THÉORIE ALGÉBRIQUE DES NOMBRES.

Richard Ganaye

10 décembre 2023

Chapitre 1

Décomposition en somme de carrés.

Nous commençons par donner les premiers exemples d'anneaux d'entiers de corps quadratiques, à savoir $\mathbb{Z}[i], \mathbb{Z}[i\sqrt{2}]$, et $\mathbb{Z}[\omega]$ (où $\omega = e^{\frac{2i\pi}{3}}$). Nous étudierons dans les chapitres suivants des anneaux d'entiers plus généraux.

Ce traitement à part est dû au fait que ces anneaux sont euclidiens pour la norme usuelle des nombres complexes, et donc principaux et factoriels. Ils permettront de donner les premiers résultats sur la décomposition des nombres premiers sous la forme $x^2 + y^2, x^2 + 2y^2$ ou $x^2 + 3y^2$. Les anneaux $\mathbb{Z}[i], \mathbb{Z}[\omega]$ seront indispensables à la théorie de la réciprocité cubique, et biquadratique.

1.1 Les anneaux $\mathbb{Z}[i], \mathbb{Z}[i\sqrt{2}]$.

$\mathbb{Z}[i]$ est l'ensemble des nombres complexes de la forme $a + bi$, où a, b sont des entiers de $\mathbb{Z}$:

$$\mathbb{Z}[i] = \{z \in \mathbb{C} \mid \exists a \in \mathbb{Z}, \exists b \in \mathbb{Z}, z = a + bi\}.$$

Les éléments de $\mathbb{Z}[i]$ s'appellent les entiers de Gauss.

$\mathbb{Z}[i]$ est bien un anneau (commutatif unitaire), un sous-anneau de $(\mathbb{C}, +, \times)$. En effet, $1 = 1 + 0i \in \mathbb{Z}[i]$, et si z, z' sont dans $\mathbb{Z}[i]$, alors $z = a + bi, z' = a' + b'i$, donc $z - z' = (a - a') + (b - b')i \in \mathbb{Z}[i]$, et $zz' = (a + bi)(a' + b'i) = (aa' - bb') + (ab' + ba')i \in \mathbb{Z}[i]$.

$\mathbb{Z}[i]$ est le plus petit sous-anneau de $\mathbb{C}$ contenant $\mathbb{Z}$ et i.

De la même façon,

$$\mathbb{Z}[i\sqrt{2}] = \{z \in \mathbb{C} \mid \exists a \in \mathbb{Z}, \exists b \in \mathbb{Z}, z = a + bi\sqrt{2}\}$$

est le plus petit sous-anneau de $\mathbb{C}$ contenant $\mathbb{Z}$ et la racine $i\sqrt{2}$ de -2.

Comme $\mathbb{Z}[i] = \mathbb{Z}[-i]$, et $\mathbb{Z}[i\sqrt{2}] = \mathbb{Z}[-i\sqrt{2}]$, on peut désigner sans ambiguïté ces deux anneaux par $\mathbb{Z}[\sqrt{-1}], \mathbb{Z}[\sqrt{-2}]$, le choix de la racine de -1 ou de -2 n'ayant pas d'importance.

Montrons que ces deux anneaux sont euclidiens, pour la norme usuelle $\mathrm{N}(\cdot)$ des nombres complexes, définie pour tout $z \in \mathbb{C}$ par $\mathrm{N}(z) = |z|^2$.

Proposition 1. *(i) Si $z \in \mathbb{C}$, il existe $z_0 \in \mathbb{Z}[i]$ tel que $\mathrm{N}(z - z_0) < 1$.*

(ii) Si $z \in \mathbb{C}$, il existe $z_1 \in \mathbb{Z}[i\sqrt{2}]$ tel que $\mathrm{N}(z - z_1) < 1$.

Démonstration. (i) Soit $z = a + bi \in \mathbb{C}$. Il existe des entiers $a_0, b_0 \in \mathbb{Z}$ tels que

$$|a - a_0| < \frac{1}{2}, \quad |b - b_0| < \frac{1}{2}.$$

($a_0 = \lfloor a \rfloor$ convient si $\lfloor a \rfloor \leq a < \lfloor a \rfloor + 1/2$, et $a_0 = \lfloor a \rfloor + 1 = \lceil a \rceil$ convient si $\lfloor a \rfloor + 1/2 \leq a < \lfloor a \rfloor + 1$. Idem pour b_0). Posons $z_0 = a_0 + b_0 i$. Alors $\mathrm{N}(z - z_0) = (a - a_0)^2 + (b - b_0)^2 < \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$.

(ii) Tout élément $z \in \mathbb{C}$ peut s'écrire sous la forme $z = a + bi\sqrt{2},\ a, b \in \mathbb{R}$. Soient $a_0, b_0 \in \mathbb{Z}$ vérifiant $|a - a_0| < \frac{1}{2}, \quad |b - b_0| < \frac{1}{2}$. Posons $z_1 = a_0 + b_0 i\sqrt{2}$. Alors $\mathrm{N}(z - z_1) = (a - a_0)^2 + 2(b - b_0)^2 < \frac{1}{4} + 2 \times \frac{1}{4} = \frac{3}{4} < 1$.

□

Proposition 2. *$\mathbb{Z}[i]$ et $\mathbb{Z}[i\sqrt{2}]$ sont des anneaux euclidiens, pour la norme $\mathrm{N}(\cdot)$ de $\mathbb{C}$.*

Démonstration. Donnons une démonstration commune pour $A = \mathbb{Z}[i]$, ou $A = \mathbb{Z}[i\sqrt{2}]$.

Si $a, b \in A$, et $b \neq 0$, il existe d'après la proposition précédente $q \in A$ tel que $\left|\frac{a}{b} - q\right| < 1$. Posons alors $r = a - bq = b\left(\frac{a}{b} - q\right)$. Alors $r \in A$, et

$$a = bq + r, \quad 0 \leq \mathrm{N}(r) < \mathrm{N}(b).$$

Il existe donc une division euclidienne dans A. □

En conclusion, d'après le chapitre "Anneaux", ces anneaux sont principaux et factoriels.

Avant d' expliciter la décomposition en facteurs premiers, précisons les unités de ces anneaux. Notons $A^\times$ l'ensemble des unités de A, où A est un sous-anneaux de $\mathbb{C}$. Alors

Proposition 3. *Soit $A = \mathbb{Z}[i]$ (ou $A = \mathbb{Z}[i\sqrt{2}]$), et $A^\times$ l'ensemble des unités de A. Si $z \in A$,*

$$z \in A^\times \iff \mathrm{N}(z) = 1.$$

Démonstration. Si $z \in A^\times$, alors il existe $z' \in A$ tel que $zz' = 1$, Donc $\mathrm{N}(z)\mathrm{N}(z') = 1$, où $\mathrm{N}(z), \mathrm{N}(z')$ sont des entiers naturels de $\mathbb{N}$. Donc $\mathrm{N}(z) = 1$.

Réciproquement, supposons $\mathrm{N}(z) = 1$, alors $z\overline{z} = 1$.

Si $A = \mathbb{Z}[i]$, alors $z = a + ib,\ a, b \in \mathbb{Z}$, donc $\overline{z} = a - ib \in A$.

Si $A = \mathbb{Z}[i\sqrt{2}]$, alors $z = a + ib\sqrt{2},\ a, b \in \mathbb{Z}$, donc $\overline{z} = a - ib\sqrt{2} \in A$.

Dans les deux cas, $z' = \overline{z} \in A$ vérifie $zz' = 1$, donc $z \in A^\times$. □

Proposition 4. *(i) Les unités de $\mathbb{Z}[i]$ sont $1, i, i^2 = -1, i^3 = -i$.*

$$\mathbb{Z}[i]^\times = \{1, i, i^2, i^2\} = \mathbb{U}_4.$$

(i) Les unités de $\mathbb{Z}[i\sqrt{2}]$ sont 1 et -1.

$$\mathbb{Z}[i\sqrt{2}]^\times = \{1, -1\} = \mathbb{U}_2.$$

Démonstration. (i) Soit $z = a + bi \in \mathbb{Z}[i]$. Alors $z = a + ib \in \mathbb{Z}[i]^\times$ si et seulement si $a^2 + b^2 = 1$. Comme $|a| \leq 1, |b| \leq 1$, l'ensemble des solutions de cette équation dans $\mathbb{Z}$ est $\{(1,0),(0,1),(-1,0),(0,-1)\}$, ce qui donne les solutions complexes $1, i, -1, -i$ de $\mathrm{N}(z) = 1$.

(ii) Soit $z = a + bi \in \mathbb{Z}[i\sqrt{2}]$. Alors $z = a + ib\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]^\times$ si et seulement si $a^2 + 2b^2 = 1$. Alors $|b| \leq 1/2$, donc $b = 0$, et les seules solutions sont $(1,0),(-1,0)$.

□

1.2 Somme de deux carrés : une première preuve.

Avant de donner la liste des éléments premiers dans $\mathbb{Z}[i]$, on peut utiliser le fait que $\mathbb{Z}[i]$ est principal dans une démonstration courte du théorème des deux carrés.

Proposition 5. *Soit p un nombre premier congru à 1 modulo 4. Alors il existe un entier $a \in \mathbb{Z}$ tels que p divise a^2+1.*

Démonstration. Notons $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$ à p éléments. Pour tout $\alpha \in \mathbb{F}_p^*$,

$$0 = \alpha^{p-1} - 1 = (\alpha^{\frac{p-1}{2}} - 1)(\alpha^{\frac{p-1}{2}} + 1).$$

Comme le polynôme $x^{\frac{p-1}{2}} - 1 \in \mathbb{F}_p[x]$ admet au plus $\frac{p-1}{2}$ racines dans $\mathbb{F}_p^*$, et que le cardinal de $\mathbb{F}_p^*$ est $p-1$, il existe au moins un $\beta \in \mathbb{F}_p$ tel que $\beta^{\frac{p-1}{2}} + 1 = 0$, soit $\left(\beta^{\frac{p-1}{4}}\right)^2 + 1 = 0$, où l'exposant $(p-1)/4$ est entier, puisque $p \equiv 1 \pmod 4$.

Posons $\gamma = \beta^{\frac{p-1}{4}}$. Alors $\gamma^2 + 1 = 0$.

Si $a \in \mathbb{Z}$ est un représentant de $\gamma \in \mathbb{F}_p$, alors p divise a^2+1. □

Donnons maintenant le théorème des deux carrés.

Proposition 6. *Soit p un nombre premier impair. Alors $p \equiv 1 \pmod 4$ si et seulement s'il existe un couple d'entiers (x, y) tel que $p = x^2 + y^2$.*

Démonstration. Soit p un nombre premier impair.

($\Leftarrow$) Si $p = x^2 + y^2$, alors $x^2 \equiv 0, 1 \pmod 4$, $y^2 \equiv 0, 1 \pmod 4$, donc $x^2 + y^2 \equiv 0, 1, 2 \pmod 4$. Comme p est impair, $p \equiv 1 \pmod 4$.

($\Rightarrow$) Soit a un entier, dont l'existence est prouvée dans la proposition précédente, tel que $p \mid a^2 + 1$.

Soit I l'idéal de $\mathbb{Z}[i]$ défini par

$$I = p\mathbb{Z}[i] + (a+i)\mathbb{Z}[i] = \langle p, a+i \rangle.$$

Montrons que $I \neq \mathbb{Z}[i]$, en prouvant que l'hypothèse $I = \mathbb{Z}[i]$ est absurde.

Soit λ un diviseur premier de p dans $\mathbb{Z}[i]$: un tel diviseur existe puisque $\mathbb{Z}[i]$ est principal.

Alors $\lambda \mid p$, et $p \mid a^2 + 1 = (a+i)(a-i)$, donc $\lambda \mid (a+i)(a-i)$. L'entier de Gauss λ étant premier, il divise soit $a+i$, soit $a-i$.

Dans la premier cas, λ divise p et $a+i$. Dans le deuxième cas, $\lambda \mid a-i$, alors $a-i = \lambda\mu$, donc $a + i = \overline{\lambda}\overline{\mu}$, où $\overline{\mu} \in \mathbb{Z}[i]$, donc $\overline{\lambda} \mid a+i$. De plus $\overline{\lambda} \mid p$: en effet $p = \lambda\nu$ pour un certain $\nu \in \mathbb{Z}[i]$, donc $p = \overline{\lambda}\overline{\nu}$. Notons que $\mathrm{N}(\lambda) = \mathrm{N}(\overline{\lambda}) > 1$.

Dans les deux cas, il existe $\xi \in \mathbb{Z}[i]$ (où $\xi = \lambda$ ou $\xi = \overline{\lambda}$) tel que $\xi \mid p, \xi \mid a+i$, et $\mathrm{N}(\xi) > 1$.

Sous l'hypothèse $I = \mathbb{Z}[i]$, alors $1 = p\zeta + (a+i)\eta$, où ζ, η sont des entiers de Gauss. Alors $\xi \mid 1$, en contradiction avec $\mathrm{N}(\xi) > 1$, ce qui prouve que $I \neq \mathbb{Z}[i]$.

Comme $\mathbb{Z}[i]$ est principal, il existe $\pi \in \mathbb{Z}[i]$ tel que

$$p\mathbb{Z}[i] + (a+i)\mathbb{Z}[i] = \pi\mathbb{Z}[i].$$

De plus π n'est pas une unité, sinon $\pi\mathbb{Z}[i] = \mathbb{Z}[i]$. Par conséquent $\mathrm{N}(\pi) > 1$. Nous venons de prouver l'existence d'un pgcd non trivial π de p et $a+i$.

Comme $p = p \times 1 + (a+i) \times 0 \in p\mathbb{Z}[i] + (a+i)\mathbb{Z}[i] = \pi\mathbb{Z}[i]$, il existe $\gamma \in \mathbb{Z}[i]$ tel que $p = \pi\gamma$, et donc $p^2 = \mathrm{N}(\pi)\mathrm{N}(\gamma)$.

Si $\mathrm{N}(\gamma) = 1$, alors γ est une unité, donc p et π sont associés, et π divise $a + i$, donc p divise $a + i$, ce qui est absurde puisque $\frac{a}{p} + \frac{1}{p}i \notin \mathbb{Z}[i]$. Ainsi $\mathrm{N}(\gamma) > 1$.

L'égalité $p^2 = \mathrm{N}(\pi)\mathrm{N}(\gamma)$, où $\mathrm{N}(\pi) > 1, \mathrm{N}(\gamma) > 1$, montre que

$$p = \mathrm{N}(\pi).$$

Si $\pi = x + iy,\ x, y \in \mathbb{Z}$, alors $p = x^2 + y^2$, ce qui prouve le théorème. □

La démonstration d'existence fournit un premier algorithme efficace pour décomposer un nombre premier p en somme de deux carrés.

- Première étape : trouver un entier a tel que $p \mid a^2 + 1$.
  La démonstration de la proposition 5 montre que la moitié (à savoir $\frac{p-1}{2}$) des éléments α de $\mathbb{F}_p^*$ vérifie $\alpha^{\frac{p-1}{2}} = 1$, l'autre moitié vérifie $\alpha^{\frac{p-1}{2}} = -1$.
  Il suffit donc de tirer au sort un élément $a,\ 1 \leq a < p$, et de calculer le moindre reste de $a^{\frac{p-1}{2}}$ modulo p par une exponentiation rapide modulaire. Si le résultat est -1, a convient, sinon on recommence le tirage jusqu'à obtenir -1. Le temps d'attente d'un résultat suis une loi géométrique de paramètre $1/2$. Ce temps d'attente a donc une espérance de deux tirages.
  Evidemment on ne peut garantir que cet algorithme probabiliste donne un résultat rapide, mais la probabilité que ce soit le cas est forte. On ne connait pas d'algorithme déterministe plus efficace.
- Trouver un pgcd de p et $a + i$.
  L'anneau $\mathbb{Z}[i]$ étant euclidien, l'algorithme d'Euclide s'applique pour obtenir un tel pgcd : on définit les suites finies (r_n) d'entiers de Gauss par des divisions euclidiennes successives dans $\mathbb{Z}[i]$, tant que le reste r_n est non nul

$$\begin{aligned} &r_0 = p, \quad r_1 = a + i, \\ &r_n = r_{n+1}q_{n+1} + r_{n+2},\ \mathrm{N}(r_{n+2}) < \mathrm{N}(r_{n+1}) \qquad (0 \leq n \leq l) \\ &r_{l+2} = 0 \end{aligned}$$

  $r_{l+1} = x + iy$ donne alors un pgcd de p et $a + i$, et $p = x^2 + y^2$.

Le programme correspondant est donné dans l'appendice.

1.3 Elements premiers dans $\mathbb{Z}[i]$.

Proposition 7. *Soit $\pi \in \mathbb{Z}[i]$. Si $\mathrm{N}(\pi)$ est premier dans $\mathbb{Z}$, alors π est premier dans $\mathbb{Z}[i]$.*

Démonstration. Supposons que $\pi = \alpha\beta$, où α, β sont dans $\mathbb{Z}[i]$. Par hypothèse, $p = \mathrm{N}(\pi) = \mathrm{N}(\alpha)\mathrm{N}(\beta)$ est premier dans $\mathbb{Z}$, $p > 0$, donc $\mathrm{N}(\alpha) = 1$ ou $\mathrm{N}(\beta) = 1$. D'après la proposition 3, α ou β est une unité, ce qui prouve que π est irréductible, donc premier dans $\mathbb{Z}[i]$, puisque $\mathbb{Z}[i]$ est principal. □

Par exemple $\mathrm{N}(2+3i) = 13$, donc $2+3i$ est premier. Nous allons voir que la réciproque de cette proposition est fausse.

Proposition 8. *Soit π un élément premier dans $\mathbb{Z}[i]$. Alors il existe un unique entier rationnel premier $p \in \mathbb{N}$ tel que $\pi \mid p$.*

Démonstration. Le premier π divise l'entier naturel $n = \mathrm{N}(\pi) = \pi\overline{\pi}$. Alors $n > 1$, sinon π serait une unité. L'entier rationnel n se décompose en facteurs premiers dans $\mathbb{N}$ sous la forme $n = p_1^{a_1} \cdots p_l^{a_l}$. Comme π est premier, π divise l'un des p_i. Si p désigne un tel p_i, $\pi \mid p$, et $p \in \mathbb{N}$ est un entier rationnel premier.

Supposons que $\pi \mid p, \pi \mid q$, où p, q sont des nombres premiers rationnels distincts. Alors p, q sont premiers entre eux, donc il existe des entiers u, v dans $\mathbb{Z}$ tels que $up + vq = 1$. Mais alors $\pi \mid up + vq = 1$, et π est une unité : c'est une contradiction, qui prouve l'unité de l'entier p de l'énoncé. □

Cette proposition montre que pour lister tous les éléments premiers de $\mathbb{Z}[i]$, il suffit de factoriser tous les nombres premiers rationnels. Un tel premier rationnel admet toujours au moins un diviseur premier $\pi \in \mathbb{Z}[i]$.

Donnons d'abord une liste d'éléments premiers :

- $\mathrm{N}(1 + i) = 2$ est premier dans $\mathbb{Z}$, donc $1 + i$ est premier, ainsi que ses associés $-1 + i, -1 - i, 1 - i$.
- Soit $q \equiv 3 \pmod 4$ un nombre premier dans $\mathbb{Z}$, $q > 0$. Montrons que q est irréductible dans $\mathbb{Z}[i]$. Dans le cas contraire, $q = \alpha\beta$, où α, β sont des entiers de Gauss vérifiant $\mathrm{N}(\alpha) > 1, \mathrm{N}(\beta) > 1$. Alors $q^2 = \mathrm{N}(\alpha)\mathrm{N}(\beta)$, donc $q = \mathrm{N}(\alpha)$ (nous utilisons ici l'hypothèse $q > 0$). Si $\alpha = a + bi$, alors $q = a^2 + b^2$, mais $a^2 + b^2 \equiv 3 \pmod 4$ est impossible, ce qui montre que q est irréductible dans $\mathbb{Z}[i]$. Comme $\mathbb{Z}[i]$ est principal, q est premier dans $\mathbb{Z}[i]$, ainsi que ses associés iq, i^2q, i^3q. Notons que si $\pi \sim q$, où $q > 0, q \equiv 3 \pmod 4$, alors π est premier dans $\mathbb{Z}[i]$, mais $\mathrm{N}(\pi) = q^2$ n'est pas premier dans $\mathbb{Z}$. La réciproque de la proposition **??** est fausse.
- Soit p un nombre premier tel que $p = \mathrm{N}(\pi)$, $\pi = a + bi \in \mathbb{Z}[i]$ (donc $p = a^2 + b^2 \equiv 1 \pmod 4$). Alors π est premier dans $\mathbb{Z}[i]$ puisque $\mathrm{N}(\pi)$ est premier dans $\mathbb{Z}$.

Ces éléments seront désignés comme les éléments premiers connus dans $\mathbb{Z}[i]$. Montrons qu'il n'existe pas d'autres éléments premiers.

Proposition 9. *Les éléments premiers dans $\mathbb{Z}[i]$ sont*

(i) $1 + i$ et ses associés,

(ii) les entiers rationnels $q \equiv 3 \pmod 4$, $q > 0$, premiers dans $\mathbb{Z}$, ainsi que leurs associés,

(iii) les éléments $\pi = a + ib$ tels que $p = \pi\overline{\pi} = a^2 + b^2$ soit premier dans $\mathbb{Z}$.

Démonstration. Soit $\pi = a + bi$ un élément premier dans $\mathbb{Z}[i]$. La proposition 8 montre qu'il existe un nombre premier $p \in \mathbb{N}$ tel que $\pi \mid p$.

Discutons les trois seuls cas possibles, $p = 2, p \equiv 3 \pmod 4$, et $p \equiv 1 \pmod 4$.

(i) Supposons que $\pi \mid 2$. Comme $2 = (1 + i)(1 - i) = -i(1 + i)^2$, où $1 + i$ est premier, et $-i$ est une unité, alors $\pi \mid 1 + i$. Comme $1 + i$ est premier, π est associé à $1 + i$.

(ii) Supposons que $\pi \mid p$, où $p \equiv 3 \pmod 4$. Puisque p est un élément premier connu de $\mathbb{Z}[i]$, π est associé à p.

(iii) Supposons que $\pi \mid p$, où $p \equiv 1 \pmod 4$. Alors $p = \pi\lambda$ pour un certain $\lambda \in \mathbb{Z}[i]$.
Montrons par l'absurde que p n'est pas premier dans $\mathbb{Z}[i]$.
D'après la proposition 5, il existe $a \in \mathbb{Z}$ tel que $p \mid a^2 + 1$, donc $p \mid (a + i)(a - i)$, et p étant premier dans $\mathbb{Z}[i]$, $p \mid a + i$, ou $p \mid a - i$. Ceci est absurde puisque $\frac{a}{p} \pm \frac{1}{p}i \notin \mathbb{Z}[i]$.
Alors λ n'est pas une unité, sinon p serait associé à π et serait donc premier. Ainsi $p = \pi\lambda$, où $\mathrm{N}(\pi) > 1, \mathrm{N}(\lambda) > 1$. L'égalité $p^2 = \mathrm{N}(\pi)\mathrm{N}(\lambda)$ montre que $p = \mathrm{N}(\pi) = \pi\overline{\pi} = a^2 + b^2$.

□

Incidemment, nous obtenons une deuxième preuve du théorème des deux carrés :

Soit $p \in \mathbb{N}$ un entier premier tel que $p \equiv 1 \pmod 4$, alors $p = a^2 + b^2$ est somme de deux carrés d'entiers.

Démonstration. Reprenons l'argument de la partie (iii) de la démonstration précédente : Si $p \equiv 1 \pmod 4$, alors (proposition 5) il existe un entier a tel que $p \mid a^2+1 = (a+i)(a-i)$, mais $p \nmid a+i, p \nmid a-i$, donc p n'est pas premier, a fortiori il n'est pas irréductible, donc

$$p = \alpha\beta, \text{ où } \mathrm{N}(\alpha) > 1, \mathrm{N}(\beta) > 1.$$

Alors $p^2 = \mathrm{N}(\alpha)\mathrm{N}(\beta)$, donc $p = \mathrm{N}(\alpha)$. Si $\alpha = a + bi$, alors $p = a^2 + b^2$. □

Cette démonstration ne donne pas explicitement un algorithme pour obtenir la décomposition $p = a^2 + b^2$. Un tel algorithme est donné dans la section précédente. Nous expliciterons d'autres algorithmes dans le paragraphe suivant.

Prouvons maintenant l'unicité de la décomposition en somme de deux carrés.

Proposition 10. *Si $p \equiv 1 \pmod 4$, il existe exactement un couple d'entiers (a, b) tel que $p = a^2 + b^2$, où $0 < a < b$.*

Démonstration. La proposition 6 prouve l'existence d'entiers x, y tels que $p = x^2 + y^2$. Posons $a = \min(|x|, |y|), b = \max(|x|, |y|)$. Alors $p = a^2 + b^2$, où $0 \leq a \leq b$. De plus $a = 0$ est impossible : un nombre premier ne peut être le carré de b, et $a = b$ est impossible, sinon $p = 2b^2$, où $b > 1$, n'est pas premier. Donc $p = a^2 + b^2,\ 0 < a < b$.

Supposons que $p = a^2 + b^2 = c^2 + d^2$, où $0 < a < b$ et $0 < c < d$. Posons $\pi = a + bi, \lambda = c + di$. La proposition 7 montre que $\pi, \overline{\pi}, \lambda, \overline{\lambda}$ sont premiers dans $\mathbb{Z}[i]$, et

$$p = \pi\overline{\pi} = \lambda\overline{\lambda}.$$

Comme le premier π divise $\lambda\overline{\lambda}$, π divise λ ou $\pi \mid \overline{\lambda}$. Ces éléments étant tous premiers, π est associé à λ ou $\overline{\lambda}$, soit

$$a + ib \in \{c + id, i(c + id), -(c + id), -i(c + id), c - id, i(c - id) - (c - id), -i(c - id)\}.$$

Par conséquent $a = \pm c, b = \pm d$, ou $a = \pm d, b = \pm c$. Comme a, b, c, d sont positifs $(a, b) = (c, d)$ ou $(a, b) = (d, c)$. Mais $a < b$ et $c < d$, donc $(a, b) = (c, d)$. □

Remarque : si on oublie la condition $0 < x < y$, l'équation $p = x^2 + y^2$ admet 8 solutions : $(a, b), (-a, b), (a, -b), (-a, -b), (b, a), (-b, a), (a, -b), (-a, -b)$.

Nous pouvons préciser les éléments premiers du type (iii) dans la proposition 9 :

Proposition 11. *Soit $p \equiv 1 \pmod 4$ un premier rationnel positif. Il existe 8 diviseurs premiers de p dans $\mathbb{Z}[i]$, constituant deux classes d'association distinctes.*

Démonstration. Comme $p \equiv 1 \pmod 4$, le théorème des deux carrés montre que $p = a^2 + b^2 = \mathrm{N}(\pi) = \pi\overline{\pi}$, où $\pi = a + bi \in \mathbb{Z}[i]$. Les quatre associés de π et les quatre associés de $\overline{\pi}$ sont des diviseurs de p. Montrons que π et $\overline{\pi}$ ne sont pas associés. Comme

$$\frac{\pi}{\overline{\pi}} = \frac{a + bi}{a - bi} = \frac{(a + bi)^2}{a^2 + b^2} = \frac{a^2 - b^2}{a^2 + b^2} + i\frac{2ab}{a^2 + b^2},$$

$\frac{\pi}{\overline{\pi}} \in \{1, -1, i, -i\}$ entraîne $a^2 - b^2 = 0$ ou $2ab = 0$, donc $a = b$ ou $a = -b$ ou $a = 0$ ou $b = 0$. Aucune de ces éventualités n'est compatible avec l'égalité $p = a^2 + b^2$, où p est premier impair. Ainsi π et $\overline{\pi}$ ne sont pas associés.

De plus, tout diviseur premier $\lambda \in \mathbb{Z}[i]$ de p vérifie $\lambda \mid \pi\overline{\pi}$, donc $\lambda \mid \pi$ ou $\lambda \mid \overline{\pi}$, et alors $\lambda \sim \pi$ ou $\lambda \sim \overline{\pi}$, et ainsi λ est dans l'une des deux classes d'association de π ou $\overline{\pi}$. □

1.4 Sommes de deux carrés : la méthode d'Euler.

Nous allons prouver que tout nombre premier de la forme $4k + 1$ est somme de deux carrés d'entiers, en suivant les étapes de la première démonstration donnée par Euler, mais en utilisant le langage des entiers de Gauss, ce qui permet de mieux comprendre les idées de cette preuve.

La démonstration se fait traditionnellement, depuis Euler, en deux étapes, nommées réciprocité et descente. La proposition 5 montre que $p \mid a^2 + 1$ pour un certain entier $a \in \mathbb{Z}$. L'étape "réciprocité" est le fait que p divise une somme de deux carrés $x^2 + y^2$, où x, y sont premiers entre eux : il suffit de poser $x = a, y = 1$.

Poursuivons maintenant avec l'étape "descente", en commençant par le lemme suivant, dû à Euler.

Proposition 12. *Soit n un entier positif, et q un diviseur premier de n.*

Si q, n se décomposent en somme de deux carrés, i.e. $n = a^2 + b^2, q = c^2 + d^2$, alors n/q est somme de deux carrés.

Démonstration.

$$\frac{n}{q} = \frac{\mathrm{N}(a+bi)}{\mathrm{N}(c+di)} = \mathrm{N}\left(\frac{a+bi}{c+di}\right) = \mathrm{N}\left(\frac{(a+bi)(c-di)}{c^2+d^2}\right) = \mathrm{N}\left(\frac{ac+bd}{q} + i\frac{bc-ad}{q}\right),$$

donc

$$\frac{n}{q} = \left(\frac{ac+bd}{q}\right)^2 + \left(\frac{bc-ad}{q}\right)^2. \tag{1.1}$$

Rien ne permet d'affirmer que $\frac{ac+bd}{q}, \frac{bc-ad}{q}$ sont des entiers, mais comme $q = \mathrm{N}(c + di) = \mathrm{N}(c - di)$, nous pouvons remplacer d par $-d$, et nous obtenons aussi bien

$$\frac{n}{q} = \left(\frac{ac-bd}{q}\right)^2 + \left(\frac{bc+ad}{q}\right)^2. \tag{1.2}$$

Montrons qu'une des deux formules (1.1) ou (1.2) donne une décomposition de n/q en somme de carrés d'entiers.

Notons $z = a + bi$, et $\pi = c + di$. D'après la proposition 7, π est premier dans $\mathbb{Z}[i]$. De plus $\pi \mid \mathrm{N}(\pi) = q$, et $q \mid n = \mathrm{N}(z) = z\overline{z}$. L'anneau $\mathbb{Z}[i]$ étant principal, ceci entraîne que $\pi \mid z$, ou $\pi \mid \overline{z}$.

Si $\pi \mid z$, alors $q = \pi\overline{\pi} \mid z\overline{\pi} = (ac + bd) + i(bc - ad)$, donc $\frac{ac+bd}{q} + i\frac{bc-ad}{q} \in \mathbb{Z}[i]$, ce qui montre que $q \mid ac + bd$, et $q \mid bc - ad$: la formule (1.1) donne la décomposition de n/q en somme de deux carrés d'entiers.

Si $\pi \mid \overline{z}$, alors $q = \pi\overline{\pi} \mid \overline{z}\overline{\pi} = (ac - bd) - i(bc + ad)$, donc $q \mid ac - bd$, et $q \mid bc + ad$: la formule (1.2) donne la décomposition de n/q en somme de deux carrés d'entiers.

□

Ceci donne la preuve originale du théorème des deux carrés :

soit p un nombre premier impair. Si $p \equiv 1 \pmod 4$, alors il existe un couple $(x, y) \in \mathbb{N}^2$ tel que $p = x^2 + y^2$.

Démonstration. Soit p premier, $p \equiv 1 \pmod 4$. Supposons que tout nombre premier inférieur à p et congru à 1 modulo 4 soit somme de deux carrés d'entiers. Montrons qu'il en va de même pour p.

Nous savons que p divise $a^2 + 1$ pour un certain $a \in \mathbb{Z}$ (proposition 5). Si A est le moindre reste de a modulo p, alors $p \mid A^2 + 1$ et $-p/2 < A < p/2$.

Alors $A^2 + 1 = pK, K \in \mathbb{N}^*$ et $A^2 + 1 < \frac{p^2}{4} + 1$, donc $K < \frac{p}{4} + \frac{1}{p} < \frac{p}{4} + 1 < p$.

Si $K = 1$, $p = A^2 + 1$ est somme de deux carrés. Sinon K se décompose en facteurs premiers sous la forme $K = q_1 q_2 \cdots q_l$ (avec d'éventuelles répétitions).

$$A^2 + 1 = p\, q_1 q_2 \cdots q_l.$$

Ici q_i divise $A^2 + 1$, soit $-1 \equiv A^2 \pmod{q_i}$ donc $\left(\frac{-1}{q_i}\right) = 1$, donc $q_i = 2$ ou $q_i \equiv 1 \pmod 4$, et $q_i \leq K < p$. On peut donc appliquer l'hypothèse de récurrence à chaque q_i : $q_i = a_i^2 + b_i^2$ (et aussi $2 = 1^2 + 1^2$).

Nous allons diviser cette égalité successivement par chacun des q_i.

Faisons l'hypothèse suivante (pour $1 \leq m \leq l$) : supposons qu'il existe un couple $(a, b) \in \mathbb{Z}^2$ tels que

$$a^2 + b^2 = p\, q_1 q_2 \cdots q_m,$$

où on rappelle que $q_i < p, i = 1, \cdots, m$, et que chaque q_i est somme de carrés d'entiers.

Au départ $l = m, a = A, b = 1$ et l'hypothèse est vérifiée au rang l.

Il existe deux entiers c, d tels que $q_m = c^2 + d^2$.

Si $n = a^2 + b^2$, alors $q_m \mid n$: le lemme précédent (proposition 11) montre que $\frac{n}{q_m}$ est somme de deux carrés d'entiers, ce qui signifie qu'il existe des entiers u, v tels que

$$u^2 + v^2 = p\, q_1 q_2 \cdots q_{m-1}.$$

On prouve ainsi successivement que les nombres $p\, q_1 q_2 \cdots q_m, m = l, l-1, \cdots, 1$ sont sommes de deux carrés. La dernière étape montre que $p = x^2 + y^2$.

□

Exemple : décomposons le premier $p = 11213$ en somme de deux carrés.

Comme la moitié des éléments de $(\mathbb{Z}/11213\mathbb{Z})^*$ vérifie $x^{\frac{p-1}{2}} + 1 = 0$, on trouve rapidement, à l'aide de l'exponentiation rapide, que $\dot{2}^{\frac{p-1}{2}} + 1 = 0$, et $\dot{2}^{\frac{p-1}{4}} = 1505$, donc $p = 11213 \mid 1505^2 + 1 = n$.

$n = 2265026 = 202 \times 11213 = 2 \times 101 \times 11213$,

et $2 = 1^2 + 1^2, 101 = 10^2 + 1^2$.

$$2 \times 11213 = \frac{n}{101} = \mathrm{N}\left(\frac{1505 + i}{10 + i}\right) = \mathrm{N}\left(\frac{15051}{101} + i\frac{1495}{101}\right),$$

et aussi

$$2 \times 11213 = \frac{n}{101} = \mathrm{N}\left(\frac{1505 + i}{10 - i}\right) = \mathrm{N}\left(\frac{15049}{101} + i\frac{1515}{101}\right).$$

Seule la deuxième décomposition donne des entiers

$$2 \times 11213 = \mathrm{N}(149 + 15i) = 149^2 + 15^2,$$

et enfin

$$11213 = \mathrm{N}\left(\frac{149 + 15i}{1 + i}\right) = \mathrm{N}(82 + 67i),$$

$$11213 = 82^2 + 67^2.$$

Remarque : cette démonstration suis les étapes de la première démonstration due à Euler, en utilisant les nombres complexes, ce qu'Euler voulait éviter en donnant une démonstration élémentaire. Cette preuve étant constructive, elle permet d'obtenir des décompositions effectives. Néanmoins elle n'est pas la plus rapide sur le plan algorithmique, puisqu'elle nécessite une factorisation en facteurs premiers, qui peut être très gourmande en temps de calcul. La variante de descente donnée dans le paragraphe suivant évite cet écueil.

1.5 Autre preuve et algorithme pour la décomposition en somme de deux carrés.

Cet autre démonstration-algorithme vient de [Lehman].
Cette proposition donne une variante de la descente donnée par Euler.

Proposition 13. *Soit $p \in \mathbb{N}$ un nombre premier impair. Supposons que l'entier k soit tel qu'il existe des entiers a, b vérifiant*

$$kp = a^2 + b^2, \qquad 1 < k < p.$$

Alors il existe un entier l, où $1 \leq l \leq \frac{k}{2} < k$, et des entiers c, d tels que $lp = c^2 + d^2$.

Démonstration. Partons de l'hypothèse $kp = a^2 + b^2$, avec $1 < k < p$. Soient m, n les moindres restes de a, b modulo k :

$$m \equiv a \pmod{k}, \quad n \equiv b \pmod{k}, \qquad -\frac{k}{2} \leq m < \frac{k}{2}, \quad -\frac{k}{2} \leq n < \frac{k}{2}.$$

Notons que m, n ne sont pas tous deux nuls. Sinon $k \mid a, k \mid b$, donc $k^2 \mid a^2 + b^2 = kp$, ce qui entraîne que $k \mid p$, en contradiction avec les hypothèses p premier et $1 < k < p$.

De plus $m^2 + n^2 \equiv a^2 + b^2 \equiv 0 \pmod{k}$, et ainsi $k \mid m^2 + n^2$. Il existe donc un entier l tel que $m^2 + n^2 = kl$. Puisque m, n ne sont pas tous deux nuls, $l \geq 1$. Comme $|m| \leq \frac{k}{2}$ et $|n| \leq \frac{k}{2}$, on obtient $kl = m^2 + n^2 \leq \frac{k^2}{4} + \frac{k^2}{4} = \frac{k^2}{2}$, donc $1 \leq l \leq \frac{k}{2} < k$.

La division des deux égalités

$$kp = a^2 + b^2 = \mathrm{N}(a + bi),$$
$$kl = m^2 + n^2 = \mathrm{N}(m + ni),$$

donne

$$\begin{aligned}\frac{p}{l} &= \mathrm{N}\left(\frac{a+bi}{m+ni}\right)\\ &= \mathrm{N}\left(\frac{(a+bi)(m-ni)}{m^2+n^2}\right)\\ &= \mathrm{N}\left(\frac{(a+bi)(m-ni)}{kl}\right)\\ &= \frac{1}{l^2}\left[\left(\frac{am+bn}{k}\right)^2+\left(\frac{bm-an}{k}\right)^2\right],\end{aligned}$$

donc

$$lp = \left(\frac{am+bn}{k}\right)^2+\left(\frac{bm-an}{k}\right)^2.$$

Puisque $m \equiv a \pmod{k}, n \equiv b \pmod{k}$, nous obtenons

$$\begin{aligned}am+bn \equiv a^2+b^2 \equiv 0 \pmod{k},\\ bm-an \equiv ba-ab \equiv 0 \pmod{k},\end{aligned}$$

donc $c = \frac{am+bn}{k}$ et $d = \frac{bm-an}{k}$ sont des entiers, et ils vérifient

$$lp = c^2+d^2, \text{ où } 1 \leq l < \frac{k}{2} < k.$$

□

Ceci donne une nouvelle preuve du théorème des deux carrés :

Soit $p \in \mathbb{N}$ un entier premier tel que $p \equiv 1 \pmod{4}$, alors $p = a^2+b^2$ est somme de deux carrés d'entiers.

Démonstration. Comme $p \equiv 1 \pmod{4}$, la proposition 5 donne l'existence d'un entier a tel que $p \mid a^2+1$. Si b est le moindre reste de a dans la division par p, alors $b \equiv a \pmod{p}$ et $-\frac{p}{2} < b < \frac{p}{2}$. Alors $p \mid b^2+1$, avec $|b| < \frac{p}{2}$. Quitte à remplacer b par $-b$, on peut supposer $b > 0$. Ainsi il existe un entier k tel que

$$kp = b^2+1,$$

et puisque $0 < b < \frac{p}{2}$, $kp < \frac{p^2}{4}+1$, donc $k < \frac{p}{4}+\frac{1}{p} < \frac{p}{4}+1 < p$.

Si $k = 1$, $p = b^2+1$ est somme de deux carrés. Sinon, $kp = b^2+1,\ 1 < k < p$, et ainsi l'hypothèse de la proposition 12 est vérifiée.

La proposition 12 donne alors un entier k_1 tel que $1 \leq k_1 < k$ tel que $k_1 p$ est somme de deux carrés. Si $k_1 = 1$, p est some de deux carrés. Sinon on continue. On construit ainsi une suite strictement décroissante $k_1 > k_2 > \cdots > k_n > \cdots$ d'entiers, tant qu'aucun terme de cette suite n'est égal à 1, et vérifiant tous $k_n p = a_n^2+b_n^2$ pour des entiers a_n, b_n. Comme il n'existe pas de suite infinie strictement décroissante d'entiers naturels, cette suite est nécessairement finie : il existe un indice t tel que $k_t = 1$, et donc p est somme de deux carrés.

□

L'algorithme correspondant ne demande pas de factorisations, et il est efficace. En effet la proposition 13 montre que $k_{n+1} < \frac{k_n}{2}$. On atteint donc $k_t = 1$ en un temps $t = O(\log(n))$. Le programme correspondant à cet algorithme est donné dans l'appendice à ce chapitre.

Une autre preuve du théorème des deux carrés sera donnée dans un chapitre ultérieur par la méthode de Lagrange pour obtenir une forme réduite, une avec les sommes de Jacobi, et une autre encore dans le chapitre sur la géométrie des nombres.

1.6 Représentation d'un nombre premier par la forme $x^2 + 2y^2$.

Le nombre 2 se décompose sous la forme $2 = 0^2 + 2 \times 1^2$.

