x \equiv a \bmod I} \chi(x)\psi(ba) = \psi(ba) \sum_{x \equiv a \bmod I} \chi(x)$$

Et la somme de droite est nulle d'après le lemme précédent. □

Preuve du théorème (2).
Notons $S = G_\psi(\chi)G_\psi(\overline{\chi})$ qui par définition vaut :

$$S = \sum_{x,y \in R} \psi(x)\chi(x)\psi(y)\overline{\chi}(y) = \sum_{x \in R, y \in R^\times} \psi(x)\psi(y)\chi(xy^{-1})$$

En posant $u = xy^{-1}$, on a $x = uy$ si bien que :

$$S = \sum_{u \in R, y \in R^\times} \psi(uy)\psi(y)\chi(u) = \sum_{y \in R^\times} \psi(y) \sum_{u \in R} \psi(uy)\chi(u)$$

Et c'est maintenant là la clef : si y est non inversible, la somme $\sum_{u \in R} \psi(uy)\chi(u)$ est nulle (lemme précédent appliqué à $b \leftrightarrow y$). Si bien que l'on peut sommer sur R tout entier puis permuter sommations en u et en y :

$$S = \sum_{y \in R} \psi(y) \sum_{u \in R} \psi(uy)\chi(u) = \sum_{u \in R} \chi(u) \sum_{y \in R} \psi((1+u)y) \overset{\text{def}}{=} \sum_{u \in R} \chi(u) \sum_{y \in R} \psi_{1+u}(y)$$

Si $1 + u \neq 0$, alors, comme ψ est primitif, le caractère additif ψ_{1+u} n'est pas trivial et par conséquent (premier lemme de cette section) $\sum_{y \in R} \psi_{1+u}(y) = 0$.
Il reste donc :

$$S = \sum_{u \in R} \chi(-1) \times 1 = \chi(-1) \times \#R$$

OUF. □

Lois de réciprocité quadratique : en cours

On va pouvoir appliquer le résultat précédent à une somme de Gauss définie sur un corps fini. Mais c'est anti-pédagogique de procéder aini. Et on va donc refaire le calcul spécifique à ce cadre. En y apportant une variation sur le but (un corps quelconque au lieu de $\mathbb{C}$), ce qui permettra de prouver les lois de réciprocité quadratique.
A AMENAGER.

Corollaire 1 (La somme de Gauss quadratique τ_{p^*} pour un premier impair $p \geq 3$)**.**
Soit p un premier impair et $p^* = (-1)^{\frac{p-1}{2}}$. On définit la somme de Gauss

$$\tau_{p^*} = \tau_0 - \tau_1, \qquad \tau_0 = \sum_{i \in \mathbb{F}_p^{*2}} \zeta_p^i, \qquad \tau_1 = \sum_{i \in \mathbb{F}_p^* \setminus \mathbb{F}_p^{*2}} \zeta_p^i$$

(i) On a l'inclusion :

$$\mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\sqrt[p]{1}) \qquad \textit{certifiée par} \qquad \boxed{\tau_{p^*}^2 = p^*}$$

(ii) L'écriture $\tau = \tau_0 - \tau_1$ fournit un bonus arithmétique. En effet, puisque $\tau_0 + \tau_1 = -1$, on a :

$$4\tau_0\tau_1 = (\tau_0 + \tau_1)^2 - (\tau_0 - \tau_1)^2 = 1 - p^*$$

On en déduit que τ_0, τ_1 sont les racines de

$$X^2 - X + \frac{1-p^*}{4} \quad \textit{de discriminant } p^*$$

Et par suite

$$\boxed{\textit{Anneau des entiers de } \mathbb{Q}(\sqrt{p^*}) = \mathbb{Z}[\tau_1] = \mathbb{Z}[\tau_1] \subset \mathbb{Z}[\sqrt[p]{1}]}$$

Preuve.
A ECRIRE

□

Le caractère associé à un anneau quadratique (symbole de Kronecker)