Maintenant, soit p un nombre premier impair. A quelle condition peut-il se décomposer sous la forme $p = x^2 + 2y^2$? Donnons d'abord une condition nécessaire :

Si $p = x^2 + 2y^2$, alors $p \nmid y$, sinon $p \mid y, p \mid x$, donc $p^2 \mid x^2 + 2y^2 = p$, et $p \mid 1$: c'est absurde. Par conséquent la classe $\dot{y}$ de y est non nulle dans $\mathbb{Z}/p\mathbb{Z}$, et $-2 = (\dot{x}\dot{y}^{-1})^2$, donc $\left(\frac{-2}{p}\right) = 1$. Ceci équivaut d'après les caractères quadratique de -1 et 2 à

$$(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{p-1}{2}}.$$

Résumons le tableau de ces valeurs pour chaque valeur de p modulo 8 :

p	1	3	5	7
$(-1)^{\frac{p-1}{2}}$	1	−1	1	−1
$(-1)^{\frac{p^2-1}{8}}$	1	−1	−1	1

Donc

$$\left(\frac{-2}{p}\right) = 1 \iff p \equiv 1, 3 \pmod 8.$$

Montrons que cette condition est suffisante

Proposition 14. *Soit p un nombre premier impair . Alors*

$$\exists x \in \mathbb{Z},\ \exists y \in \mathbb{Z},\ p = x^2 + 2y^2 \iff p \equiv 1 \text{ or } p \equiv 3 \pmod 8.$$

Démonstration. Il reste à prouver que la condition est suffisante. Supposons que $p \equiv 1, 3 \pmod 8$. Le calcul précédent montre que $\left(\frac{-2}{p}\right) = 1$, donc il existe un entier a tel que $p \mid a^2 + 2$.

L'anneau $\mathbb{Z}[i\sqrt{2}]$ étant principal (proposition 2), nous pouvons calquer la preuve de la proposition 6.

Notons $\rho = i\sqrt{2}$. Soit I l'idéal de $\mathbb{Z}[\rho]$ défini par

$$I = p\mathbb{Z}[\rho] + (a + \rho)\mathbb{Z}[i] = \langle p, a + \rho \rangle.$$

Montrons que $I \neq \mathbb{Z}[\rho]$, en prouvant que l'hypothèse $I = \mathbb{Z}[\rho]$ est absurde.

Soit λ un diviseur premier de p dans $\mathbb{Z}[\rho]$: un tel diviseur existe puisque $\mathbb{Z}[\rho]$ est principal.

Alors $\lambda \mid p$, et $p \mid a^2 + 2 = (a + \rho)(a - \rho)$, donc $\lambda \mid (a + \rho)(a - \rho)$. L'élément λ étant premier, il divise soit $a + \rho$, soit $a - \rho$.

Dans la premier cas, λ divise p et $a+\rho$. Dans le deuxième cas, si $\lambda \mid a-\rho$, alors $a-\rho = \lambda\mu$, donc $a+\rho = \overline{\lambda}\overline{\mu}$, où $\overline{\mu} \in \mathbb{Z}[\rho]$, donc $\overline{\lambda} \mid a+\rho$. De plus $\overline{\lambda} \mid p$: en effet $p = \lambda\nu$ pour un certain $\nu \in \mathbb{Z}[\rho]$, donc $p = \overline{\lambda}\overline{\nu}$. Notons que $\mathrm{N}(\lambda) = \mathrm{N}(\overline{\lambda}) > 1$.

Dans les deux cas, il existe $\xi \in \mathbb{Z}[\rho]$ (où $\xi = \lambda$ ou $\xi = \overline{\lambda}$) tel que $\xi \mid p, \xi \mid a+\rho$, et $\mathrm{N}(\xi) > 1$.

Sous l'hypothèse $I = \mathbb{Z}[\rho]$, alors $1 = p\zeta + (a+\rho)\eta$, où ζ, η sont dans $\mathbb{Z}[\rho]$. Alors $\xi \mid 1$, en contradiction avec $\mathrm{N}(\xi) > 1$, ce qui prouve que $I \neq \mathbb{Z}[\rho]$.

Comme $\mathbb{Z}[\rho]$ est principal, il existe $\pi \in \mathbb{Z}[\rho]$ tel que

$$p\mathbb{Z}[\rho] + (a+\rho)\mathbb{Z}[\rho] = \pi\mathbb{Z}[\rho].$$

De plus π n'est pas une unité, sinon $I = \pi\mathbb{Z}[\rho] = \mathbb{Z}[\rho]$. Par conséquent $\mathrm{N}(\pi) > 1$. Nous venons de prouver l'existence d'un pgcd non trivial π de p et $a+\rho$.

Comme $p = p \times 1 + (a+\rho) \times 0 \in p\mathbb{Z}[\rho] + (a+\rho)\mathbb{Z}[\rho] = \pi\mathbb{Z}[\rho]$, il existe $\gamma \in \mathbb{Z}[\rho]$ tel que $p = \pi\gamma$, et donc $p^2 = \mathrm{N}(\pi)\mathrm{N}(\gamma)$.

Si $\mathrm{N}(\gamma) = 1$, alors γ est une unité, donc p et π sont associés, et π divise $a+\rho$, donc p divise $a+\rho$, ce qui est absurde puisque $\frac{a}{p} + \frac{1}{p}\rho \notin \mathbb{Z}[\rho]$. Ainsi $\mathrm{N}(\gamma) > 1$.

L'égalité $p^2 = \mathrm{N}(\pi)\mathrm{N}(\gamma)$, où $\mathrm{N}(\pi) > 1, \mathrm{N}(\gamma) > 1$, montre que

$$p = \mathrm{N}(\pi).$$

Si $\pi = x + i\sqrt{2}y,\ x, y \in \mathbb{Z}$, alors $p = x^2 + 2y^2$, ce qui prouve le théorème. □

1.7 L'anneau $\mathbb{Z}[\omega]$.

Soit $\omega = e^{2i\pi/3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Alors $\omega^2 + \omega + 1 = 1, \omega^3 = 1$ et $\overline{\omega} = \omega^2 = -1 - \omega$.

Notons $\mathbb{Z}[\omega]$ l'ensemble des nombres complexes de la forme $a + b\omega$:

$$A = \{z \in \mathbb{C} \mid \exists a \in \mathbb{Z},\ \exists b \in \mathbb{Z},\ z = a + b\omega\}.$$

A est le plus petit sous-anneau de $\mathbb{C}$ qui contient $\mathbb{Z}$ et ω.

Si $z = a + b\omega \in \mathbb{Z}[\omega]$, alors $\mathrm{N}(z) = (a+b\omega)(a+b\omega^2) = a^2 - ab + b^2$.

Notons que $\mathbb{Z}[\omega]$ est stable par conjugaison :

$$\overline{z} = a + b\omega^2 = a + b(-1-\omega) = (a-b) - b\omega \in \mathbb{Z}[\omega].$$

Montrons que cet anneau est euclidien, pour la norme usuelle des nombres complexes.

Proposition 15. *Si $z \in \mathbb{C}$, il existe $z_0 \in \mathbb{Z}[\omega]$ tel que $\mathrm{N}(z - z_0) < 1$.*

Démonstration. Soit $z = a + b\omega \in \mathbb{Z}[\omega]$. Il existe des entiers a_0, b_0 tels que

$$|a - a_0| < \frac{1}{2}, \quad |b - b_0| < \frac{1}{2}.$$

Alors

$$\begin{aligned}
\mathrm{N}(z - z_0) &= \mathrm{N}[(a-a_0) + \omega(b-b_0)] \\
&= (a-a_0)^2 - (a-a_0)(b-b_0) + (b-b_0)^2 \\
&\leq |a-a_0|^2 + |a-a_0||b-b_0| + |b-b_0|^2 \\
&\leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{3}{4}
\end{aligned}$$

□

Proposition 16. *$\mathbb{Z}[\omega]$ est un anneau euclidien pour la norme $\mathrm{N}(\cdot)$ de $\mathbb{C}$.*

Même preuve que celle de la proposition 2 :

Démonstration. Si $a, b \in \mathbb{Z}[\omega]$, et $b \neq 0$, il existe d'après la proposition précédente $q \in \mathbb{Z}[\omega]$ tel que $\left|\frac{a}{b} - q\right| < 1$. Posons alors $r = a - bq = b\left(\frac{a}{b} - q\right)$. Alors $r \in \mathbb{Z}[\omega]$, et

$$a = bq + r, \quad 0 \leq \mathrm{N}(r) < \mathrm{N}(b).$$

Il existe donc une division euclidienne dans $\mathbb{Z}[\omega]$. □

Précisons les unités de $\mathbb{Z}[\omega]$.

Proposition 17. *Pour tout $z \in \mathbb{Z}[\omega]$,*

$$z \in \mathbb{Z}[\omega]^\times \iff \mathrm{N}(z) = 1.$$

(Même démonstration que celle de la proposition 3, en utilisant le fait que $\mathbb{Z}[\omega]$ est stable par conjugaison.)

Proposition 18.

$$\mathbb{Z}[\omega]^\times = \{1, \omega, \omega^2, -1, -\omega, -\omega^2\} = \mathbb{U}_6.$$

Démonstration. Soit $\alpha = a+b\omega$ une unité dans $\mathbb{Z}[\omega]$. Alors $\mathrm{N}(\omega) = 1$, soit $a^2-ab+b^2 = 1$. Donc $4 = 4a^2 - 4ab + 4b^2 = (2a - b)^2 + 3b^2$. Ceci implique $3b^2 \leq 4$, donc $|b| \leq 1$. Ceci donne deux cas :

- $b = 0, 2a - b = \pm 2$.
- $b = \pm 1, 2a - b = \pm 1$,

Alors $(a, b) \in \{(1, 0), (-1, 0), (1, 1), (0, 1), (0, -1), (-1, -1)\}$, donc

$$z = a + b\omega \in \{1, -1, 1 + \omega, \omega, -\omega, -1 - \omega\}.$$

Puisque $1 + \omega = -\omega^2$, on obtient bien

$$z \in \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}.$$

Réciproquement, ces 6 éléments sont de norme 1, donc sont des unités. Ils constituent le groupe des racines 6-ième de l'unité dans $\mathbb{C}$, engendré par $1 + \omega = -\omega^2 = e^{i\pi/3}$. □

1.8 Représentation des nombres premiers sous la forme $x^2 + 3y^2$.

Sachant que $\mathbb{Z}[\omega]$ est principal, donnons maintenant la représentation d'un nombre premier sous la forme $x^2 + 3y^2$.

Le nombre 3 se décompose sous la forme $3 = 0^2 + 3 \times 1^2$. Prenons maintenant un autre nombre premier.

Proposition 19. *Soit p un nombre premier différent de 3. Alors*

$$\exists x \in \mathbb{Z},\ \exists y \in \mathbb{Z},\ p = x^2 + 3y^2 \iff p \equiv 1 \pmod 3.$$

Démonstration. ($\Rightarrow$) Si $p \neq 3$ vérifie $p = x^2 + 3y^2,\ x, y \in \mathbb{Z}$, alors $p \equiv x^2 \pmod 3$, et $p \nmid x$ (sinon $p \mid x$, donc $p \mid y,\ p^2 \mid x^2 + 3y^2 = p$: c'est absurde). Par conséquent $p \equiv 1 \pmod 3$.

($\Leftarrow$) Notons que, pour tout premier impair différent de 3,

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{3-1}{2}\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Par conséquent,

$$\left(\frac{-3}{p}\right) = 1 \iff \left(\frac{p}{3}\right) = 1 \iff p \equiv 1 \pmod 3.$$

Si $p \equiv 1 \pmod 3$, l'équivalence précédente montre que $\left(\frac{-3}{p}\right) = 1$, donc il existe un entier a tel que $p \mid a^2 + 3$.

Comme $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, alors $i\sqrt{3} = 1 + 2\omega$, donc

$$a^2 + 3 = (a + i\sqrt{3})(a - i\sqrt{3}) = (a + 1 + 2\omega)(a + 1 + 2\omega^2).$$

Reprenons le schéma de démonstration de la proposition 14. Soit I l'idéal de $\mathbb{Z}[\omega]$ défini par

$$I = p\mathbb{Z}[\omega] + (a + 1 + 2\omega)\mathbb{Z}[\omega] = \langle p, a + 1 + 2\omega\rangle.$$

Montrons que $I \neq \mathbb{Z}[\omega]$, en prouvant que l'hypothèse $I = \mathbb{Z}[\omega]$ est absurde.

Soit λ un diviseur premier de p dans $\mathbb{Z}[\omega]$: un tel diviseur existe puisque $\mathbb{Z}[\omega]$ est principal.

Alors $\lambda \mid p$, et $p \mid a^2+3 = (a+1+2\omega)(a+1+2\omega^2)$, donc $\lambda \mid (a+1+2\omega)(a+1+2\omega^2)$. L'élément λ étant premier, il divise soit $a + 1 + 2\omega$, soit $a + 1 + 2\omega^2$.

Dans la premier cas, λ divise p et $a+1+2\omega$. Dans le deuxième cas, si $\lambda \mid a+1+2\omega^2$, alors $a + 1 + 2\omega^2 = \lambda\mu$. Par passage aux conjugués, $a + 1 + 2\omega = \overline{\lambda}\overline{\mu}$, où $\overline{\mu} \in \mathbb{Z}[\omega]$, donc $\overline{\lambda} \mid a + 1 + 2\omega$. De plus $\overline{\lambda} \mid p$: en effet $p = \lambda\nu$ pour un certain $\nu \in \mathbb{Z}[\omega]$, donc $p = \overline{\lambda}\overline{\nu}$. Notons que $\mathrm{N}(\lambda) = \mathrm{N}(\overline{\lambda}) > 1$.

Dans les deux cas, il existe $\xi \in \mathbb{Z}[\omega]$ (où $\xi = \lambda$ ou $\xi = \overline{\lambda}$) tel que $\xi \mid p, \xi \mid a+1+2\omega$, et $\mathrm{N}(\xi) > 1$.

Sous l'hypothèse $I = \mathbb{Z}[\omega]$, alors $1 = p\zeta + (a + 1 + 2\omega)\eta$, où ζ, η sont dans $\mathbb{Z}[\omega]$. Alors $\xi \mid 1$, en contradiction avec $\mathrm{N}(\xi) > 1$, ce qui prouve que $I \neq \mathbb{Z}[\omega]$.

Comme $\mathbb{Z}[\omega]$ est principal, il existe $\pi \in \mathbb{Z}[\omega]$ tel que

$$p\mathbb{Z}[\omega] + (a + 1 + 2\omega)\mathbb{Z}[\omega] = \pi\mathbb{Z}[\omega].$$

De plus π n'est pas une unité, sinon $\pi\mathbb{Z}[\omega] = \mathbb{Z}[\omega]$. Par conséquent $\mathrm{N}(\pi) > 1$. Nous venons de prouver l'existence d'un pgcd non trivial π de p et $a + 1 + 2\omega$.

Comme $p \in p\mathbb{Z}[\omega] + (a + 1 + 2\omega)\mathbb{Z}[\omega] = \pi\mathbb{Z}[\omega]$, il existe $\gamma \in \mathbb{Z}[\omega]$ tel que $p = \pi\gamma$, et donc $p^2 = \mathrm{N}(\pi)\mathrm{N}(\gamma)$.

Si $\mathrm{N}(\gamma) = 1$, alors γ est une unité, donc p et π sont associés, et π divise $a+1+2\omega$, donc p divise $a + 1 + 2\omega$, ce qui est absurde puisque $\frac{a+1}{p} + \frac{2}{p}\omega \notin \mathbb{Z}[\omega]$. Ainsi $\mathrm{N}(\gamma) > 1$.

L'égalité $p^2 = \mathrm{N}(\pi)\mathrm{N}(\gamma)$, où $\mathrm{N}(\pi) > 1, \mathrm{N}(\gamma) > 1$, montre que

$$p = \mathrm{N}(\pi).$$

Si $\pi = x + \omega y,\ x, y \in \mathbb{Z}$, alors $p = \mathrm{N}(\pi) = \mathrm{N}(\omega\pi)$, où

$$\pi = x + \omega y, \qquad \omega\pi = -y + (x - y)\omega.$$

La formule $p = \mathrm{N}(\pi)$ donne $p = x^2 - xy + y^2$, soit $4p = 4x^2 - 4xy + 4y^2 = (2x-y)^2 + 3y^2$.
La substitution $(x, y) \leftarrow (-y, x-y)$ donne $4p = (-2y - x + y)^2 + 3(x-y)^2 = (x+y)^2 + 3(x-y)^2$.
Comme $\mathrm{N}(x + \omega y) = x^2 - xy + y^2 = \mathrm{N}(y + \omega x)$, on peut échanger x et y.
En résumé, on obtient les trois formules équivalentes suivantes :

$$\begin{aligned} 4p &= (2x-y)^2 + 3y^2, \\ 4p &= (2y-x)^2 + 3x^2, \\ 4p &= (x+y)^2 + 3(x-y)^2. \end{aligned}$$

Si x impair et y pair, alors $p = \left(x - \frac{y}{2}\right)^2 + 3\left(\frac{y}{2}\right)^2$.
Si x pair et y impair, alors $p = \left(y - \frac{x}{2}\right)^2 + 3\left(\frac{x}{2}\right)^2$.
Si x, y sont de même parité, alors $p = \left(\frac{x+y}{2}\right)^2 + 3\left(\frac{x-y}{2}\right)^2$.
Dans les trois cas, p est de la forme $a^2 + 3b^2$, où a, b sont entiers.

□

1.9 Eléments premiers dans $\mathbb{Z}[\omega]$.

Les deux propositions suivantes se démontrent comme dans $\mathbb{Z}[i]$ à la section 1.1.

Proposition 20. *Soit $\pi \in \mathbb{Z}[\omega]$. Si $\mathrm{N}(\pi)$ est premier dans $\mathbb{Z}$, alors π est premier dans $\mathbb{Z}[\omega]$.*

Proposition 21. *Soit π un élément premier dans $\mathbb{Z}[\omega]$. Alors il existe un unique entier rationnel premier $p \in \mathbb{N}$ tel que $\pi \mid p$.*

Donnons d'abord une liste d'éléments premiers dans $\mathbb{Z}[\omega]$:

- Comme $x^2 + x + 1 = (x-\omega)(x-\omega^2)$, $\mathrm{N}(1-\omega) = (1-\omega)(1-\omega^2) = 3$ est premier dans $\mathbb{Z}$, donc $1-\omega$ est premier dans $\mathbb{Z}[i]$, ainsi que ses 6 associés $1-\omega, 1+2\omega, -2-\omega, -1+\omega, -1-2\omega, 2+\omega$.
- Soit $q \equiv 2 \pmod 3$ un premier rationnel, $q > 0$. Montrons que q est premier dans $\mathbb{Z}[\omega]$. Dans le cas contraire, $q = \alpha\beta$, où $\alpha, \beta \in \mathbb{Z}[\omega]$ vérifient $\mathrm{N}(\alpha) > 1, \mathrm{N}(\beta) > 1$. Alors $q^2 = \mathrm{N}(\alpha)\mathrm{N}(\beta)$, donc $\mathrm{N}(\alpha) = q$. Si $\alpha = a + b\omega$, alors $q = a^2 - ab + b^2$, donc $4q = (2a-b)^2 + 3b^2$, et ainsi $q \equiv (2a-b)^2 \not\equiv -1 \pmod 3$. Cette contradiction montre que q est premier dans $\mathbb{Z}[\omega]$ (ainsi que ses associés $\pm q, \pm\omega q, \pm\omega^2 q$).
- Soit $\pi = a + b\omega \in \mathbb{Z}[\omega]$ tel que $p = \mathrm{N}(\pi) = a^2 - ab + b^2$ est premier dans $\mathbb{Z}$ (donc $4p = (2a-b)^2 + 3b^2$, ce qui montre que $p \equiv 1 \pmod 3$). Alors π est premier dans $\mathbb{Z}[\omega]$ puisque $\mathrm{N}(\pi)$ est premier dans $\mathbb{Z}$.

Ces éléments seront appelés les éléments premiers connus dans $\mathbb{Z}[\omega]$. Montrons que cette liste est exhaustive.

Proposition 22. *Les éléments premiers dans $\mathbb{Z}[\omega]$ sont*

(i) $1 - \omega$ *et ses associés,*

(ii) les entiers rationnels $q \equiv 2 \pmod 3, q > 0$, premiers dans $\mathbb{Z}$, ainsi que leurs associés,

(iii) les éléments $\pi = a + b\omega$ *tels que* $p = \pi\overline{\pi} = a^2 - ab + b^2 \equiv 1 \pmod 3$ *soit premier dans* $\mathbb{Z}$.

Démonstration. Soit $\pi = a+b\omega$ un élément premier dans $\mathbb{Z}[\omega]$. La proposition 21 montre qu'il existe un premier rationnel $p \in \mathbb{N}$ tel que $\pi \mid p$. Discutons les trois seuls cas possibles, $p = 3$, $p \equiv 2 \pmod 3$, et $p \equiv 1 \pmod 3$.

(i) Supposons que $\pi \mid 3$. Comme $3 = (1-\omega)(1-\omega^2) = (1+\omega)(1-\omega)^2 = -\omega^2(1-\omega)^2$, où $1-\omega$ est premier, et $-\omega^2$ est une unité, alors π est associé à $1-\omega$.

(ii) Supposons que $\pi \mid p$, où $p \equiv 2 \pmod 3$. Comme p est un élément premier connu, π est associé à p.

(iii) Supposons que $\pi = a + b\omega \mid p$, où $p \equiv 1 \pmod 4$. Alors $p = \pi\lambda$ pour un certain $\lambda \in \mathbb{Z}[\omega]$. Montrons par l'absurde que p n'est pas premier dans $\mathbb{Z}[\omega]$. Comme vu dans la section 1.8, $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 1$, donc il existe un entier a tel que $p \mid a^2 + 3$.

Alors $p \mid a^2 + 3 = (a + 1 + 2\omega)(a + 1 + 2\omega^2)$. Ici p est supposé premier, donc $p \mid a+1+2\omega$, ou $p \mid a+1+2\omega^2$, en contradiction avec le fait que $\frac{a+1}{p} + \frac{2}{p}\omega \notin \mathbb{Z}[\omega]$ (ni son conjugué, puisque $\mathbb{Z}[\omega]$ est stable par conjugaison).

Ainsi p n'est pas premier, donc λ n'est pas une unité. Par conséquent $p = \pi\lambda,$, où $\mathrm{N}(\pi) > 1, \mathrm{N}(\lambda) > 1$. L'égalité $p^2 = \mathrm{N}(\pi)(\mathrm{N}(\lambda)$ montre que $p = \mathrm{N}(\pi) = \pi\overline{\pi} = a^2 - ab + b^2$.

Remarque : si p est un premier rationnel tel que $p \equiv 1 \pmod 3$, il admet un diviseur premier $\pi = a + b\omega \in \mathbb{Z}[\omega]$, et le (iii) prouve que $p = a^2 - ab + b^2$. D'après la fin du raisonnement de la section 1.8, ceci montre que p est de la forme $x^2 + 3y^2$, ce qui donne une nouvelle preuve de la proposition 19. □

Nous pouvons donner l'analogue de la proposition 11 dans $\mathbb{Z}[\omega]$:

Proposition 23. *Soit* $p \equiv 1 \pmod 3$ *un premier rationnel. Il existe 12 diviseurs premiers de* p *dans* $\mathbb{Z}[\omega]$*, constituant deux classes d'association distinctes.*

Démonstration. Comme $p \equiv 1 \pmod 3$, la remarque précédente montre que $p = \pi\overline{\pi} = a^2 - ab + b^2$, où $\pi = a + b\omega \in \mathbb{Z}[\omega]$. Comme

$$\frac{\pi}{\overline{\pi}} = \frac{a + b\omega}{a + b\omega^2} = \frac{(a + b\omega)^2}{\mathrm{N}(\pi)} = \frac{a^2 - b^2}{\mathrm{N}(\pi)} + \frac{(2a - b)b}{\mathrm{N}(\pi)}\omega,$$

alors $\frac{\pi}{\overline{\pi}} \in \{1, -1, \omega, -\omega, -1 - \omega, 1 + \omega\}$ entraîne $a^2 - b^2 = 0$ ou $(2a - b)b = 0$ ou $a^2 - b^2 = (2a - b)b$, soit $a = b$ ou $a = -b$ ou $2a - b = 0$ ou $b = 0$ ou $a = 0$ ou $2b - a = 0$. L'égalité $p = a^2 - ab + b^2$, où p est un premier différent de 3, montre que $a = \pm b$ est impossible, ainsi que $a = 0$ ou $b = 0$. L'égalité $4p = (2a-b)^2 + 3b^2$ montre que $2a - b = 0$ est impossible, et l'égalité $4p = (2b - a)^2 + 3a^2$ montre que $2b - a = 0$ est impossible. Ceci montre que π n'est pas associé à $\overline{\pi}$.

Le reste de la démonstration se fait comme dans la proposition 11. □

1.10 La forme $x^2 + ny^2$ si $n > 3$.

Nous savons que si $p \equiv 1 \pmod 4$, alors $p = x^2 + y^2$. Alors x et y sont de parité distinctes, sinon p serait pair, donc $p = 2$, mais $2 \not\equiv 1 \pmod 4$. Quitte à échanger x, y, on peut supposer que x est impair et y pair. Donc $y = 2z, z \in \mathbb{Z}$, et donc $p = x^2 + 4z^2$. Inversement, puisque 2 ne s'exprime pas sous la forme x^2+4z^2, si $p = x^2+4z^2 = x^2+(2z)^2$, alors $p \equiv 1 \pmod 4$.

A ce stade, nous avons prouvé les équivalence suivantes :
si p est un nombre premier ($p \neq 2, p \neq 3$) alors

$$p = x^2 + y^2,\ x, y \in \mathbb{Z} \iff p \equiv 1 \pmod 4 \iff \left(\frac{-1}{p}\right) = 1$$

$$p = x^2 + 2y^2,\ x, y \in \mathbb{Z} \iff p \equiv 1, 3 \pmod 8 \iff \left(\frac{-2}{p}\right) = 1$$

$$p = x^2 + 3y^2,\ x, y \in \mathbb{Z} \iff p \equiv 1 \pmod 3 \iff \left(\frac{-3}{p}\right) = 1$$

$$p = x^2 + 4y^2,\ x, y \in \mathbb{Z} \iff p \equiv 1 \pmod 4 \iff \left(\frac{-4}{p}\right) = 1$$

Si on voulait généraliser, on peut bien sûr affirmer que

$$p = x^2 + ny^2 \Rightarrow \left(\frac{-n}{p}\right) = 1,$$

mais l'équivalence est fausse dès $n = 5$. En effet $\left(\frac{-5}{p}\right) = 1 \iff p \equiv 1, 3, 7, 9 \pmod{20}$, mais, comme l'ont remarqué Fermat et Euler, $p = x^2 + 5y^2,\ x, y \in \mathbb{Z}$ équivaut à $p = 1, 9 \pmod{20}$, et $2p = x^2 + 5y^2$ équivaut à $p \equiv 3, 7 \pmod{20}$. Par exemple 23 ne s'écrit pas sous la forme $x^2 + 5y^2$, mais $2 \times 23 = 46 = 1^2 + 5 \times 3^2$.

Les démonstrations précédentes ne peuvent se généraliser, car $\mathbb{Z}[\sqrt{-5}]$ n'est pas principal. Si $\omega = i\sqrt{5}$, alors $6 = 2 \times 3 = (1 + \omega)(1 - \omega)$. On vérifie au chapitre "Entiers d'un corps quadratique", que $2, 3 = 1 + \omega, 1 - \omega$ sont des éléments premiers non associés. Cette égalité montre donc que $\mathbb{Z}[\sqrt{-5}]$ n'est pas factoriel, et a fortiori il n'est pas principal. Les chapitres suivants nous permettrons de traiter ce cas.

APPENDICE AU CHAPITRE 1.

1.11 Récréation informatique.

Nous choisissons dans ces récréations de présenter les algorithmes étudiés précédemment sous la forme de programme Python (ou Sage). Il sera possible de télécharger ces programmes sur le site

`https://github.com/RichardGanaye`

1.11.1 Quelques procédures arithmétique générales.

Donnons d'abord le module "numtheory" présentant les procédures usuelles de théorie des nombres.

La fonction **isprime** est un test de primalité probaliliste, avec une certaine probabilité d'erreur.

La fonction **ifactors** est naïve. Elle ne peut fonctionner que pour des petits nombres. Il sera préférable de la remplacer par l'ordre **factor** de Sage pour les grands nombres.

```
"""
    Created on Sat Aug 31 19:21:15 2013
    @author: Richard Ganaye
"""

from random import randint

def powermod(a,n,p):
    """retourne a^n mod p (exponentiation rapide )
       resultat positif
    """
    resu=1
    while n!= 0:
        if n%2 != 0:
            resu = (a*resu) % p
        a = (a*a) % p
        n=n//2
    return resu

def expomod(a,n,p):
    """retourne a^n mod p (exponentiation rapide )
       resultat entre -p/2 et p/2
    """
    resu=1
    while n!= 0:
        if n%2 != 0:
            resu = (a*resu) % p
        a = (a*a) % p
        n=n//2
    if resu>p//2:
        resu -=p
```

```
    return resu

def legendre(a,p):
    """retourne le symbole de Legendre (a/p) si p premier"""
    return expomod(a,(p-1)//2,p)

def jacobi2(n):
    """retourne jacobi(n,2)"""
    r = n%8
    if r==1 or r==7:
        return 1
    else:
        return -1

def jacobi(n,m):
    """retourne le symbole de Jacobi (n/m)"""
    if n==0: return 0
    prod = 1
    while m>1:
        k = 0
        while n%2 == 0:
            k += 1
            n = n//2
        if k%2 == 1:
            prod = prod*jacobi2(m)
        if (n%4 == 3 and m%4 == 3):
            prod = -prod
        num = m%n
        m = n
        n = num
    return prod

def pgcd(a,b):
    a , b = abs(a), abs(b)
    while b != 0:
        a, b = b, a%b
    return a


def isprime(p,k=30):
    """ test de primalite, proba d'erreur < 2^(-k)"""
    if p <= 1: return False
    if p <= 3: return True
    test = True
    while k>0:
        k-=1
        b = randint(2,p-2)
        if pgcd(b,p) !=1:
            test = False
```

```
        else:
            if legendre(b,p) != jacobi(b,p):
                test = False
    return test

def nextprime(n):
    q=n+1
    while not isprime(q):
        q += 1
    return q

def plusPetitFacteur(n):
    """ plus petit facteur premier si n>1"""
    if n==1 or isprime(n):
        return n
    else:
        d = 2
        while n%d != 0:
            d += 1
        return d

def ifactors(n):
    """decomposition en facteurs d'un entier n>1"""
    l=[]
    while n!=1:
        p=plusPetitFacteur(n)
        alpha = 0
        while n%p == 0:
            n //=p
            alpha += 1
        l.append([p,alpha])
    return l

def factorielle(n):
    fact = 1
    while n>1:
        fact *= n
        n -= 1
    return fact


def lucas(p):
    """ retourne True ssi 2**p-1 est premier """
    def S(n,p):
        Mp=2**p-1
        s=4
        i=1
        while i<n:
            s=(s*s - 2) % Mp
```

```
            i+=1
        return s

    if S(p-1,p) == 0:
        return True
    else:
        return False


def bezout(a,b):
    """input  : couple d'entiers (a,b)
        output : triplet (x,y,d),
        (x,y) solution de ax+by =d, d = pgcd(a,b)
    """
    sgn_a = 1 if a >= 0 else -1
    sgn_b = 1 if b >= 0 else -1
    (r0, r1)=(abs(a), abs(b))
    (u0, v0) = (1, 0)
    (u1, v1) = (0, 1)
    while r1 != 0:
        q = r0 // r1
        (r2, u2, v2) = (r0 - q * r1, u0 - q * u1, v0 - q * v1)
        (r0, r1) = (r1, r2)
        (u0, u1) = (u1, u2)
        (v0, v1) = (v1, v2)
    x , y, d  = sgn_a * u0, sgn_b * v0, r0
    if x <= 0: x, y = x + abs(b), y - sgn_b * a
    return x, y, d

def inverse(a,modulo):
    """retourne l'inverse de a mod modulo
    """
    return bezout(a,modulo)[0] % modulo

def racineEntiere(n):
    """input  : entier n positif ou nul
        output : partie entière de la racine de n
    """
    a=n
    b=(n+1)//2
    while b<a:
        a=b
        b=(a*a+n)//(2*a)
    return a

def carre(A):
    """ input : entier naturel A
        output: True ssi A est un carré
    """
```

```
    a=racineEntiere(A)
    if a*a==A:
        return True
    else:
        return False

def convert(n,base=10):
    l=[]
    while n!=0:
        r=n%base
        l.append(r)
        n = n//base
    return l

def primroot(p):
    assert(isprime(p))
    pas_trouve = True
    g = 1
    while pas_trouve:
        g += 1
        l = ifactors(p-1)
        k = 0
        test = True
        while k<len(l) and test:
            q = l[k][0]
            if expomod(g,(p-1)//q, p) == 1:
                test = False
            k += 1
        if test: pas_trouve = False
    return g

def chinois(a1,a2,n1,n2):
    "retourne x tel que x=a1[n1], x=a2[n2]"
    t = bezout(n1,n2)
    (u,v)=(t[0],t[1])
    r = (n2*v*a1 + n1*u*a2) % (n1*n2)
    return (n2*v*a1 + n1*u*a2) % (n1*n2)

def chinoiserie(liste,modules):
    "reste chinois pour des listes"
    liste = liste[:]
    modulos = modules[:]
    lg = len(liste)
    if lg==1:
        return liste[0] % modulos[0]
    else:
        a2 = liste.pop(0)
        n2 = modulos.pop(0)
        prod=1
```

```
        for nombre in modulos:
            prod *= nombre
        z = chinoiserie(liste,modulos)
        return chinois(z,a2,prod,n2)

if __name__ == '__main__':
    print(inverse(217,11213))
```

1.11.2 Méthode d'Euler.

Mettons d'abord en oeuvre l'algorithme correspondant à la descente d'Euler proposé au la section 1.4 "Sommes de deux carrés : la méthode d'Euler". Ce n'est pas la plus efficace puisqu'elle nécessite une factorisation.

```
from numtheory import jacobi, carre, isprime, ifactors, nextprime
from random import randint

def reste_minimal(a,b):
    assert(b > 0)
    r = a % b
    if 2 * r > b:
        r -= b
    return r

def racine_de_moins_un(p):
    """
    input : p premier congru à 1 modulo 4
    output :  k tel que k^2 = -1 mod p
    |k| minimal, k > 0
    """
    assert isprime(p), "p non premier"
    assert p % 4 == 1, "p premier non congru à 1 modulo 4"
    while True:
        a = randint(2, p - 2)
        if jacobi(a, p) == -1:
            break
    b = pow(a, (p - 1) // 4, p)
    k = reste_minimal(b, p)
    return abs(k)

def decomposition(p):
    if p == 2:
        return (1,1)
    k = racine_de_moins_un(p)
    u = (k**2 + 1) // p
    l = ifactors(u)
    li = []
    for p,alpha in l:
        for i in range(alpha):
```

```
            li.append(p)
    if li == []:
        return (k,1)
    a, b = k, 1
    for q in li:
        c,d = decomposition(q)
        if (a*c + b*d) % q == 0:
            a, b = (a*c + b*d) // q, (b*c - a*d) // q
        else: # (a*c - b*d) % q == 0
            a, b = (a*c - b*d) // q, (b*c + a*d) // q
    return (abs(a),abs(b))


if __name__ == "__main__":
    ttest = [13, 101, 10009, 11213,  100049, 1000000009,
             12345678912345678912345679O9, 10**50 + 577]
    for p in ttest:
        a,b = decomposition(p)
        assert p == a**2 + b**2, "erreur test"
        print(p,'=>', a, b)
```

Notons que si on ajoute aux tests le nombre premier $10 * *100 + 949$, le programme ne donne pas de réponse dans des délais raisonnables, ce qui ne sera pas le cas pour les procédures suivantes.

1.11.3 Calcul du pgcd dans $\mathbb{Z}[i]$.

Donnons d'abord le module **Zi** qui construit la classe des entiers de Gauss.

```
class Zi:
    """ classe Zi des entiers de Gauss a + ib"""

    def __init__(self,a = 0,b = 0):
        self.re = int(a)
        self.im = int(b)

    def Re(self):
        return self.re

    def Im(self):
        return self.im

    def couple(self):
        return [self.re, self.im]

    def norme(self):
        return (self.re)**2+(self.im)**2

    def bar(self):
        return Zi(self.re, -self.im)
```

```
    def div(self, n):
        return Zi(self.re // n, self.im // n)

    def __repr__(self):
        if self.im>0:
            return f"{self.re} + {self.im} i"
        if self.im<0:
            return f"{self.re} - {abs(self.im)} i"
        if self.im == 0:
            return f"{self.re}"

    def __eq__(self, other):
        if isinstance(other,int):
            return self.im == 0 and self.re == other
        return self.re == other.re and self.im == other.im

    def __hash__(self):
        return (11 * self.re + self.im) // 16

    def __add__(self,other):
        if isinstance(other,int): return Zi(self.re + other,self.im)
        return Zi(self.re + other.re, self.im + other.im)

    def __sub__(self,other):
        if isinstance(other,int): return Zi(self.re - other,self.im)
        return Zi(self.re - other.re, self.im - other.im)

    def __mul__(self,other):
        if isinstance(other,int): return Zi(self.re * other,self.im * other)
        return Zi(self.re * other.re - self.im * other.im,
            self.re * other.im + self.im * other.re)

    def __floordiv__(self, other):
        a = self.re; b = self.im
        c = other.re; d = other.im
        return Zi((2*(a*c+b*d) +c*c+d*d) // (2*(c*c + d*d)),
            (2*(b*c-a*d) + c*c + d*d) // (2*(c*c+d*d)))

    def __mod__(self, other):
        return self - ( self // other) * other

    def __rmul__(self, a):
        return Zi(a * self.re, a* self.im)

    def __radd__(self, other):
        return Zi(other + self.re, self.im)

    def __rsub__(self,other):
```

```
        return Zi(other - self.re, -self.im)

    def __neg__(self):
        return Zi(-self.re, -self.im)

    def __pos__(self):
        return self

    def __pow__(self,n):
        resu = Zi(1)
        a = self
        while n!= 0:
            if n % 2 != 0:
                resu = resu * a
            a = a * a
            n = n // 2
        return resu

i = Zi(0,1)

if __name__ == "__main__":
    z = Zi(31,7)
    t = Zi(3,5)
    print(z,t)
    print(z//t, z % t)
```

Le programme suivant permet la décomposition d'un nombre premier de la forme $4k+1$ en somme de deux carrés, à la vitesse de l'algorithme d'Euclide. Il suit l'algoritme présenté dans le paragraphe 1.2 "Somme de deux carrés : une première preuve.".

```
from random import randint
from numtheory import isprime
from Zi import *

def pgcd(a,b):
    while b != Zi(0, 0):
        a, b = b, a % b
    return a

def racine_de_moins_un(p):
    pas_trouve = True
    while pas_trouve:
        a = randint(2, p - 2)
        b = pow(a, (p - 1)//4, p)
        if (b * b) % p == p-1:
            pas_trouve = False
    if 2 * b > p:
        b = b - p
    return b
```

```
def decomposition_carres(p):
    assert(p % 4 == 1)
    assert(isprime(p))
    a = racine_de_moins_un(p)
    pr = Zi(p)
    z = pgcd(pr, a+i)
    return abs(z.Re()), abs(z.Im())

if __name__ == "__main__":
    ttest = [13, 101, 10009, 11213,  100049, 1000000009,
             12345678912345678912345679O9, 10**50 + 577, 10**100 + 949]
    for p in ttest:
        a,b = decomposition_carres(p)
        assert p == a**2 + b**2, "erreur test"
        print(p,'=>', a, b)
```

Notons qu'il donne une réponse immédiate, même pour le nombre premier $10^{100}+949$, sur lequel buttait le programme précédent.

1.11.4 L'algorithme de Lehmmann.

Il correspond à l'algorithme présenté à la section 1.5 "Autre preuve et algorithme pour la décomposition en somme de deux carrés", donné dans [Lehmann] "Quadratic numbers".

```
"""algorithme de Lehman, quadratic numbers"""

from numtheory import jacobi, carre, isprime
from random import randint
from Zn import Mod

def reste_minimal(a,b):
    assert(b > 0)
    r = a % b
    if 2 * r > b:
        r -= b
    return r

def racine_de_moins_un(p):
    """
    input : p premier congru à 1 modulo 4
    output :  k tel que k^2 = -1 mod p
    |k| minimal, k > 0
    """
    assert isprime(p), "p non premier"
    assert p % 4 == 1, "p premier non congru à 1 modulo 4"
    while True:
        a = randint(2, p - 2)
        if jacobi(a, p) == -1:
```

```
            break
    b = pow(a, (p - 1) // 4, p)
    k = reste_minimal(b, p)
    return abs(k)

def somme_carres(p):
    k = racine_de_moins_un(p)
    a = (k**2 + 1) // p
    q, r = k, 1
    while a != 1:
        m, n = reste_minimal(q, a), reste_minimal(r, a)
        b = (m**2 + n**2) // a
        q, r = (q * m + r * n) // a, (q *n - r * m) // a
        a = b
    return abs(q),abs(r)


if __name__ == "__main__":
    ttest = [13, 101, 10009, 11213,  100049, 1000000009,
             12345678912345678912345679O9, 10**50 + 577, 10**100 + 949]
    for p in ttest:
        a,b = somme_carres(p)
        assert p == a**2 + b**2, "erreur test"
        print(p,'=>', a, b)
```

Il donne lui aussi des réponses immédiates.

Un autre algorithme de décomposition en sommes de deux carrés, très différent, sera présenté dans le chapitre “Formes quadratiques”.

Chapitre 2

Sommes de Gauss et sommes de Jacobi.

Les résultats de ce chapitre sont adaptés de [Ireland,Rosen].

2.1 Caractérisation des puissances n-ièmes dans un corps fini.

Proposition 24. *Soit $\mathbb{F}_q$ un corps fini à q éléments, et soit $\alpha \in \mathbb{F}_q^*$.*

(a) L'équation $x^n = \alpha$ a au moins une solution si et seulement si $\alpha^{\frac{q-1}{d}} = 1$, où $d = n \wedge (q-1)$.

$$\exists x \in \mathbb{F}_q^*,\ x^n = \alpha \iff \alpha^{\frac{q-1}{d}} = 1 \qquad (\text{où } d = n \wedge (q-1)).$$

(b) Si l'équation $x^n = \alpha$ a une solution, elle en a exactement $d = n \wedge (q-1)$.

Démonstration. Rappelons que, le groupe $\mathbb{F}_q^*$ ayant $q-1$ éléments, tout élément α de $\mathbb{F}_q^*$ vérifie $\alpha^{q-1} = 1$, et aussi que $\mathbb{F}_q^*$ est cyclique : appelons g un générateur de ce groupe.

Alors il existe un entier a tel que $\alpha = g^a$, et tout $x \in \mathbb{F}_q^*$ s'écrit sous la forme $x = g^y$ pour un certain entier y. Alors

$$x^n = \alpha \iff g^{ny} = g^a \iff g^{ny-a} = 1 \iff q-1 \mid ny-a.$$

(a) Supposons qu'il existe $x \in \mathbb{F}_q$ tel que $x^n = \alpha$. Alors il existe $y \in \mathbb{Z}$ tel que $q-1 \mid ny-a$. Comme $d \mid q-1$, et $d \mid n$, alors $d \mid a$.
Puisque $\frac{a}{d}$ est un entier,

$$\alpha^{\frac{q-1}{d}} = g^{a\frac{q-1}{d}} = \left(g^{q-1}\right)^{\frac{a}{d}} = 1.$$

Réciproquement, supposons que $\alpha^{\frac{q-1}{d}} = 1$. Alors $g^{a\frac{q-1}{d}} = 1$, donc $q-1 \mid a\,\frac{q-1}{d}$, soit $d \mid a$. Comme $d = n \wedge (q-1)$, il existe des entiers u, v tels que $un + v(q-1) = d$, donc $u\frac{n}{d} + v\frac{q-1}{d} = 1$. Alors, puisque $\frac{a}{d}$ est un entier,

$$\begin{aligned}\alpha &= g^a \\ &= g^{\left(u\frac{n}{d} + v\frac{q-1}{d}\right)a} \\ &= \left(g^{u\frac{a}{d}}\right)^n \left(g^{q-1}\right)^{v\frac{a}{d}} \\ &= \left(g^{u\frac{a}{d}}\right)^n\end{aligned}$$

Ainsi $x = g^{u\frac{a}{d}}$ est une solution de $x^n = \alpha$.

(b) Supposons que l'équation $x^n = \alpha$ ait une solution $x = g^y$. D'après la partie (a), avec les mêmes notations, d divise a. Cherchons alors toutes les solutions de $x^n = \alpha$, ce qui revient à trouver tous les $y \in \mathbb{Z}$ tels que $q-1 \mid ny - a$ soit $\frac{n}{d}y \equiv \frac{a}{d} \pmod{\frac{q-1}{d}}$.

Si u, v sont les entiers tels que $un + v(q-1) = d$, alors $u\frac{n}{d} + v\frac{q-1}{d} = 1$, donc $u\frac{n}{d} \equiv 1 \pmod{\frac{q-1}{d}}$. Ainsi

$$\frac{n}{d}y \equiv \frac{a}{d} \pmod{\frac{q-1}{d}} \iff y \equiv u\frac{a}{d} \pmod{\frac{q-1}{d}}.$$

Les solutions $x = g^y$ de $x^n = \alpha$ sont données par les valeurs de y vérifiant

$$y = u\frac{a}{d} + k\frac{q-1}{d},\ k \in \mathbb{Z}.$$

Notons $y_k = u\frac{a}{d} + k\frac{q-1}{d}$, et $x_k = g^{y_k}$. Alors $y_{k+d} = u\frac{a}{d} + (k+d)\frac{q-1}{d} \equiv y_k \pmod{q-1}$, donc $x_{k+d} = x_k$.

Les solutions de $x^n = \alpha$ sont donc $x_0, \cdots, x_{d-1}$. Vérifions que ces solutions sont distinctes. Supposons que $x_k = x_l$, où $0 \leq k < d, 0 \leq l < d$. Alors $g^{y_k} = g^{y_l}$, donc $q-1 \mid y_k - y_l = (k-l)\frac{q-1}{d}$, donc $d \mid (k-l)$, où $|k-l| < d$, donc $k = l$.

En conclusion, ou bien $x^n = \alpha$ n'a pas de solution, ou bien les solutions de cette équation sont les d éléments distincts

$$x = g^{u\frac{a}{d} + k\frac{q-1}{d}}, \qquad k = 0, 1, \cdots, d-1.$$

□

Exemple 1. Si $q = p$ est un nombre premier impair, et $p \nmid a$, on déduit de cette proposition le résultat bien connu

$$\exists x \in \mathbb{Z},\ x^2 \equiv a \pmod{p} \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Exemple 2. Soit $q = p^s$ une puissance d'un nombre premier p.

Si $q \equiv 2 \pmod 3$, et $a \in \mathbb{F}_q^*$, alors l'équation $x^3 = a$ a au moins une solution dans $\mathbb{F}_q^*$ si $a^{q-1} = 1$, ce qui est toujours vrai. Ainsi, tout $a \in \mathbb{F}_q$ est un cube dans $\mathbb{F}_q$. De plus $d = 3 \wedge (q-1) = 1$, donc $a \in \mathbb{F}_q^*$ est le cube d'un unique élément de $\mathbb{F}_q^*$. Autrement dit l'application $\mathbb{F}_q^* \to \mathbb{F}_q^*, x \mapsto x^3$ est un automorphisme de groupe de $\mathbb{F}_q^*$.

Si $q \equiv 1 \pmod 3$, alors l'équation $x^3 = a$ a au moins une solution dans $\mathbb{F}_p^*$ si $a^{\frac{q-1}{3}} = 1$, auquel cas elle admet 3 solutions.

2.2 Trace et norme dans les corps finis.

2.2.1 Groupe de Galois d'un corps fini.

La théorie de Galois d'un corps fini est particulièrement simple, et nous la développons ici, sans utiliser les théorèmes généraux de la théorie de Galois.

Soit $F = \mathbb{F}_q$ un corps à q éléments, et $K = \mathbb{F}_{q^s} \supset \mathbb{F}_q$ une extension de F à q^s éléments. Alors $[K : F] = s$.

Définition 1. *Un automorphisme σ du corps K s'appelle un F-automorphisme si pour tout élément α de F, $\sigma(\alpha) = \alpha$. L'ensemble de ces F-automorphismes forment un groupe, appelé groupe de Galois de K sur F, et noté*

$$G = \mathrm{Gal}(K/F).$$

Exemples : 1_K est un élément du groupe de Galois. Un exemple plus intéressant est l'automorphisme de Frobenius F (il faut distinguer F et F !), défini par

$$\mathrm{F} \left\{ \begin{array}{ccc} K & \to & K \\ \alpha & \mapsto & \alpha^q. \end{array} \right.$$

Si α est un élément du corps K alors $\mathrm{F}(\alpha) = \alpha^q \in K$. Puisque $q = p^k, k \in \mathbb{N}^*$, où p est la caractéristique de F, pour tous les $\alpha, \beta \in K$, $\mathrm{F}(x+y) = (x+y)^q = (x+y)^{p^k} = x^{p^k} + y^{p^k} = \mathrm{F}(\alpha) + \mathrm{F}(\beta)$, et $\mathrm{F}(1) = 1$, $\mathrm{F}(\alpha\beta) = (\alpha\beta)^q = \alpha^q\beta^q = \mathrm{F}(\alpha)F(\beta)$. De plus comme tout morphisme de corps, F est injectif : si $\alpha \neq 0$, alors $\mathrm{F}(\alpha)\mathrm{F}(\alpha^{-1}) = \mathrm{F}(\alpha\alpha^{-1}) = \mathrm{F}(1) = 1 \neq 0$, donc $\mathrm{F}(\alpha) \neq 0$. Comme l'injection F applique K dans K, où K est fini, F est une bijection.

Si $\alpha \in F = \mathbb{F}_q$, alors $\alpha^q = \alpha$, donc $\mathrm{F}(\alpha) = \alpha$. Ainsi $\mathrm{F} \in \mathrm{Gal}(K/F)$.

Cet automorphisme suffit pour décrire le groupe G.

Proposition 25. *Le groupe de Galois $G = \mathrm{Gal}(K/F)$ est un groupe cyclique d'ordre $s = [K : F]$, engendré par l'automorphisme de Frobenius* F.

Démonstration. Soit g un générateur du groupe cyclique K^*. Considérons un élément quelconque $\sigma \in G$. Alors $(\mathrm{F}^{-1} \circ \sigma)(g) \neq 0$, et donc $(\mathrm{F}^{-1} \circ \sigma)(g) = g^i$, pour un certain $i \in [\![0, q^s - 2]\!]$, ce qui donne $\sigma(g) = \mathrm{F}(g)^i$. Si α est un élément de K^*, alors $\alpha = g^k$, où k est un entier, donc $\sigma(\alpha) = \sigma(g)^k = \mathrm{F}(g)^{ik} = \mathrm{F}(g^k)^i = \mathrm{F}^i(\alpha)$ (et $\sigma(0) = 0 = \mathrm{F}^i(0)$). Ceci prouve que $\sigma = \mathrm{F}^i$, et ainsi G est cyclique, engendré par F.

Pour tout $\alpha \in K$, $\mathrm{F}^s(\alpha) = \alpha^{q^s} = \alpha$, donc $\mathrm{F}^s = 1_K$. De plus, si $\mathrm{F}^k = 1_K$ pour un entier k, alors pour tout $\alpha \in K$, $\alpha^{q^k} = \mathrm{F}^k(\alpha) = \alpha$, en particulier $g^{q^k} = g$, donc $g^{q^k - 1} = 1$, où le générateur g est d'ordre $q^s - 1$, ce qui prouve que $q^s - 1 \mid q^k - 1$, donc $s \mid k$. L'ordre de F est donc égal à s, ainsi que l'ordre du groupe $G = \langle \mathrm{F} \rangle = \{1_K, \mathrm{F}, \ldots, \mathrm{F}^{s-1}\}$. □

La proposition suivante montre que l'extension $F \subset K$ entre deux corps finis est galoisienne.

Proposition 26. *Soient F, K deux corps finis tels que $F \subset K$, et soit $\alpha \in K$. Notons $p(x) = \Pi_{\alpha,F} \in F[x]$ le polynôme minimal de α sur F, où $r = \deg(p) = [F[\alpha] : F]$. Alors*

(i) Le polynôme p est scindé dans K, i.e. p est produit de facteurs linéaires $x - \beta$, où $\beta \in K$.

(ii) Toutes les racines du polynôme p sont simples.

Ainsi $p(x) = \prod_{\beta \in S}(x - \beta) = (x - \beta_1) \ldots (x - \beta_r)$, où $S = \{\beta_1, \ldots, \beta_r\} \subset K$, et les β_i, $i = 1, \ldots, r$, sont distincts.

Démonstration. Ici $|F| = q$, et $|K| = p^s$. Notons $L = F[\alpha]$.

Comme $F \subset K$, et $\alpha \in K$, alors $F \subset L \subset K$. Alors L est un corps à q^r éléments, où $r = [L : F] = \deg(p)$, et $r \mid s$.

Par conséquent tout élément $\gamma \in L$ vérifie $\gamma^{q^r} = \gamma$. Puisque $\alpha \in L$, α est racine du polynôme $x^{q^r} - x \in F[x]$, donc son polynôme minimal $p(x)$ divise $x^{q^r} - x = \prod_{\beta \in L}(x - \beta)$.

Le polynôme $x^{q^r} - x$ ayant q^r racines distincts dans $L \subset K$, il en va de même de son diviseur $p(x)$. Ainsi $p(x) = \prod_{x \in S}(x - \beta)$, où $S \subset L \subset K$, ce qui montre (i) et (ii). □

Nous pouvons préciser les racines de $p(x)$.

Proposition 27. *En gardant les conditions de la proposition* 26*, notons* F *le F-automorphisme de Frobenius de K. Alors*

$$p(x) = \Pi_{\alpha,F}(x) = \prod_{i=0}^{r-1}(x - \mathrm{F}^i(\alpha)) = \prod_{i=0}^{r-1}(x - \alpha^{q^i}).$$

Démonstration. Si $q = \sum_{i=0}^{d} a_i x^i \in K[x]$, notons $\mathrm{F} \cdot q = \sum_{i=0}^{d} \mathrm{F}(a_i)x^i$. Si $q, r \in K[x]$, $\mathrm{F}\cdot(q+r) = (\mathrm{F}\cdot q) + (\mathrm{F}\cdot r)$ et $\mathrm{F}\cdot(qr) = (\mathrm{F}\cdot q)(\mathrm{F}\cdot r)$. Alors, en appliquant F au polynôme $s = \prod_{i=0}^{r-1}(x - \mathrm{F}^i(\alpha))$, nous obtenons, en utilisant $\alpha^{q^r} = \alpha$, soit $\mathrm{F}^r(\alpha) = \alpha$,

$$\begin{aligned}
\mathrm{F}\cdot s &= \mathrm{F}\left(\prod_{i=0}^{r-1}\left(x - \mathrm{F}^i(\alpha)\right)\right) \\
&= \prod_{i=0}^{r-1} \mathrm{F}\cdot(x - \mathrm{F}^i(\alpha)) \\
&= \prod_{i=0}^{r-1}(x - \mathrm{F}^{i+1}(\alpha)) \\
&= \prod_{j=1}^{r}(x - \mathrm{F}^j(\alpha)) \qquad (j = i+1) \\
&= (x - \mathrm{F}^r(\alpha)) \prod_{j=1}^{r-1}(x - \mathrm{F}^j(\alpha)) \\
&= (x - \alpha) \prod_{j=1}^{r-1}(x - \mathrm{F}^j(\alpha)) \\
&= \prod_{j=0}^{r-1}(x - \mathrm{F}^j(\alpha)) \\
&= s
\end{aligned}$$

L'égalité $\mathrm{F}\cdot s = s$ montre que tous les coefficients de s sont dans F, soit $s \in F[x]$. Puisque $s(\alpha) = 0$, le polynôme minimal p divise s. Mais p et R sont de même degré r, et sont normalisés, donc $p = r$, ce qui prouve

$$p(x) = \Pi_{\alpha,F}(x) = \prod_{i=0}^{r-1}(x - \mathrm{F}^i(\alpha)) = \prod_{i=0}^{r-1}(x - \alpha^{q^i}).$$

□

2.2.2 Trace et norme.

Considérons encore l'extension $F \subset K$ de degré s.

Pour chaque $\alpha \in K$, définissons l'application m_α de multiplication par α par

$$m_\alpha \left\{ \begin{array}{ccc} K & \to & K \\ \gamma & \mapsto & \alpha\gamma. \end{array} \right.$$

Alors m_α est un endomorphisme du F-espace vectoriel K.

Définition 2. *$\chi_{\alpha,K/F} \in F[x]$ est le polynôme caractéristique de m_x :*

$$\chi_{\alpha,K/F}(x) = \det(x\,\mathrm{Id}_L - m_\alpha),$$

et la trace et la norme de α sont définis par

$$\mathrm{Tr}_{K/F}(\alpha) = \mathrm{tr}(m_\alpha), \qquad \mathrm{N}_{K/F}(\alpha) = \det(m_\alpha),$$

où tr *et* det*, définis en algèbre linéaire, désignent la trace et la norme d'un endomorphisme.*

Cette définition montre que, pour tout $\alpha \in K$, $\mathrm{Tr}_{K/F}(\alpha)$ et $\mathrm{N}_{K/F}(\alpha)$ sont des éléments de F.

Proposition 28. *Si $a, b \in F$, et $\alpha, \beta \in K$,*

(i)

$$\mathrm{Tr}_{K/F}(a\alpha + b\beta) = a\mathrm{Tr}_{K/F}(\alpha) + b\mathrm{Tr}_{K/F}(\beta).$$

Autrement dit, la trace est F-linéaire.

(ii)

$$\mathrm{N}_{K/F}(\alpha\beta) = \mathrm{N}_{K/F}(\alpha)\mathrm{N}_{K/F}(\beta),$$
$$\mathrm{N}_{K/F}(a\alpha) = a^s\mathrm{N}_{K/F}(\alpha),$$

où $s = [K : F]$.

Démonstration. (i) Notons que $m_{a\alpha+b\beta} = am_\alpha + bm_\beta$. La linéarité de la trace donne alors

$$\begin{aligned}\mathrm{Tr}_{K/F}(a\alpha + b\beta) &= \mathrm{tr}(am_\alpha + bm_\beta)\\ &= a\,\mathrm{tr}(m_\alpha) + b\,\mathrm{tr}(m_\beta)\\ &= a\mathrm{Tr}_{K/F}(\alpha) + b\mathrm{Tr}_{K/F}(\beta).\end{aligned}$$

(ii) Comme $m_{\alpha\beta} = m_\alpha \circ m_\beta$,

$$\begin{aligned}\mathrm{N}_{K/F}(\alpha\beta) &= \det(m_{\alpha\beta})\\ &= \det(m_\alpha \circ m_\beta)\\ &= \det(m_\alpha)\det(m_\beta)\\ &= \mathrm{N}_{K/F}(\alpha)\mathrm{N}_{K/F}(\beta).\end{aligned}$$

En utilisant $m_{a\alpha} = am_\alpha$ si $a \in F$,

$$\begin{aligned}\mathrm{N}_{K/F}(a\alpha) &= \det(m_{a\alpha})\\ &= \det(am_\alpha)\\ &= a^s\det(m_\alpha)\\ &= a^s\mathrm{N}_{K/F}(\alpha).\end{aligned}$$

□

Si $\alpha \in K$, la relation entre le polynôme minimal $\Pi_{\alpha,F}$ et le polynôme caractéristique $\chi_{\alpha,K/F}$ est donnée dans la proposition suivante.

Proposition 29. *Si $\alpha \in K$, alors $\chi_{\alpha,K/F} = \Pi_{\alpha,F}^r$, où $r = [K : F(\alpha)]$.*

Démonstration. Notons $n = [F(\alpha) : F], r = [K : F(\alpha)]$. Si $(e_1, \dots, e_r)$ est une base de K sur $F(\alpha)$, comme $(1, \alpha, \dots, \alpha^{n-1})$ est une base de $F(\alpha)$ sur F, le lemme télescopique montre que

$$\mathcal{B} = (e_1, \alpha e_1, \dots, \alpha^{n-1}e_1,\ e_2, \alpha e_2, \dots, \alpha^{n-1}e_2,\ \dots, e_r, \alpha e_r, \dots, \alpha^{n-1}e_r)$$

est une base de K sur F.

Les sous-espaces $E_i = \mathrm{Vect}(e_i, \dots, \alpha^{n-1}e_i),\ i = 1, \dots r$ sont stables pour l'endomorphisme m_α : en effet, si on note $P(x) = \Pi_{\alpha,K}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, alors $\alpha^n = -a_0 - \cdots - a_{n-1}\alpha^{n-1}$, et

$$\begin{aligned} m_\alpha(\alpha^i e_j) &= \alpha^{i+1}e_j \ (0 \le i \le n-2, 1 \le j \le r), \\ m_\alpha(\alpha^{n-1}e_j) &= \alpha^n e_j = -\sum_{k=0}^{n-1} a_k \alpha^k e_j. \end{aligned}$$

Donc la matrice de l'application induite par m_α sur E_i est la matrice compagnon

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & & & -a_1 \\ 0 & 1 & \ddots & & -a_2 \\ \vdots & \ddots & 1 & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix},$$

et

$$M = \mathcal{M}_{\mathcal{B}}(m_\alpha) = \begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & A \end{pmatrix}.$$

Rappelons le calcul du polynôme caractéristique de la matrice compagnon A :

$$\chi_A(x) = \det(xI_n - A) = \begin{vmatrix} x & 0 & \cdots & 0 & a_0 \\ -1 & x & & & a_1 \\ 0 & -1 & \ddots & & a_2 \\ \vdots & \ddots & -1 & x & \vdots \\ 0 & \cdots & 0 & -1 & x + a_{n-1} \end{vmatrix}$$

Ce déterminant se calcule par une relation de récurrence : posons

$$D_k = \begin{vmatrix} x & 0 & \cdots & 0 & a_0 \\ -1 & x & & & a_1 \\ 0 & -1 & \ddots & & a_2 \\ \vdots & \ddots & -1 & x & \vdots \\ 0 & \cdots & 0 & -1 & a_k \end{vmatrix}$$

Le développement de D_k suivant la dernière ligne donne $D_k = a_k x^k + D_{k-1}$, et par récurrence $D_k = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0$.

Ce résultat, appliqué à la matrice $xI_n - A$ donne $\det(xI_n - A) = (x + a_{n-1})x^{n-1} + D_{n-2} = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = P(x)$, donc

$$\det(xI_n - M) = P(x)^r.$$

Ainsi $\chi_{\alpha,K/F} = \Pi_{\alpha,F}^r$, où $r = [K : F(\alpha)]$. □

Proposition 30. *Soit $F \subset K$ une extension de corps finis, avec $|F| = q, |K| = q^s$, et soit $\alpha \in K$. Notons $G = \mathrm{Gal}(K/F)$ le groupe de Galois de K sur F. Alors*

(i) $\chi_{\alpha,K/F}(x) = \prod_{\sigma\in G}(x - \sigma(\alpha)) = (x - \alpha)(x - \alpha^q)\cdots(x - \alpha^{q^{s-1}})$.

(ii) $\mathrm{Tr}_{K/F}(\alpha) = \sum_{\sigma\in G}\sigma(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{s-1}}$.

(iii) $\mathrm{N}_{K/F}(\alpha) = \prod_{\sigma\in G}\sigma(\alpha) = \alpha \cdot \alpha^q \cdot \ \cdots \ \cdot \alpha^{q^{s-1}}$.

Démonstration. (i) Partons de la factorisation dans $K[x]$ du polynôme minimal de α sur F :

$$\Pi_{\alpha,F}(x) = \prod_{i=0}^{r-1}(x - \alpha^{q^i}) = \prod_{i=0}^{r-1}(x - \mathrm{F}^i(\alpha)) \qquad (r = [F[\alpha] : F],\ r \mid s).$$

Posons $e = [K : F[\alpha]]$, si bien que $s = er$. Tout entier $k \in [\![0, s[\![$ s'écrit, par la division euclidienne de k par r, sous la forme $k = jr + i,\ 0 \le i < r,\ 0 \le j < e$. Ceci justifie les égalités suivantes :

$$\begin{aligned}
\prod_{\sigma\in G}(x - \sigma(\alpha)) &= \prod_{k=0}^{s-1}(x - \mathrm{F}^k(\alpha)) \\
&= \prod_{j=0}^{e-1}\prod_{i=0}^{r-1}(x - \mathrm{F}^{jr+i}(\alpha)) \\
&= \prod_{j=0}^{e-1}\prod_{i=0}^{r-1}(x - \mathrm{F}^i(\alpha)) \qquad (\text{car } F^r(\alpha) = \alpha) \\
&= \prod_{j=0}^{e-1}\Pi_{\alpha,F}(x) \\
&= \Pi_{\alpha,F}^e \\
&= \chi_{\alpha,K/F}(x),
\end{aligned}$$

la dernière égalité venant de la proposition 29. Ceci prouve (i).

(ii),(iii) Le développement de $\chi_{\alpha,K/F}(x)$ donne, par définition de la trace et de la norme d'un nombre algébrique :

$$\chi_{\alpha,K/F}(x) = x^n - \mathrm{Tr}_{K/F}(\alpha)x^{n-1} + \cdots + (-1)^n\mathrm{N}_{K/F}(\alpha) \quad (n = [K : F]),$$

et le développement de la formule de la partie (i) donne

$$\chi_{\alpha,K/F}(x) = x^n - \left(\sum_{\sigma\in G}\sigma(\alpha)\right)x^{n-1} + \cdots + (-1)^n\prod_{\sigma\in G}\sigma(\alpha).$$

Ainsi

$$\mathrm{Tr}_{K/F}(\alpha) = \sum_{\sigma\in G} \sigma(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{s-1}}.$$

$$\mathrm{N}_{K/F}(\alpha) = \prod_{\sigma\in G} \sigma(\alpha) = \alpha \cdot \alpha^q \cdot \ \cdots \ \cdot \alpha^{q^{s-1}}.$$

□

Donnons quelques propriétés de la trace et de la norme.

Proposition 31. *(i) L'application* $\mathrm{Tr} = \mathrm{Tr}_{K/F} : K \to F$ *est surjective.*

(ii) La restriction

$$\varphi \left\{ \begin{array}{ccc} K^* & \to & F^* \\ \alpha & \mapsto & \mathrm{N}_{K/F}(\alpha) \end{array} \right.$$

est surjective.

Démonstration. (i) Le polynôme $p(x) = x + x^q + \cdots + x^{q^{s-1}}$, de degré q^{s-1}, a au plus q^{s-1} racines. Comme $|K| = q^s$, il existe un élément $\alpha \in K$ tel que $p(\alpha) \neq 0$. Alors $c = \mathrm{Tr}(\alpha) = p(\alpha) \neq 0$. Si $b \in F$, alors $\mathrm{Tr}(c^{-1}b\alpha) = c^{-1}b\mathrm{Tr}(\alpha) = b$, ce qui prouve la surjectivité de $\mathrm{Tr}_{K/F} : K \to F$.

(ii) Notons d'abord que $\alpha \neq 0$ entraîne $\mathrm{N}_{K/F}(\alpha) = \alpha \cdot \alpha^q \cdot \ \cdots \ \cdot \alpha^{q^{s-1}} \neq 0$, ce qui montre que φ est correctement défini.

L'application φ est un homomorphisme de groupes. Précisons son noyau. Si $\alpha \in K$,

$$\begin{aligned} \alpha \in \ker(\varphi) &\iff 1 = \alpha \cdot \alpha^q \cdot \ \cdots \ \cdot \alpha^{q^{s-1}} \\ &\iff 1 = \alpha^{1+q+\cdots+q^{s-1}} = \alpha^{\frac{q^s-1}{q-1}}. \end{aligned}$$

Puisque $\frac{q^s-1}{q-1}$ divise $q^s - 1 = |K|$, la proposition 24 du chapitre "Sommes de Gauss et somme de Jacobi" montre que l'équation $\alpha^{\frac{q^s-1}{q-1}} = 1$ a exactement $\frac{q^s-1}{q-1} = (\frac{q^s-1}{q-1}) \wedge (q^s - 1)$ solutions. Ainsi

$$|\ker(\varphi)| = \frac{q^s - 1}{q - 1}.$$

Le premier théorème d'isomorphisme donne alors $|\mathrm{im}(\varphi)| = |K^*|/|\ker(\varphi)| = q-1$. Ainsi $|\mathrm{im}(\varphi)| = |F^*|$, avec $\mathrm{im}(\varphi) \subset F^*$, donc $\mathrm{im}(\varphi) = F^*$, ce qui prouve que l'application φ est surjective.

□

Proposition 32. *Soient* $F \subset E \subset K$ *trois corps finis, et* $\alpha \in K$*. Alors*

(i) $\mathrm{Tr}_{K/F}(\alpha) = \mathrm{Tr}_{E/F}(\mathrm{Tr}_{K/E}(\alpha))$,

(ii) $\mathrm{N}_{K/F}(\alpha) = \mathrm{N}_{E/F}(\mathrm{N}_{K/E}(\alpha))$.

Démonstration. Posons $d = [E : F], m = [K : E]$, et $n = [K : F]$. Alors $n = dm$. Si $q = |F|$, alors $q_1 = |E| = q^d$ et $|K| = q^n$. De plus

$$\mathrm{Tr}_{K/E}(\alpha) = \alpha + \alpha^{q_1} + \cdots + \alpha^{q_1^{m-1}}.$$

Alors

$$\begin{aligned}\mathrm{Tr}_{E/F}(\mathrm{Tr}_{K/E}(\alpha)) &= \sum_{i=0}^{d} \mathrm{Tr}_{K/E}(\alpha)^{q^i} \\ &= \sum_{i=0}^{d}\sum_{j=0}^{m-1} \alpha^{q_1^j q^i} \\ &= \sum_{i=0}^{d}\sum_{j=0}^{m-1} \alpha^{q^{dj+i}} \\ &= \sum_{k=0}^{n-1} \alpha^{q^k} \\ &= \mathrm{Tr}_{K/F}(\alpha).\end{aligned}$$

Nous avons utilisé le fait que tout entier $k \in [\![0, n[\![$ s'écrit de façon unique sous la forme $k = dj + i, 0 \leq i < d, 0 \leq j < m$.

En remplaçant les sommes par des produits, nous obtenons la même démonstration pour les normes. □

La connaissance du polynôme minimal de $\alpha \in K$ suffit pour calculer sa trace et sa norme sur F. Précisons.

Proposition 33. *Soit $F \subset K$ une extension de corps finis, et soit $\alpha \in K$, et $E = F[\alpha]$. Notons $n = [K : F], d = [E : F]$, et*

$$f(x) = x^d - c_1 x^{d-1} + \cdots + (-1)^d c_d$$

le polynôme minimal de α sur F. Alors

(i) $\mathrm{Tr}_{K/F}(\alpha) = \frac{n}{d} c_1$,

(ii) $\mathrm{N}_{K/F}(\alpha) = c_d^{n/d}$.

Démonstration. Notons $e = n/d$. La proposition 29 donne $\chi_{\alpha,K/F}(x) = f(x)^e$, où $\chi_{\alpha,K/F}(x)$ est le polynôme caractéristique de $\alpha \in K$ sur F. Alors

$$\begin{aligned}\chi_{\alpha,K/F}(x) &= (x^d - c_1 x^{d-1} + \cdots + (-1)^d c_d)^e \\ &= x^n - e c_1 x^{n-1} + \cdots + (-1)^n c_d^e.\end{aligned}$$

La comparaison avec

$$\chi_{\alpha,K/F}(x) = x^n - \mathrm{Tr}_{K/F}(\alpha) x^{n-1} + \cdots + (-1)^n \mathrm{N}_{K/F}(\alpha)$$

montre que $\mathrm{Tr}_{K/F}(\alpha) = e c_1, \mathrm{N}(\alpha) = c_d^e$, ce qu'il fallait prouver. □

2.3 Caractères multiplicatifs.

Soit $q = p^s$ une puissance d'un nombre premier p, et $\mathbb{F}_q$ un corps de cardinal q.

Un caractère multiplicatif sur $\mathbb{F}_q^*$ est un homomorphisme de groupe χ du groupe multiplicatif $\mathbb{F}_q^*$ dans le groupe $\mathbb{C}^*$. Il vérifie ainsi, pour tous les éléments a, b de $\mathbb{F}_q^*$, la relation

$$\chi(ab) = \chi(a)\chi(b).$$

Exemple 1. Nous savons que pour tout $a \in \mathbb{Z}$, pour tout $b \in \mathbb{Z}$, $a \equiv b \pmod p$ entraîne $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, et aussi $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. L'application

$$\chi \left\{ \begin{array}{ccc} \mathbb{F}_p^* & \to & \mathbb{C}^* \\ [a]_p & \mapsto & \left(\frac{a}{p}\right) \end{array} \right.$$

est donc bien définie, et c'est un caractère sur $\mathbb{F}_p^*$.

Exemple 2. L'application ε définie pour tout $a \in \mathbb{F}_q^*$ par $\varepsilon(a) = 1$ est un caractère.

Il est commode de prolonger ces applications sur $\mathbb{F}_q$ tout entier en posant $\chi(0) = 0$ si $\chi \neq \varepsilon$, et $\varepsilon(0) = 1$. Nous dirons alors que χ est un caractère sur $\mathbb{F}_q$.

Un caractère étant d'abord un homomorphisme de groupes, il vérifie donc

(a) $\chi(1) = 1$,

(b) $\chi(a^{-1}) = \chi(a)^{-1}$, pour tout $a \in \mathbb{F}_q^*$.

De plus, tout caractère vérifie la proposition suivante.

Proposition 34. *Soit χ un caractère sur $\mathbb{F}_q^*$.*
Pour tout $a \in \mathbb{F}_q^*$, $\chi(a)$ est une racine $q-1$-ième de l'unité.

Démonstration. Soit $a \in \mathbb{F}_q^*$. Alors $a^{q-1} = 1$, donc $\chi(a)^{q-1} = \chi(a^{q-1}) = \chi(1) = 1$. □

Le caractère χ induit donc un homomorphisme de $\mathbb{F}_q^*$ sur le groupe $\mathbb{U}_{q-1} \subset \mathbb{U}$ des racines $(q-1)$-ièmes de l'unité.

Si $z \in \mathbb{U}$, alors $|z| = 1$, donc $z^{-1} = \overline{z}$, et ainsi

$$\chi(a^{-1}) = \overline{\chi(a)}.$$

Proposition 35. *Soit χ un caractère multiplicatif sur $\mathbb{F}_q$.*

(a) Si $\chi \neq \varepsilon$, alors $\sum_{t \in \mathbb{F}_q} \chi(t) = 0$.

(b) Si $\chi = \varepsilon$, alors $\sum_{t \in \mathbb{F}_q} \varepsilon(t) = q$.

Démonstration. (a) Comme $\chi \neq \varepsilon$, il existe $a \in \mathbb{F}_q^*$ tel que $\chi(a) \neq 1$.
Posons $S = \sum_{t \in \mathbb{F}_q} \chi(t)$. Alors, puisque l'application $t \mapsto at$ est une permutation des éléments de $\mathbb{F}_q^*$,

$$\begin{aligned} \chi(a)S &= \sum_{t \in \mathbb{F}_q} \chi(a)\chi(t) \\ &= \sum_{t \in \mathbb{F}_q} \chi(at) \\ &= \sum_{s \in \mathbb{F}_q} \chi(s) \qquad (s = at) \\ &= S \end{aligned}$$

Ainsi $(\chi(a) - 1)S = 0$, où $\chi(a) \neq 1$, donc $S = 0$.

(b) Si $\chi = \varepsilon$, alors $\sum_{t \in \mathbb{F}_q} \varepsilon(t) = \sum_{t \in \mathbb{F}_q} 1 = |\mathbb{F}_q| = q$.

□

L'ensemble des caractères sur $\mathbb{F}_q^*$ est l'ensemble $\mathrm{Hom}(\mathbb{F}_q^*, \mathbb{C}^*)$. Il forme donc un groupe pour la loi $(\chi, \lambda) \mapsto \chi\lambda$, où $\chi\lambda$ est défini par

$$(\chi\lambda)(a) = \chi(a)\lambda(a), \text{ pour tout } a \in \mathbb{F}_p^*.$$

Remarquons que cette relation reste vraie si $a = 0$.

L'élément neutre est ε, et le symétrique d'un caractère χ dans ce groupe est le caractère χ^{-1} vérifiant, pour tout $a \in \mathbb{F}_q^*$, $\chi^{-1}(a) = (\chi(a))^{-1}$.

Notons maintenant $C = \mathrm{Hom}(\mathbb{F}_q^*, \mathbb{C}^*)$ le groupe des caractères sur $\mathbb{F}_q^*$.

Proposition 36. *Le groupe C des caractères sur $\mathbb{F}_q^*$ est un groupe cyclique d'ordre $q-1$.*

Démonstration. Nous savons que $\mathbb{F}_q^*$ est cyclique. Soit g un générateur de ce groupe, si bien que tout $a \in \mathbb{F}_q^*$ est une puissance de g.

χ est entièrement déterminé par la valeur de $\chi(g)$: si $a \in \mathbb{F}_q^*$, alors $a = g^l$, $l \in \mathbb{N}$, donc $\chi(a) = \chi(g)^l$. Comme $\chi(g) \in \mathbb{U}_{q-1}$, où $|\mathbb{U}_{q-1}| = q-1$, il existe au plus $q-1$ caractères, soit $|C| \leq q-1$.

Il existe un (et un seul) caractère λ tel que $\lambda(g) = e^{2i\frac{\pi}{q-1}}$. En effet, l'application λ telle que $\lambda(g^k) = e^{2ik\frac{\pi}{q-1}}$ est bien définie, et c'est un caractère :

- si $a = g^k = g^l$, alors $k \equiv l \pmod{q-1}$, soit $l = k + s(q-1), s \in \mathbb{Z}$, donc
$$e^{2il\frac{\pi}{q-1}} = e^{2i(k+s(q-1))\frac{\pi}{q-1}} = e^{2ik\frac{\pi}{q-1}} e^{2i\pi s} = e^{2ik\frac{\pi}{q-1}},$$
- si $a, b \in \mathbb{F}_q^*$, il existe des entiers k, l tels que $a = g^k, b = g^l$, et
$$\lambda(ab) = \lambda(g^{k+l}) = e^{2i(k+l)\frac{\pi}{q-1}} = e^{2ik\frac{\pi}{q-1}} e^{2il\frac{\pi}{q-1}} = \lambda(a)\lambda(b).$$

Montrons que λ est d'ordre $q-1$ dans le groupe des caractères. D'abord, pour tout $a = g^k \in \mathbb{F}_q^*$, $\lambda^{q-1}(a) = e^{2ik\pi} = 1$, donc $\lambda^{q-1} = \varepsilon$.

Inversement, si $\lambda^n = \varepsilon$, alors $\lambda^n(g) = \varepsilon(g) = 1$, donc $\lambda(g^n) = 1$, soit $e^{2in\frac{\pi}{q-1}} = 1$, ce qui impose $\frac{n}{q-1} \in \mathbb{Z}$, donc $q-1 \mid n$.

Ceci prouve que l'ordre de λ est $q-1$, et donc $|C| \geq q-1$. Ainsi $|C| = q-1$, et λ est un générateur de ce groupe. □

Retenons l'expression d'un tel générateur. Nous avons prouvé la proposition suivante.

Proposition 37. *Si g est un générateur de $\mathbb{F}_q^*$, il existe un et un seul caractère λ tel que $\lambda(g) = e^{2i\frac{\pi}{q-1}}$, et λ est un générateur du groupe des caractères C.*

A titre de corollaire de la proposition 36, nous avons le résultat suivant.

Proposition 38. *Si n divise $q-1$, alors il existe exactement n caractères χ vérifiant $\chi^n = \varepsilon$.*

Ces caractères forment un sous-groupe C_n de C, cyclique et d'ordre n.

Démonstration. Ceci est une conséquence du fait que C est cyclique. Rappelons une démonstration de ce fait.

Si λ est un générateur de C, d'ordre $q-1$, alors tout caractère χ est de la forme $\chi = \lambda^k, k \in \mathbb{Z}$, donc $\chi^n = \varepsilon$ équivaut à $\lambda^{kn} = \varepsilon$, soit $q-1 \mid kn$, ou encore $\frac{q-1}{n} \mid k$. Les solutions de $\chi^n = 1$ sont donc de la forme $\lambda^{j\frac{q-1}{n}}$, où on peut prendre $0 \leq j < n$, puisque $\lambda^{(j+n)\frac{q-1}{n}} = \lambda^{j\frac{q-1}{n}}$.

L'ensemble des solutions de $\chi^n = \varepsilon$ est donc donc l'ensemble

$$C_n = \{\varepsilon, \lambda^{\frac{q-1}{n}}, \lambda^{2\frac{q-1}{n}}, \ldots, \lambda^{(n-1)\frac{q-1}{n}}\},$$

et ces solutions sont distinctes, puisque $\lambda^{j\frac{q-1}{n}} = \lambda^{l\frac{q-1}{n}}$, où $0 \leq j < n, 0 \leq l < n$, implique $\lambda^{(j-l)\frac{q-1}{n}} = 1$, donc $q-1 \mid (j-l)\frac{q-1}{n}$, soit $n \mid j-l$, où $|j-l| < n$, donc $j = l$. Ainsi $|C_n| = n$, et C_n est cyclique, engendré par $\lambda^{\frac{q-1}{n}}$.

□

Nous pouvons préciser la condition pour qu'existent des caractères d'ordre n.

Proposition 39. *Il existe un caractère d'ordre n sur $\mathbb{F}_q$ si et seulement si $q \equiv 1 \pmod{n}$.*

Démonstration. Supposons que $q \equiv 1 \pmod{n}$. La proposition 38 montre que C_n est cyclique d'ordre n, donc admet un générateur d'ordre n, qui est dans C.

Réciproquement, s'il existe un caractère χ d'ordre n, alors le sous-groupe engendré par χ est d'ordre n, et le théorème de Lagrange montre que $n \mid q-1$. □

La proposition suivante sert de lemme à la proposition 41.

Proposition 40. *Si $a \in \mathbb{F}_q^*$, et $a \neq 1$, alors il existe un caractère λ sur $\mathbb{F}_q$ tel que $\lambda(a) \neq 1$.*

Démonstration. Soit g un générateur de $\mathbb{F}_q^*$, et λ le caractère défini dans la proposition 37. Puisque $a \in \mathbb{F}_q^*$, il existe un entier k tel que $a = g^k$, et comme $a \neq 1$, $q-1 \nmid k$.

Alors $\lambda(a) = \lambda(g^k) = e^{2ik\frac{\pi}{q-1}} \neq 1$, puisque $\frac{k}{q-1} \notin \mathbb{Z}$. □

Proposition 41. *Si $a \in \mathbb{F}_q^*$, et $a \neq 1$, alors $\sum_{\chi \in C} \chi(a) = 0$.*

Démonstration. D'après le lemme précédent, il existe un caractère λ tel que $\lambda(a) \neq 1$. Soit $S = \sum_{\chi \in C} \chi(a)$. Alors, puisque l'application $\chi \mapsto \lambda\chi$ est une bijection de C sur C,

$$\begin{aligned}
\lambda(a)S &= \sum_{\chi \in C} \lambda(a)\chi(a) \\
&= \sum_{\chi \in C} (\lambda\chi)(a) \\
&= \sum_{\mu \in C} \mu(a) \qquad (\mu = \lambda\chi) \\
&= S.
\end{aligned}$$

Puisque $\lambda(a) \neq 1$, nous en concluons que $S = 0$. □

Les caractères sont utiles pour connaître le nombre de solutions de l'équation $x^n = a$ dans $\mathbb{F}_q$, comme nous allons le voir dans les trois propositions suivantes.