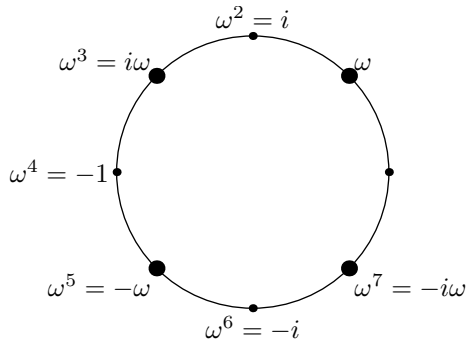
ATTENTION Oeuf-poule. On vise l'inclusion $\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\sqrt[|D|]{1})$ pour un discriminant quadratique fondamental D. Cela permettra de donner une assise propre au symbole de Kronecker χ_D. L'inclusion en question va être assurée en décomposant D en discriminants quadratiques fondamentaux élémentaires (ou primaires). Une fois le fondement de χ_D assuré, on pourra définir la somme quadratique de Gauss τ_D, qui habite $\mathbb{Q}(\sqrt[|D|]{1})$ et qui vérifie $\tau_D^2 = D$.

Les 3 discriminants exceptionnels $-4, 8, -8$

$$-4 = \mathrm{Disc}(\mathbb{Z}[i]), \qquad 8 = \mathrm{Disc}(\mathbb{Z}[\sqrt{2}]), \qquad -8 = \mathrm{Disc}(\mathbb{Z}[\sqrt{-2}])$$

liés aux inclusions cyclotomiques :

$$\mathbb{Z}[i] = \mathbb{Z}[\sqrt[4]{1}], \qquad \mathbb{Z}[\sqrt{2}] \subset \mathbb{Z}[\sqrt[8]{1}], \qquad \mathbb{Z}[\sqrt{-2}] \subset \mathbb{Z}[\sqrt[8]{1}]$$



On a les relations immédiates à établir :

$\omega = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \qquad i\omega = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2},$

$\omega^2 = i, \quad \omega^4 = -1$

Décomposition d'un discriminant quadratique fondamental en discriminants quadratiques fondamentaux primaires

Un discriminant quadratique Δ est le discriminant d'un anneau quadratique $\mathbb{Z}[\theta]$ où $\theta \notin \mathbb{Z}$ est racine d'un trinôme du second degré à coefficients entiers

$$X^2 - SX + P \in \mathbb{Z}[X], \qquad S^2 - 4P = \Delta$$

Les anneaux quadratiques sont classifiés par leur discriminant. Celui-ci doit vérifier :

$$\Delta \equiv 0, 1 \bmod 4, \qquad \Delta \text{ n'est pas un carré dans } \mathbb{Z}$$

On peut par exemple prendre pour représenter l'anneau quadratique de discriminant Δ :

$$\theta = \frac{\pm\Delta \pm \sqrt{\Delta}}{2} \qquad \text{de polynôme minimal} \qquad X^2 \pm \Delta X + \frac{\Delta^2 - \Delta}{4}$$

Cet anneau a pour description :

$$\left\{ \frac{x + y\sqrt{\Delta}}{2}, \quad x, y \in \mathbb{Z} \mid x \equiv y\Delta \bmod 2 \right\}$$

Un discriminant quadratique fondamental est le discriminant de l'anneau des entiers d'un corps quadratique. Il est noté D dans la suite. Il est caractérisé par la propriété arithmétique suivante :

$$\begin{cases} \text{soit } D \equiv 8, 12 \bmod 16 \text{ et } D/4 \text{ est sans facteur carré} \\ \text{soit } D \equiv 1 \bmod 4 \text{ et } D \text{ est sans facteur carré} \end{cases}$$

Ecrire un discriminant quadratique fondamental D sous la forme d'un produit de discriminants quadratiques fondamentaux primaires, premiers entre eux deux à deux :

$$(\star) \qquad D = D_1 \cdots D_k, \qquad D_i \in \{p^*, -4, 8, -8\}$$

Unicité.