Proposition 42. *Si $a \in \mathbb{F}_q^*$, $n \mid q-1$ et $x^n = a$ n'est pas résoluble dans $\mathbb{F}_q$, alors il existe un caractère χ tel que*

(a) $\chi^n = \varepsilon$.

(b) $\chi(a) \neq 1$.

(Notons que la réciproque est vraie : en supposant (a), si $x^n = a,\ x \in \mathbb{F}_q^*$, alors $\chi(a) = \chi(x^n) = (\chi(x))^n = \chi^n(x) = \varepsilon(x) = 1$, donc (a) et (b) impliquent l'impossibilité de l'égalité $x^n = a$ dans $\mathbb{F}_q$.)

Démonstration. Soit g un générateur de $\mathbb{F}_q^*$, et λ le générateur de C associé, donné par la proposition 37 : l'ordre de λ est donc $q-1$. En utilisant $n \mid q-1$, définissons $\chi = \lambda^{\frac{q-1}{n}}$. Alors $\chi^n = \lambda^{q-1} = \varepsilon$, et ainsi (a) est vérifié.

Il existe un entier l tel que $a = g^l$. En raisonnant par l'absurde, si $n \mid l$, alors $l = kn,\ k \in \mathbb{Z}$, donc $(g^k)^n = g^l = a$, et l'équation $x^n = a$ admettrait une solution $x = g^k$. Par conséquent, $n \nmid l$.

$$\chi(g) = \lambda^{\frac{q-1}{n}}(g) = \lambda(g)^{\frac{q-1}{n}} = \left(e^{2i\frac{\pi}{q-1}}\right)^{\frac{q-1}{n}} = e^{2i\frac{\pi}{n}},$$

donc

$$\chi(a) = \chi(g^l) = e^{2i\pi\frac{l}{n}},$$

où $n \nmid l$, donc $\chi(a) \neq 1$, et (b) est vérifié. □

Si $a \in \mathbb{F}_q$, Notons $N(x^n = a)$ le nombre de solutions de l'équation $x^n = a$ dans $\mathbb{F}_q$.

A titre d'exemple, supposons que $q = p$ est premier. Vérifions alors que $N(x^2 = a) = 1 + \left(\frac{a}{p}\right)$, en faisant trois cas : si a est un carré de $\mathbb{F}_p^*$, alors $\left(\frac{a}{p}\right) = 1$, et $N(x^2 = a) = 2 = 1 + \left(\frac{a}{p}\right)$, et dans le cas contraire $\left(\frac{a}{p}\right) = -1$, donc $N(x^2 = a) = 0 = 1 + \left(\frac{a}{p}\right)$. Enfin, si $a = 0$, $1 + \left(\frac{a}{p}\right) = 1 = N(x^2 = 0)$.

Comme ε et le caractère de Legendre sont les seuls caractères dont l'ordre divise 2, on peut encore écrire cette formule sous la forme

$$N(x^2 = a) = \sum_{\chi^2 = \varepsilon} \chi(a).$$

Généralisons cette formule.

Proposition 43. *Si $n \mid q-1$, et $a \in \mathbb{F}_q$,*

$$N(x^n = a) = \sum_{\chi^n = \varepsilon} \chi(a).$$

Démonstration. La somme de l'énoncé s'effectue sur le groupe C_n des caractères χ tel que $\chi^n = \varepsilon$, ce qui revient à dire que l'ordre de χ divise n. Comme n divise $|C| = q-1$, la proposition 38 montre que $|C_n| = n$: il existe exactement n tels caractères.

- Si $a = 0$, $\varepsilon(0) = 1$, et $\chi(0) = 0$ si $\chi \neq \varepsilon$, donc $\sum_{\chi^n = \varepsilon} \chi(a) = 1 = N(x^n = a)$.
- Si $a \neq 0$, et si de plus $x^n = a$ est résoluble, alors il existe un élément $b \in \mathbb{F}_p^*$ tel que $b^n = a$. Si $\chi^n = \varepsilon$, alors $\chi(a) = \chi(b^n) = \chi(b)^n = \chi^n(b) = \varepsilon(b) = 1$. Ainsi $\sum_{\chi^n = \varepsilon} \chi(a) = |C_n| = n$. Comme $n \mid q-1$, alors $d = n \wedge (q-1) = n$ est d'après la proposition 24 le nombre de solutions de l'équation $x^n = a$. Dans ce cas

$$\sum_{\chi^n = \varepsilon} \chi(a) = n = N(x^n = a).$$

- Si $a \neq 0$ et si $x^n = a$ n'est pas résoluble, alors nous devons prouver $\sum_{\chi^n=\varepsilon} \chi(a) = 0$.
  Notons $S = \sum_{\chi^n=\varepsilon} \chi(a)$. D'après la proposition précédente, il existe un caractère ρ tel que $\rho^n = \varepsilon$ et $\rho(a) \neq 1$.
  Comme l'application $\chi \mapsto \rho\chi$ est une permutation de C_n,

$$\begin{aligned} \rho(a)S &= \sum_{\chi^n=\varepsilon} \rho(a)\chi(a) \\ &= \sum_{\chi^n=\varepsilon} (\rho\chi)(a) \\ &= \sum_{\mu^n=\varepsilon} \mu(a) \qquad (\mu = \rho\chi) \\ &= S \end{aligned}$$

  Puisque $\rho(a) \neq 1$, $S = 0$.

□

Remarque : si χ est un caractère d'ordre n, il engendre le sous-groupe C_n de C des caractères dont l'ordre divise n, et donc la formule précédente peut s'écrire

$$N(x^n = a) = \sum_{i=0}^{n-1} \chi^i(a).$$

Si on oublie l'hypothèse $n \mid q-1$, nous obtenons :

Proposition 44. *Soit $q = p^s$ une puissance d'un nombre premier, et $d = n \wedge (q-1)$. Si $a \in \mathbb{F}_q$, alors*

(a)

$$N(x^n = a) = N(x^d = a).$$

(b)

$$N(x^n = a) = \sum_{\chi^d=\varepsilon} \chi(a).$$

Démonstration. Soit d le pgcd de n et $p-1$.

(a)
- Si $a = 0$, 0 est la seule solution des équations $x^m = a$ ou $x^d = a$, donc $N(x^n = a) = N(x^d = a) = 1$.
- Si $a \in \mathbb{F}_q^*$ et si $x^n = a$ a une solution, d'après la proposition 24(b), le nombre de solutions de $x^n = a$ est $n \wedge (q-1) = d$, et le nombre de solutions de $x^d = a$ est $d \wedge (q-1) = d$. Ainsi $N(x^n = a) = N(x^d = a) = d$.
- Si $a \in \mathbb{F}_q^*$ et si $x^n = a$ n'a pas de solution, alors la proposition 1(a) montre que $a^{\frac{q-1}{d}} \neq 1$. Comme $d = d \wedge (q-1)$, la même proposition montre que $x^d = a$ n'a pas de solution. Ainsi $N(x^n = a) = N(x^d = a) = 0$.

(b) Comme $d \mid q-1$, la proposition précédente donne

$$N(x^n = a) = N(x^d = a) = \sum_{\chi^d=\varepsilon} \chi(a).$$

□

Proposition 45. *Supposons que $q \equiv 1 \pmod{n}$. Soit χ un caractère d'ordre n sur $\mathbb{F}_q^*$, et $a \in \mathbb{F}_q^*$. Alors*

$$\exists x \in \mathbb{F}_q^*,\ x^n = a \iff \chi(a) = 1.$$

Démonstration. La proposition 39 montre que l'existence d'un tel caractère χ sur $\mathbb{F}_q^*$ équivaut à $q \equiv 1 \pmod{n}$.

($\Rightarrow$) Si $x^n = a$, où $x \in \mathbb{F}_q^*$, alors $\chi(a) = \chi(x^n) = \chi(x)^n = \chi^n(x) = \varepsilon(x) = 1$.

($\Leftarrow$) Supposons $\chi(a) = 1$. Soit g un générateur de $\mathbb{F}_q^*$. Alors il existe un entier l tel que $a = g^l$. Notons λ le générateur (d'ordre $q-1$) du groupe des caractères donné par la proposition 39, caractérisé par $\lambda(g) = e^{\frac{2i\pi}{q-1}}$. Alors $\chi = \lambda^k$ pour un certain entier k.

Rappelons que l'ordre de λ^k est donné par

$$\mathrm{ord}(\lambda^k) = \frac{q-1}{(q-1) \wedge k}.$$

En effet, notons $d = (q-1) \wedge k$. Alors $\frac{q-1}{d} \wedge \frac{k}{d} = 1$. Pour tout $m \in \mathbb{Z}$,

$$\left(\lambda^k\right)^m = 1 \iff q-1 \mid km \iff \frac{q-1}{d} \mid \frac{k}{d}m \iff \frac{q-1}{d} \mid m.$$

Ainsi $n = \mathrm{ord}(\chi) = \frac{q-1}{d}$, où $d = (q-1) \wedge k$. Par conséquent, en utilisant $\frac{q-1}{d} \wedge \frac{k}{d} = 1$,

$$\begin{aligned}
\chi(a) = 1 &\iff \lambda^k(a) = 1 \\
&\iff e^{\frac{2i\pi kl}{q-1}} = 1 \\
&\iff q-1 \mid kl \\
&\iff \frac{q-1}{d} \mid \frac{k}{d}l \\
&\iff \frac{q-1}{d} \mid l \\
&\iff n \mid l
\end{aligned}$$

L'hypothèse $\chi(a) = 1$ montre donc que $l = qn$, pour un certain entier q, et donc $a = g^l = (g^q)^n$. Si on pose $x = g^q \in \mathbb{F}_q^*$, alors $a = x^n$ est bien une puissance n-ième dans $\mathbb{F}_q^*$. □

2.4 Sommes de Gauss.

Définissons d'abord la somme de Gauss associée à un caractère χ sur $\mathbb{F}_p$, où p est premier. Notons $\zeta = e^{\frac{2i\pi}{p}}$, et posons, pour $a \in \mathbb{F}_p$,

$$g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(t)\zeta^{at}. \tag{2.1}$$

(ζ^u a bien un sens si $u \in \mathbb{F}_p$: en effet, si $a, b \in \mathbb{Z}$ sont des représentants de $u \in \mathbb{F}_p$, alors $b = a + kp,\ k \in \mathbb{Z}$, donc $\zeta^b = \zeta^a(\zeta^p)^k = \zeta^a$.)

$g_a(\chi)$ s'appelle la somme de Gauss sur $\mathbb{F}_p$, relative au caractère χ.

Par exemple, si χ est le caractère quadratique relatif au nombre premier p, $g_a(\chi) = \sum_{t \in \mathbb{F}_p} \left(\frac{t}{p}\right)\zeta^{at}$. Ce sont ces sommes de Gauss que nous avions utilisées dans la preuve du théorème de réciprocité quadratique.

Généralisons maintenant les sommes de Gauss aux caractères χ sur $\mathbb{F}_q$, où $q = p^n$ est une puissance du nombre premier p. À cette fin, notons que l'application $\psi : \mathbb{F}_p \to \mathbb{C}^*$

définie par $\psi(\alpha) = \zeta_p^\alpha$ vérifie $\psi(\alpha+\beta) = \psi(\alpha)\psi(\beta)$, et donc $\psi : \mathbb{F}_p \to \mathbb{C}^*$ est un homomorphisme de groupes, du groupe $(\mathbb{F}_p, +)$ dans $(\mathbb{C}^*, \times)$.

Recherchons maintenant les homomorphismes de $\mathbb{F}_q$ dans $\mathbb{C}^*$.

Proposition 46. *Soit $\psi : \mathbb{F}_q \to \mathbb{C}^*$, où $q = p^n$, p premier.*

Alors ψ est un homomorphisme de $(\mathbb{F}_q, +)$ dans $(\mathbb{C}^*, \times)$ si et seulement s'il existe $\gamma \in \mathbb{F}_q$ tel que

$$\forall x \in \mathbb{F}_q,\ \psi(x) = \zeta^{\mathrm{tr}(\gamma x)}, \tag{2.2}$$

où $\zeta = e^{\frac{2i\pi}{p}}$, et $\mathrm{tr}(x) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)$ $(x \in \mathbb{F}_q)$.

Démonstration. Soit ψ est un homomorphisme de $(\mathbb{F}_q, +)$ dans $(\mathbb{C}^*, \times)$. Alors $\psi(0) = 1$, et $\psi(a\alpha) = \psi(\alpha)^a$, pour tout $\alpha \in \mathbb{F}_q$ et tout $a \in \mathbb{Z}$.

Soit $(\omega_1, \ldots, \omega_n)$ une base de $\mathbb{F}_q = \mathbb{F}_{p^n}$ sur $\mathbb{F}_p$. La caractéristique du corps $\mathbb{F}_q$ étant égale à p,

$$\psi(\omega_k)^p = \psi(p\omega_k) = \psi(0) = 1 \qquad (1 \le k \le n).$$

Ainsi $\psi(\omega_k)$ est une racine p-ième de l'unité, de la forme

$$\psi(\omega_k) = \zeta^{c_k}, \qquad c_k \in \{0, , \ldots, p-1\}. \tag{2.3}$$

Puisque $\zeta^{c_k} = \zeta^{c_k + lp}$, on peut donner un sens à $\zeta^{[c_k]}$, où $[c_k]$ est la classe de c_k modulo p. Alors $\psi(\omega_k) = \zeta^{[c_k]}$.

Considérons l'application

$$\varphi \left\{ \begin{array}{ccc} \mathbb{F}_q & \to & (\mathbb{F}_p)^n \\ \alpha & \mapsto & (\mathrm{tr}(\alpha\omega_1), \ldots, \mathrm{tr}(\alpha\omega_n)). \end{array} \right.$$

où tr désigne l'application $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$.

Montrons que l'application $\mathbb{F}_p$-linéaire φ est bijective.

Si $\alpha \in \ker(\varphi)$, alors $\mathrm{tr}(\alpha\omega_1) = \ldots = \mathrm{tr}(\alpha\omega_n) = 0$. Si y est un élément arbitraire de $\mathbb{F}_q$, alors $y = b_1\omega_1 + \cdots + b_n\omega_n$, où $b_1, \ldots, b_n \in \mathbb{F}_p$. Alors $\mathrm{tr}(\alpha y) = b_1\mathrm{tr}(\alpha\omega_1) + \cdots + b_n\mathrm{tr}(\alpha\omega_n) = 0$, ce qui donne

$$\forall y \in \mathbb{F}_q,\ \mathrm{tr}(\alpha y) = 0.$$

En raisonnant par l'absurde, supposons que $\alpha \neq 0$. Puisque l'application $\mathrm{tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p$ est surjective (Proposition 31), il existe un élément $\delta \in \mathbb{F}_q$ tel que $\delta = 1$. Pour $y = \delta\alpha^{-1}$, alors $0 = \mathrm{tr}(\alpha y) = \mathrm{tr}(\delta) = 1$. C'est une contradiction, donc $\alpha = 0$. Ceci montre que $\ker(\varphi) = \{0\}$.

De plus $\dim_{\mathbb{F}_p}(\mathbb{F}_q) = \dim_{\mathbb{F}_p}(\mathbb{F}_p)^n = n$, donc φ est une bijection. La surjectivité de φ montre qu'il existe $\gamma \in \mathbb{F}_q$ tel que

$$\mathrm{tr}(\gamma\omega_k) = [c_k], \qquad k = 1, \ldots, n. \tag{2.4}$$

Si x est un élément arbitraire de $\mathbb{F}_q$, nous pouvons écrire x sous la forme $x = a_1\omega_1 + \cdots + a_n\omega_n$, où $a_1, \ldots, a_k \in \mathbb{F}_p$. En utilisant les égalités (2.3) et (2.4), nous obtenons

$$\begin{aligned} \psi(x) &= \psi(a_1\omega_1 + \cdots + a_n\omega_n) \\ &= \psi(\omega_1)^{a_1} \cdots \psi(\omega_n)^{a_n} \\ &= \zeta^{a_1\mathrm{tr}(\gamma\omega_1) + \cdots + a_n\mathrm{tr}(\gamma\omega_n)} \\ &= \zeta^{\mathrm{tr}(\gamma x)}. \end{aligned}$$

Réciproquement, vérifions que, $\gamma \in \mathbb{F}_q$ étant donné, l'application $\psi : \mathbb{F}_q \to \mathbb{C}^*$ défini par $\psi(x) = \zeta^{\mathrm{tr}(\gamma x)}$ est bien un homomorphisme de groupes.

Si $x, y \in \mathbb{F}_q$, alors

$$\psi(x+y) = \zeta^{\mathrm{tr}(\gamma(x+y))} = \zeta^{\mathrm{tr}(\gamma x)+\mathrm{tr}(\gamma x)} = \zeta^{\mathrm{tr}(\gamma x)}\zeta^{\mathrm{tr}(\gamma y)} = \psi(x)\psi(y).$$

□

Notons maintenant ψ l'homomorphisme défini par $\psi(x) = \zeta^{\mathrm{tr}(x)}$, $x \in \mathbb{F}_q$. Donnons quelques propriétés de ψ.

Proposition 47. *L'application $\psi : \mathbb{F}_q \to \mathbb{C}^*$ définie par $\psi(x) = \zeta^{\mathrm{tr}(x)}$ vérifie*

(a) $\psi(\alpha+\beta) = \psi(\alpha)\psi(\beta)$ $(\alpha, \beta \in \mathbb{F}_q)$.

(b) Il existe un $\alpha \in \mathbb{F}_q$ tel que $\psi(\alpha) \neq 1$.

(c) $\sum_{\alpha \in \mathbb{F}_q} \psi(\alpha) = 0$.

Démonstration.

(a) Cette relation a été prouvée dans la proposition 46.

(b) L'application $\mathrm{tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p$ est surjective (Proposition 31). Par conséquent, il existe $\alpha \in \mathbb{F}_q$ tel que $\mathrm{tr}(\alpha) = 1$. Alors $\psi(\alpha) = \zeta \neq 1$.

(c) Soit $S = \sum_{\alpha \in \mathbb{F}_q} \psi(\alpha)$, et $\beta \in \mathbb{F}_q$ tel que $\psi(\beta) \neq 1$. Alors

$$\psi(\beta)S = \sum_{\alpha \in \mathbb{F}_q} \psi(\beta)\psi(\alpha) = \sum_{\alpha \in \mathbb{F}_q} \psi(\beta+\alpha) = \sum_{\gamma \in \mathbb{F}_q} \psi(\gamma) = S,$$

donc $S = 0$. □

Proposition 48. *Si $\alpha, x, y \in \mathbb{F}_q$, alors*

$$\frac{1}{q} \sum_{\alpha \in \mathbb{F}_q} \psi(\alpha(x-y)) = \delta(x,y),$$

où $\delta(x,y) = 1$ si $x = y$ et 0 sinon.

Démonstration. Si $x = y$, alors

$$\sum_{\alpha \in \mathbb{F}_q} \psi(\alpha(x-y)) = \sum_{\alpha \in \mathbb{F}_q} \psi(0) = q.$$

Si $x \neq y$, alors le changement d'indice $\beta = \alpha(x-y)$, où $x - y \neq 0$, donne

$$\sum_{\alpha \in \mathbb{F}_q} \psi(\alpha(x-y)) = \sum_{\beta \in \mathbb{F}_q} \psi(\beta) = 0,$$

d'après la proposition 47(c). □

La définition 2.1 se généralise aux caractères sur $\mathbb{F}_q$, où $q = p^s$, sous la forme

$$g_\alpha(\chi) = \sum_{t \in \mathbb{F}_q} \chi(t)\psi(\alpha t) = \sum_{t \in \mathbb{F}_q} \chi(t)\zeta^{\mathrm{tr}(\alpha t)}, \qquad \text{où } \zeta = e^{\frac{2i\pi}{p}}, \mathrm{tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}. \tag{2.5}$$

Si $q = p$ est premier, et $\alpha = a \in \mathbb{F}_p$, alors $\mathrm{tr}(ay) = at$, et nous obtenons bien $g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(t)\zeta^{at}$ ce qui montre que (2.5) généralise bien la définition (2.1).

Précisons quelques valeurs de $g_\alpha(\chi)$.

Proposition 49. *Soit $\alpha \in \mathbb{F}_q$, et χ un caractère sur $\mathbb{F}_q$.*

(a) Si $\alpha \neq 0$ et $\chi = \varepsilon$, alors $g_\alpha(\varepsilon) = 0$.

(b) Si $\alpha = 0$ et $\chi = \varepsilon$, alors $g_0(\varepsilon) = q$.

(c) Si $\alpha = 0$ et $\chi \neq \varepsilon$, alors $g_0(\chi) = 0$.

Démonstration. (a) Ici $\alpha \neq 0$. En utilisant la proposition 47(c), nous obtenons

$$\begin{aligned} g_\alpha(\varepsilon) &= \sum_{t\in\mathbb{F}_q} \varepsilon(t)\zeta^{\mathrm{tr}(\alpha t)} \\ &= \sum_{t\in\mathbb{F}_q} \zeta^{\mathrm{tr}(\alpha t)} \\ &= \sum_{u\in\mathbb{F}_q} \zeta^{\mathrm{tr}(u)} \qquad (u = \alpha t) \\ &= \sum_{u\in\mathbb{F}_q} \psi(u) \\ &= 0 \end{aligned}$$

(b) Comme $\alpha = 0$,

$$g_0(\varepsilon) = \sum_{t\in\mathbb{F}_q} \varepsilon(t) = \sum_{t\in\mathbb{F}_q} 1 = q.$$

(c) Si $\chi \neq \varepsilon$, la proposition 35 donne

$$g_0(\chi) = \sum_{t\in\mathbb{F}_q} \chi(t) = 0.$$

□

Proposition 50. *Si $\alpha \in \mathbb{F}_q^*$, alors $g_\alpha(\chi) = \chi(\alpha^{-1})g_1(\chi) = \overline{\chi(\alpha)}g_1(\chi)$.*

Démonstration. Si $\alpha \in \mathbb{F}_q^*$,

$$\begin{aligned} \chi(\alpha)g_\alpha(\chi) &= \sum_{t\in\mathbb{F}_q} \chi(\alpha)\chi(t)\psi(\alpha t) \\ &= \sum_{t\in\mathbb{F}_q} \chi(\alpha t)\psi(\alpha t) \\ &= \sum_{s\in\mathbb{F}_q} \chi(s)\psi(s) \qquad (s = \alpha t) \\ &= g(\chi). \end{aligned}$$

Puisque $|\chi(\alpha)| = 1$, $\chi(\alpha)^{-1} = \overline{\chi(\alpha)}$, alors

$$g_\alpha(\chi) = \overline{\chi(\alpha)}g(\chi).$$

□

Nous noterons par la suite $g(\chi) = g_1(\chi)$.

Proposition 51. *Si $\chi \neq \varepsilon$ est un caractère sur $\mathbb{F}_q$, alors $|g(\chi)| = \sqrt{q}$.*

Démonstration. Nous évaluons la somme $S = \sum_{a\in\mathbb{F}_q} g_a(\chi)\overline{g_a(\chi)}$ de deux façons.

- Comme $\chi \neq \varepsilon$, la proposition 49(c) donne $g_0(\chi) = 0$. Si $a \in \mathbb{F}_q^*$, alors $g_a(\chi) = \chi(a^{-1})g(\chi)$ (proposition 50), et $\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = \chi(a)\overline{g(\chi)}$. Par conséquent,

$$\begin{aligned} S &= \sum_{a\in\mathbb{F}_q^*} \chi(a^{-1})g(\chi)\chi(a)\overline{g(\chi)} \\ &= \sum_{a\in\mathbb{F}_q^*} |g(\chi)|^2 \\ &= (q-1)|g(\chi)|^2 \end{aligned}$$

- De plus, puisque $\psi(a(x-y)) = \psi(ax)\psi(ay)^{-1} = \psi(ax)\overline{\psi(ay)}$,

$$g_a(\chi)\overline{g_a(\chi)} = \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q} \chi(x)\overline{\chi(y)}\psi(a(x-y)).$$

  Par conséquent,

$$\begin{aligned} S &= \sum_{a\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q} \chi(x)\overline{\chi(y)}\psi(a(x-y)) \\ &= \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q} \chi(x)\overline{\chi(y)} \left(\sum_{a\in\mathbb{F}_q} \psi(a(x-y))\right) \end{aligned}$$

  D'après la proposition 48,

$$\sum_{a\in\mathbb{F}_q} \psi(a(x-y)) = q\delta(x,y),$$

  donc,

$$\begin{aligned} S &= q\sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q} \chi(x)\overline{\chi(y)}\delta(x,y) \\ &= q\sum_{x\in\mathbb{F}_q} \chi(x)\overline{\chi(x)} \end{aligned}$$

  Puisque $\chi(x)\overline{\chi(x)} = 1$ si $x \neq 0$, et $\chi(x)\overline{\chi(x)} = 0$ si $x = 0$, nous obtenons

$$S = q(q-1).$$

La comparaison de ces deux résultats donne

$$(q-1)|g(\chi)|^2 = (q-1)q,$$

donc

$$|g(\chi)| = \sqrt{q}.$$

□

Exprimons le lien entre $\overline{g(\chi)}$ et $g(\overline{\chi})$. Ici $\overline{\chi}$ est le caractère qui envoie tout $a \in \mathbb{F}_q$ sur $\overline{\chi(a)} = \chi(a)^{-1} = \chi^{-1}(a)$, donc $\overline{\chi} = \chi^{-1}$.

Proposition 52. *Si χ est un caractère sur $\mathbb{F}_q$, alors*

$$\overline{g(\chi)} = \chi(-1)g(\overline{\chi}).$$

Démonstration. Puisque $(-1)^2 = 1$, $(\chi(-1))^2 = 1$, donc $\chi(-1) = \pm 1$ est réel, et ainsi $\overline{\chi(-1)} = \chi(-1)$. Ceci donne

$$\begin{aligned}
\overline{g(\chi)} &= \sum_{t\in\mathbb{F}_q} \overline{\chi(t)}\zeta_p^{-\mathrm{tr}(t)} \\
&= \sum_{t\in\mathbb{F}_q} \overline{\chi(-1)\chi(-t)}\zeta_p^{-\mathrm{tr}(t)} \\
&= \chi(-1)\sum_{t\in\mathbb{F}_q} \overline{\chi(-t)}\zeta_p^{\mathrm{tr}(-t)} \\
&= \chi(-1)\sum_{s\in\mathbb{F}_q} \overline{\chi(s)}\zeta_p^{\mathrm{tr}(s)} \qquad (s=-t) \\
&= \chi(-1)g(\overline{\chi}).
\end{aligned}$$

□

Remarque : si λ est le caractère de Legendre défini par $\lambda(a) = \left(\frac{a}{p}\right)$, alors λ est d'ordre 2, donc $\lambda = \lambda^{-1} = \overline{\lambda}$. Ainsi

$$g(\lambda)^2 = g(\lambda)g(\overline{\lambda}) = \lambda(-1)g(\lambda)\overline{g(\lambda)} = \lambda(-1)p = (-1)^{\frac{p-1}{2}}p.$$

On retrouve ainsi le calcul de $g^2 = (-1)^{\frac{p-1}{2}}p$ dans le chapitre "Loi de réciprocité quadratique".

2.5 Sommes de Jacobi.

Les sommes de Jacobi interviennent naturellement dans le calcul du nombre de points de courbes algébriques sur $\mathbb{F}_q$. Notons $N(x^3+y^3=1)$ le nombre de solutions $(x,y)\in\mathbb{F}_q^2$ de la cubique Γ d'équation $x^3+y^3=1$ sur $\mathbb{F}_q$.

Alors

$$N(x^3+y^3=1) = \sum_{a+b=1} N(x^3=a)N(y^3=b).$$

En effet, si on note $A_k = \{x\in\mathbb{F}_q \,|\, x^3 = k\}$ pour tout $k\in\mathbb{F}_q$, alors

$$\begin{aligned}
\Gamma &= \{(x,y)\in\mathbb{F}_q^2 \mid x^3+y^3=1\} \\
&= \coprod_{(a,b)\in\mathbb{F}_q^2,\, a+b=1} \{(x,y)\in\mathbb{F}_p^2 \mid x^3=a \text{ et } y^3=b\} \\
&= \coprod_{(a,b)\in\mathbb{F}_q^2,\, a+b=1} A_a\times A_b.
\end{aligned}$$

Comme $|A_k| = N(x^3=k)$, nous obtenons bien le résultat annoncé.

• Si $q\equiv 2 \pmod 3$, d'après la proposition 24 et l'exemple 2 qui suit, nous savons que $N(x^3=a)=1$ pour tout $a\in\mathbb{F}_q$. Alors, d'après la formule précédente, $N(x^3+y^3=1) = q$.

• Supposons maintenant que $q \equiv 1 \pmod 3$. Comme $3 \mid q-1$, Il existe alors au moins un caractère d'ordre 3, et même exactement 2, d'après la proposition 38. Soit χ un tel caractère d'ordre 3 (appelé caractère cubique). Alors χ^2 est d'ordre 3, et $\{\varepsilon, \chi, \chi^2\}$ est l'ensemble des caractères dont l'ordre divise 3. La proposition 43 donne alors

$$N(x^3 = a) = 1 + \chi(a) + \chi^2(a).$$

Par conséquent,

$$\begin{aligned} N(x^3 + y^3 = 1) &= \sum_{a+b=1} \sum_{i=0}^{2} \chi^i(a) \sum_{j=0}^{2} \chi^j(b) \\ &= \sum_{i=0}^{2} \sum_{j=0}^{2} \left(\sum_{a+b=1} \chi^i(a)\chi^j(b) \right). \end{aligned}$$

Ceci conduit à la définition suivante.

Définition 3. *Soient χ et λ des caractères sur $\mathbb{F}_q$. Alors*

$$J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$$

s'appelle la somme de Jacobi associée à χ, λ.

Avec cette notation, le résultat précédent s'écrit

$$N(x^3 + y^3 = 1) = \sum_{i=0}^{2} \sum_{j=0}^{2} J(\chi^i, \chi^j). \tag{2.6}$$

Donnons les propriétés usuelles de ces sommes de Jacobi.

Proposition 53. *Soit χ un caractère non trivial sur $\mathbb{F}_q$. Alors*

(a) $J(\varepsilon, \varepsilon) = q$.

(b) $J(\varepsilon, \chi) = 0$.

(c) $J(\chi, \chi^{-1}) = -\chi(-1)$.

Démonstration. (a) Puisque le cardinal de l'ensemble $\{(a, b) \in \mathbb{F}_q^2 \mid a + b = 1\}$ est égal à q,

$$J(\varepsilon, \varepsilon) = \sum_{a+b=1} 1 = q.$$

(b) D'après la proposition 35,

$$J(\varepsilon, \chi) = \sum_{a+b=1} \chi(a) = \sum_{a \in \mathbb{F}_q} \chi(a) = 0.$$

(c) Remarquons que

$$\begin{aligned} J(\chi, \chi^{-1}) &= \sum_{a+b=1} \chi(a)\chi^{-1}(b) \\ &= \sum_{a+b=1,\, b \neq 0} \chi\left(\frac{a}{b}\right) \\ &= \sum_{a \neq 1} \chi\left(\frac{a}{1-a}\right). \end{aligned}$$

Comme l'application homographique

$$\left\{ \begin{array}{ccc} \mathbb{F}_q \setminus \{1\} & \to & \mathbb{F}_q \setminus \{-1\} \\ a & \mapsto & \frac{a}{1-a} \end{array} \right.$$

est une bijection, d'application réciproque $\left\{ \begin{array}{ccc} \mathbb{F}_q \setminus \{-1\} & \to & \mathbb{F}_q \setminus \{1\} \\ b & \mapsto & \frac{b}{1+b} \end{array} \right.$, le changement d'indice $b = \frac{a}{1-a}$ donne

$$\begin{aligned} J(\chi, \chi^{-1}) &= \sum_{a \neq 1} \chi\left(\frac{a}{1-a}\right) \\ &= \sum_{b \neq -1} \chi(b) \\ &= \sum_{b \in \mathbb{F}_p} \chi(b) - \chi(-1) \\ &= -\chi(-1). \end{aligned}$$

□

La proposition suivante donne de lien entre les sommes de Jacobi et les sommes de Gauss.

Proposition 54. *Si χ, λ sont des caractères sur $\mathbb{F}_q$ tels que $\chi \neq \varepsilon, \lambda \neq \varepsilon, \chi\lambda \neq \varepsilon$, alors*

$$J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$

Démonstration. En notant comme d'habitude $\psi(x) = \zeta_p^{\mathrm{tr}(x)}$ pour $x \in \mathbb{F}_q$,

$$\begin{aligned} g(\chi)g(\lambda) &= \left(\sum_{x \in \mathbb{F}_q} \chi(x)\psi(x) \right) \left(\sum_{y \in \mathbb{F}_q} \lambda(y)\psi(y) \right) \\ &= \sum_{(x,y) \in \mathbb{F}_q^2} \chi(x)\lambda(y)\psi(x+y) \\ &= \sum_{t \in \mathbb{F}_q} \left(\sum_{x+y=t} \chi(x)\lambda(y) \right) \psi(t). \end{aligned}$$

Si $t = 0$, alors

$$\sum_{x+y=0} \chi(x)\lambda(y) = \sum_{x \in \mathbb{F}_q} \chi(x)\lambda(-x) = \lambda(-1) \sum_{x \in \mathbb{F}_q} (\chi\lambda)(x) = 0,$$

puisque $\chi\lambda \neq \varepsilon$.

Si $t \neq 0$, l'application

$$\left\{ \begin{array}{ccc} \{(x', y') \in \mathbb{F}_q^2 \mid x' + y' = 1\} & \to & \{(x, y) \in \mathbb{F}_q^2 \mid x + y = t\} \\ (x', y') & \mapsto & (x, y) = (tx', ty') \end{array} \right.$$

étant bijective, le changement d'indices $(x, y) = (tx', ty')$ donne

$$\begin{aligned} \sum_{x+y=t} \chi(x)\lambda(y) &= \sum_{x'+y'=1} \chi(tx')\lambda(ty') \\ &= (\chi\lambda)(t)J(\chi, \lambda). \end{aligned}$$

Par conséquent,

$$\begin{aligned} g(\chi)g(\lambda) &= \sum_{t\in\mathbb{F}_q^*}\left(\sum_{x+y=t}\chi(x)\lambda(y)\right)\psi(t) \\ &= J(\chi,\lambda)\sum_{t\in\mathbb{F}_q^*}(\chi\lambda)(t)\psi(t) \\ &= J(\chi,\lambda)g(\chi\lambda). \end{aligned}$$

La proposition 51 montre que si $\chi \neq \varepsilon, g(\chi) \neq 0$. Comme ici $\chi\lambda \neq \varepsilon$, $g(\chi\lambda) \neq 0$, donc

$$J(\chi,\lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$

□

Nous en tirons le corollaire suivant

Proposition 55. *Soient χ, λ des caractères sur $\mathbb{F}_q$. Si χ, λ et $\chi\lambda$ sont différents de ε, alors*

$$|J(\chi,\lambda)| = \sqrt{q}.$$

Démonstration. Comme $|g(\chi)| = \sqrt{q}$ pour tout caractère $\chi \neq \varepsilon$ (proposition 51), nous obtenons

$$|J(\chi,\lambda)| = \frac{|g(\chi)|\,|g(\lambda)|}{|g(\chi\lambda)|} = \frac{\sqrt{q}\sqrt{q}}{\sqrt{q}} = \sqrt{q}.$$

□

Reprenons l'évaluation de $N(x^3+y^3=1)$ pour $q \equiv 1 \pmod 3$. L'égalité (2.6) devient, en utilisant la proposition 53, ainsi que $\chi^2 = \chi^{-1}$,

$$\begin{aligned} N(x^3+y^3=1) &= \sum_{i=0}^{2}\sum_{j=0}^{2} J(\chi^i,\chi^j) \\ &= J(\varepsilon,\varepsilon) + J(\varepsilon,\chi) + J(\varepsilon,\chi^2) + \\ &\quad J(\chi,\varepsilon) + J(\chi,\chi) + J(\chi,\chi^2) + \\ &\quad J(\chi^2,\varepsilon) + J(\chi^2,\chi) + J(\chi^2,\chi^2) \\ &= q - \chi(-1) - \chi^2(-1) + J(\chi,\chi) + J(\chi^2,\chi^2) \end{aligned}$$

Comme $-1 = (-1)^3$, nous avons $\chi(-1) = \chi^2(-1) = 1$. De plus $J(\chi^2,\chi^2) = J(\overline{\chi},\overline{\chi}) = \overline{J(\chi,\chi)}$, donc

$$N(x^3+y^3=1) = q - 2 + 2\,\mathrm{Re}(J(\chi,\chi)). \tag{2.7}$$

Nous ne connaissons pas explicitement $J(\chi,\chi)$ pour toutes les valeurs de q. Néanmoins $|\mathrm{Re}(J(\chi,\chi))| \leq |J(\chi,\chi)| = \sqrt{q}$, donc

$$|N(x^3+y^3=1) - (q-2)| \leq 2\sqrt{q}.$$

qui donne l'ordre de grandeur de $N(x^3+y^3=1)$.

Un calcul semblable permet d'obtenir explicitement $N(x^2+y^2=1)$, que nous présentons en supposant ici $q=p$ premier. Soit χ l'unique caractère d'ordre 2 : $\chi(a)=\left(\frac{a}{p}\right)$ pour tout $a\in\mathbb{F}_p$.

$$\begin{aligned} N(x^2+y^2=1) &= \sum_{a+b=1} N(x^2=a)N(x^2=b) \\ &= \sum_{a+b=1}(1+\chi(a))(1+\chi(b)) \\ &= p+\sum_{a\in\mathbb{F}_p}\chi(a)+\sum_{b\in\mathbb{F}_p}\chi(b)+\sum_{a+b=1}\chi(a)\chi(b) \\ &= p+J(\chi,\chi). \end{aligned}$$

Comme $\chi=\chi^{-1}$, la proposition 53 donne $J(\chi,\chi)=-\chi(-1)=-\left(\frac{-1}{p}\right)=-(-1)^{\frac{p-1}{2}}$. Ainsi

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

Autrement dit

$$\begin{aligned} N(x^2+y^2=1)&=p-1 \qquad \text{si } p\equiv 1 \pmod 4, \\ N(x^2+y^2=1)&=p+1 \qquad \text{si } p\equiv 3 \pmod 4. \end{aligned}$$

La proposition 55 permet de retrouver le théorème des deux carrés :

Proposition 56. *Si $p\equiv 1 \pmod 4$, alors il existe des entiers a et b tels que $p=a^2+b^2$.*

Démonstration. Comme $p\equiv 1 \pmod 4$, il existe d'après la proposition 39 un caractère χ d'ordre 4 sur $\mathbb{F}_p$. Pour tout $a\in\mathbb{F}_p^*$, $(\chi(a))^4=\chi^4(a)=\varepsilon(a)=1$, donc $\chi(a)\in\{1,i,-1,-i\}$, et $\chi(0)=0$. Par conséquent, $J(\chi,\chi)=\sum_{a+b=1}\chi(a)\chi(b)\in\mathbb{Z}[i]$. Ainsi $J(\chi,\chi)$ s'écrit sous la forme $J(\chi,\chi)=a+bi,\ a,b\in\mathbb{Z}$. La proposition 55 montre que

$$a^2+b^2=\mathrm{N}(a+bi)=\mathrm{N}(J(\chi,\chi))=p.$$

□

On obtient de même la proposition suivante, déjà prouvée dans la section 1.8 du chapitre "Entiers de Gauss".

Proposition 57. *Si $p\equiv 1 \pmod 3$, alors il existe des entiers a et b tels que $p=a^2-ab+b^2$.*

Démonstration. Comme $p\equiv 1 \pmod 3$, il existe un caractère χ d'ordre 3. Pour tout $a\in\mathbb{F}_p^*$, $(\chi(a))^3=1$, $\chi(a)\in\{1,\omega,\omega^2\}$, donc $J(\chi,\chi)\in\mathbb{Z}[\omega]$. Ainsi $J(\chi,\chi)=a+b\omega,\ a,b\in\mathbb{Z}$, et $p=\mathrm{N}(J(\chi,\chi))=a^2-ab+b^2$. □

Nous avons vu dans cette même section que ceci entraînait, pour les premiers $p\equiv 1 \pmod 3$, l'existence d'entiers x,y tels que $p=x^2+3y^2$.

Soit χ un caractère d'ordre 3 sur $\mathbb{F}_q$ (ce qui n'est possible que si $q\equiv 1 \pmod 3$). Alors $\chi\neq\varepsilon, \chi^2\neq\varepsilon$. La proposition 18 donne alors

$$g(\chi)^2=J(\chi,\chi)g(\chi^2).$$

En multipliant cette relation par $g(\chi)$, nous obtenons, en utilisant $\chi(-1)g(\overline{\chi}) = \overline{g(\chi)}$ (proposition 52), où ici $\chi(-1) = 1$,

$$\begin{aligned} g(\chi)^3 &= J(\chi,\chi)g(\chi)g(\chi^2) \\ &= J(\chi,\chi)g(\chi)g(\overline{\chi}) \\ &= J(\chi,\chi)g(\chi)\overline{g(\chi)} \\ &= q\,J(\chi,\chi) \end{aligned}$$

Nous avons prouvé la proposition suivante.

Proposition 58. *Si χ est un caractère d'ordre 3 sur $\mathbb{F}_q$, alors*

$$g(\chi)^3 = q\,J(\chi,\chi).$$

Généralisons :

Proposition 59. *Supposons que χ est un caractère d'ordre $n > 2$ sur $\mathbb{F}_q$. Alors*

$$g(\chi)^n = \chi(-1)qJ(\chi,\chi)\cdots J(\chi,\chi^{n-2}).$$

Démonstration. Ici $\chi, \chi^2, \ldots, \chi^{n-1}$ sont différents de ε. Donc, comme précédemment, $g(\chi)^2 = J(\chi,\chi)g(\chi^2)$.