Les fonctions qui font le job (in DiscriminantsQuadratiquesFondamentaux.magma)

```
Z := IntegerRing() ;
Values := {-1,0,1} ;
Chi8 := map < Z -> Values | m :-> IsOdd(m) select (-1)^ExactQuotient(m^2-1,8) else 0 > ;
ChiMinus4 := map < Z -> Values | m :-> IsOdd(m) select (-1)^ExactQuotient(m-1,2) else 0 > ;
ChiMinus8 := map < Z -> Values | m :-> Chi8(m)*ChiMinus4(m) > ;
Epsilon := map < Z -> Values | m :-> 1 > ;

// Le reste modulo p va fournir 0,1,p-1. A transformer en 0,1,-1
CenteredRemainder := func < x | x in {0,1} select x else -1 > ;
MetaChi := map < Z -> Maps(Z, Values) | p :->
                     map <Z -> Values | m :-> CenteredRemainder(Modexp(m, ExactQuotient(p-1,2), p)) > > ;

PrimaryDiscrimantalDecomposition := function(D)
  assert IsFundamentalDiscriminant(D) ;
  AbsD := Abs(D) ;
  Dodd := ExactQuotient(AbsD, 2^Valuation(AbsD,2)) ;
  OddPrimes := [Z| item[1] : item in Factorisation(Dodd)] ;
  assert Dodd eq &*OddPrimes ;
  Pstar := [Z| (-1)^ExactQuotient(p-1,2) * p : p in OddPrimes] ;
  D0 := ExactQuotient(D, &*Pstar) ;
  assert D0 in {1, -4, 8, -8} ;
  return D0, Pstar ;
end function ;

MyKroneckerCharacter := function(D)
  D0, Pstar := PrimaryDiscrimantalDecomposition(D) ;
  ChiD0 := D0 eq 1 select Epsilon
           else D0 eq -4 select ChiMinus4
           else D0 eq 8 select Chi8
           else ChiMinus8 ;
  return map < Z -> Values | m :-> ChiD0(m) * &*[Z| MetaChi(Abs(p))(m)  : p in Pstar] > ;
end function ;

borne := 10^4 ;
SomeFundamentalDiscriminants := [D : D in [-borne .. borne] | IsFundamentalDiscriminant(D)] ;
SFD := SomeFundamentalDiscriminants ;
```

Le fondement de χ_D pour un discriminant quadratique fondamental D

Théorème 3. *Soit D un discriminant quadratique fondamental.*
(1) On a l'inclusion :

$$\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\sqrt[|D|]{1})$$

(2) Cette inclusion fait naître un caractère quadratique, dit symbole de Kronecker :

$$\chi_D : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$$

de la manière suivante :

$$\sigma_m(\sqrt{D}) = \chi_D(m)\sqrt{D} \qquad m \wedge D = 1$$

Ici σ_m désigne, pour $m \wedge D = 1$, l'automorphisme de $\mathrm{Gal}\big(\mathbb{Q}(\sqrt[|D|]{1})/\mathbb{Q}\big)$ qui élève chaque racine de l'unité de $\mathbb{U}_{|D|}$ à la puissance m.

(3) Le symbole de Kronecker est relié au symbole de Legendre par le fait que pour tout nombre premier impair $p \geq 3$:

$$\chi_D(p) = \left(\frac{D}{p}\right)$$

(4) On a pour m impair

$$\chi_{-4}(m) = (-1)^{\frac{m-1}{4}}, \qquad \chi_8(m) = (-1)^{\frac{m^2-1}{8}}, \qquad \chi_{-8}(m) = -\chi_8(m+2) = \chi_{-4}(m)\chi_8(m)$$

(5) On suppose D impair (donc $D \equiv 1 \bmod 4$) :

$$\chi_D(2) = \chi_8(D) = (-1)^{\frac{D^2-1}{8}} = \begin{cases} 1 & \text{si } D \equiv 1 \bmod 8 \\ -1 & \text{si } D \equiv 5 \bmod 8 \end{cases}$$

Preuve.
On écrit $D = D_1 \cdots D_k$ où les D_i sont des discriminants quadratiques fondamentaux élémentaires, premiers deux à deux ; élémentaire signifie de la forme q^* avec q premier impair ≥ 3 ou dans $\{-4, 8, -8\}$.

(1) On a :

$$\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\sqrt{D_1}, \dots, \sqrt{D_k}), \qquad \mathbb{Q}(\sqrt[|D_i|]{1}) \subset \mathbb{Q}(\sqrt[|D|]{1})$$

Il suffit donc de voir que $\mathbb{Q}(\sqrt{D_i}) \subset \mathbb{Q}(\sqrt[|D_i|]{1})$ pour un discriminant quadratique fondamental primaire. Mais justement, cela a été établi auparavant.
(2) Cela vient du fait que $\mathbb{Q}(\sqrt{D})$ est stable par chaque σ_m ou plus innocemment que $\sigma_m(D) = D$ donc $\sigma_m(\sqrt{D}) = \pm\sqrt{D}$.
(3) On va utiliser la loi de réciprocité quadratique pour chaque D_i en montrant que :

$$\sigma_p(\sqrt{D_i}) = \left(\frac{D_i}{p}\right)\sqrt{D_i}$$

En multipliant ces égalités, on obtiendra $\sigma_p(\sqrt{D}) = \left(\frac{D}{p}\right)\sqrt{D}$.
Allons-y pour D_i de la forme q^*. On écrit :

$$\sqrt{q^*} = \tau_0 - \tau_1, \qquad \tau_0 = \sum_{i \in \mathbb{F}_q^{*2}} \zeta_q^i, \qquad \tau_1 = \sum_{j \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*2}} \zeta_q^j$$

On a alors :

$$\begin{cases} \sigma_p(\tau_0) = \tau_0 \\ \sigma_p(\tau_1) = \tau_1 \end{cases} \text{ si } p \text{ est un carré modulo } q \qquad \begin{cases} \sigma_p(\tau_0) = \tau_1 \\ \sigma_p(\tau_1) = \tau_0 \end{cases} \text{ si } p \text{ non carré modulo } q$$

Et donc :

$$\sigma_p(\sqrt{q^*}) = \left(\frac{p}{q}\right)\sqrt{q^*}$$

Mais (loi de réciprocité quadratique)

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$$

Et c'est donc gagné pour D_i de la forme q^*.
Pour $D_i \in \{-4, 8, -8\}$, on procède de la même manière en utilisant les 2 lois complémentaires de réciprocité quadratique. Par exemple pour -4, en écrivant $\sqrt{-4} = 2i$:

$$\sigma_p(2i) = 2i^p = 2\left(\frac{-1}{p}\right) i = \left(\frac{-4}{p}\right) 2i$$

(4) Les deux lois complémentaires de réciprocité quadratique.
(5) Ecrire $D = D_1 \dots D_k$ où les D_i sont élémentaires et le faire pour chaque D_i. □

Lemme 8 (calcul de $\chi_D(m)$)**.**
(i) On peut déterminer $\chi_D(m)$ en ayant décomposé D décomposé sous la forme $(\star)$:

$$\chi_D(m) = \chi_{D_1}(m) \cdots \chi_{D_k}(m)$$

(ii) Mieux : pour deux discriminants quadratiques fondamentaux D_1, D_2 premiers entre eux, alors $D = D_1 D_2$ est un discriminant quadratique fondamental et

$$\chi_D(m) = \chi_{D_1}(m)\chi_{D_2}(m)$$

Preuve. A FAIRE □

Lemme 9.
Soit D un discriminant quadratique fondamental et χ_D le symbole de Kronecker associé (c'est un caractère multiplicatif sur $(\mathbb{Z}/D\mathbb{Z})^\times$).
(1) C'est un caractère **primitif**.
(2) Si $\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\sqrt[m]{1})$, alors $|D|$ divise m. C.a.d que le conducteur cyclotomique de $\mathbb{Q}(\sqrt{D})$ est $|D|$.

Preuve.
► Montrons le côté primitif d'abord pour un discriminant fondamental primaire.
A FAIRE.

► Utilisons ensuite « l'assemblage » qui vient. Considérons deux discriminants quadratiques fondamentaux D_1, D_2 premiers entre eux, de sorte que $D = D_1 D_2$ est un discriminant quadratique fondamental ; supposons que χ_{D_1} et χ_{D2} sont primitifs, et montrons qu'il en est de même de χ_D.
Soit D' un diviseur strict de D. On a $D' = D'_1 D'_2$ avec $D'_i = \gcd(D_i, D')$. On a par exemple que D'_1 est un diviseur strict de D_1. Puisque χ_{D_1} est primitif, il existe $m_1 \in \mathbb{Z}$ vérifiant :

$$m_1 \wedge D_1 = 1, \qquad m_1 \equiv 1 \bmod D'_1, \qquad \chi_{D_1}(m_1) = -1$$

Choisissons m vérifiant :

$$m \equiv \begin{cases} m_1 & \bmod D_1 \\ 1 & \bmod D_2 \end{cases}$$

Alors :

$$m \wedge D = 1, \qquad m \equiv 1 \bmod D', \qquad \chi_D(m) = \chi_{D_1}(m)\chi_{D_2}(m) = \chi_{D_1}(m_1)\chi_{D_2}(1) = -1$$

ce qu'il fallait montrer (l'existence d'un tel m).