Supposons, à titre d'hypothèse de récurrence, que

$$g(\chi)^k = J(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{k-1})g(\chi^k),$$

pour un entier k tel que $2 \leq k < n-1$. En multipliant par $g(\chi)$, on obtient

$$g(\chi)^{k+1} = J(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{k-1})g(\chi)g(\chi^k).$$

Comme $k+1 < n$, χ, χ^k et χ^{k+1} sont différents de ε. Alors la proposition 54 montre que

$$g(\chi)g(\chi^k) = J(\chi,\chi^k)g(\chi^{k+1}).$$

Par conséquent,

$$g(\chi)^k = J(\chi,\chi)J(\chi,\chi^2)\cdots J(\chi,\chi^{k-1})J(\chi,\chi^k)g(\chi^{k+1}),$$

ce qui achève la récurrence. Ainsi la propriété est vraie jusqu'à la valeur $k = n-1$. Donc

$$g(\chi)^{n-1} = J(\chi,\chi)\cdots J(\chi,\chi^{n-2})g(\chi^{n-1}). \tag{2.8}$$

Enfin, comme $\chi^{n-1} = \chi^{-1} = \overline{\chi}$ (et $\chi(-1) = \pm 1$), nous obtenons, en utilisant les propositions 52 et 55,

$$g(\chi)g(\chi^{n-1}) = g(\chi)g(\overline{\chi}) = \chi(-1)g(\chi)\overline{g(\chi)} = \chi(-1)q.$$

En multipliant une dernière fois l'égalité (2.8) par $g(\chi)$, nous obtenons

$$g(\chi)^n = \chi(-1)qJ(\chi,\chi)\cdots J(\chi,\chi^{n-2}).$$

□

Nous pouvons maintenant compléter le calcul de $N(x^3+y^3=1) = p-2+2\,\mathrm{Re}(J(\chi,\chi))$ dans le cas où $q=p$ est un nombre premier. Nous savons que, χ étant un caractère d'ordre 3, $J(\chi,\chi) \in \mathbb{Z}[\omega]$, soit

$$J(\chi,\chi) = a + b\omega,\ a,b \in \mathbb{Z}.$$

Proposition 60. *Supposons que $p \equiv 1 \pmod 3$ et que χ est un caractère cubique sur $\mathbb{F}_p$. Soient a, b les entiers tels que $J(\chi,\chi) = a + b\omega$. Alors*

(a) $b \equiv 0 \pmod 3$,

(b) $a \equiv -1 \pmod 3$.

Démonstration. Nous utilisons des congruences modulo 3 dans l'anneau des entiers algébriques.

$$g(\chi)^3 = \left(\sum_{t\in\mathbb{F}_p} \chi(t)\zeta^t\right)^3 \equiv \sum_{t\in\mathbb{F}_p} \chi(t)^3\zeta^{3t} \pmod 3.$$

Puisque $\chi(0) = 0$, et $\chi(t)^3 = 1$ pour $t \neq 0$, nous obtenons

$$\sum_{t\in\mathbb{F}_p} \chi(t)^3\zeta^{3t} = \sum_{t\in\mathbb{F}_p^*} \zeta^{3t} = -1.$$

La proposition 58 donne alors, puisque $p \equiv 1 \pmod 3$,

$$g(\chi)^3 = pJ(\chi,\chi) \equiv a + b\omega \equiv -1 \pmod 3.$$

Le même calcul appliqué à $\overline{\chi}$ donne $g(\overline{\chi})^3 \equiv -1 \pmod 3$, et $\overline{g(\chi)} = g(\overline{\chi})$ (proposition 52). Le passage au conjugué dans la relation précédente donne alors

$$g(\overline{\chi})^3 = pJ(\overline{\chi},\overline{\chi}) \equiv a + b\overline{\omega} \equiv -1 \pmod 3.$$

En soustrayant ces deux congruences, nous obtenons $b(\omega-\overline{\omega}) \equiv 0 \pmod 3$, soit $bi\sqrt{3} \equiv 0 \pmod 3$. L'élévation au carré donne $-3b^2 \equiv 0 \pmod 9$, et cette congruence est alors vraie dans l'anneau $\mathbb{Z}$. Par conséquent $3 \mid b^2$ dans $\mathbb{Z}$, et $3 \mid b$, ce qui prouve (a).

Comme $b \equiv 0 \pmod 3$ et $a + b\omega \equiv -1 \pmod 3$, nous obtenons $a \equiv -1 \pmod 3$. □

Nous pouvons maintenant prouver le beau résultat dû à Gauss.

Proposition 61. *(a) Soit $p \equiv 1 \pmod 3$ un nombre premier. Alors il existe un et un seul couple d'entiers (A,B) tel que $4p = A^2 + 27B^2$, $A \equiv 1 \pmod 3, B > 0$.*

(b) Cet unique élément A vérifie

$$N(x^3 + y^3 = 1) = p - 2 + A.$$

Démonstration. (a) • Existence.

Comme $p \equiv 1 \pmod 3$, il existe un caractère χ d'ordre 3. Il vérifie $J(\chi,\chi) = a+b\omega$ et $|J(\chi,\chi)|^2 = p$, donc $p = a^2 - ab + b^2$, soit $4p = (2a-b)^2 + 3b^2$. La proposition 60 montre que $b \equiv 0, a \equiv -1 \pmod 3$. Posons alors $A = 2a - b$, et $B = \frac{|b|}{3}$, avec $B \neq 0$ puisque p est premier. Alors A, B sont entiers, et

$$4p = A^2 + 27B^2, \qquad A \equiv 1 \pmod 3,\ B > 0.$$

• Unicité.

Supposons que $4p = A^2+27B^2 = C^2+27D^2$, où $A \equiv C \equiv 1 \pmod 3, B > 0, D > 0$. Nous allons montrer que $A = C, B = D$.
Comme $\omega = e^{\frac{2i\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, alors $i\sqrt{3} = 2\omega + 1$, et pour tout couple d'entiers x, y, $x^2 + 3y^2 = (x + i\sqrt{3}y)(x - i\sqrt{3}y) = (x + (2\omega + 1)y)(x - (2\omega + 1)y)$,

$$x^2 + 3y^2 = (x + y + 2\omega y)(x - y - 2\omega y).$$

Avec $x = A, y = 3B$, nous obtenons

$$4p = A^2 + 27B^2 = (A + 3B + 6\omega B)(A - 3B - 6\omega B).$$

Notons que A, B sont de même parité, puisque $4p = A^2 + 27B^2$.
Nous pouvons donc écrire $p = (\frac{A+3B}{2} + 3\omega B)(\frac{A-3B}{2} - 3\omega B)$, soit

$$p = \pi\overline{\pi}, \text{ où } \pi = \frac{A + 3B}{2} + 3\omega B \in \mathbb{Z}[\omega].$$

Par conséquent π est premier dans $\mathbb{Z}[\omega]$ (proposition 20 du chapitre "Entiers de Gauss").

$$\pi\overline{\pi} = \left(\frac{A + 3B}{2} + 3\omega B\right)\left(\frac{A - 3B}{2} - 3\omega B\right) = \left(\frac{C + 3D}{2} + 3\omega D\right)\left(\frac{C - 3D}{2} - 3\omega D\right).$$

Comme π est premier, il divise $\frac{C+3D}{2} + 3\omega D$ ou son conjugué. Puisqu'ils ont la même norme p, ils sont associés. Les unités de $\mathbb{Z}[\omega]$ sont $\pm 1, \pm\omega, \pm\omega^2$, si bien qu'il existe 12 cas :

$$\begin{aligned}
\frac{A + 3B}{2} + 3\omega B &= \pm\left(\frac{C + 3D}{2} + 3\omega D\right),\\
\frac{A + 3B}{2} + 3\omega B &= \pm\omega\left(\frac{C + 3D}{2} + 3\omega D\right),\\
\frac{A + 3B}{2} + 3\omega B &= \pm\omega^2\left(\frac{C + 3D}{2} + 3\omega D\right),\\
\frac{A + 3B}{2} + 3\omega B &= \pm\left(\frac{C - 3D}{2} - 3\omega D\right),\\
\frac{A + 3B}{2} + 3\omega B &= \pm\omega\left(\frac{C - 3D}{2} - 3\omega D\right),\\
\frac{A + 3B}{2} + 3\omega B &= \pm\omega^2\left(\frac{C - 3D}{2} - 3\omega D\right).
\end{aligned}$$

Pour prouver que $A = C$, si on remplace D par $-D$, nous obtenons les 6 derniers cas à partir des 6 premiers, si bien qu'il suffit d'examiner les 6 premiers cas.
Rappelons que $(1, \omega)$ est une $\mathbb{Z}$-base de $\mathbb{Z}[\omega]$.

1) $A + 3B + 6\omega B = C + 3D + 6\omega D$.
   Alors $B = D$ et $A + 3B = C + 3D$, donc $A = C$, ce qui est le résultat attendu.
   Les cinq autres cas ne peuvent se produire :
2) $A + 3B + 6\omega B = -C - 3D - 6\omega D$.
   Alors $B = -D, A = -C$. Comme $A \equiv C \equiv 1 \pmod 3$, c'est impossible.

3) $A+3B+6\omega B=\omega(C+3D+6\omega D)=\omega(C+3D)+(-1-\omega)6D=-6D+\omega(C-3D)$.

   Alors $A+3B=-6D$, $A\equiv 0 \pmod 3$, c'est impossible.

4) $A+3B+6\omega B=-\omega(C+3D+6\omega D)=-\omega(C+3D)+(1+\omega)6D=6D+\omega(-C+3D)$.

   Alors $A+3B=-6D$, $A\equiv 0 \pmod 3$, c'est impossible.

5) $A+3B+6\omega B=\omega^2(C+D+6\omega D)=(-1-\omega)(C+3D)+6D=-C+3D+\omega(-C-3D)$. Alors $A+3B=-C+3D$, $A\equiv -C \pmod 3$, c'est impossible.

6) $A+3B+6\omega B=-\omega^2(C+3D+6\omega D)=(1+\omega)(C+3D)-6D=(C-3D)+\omega(C+3D)$.

   Alors $6B=C+3D$, $C\equiv 0 \pmod 3$, c'est impossible.

En conclusion $A=C$. Alors $B^2=D^2$, où $B>0, D>0$, donc $B=D$.

(b) Nous avons déjà prouvé (voir l'égalité (1)) que

$$N(x^3+y^3=1)=p-2+2\ \mathrm{Re}(J(\chi,\chi)).$$

Comme $J(\chi,\chi)=a+b\omega$, nous obtenons $2\mathrm{Re}(J(\chi,\chi))=2a-b=A\equiv 1 \pmod 3$, si bien que

$$N(x^3+y^3=1)=p-2+A,$$

où A est l'unique entier tel qu'il existe un entier B vérifiant $4p=A^2+27B^2, A\equiv 1 \pmod 3$.

□

Exemple 1 : soit $p=37$. Alors $4p=148=(-11)^2+27\times 1^2$, où $-11\equiv 1 \pmod 3$, donc $A=-11$. Alors, dans $\mathbb{F}_{37}$,

$$N(x^3+y^3=1)=37-2-11=24 \qquad (p=37).$$

Exemple 2 : soit $p=97$. Alors $4p=388=19^2+27\times 1^2$, où $19\equiv 1 \pmod 3$, donc $A=19$. Dans $\mathbb{F}_{97}$,

$$N(x^3+y^3=1)=97-2+19=114 \qquad (p=97).$$

2.6 L'équation $x^n+y^n=1$ dans $\mathbb{F}_p$.

Ici p est premier. Supposons d'abord que $p\equiv 1 \pmod n$. Alors $d=n\wedge(p-1)=n$. Nous savons que

$$N(x^n+y^n=1)=\sum_{a+b=1} N(x^n=a)N(x^n=b).$$

Soit χ un caractère d'ordre n. D'après la proposition 38, les éléments du groupe des caractères d'ordre divisant n sont $\varepsilon,\chi,\chi^2,\ldots,\chi^{n-1}$. La proposition 43 montre que

$$N(x^n=a)=\sum_{i=0}^{n-1}\chi^i(a).$$

Ces deux résultats prouvent que

$$\begin{aligned} N(x^n + y^n = 1) &= \sum_{a+b=1} \sum_{i=0}^{n-1} \chi^i(a) \sum_{j=0}^{n-1} \chi^j(b) \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} \left(\sum_{a+b=1} \chi^i(a)\chi^j(b) \right) \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} J(\chi^i, \chi^j). \end{aligned}$$

La proposition 53 permet d'estimer cette somme.

- Si $i = j = 0$, $J(\chi^i, \chi^j) = J(\varepsilon, \varepsilon) = p$.
- Si $i = 0$ et $j \neq 0$, ou si $j = 0$ et $i \neq 0$, $J(\chi^i, \chi^j) = 0$.
- Si $i + j = n, i \neq 0, j \neq 0$, alors $J(\chi^i, \chi^j) = J(\chi^i, \chi^{-i}) = -\chi^i(-1)$, si bien que la somme de ces termes est

$$\sum_{i+j=n, i>0, j>0} J(\chi^i, \chi^j) = -\sum_{i=1}^{n-1} \chi^i(-1).$$

Comme l'ordre de χ est n,

$$\sum_{i=0}^{n-1} \chi^i(-1) = \begin{cases} \frac{1-\chi^n(-1)}{1-\chi(-1)} = 0 & \text{si } \chi(-1) \neq 1, \\ n & \text{si } \chi(-1) = 1. \end{cases}$$

Soit $a \in \mathbb{F}_p^*$. Définissons $\delta_n(a)$ par

$$\delta_n(a) = \begin{cases} 1 & \text{s'il existe } x \in \mathbb{F}_p \text{ tel que } x^n = a, \\ 0 & \text{sinon.} \end{cases}$$

La proposition 45 montre que $\delta_n(a) = 1$ si et seulement si $\chi(a) = 1$ (et $\delta_n(a) = 0$ sinon). Cette notation permet d'écrire

$$\sum_{i=0}^{n-1} \chi^i(-1) = \delta_n(-1)n.$$

Par conséquent,

$$\begin{aligned} \sum_{i+j=n, i>0, j>0} J(\chi^i, \chi^j) &= -\sum_{i=1}^{n-1} \chi^i(-1) \\ &= 1 - \sum_{i=0}^{n-1} \chi^i(-1) \\ &= 1 - \delta_n(-1)n \end{aligned}$$

En résumé,

$$N(x^n + y^n = 1) = p + 1 - \delta_n(-1)n + \sum_{(i,j)\in A} J(\chi^i, \chi^j),$$

où A est l'ensemble des couples (i, j) tels que $1 \leq i \leq n-1, 1 \leq j \leq n-1, i+j \neq n$. Ainsi $|A| = (n-1)^2 - (n-1) = (n-1)(n-2)$. Comme $|J(\chi^i, \chi^j)| = \sqrt{p}$ si $(i, j) \in A$, nous avons prouvé la proposition suivante.

Proposition 62. *Si p est premier et $p \equiv 1 \pmod{n}$,*

$$|N(x^n + y^n = 1) + \delta_n(-1)n - (p+1)| \leq (n-1)(n-2)\sqrt{p}.$$

Le terme $\delta_n(-1)n$ peut s'interpréter comme le nombre de points à l'infini de la courbe $x^n + y^n = 1$. En effet la complétion projective de cette courbe est la courbe projective d'équation homogène $x^n + y^n = t^n$, et les points à l'infini sont donnés par l'intersection avec la droite de l'infini d'équation $t = 0$. Les points à l'infini sont donc les points projectifs de coordonnées homogènes $(x, y, 0)$ vérifiant $x^n + y^n = 0$. Alors $y \neq 0$, sinon $x = y = t = 0$, donc $(x, y, 0) = y(a, 1, 0)$, où $a = \frac{x}{y}$ vérifie $a^n = -1$. Le nombre N points à l'infini de la courbe $x^n + y^n = 1$ est donc égal au nombre de solutions de $a^n = -1$ dans $\mathbb{F}_p$. La proposition 24 montre que le nombre N de solutions de $a^n = -1$ est 0 si $\delta_n(-1) = 0$, et $n = n \wedge (p-1)$ si $\delta_n(-1) = 1$. Ainsi $N = \delta_n(-1)n$. Par conséquent la somme des deux termes $N(x^n + y^n = 1) + \delta_n(-1)n$ désigne le nombre de points projectifs de la courbe d'équation homogène $x^n + y^n = t^n$.

Traitons maintenant le cas général, sans l'hypothèse $p \equiv 1 \pmod{n}$.

Proposition 63. *Soit $(a_1, \ldots, a_n) \in \mathbb{F}_p^n, (m_1, \ldots, m_n) \in \mathbb{N}^n, b \in \mathbb{F}_p$.*

Posons $d_i = m_i \wedge (p-1),\ 1 \leq i \leq n$. Alors

$$N\left(\sum_{i=0}^{n} a_i x_i^{m_i} = b\right) = N\left(\sum_{i=0}^{n} a_i x_i^{d_i} = b\right).$$

Démonstration. La proposition 44 montre que, pour tout $(u_1, \ldots, u_n) \in \mathbb{F}_p^n$,

$$N(x^{m_i} = u_i) = N(x^{d_i} = u_i).$$

En utilisant ce résultat, nous obtenons

$$\begin{aligned} N\left(\sum_{i=1}^{n} a_i x_i^{m_i} = b\right) &= \sum_{a_1 u_1 + \cdots + a_l u_l = b} \prod_{i=1}^{n} N(x^{m_i} = u_i) \\ &= \sum_{a_1 u_1 + \cdots + a_n u_n = b} \prod_{i=1}^{l} N(x^{d_i} = u_i) \\ &= N\left(\sum_{i=1}^{n} a_i x_i^{d_i} = b\right). \end{aligned}$$

□

Cette proposition montre que

$$N(x^n + y^n = 1) = N(x^d + y^d = 1), \text{ où } d = n \wedge (p-1),\ p \equiv 1 \pmod{d}.$$

La proposition 62 permet alors d'estimer $N(x^d + y^d = 1)$.

2.7 Sommes de Jacobi généralisées.

La généralisation des sommes de Jacobi est donnée par la définition suivante.

Définition 4. *Si $\chi_1, \ldots, \chi_l$ sont des caractères sur $\mathbb{F}_q$, la somme de Jacobi associée est donnée par*

$$J(\chi_1, \ldots, \chi_l) = \sum_{t_1 + \cdots + t_l = 1} \chi_1(t_1) \cdots \chi_l(t_l).$$

Pour compléter cette définition, définissons J_0 par

Définition 5.
$$J_0(\chi_1,\dots,\chi_l)=\sum_{t_1+\cdots+t_l=0}\chi_1(t_1)\cdots\chi_l(t_l).$$

Donnons quelques valeurs particulières de J et J_0 associées à l caractères.

Proposition 64. *Soient $\chi_1,\dots,\chi_l$ des caractères sur $\mathbb{F}_q$.*

(a) Si $\chi_1=\cdots=\chi_l=\varepsilon$, alors
$$J_0(\chi_1,\dots,\chi_l)=q^{l-1},$$
$$J(\chi_1,\dots,\chi_l)=q^{l-1}.$$

(b) Si certains des caractères χ_i, $1\le i\le l$ sont triviaux, mais pas tous, alors
$$J_0(\chi_1,\dots,\chi_l)=0,$$
$$J(\chi_1,\dots,\chi_l)=0.$$

(c) Supposons que $\chi_l\neq\varepsilon$. Alors
$$J_0(\chi_1,\dots,\chi_l)=\begin{cases}0 & \text{si } \chi_1\cdots\chi_l\neq\varepsilon,\\ \chi_l(-1)(q-1)J(\chi_1,\dots,\chi_{l-1}) & \text{sinon.}\end{cases}$$

Démonstration. (a) Si $\chi_1=\cdots=\chi_l=\varepsilon$, alors
$$J_0(\chi_1,\dots,\chi_l)=\sum_{t_1+\cdots+t_l=0}1=\mathrm{Card}\{(t_1,\dots,t_l)\in\mathbb{F}_q^l\mid t_1+\cdots+t_l=0\}=q^{l-1}.$$

En effet le nombre de solutions de l'équation de l'équation $t_1+\cdots+t_l=0$ est q^{l-1}, puisqu'une telle solution est déterminée par le choix arbitraire de $(t_1,\dots,t_{l-1})$ dans $\mathbb{F}_q^{l-1}$ (alors $t_l=-t_1-\cdots-t_{l-1}$).
De même,
$$J(\chi_1,\dots,\chi_l)=\sum_{t_1+\cdots+t_l=1}1=\mathrm{Card}\{(t_1,\dots,t_l)\in\mathbb{F}_q^l\mid t_1+\cdots+t_l=1\}=q^{l-1}.$$

(b) Supposons, quitte à changer l'ordre des caractères, que $\chi_1,\dots,\chi_s$ sont non triviaux (avec $s\ge1$), et que $\chi_{s+1}=\cdots=\chi_l=\varepsilon$. Alors
$$\begin{aligned}J_0(\chi_1,\dots,\chi_l)&=\sum_{t_1+\cdots+t_l=0}\chi_1(t_1)\cdots\chi_l(t_l)\\&=\sum_{t_1\in\mathbb{F}_q}\chi_1(t_1)\cdots\sum_{t_s\in\mathbb{F}_q}\chi_s(t_s)\left(\sum_{t_{s+1}+\cdots+t_l=-t_1-\cdots-t_s}1\right)\\&=q^{l-s-1}\left(\sum_{t_1\in\mathbb{F}_q}\chi_1(t_1)\right)\cdots\left(\sum_{t_s\in\mathbb{F}_q}\chi_s(t_s)\right)\end{aligned}$$

(si $t_1,\dots,t_s$ sont fixés, l'équation $t_{s+1}+\cdots+t_l=-t_1-\cdots-t_s$ a q^{l-s-1} solutions.)
De plus $\sum_{t_1\in\mathbb{F}_q}\chi_1(t_1)=0$ (proposition 35(a)), et $s\ge1$, donc $J_0(\chi_1,\dots,\chi_l)=0$.
Même preuve pour $J(\chi_1,\dots\chi_l)=0$, l'équation $t_{s+1}+\cdots+t_l=-t_1-\cdots-t_s$ étant remplacée par $t_{s+1}+\cdots+t_l=1-t_1-\cdots-t_s$.

(c) Partons de

$$J_0(\chi_1,\dots,\chi_l)=\sum_{s\in\mathbb{F}_q}\left(\sum_{t_1+\cdots+t_{l-1}=-s}\chi_1(t_1)\cdots\chi_{l-1}(t_{l-1})\right)\chi_l(s).$$

Comme $\chi_l\neq\varepsilon$, $\chi_l(0)=0$, donc

$$J_0(\chi_1,\dots,\chi_l)=\sum_{s\in\mathbb{F}_q^*}\left(\sum_{t_1+\cdots+t_{l-1}=-s}\chi_1(t_1)\cdots\chi_{l-1}(t_{l-1})\right)\chi_l(s).$$

Le changement d'indice donné par $(t_1,\dots,t_{l-1})=(-st'_1,\dots,-st'_{l-1})$ donne

$$\begin{aligned}\sum_{t_1+\cdots+t_{l-1}=-s}\chi_1(t_1)\cdots\chi_{l-1}(t_{l-1})&=(\chi_1\cdots\chi_{l-1})(-s)\sum_{t'_1+\cdots+t'_{l-1}=1}\chi_1(t'_1)\cdots\chi_{l-1}(t'_{l-1})\\&=(\chi_1\cdots\chi_{l-1})(-s)J(\chi_1,\dots,\chi_{l-1}).\end{aligned}$$

En reportant ce résultat dans le calcul de $J_0(\chi_1,\dots,\chi_l)$, nous obtenons

$$J_0(\chi_1,\dots,\chi_l)=(\chi_1\cdots\chi_{l-1})(-1)J(\chi_1,\dots,\chi_{l-1})\sum_{s\in\mathbb{F}_p^*}(\chi_1\cdots\chi_l)(s).$$

Si $\chi_1\cdots\chi_l\neq\varepsilon$, alors $\sum_{s\in\mathbb{F}_q^*}(\chi_1\cdots\chi_l)(s)=0$. Dans le cas contraire, $\sum_{s\in\mathbb{F}_q^*}(\chi_1\cdots\chi_l)(s)=q-1$, donc

$$\begin{aligned}J_0(\chi_1,\dots,\chi_l)&=(\chi_1\cdots\chi_{l-1})(-1)(q-1)J(\chi_1,\dots,\chi_{l-1})\\&=\overline{\chi_l(-1)}(q-1)J(\chi_1,\dots,\chi_{l-1})\\&=\chi_l(-1)(q-1)J(\chi_1,\dots,\chi_{l-1}).\end{aligned}$$

□

La proposition 54 se généralise de la façon suivante.

Proposition 65. *Supposons que $\chi_1,\dots,\chi_r$ sont non triviaux, ainsi que $\chi_1\cdots\chi_r$. Alors*

$$g(\chi_1)\cdots g(\chi_r)=J(\chi_1,\dots,\chi_r)g(\chi_1\cdots\chi_r).$$

Démonstration. En effet, en notant $\psi(s)=\zeta_p^{\mathrm{tr}(s)}$ pour $s\in\mathbb{F}_q$, nous obtenons

$$\begin{aligned}g(\chi_1)\cdots g(\chi_r)&=\left(\sum_{t_1\in\mathbb{F}_q}\chi_1(t_1)\psi(t_1)\right)\cdots\left(\sum_{t_r\in\mathbb{F}_q}\chi_r(t_r)\psi(t_r)\right)\\&=\sum_{s\in\mathbb{F}_q}\left(\sum_{t_1+\cdots+t_r=s}\chi_1(t_1)\cdots\chi_r(t_r)\right)\psi(s).\end{aligned}$$

Notons $S(s)=\sum_{t_1+\cdots+t_r=s}\chi_1(t_1)\cdots\chi_r(t_r)$ la somme intérieure. L'hypothèse $\chi_1\cdots\chi_r\neq\varepsilon$ permet d'appliquer la proposition 64(c) pour $s=0$:

$$S(0)=\sum_{t_1+\cdots+t_r=0}\chi_1(t_1)\cdots\chi_r(t_r)=J_0(\chi_1,\dots,\chi_r)=0,$$

Si $s \neq 0$, le changement d'indice $(t_1, \ldots, t_r) = (st'_1, \ldots, st'_r)$ donne

$$S(s) = (\chi_1 \cdots \chi_r)(s) J(\chi_1, \ldots, \chi_r)$$

et ainsi

$$\begin{aligned} g(\chi_1) \cdots g(\chi_r) &= \sum_{s \in \mathbb{F}_p^*} (\chi_1 \cdots \chi_r)(s) J(\chi_1, \ldots, \chi_r) \zeta^s \\ &= J(\chi_1, \ldots, \chi_r) g(\chi_1 \cdots \chi_r). \end{aligned}$$

□

Nous en tirons les conséquences suivantes.

Proposition 66. *Supposons que $\chi_1, \ldots, \chi_r$ sont non triviaux, mais que $\chi_1 \cdots \chi_r$ est trivial. Alors*

$$g(\chi_1) \cdots g(\chi_r) = \chi_r(-1)\, q\, J(\chi_1, \cdots, \chi_{r-1}).$$

Démonstration. La proposition 65 montre que

$$g(\chi_1) \cdots g(\chi_{r-1}) = J(\chi_1, \ldots, \chi_{r-1}) g(\chi_1 \cdots \chi_{r-1}).$$

En multipliant les deux membres de cette égalité par $g(\chi_r)$, puisque $\chi_1 \cdots \chi_{r-1} = \chi_r^{-1} = \overline{\chi_r}$, nous obtenons

$$g(\chi_1) \cdots g(\chi_r) = g(\chi_r) g(\overline{\chi_r}) J(\chi_1, \ldots, \chi_{r-1}).$$

En utilisant les propositions 51 et 52,

$$g(\chi_r) g(\overline{\chi_r}) = \chi_r(-1) g(\chi_r) \overline{g(\chi_r)} = \chi_r(-1) q,$$

donc

$$g(\chi_1) \cdots g(\chi_r) = \chi_r(-1) q J(\chi_1, \ldots, \chi_{r-1}).$$

□

Proposition 67. *Supposons que $\chi_1, \ldots, \chi_r$ sont non triviaux, mais que $\chi_1 \cdots \chi_r$ est trivial. Alors*

$$J(\chi_1, \ldots, \chi_r) = -\chi_r(-1) J(\chi_1, \ldots, \chi_{r-1}).$$

(pour $r = 2$, nous posons $J(\chi_1) = 1$.)

Démonstration. Pour $r = 2$, il s'agit de la proposition 53(c). Supposons maintenant que $r > 2$.

Comme au début de la démonstration de la proposition 65, nous obtenons

$$g(\chi_1) \cdots g(\chi_r) = \sum_{s \in \mathbb{F}_q} \left(\sum_{t_1 + \cdots + t_r = s} \chi_1(t_1) \cdots \chi_r(t_r) \right) \psi(s), \tag{2.9}$$

mais maintenant, l'hypothèse $\chi_1 \cdots \chi_r = \varepsilon$ donne, à l'aide de la proposition 64(c),

$$S(0) = \sum_{t_1 + \cdots + t_r = 0} \chi_1(t_1) \cdots \chi_r(t_r) = J_0(\chi_1, \ldots, \chi_r) = \chi_r(-1)(q-1) J(\chi_1, \ldots, \chi_{r-1}), \tag{2.10}$$

et pour $s \neq 0$, comme dans la démonstration de la proposition 64,

$$S(s) = \sum_{t_1+\cdots+t_r=s} \chi_1(t_1)\cdots\chi_r(t_r) = (\chi_1\cdots\chi_r)(s)J(\chi_1,\ldots,\chi_r). \tag{2.11}$$

Ici $\chi_1\cdots\chi_r = \varepsilon$, donc $S(s) = J(\chi_1,\ldots,\chi_r)$.

Ainsi, en utilisant les égalités (2.9), (2.10), et (2.11), ainsi que $\sum_{s\in\mathbb{F}_q}\psi(s) = 0$ (proposition 47),

$$\begin{aligned} g(\chi_1)\cdots g(\chi_r) &= J_0(\chi_1,\ldots,\chi_r) + J(\chi_1,\ldots,\chi_r)\sum_{s\in\mathbb{F}_q^*}\psi(s) \\ &= \chi_r(-1)(q-1)J(\chi_1,\ldots,\chi_{r-1}) - J(\chi_1,\ldots,\chi_r) \end{aligned}$$

La proposition 66 donne

$$g(\chi_1)\cdots g(\chi_r) = \chi_r(-1)\, q\, J(\chi_1,\cdots,\chi_{r-1}).$$

Par conséquent,

$$\chi_r(-1)\, q\, J(\chi_1,\cdots,\chi_{r-1}) = \chi_r(-1)(q-1)J(\chi_1,\ldots,\chi_{r-1}) - J(\chi_1,\ldots,\chi_r)$$

et donc

$$J(\chi_1,\ldots,\chi_r) = -\chi_r(-1)J(\chi_1,\ldots,\chi_{r-1}).$$

□

Proposition 68. *Supposons que $\chi_1,\ldots,\chi_r$ sont des caractères non triviaux sur $\mathbb{F}_q$.*

(a) Si $\chi_1\cdots\chi_r \neq \varepsilon$, alors

$$\begin{aligned} |J_0(\chi_1,\ldots,\chi_r)| &= 0, \\ |J(\chi_1,\ldots,\chi_r)| &= q^{\frac{r-1}{2}}. \end{aligned}$$

(b) Si $\chi_1\cdots\chi_r = \varepsilon$, alors

$$\begin{aligned} |J_0(\chi_1,\ldots,\chi_r)| &= (q-1)q^{\frac{r}{2}-1}, \\ |J(\chi_1,\ldots,\chi_r)| &= q^{\frac{r}{2}-1}. \end{aligned}$$

Démonstration. Si χ n'est pas un caractère trivial, alors $|g(\chi)| = \sqrt{q}$.

(a) Si $\chi_1\cdots\chi_r \neq \varepsilon$, la proposition 64(c) donne $J_0(\chi_1,\ldots,\chi_r) = 0$, et la proposition 65 donne

$$|J(\chi_1,\ldots,\chi_r)| = \frac{(\sqrt{q})^r}{\sqrt{q}} = q^{\frac{r-1}{2}}.$$

(b) Si $\chi_1\cdots\chi_r = \varepsilon$, la proposition 64(c) et la relation précédente donnent, puisque $\chi_1\cdots\chi_{r-1} = \chi_r^{-1} \neq \varepsilon$,

$$\begin{aligned} |J_0(\chi_1,\ldots,\chi_r)| &= (q-1)|J(\chi_1,\ldots,\chi_{r-1})| \\ &= (q-1)q^{\frac{r}{2}-1}. \end{aligned}$$

Enfin,

$$\begin{aligned} |J(\chi_1,\ldots,\chi_r)| &= |J(\chi_1,\ldots,\chi_{r-1})| && \text{(proposition 67)} \\ &= q^{\frac{r}{2}-1} && \text{(partie (a)).} \end{aligned}$$

□

2.8 Applications arithmétiques des sommes de Jacobi.

Généralisons le calcul de $N(x^2+y^2=1)$ à $N(x_1^2\cdots+x_r^2=1)$ dans $\mathbb{F}_p$, où p est premier.

Soit χ l'unique caractère d'ordre 2, le caractère de Legendre. Nous avons vu que $N(x^2=a)=1+\chi(a)$. Alors

$$\begin{aligned}N(x_1^2+\cdots+x_r^2=1) &= \sum_{a_1+\cdots+a_r=1} N(x_1^2=a_1)\cdots N(x_r^2=a_r)\\ &= \sum_{a_1+\cdots+a_r=1} (1+\chi(a_1))\cdots(1+\chi(a_r))\\ &= \sum_{a_1+\cdots+a_r=1}\ \sum_{(i_1,\ldots,i_r)\in\{0,1\}^r} \chi^{i_1}(a_1)\cdots\chi^{i_r}(a_r)\\ &= \sum_{(i_1,\ldots,i_r)\in\{0,1\}^r} J(\chi^{i_1},\ldots,\chi^{i_r})\end{aligned}$$

Si $i_1=\cdots=i_r=0$, alors $J(\chi^{i_1},\ldots,\chi^{i_r})=J(\varepsilon,\ldots,\varepsilon)=p^{r-1}$ d'après la proposition 64(a).

Si l'un des exposant i_k est nul, mais pas tous, la proposition 64(b) donne $J(\chi^{i_1},\ldots,\chi^{i_r})=0$. Il ne reste que le cas où $i_1=\cdots=i_r=1$, donc

$$N(x_1^2+\cdots+x_r^2=1)=p^{r-1}+J(\chi,\ldots,\chi).$$

Notons que $\chi^r=\chi$ si r est impair et $\chi^r=\varepsilon$ si r est pair.

Supposons d'abord que r est impair. Alors $\chi^r=\chi$ n'est pas trivial, donc la proposition 65 donne

$$J(\chi,\cdots,\chi)=g(\chi)^{r-1}.$$

Les propositions 51 et 52 donnent, puisque χ est à valeur réelles, $g(\chi)^2=g(\chi)g(\overline{\chi})=\chi(-1)g(\chi)\overline{g(\chi)}=\chi(-1)p$, et ainsi

$$g(\chi)^2=\chi(-1)p.$$

Alors $J(\chi,\cdots,\chi)=(\chi(-1)p)^{\frac{r-1}{2}}=(-1)^{\frac{r-1}{2}\frac{p-1}{2}}p^{\frac{r-1}{2}}$.

Si r est pair, alors $\chi^r=\varepsilon$. La proposition 67 donne

$$J(\chi,\ldots,\chi)=-\chi(-1)(\chi(-1)p)^{\frac{r}{2}-1}=-(-1)^{\frac{r}{2}\frac{p-1}{2}}p^{\frac{r}{2}-1}.$$

Nous avons donc prouvé la proposition suivante :

Proposition 69. *Si r est impair,*

$$N(x_1^2+\cdots+x_r^2=1)=p^{r-1}+(-1)^{\frac{r-1}{2}\frac{p-1}{2}}p^{\frac{r-1}{2}},$$

et si r est pair,

$$N(x_1^2+\cdots+x_r^2=1)=p^{r-1}-(-1)^{\frac{r}{2}\frac{p-1}{2}}p^{\frac{r}{2}-1}.$$

2.9 Un théorème général.

Généralisant les résultats précédents, nous estimons maintenant le nombre de solutions N dans $\mathbb{F}_q$ de

$$a_1 x_1^{l_1} + \cdots + a_r x_r^{l_r} = b,$$

où $a_1, \ldots, a_r \in \mathbb{F}_q^*, b \in \mathbb{F}_q$ et $l_i \in \mathbb{N}^*$.

Puisque $N(x^m = a) = N(x^d = a)$, où $d = m \wedge (q-1)$, nous pouvons supposer que les exposants l_i sont des diviseurs de $q-1$ (proposition 63).

Nous partons de

$$N = \sum_{\sum_{i=1}^r a_i u_i = b} N(x_1^{l_1} = u_1) \cdots N(x_r^{l_r} = u_r).$$

Comme dans le paragraphe 2.3, notons C_l l'ensemble des caractères sur $\mathbb{F}_p$ dont l'ordre divise l. La proposition 10 donne

$$N(x_i^{l_i} = u_i) = \sum_{\chi_i \in C_{l_i}} \chi_i(u_i).$$

Ainsi

$$N = \sum_{(\chi_1, \ldots, \chi_r) \in C_{l_1} \times \cdots C_{l_r}} \left(\sum_{\sum_{i=1}^r a_i u_i = b} \chi_1(u_1) \cdots \chi_r(u_r) \right).$$

Traitons la somme intérieure

$$T = T_{\chi_1, \ldots, \chi_r} = \sum_{\sum_{i=1}^r a_i u_i = b} \chi_1(u_1) \cdots \chi_r(u_r),$$

en distinguant les cas $b = 0, b \neq 0$.

- Si $b = 0$, le changement de variable $t_i = a_i u_i$ donne

$$\begin{aligned} T &= \sum_{t_1 + \cdots + t_r = 0} \chi_1(a_1^{-1} t_1) \cdots \chi_r(a_r^{-1} t_r) \\ &= \chi_1(a_1^{-1}) \cdots \chi_r(a_r)^{-1} J_0(\chi_1, \ldots, \chi_r). \end{aligned}$$

  La proposition 64 donne $J_0(\chi_1, \ldots, \chi_r) = q^{r-1}$ si $\chi_1 = \cdots = \chi_r = \varepsilon$, et $J_0(\chi_1, \ldots, \chi_r) = 0$ si l'un des χ_i est trivial, mais pas tous. Enfin, si $\chi_1 \ldots \chi_r = \varepsilon \neq 0$, alors $J_0(\chi_1, \ldots, \chi_r) = 0$.

  Ainsi

$$N = q^{r-1} + \sum_{(\chi_1, \ldots, \chi_r) \in A} \chi_1(a_1^{-1}) \cdots \chi_r(a_r)^{-1} J_0(\chi_1, \ldots, \chi_r),$$

  où A est l'ensemble des r-uplets $(\chi_1, \ldots, \chi_r)$ tels que $\chi_i^{l_i} = \varepsilon, \chi_i \neq \varepsilon$ et $\chi_1 \cdots \chi_r = \varepsilon$.

  Posons $M = |A|$. Si $(\chi_1, \ldots, \chi_r) \in A$, la proposition 68 donne $|J_0(\chi_1, \ldots, \chi_r)| = (q-1) q^{\frac{r}{2}-1}$. Par conséquent,

$$|N - q^{r-1}| \leq M(q-1) q^{\frac{r}{2}-1}.$$

- Si $b \neq 0$, le changement de variable $t_i = b^{-1}a_i u_i$ donne

$$\begin{aligned} T &= \sum_{t_1+\cdots+t_r=1} \chi_1(ba_1^{-1}t_1)\cdots\chi_r(ba_r^{-1}t_r) \\ &= (\chi_1\cdots\chi_r)(b)\chi_1(a_1^{-1})\cdots\chi_r(a_r)^{-1}J(\chi_1,\ldots,\chi_r). \end{aligned}$$

La proposition 64 donne $J(\chi_1,\ldots,\chi_r) = q^{r-1}$ si $\chi_1 = \cdots = \chi_r = \varepsilon$, et $J(\chi_1,\ldots,\chi_r) = 0$ si l'un des χ_i est trivial, mais pas tous.
Ainsi

$$N = q^{r-1} + \sum_{(\chi_1,\ldots,\chi_r)\in B} (\chi_1\cdots\chi_r)(b)\chi_1(a_1^{-1})\cdots\chi_r(a_r)^{-1}J(\chi_1,\ldots,\chi_r),$$

où B est l'ensemble des r-uplets $(\chi_1,\ldots,\chi_r)$ tels que $\chi_i^{l_i} = \varepsilon, \chi_i \neq \varepsilon$.
Alors, d'après la proposition 68,

$$|J(\chi_1,\ldots,\chi_r)| = \begin{cases} q^{\frac{r}{2}-1} & \text{si } \chi_1\cdots\chi_r = \varepsilon, \\ q^{\frac{r-1}{2}} & \text{si } \chi_1\cdots\chi_r \neq \varepsilon. \end{cases}$$

Alors

$$\begin{aligned} N = q^{r-1} &+ \sum_{(\chi_1,\ldots,\chi_r)\in C} (\chi_1\cdots\chi_r)(b)\chi_1(a_1^{-1})\cdots\chi_r(a_r)^{-1}J(\chi_1,\ldots,\chi_r) \\ &+ \sum_{(\chi_1,\ldots,\chi_r)\in D} (\chi_1\cdots\chi_r)(b)\chi_1(a_1^{-1})\cdots\chi_r(a_r)^{-1}J(\chi_1,\ldots,\chi_r), \end{aligned}$$

où
C est l'ensemble des r-uplets $(\chi_1,\ldots,\chi_r)$ tels que $\chi_i^{l_i} = \varepsilon, \chi_i \neq \varepsilon$ et $\chi_1\cdots\chi_r = \varepsilon$,
D est l'ensemble des r-uplets $(\chi_1,\ldots,\chi_r)$ tels que $\chi_i^{l_i} = \varepsilon, \chi_i \neq \varepsilon$ et $\chi_1\cdots\chi_r \neq \varepsilon$.
Notons $M_0 = |B|, M_1 = |C|$. Alors,

$$|N - q^{r-1}| \leq M_0\, q^{\frac{r}{2}-1} + M_1\, q^{\frac{r-1}{2}}.$$

Nous avons prouvé la proposition suivante.

Proposition 70. *Soit N le nombre de solutions dans $\mathbb{F}_q^r$ de*

$$a_1x_1^{l_1} + \cdots + a_rx_r^{l_r} = b,$$

où $a_1,\ldots,a_r \in \mathbb{F}_q^*, b \in \mathbb{F}_q, l_i \in \mathbb{N}^*$ (et $l_i \mid q-1,\ i = 1,\ldots,r$).

- *Si $b = 0$, alors*

$$N = q^{r-1} + \sum_{(\chi_1,\ldots,\chi_r)\in A} \chi_1(a_1^{-1})\cdots\chi_r(a_r)^{-1}J_0(\chi_1,\ldots,\chi_r),$$

où A est l'ensemble des r-uplets $(\chi_1,\ldots,\chi_r)$ tels que $\chi_i^{l_i} = \varepsilon, \chi_i \neq \varepsilon$ et $\chi_1\cdots\chi_r = \varepsilon$. Si $M = |A|$, alors

$$|N - q^{r-1}| \leq M(q-1)q^{\frac{r}{2}-1}.$$

- *Si* $b \neq 0$, *alors*

$$N = q^{r-1} + \sum_{(\chi_1,\dots,\chi_r)\in B} (\chi_1 \cdots \chi_r)(b)\chi_1(a_1^{-1}) \cdots \chi_r(a_r)^{-1} J(\chi_1, \dots, \chi_r),$$

où B *est l'ensemble des* r*-uplets* $(\chi_1, \dots, \chi_r)$ *tels que* $\chi_i^{l_i} = \varepsilon, \chi_i \neq \varepsilon$.
Si M_0 *est le nombre des* p*-uplets de* B*, vérifiant de plus* $\chi_1 \cdots \chi_r = \varepsilon$*, et* M_1 *le nombre des* p*-uplets de* B *vérifiant* $\chi_1 \cdots \chi_r \neq \varepsilon$*, alors*

$$|N - q^{r-1}| \leq M_0\, q^{\frac{r}{2}-1} + M_1\, q^{\frac{r-1}{2}}.$$

Cette proposition prouve en particulier que l'équation $a_1 x_1^{l_1} + \cdots + a_r x_r^{l_r} = b$ a des solutions dans $\mathbb{F}_q$ si q est assez grand, et que le nombre de ces solutions tend vers l'infini quand q tend vers l'infini.

Chapitre 3

Réciprocité cubique.

Les résultats de ce chapitre, ainsi que du chapitre suivant, viennent de [Ireland, Rosen], [Cox2] et [Lemmermeyer]. Notons ici $A = \mathbb{Z}[\omega]$, où, comme dans le chapitre précédent $\omega^3 = 1, \omega \neq 1$. Les nombres premiers de $\mathbb{Z}$ serons nommés "premiers rationnels", pour les distinguer des éléments premiers de A.

3.1 Anneaux quotients de $\mathbb{Z}[\omega]$.

Si π est premier dans A, alors $A/\pi A$ est un corps (voir le chapitre anneaux).

Proposition 71. *Soit $\pi \in A = \mathbb{Z}[\omega]$ un élément premier. Alors $A/\pi A$ est un corps à $\mathrm{N}(\pi)$ éléments :*

$$\mathrm{N}(\pi) = |A/\pi A|.$$

Démonstration. Nous prouvons cette proposition en considérant les différents types d'éléments premiers de $\mathbb{Z}[\omega]$, donnés dans la proposition 22 du chapitre "Entiers de Gauss".

- Supposons que $\pi = q$ est un premier rationnel, où $q \equiv 2 \pmod 3, q > 0$. Vérifions que
$$S = \{a + b\omega \mid 0 \leq a < q,\ 0 \leq b < q\}$$
est un système complet de représentants des classes modulo π.
Si $\alpha = u + \omega v \in A$, alors les divisions euclidiennes de u et v par q donnent des entiers a, b, s, t tels que $u = qs + a, v = qt + b$, où $0 \leq a < q, 0 \leq b < q$. Alors $\alpha \equiv a + b\omega \pmod q$, où $a + b\omega \in S$.
Vérifions que les éléments de S sont dans des classes distinctes. Si $\alpha = a+b\omega \equiv \beta = a'+b'\omega \pmod q$, où $\alpha, \beta \in S$, alors $q \mid (a-a')+(b-b')\omega$, donc $\frac{a-a'}{q}+\omega\frac{b-b'}{q} \in \mathbb{Z}[\omega]$, ce qui implique $q \mid a - a', q \mid b - b'$. Comme $|a - a'| < q$ et $|b - b'| < q$, il s'ensuit que $a = a', b = b'$, donc $\alpha = \beta$. Ainsi $|A/\pi A| = |S| = q^2 = \mathrm{N}(q) = \mathrm{N}(\pi)$.
- Supposons que $\pi = a + b\omega$ vérifie $\mathrm{N}(\pi) = p$, où p est un premier rationnel, $p \equiv 1 \pmod 3$. Vérifions que
$$T = \{0, 1, \cdots, p - 1\}$$
est un système complet de représentants des classes.
Comme $\mathrm{N}(\pi) = p = a^2 - ab + b^2$, il s'ensuit que $p \nmid b$, sinon $p \mid a, p \mid b$, donc $p^2 \mid a^2 - ab + b^2 = p$, donc $p \mid 1$: c'est absurde.
Soit $\alpha = u + \omega v \in A$. Comme $p \nmid b$, il existe un entier c tel que $cb \equiv v \pmod p$, a fortiori modulo π. Alors $\alpha - c\pi = u - ca + \omega(v - cb)$, donc $\alpha \equiv u - ca \pmod \pi$.

Posons $n = u - ca$. Alors $n \in \mathbb{Z}$, et $\alpha \equiv n \pmod{\pi}$. La division euclidienne de n par p donne $n = ps + r,\ 0 \leq r < p$, donc $\alpha \equiv r \pmod{\pi}$, où $r \in T$.

Les éléments de T sont dans des classes distinctes modulo π. En effet, si $r, s \in T$, et $r \equiv s \pmod{\pi}$, alors $\pi \mid r - s$, soit $r - s = \pi\lambda, \lambda \in A$, donc $(r-s)^2 = \mathrm{N}(\pi)\mathrm{N}(\lambda) = p\mathrm{N}(\lambda)$. Ainsi $p \mid (r-s)^2$, où p est un premier rationnel, donc $p \mid r-s$, où $|r - s| < p$, donc $r = s$.

Par conséquent, $|A/\pi A| = |T| = p = \mathrm{N}(\pi)$.

- Supposons que $\pi = 1 - \omega$. Vérifions que

$$U = \{0, 1, 2\}$$

est un système complet de représentants des classes modulo $\pi = 1 - \omega$.

Soit $\alpha = a + b\omega \in A$ quelconque. Comme $\omega \equiv 1 \pmod{\pi}$, $\alpha \equiv a + b \pmod{\pi}$. Posons $n = a + b$; alors $n \in \mathbb{Z}$ et $\alpha \equiv n \pmod{\pi}$. La division euclidienne de n par 3 donne les entiers q, r tels que $n = 3q + r, r \in \{0, 1, 2\}$, donc $n \equiv r \pmod{3}$, et puisque $1 - \omega \mid 3$, $\alpha \equiv n \equiv r \pmod{\pi}$, où $r \in U$.

De plus, $0 \not\equiv 2 \pmod{\pi}$, sinon $\pi \mid 2$, et $\pi \mid 3$, donc $\pi \mid 1$: c'est absurde puisque π est premier, et n'est donc pas une unité. De même, $0 \equiv 1$, ou $1 \equiv 2$, entraîne $\pi \mid 1$, ce qui contredit l'hypothèse π premier.

Ainsi $|A/\pi A| = |U| = 3 = \mathrm{N}(\pi)$.

Si λ est un élément premier quelconque de A, alors λ est associé à un élément π appartenant à l'un des trois types considérés, donc vérifiant $\mathrm{N}(\pi) = |A/\pi A|$. Alors $\mathrm{N}(\pi) = \mathrm{N}(\lambda)$, et $\pi A = \lambda A$, donc $\mathrm{N}(\lambda) = |A/\lambda A|$.

□

3.2 Caractère cubique.

Ici $A = \mathbb{Z}[\omega]$. Donnons l'analogue du théorème de Fermat dans A.

Proposition 72. *Soit $\alpha \in A$, et π un premier de A tel que π ne divise pas α. Alors*

$$\alpha^{\mathrm{N}(\pi)-1} \equiv 1 \pmod{\pi}.$$

Démonstration. Soit K le corps $A/\pi A$. Le cardinal du groupe K^* est $\mathrm{N}(\pi) - 1$, donc l'ordre de la classe $[\alpha] \in K^*$ divise $\mathrm{N}(\pi) - 1$. Ainsi $[\alpha]^{\mathrm{N}(\pi)-1} = 1$, donc $\alpha^{\mathrm{N}(\pi)-1} \equiv 1 \pmod{\pi}$. □

Proposition 73. *Si π est un premier de A, et si $\mathrm{N}(\pi) \neq 3$, alors*

$$3 \mid \mathrm{N}(\pi) - 1.$$

Démonstration. Notons que si $\mathrm{N}(\pi) \neq 3$, alors les classes modulo π de $1, \omega, \omega^2$ sont distinctes.

En raisonnant par l'absurde, supposons que $1 \equiv \omega \pmod{\pi}$. Alors $\pi \mid 1 - \omega$, où $1 - \omega$ est premier, donc π serait associé à $1 - \omega$, mais alors $\mathrm{N}(\pi) = \mathrm{N}(1 - \omega) = 3$, contrairement à l'hypothèse. Comme $\omega^2 - 1 = (\omega + 1)(\omega - 1) = \omega^2(1 - \omega)$, et $\omega - \omega^2 = \omega(1 - \omega)$ sont tous deux associés à $1 - \omega$, le même raisonnement montre que $1 \not\equiv \omega^2 \pmod{\pi}$ et $\omega \not\equiv \omega^2 \pmod{\pi}$.

L'ensemble des classes $\{[1], [\omega], [\omega]^2\}$ est donc un sous-groupe à trois éléments du groupe $(A/\pi A)^*$. Le théorème de Lagrange montre alors que

$$3 \mid \mathrm{N}(\pi) - 1.$$

□

A titre de vérification, si $\pi = q$, où $q \equiv 2 \pmod 3$, alors $\mathrm{N}(\pi) = q^2 \equiv 1 \pmod 3$, et si π vérifie $\mathrm{N}(\pi) = p$, alors $p \equiv 1 \pmod 3$.

Proposition 74. *Supposons que π est un premier de A tel que $\mathrm{N}(\pi) \neq 3$, et que $\pi \nmid \alpha$. Alors il existe un unique entier $m \in \{0, 1, 2\}$ tel que*

$$\alpha^{\frac{\mathrm{N}(\pi)-1}{3}} \equiv \omega^m \pmod \pi.$$

Démonstration. Nous savons que π divise $\alpha^{\mathrm{N}(\pi)-1} - 1$, et comme $\mathrm{N}(\pi) - 1$ est un multiple de 3,

$$\alpha^{\mathrm{N}(\pi)-1} - 1 = (\alpha^{\frac{\mathrm{N}(\pi)-1}{3}} - 1)(\alpha^{\frac{\mathrm{N}(\pi)-1}{3}} - \omega)(\alpha^{\frac{\mathrm{N}(\pi)-1}{3}} - \omega^2).$$

Comme π est premier, il divise l'un des trois facteurs. De plus $1, \omega, \omega^2$ sont dans des classes distinctes modulo π, donc il divise au plus un de ces facteurs. Ainsi $\alpha^{\mathrm{N}(\pi)-1} \equiv \omega^m \pmod \pi$, pour un unique $m \in \{0, 1, 2\}$. □

Notons que dans le cas où $\pi \mid \alpha$, $\alpha^{\frac{\mathrm{N}(\pi)-1}{3}} \equiv 0 \pmod \pi$.

Nous savons que les classes de $1, \omega, \omega^2$ dans $A/\pi A$ sont distinctes. De plus, les classes de $0, 1, \omega, \omega^2$ sont distinctes, puisque $\omega^k \equiv 0 \pmod \pi$, entraîne $\pi \mid \omega^k$, donc $\pi \mid 1$, ce qui est absurde puisque π premier n'est pas une unité. Pour tout $\alpha \in A$, $[\alpha]^{\frac{\mathrm{N}(\pi)-1}{3}} \in \{[0], [1], [\omega], [\omega]^2\}$, donc il existe un et un seul $z \in \{0, 1, \omega, \omega^2\}$ tel que $\alpha^{\frac{\mathrm{N}(\pi)-1}{3}} \equiv z \pmod \pi$. Ceci justifie la définition suivante :

Définition 6. *Soit π un premier de A tel que $\mathrm{N}(\pi) \neq 3$. Le caractère cubique de $\alpha \in A$ modulo π, noté $\left(\frac{\alpha}{\pi}\right)_3$ (ou $(\alpha/\pi)_3$) est le nombre complexe de l'ensemble $\{0, 1, \omega, \omega^2\}$ caractérisé par*

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{\mathrm{N}(\pi)-1}{3}} \pmod \pi.$$

Cette définition implique que $\left(\frac{\alpha}{\pi}\right)_3 = 0 \iff \pi \mid \alpha$.

Proposition 75. *Si $\left(\frac{\alpha}{\pi}\right)_3 \equiv \zeta \pmod \pi$, où $\zeta \in \{0, 1, \omega, \omega^2\}$, alors $\left(\frac{\alpha}{\pi}\right)_3 = \zeta$.*

Démonstration. En effet, $\left(\frac{\alpha}{\pi}\right)_3$ et ζ sont des éléments de $\{0, 1, \omega, \omega^2\}$, et les classes de ces éléments sont distinctes modulo π. □

Donnons les premières propriétés de ce caractère cubique

Proposition 76. *Si $\alpha, \beta \in A$, et si π est un premier de A tel que $\mathrm{N}(\pi) \neq 3$,*

(a) $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$.

(b) Si $\alpha \equiv \beta \pmod \pi$, alors $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$.

Démonstration. (a) Par définition

$$\left(\frac{\alpha\beta}{\pi}\right)_3 \equiv (\alpha\beta)^{\frac{\mathrm{N}(\pi)-1}{3}} = \alpha^{\frac{\mathrm{N}(\pi)-1}{3}} \beta^{\frac{\mathrm{N}(\pi)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3 \pmod \pi.$$

La proposition 75 permet de conclure que

$$\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3.$$

(b) Si $\alpha \equiv \beta \pmod{\pi}$, alors $\alpha^{\frac{\mathrm{N}(\pi)-1}{3}} \equiv \beta^{\frac{\mathrm{N}(\pi)-1}{3}} \pmod{\pi}$, donc $\left(\frac{\alpha}{\pi}\right)_3 \equiv \left(\frac{\beta}{\pi}\right)_3 \pmod{\pi}$. La proposition 75 montre alors que $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$.

□

Notons que (b) assure que l'application χ

$$\begin{array}{ccc} (A/\pi A)^* & \to & \mathbb{C}^* \\ [\alpha] & \mapsto & \left(\frac{\alpha}{\pi}\right)_3 \end{array}$$

est bien définie, et le (a) montre que χ est un homomorphisme de groupe. Ainsi χ est un caractère multiplicatif sur $(A/\pi A)^*$, et il est d'ordre 3.

Le caractère cubique permet de caractériser les cubes de A modulo π.

Proposition 77. *Soit $\alpha \in A = \mathbb{Z}[\omega]$, et π un premier de A tel que $\mathrm{N}(\pi) \neq 3$ et $\pi \nmid \alpha$. Alors*

$$\left(\frac{\alpha}{\pi}\right)_3 = 1 \iff \exists x \in A,\ x^3 \equiv \alpha \pmod{\pi}.$$

Démonstration. $A/\pi A$ est un corps à $\mathrm{N}(\pi)$ éléments d'après la proposition 71, et 3 divise $\mathrm{N}(\pi)-1$ d'après la proposition 73, donc $d = 3 \wedge (\mathrm{N}(\pi)-1) = 3$. Alors la proposition 1 du chapitre "Sommes de Gauss et sommes de Jacobi" montre que l'équation $[x]^3 = [\alpha]$ a une solution dans $(A/\pi A)^*$ si et seulement si $[\alpha]^{\frac{\mathrm{N}(\pi)-1}{3}} = 1$, ce qui équivaut à $\left(\frac{\alpha}{\pi}\right)_3 = 1$. □

Nous verrons comment ceci permet de caractériser les cubes de $\mathbb{F}_p^*$.

Notons dans cette section $\chi_\pi(\alpha) = \left(\frac{\alpha}{\pi}\right)_3$, si $\alpha \in A$.

Proposition 78. *Si $\alpha \in A$,*

$$\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha}).$$

Démonstration. La définition de χ_π donne la relation

$$\alpha^{\frac{\mathrm{N}(\pi)-1}{3}} \equiv \chi_\pi(\alpha) \pmod{\pi}.$$

Le passage au conjugué donne

$$\overline{\alpha}^{\frac{\mathrm{N}(\pi)-1}{3}} \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}.$$

Comme $\mathrm{N}(\pi) = \mathrm{N}(\overline{\pi})$,

$$\begin{aligned} \chi_{\overline{\pi}}(\overline{\alpha}) &\equiv \overline{\alpha}^{\frac{\mathrm{N}(\overline{\pi})-1}{3}} \pmod{\overline{\pi}} \\ &= \overline{\alpha}^{\frac{\mathrm{N}(\pi)-1}{3}} \\ &\equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}. \end{aligned}$$

La conclusion vient alors de la proposition 75. □

Proposition 79. *Soit q un premier rationnel, $q \equiv 2 \pmod 3, q > 0$. Si $n \in \mathbb{Z}$ est premier avec q, alors $\chi_q(n) = 1$.*

Démonstration. L'élément q est premier dans A, et par définition de χ_q,

$$\chi_q(n) \equiv n^{\frac{\mathrm{N}(q)-1}{3}} = n^{\frac{q^2-1}{3}} = (n^{q-1})^{\frac{q+1}{3}} \equiv 1 \pmod{q}.$$

□

Remarque 1 : l'exemple 2 de la proposition 24 du chapitre "Sommes de Gauss et sommes de Jacobi" démontre que dans le cas $q \equiv 2 \pmod 3, q \nmid n$, il existe un entier $x \in \mathbb{Z}$ tel que $x^3 \equiv n \pmod q$. La proposition 77 donne alors $\chi_q(n) = 1$, ce qui prouve à nouveau la proposition.

Remarque 2 : si $q \neq q'$ sont des premiers rationnels tous deux congrus à 2 modulo 3, alors $\chi_q(q') = \chi_{q'}(q) = 1$, ce qui est un cas particulier de la loi de réciprocité cubique.

3.3 Éléments primaires de $\mathbb{Z}[\omega]$

Introduisons la notion d'élément primaire, qui permet de choisir un élément privilégié parmi les associés d'un élément de A.

Définition 7. *Un élément $\alpha = a + b\omega \in A = \mathbb{Z}[\omega], (a, b \in \mathbb{Z})$, qui n'est pas une unité, est dit primaire si $\alpha \equiv -1 \pmod 3$.*

Si $\alpha = a+b\omega$ est premier dans A, α est primaire signifie que $a \equiv -1 \pmod 3$ et $b \equiv 0 \pmod 3$. En effet $a + b\omega \equiv -1 \pmod 3$ équivaut à $3 \mid a + 1 + b\omega$, soit $\frac{a+1}{3} + \frac{b}{3}\omega \in \mathbb{Z}[\omega]$.

Ce concept d'élément primaire permet de distinguer un élément parmi les 6 conjugués d'un élément de A.

Proposition 80. *Soit α un élément de $A = \mathbb{Z}[\omega]$ qui n'est pas une unité et tel que $\lambda = 1 - \omega \nmid \alpha$. Parmi les associés de α, exactement un est primaire.*

Démonstration. Rappelons que $3 = \mathrm{N}(\lambda) = \lambda\overline{\lambda} = -\omega^2\lambda^2$, et donc $\lambda \mid 3$ dans A.

Les associés de $\alpha = a + b\omega$ sont $\alpha, \omega\alpha, \omega^2\alpha, -\alpha, -\omega\alpha, -\omega^2\alpha$, soit

$$a + b\omega, -b + (a - b)\omega, (b - a) - a\omega, -a - b\omega, b + (b - a)\omega, (a - b) + a\omega.$$

Puisque $\lambda \nmid \alpha$, a fortiori $3 \nmid \alpha$, donc a et b ne sont pas tous deux divisibles par 3. Posons $A + B\omega = a + b\omega$ si $3 \nmid a$, et $A + B\omega = -b + (a - b)\omega$ sinon : dans les deux cas $3 \nmid A$. Les éléments $A + B\omega$ et $-A - B\omega$ sont des conjugués de α, et $A \equiv -1 \pmod 3$, ou $-A \equiv -1 \pmod 3$, donc l'un des conjugués $\beta = c + d\omega$ de α vérifie $c \equiv -1 \pmod 3$.

Alors $d \not\equiv 1 \pmod 3$. Sinon $\beta = 3m - 1 + (3n + 1)\omega$, où $m, n \in \mathbb{Z}$, et alors $\beta = 3(m + n\omega) - (1 - \omega)$ est divisible par $1 - \omega$, et donc aussi son associé α, contrairement à l'hypothèse. Ainsi $d \equiv 0 \pmod 3$ ou $d \equiv -1 \pmod 3$. Dans le premier cas, β est primaire, et dans le deuxième cas son associé $-\omega\beta = d + (d - c)\omega \equiv -1 \pmod 3$ est primaire.

Pour montrer l'unicité, notons $a + b\omega$ un des conjugués primaires de α, alors $a \equiv -1, b \equiv 0 \pmod 3$. Vérifions alors que les 5 autres conjugués ne sont pas primaires. Comme $b \equiv 0 \pmod 3$, alors $-b + (a - b)\omega$ n'est pas primaire, ni $b + (b - a)\omega$. De même $a \not\equiv 0 \pmod 3$, donc $(b - a) - a\omega$ n'est pas primaire, ni $(a - b) + a\omega$. Enfin $-a \equiv 1 \pmod 3$, donc $-a - b\omega$ n'est pas primaire. □

Précisons la décomposition d'un élément de A en facteurs premiers.

Proposition 81. *Soit S l'ensemble contenant $\lambda = 1 - \omega$ et tous les premiers primaires. S est un système complet de représentants des classes d'association, soit*

(a) Tout premier de A est associé à un premier de S.

(b) Deux éléments arbitraires distincts de S ne sont pas associés.

Démonstration. (a) Soit π un élément premier de A. Si $\mathrm{N}(\pi) = 3$, π est associé à $1 - \lambda$. Sinon, la proposition 80 montre que π est associé à exactement un premier primaire.

(b) Soient π, μ deux éléments de S associés. Alors ils ont même norme. Ils s'agit de prouver qu'ils sont égaux.

Si $\mathrm{N}(\pi) = \mathrm{N}(\mu) = 3$, alors $\pi = \mu = \lambda$, puisque S contient un seul élément de norme 3, à savoir λ.

Si $\mathrm{N}(\pi) = \mathrm{N}(\mu) \neq 3$, alors π, μ sont des premiers primaires par définition de S, et la proposition 80 montre qu'il n'y a qu'un premier primaire associé π, donc $\pi = \mu$.

□

Proposition 82. *Tout élément $\alpha \in A$ se décompose sous la forme*

$$\alpha = (-1)^a \omega^b \lambda^c \pi_1^{a_1} \cdots \pi_t^{a_t},$$

où les π_i sont des premiers primaires, et a, b, c, a_i sont des entiers, $0 \leq a \leq 1, 0 \leq b \leq 2, a_i > 0$. Cette décomposition est unique à l'ordre près des éléments $\pi_1, \ldots, \pi_t$.

Démonstration. Puisque $A = \mathbb{Z}[\omega]$ est principal, donc factoriel, et S étant un système complet de représentant des classes d'association, tout élément α de A s'écrit de façon unique sous la forme

$$\alpha = u \prod_{\pi \in S} \pi^{e(\pi)},$$

où $e(\pi) \geq 0$ est nul sauf sur un ensemble fini de valeurs de $\pi \in S$, et où u est une unité, donc $u = (-1)^a \omega^b, 0 \leq a \leq 1, 0 \leq b \leq 2$, et a, b sont alors uniquement déterminés. Par définition de S,

$$\alpha = (-1)^a \omega^b \lambda^c \pi_1^{a_1} \cdots \pi_t^{a_t}.$$

□

Notons que si $\gamma, \rho \in A$ sont primaires, alors $-\gamma\rho$ est primaire. En effet, $\gamma \equiv \rho \equiv -1 \pmod 3$, donc $-\gamma\rho \equiv -1 \pmod 3$. Plus généralement, si $\gamma_1, \cdots, \gamma_t$ sont primaires, alors $(-1)^{t-1}\gamma_1 \cdots \gamma_t \equiv -1 \pmod 3$ est primaire.

Proposition 83. *Si γ est un élément primaire de A, alors*

$$\gamma = \pm\gamma_1 \cdots \gamma_t,$$

où $t \geq 1$, et les γ_i sont des premiers primaires (pas nécessairement distincts).

Démonstration. D'après la proposition 12,

$$\gamma = (-1)^a \omega^b \lambda^c \gamma_1 \cdots \gamma_t,$$

où les γ_i sont des premiers primaires, et $a \in \{0, 1\}, b \in \{0, 1, 2\}, c \in \mathbb{N}$. Il faut montrer que $b = c = 0$.

Comme $\gamma, \gamma_1, \ldots \gamma_t$ sont congrus à -1 modulo 3, nous obtenons

$$\omega^b \lambda^c \equiv \pm 1 \pmod 3.$$

Si $c \geq 1$, comme $\lambda \mid 3$, nous obtenons $\lambda \mid 1$. Puisque $\lambda \nmid 1$, c'est une contradiction, donc $c = 0$.

Alors $\omega^b \equiv \pm 1 \pmod 3$, où $\omega^b \in \{1, \omega, -1-\omega\}$. Puisque $\omega \not\equiv \pm 1 \pmod 3$, et $-1-\omega \not\equiv \pm 1 \pmod 3$, alors $\omega^b = 1$, avec $0 \leq b \leq 2$, donc $b = 0$.

En conclusion, tout élément primaire $\gamma \in A$ se décompose sous la forme

$$\gamma = \pm\gamma_1 \cdots \gamma_t,$$

où les γ_i sont des premiers primaires (et le signe $\pm$ est égal à $(-1)^{t-1}$). Ici $t \geq 1$, puisque par définition d'un élément primaire, γ n'est pas une unité. □

3.4 Caractères cubiques généralisés.

De manière analogue à l'extension du symbole de Legendre au symbole de Jacobi, nous allons étendre la définition de χ_γ à des éléments primaires γ de A, pas nécessairement premiers.

Définition 8. *Soit γ un élément primaire de A, et $\gamma = \pm\gamma_1 \cdots \gamma_t$ la décomposition de γ en facteurs premiers primaires. Alors, pour tout $\alpha \in A$,*

$$\chi_\gamma(\alpha) = \chi_{\gamma_1}(\alpha) \cdots \chi_{\gamma_t}(\alpha).$$

Nous noterons aussi

$$\chi_\gamma(\alpha) = \left(\frac{\alpha}{\gamma}\right)_3.$$

Proposition 84. *Soient γ, ρ des éléments primaires de A, et $\alpha, \beta \in A$. Alors*

(a) $\alpha \equiv \beta \pmod{\gamma} \Rightarrow \chi_\gamma(\alpha) = \chi_\gamma(\beta)$.

(b) $\chi_\gamma(\alpha\beta) = \chi_\gamma(\alpha)\chi_\gamma(\beta)$.

(c) $\chi_\rho(\alpha)\chi_\gamma(\alpha) = \chi_{-\rho\gamma}(\alpha)$.

Démonstration. (a) Soit $\gamma = \pm\gamma_1 \cdots \gamma_t$ la décomposition de γ en facteurs premiers primaires. Alors pour tout i, $\alpha \equiv \beta \pmod{\gamma_i}$, donc $\chi_{\gamma_i}(\alpha) = \chi_{\gamma_i}(\beta)$ (proposition 76(b)). Par conséquent $\chi(\alpha) = \prod_{i=1}^t \chi_{\gamma_i}(\alpha) = \prod_{i=1}^t \chi_{\gamma_i}(\beta) = \chi_\gamma(\beta)$.

(b) La proposition 76(a) montre que

$$\begin{aligned}\chi_\gamma(\alpha\beta) &= \chi_{\gamma_1}(\alpha\beta)\chi_{\gamma_2}(\alpha\beta)\cdots\chi_{\gamma_t}(\alpha\beta)\\ &= \chi_{\gamma_1}(\alpha)\chi_{\gamma_2}(\alpha)\cdots\chi_{\gamma_t}(\alpha)\chi_{\gamma_1}(\beta)\chi_{\gamma_2}(\beta)\cdots\chi_{\gamma_t}(\beta)\\ &= \chi_\gamma(\alpha)\chi_\gamma(\beta)\end{aligned}$$

(c) Si $\rho = \pm\rho_1\rho_2\cdots\rho_l$ est primaire, alors $-\rho\gamma$ est primaire, et $-\rho\gamma = \pm\rho_1\rho_2\cdots\rho_l\gamma_1\gamma_2\cdots\gamma_t$, donc

$$\chi_{-\rho\gamma}(\alpha) = (\chi_{\rho_1}\chi_{\rho_2}\cdots\chi_{\rho_l}\chi_{\gamma_1}\chi_{\gamma_2}\cdots\chi_{\gamma_t})(\alpha) = \chi_\rho(\alpha)\chi_\gamma(\alpha).$$

□

3.5 Somme de Gauss associée au caractère χ_π.

Soit π un premier primaire de norme $N(\pi) = p, p \equiv 1 \pmod 3$.

Nous savons que $A/\pi A$ est un corps à p éléments (proposition 71). Il existe donc un isomorphisme φ, et un seul, de $\mathbb{F}_p$ sur $A/\pi A$: cet isomorphisme envoie $[1]_p$ sur $[1]_\pi = 1 + \pi A$, donc $[k]_p$ sur $[k]_\pi = k + \pi A$.

La proposition 76 et son commentaire montrent que l'application χ

$$\begin{array}{ccc}(A/\pi A)^* & \to & \mathbb{C}^*\\ [\alpha] & \mapsto & \left(\frac{\alpha}{\pi}\right)_3\end{array}$$

est un homomorphisme de groupes, et la restriction ϕ de φ à $\mathbb{F}_p^*$ aussi, donc la composée $\psi = \chi \circ \phi$ aussi :

$$\mathbb{F}_p^* \to (A/\pi A)^* \to \mathbb{C}^*.$$

ψ est donc ainsi un caractère cubique sur $\mathbb{F}_p^*$, auquel on peut appliquer les concepts de sommes de Gauss et de Jacobi. En identifiant $\mathbb{F}_p$ avec $A/\pi A$, et ψ avec χ, nous obtenons donc, pour les caractères cubiques χ,

$$g(\chi) = \sum_{t=0}^{p-1} \chi(t)\zeta^t.$$

Les propositions 58 et 60 du chapitre "Sommes de Gauss et sommes de Jacobi" montrent que, pour tout caractère cubique χ sur $\mathbb{F}_p$,

(a) $g(\chi)^3 = pJ(\chi,\chi)$.

(b) Si $J(\chi,\chi) = a + b\omega$, alors $a \equiv -1 \pmod 3$ et $b \equiv 0 \pmod 3$.

Puisque $\mathrm{N}(J(\chi,\chi)) = p$, $J(\chi,\chi)$ est premier dans A, et l'affirmation (b) montre que $J(\chi,\chi)$ est un premier primaire.

• Supposons que π est primaire. Montrons que

$$J(\chi_\pi, \chi_\pi) = \pi.$$

Posons $J(\chi_\pi,\chi_\pi) = \pi'$. Alors $\pi\overline{\pi} = p = \pi'\overline{\pi'}$, si bien que $\pi \mid \pi'$ ou $\pi \mid \overline{\pi'}$, et puisque tous ces éléments ont pour norme p, $\pi \sim \pi'$ ou $\pi \sim \overline{\pi'}$. De plus ces premiers sont primaires, donc $\pi = \pi'$ ou $\pi = \overline{\pi'}$. Il s'agit d'éliminer la seconde possibilité.

Par définition,

$$\begin{aligned} J(\chi_\pi,\chi_\pi) &= \sum_{x=0}^{p-1} \chi_\pi(x)\chi_\pi(1-x) \\ &\equiv \sum_{x=0}^{p-1} x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}} \pmod \pi. \end{aligned}$$

Le polynôme $X^{\frac{p-1}{3}}(1-X)^{\frac{p-1}{3}} = \sum_{k=0}^{d} a_k X^k$ est de degré $d = \frac{2}{3}(p-1) < p-1$, et son coefficient constant a_0 est nul.

Si $1 \le k \le d < p-1$, posons $S_k = 1^k + 2^k + \cdots + (p-1)^k$. Comme $p-1 \nmid k$, il existe un élément $a \in \mathbb{F}_p^*$ tel que $a^k \neq 1$ (on peut prendre par exemple pour a un générateur de $\mathbb{F}_p^*$). Puisque $i \mapsto j = ai$ est une bijection de $\mathbb{F}_p^*$, le changement d'indice $j = ai$ donne

$$a^k S_k \equiv \sum_{i=0}^{p-1} (ai)^k \equiv \sum_{j=0}^{p-1} j^k = S_k \pmod p.$$

Comme $a^k \not\equiv 1 \pmod p$, $S_k \equiv 0 \pmod p$, a fortiori $S_k \equiv 0 \pmod \pi$, donc $J(\chi_\pi,\chi_\pi) = \sum_{k=1}^{d} a_k S_k \equiv 0 \pmod \pi$. Ainsi

$$J(\chi_\pi,\chi_\pi) \equiv 0 \pmod \pi.$$

Donc $\pi \mid \pi'$, et ainsi $\pi = \pi' = J(\chi_\pi,\chi_\pi)$.

En utilisant l'affirmation (a), nous obtenons alors $g(\chi_\pi)^3 = p\pi$.

Nous avons prouvé la proposition suivante :

Proposition 85. *Soit π un premier primaire de norme $\mathrm{N}(\pi) = p$, $p \equiv 1 \pmod 3$. Alors*

$$g(\chi_\pi)^3 = p\pi.$$

3.6 Loi de réciprocité cubique.

Puisque $\overline{\lambda} = 1 - \omega^2 = -\omega^2(1-\omega) = -\omega^2\lambda$, les premiers $\lambda, \overline{\lambda}$ sont associés. Alors les éléments α de norme 3 sont premiers, et vérifient $\alpha\overline{\alpha} = 3 = \lambda\overline{\lambda} = -\omega^2\lambda^2$. Ils sont donc associés à λ, et ne sont pas primaires. Ainsi un premier primaire π vérifie $\mathrm{N}(\pi) \neq 3$.

Nous pouvons maintenant énoncer la loi de réciprocité cubique, en considérant d'abord le cas de deux premiers primaires de normes distinctes, ce qui revient à dire qu'ils sont distincts et non conjugués.

Proposition 86. *Soient π_1, π_2 des premiers primaires tels que $\mathrm{N}(\pi_1) \neq \mathrm{N}(\pi_2)$. Alors*

$$\left(\frac{\pi_2}{\pi_1}\right)_3 = \left(\frac{\pi_1}{\pi_2}\right)_3.$$

Démonstration. Trois cas sont à considérer. Le premier cas correspond à $\pi_1 = q, \pi_2 = q'$, où q, q' sont des premiers rationnels positifs congrus à -1 modulo 3 : ce cas a déjà été traité dans la remarque 2 suivant la proposition 79. Le deuxième cas consiste à supposer que $\pi_1 = q$, et que π_2 vérifie $\mathrm{N}(\pi) = p$, p premier rationnel congru à 1 modulo 3. Le troisième cas est la cas où π_1, π_2 ont tous deux pour norme un nombre premier.

• Commençons par le cas 2 : $q \equiv -1 \pmod 3$ est un premier rationnel positif, et π un premier de A tel que $\mathrm{N}(\pi) = p \equiv 1 \pmod 3$, p premier. Il s'agit de prouver que $\left(\frac{\pi}{q}\right)_3 = \left(\frac{q}{\pi}\right)_3$.

La proposition 85 donne

$$g(\chi_\pi)^3 = p\pi.$$

Elevons cette égalité à la puissance $(q^2-1)/3$:

$$g(\chi_\pi)^{q^2-1} = (p\pi)^{\frac{q^2-1}{3}}.$$

En réduisant modulo q, comme $\mathrm{N}(q) = q^2$,

$$g(\chi_\pi)^{q^2-1} \equiv \chi_q(p\pi) \pmod q.$$

Comme $\chi_q(p) = 1$ (proposition 79), ceci donne, en multipliant par $g(\chi_\pi)$,

$$g(\chi_\pi)^{q^2} \equiv \chi_q(\pi) g(\chi_\pi) \pmod q. \tag{3.1}$$

Par ailleurs,

$$\begin{aligned} g(\chi_\pi)^{q^2} &= \left(\sum_{t=0}^{p-1} \chi_\pi(t)\zeta^t\right)^{q^2} \\ &\equiv \sum_{t=0}^{p-1} \chi_\pi(t)^{q^2} \zeta^{q^2 t} \pmod q. \end{aligned}$$

Puisque $q^2 \equiv 1 \pmod 3$, et que $\chi_\pi(t)$ est une racine cubique de l'unité, $\chi_\pi(t)^{q^2} = \chi_\pi(t)$, donc

$$g(\chi_\pi)^{q^2} \equiv g_{q^2}(\chi_\pi) \pmod q.$$

La proposition 50 du chapitre "Sommes de Gauss et sommes de Jacobi" donne $g_{q^2}(\chi_\pi) = \chi_\pi(q^{-2})g(\chi_\pi) = \chi_\pi(q)g(\chi_\pi)$. Ainsi

$$g(\chi_\pi)^{q^2} \equiv \chi_\pi(q)g(\chi_\pi) \pmod{q} \tag{3.2}$$

En combinant (3.1) et (3.2), nous obtenons

$$\chi_\pi(q)g(\chi_\pi) \equiv \chi_q(\pi)g(\chi_\pi) \pmod{q}.$$

Multiplions les deux membres de cette congruence par $\overline{g(\chi_\pi)}$. Puisque $g(\chi_\pi)\overline{g(\chi_\pi)} = p$,

$$\chi_\pi(q)p \equiv \chi_q(\pi)p \pmod{q}.$$

Comme $p \wedge q = 1$,

$$\chi_\pi(q) \equiv \chi_q(\pi) \pmod{q}.$$

Les classes de $1, \omega, \omega^2$ étant distinctes dans A/qA,

$$\chi_\pi(q) = \chi_q(p).$$

• Il reste à traiter le cas où π_1, π_2 sont des premiers tels que $\mathrm{N}(\pi_1) = p_1 \equiv 1 \pmod 3$ et $\mathrm{N}(\pi_2) = p_2 \equiv 1 \pmod 3$.

Notons $\gamma_1 = \overline{\pi_1}$ et $\gamma_2 = \overline{\pi_2}$. Alors γ_1 et γ_2 sont des premiers primaires, et $p_1 = \pi_1\gamma_1, p_2 = \pi_2\gamma_2$.

Mettons en oeuvre la même méthode que précédemment. Partons de l'égalité

$$g(\chi_{\gamma_1})^3 = p_1\gamma_1$$

prouvée ci dessus pour les premiers primaires. L'élévation à la puissance $\frac{\mathrm{N}(\pi_2)-1}{3} = \frac{p_2-1}{3}$ donne

$$g(\chi_{\gamma_1})^{p_2-1} = (p_1\gamma_1)^{\frac{p_2-1}{3}},$$

et la réduction modulo π_2 donne

$$g(\chi_{\gamma_1})^{p_2-1} \equiv \chi_{\pi_2}(p_1\gamma_1) \pmod{\pi_2},$$

donc

$$g(\chi_{\gamma_1})^{p_2} \equiv \chi_{\pi_2}(p_1\gamma_1)g(\chi_{\gamma_1}) \pmod{\pi_2}. \tag{3.3}$$

De plus,

$$\begin{aligned} g(\chi_{\gamma_1})^{p_2} &= \left(\sum_{t=0}^{p_2-1} \chi_{\gamma_1}(t)\zeta^t\right)^{p_2} \\ &\equiv \sum_{t=0}^{p_2-1} \chi_{\gamma_1}(t)^{p_2}\zeta^{p_2 t} \pmod{\pi_2} \end{aligned}$$

Comme $p_2 \equiv 1 \pmod 3$, $\chi_{\gamma_1}(t)^{p_2} = \chi_{\gamma_1}(t)$, donc

$$g(\chi_{\gamma_1})^{p_2} \equiv g_{p_2}(\chi_{\gamma_1}) \pmod{\pi_2}$$

Comme

$$\begin{aligned} g_{p_2}(\chi_{\gamma_1}) &= \chi_{\gamma_1}(p_2^{-1})g(\chi_{\gamma_1}) \\ &= \chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1}), \end{aligned}$$

nous en déduisons

$$g(\chi_{\gamma_1})^{p_2} \equiv \chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1}) \pmod{\pi_2}. \tag{3.4}$$

La comparaison des congruences (3.3) et (3.4) donne

$$\chi_{\gamma_1}(p_2^2)g(\chi_{\gamma_1}) \equiv \chi_{\pi_2}(p_1\gamma_1)g(\chi_{\gamma_1}) \pmod{\pi_2}.$$

En multipliant par $\overline{g(\chi_{\gamma_1})}$, puisque $g(\chi_{\gamma_1})\overline{g(\chi_{\gamma_1})} = p_1$, nous obtenons

$$p_1\,\chi_{\gamma_1}(p_2^2) \equiv p_1\,\chi_{\pi_2}(p_1\gamma_1) \pmod{\pi_2}.$$

Comme $\mathrm{N}(\pi_1) \neq \mathrm{N}(\pi_2)$ par hypothèse, $p_1 \neq p_2$, donc les entiers p_1, p_2 sont premiers entre eux dans $\mathbb{Z}$, donc dans A, a fortiori π_2 est premier avec p_1 dans A. Par conséquent

$$\chi_{\gamma_1}(p_2^2) \equiv \chi_{\pi_2}(p_1\gamma_1) \pmod{\pi_2}.$$

Les classes de $1, \omega, \omega^2$ étant distinctes dans $A/\pi_2 A$, nous pouvons conclure que

$$\chi_{\gamma_1}(p_2^2) = \chi_{\pi_2}(p_1\gamma_1). \tag{3.5}$$

En remplaçant dans les calculs précédents le couple (γ_1, π_2) par le couple (π_2, π_1), et donc en échangeant p_1 et p_2, nous obtenons de même

$$\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\pi_2). \tag{3.6}$$

Rappelons le résultat de la proposition 78, qui montre que $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$. Alors

$$\chi_{\gamma_1}(p_2^2) = \chi_{\overline{\pi_1}}(p_2^2) = \chi_{\overline{\pi_1}}\left(\overline{p_2^2}\right) = \overline{\chi_{\pi_1}(p_2^2)} = \overline{\chi_{\pi_1}(p_2)^2} = \chi_{\pi_1}(p_2),$$

et ainsi

$$\chi_{\gamma_1}(p_2^2) = \chi_{\pi_1}(p_2). \tag{3.7}$$

En utilisant les égalités (3.5),(3.6) et (3.7), nous obtenons

$$\begin{aligned} \chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) &= \chi_{\pi_1}(\pi_2)\chi_{\gamma_1}(p_2^2) && \text{(égalité (3.5))} \\ &= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2) && \text{(égalité (3.7))} \\ &= \chi_{\pi_1}(p_2\pi_2) \\ &= \chi_{\pi_2}(p_1^2) && \text{(égalité (3.6))} \\ &= \chi_{\pi_2}(p_1\pi_1\gamma_1) \\ &= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1) \end{aligned}$$

En simplifiant par $\chi_{\pi_2}(p_1\gamma_1) \neq 0$, nous obtenons bien

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1).$$

□

3.7 Autre démonstration de la réciprocité cubique.

A l'aide des sommes de Jacobi généralisées, donnons une nouvelle preuve de la loi de réciprocité cubique (proposition 16).