(2) A FAIRE. Fröhlich-Taylor p. 22 dans la preuve du th. 48 □

Somme de Gauss τ_D en chantier

Somme de Gauss

$$\tau_D = \sum_{m \in (\mathbb{Z}/D\mathbb{Z})^\times} \chi_D(m)\zeta_{|D|}^m$$

Lemme 10 (multiplicativité des sommes de Gauss)**.**
Pour deux discriminants quadratiques fondamentaux D_1, D_2 premiers entre eux, leur produit est un discriminant quadratique fondamental et l'on a :

$$\tau_{D_1 D_2} = \varepsilon\ \tau_{D_1}\tau_{D_2}, \qquad \varepsilon = \chi_{D_1}(D_2)\chi_{D_2}(D_1)$$

Preuve. A FAIRE □

Corollaire 2.
Pour un discriminant quadratique fondamental D, notons τ_D la somme de Gauss quadratique :

$$\tau_D = \sum_{m \in (\mathbb{Z}/D\mathbb{Z})^\times} \chi_D(m)\zeta_{|D|}^m$$

Alors :

$$\boxed{\tau_D^2 = D}$$

Preuve. L'anneau $\mathbb{Z}/D\mathbb{Z}$ est de cardinal $|D|$ donc :

$$\tau_D^2 = \chi_D(-1) \times |D| = \text{signe de } D \times |D| = D$$

□

Lemme 11.
Soit $N \geq 1$. Alors la somme s_N des racines primitives N-èmes de l'unité (ou encore le coefficient de degré $\varphi(n) - 1$ du polynôme cyclotomique Φ_n) vaut $0, \pm 1$. Très exactement :

$$s_N = \mu(N)$$

où μ est la fonction de Moebius définie par

$$\mu(N) = \begin{cases} (-1)^r & \text{si } N = p_1 \cdots p_r \text{ où } p_1, \cdots, p_r \text{ sont des premiers distincts} \\ 0 & \text{sinon} \end{cases}$$

Preuve.
Soit ζ_N une racine primitive d'ordre N. Puisqu'une racine N-ème de l'unité possède un ordre d (et un seul !) qui est un entier divisant N, on a :

$$\sum_{d|N} s_d = \sum_{k=0}^{N-1} \zeta_N^k = \begin{cases} 0 & \text{si } N > 1 \\ 1 & \text{si } N = 1 \end{cases}$$

Mais une telle égalité est vérifiée par la fonction de Möbius :

$$\sum_{d|N} \mu(d) = \begin{cases} 0 & \text{si } N > 1 \\ 1 & \text{si } N = 1 \end{cases}$$

égalité qui est à la base du produit arithmétique. Quelques rappels. L'élément neutre du produit arithmétique est la fonction δ_1 :

$$\delta_1 : n \longmapsto \begin{cases} 0 & \text{si } n > 1 \\ 1 & \text{si } n = 1 \end{cases}$$

Et l'égalité ci-dessus dit que la fonction μ et la fonction constante 1 sont inverses l'une de l'autre pour le produit arithmétique :

$$\mu \star \mathrm{cst}_1 = \delta_1$$

Bref : $s = \mu$. □

Bonus arithmétique pour la somme de Gauss τ_D

On fixe D et on écrit $\tau = \tau_D$ sous la forme :

$$\tau = \tau_0 - \tau_1, \qquad \tau_0 = \sum_{m|\chi_D(m)=1} \zeta_{|D|}^m, \qquad \tau_1 = \sum_{m|\chi_D(m)=-1} \zeta_{|D|}^m$$

Alors :

$$\tau_0 + \tau_1 = \mu(|D|) = \begin{cases} 0 & \text{si } D \text{ est pair} \\ -1 & \text{si } |D| \text{ est impair, composé d'un nombre impair de premiers} \\ 1 & \text{si } |D| \text{ est impair, composé d'un nombre pair de premiers} \end{cases}$$

En conséquence :

$$4\tau_0\tau_1 = (\tau_0 + \tau_1)^2 - (\tau_0 - \tau_1)^2 = \mu(|D|)^2 - D$$

Et τ_0, τ_1 sont racines du trinôme de discriminant D :

$$X^2 - \mu(|D|)X + \frac{\mu(|D|)^2 - D}{4} = \begin{cases} X^2 - \frac{D}{4} & \text{si } D \text{ est pair} \\ X^2 \pm X + \frac{1-D}{4} & \text{si } D \text{ est impair} \end{cases}$$

En conséquence :

$$\mathbb{Z}[\tau_0] = \mathbb{Z}[\tau_1] = \text{ anneau des entiers de } \mathbb{Q}(\sqrt{D})$$