Lemme. *Soient p, q deux nombres premiers rationnels distincts, et χ un caractère sur $\mathbb{F}_p$. Considérons*

$$S = J(\chi, \ldots, \chi)$$

la somme de Jacobi avec q entrées égales à χ. Alors

$$J(\chi, \ldots, \chi) \equiv \chi^q(q^{-1}) \pmod{q}.$$

Démonstration. Considérons la somme de Jacobi $S = J(\chi, \ldots, \chi)$, avec q entrées égales à χ :

$$S = J(\chi_1, \ldots, \chi_q), \quad \text{où } \chi_1 = \ldots = \chi_q = \chi,$$

χ étant un caractère sur $\mathbb{F}_p$.

Alors

$$S = J(\chi, \ldots, \chi) = \sum_{(x_1,\ldots,x_q)\in X} \chi(x_1)\cdots\chi(x_q),$$

où

$$X = \{(x_1, \ldots, x_q) \in (\mathbb{F}_p)^q \mid x_1 + \cdots + x_q = 1\}.$$

Définissons une action à droite de S_q sur $(\mathbb{F}_p)^q$ par

$$(x_1, \ldots, x_q)^\sigma = (x_{\sigma(1)}, \ldots, x_{\sigma(q)}), \qquad (x_1, \ldots, x_q) \in \mathbb{F}_p^q, \sigma \in S_q.$$

Vérifions qu'il s'agit bien d'une action à droite :

si $x = (x_1, \ldots, x_q) \in (\mathbb{F}_p)^q$, et $\sigma, \sigma' \in S_n$, alors

$$\begin{aligned}
x^e &= x, \\
(x^\sigma)^{\sigma'} &= ((x_1, \ldots, x_q)^\sigma)^{\sigma'} \\
&= (x_{\sigma(1)}, \ldots, x_{\sigma(q)})^{\sigma'} \\
&= (y_1, \ldots, y_q)^{\sigma'} && (\text{où } y_i = x_{\sigma(i)}) \\
&= (y_{\sigma'(1)}, \ldots, y_{\sigma'(q)}) \\
&= (x_{\sigma(\sigma'(1))}, \ldots, x_{\sigma(\sigma'(q))}) && (\text{puisque } y_{\sigma'(j)} = x_{\sigma(\sigma'(j))}) \\
&= (x_1, \ldots, x_q)^{\sigma\circ\sigma'} \\
&= x^{\sigma\sigma'}.
\end{aligned}$$

Le cycle $\tau = (1\,2\,\cdots\,q) \in S_q$ engendre un sous-groupe $H = \langle\tau\rangle$ de S_q d'ordre q. Pour tout $x = (x_1, \cdots, x_q) \in (\mathbb{F}_p)^q$, $(x_1, \cdots, x_q)^\tau = (x_2, \ldots, x_q, x_1)$. Par conséquent τ laisse stable X, puisque

$$x = (x_1, \cdots, x_q) \in X \Rightarrow x_1 + \cdots + x_q = 1 \Rightarrow x_2 + \ldots + x_q + x_1 = 1 \Rightarrow x^\tau \in X.$$

Ceci prouve

$$x \in X \Rightarrow x^\tau \in X.$$

Par conséquent, si on restreint l'action de G au sous-groupe H, $H = \langle\tau\rangle$ opère à droite sur X.

Calculons le cardinal de X. Puisqu'un q-uplet de X est déterminé par ses $q-1$ premiers éléments,

$$|X| = p^{q-1}.$$

Comme $H = \langle\tau\rangle$ opère sur X, la formule orbite-stabilisateur donne, pour tout $x \in X$, en notant $\mathcal{O}_x = x^H$ l'orbite de x sous l'action de H, et H_x le stabilisateur de x,

$$|\mathcal{O}_x| = (H : H_x) = |H|/|H_x|.$$

Par conséquent $|\mathcal{O}_x|$ divise $|H| = q$. Comme q est premier, le cardinal d'une orbite $\mathcal{O}_x$ est soit 1, soit q.

$$\forall x \in X,\ |\mathcal{O}_x| = 1 \text{ ou } |\mathcal{O}_x| = q.$$

A quelle condition $x \in X$ vérifie-t-il $|\mathcal{O}_x| = 1$?

Comme $H = \{e, \tau, \cdots, \tau^{q-1}\}$,

$$\mathcal{O}_x = \{x, x^\tau, \cdots, x^{\tau^{q-1}}\}.$$

Par conséquent, pour tout $x = (x_1, \ldots, x_q) \in X$,

$$\begin{aligned} |\mathcal{O}_x| = 1 &\iff x = x^\tau = x^{\tau^2} = \cdots = x^{\tau^{q-1}} \\ &\iff x^\tau = x \\ &\iff (x_2, x_3, \ldots, x_q, x_1) = (x_1, x_2, \ldots, x_q) \\ &\iff x_1 = x_2 = \cdots = x_q. \end{aligned}$$

Définissons

$$Y = \{(x_1, \ldots, x_q) \in X \mid x_1 = x_2 = \cdots = x_q\}.$$

Soit $x = (x_1, \ldots, x_q) \in \mathbb{F}_p^q$. Alors $x \in Y$ si et seulement s'il existe $a \in \mathbb{F}_p$ tel que $x = (a, \ldots, a)$ et $qa = 1$, soit $a = q^{-1}$. Ainsi $|Y| = 1$, le seul élément de Y étant l'élément $y = (a, \ldots, a)$, où $a = q^{-1}$ est l'inverse de q dans $\mathbb{F}_p$.

Nous avons montré que

$$Y = \{(x_1, \ldots, x_q) \in X \mid x_1 = x_2 = \cdots = x_p\} = \{x \in X \mid \quad |\mathcal{O}_x| = 1\} = \{y\}.$$

Comme les orbites de l'action de H sur X forment une partition de X, en notant S un système complet de représentants des orbites,

$$X = \coprod_{x \in S} \mathcal{O}_x$$

(réunion disjointe des orbites).

Si une orbite est réduite à un seul élément, i.e. $\mathcal{O}_x = \{x\}$, alors son unique représentant ne peut être que y, donc $y \in S$, et ainsi

$$X = \{y\} \cup \bigcup_{x \in S \setminus \{y\}} \mathcal{O}_x.$$

(Alors $|X| = \sum_{x \in S} |\mathcal{O}_x| = 1 + \sum_{x \in S\setminus\{y\}} |\mathcal{O}_x|$. Comme $q \mid |\mathcal{O}_x|$ pour tout $x \neq y$, nous obtenons $|X| \equiv 1 \pmod q$, ce qui n'est pas surprenant puisque $|X| = p^{q-1} \equiv 1 \pmod q$!)

Par conséquent,

$$\begin{aligned} S = J(\chi,\dots,\chi) &= \sum_{(x_1,\dots,x_q)\in X} \chi(x_1)\cdots\chi(x_q) \\ &= \chi(a)^q + \sum_{x\in S\setminus\{y\}} \sum_{(x_1,\dots,x_q)\in\mathcal{O}_x} \chi(x_1)\dots\chi(x_q) \\ &= \chi^q(q^{-1}) + \sum_{x\in S\setminus\{y\}} \sum_{(x_1,\dots,x_q)\in\mathcal{O}_x} \chi(x_1)\dots\chi(x_q). \end{aligned}$$

De plus, si $x \in S\setminus\{y\}$, le produit $\chi(x_1)\cdots\chi(x_p)$ est constant sur l'orbite $\mathcal{O}_x$, puisque $\chi(x_{\tau(1)})\cdots\chi(x_{\tau(p)}) = \chi(x_1)\cdots\chi(x_p)$. Par conséquent

$$q \mid \sum_{(x_1,\dots,x_q)\in\mathcal{O}_x} \chi(x_1)\cdots\chi(x_q), \qquad (x \in S\setminus\{y\}).$$

Ainsi

$$S = J(\chi,\dots,\chi) \equiv \chi^q(q^{-1}) \pmod q.$$

□

Démonstration. (proposition 86)

Trois cas sont à considérer.

- Le premier cas correspond à $\pi_1 = q, \pi_2 = q'$, où q, q' sont des premiers rationnels positifs distincts congrus à -1 modulo 3.

  Alors $q \wedge q' = 1$. La proposition 79 donne $\chi_q(q') = 1 = \chi_{q'}(q)$.

- Dans le deuxième cas, $\pi_1 = q$ est un premier rationnel positif congru à -1 modulo 3, et $\pi_2 = \pi$ vérifie $\mathrm{N}(\pi) = p$, où p est un premier rationnel congru à 1 modulo 3.

  Posons $\chi = \chi_\pi$. Appliquons le lemme à $J(\chi,\dots,\chi)$, avec q entrées égales à χ :

$$J(\chi,\dots,\chi) \equiv \chi^q(q^{-1}) \pmod q.$$

  Puisqu'ici $q \equiv 2 \pmod 3$, $\chi^q = \chi^2 = \chi^{-1}$, donc

$$J(\chi,\dots,\chi) \equiv \chi(q) \pmod q.$$

  Comme $3 \mid q+1$, $\chi^{q+1} = \varepsilon$ est le caractère trivial, et χ n'est pas trivial. La proposition 66 du chapitre "Sommes de Gauss et sommes de Jacobi" donne

$$g(\chi)^{q+1} = pJ(\chi,\dots,\chi).$$

  D'après la proposition 85, $g(\chi_\pi)^3 = p\pi$, donc

$$g(\chi)^{q+1} = (p\pi)^{\frac{q+1}{3}}.$$

Par conséquent,

$$(p\pi)^{\frac{q+1}{3}} \equiv p\chi(q) \pmod q,$$

ou encore

$$p^{\frac{q-2}{3}}\pi^{\frac{q+1}{3}} \equiv \chi(q) \pmod q.$$

En élevant les deux membres à la puissance $q-1$, sachant que $q-1 \equiv 1 \pmod 3$,

$$(p^{\frac{q-2}{3}})^{q-1}\pi^{\frac{q^2-1}{3}} \equiv \chi(q) \pmod q.$$

Comme $(p^{\frac{q-2}{3}})^{q-1} \equiv 1 \pmod{q}$ d'après le petit théorème de Fermat, et puisque $\pi^{\frac{q^2-1}{3}} \equiv \chi_q(\pi) \pmod{q}$ par définition, nous obtenons

$$\chi_q(\pi) \equiv \chi_\pi(q) \pmod{q},$$

donc

$$\chi_q(\pi) = \chi_\pi(q).$$

- Il reste le cas où π_1, π_2 sont des premiers primaires tels que $p_1 = \mathrm{N}(\pi_1) = \pi_1\overline{\pi_1}, p_2 = \mathrm{N}(\pi_2) = \pi_2\overline{\pi_2}$ sont des premiers rationnels congrus à 1 modulo 3. Ecrivons $\gamma_1 = \overline{\pi_1}, \gamma_2 = \overline{\pi_2}$, si bien que

$$p_1 = \pi_1\gamma_1, \qquad p_2 = \pi_2\gamma_2.$$

Comme χ_{γ_1} est un caractère d'ordre 3, et $p_2 \equiv 1 \pmod{3}$, $\chi_{\gamma_1}^{p_2} = \chi_{\gamma_1} \neq \varepsilon$. La proposition 65 du chapitre "Sommes de Gauss et sommes de Jacobi" donne alors

$$g(\chi_{\gamma_1})^{p_2} = J(\chi_{\gamma_1}, \ldots, \chi_{\gamma_1}) g(\chi_{\gamma_1}^{p_2}),$$

où la somme de Jacobi $J(\chi_{\gamma_1}, \ldots, \chi_{\gamma_1})$ a p_2 entrées égales à χ_{γ_1}.

Puisque $\chi_{\gamma_1}^{p_2} = \chi_{\gamma_1}$,

$$\left[g(\chi_{\gamma_1})^3\right]^{\frac{p_2-1}{3}} = J(\chi_{\gamma_1}, \ldots, \chi_{\gamma_1}).$$

La proposition 85 montre que $g(\chi_{\gamma_1})^3 = p_1\gamma_1$, donc

$$(p_1\gamma_1)^{\frac{p_2-1}{3}} = J(\chi_{\gamma_1}, \ldots, \chi_{\gamma_1}).$$

En appliquant une nouvelle fois le lemme, avec ici $p = p_1, q = p_2$, (où $p_1 \neq p_2$) et $\chi = \chi_{\gamma_1}$, nous obtenons

$$J(\chi_{\gamma_1}, \ldots, \chi_{\gamma_1}) \equiv \chi_{\gamma_1}^{p_2}(p_2^{-1}) \pmod{p_2}.$$

Comme $p_2 \equiv 1 \pmod{3}$,

$$J(\chi_{\gamma_1}, \ldots, \chi_{\gamma_1}) \equiv \chi_{\gamma_1}(p_2^{-1}) = \chi_{\gamma_1}(p_2^2) \pmod{p_2}.$$

Par conséquent,

$$(p_1\gamma_1)^{\frac{p_2-1}{3}} \equiv \chi_{\gamma_1}(p_2^2) \pmod{\pi_2},$$

soit encore

$$\chi_{\pi_2}(p_1\gamma_1) \equiv \chi_{\gamma_1}(p_2^2) \pmod{\pi_2}. \tag{3.8}$$

En remplaçant dans les calculs précédents le couple (γ_1, π_2) par le couple (π_2, π_1), et donc en échangeant p_1 et p_2, nous obtenons de même

$$\chi_{\pi_2}(p_1^2) = \chi_{\pi_1}(p_2\pi_2). \tag{3.9}$$

Rappelons le résultat de la proposition 78, qui montre que $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$. Alors

$$\chi_{\gamma_1}(p_2^2) = \chi_{\overline{\pi_1}}(p_2^2) = \chi_{\overline{\pi_1}}\left(\overline{p_2^2}\right) = \overline{\chi_{\pi_1}(p_2^2)} = \overline{\chi_{\pi_1}(p_2)^2} = \chi_{\pi_1}(p_2),$$

et ainsi

$$\chi_{\gamma_1}(p_2^2) = \chi_{\pi_1}(p_2). \tag{3.10}$$

En utilisant les égalités (3.8),(3.9) et (3.10), nous obtenons

$$\begin{aligned}
\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) &= \chi_{\pi_1}(\pi_2)\chi_{\gamma_1}(p_2^2) && \text{(égalité (3.8))}\\
&= \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2) && \text{(égalité (3.10))}\\
&= \chi_{\pi_1}(p_2\pi_2)\\
&= \chi_{\pi_2}(p_1^2) && \text{(égalité (3.9))}\\
&= \chi_{\pi_2}(p_1\pi_1\gamma_1)\\
&= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1)
\end{aligned}$$

En simplifiant par $\chi_{\pi_2}(p_1\gamma_1) \neq 0$, on obtient bien

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1).$$

□

3.8 Réciprocité cubique générale.

Le cas où $\mathrm{N}(\pi_1) = \mathrm{N}(\pi_2)$ n'est pas traité dans la proposition 86. Étendons à ce cas la réciprocité cubique.

Lemme. *Soit $n \in \mathbb{Z}$ un entier primaire (i.e. $n \equiv -1 \pmod 3$), et soit π un premier primaire tel que $\mathrm{N}(\pi) = p \equiv 1 \pmod 3$. Alors*

$$\left(\frac{n}{\pi}\right)_3 = \left(\frac{\pi}{n}\right)_3.$$

Démonstration. Si $p \mid n$, alors $\pi \mid n$, donc $\left(\frac{n}{\pi}\right)_3 = 0 = \left(\frac{\pi}{n}\right)_3$. Nous pouvons maintenant supposer que $p \wedge n = 1$.

Comme n est primaire, il se décompose sous la forme

$$\begin{aligned}
n &= \pm p_1 \cdots p_s q_1 \cdots q_r \qquad (p_i \equiv 1\ [3], q_j \equiv -1\ [3])\\
&= \pm \pi_1\overline{\pi_1} \cdots \pi_s\overline{\pi}_s q_1 \cdots q_r,
\end{aligned}$$

où $\pi_i, \overline{\pi_i} (1 \leq i \leq s)$ et $q_j (1 \leq j \leq r)$ sont des premiers primaires.

Puisque $\mathrm{N}(\pi) = p \neq p_i = \mathrm{N}(\pi_i)$ et $\mathrm{N}(\pi) = p \neq \mathrm{N}(q_j) = q_j^2$, la proposition 86 (réciprocité cubique) montre que

$$\begin{aligned}
\left(\frac{n}{\pi}\right)_3 &= \left(\frac{\pi_1}{\pi}\right)_3 \left(\frac{\overline{\pi_1}}{\pi}\right)_3 \cdots \left(\frac{\pi_s}{\pi}\right)_3 \left(\frac{\overline{\pi_s}}{\pi}\right)_3 \left(\frac{q_1}{\pi}\right)_3 \cdots \left(\frac{q_r}{\pi}\right)_3\\
&= \left(\frac{\pi}{\pi_1}\right)_3 \left(\frac{\pi}{\overline{\pi_1}}\right)_3 \cdots \left(\frac{\pi}{\pi_s}\right)_3 \left(\frac{\pi}{\overline{\pi_s}}\right)_3 \left(\frac{\pi}{q_1}\right)_3 \cdots \left(\frac{\pi}{q_r}\right)_3\\
&= \left(\frac{\pi}{n}\right)_3.
\end{aligned}$$

□

Nous pouvons alors supprimer l'hypothèse inutile $\mathrm{N}(\pi_1) \neq \mathrm{N}(\pi_2)$ dans la proposition 86.

Proposition 87. *Soient π_1, π_2 des premiers primaires. Alors*

$$\left(\frac{\pi_2}{\pi_1}\right)_3 = \left(\frac{\pi_1}{\pi_2}\right)_3.$$

Démonstration. Il ne reste à examiner que le cas où $\mathrm{N}(\pi_1) = \mathrm{N}(\pi_2)$.

Si $\pi_1 = \pi_2$, alors $\left(\frac{\pi_2}{\pi_1}\right)_3 = \left(\frac{\pi_1}{\pi_2}\right)_3 = 0$.

Si $\pi_1 \neq \pi_2$, comme π_1 et π_2 sont primaires, alors π_1, π_2 sont des premiers tels que $\mathrm{N}(\pi_1) = \mathrm{N}(\pi_2) = p \equiv 1 \pmod 3$, et $\pi_2 = \overline{\pi_1}$. En notant $\pi = \pi_1$, il suffit de prouver que

$$\left(\frac{\overline{\pi}}{\pi}\right)_3 = \left(\frac{\pi}{\overline{\pi}}\right)_3.$$

Utilisons la "ruse d'Evans" (voir [Lemmermayer]). L'élément $n = -\pi - \overline{\pi}$ est un entier rationnel, qui est primaire. Le lemme donne alors

$$\begin{aligned}
\left(\frac{\overline{\pi}}{\pi}\right)_3 &= \left(\frac{\pi + \overline{\pi}}{\pi}\right)_3 \\
&= \left(\frac{-\pi - \overline{\pi}}{\pi}\right)_3 \\
&= \left(\frac{\pi}{-\pi - \overline{\pi}}\right)_3 \\
&= \left(\frac{-\overline{\pi}}{-\pi - \overline{\pi}}\right)_3 \\
&= \left(\frac{\overline{\pi}}{-\pi - \overline{\pi}}\right)_3 \\
&= \left(\frac{-\pi - \overline{\pi}}{\overline{\pi}}\right)_3 \qquad \text{(lemme)} \\
&= \left(\frac{-\pi}{\overline{\pi}}\right)_3 \\
&= \left(\frac{\pi}{\overline{\pi}}\right)_3
\end{aligned}$$

□

Nous obtenons alors la loi de réciprocité cubique pour les caractères généralisés.

Proposition 88. *Si χ, ρ sont des éléments primaires de A, alors*

$$\chi_\gamma(\rho) = \chi_\rho(\gamma).$$

Démonstration. Décomposons ρ, γ en facteurs premiers primaires, sous la forme

$$\begin{aligned}
\rho &= \pm\rho_1\rho_2\cdots\rho_l, \\
\gamma &= \pm\gamma_1\gamma_2\cdots\gamma_m,
\end{aligned}$$

La loi de réciprocité cubique donne alors

$$\begin{aligned}\chi_\gamma(\rho) &= \prod_{j=1}^{m} \chi_{\gamma_j}(\rho) \\ &= \prod_{j=1}^{m}\prod_{i=1}^{l} \chi_{\gamma_j}(\rho_i) \\ &= \prod_{i=1}^{l}\prod_{j=1}^{m} \chi_{\gamma_j}(\rho_i) \\ &= \prod_{i=1}^{l}\prod_{j=1}^{m} \chi_{\rho_i}(\gamma_j) \\ &= \prod_{i=1}^{l} \chi_{\rho_i}(\gamma) \\ &= \chi_\rho(\gamma).\end{aligned}$$

□

3.9 Résidus cubiques entiers.

Soit p un premier rationnel. A quelle condition un entier $a \in \mathbb{Z}$, où $p \nmid a$, est-il un résidu cubique, i.e. existe-t-il $x \in \mathbb{Z}$ tel que $x^3 \equiv a \pmod p$?

Si $p = 3$, $a^2 \equiv 1 \pmod 3$, donc $a^3 \equiv a \pmod 3$, et donc a est un résidu cubique.

Supposons maintenant que $p \equiv 2 \pmod 3$. Puisque $d = 3 \wedge (p-1) = 1$, et $a^{p-1} \equiv 1 \pmod p$, la proposition 24 du chapitre "Sommes de Gauss et sommes de Jacobi" montre qu'il existe un $x \in \mathbb{Z}$ tel que $x^3 \equiv a \pmod p$, et qu'il n'existe qu'une solution modulo p. Autrement dit l'application

$$\begin{cases} \mathbb{F}_p^* \to \mathbb{F}_p^* \\ x \mapsto x^3 \end{cases}$$

est une bijection.

Plus intéressant est le cas où $p \equiv 1 \pmod 3$. Alors $p = \mathrm{N}(\pi)$, où $\pi = a + b\omega$ est un premier de A.

S'il existe $x \in \mathbb{Z}$ tel que $x^3 \equiv a \pmod p$, a fortiori $x^3 \equiv a \pmod \pi$. Alors la proposition 77 montre que $\left(\frac{a}{\pi}\right)_3 = 1$.

Réciproquement, si $\left(\frac{a}{\pi}\right)_3 = 1$, la proposition 77 montre l'existence de $\alpha \in A$ tel que $\alpha^3 \equiv a \pmod \pi$. De plus nous savons (voir la démonstration de la proposition 71) qu'il existe $x \in T = \{0, 1, \cdots, p-1\}$ tel que $\alpha \equiv x \pmod \pi$, donc $x^3 \equiv a \pmod \pi$, où $x \in \mathbb{Z}$.

Alors $\pi \mid x^3 - a$, donc $p = \mathrm{N}(\pi) \mid \mathrm{N}(x^3 - a) = (x^3 - a)^2$, et p est un premier rationnel, donc $p \mid x^3 - a$, soit $x^3 \equiv a \pmod p$.

Notons que 0 est toujours le cube de 0.

Nous avons donc prouvé la proposition suivante.

Proposition 89. *Soit p un nombre premier, et $a \in \mathbb{Z}$.*

- *Si $p = 3$, ou si $p \equiv 2 \pmod 3$, il existe un $x \in \mathbb{Z}$ tel que $x^3 \equiv a \pmod p$.*
- *Si $p \equiv 1 \pmod 3$, où $p \nmid a$, alors $p = \mathrm{N}(\pi)$, où π est un premier de A, et*

$$\exists x \in \mathbb{Z},\ x^3 \equiv a \pmod p \iff \left(\frac{a}{\pi}\right)_3 = 1 \iff \exists \alpha \in A,\ \alpha^3 \equiv a \pmod \pi.$$

3.10 Le caractère cubique de 2.

Nous étudions ici la question suivante. Quels sont les premiers π de A tels que l'équation $x^3 \equiv 2 \pmod{\pi}$ admet une solution dans A ?

Notons d'abord que, si π, π' sont associés, l'équation $x^3 \equiv 2 \pmod{\pi}$ a des solutions si et seulement si $x^3 \equiv 2 \pmod{\pi'}$ a des solutions. Il suffit donc d'étudier le cas où π est un premier primaire.

Si $\pi = q$ est un premier de $\mathbb{N}$, où $q \equiv 2 \pmod 3, q \neq 2$, alors $\chi_q(2) = 1$, donc 2 est un résidu cubique pour q.

Supposons maintenant que $\pi = a + b\omega$ est un premier primaire tel que $\mathrm{N}(\pi) = p$, où $p \equiv 1 \pmod 3$ est premier. Comme 2 et π sont des premiers primaires, la loi de réciprocité cubique donne

$$\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3.$$

Par définition de $\left(\frac{\pi}{2}\right)_3$, comme $\mathrm{N}(2) = 4$,

$$\left(\frac{\pi}{2}\right)_3 \equiv \pi^{\frac{\mathrm{N}(2)-1}{3}} = \pi \pmod 2.$$

Ainsi $\left(\frac{2}{\pi}\right)_3 = 1$ si et seulement si $\pi \equiv 1 \pmod 2$, soit $a \equiv 1 \pmod 2, b \equiv 0 \pmod 2$. En utilisant la proposition 89, nous avons prouvé la proposition suivante.

Proposition 90. *Si $\pi = a + b\omega$ est un premier primaire de A tel que $\mathrm{N}(\pi) = p \equiv 1 \pmod 3$, alors*

$$\begin{aligned} \exists x \in \mathbb{Z},\ x^3 \equiv 2 \pmod p &\iff \exists \alpha \in A,\ \alpha^3 \equiv 2 \pmod \pi \\ &\iff \begin{cases} a \equiv 1 \pmod 2 \\ b \equiv 0 \pmod 2. \end{cases} \end{aligned}$$

Si nous appliquons ceci au problème de la représentation des nombres premiers par la forme $x^2 + ny^2$, nous obtenons

Proposition 91. *Soit p un nombre premier. Alors*

$$\exists x \in \mathbb{Z},\ \exists y \in \mathbb{Z},\ p = x^2 + 27y^2 \iff \begin{cases} p \equiv 1 \pmod 3, \\ \exists t \in \mathbb{Z},\ t^3 \equiv 2 \pmod p. \end{cases}$$

Autrement dit, p se décompose sous la forme $x^2 + 27y^2$ si et seulement si p est congru à 1 modulo 3 et si 2 est un résidu cubique modulo p.

Démonstration. ($\Rightarrow$) Si $p = x^2 + 27y^2,\ x, y \in \mathbb{Z}$, alors $p \neq 3$, et $p \equiv x^2 \pmod 3$, donc $p \equiv 1 \pmod 3$. Puisque $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $i\sqrt{3} = 1 + 2\omega$, donc

$$\begin{aligned} p &= (x + 3i\sqrt{3}y)(x - 3i\sqrt{3}y) \\ &= \mathrm{N}(x + 3i\sqrt{3}y) \\ &= \mathrm{N}(x + 3y + 6y\omega). \end{aligned}$$

Par conséquent $p = \mathrm{N}(\pi)$, où $\pi = x+3y+6y\omega$ est un premier de A. Posons $a = x+3y, b = 6y$. Alors b est pair, et $a \equiv x + y \equiv x^2 + 27y^2 = p \equiv 1 \pmod 2$. La proposition 90 montre alors que 2 est un résidu cubique modulo p.

($\Leftarrow$) Réciproquement, supposons que $p \equiv 1 \pmod 3$ et que 2 est un résidu cubique modulo p.

Puisque $p \equiv 1 \pmod 3$, on peut alors écrire $p = \pi\overline{\pi}$, où π est un premier primaire, donc π est de la forme $\pi = a + 3b\omega, a \equiv -1 \pmod 3$. Alors

$$4p = 4\mathrm{N}(\pi) = 4(a^2 - 3ab + 9b^2) = (2a - 3b)^2 + 27b^2.$$

Sachant que 2 est un résidu cubique modulo p, la proposition 90 montre que b est pair. En posant $x = a - 3\frac{b}{2} \in \mathbb{Z}, y = \frac{b}{2} \in \mathbb{Z}$, nous obtenons $p = x^2 + 27y^2$. □

3.11 Compléments à la loi de réciprocité cubique.

Donnons maintenant cette proposition, qui complète la proposition 79.

Proposition 92. *Soit $a \equiv -1 \pmod 3$ un entier rationnel ($a \neq -1$), et $n \in \mathbb{Z}$ un entier premier avec a. Alors $\chi_a(n) = 1$.*

Démonstration. Nous savons déjà que si $q \equiv -1 \pmod 3$ est un premier rationnel tel que $q \wedge n = 1$, alors $\chi_q(n) = 1$ (proposition 79).

Si $p \equiv 1 \pmod 3$ est un premier rationnel tel que $p \wedge n = 1$, alors $p = \pi\overline{\pi}$, où π est un premier primaire de A, ainsi que $\overline{\pi}$, non associé à π, et par définition de χ_p, $\chi_{-p}(n) = \chi_\pi(n)\chi_{\overline{\pi}}(n)$.

Comme $\chi_{\overline{\pi}}(n) = \chi_{\overline{\pi}}(\overline{n}) = \overline{\chi_\pi(n)}$ (proposition 78), et donc $\chi_{-p}(n) = |\chi_\pi(n)|^2 = 1$.

La décomposition de a en facteurs premiers primaires est de la forme

$$a = \pm q_1 q_2 \cdots q_k p_1 p_2 \cdots p_l = \pm q_1 q_2 \cdots q_k \pi_1\overline{\pi_1}\pi_2\overline{\pi_2}\cdots\pi_l\overline{\pi_l},$$

où $q_i \equiv -1 \pmod 3, p_j \equiv 1 \pmod 3$, et où les π_k sont des premiers primaires. Notons que les diviseurs premiers $q_i, \pi_j, \overline{\pi_j}$ de a sont premiers avec n.

La définition des caractères généralisés donne alors

$$\chi_a(n) = \chi_{q_1}(n)\cdots\chi_{q_k}(n)\chi_{\pi_1}(n)\chi_{\overline{\pi_1}}(n)\cdots\chi_{\pi_l}(n)\chi_{\overline{\pi_l}}(n) = 1.$$

□

Donnons le caractère cubique des unités, d'abord dans le cas où π est un premier de A tel que $\mathrm{N}(\pi) \neq 3$.

Comme $-1 = (-1)^3$, puisque $\chi_\pi(-1) \in \{1, \omega, \omega^2\}$, $\chi_\pi(-1) = \chi_\pi(-1)^3 = 1$.

Par définition, $\chi_\pi(\omega) \equiv \omega^{\frac{\mathrm{N}(\pi)-1}{3}} \pmod \pi$. Comme $\chi_\pi(\omega)$ et $\omega^{\frac{\mathrm{N}(\pi)-1}{3}}$ sont tous deux dans l'ensemble $\{1, \omega, \omega^2\}$, et que les classes de $1, \omega, \omega^2$ sont distinctes modulo π, nous en déduisons que

$$\chi_\pi(\omega) = \omega^{\frac{\mathrm{N}(\pi)-1}{3}}.$$

Comme $3 \mid \mathrm{N}(\pi) - 1$, $\mathrm{N}(\pi)$ est congru à 1,4 ou 7 modulo 9. Ainsi,

$$\begin{aligned}
\chi_\pi(\omega) = 1 &\iff \mathrm{N}(\pi) \equiv 1 \pmod 9,\\
\chi_\pi(\omega) = \omega &\iff \mathrm{N}(\pi) \equiv 4 \pmod 9,\\
\chi_\pi(\omega) = \omega^2 &\iff \mathrm{N}(\pi) \equiv 7 \pmod 9.
\end{aligned}$$

Comme $\chi_\pi = \chi_{\pi'}$ si π et π' sont associés, on peut se limiter au cas où π est un premier primaire, de la forme $\pi = 3m - 1 + 3n\omega$. Alors

$$\begin{aligned} \mathrm{N}(\pi) - 1 &= (3m-1)^2 + (3n)^2 - 3n(3m-1) - 1 \\ &= 9m^2 - 6m + 9n^2 - 9nm + 3n, \\ \frac{\mathrm{N}(\pi)-1}{3} &= 3m^2 - 2m + 3n^2 - 3nm + n \equiv n + m \pmod 3. \end{aligned}$$

Ainsi, si $\pi = a + b\omega = 3m - 1 + 3n\omega$,

$$\chi_\pi(\omega) = \omega^{\frac{\mathrm{N}(\gamma)-1}{3}} = \omega^{n+m}.$$

Généralisons ce résultat à un élément primaire $\gamma = 3m - 1 + 3n\omega$, pas nécessairement premier.

Nous vérifions d'abord que si $\gamma = -\gamma_1\gamma_2$, avec

$$\begin{array}{lll} \gamma = a + b\omega, & a = 3m - 1, & b = 3n, \\ \gamma_1 = a_1 + b_1\omega, & a_1 = 3m_1 - 1, & b_1 = 3n_1, \\ \gamma_2 = a_2 + b_2\omega, & a_2 = 3m_2 - 1, & b_2 = 3n_2, \end{array}$$

alors $m \equiv m_1 + m_2 \pmod 3$, $n \equiv n_1 + n_2 \pmod 3$.

$$-\gamma_1\gamma_2 = -a_1a_2 + b_1b_2 + (-a_1b_2 - a_2b_1 + b_1b_2)\omega = a + b\omega,$$

donc

$$3m - 1 = a = -a_1a_2 + b_1b_2 \equiv 3(m_1 + m_2) - 1 \pmod 9,$$

et ainsi $m \equiv m_1 + m_2 \pmod 3$.

$$3n = b = -a_1b_2 - a_2b_1 + b_1b_2 \equiv 3(n_1 + n_2) \pmod 9,$$

et donc $n \equiv n_1 + n_2 \pmod 3$.

Par récurrence, si $\gamma = \pm\gamma_1\gamma_2\cdots\gamma_t = (-1)^{t-1}\gamma_1\gamma_2\cdots\gamma_t$, où $\gamma_i = a_i + b_i\omega, a_i = 3m_i - 1, b_i = 3n_i$, alors

$$m \equiv m_1 + \cdots + m_t \pmod 3, \quad n \equiv n_1 + \cdots + n_t \pmod 3.$$

Par définition de χ_γ,

$$\begin{aligned} \chi_\gamma(\omega) &= \chi_{\gamma_1}(\omega)\cdots\chi_{\gamma_t}(\omega) \\ &= \omega^{m_1+n_1}\cdots\omega^{m_t+n_t} \\ &= \omega^{(m_1+\cdots+m_t)+(n_1+\cdots+n_t)} \\ &= \omega^{m+n}. \end{aligned}$$

Nous avons donc prouvé la proposition qui suit.

Proposition 93. *Soit $\gamma \in A$ un élément primaire, de la forme $\gamma = 3m-1+3n\omega$, $m, n \in \mathbb{Z}$, alors*

$$\chi_\gamma(\omega) = \omega^{m+n}.$$

Pour calculer $\chi_\gamma(\alpha)$ où $\alpha = (-1)^a\omega^b\lambda^c\pi_1\cdots\pi_t$, où les π_i sont des premiers primaires, il reste donc à calculer $\chi_\gamma(\lambda)$, ce qui est plus délicat. Ce sera l'objet de la section suivante.

3.12 Caractère cubique de $\lambda = 1 - \omega$.

Commençons par ce cas particulier, avec une preuve due à Kronecker.

Proposition 94. *Soit q un premier rationnel, $q = 3m - 1,\ m \in \mathbb{N}^*$. Alors*

$$\chi_q(\lambda) = \omega^{2m}.$$

Démonstration. Nous savons que q est premier dans A.

Comme $\lambda^2 = -3\omega$, nous avons

$$\chi_q(\lambda^2) = \chi_q(-3)\chi_q(\omega).$$

La proposition 79 montre que $\chi_q(-3) = 1$. De plus $\chi_q(\omega) = \omega^{\frac{\mathrm{N}(q)-1}{3}} = \omega^{\frac{q^2-1}{3}}$ et ainsi

$$\chi_q(\lambda^2) = \omega^{\frac{q^2-1}{3}}.$$

Elevons cette égalité au carré. Comme $\chi_q(\lambda^2) = \chi_q(\lambda)^2$, étant donné que $x = \chi_q(\lambda) \in \{1, \omega, \omega^2\}$ vérifie $x^4 = x$, nous obtenons

$$\chi_q(1 - \omega) = \omega^{\frac{2}{3}(q^2-1)}.$$

Puisque $q^2 - 1 = (3m - 1)^2 - 1 = 9m^2 - 6m$,

$$\frac{2}{3}(q^2 - 1) = 6m^2 - 4m \equiv -4m \equiv 2m \pmod 3,$$

donc

$$\chi_q(1 - \omega) = \omega^{2m}.$$

□

La preuve de la proposition suivante suit les exercices 9.24 à 9.26 de Ireland et Rosen, reprenant une preuve de Kenneth S.Williams.

Proposition 95. Supplément à la loi de réciprocité cubique.
Soit $\pi = 3m - 1 + 3n\omega$ un élément primaire de A. Alors

$$\chi_\pi(\lambda) = \omega^{2m}.$$

Démonstration. Soit $\pi = a + b\omega$ un élément complexe primaire de $A = \mathbb{Z}[\omega]$, avec $a = 3m - 1, b = 3n$.

(a) Calculons d'abord $\chi_\pi(a)$.
Supposons d'abord que a n'est pas une unité, ce qui permet de définir χ_a.
Comme π, a sont primaires, la proposition 88 montre que $\chi_\pi(a) = \chi_a(\pi)$.
Puisque $\pi \equiv b\omega \pmod a$, $\chi_a(\pi) = \chi_a(b)\chi_a(\omega)$.
La proposition 93 donne pour $a = 3m - 1$

$$\chi_a(\omega) = \omega^m.$$

Vérifions que a est premier avec b dans $\mathbb{Z}$. Si un premier rationnel r divise a, b, alors $r \mid \pi$ dans A, donc $\mathrm{N}(r) = r^2 \mid \pi\overline{\pi} = p$ in A, donc $r^2 \mid p$ dans $\mathbb{Z}$, ce qui est absurde.

La proposition 92 donne alors $\chi_a(b) = 1$, et $\chi_a(\omega) = \omega^m$, si bien que

$$\chi_\pi(a) = \chi_a(\pi) = \chi_a(b)\chi_a(\omega) = \omega^m.$$

Si a est une unité, comme $a \in \mathbb{Z}, a \equiv -1 \pmod 3$, alors $a = -1$ et $m = 0$, donc $\chi_\pi(a) = 1 = \omega^m$.
En conclusion, dans tous les cas

$$\chi_\pi(a) = \omega^m.$$

(b) Puisque

$$a + b = [(a + b)\omega]\omega^{-1},$$

et

$$(a + b)\omega = (a + b\omega) + a\omega - a \equiv a(\omega - 1) \pmod \pi,$$

alors

$$a + b \equiv -\lambda a\omega^{-1} \pmod \pi,$$

$$\chi_\pi(a + b) = \chi_\pi(\lambda)\chi_\pi(a)\chi_\pi(\omega)^{-1},$$

$\chi_\pi(a) = \omega^m$ d'après (a), et $\chi_\pi(\omega) = \omega^{m+n}$(proposition 93), ainsi

$$\chi_\pi(a + b) = \omega^{2n}\chi_\pi(\lambda).$$

(c) Supposons maintenant que $a + b$ n'est pas une unité, ce qui permet de considérer χ_{a+b}.
Comme $\pi = a + b\omega$ et $a \equiv -b \pmod{a + b}$, alors $\pi \equiv -b(1 - \omega) \pmod{a + b}$. Ainsi

$$\chi_{a+b}(\pi) = \chi_{a+b}(b)\chi_{a+b}(1 - \omega).$$

Puisque $a \wedge b = 1$, $(a + b) \wedge b = 1$. La proposition 92 donne alors $\chi_{a+b}(b) = 1$, donc

$$\chi_{a+b}(\pi) = \chi_{a+b}(\lambda).$$

(d) Puisque le caractère χ_{a+b} est d'ordre 3,

$$\begin{aligned}\chi_{a+b}(\lambda) &= (\chi_{a+b}(\lambda^2))^2 \\ &= (\chi_{a+b}(-3\omega))^2 \\ &= [\chi_{a+b}(3)\chi_{a+b}(\omega)]^2\end{aligned}$$

$\chi_{a+b}(3) = 1$ car $(a + b) \wedge 3 = (3(m + n) - 1) \wedge 3 = 1$.
$\chi_{a+b}(\omega) = \omega^{m+n}$ (proposition 93).
En conclusion,

$$\chi_{a+b}(\lambda) = \omega^{2(m+n)}.$$

(e) Les parties (b), (c) et (d) donnent alors

$$\chi_\pi(a + b) = \omega^{2n}\chi_\pi(\lambda),$$
$$\chi_{a+b}(\pi) = \omega^{2(m+n)}.$$

Comme π et $a + b$ sont des éléments primaires de A, la réciprocité cubique (proposition 88) donne alors

$$\chi_\pi(a + b) = \chi_{a+b}(\pi).$$

Par conséquent

$$\omega^{2n}\chi_\pi(\lambda) = \omega^{2(m+n)},$$

soit

$$\chi_\pi(\lambda) = \omega^{2m}.$$

(f) Il reste le cas où $a+b$ est une unité. Alors $a+b=-1$, donc $3m-1+3n=-1$, et ainsi $n=-m$. La partie (b) montre que $1=\chi_\pi(-1)=\chi_\pi(a+b)=\omega^{2n}\chi_\pi(\lambda)$, donc

$$\chi_\pi(\lambda) = \omega^{-2n} = \omega^{2m}.$$

Dans chacun des cas, $\chi_\pi(\lambda)=\omega^{2m}$.

□

Chapitre 4

Réciprocité biquadratique.

Nous noterons dans ce chapitre $D = \mathbb{Z}[i]$ l'anneau des entiers de Gauss.

4.1 Anneaux quotients de $\mathbb{Z}[i]$.

Proposition 96. *Soit π un élément premier dans D. Alors l'anneau quotient $D/\pi D$ est un corps à $\mathrm{N}(\pi)$ éléments.*

Démonstration. Nous prouvons cette proposition en considérant les différents types d'éléments premiers de $\mathbb{Z}[i]$, donnés dans la proposition 9 du chapitre "Entiers de Gauss".

- Supposons que $\pi = q$ est un premier rationnel, où $q \equiv 3 \pmod 4$, $q > 0$. Vérifions que
$$S = \{a + bi \mid 0 \leq a < q,\ 0 \leq b < q\}$$
est un système complet de représentants des classes modulo π.
Si $\alpha = u + iv \in D$, alors les divisions euclidiennes de u et v par q donnent des entiers a, b, s, t tels que $u = qs + a, v = qt + b$, où $0 \leq a < q, 0 \leq b < q$. Alors $\alpha \equiv a + bi \pmod q$, où $a + bi \in S$.
Vérifions que les éléments de S sont dans des classes distinctes. Si $\alpha = a+bi \equiv \beta = a' + b'i \pmod q$, où $\alpha, \beta \in S$, alors $q \mid (a - a') + (b - b')i$, donc $\frac{a-a'}{q} + i\frac{b-b'}{q} \in \mathbb{Z}[i]$, ce qui implique $q \mid a - a', q \mid b - b'$. Comme $|a - a'| < q$ et $|b - b'| < q$, il s'ensuit que $a = a', b = b'$, donc $\alpha = \beta$. Ainsi $|D/\pi D| = |S| = q^2 = \mathrm{N}(q) = \mathrm{N}(\pi)$.
- Supposons que $\pi = a + bi$ vérifie $\mathrm{N}(\pi) = p$, où p est un premier rationnel, $p \equiv 1 \pmod 4$. Vérifions que
$$T = \{0, 1, \cdots, p - 1\}$$
est un système complet de représentants des classes.
Comme $\mathrm{N}(\pi) = p = a^2 + b^2$, il s'ensuit que $p \nmid b$, sinon $p \mid a, p \mid b$, donc $p^2 \mid a^2 + b^2 = p$, donc $p \mid 1$: c'est absurde.
Soit $\alpha = u + iv \in D$. Comme $p \nmid b$, il existe un entier b tel que $cb \equiv v \pmod p$, a fortiori modulo π. Alors $\alpha - c\pi = u - ca + i(v - cb)$, donc $\alpha \equiv u - ca \pmod \pi$. Posons $n = u - ca$. Alors $n \in \mathbb{Z}$, et $\alpha \equiv n \pmod \pi$. La division euclidienne de n par p donne $n = ps + r,\ 0 \leq r < p$, donc $\alpha \equiv r \pmod \pi$, où $r \in T$.
Les éléments de T sont dans des classes distinctes modulo π. En effet, si $r, s \in T$, et $r \equiv s \pmod \pi$, alors $\pi \mid r - s$, soit $r - s = \pi\lambda, \lambda \in D$, donc $(r - s)^2 = \mathrm{N}(\pi)\mathrm{N}(\lambda) = p\mathrm{N}(\lambda)$. Ainsi $p \mid (r-s)^2$, où p est un premier rationnel, donc $p \mid r-s$, où $|r - s| < p$, donc $r = s$.
Par conséquent, $|D/\pi D| = |T| = p = \mathrm{N}(\pi)$.

- Supposons que $\pi = 1 + i$. Vérifions que

$$U = \{0, 1\}$$

est un système complet de représentant des classes modulo $\pi = 1 + i$.
Soit $\alpha = a + bi \in D$ quelconque. Comme $i \equiv -1 \pmod{\pi}$, $\alpha \equiv a - b \pmod{\pi}$. Posons $n = a - b$; alors $n \in \mathbb{Z}$ et $\alpha \equiv n$. La division euclidienne de n par 2 donne les entiers q, r tels que $n = 2q + r, r \in \{0, 1\}$, donc $n \equiv r \pmod{2}$, et puisque $1 + i \mid 2$, $n \equiv r \pmod{\pi}$, où $r \in U$.
De plus, $0 \not\equiv 1 \pmod{\pi}$, sinon $\pi \mid 1$: c'est absurde puisque π est premier, et n'est donc pas une unité.
Ainsi $|D/\pi D| = |U| = 2 = \mathrm{N}(\pi)$.

Si λ est un élément premier quelconque de D, alors λ est associé à un élément π appartenant à l'un des trois types considérés, donc vérifiant $\mathrm{N}(\pi) = |D/\pi D|$. Alors $\mathrm{N}(\pi) = \mathrm{N}(\lambda)$, et $\pi D = \lambda D$, donc $\mathrm{N}(\lambda) = |D/\lambda D|$.

□

4.2 Caractère biquadratique.

Si α est un élément de D, nous noterons $[\alpha]$ sa classe dans $D/\pi D$.
L'analogue du théorème de Fermat dans D s'écrit

Proposition 97. *Soit $\alpha \in D$, et π un premier de A tel que π ne divise pas α. Alors*

$$\alpha^{\mathrm{N}(\pi)-1} \equiv 1 \pmod{\pi}.$$

Démonstration. Soit K le corps $D/\pi D$. Le cardinal du groupe K^* est $\mathrm{N}(\pi) - 1$, donc l'ordre de la classe $[\alpha] \in K^*$ divise $\mathrm{N}(\pi) - 1$. Ainsi $[\alpha]^{\mathrm{N}(\pi)-1} = 1$, donc $\alpha^{\mathrm{N}(\pi)-1} \equiv 1 \pmod{\pi}$. □

Proposition 98. *Si π est un premier de A, et si $\mathrm{N}(\pi) \neq 2$, alors*

$$4 \mid \mathrm{N}(\pi) - 1.$$

Démonstration. Montrons que les classes de $1, i, -1, -i$ modulo π sont distinctes. En effet, si $i^j \equiv i^k \pmod{\pi}$, $(0 \leq j \leq k < 4)$, alors $\pi \mid i^l - 1$, où $l = k - j$ vérifie $0 \leq l < 4$. Si $l \neq 0$, alors π divise $i - 1$, ou 2, ou $i + 1$. Dans les trois cas, π divise 2. Comme $2 = -i(1 + i)^2$, tout diviseur premier de 2 est associé à $1 + i$, et vérifie alors $\mathrm{N}(\pi) = 2$, ce qui est exclu.

Par conséquent, le sous-groupe $\{[1], [i], [-1], [-i]\}$ de $(D/\pi D)^*$, engendré par la classe de i, est un sous-groupe à 4 éléments. Le théorème de Lagrange montre alors que 4 divise $|(D/\pi D)^*| = \mathrm{N}(\pi) - 1$. □

Proposition 99. *Supposons que π est un premier de D tel que $\mathrm{N}(\pi) \neq 2$. Soit $\alpha \in D$ tel que $\pi \nmid \alpha$. Alors il existe un unique entier $m \in \{0, 1, 2, 3\}$ tel que*

$$\alpha^{\frac{\mathrm{N}(\pi)-1}{4}} \equiv i^m \pmod{\pi}.$$

Démonstration. Posons $S = \{[1], [i], [i]^2, [i]^3\}$. La démonstration précédente montre que $|S| = 4$, et S est inclus dans l'ensemble des racines du polynôme $x^4 - 1 \in K[x]$, où K est le corps $D/\pi D$. Puisqu'un polynôme de degré 4 sur un corps commutatif ne peut

admettre plus de 4 racines, S est donc l'ensemble des racines de ce polynôme. Comme $\gamma = [\alpha]^{\frac{\mathrm{N}(\pi)-1}{4}} \in D/\pi D$ vérifie $\gamma^4 - 1 = 0$, alors $\gamma \in S$, soit $[\alpha]^{\frac{\mathrm{N}(\pi)-1}{4}} = [i]^m,\ 0 \leq m < 4$. Par conséquent

$$\alpha^{\frac{\mathrm{N}(\pi)-1}{4}} \equiv i^m \pmod{\pi}.$$

Un tel m est unique puisque les classes $[i]^m,\ m \in \{0,1,2,3\}$ sont distinctes. □

Remarquons que, dans le cas où $\pi \mid \alpha$, $\alpha^{\frac{\mathrm{N}(\pi)-1}{4}} \equiv 0 \pmod{\pi}$. Nous savons que les classes de $1, i, i^2, i^3$ sont distinctes dans $D/\pi D$. De plus, les classes de $0, 1, i, i^2, i^3$ sont distinctes, sinon $\pi \mid i^k$, et π serait une unité. Pour tout $\alpha \in D$, il existe un et un seul $z \in \{0, 1, i, i^2, i^3\}$ tel que $\alpha^{\frac{\mathrm{N}(\pi)-1}{4}} \equiv z \pmod{\pi}$. Ceci justifie la définition suivante :

Définition 9. *Soit π un élément premier de $D = \mathbb{Z}[i]$ tel que $\mathrm{N}(\pi) \neq 2$, et soit $\alpha \in D$. Le caractère biquadratique de α, noté $\chi_\pi(\alpha)$, ou $\left(\frac{\alpha}{\pi}\right)_4$, est l'unique valeur complexe de l'ensemble $\{0, 1, i, i^2, i^3\}$ caractérisée par*

$$\chi_\pi(\alpha) \equiv \alpha^{\frac{\mathrm{N}(\pi)-1}{4}} \pmod{\pi}.$$

Cette définition implique que $\chi_\pi(\alpha) = 0 \iff \pi \mid \alpha$.

Proposition 100. *Si $\left(\frac{\alpha}{\pi}\right)_4 \equiv \zeta \pmod{\pi}$, où $\zeta \in \{0, 1, i, -1, -i\}$, alors $\chi_\pi(\alpha) = \zeta$.*

Démonstration. En effet, $\chi_\pi(\alpha)$ et ζ sont des éléments de $\{0, 1, i, i^2, i^3\}$ et les classes de ces éléments sont distinctes modulo π. □

Donnons les premières propriétés de ce caractère biquadratique.

Proposition 101. *Si $\alpha, \beta \in D$, et si π est un premier de D tel que $\mathrm{N}(\pi) \neq 2$, alors*

(a) $\chi_\pi(\alpha\beta) = \chi_\pi(\alpha)\chi_\pi(\beta)$,

(b) si $\alpha \equiv \beta \pmod{\pi}$, *alors* $\chi_\pi(\alpha) = \chi_\pi(\beta)$.

Démonstration. (a) Par définition,

$$\chi_\pi(\alpha\beta) \equiv (\alpha\beta)^{\frac{\mathrm{N}(\pi)-1}{4}} = \alpha^{\frac{\mathrm{N}(\pi)-1}{4}} \beta^{\frac{\mathrm{N}(\pi)-1}{4}} \equiv \chi_\pi(\alpha)\chi_\pi(\beta) \pmod{\pi}.$$

Comme $\chi_\pi(\alpha)\chi_\pi(\beta) \in \{0, 1, i, -1, -i\}$, la proposition 100 montre alors que $\chi_\pi(\alpha\beta) = \chi_\pi(\alpha)\chi_\pi(\beta)$.

(b) Si $\alpha \equiv \beta \pmod{\pi}$, alors $\alpha^{\frac{\mathrm{N}(\pi)-1}{4}} \equiv \beta^{\frac{\mathrm{N}(\pi)-1}{4}} \pmod{\pi}$, donc $\chi_\pi(\alpha) \equiv \chi_\pi(\beta) \pmod{\pi}$. La proposition 100 montre alors que $\chi_\pi(\alpha) = \chi_\pi(\beta)$.

□

Notons que le (b) assure que l'application χ

$$\begin{cases} (D/\pi D)^* & \to \mathbb{C}^* \\ [\alpha] & \mapsto \chi_\pi(\alpha) \end{cases}$$

est bien définie, et le (a) montre que χ est un homomorphisme de groupes. Ainsi χ est un caractère multiplicatif sur $(D/\pi D)^*$.

Le caractère biquadratique permet de caractériser les puissances quatrièmes de D modulo π

Proposition 102. *Soit $\alpha \in D = \mathbb{Z}[i]$, et π un premier de D tel que $\mathrm{N}(\pi) \neq 2$ et $\pi \nmid \alpha$. Alors*

$$\chi_\pi(\alpha) = 1 \iff \exists x \in D,\ x^4 \equiv \alpha \pmod{\pi}.$$

Démonstration. $D/\pi D$ est un corps à $\mathrm{N}(\pi)$ éléments d'après la proposition 96, et 4 divise $\mathrm{N}(\pi)-1$ d'après la proposition 98, donc $d = 4 \wedge (\mathrm{N}(\pi)-1) = 4$. Alors la proposition 24 du chapitre "Sommes de Gauss et sommes de Jacobi" montre que l'équation $[x]^4 = [\alpha]$ a une solution dans $(D/\pi D)^*$ si et seulement si $[\alpha]^{\frac{\mathrm{N}(\pi)-1}{4}} = 1$, ce qui équivaut à $\chi_\pi(\alpha) = 1$. □

Proposition 103. *Si $\alpha \in D$, et π un premier de D,*

$$\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha}).$$

Démonstration. La définition de χ_π donne la relation

$$\alpha^{\frac{\mathrm{N}(\pi)-1}{4}} \equiv \chi_\pi(\alpha) \pmod{\pi}.$$

Le passage au conjugué donne

$$\overline{\alpha}^{\frac{\mathrm{N}(\pi)-1}{4}} \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}.$$

Comme $\mathrm{N}(\pi) = \mathrm{N}(\overline{\pi})$,

$$\begin{aligned}\chi_{\overline{\pi}}(\overline{\alpha}) &\equiv \overline{\alpha}^{\frac{\mathrm{N}(\overline{\pi})-1}{4}} \pmod{\overline{\pi}} \\ &= \overline{\alpha}^{\frac{\mathrm{N}(\pi)-1}{4}} \\ &\equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}.\end{aligned}$$

□

Proposition 104. *Soit q un nombre premier rationnel, $q \equiv 3 \pmod 4$, et $n \in \mathbb{Z}$ premier avec q. Alors*

$$\chi_q(n) = 1.$$

Démonstration. Par définition de χ_q,

$$\chi_q(n) \equiv n^{\frac{\mathrm{N}(q)-1}{4}} = n^{\frac{q^2-1}{4}} = (n^{q-1})^{\frac{q+1}{4}} \equiv 1 \pmod{q},$$

d'après le petit théorème de Fermat. □

4.3 Eléments primaires de D.

Introduisons la notion d'élément primaire dans $D = \mathbb{Z}[i]$.

Définition 10. *Soit α un élément de D qui n'est pas une unité. Alors α est dit primaire si*

$$\alpha \equiv 1 \pmod{(1+i)^3}.$$

Proposition 105. *Soit $\alpha = a + bi \in D, \mathrm{N}(\alpha) \neq 1$. Alors*

$$\alpha \text{ est primaire} \iff \begin{cases} a \equiv 1,\ b \equiv 0 \pmod 4, \\ \quad ou \\ a \equiv 3,\ b \equiv 2 \pmod 4. \end{cases}$$

Démonstration. Puisque $(1+i)^3 = 2i(1+i)$ est associé à $2+2i$, , il s'ensuit que $a+bi$ est primaire si et seulement si

$$\frac{(a-1)+bi}{2+2i} = \frac{((a-1)+bi)(1-i)}{4} = \frac{a+b-1}{4} + \frac{b-a+1}{4}\, i \in D,$$

ce qui équivaut au système

$$\begin{cases} a+b \equiv 1 & (\text{mod } 4), \\ a-b \equiv 1 & (\text{mod } 4). \end{cases}$$

Alors $2a \equiv 2 \pmod 4$, donc a est impair, et ainsi $a \equiv 1, 3 \pmod 4$. Les seules solutions sont données par $a \equiv 1, b \equiv 0 \pmod 4$, ou $a \equiv 3, b \equiv 2 \pmod 4$. □

En particulier, si $\alpha \neq 1$ vérifie $\alpha \equiv 1 \pmod 4$, alors α est primaire. De plus, si α est primaire, alors $1+i \nmid \alpha$. Si q est un premier rationnel, où $q \equiv 3 \pmod 4$, $q > 0$, alors $-q$ est un premier primaire (mais pas les autres associés $q, iq, -iq$).

Proposition 106. *Soit α un élément de D qui n'est pas une unité, et tel que $1+i \nmid \alpha$. Alors α a un et un seul associé primaire.*

Démonstration. Soit $\alpha = a+ib$ tel que $1+i \nmid \alpha$. Comme $\alpha = (a-b)+b(1+i)$, alors $1+i \nmid a-b$, donc $2 \nmid a-b$. Ainsi a, b sont de parité distinctes. Si a est pair et b impair, alors $i\alpha = -b+ia = a'+ib'$, où a' est impair et b' pair. Ainsi il existe une unité ε ($\varepsilon = 1$ ou $\varepsilon = i$) telle que $\varepsilon\alpha = a'+b'i$ vérifie la propriété a' impair et b' pair.

Il n'existe alors que quatre cas modulo 4 : $a' \equiv 1, b' \equiv 0$, ou $a' \equiv 3, b' \equiv 2$, ou $a' \equiv 1, b' \equiv 2$, ou $a' \equiv 3, b' \equiv 0$ (modulo 4).

Dans les deux premiers cas, $a'+b'i$ est primaire.

Si $a' \equiv 1$ et $b' \equiv 2$ modulo 4, alors $a''+b''i = -a'-b'i$ vérifie $a'' \equiv 3, b'' \equiv 2 \pmod 4$, et si $a' \equiv 3, b' \equiv 0$, alors $a''+b''i$ vérifie $a'' \equiv 1, b'' \equiv 0$ modulo 4. Dans ces deux cas $a''+ib''$ est primaire.

Si $\varepsilon_1\alpha, \varepsilon_2\alpha$ sont tous deux primaires, où $\varepsilon_1, \varepsilon_2$ sont des unités, alors $(\varepsilon_1-\varepsilon_2)\alpha \equiv 0 \pmod{(1+i)^3}$. Comme $1+i$ est premier dans D et ne divise pas α, $(1+i)^3 \mid \varepsilon_1-\varepsilon_2$. Alors $\mathrm{N}((1+i)^3) \mid \mathrm{N}(\varepsilon_1-\varepsilon_2)$, soit $8 \mid \mathrm{N}(\varepsilon_1-\varepsilon_2)$. De plus $|\varepsilon_1-\varepsilon_2| \leq |\varepsilon_1|+|\varepsilon_2| = 2$, donc $\mathrm{N}(\varepsilon_1-\varepsilon_2) \leq 4$. Ceci n'est possible que si $\mathrm{N}(\varepsilon_1-\varepsilon_2) = 0$, donc $\varepsilon_1 = \varepsilon_2$. Ceci prouve l'unicité de l'associé primaire de α. □

Proposition 107. *Soit S l'ensemble contenant $1+i$ et tous les premiers primaires de D. S est un système complet de représentants des classes d'association, soit*

(a) Tout premier de D est associé à un premier de S.

(b) Deux éléments arbitraires distincts de S ne sont pas associés.

Démonstration. (a) Soit π un élément premier de D. Si $\mathrm{N}(\pi) = 2$, π est associé à $1+i$. Si $\mathrm{N}(\pi) \neq 2$, alors $1+i \nmid \pi$ (sinon les premiers $1+i$ et π seraient associés, donc de même norme égale à 2). La proposition 106 montre alors que π est associé à un premier primaire de D.

(b) Soient π, μ deux éléments de S associés. Alors ils ont même norme.
Si $\mathrm{N}(\pi) = \mathrm{N}(\mu) = 2$, alors $\pi = 1+i$, puisque $1+i$ est le seul élément de S de norme 2. De même, $\mu = \lambda$, donc $\pi = \mu$.
Si $\mathrm{N}(\pi) = \mathrm{N}(\mu) \neq 3$, alors π, μ sont des premiers primaires par définition de S, et associés. La proposition 106 montre qu'ils sont égaux.

□

Proposition 108. *Tout élément $\alpha \in D$ de décompose sous la forme*

$$\alpha = i^a(1+i)^b\pi_1^{a_1}\cdots\pi_t^{a_t},$$

où les π_i sont des premiers primaires distincts, $b \geq 0, a_i \geq 0$, et $0 \leq a < 4$. Cette décomposition est unique à l'ordre près des éléments $\pi_1, \ldots, \pi_t$.

Démonstration. Puisque $D = \mathbb{Z}[i]$ est principal, donc factoriel, et S étant un système complet de représentants des classes d'association des éléments premiers, tout élément α de A s'écrit de façon unique sous la forme

$$\alpha = u\prod_{\pi\in S}\pi^{e(\pi)},$$

où $e(\pi) \geq 0$ est nul sauf sur un ensemble fini de valeurs de $\pi \in S$, et où u est une unité, donc de la forme $u = i^k,\ k \in \{0,1,2,3\}$, où k est alors fixé. Par définition de S,

$$\alpha = i^a(1+i)^b\pi_1^{a_1}\cdots\pi_t^{a_t}.$$

□

Proposition 109. *Si γ est un élément primaire de D, alors γ se décompose sous la forme*

$$\gamma = \gamma_1\cdots\gamma_t,$$

où $t \geq 1$, et les γ_i sont des premiers primaires (pas nécessairement distincts).

Démonstration. D'après la proposition 108,

$$\gamma = i^a(1+i)^b\gamma_1\cdots\gamma_t,$$

où les γ_i sont des premiers primaires, et $0 \leq a < 4$.

Comme γ est primaire, il n'est pas divisible par $1+i$, donc $b = 0$, soit

$$\gamma = i^a\gamma_1\cdots\gamma_t,$$

où pour tout indice i, $\gamma_i \equiv 1 \pmod{(1+i)^3}$. Par conséquent

$$1 \equiv i^a \pmod{(1+i)^3}.$$

Alors $(1+i)^3 \mid i^a - 1$, donc $8 = \mathrm{N}((1+i)^3) \mid \mathrm{N}(i^a-1) \leq 4$, donc $\mathrm{N}(i^a-1) = 0$, $i^a = 1$, avec $0 \leq a < 4$, et ainsi $a = 0$:

$$\gamma = \gamma_1\cdots\gamma_t.$$

□

Un premier primaire π n'est pas associé à $1+i$ par définition. La classification des premiers de $\mathbb{Z}[i]$ montre alors que, ou bien π est associé à un entier rationnel $q \equiv 3 \pmod 4$, auquel cas $\pi = -q$, ou bien π est tel que $\mathrm{N}(\pi) = p \equiv 1 \pmod 4$. Ainsi tout élément primaire de D s'écrit sous la forme

$$\gamma = (-q_1)\cdots(-q_s)\pi_1\cdots\pi_t,$$

où les $q_i \equiv 3 \pmod 4$ sont des premiers rationnels positifs, et où les premiers primaires π_j vérifient $\mathrm{N}(\pi_j) = p \equiv 1 \pmod 4$.

4.4 Caractères biquadratiques généralisés.

Soit $\gamma \in D$ tel que γ n'est pas une unité, et $1+i \nmid \gamma$, et soit $\gamma = \lambda_1 \cdots \lambda_t$ une décomposition de γ en facteurs irréductibles. Pour tout $\beta \in D$, le produit $\prod_{i=1}^{t} \chi_{\lambda_i}(\beta)$ ne dépend pas de cette décomposition. En effet, toute autre décomposition $\gamma = \mu_1 \cdots \mu_{t'}$ en facteurs irréductibles est telle que $t' = t$, et $\mu_i = \varepsilon_i \lambda_{\sigma(i)}$, où ε_i est une unité, et $\sigma \in S_t$ est une permutation. Puisque μ_i et λ_{σ_i} sont associés, la définition du caractère biquadratique donne $\chi_{\mu_i} = \chi_{\lambda_{\sigma_i}}$, donc $\prod_{i=1}^{t} \chi_{\lambda_i}(\beta) = \prod_{i=1}^{t} \chi_{\mu_i}(\beta)$. Ceci permet de donner la définition suivante.

Définition 11. *Si $\gamma \in D$ est tel que γ n'est pas une unité, et $1+i \nmid \gamma$, et si $\gamma = \lambda_1 \cdots \lambda_t$ est une décomposition de γ en facteurs irréductibles, alors χ_γ est défini par :*

$$\forall \beta \in D,\ \chi_\gamma(\beta) = \prod_{i=1}^{t} \chi_{\lambda_i}(\beta).$$

Proposition 110. *Soient λ, ρ des éléments de D qui ne sont pas divisibles par $1+i$, et $\alpha, \beta \in D$. Alors*

(a) $\alpha \equiv \beta \pmod{\gamma} \Rightarrow \chi_\gamma(\alpha) = \chi_\gamma(\beta)$.

(b) $\chi_\gamma(\alpha\beta) = \chi_\gamma(\alpha)\chi_\gamma(\beta)$.

(c) $\chi_\rho(\alpha)\chi_\gamma(\alpha) = \chi_{\rho\gamma}(\alpha)$.

Démonstration. (a) Soit $\gamma = \gamma_1 \cdots \gamma_t$ une décomposition de γ en facteurs premiers dans D. Alors pour tout i, $\alpha \equiv \beta \pmod{\gamma_i}$, donc $\chi_{\gamma_i}(\alpha) = \chi_{\gamma_i}(\beta)$ (proposition 101(b)). Par conséquent

$$\chi(\alpha) = \prod_{i=1}^{t} \chi_{\gamma_i}(\alpha) = \prod_{i=1}^{t} \chi_{\gamma_i}(\beta) = \chi_\gamma(\beta).$$

(b) La proposition 101(a) montre que

$$\begin{aligned} \chi_\gamma(\alpha\beta) &= \chi_{\gamma_1}(\alpha\beta) \cdots \chi_{\gamma_t}(\alpha\beta) \\ &= \chi_{\gamma_1}(\alpha) \cdots \chi_{\gamma_t}(\alpha)\chi_{\gamma_1}(\beta) \cdots \chi_{\gamma_t}(\beta) \\ &= \chi_\gamma(\alpha)\chi_\gamma(\beta). \end{aligned}$$

(c) Ecrivons une décomposition de ρ en facteurs premiers sous la forme $\rho = \rho_1 \cdots \rho_l$. Comme $1+i$ est premier, $1+i \nmid \rho\gamma$, et $\rho\gamma$ se décompose sous la forme $\rho\gamma = \rho_1 \cdots \rho_l \gamma_1 \cdots \gamma_t$, donc

$$\chi_{\gamma\rho}(\alpha) = (\chi_{\rho_1} \cdots \chi_{\rho_l}\chi_{\gamma_1} \cdots \chi_{\gamma_t})(\alpha) = \chi_\rho(\alpha)\chi_\gamma(\alpha).$$

□

La proposition 103 se généralise aussitôt.

Proposition 111. *Si $\alpha \in D$, et $\pi \in D$ tel que $1+i \nmid \pi$ (en particulier si π est primaire), alors*

$$\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha}).$$

Démonstration. Décomposons π en produit de premiers dans D : $\pi = \pi_1 \cdots \pi_t$. Alors, en utilisant la proposition 103,

$$\begin{aligned}\overline{\chi_\pi(\alpha)} &= \overline{\chi_{\pi_1}(\alpha)} \cdots \overline{\chi_{\pi_1}(\alpha)} \\ &= \chi_{\overline{\pi_1}}(\overline{\alpha}) \cdots \chi_{\overline{\pi_t}}(\overline{\alpha}) \\ &= \chi_{\overline{\pi_1} \cdots \overline{\pi_t}}(\overline{\alpha}) \\ &= \chi_{\overline{\pi}}(\overline{\alpha}).\end{aligned}$$

□

Proposition 112. *Soit $\pi = a + bi$ un élément primaire de D. Alors*

$$\chi_\pi(-1) = (-1)^{\frac{a-1}{2}}.$$

Démonstration. Traitons d'abord le cas où π est un premier primaire de D. Alors a est impair, b pair et $\mathrm{N}(\pi) = a^2 + b^2$. Par conséquent,

$$\chi_\pi(-1) = (-1)^{\frac{\mathrm{N}(\pi)-1}{4}} = (-1)^{\frac{a^2-1}{4} + \frac{b^2}{4}} = [(-1)^{\frac{a+1}{2}}]^{\frac{a-1}{2}} (-1)^{\frac{b^2}{4}}.$$

D'après la proposition 105, $a \equiv 1 \pmod 4, b \equiv 0 \pmod 4$, ou $a \equiv 3 \pmod 4, b \equiv 2 \pmod 4$.

- Si $a \equiv 1 \pmod 4, b \equiv 0 \pmod 4$, alors $(-1)^{\frac{a+1}{2}} = -1, (-1)^{\frac{b^2}{4}} = +1$, donc

$$\chi_\pi(-1) = (-1)^{\frac{a-1}{2}}.$$

- Si $a \equiv 3 \pmod 4, b \equiv 2 \pmod 4$, alors $(-1)^{\frac{a+1}{2}} = 1, (-1)^{\frac{b^2}{4}} = -1$, donc

$$\chi_\pi(-1) = -1 = (-1)^{\frac{a-1}{2}}.$$

Dans tous les cas, si $\pi = a + bi$ est un premier primaire de D, alors

$$\chi_\pi(-1) = (-1)^{(a-1)/2}.$$

Passons au cas général, où π est un élément primaire de D, pas nécessairement premier. Alors la proposition 109 permet de décomposer π sous la forme

$$\pi = \pi_1 \cdots \pi_t,$$

où les $\pi_k = a_k + ib_k$ sont des premiers primaires. D'après la première partie de la preuve,

$$\begin{aligned}\chi_\pi(-1) &= \prod_{k=1}^{t} \chi_{\pi_k}(-1) \\ &= \prod_{k=1}^{t} (-1)^{\frac{a_k-1}{2}}.\end{aligned}$$

Montrons que

$$(-1)^{\frac{a-1}{2}} = \prod_{k=1}^{t} (-1)^{\frac{a_k-1}{2}}.$$

Notons Π ce dernier produit. Or, pour tout entier élément primaire $\pi = a+bi$, $(-1)^{\frac{a-1}{2}} = -1$ équivaut à $\pi \equiv 3+2i \pmod 4$, et dans le cas contraire où $\pi \equiv 1 \pmod 4$, alors $(-1)^{\frac{n-1}{2}} = 1$. Donc $\Pi = -1$ si et seulement si le nombre P de facteurs π_i congrus à 3 modulo 4 est impair. Comme les autres facteurs sont congrus à 1 modulo 4, et $(3+2i)^2 \equiv 1 \pmod 4$, $\pi = \pi_1 \cdots \pi_t \equiv 3+2i \pmod 4$ si P est impair. Ainsi

$$\Pi = -1 \iff P \equiv 1 \pmod 2 \iff \pi \equiv 3+2i \pmod 4 \iff (-1)^{\frac{a-1}{2}} = -1.$$

Comme Π et $(-1)^{\frac{a-1}{2}}$ ne peuvent prendre que les valeurs $+1, -1$, nous pouvons conclure que $\Pi = (-1)^{\frac{a-1}{2}}$, et donc $\chi_\pi(-1) = (-1)^{(a-1)/2}$.

□

Proposition 113. *Soit $n \in \mathbb{Z}$, et $a \in \mathbb{Z}$ un impair qui n'est pas une unité. Si $a \wedge n = 1$, alors*

$$\chi_a(n) = 1.$$

Démonstration. Comme $\chi_a = \chi_{-a}$, on peut supposer $a > 0$. Décomposons a sous la forme $a = \prod_{i\in I} p_i \prod_{j\in J} q_j$, où les p_i, q_j sont des premiers rationnels, $p_i \equiv 1 \pmod 4, q_j \equiv 3 \pmod 4$. La proposition 104 montre que $\chi_{q_j}(n) = 1$, puisque $q_j \wedge n = 1$. Il reste à vérifier que $\chi_{p_i}(n) = 1$. Une décomposition de p_i sous la forme $p_i = \pi\overline{\pi}$, où π est premier dans D, donne

$$\chi_{p_i}(n) = \chi_\pi(n)\chi_{\overline{\pi}}(n) = \chi_\pi(n)\overline{\chi_\pi(n)} = 1,$$

puisque $\chi_{\overline{\pi}}(n) = \chi_{\overline{\pi}}(\overline{n}) = \overline{\chi_\pi(n)}$ (proposition 104). □

Lemme. *Soit $n \in \mathbb{Z}$, $n = s_1 \cdots s_t, s_i \equiv 1 \pmod 4$ pour $i = 1, \ldots, t$. Alors*

$$\frac{n-1}{4} \equiv \sum_{i=1}^{t} \frac{s_i - 1}{4} \pmod 4.$$

Démonstration. Si $n = st, s \equiv 1, t \equiv 1 \pmod 4$, alors $s = 4k+1, t = 4l+1,\ k, l \in \mathbb{Z}$, si bien que

$$n = (4k+1)(4l+1) = 16kl+4k+4l+1, \frac{n-1}{4} = 4kl+k+l \equiv k+l = \frac{s-1}{4}+\frac{l-1}{4} \pmod 4.$$

En raisonnant par récurrence sur t, supposons que tout produit de t factors $n = s_1 s_2 \cdots s_t$, où $s_i \equiv 1 \pmod 4$ vérifie

$$\frac{n-1}{4} \equiv \sum_{i=1}^{t} \frac{s_i - 1}{4} \pmod 4.$$

Si $n' = s_1 s_2 \cdots s_t s_{t+1} = n s_{t+1}, s_i \equiv 1 \pmod 4$, alors $n \equiv 1, s_{t+1} \equiv 1 \pmod 4$, donc

$$\frac{n'-1}{4} \equiv \frac{n-1}{4} + \frac{s_{t+1}-1}{4} \equiv \sum_{i=1}^{t} \frac{s_i-1}{4} + \frac{s_{t+1}-1}{4} \equiv \sum_{i=1}^{t+1} \frac{s_i-1}{4} \pmod 4.$$

□

Proposition 114. *Si $n \neq 1$ est un entier $n \equiv 1 \pmod 4$, alors*

$$\chi_n(i) = (-1)^{\frac{n-1}{4}}.$$

Démonstration. Ici n peut être négatif. Si n est un premier rationnel $p \equiv 1 \pmod 4$, alors la décomposition $p = \pi\overline{\pi}$ donne

$$\chi_p(i) = \chi_\pi(i)\chi_{\overline{\pi}}(i) = (i^{\frac{p-1}{4}})^2 = (-1)^{\frac{p-1}{4}}.$$

Par ailleurs, si $n = -q, q \equiv 3 \pmod 4$, où $q > 0$ est un premier rationnel, alors

$$\chi_{-q}(i) = i^{\frac{q^2-1}{4}} = (i^{q-1})^{\frac{q+1}{4}} = (-1)^{\frac{q+1}{4}} = (-1)^{\frac{-q-1}{4}}.$$

Dans le cas général, décomposons n sous la forme $n = p_1 \cdots p_t(-q_1)\cdots(-q_s)$, où $p_i \equiv 1 \pmod 4, q_j \equiv 3 \pmod 4$. Alors

$$\chi_n(i) = (-1)^{\frac{p_1-1}{4}} \cdots (-1)^{\frac{p_t-1}{4}}(-1)^{\frac{-q_1-1}{4}} \cdots (-1)^{\frac{-q_s-1}{4}}.$$

En appliquant le lemme,

$$\chi_n(i) = (-1)^{\frac{p_1\cdots p_t(-q_1)\cdots(-q_s)-1}{4}} = (-1)^{\frac{n-1}{4}}.$$

□

4.5 La loi de réciprocité biquadratique.

Cette loi nécessitera plusieurs lemmes (propositions 115 à 124). Elle s'exprime, pour des premiers primaires λ, π, sous la forme

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{\frac{\mathrm{N}(\lambda)-1}{4}\frac{\mathrm{N}(\pi)-1}{4}}.$$

Rappelons qu'un premier $\pi = a + bi$ est primaire si et seulement si $a \equiv 1, b \equiv 0$, ou $a \equiv 3, b \equiv 2 \pmod 4$. Ceci équivaut à a impair, b pair et $\frac{a-1}{2} \equiv \frac{b}{2} \pmod 2$.

Si on note $\pi = 2m + 1 + 2ni$, alors $m = \frac{a-1}{2}$ et $n = \frac{b}{2}$ sont de même parité, donc

$$\frac{\mathrm{N}(\pi)-1}{4} = \frac{(2m+1)^2 + (2n)^2 - 1}{4} = m^2 + m + n^2 \equiv m = \frac{a-1}{2} \pmod 2.$$

La loi de réciprocité biquadratique peut donc s'écrire, pour $\pi = a + bi, \lambda = c + di$, sous la forme

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{\frac{a-1}{2}\frac{c-1}{2}}.$$

Autrement dit $\chi_\pi(\lambda) = \chi_\lambda(\pi)$ si π ou λ est congru à 1 modulo 4, et $\chi_\pi(\lambda) = -\chi_\lambda(\pi)$ si π et λ sont tous deux congrus à $3 + 2i$ modulo 4.

Considérons un premier primaire π tel que $\mathrm{N}(\pi) = p \equiv 1 \pmod 4$, et soit χ_π le caractère quartique associé. Dans ce cas le corps $D/\pi D$ est isomorphe à $\mathbb{F}_p$, et les éléments $\{0, 1, \ldots, p-1\}$ de D forment un système complet de représentants des classes de $D/\pi D$.

Nous noterons maintenant $\mathbb{F}_p$ ce corps à p éléments, ensemble des classes de $0, \cdots, p-1$ dans $D/\pi D$. Ceci donne un sens aux sommes de Gauss

$$g(\chi_\pi) = \sum_{j \in \mathbb{F}_p} \chi_\pi(j)\zeta^j = \sum_{j=0}^{p-1} \chi_\pi(j)\zeta^j.$$

Comme χ_π est un caractère d'ordre 4 dans le groupe des caractères sur F, $\psi = \chi_\pi^2$ est un caractère d'ordre 2. Puisqu'il n'existe qu'un seul caractère d'ordre 2 dans le groupe des caractères, ψ est le caractère de Legendre, donné par $\psi(j) = \left(\frac{j}{p}\right)$.

Proposition 115. *Les caractères χ_π et ψ étant définis comme ci-dessus,*

$$J(\chi_\pi, \chi_\pi) = \chi_\pi(-1)J(\chi_\pi, \psi).$$

Démonstration. La proposition 54 du chapitre "Sommes de Gauss et sommes de Jacobi" montre que

$$J(\chi_\pi, \chi_\pi) = \frac{g(\chi_\pi)^2}{g(\psi)}.$$

La proposition 52 de ce même chapitre (et la remarque qui suit cette proposition) donne

$$g(\psi)^2 = \psi(-1)p = (-1)^{\frac{p-1}{2}}p = p.$$

De plus, la proposition 59 du chapitre précité, appliquée au caractère χ_π d'ordre 4, donne

$$g(\chi_\pi)^4 = \chi_\pi(-1)pJ(\chi_\pi, \chi_\pi)J(\chi, \psi).$$

Ainsi

$$J(\chi_\pi, \chi_\pi)^2 = \frac{g(\chi_\pi)^4}{g(\psi)^2} = \chi_\pi(-1)J(\chi_\pi, \chi_\pi)J(\chi, \psi),$$

ce qui donne le résultat puisque $J(\chi_\pi, \chi_\pi)$, de module $\sqrt{p}$, est non nul. □

Proposition 116.

$$g(\chi_\pi)^4 = pJ(\chi_\pi, \chi_\pi)^2.$$

Démonstration. La démonstration précédente donne $J(\chi_\pi, \chi_\pi)^2 = \frac{g(\chi_\pi)^4}{g(\psi)^2}$ et $g(\psi)^2 = p$, donc $g(\chi_\pi)^4 = pJ(\chi_\pi, \chi_\pi)^2$. □

Proposition 117. *L'élément $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi)$ est primaire.*

Démonstration. La permutation de $\mathbb{F}_p$ donnée par $t \mapsto 1 - t$ a pour unique point fixe la classe de $\frac{p+1}{2}$, et laisse fixe le produit $\chi_\pi(t)\chi_\pi(1-t)$. Puisque $\chi_\pi(t)\chi_\pi(1-t) = 0$ pour $t = 0$ et $t = 1$,

$$\begin{aligned} J(\chi_\pi, \chi_\pi) &= \sum_{t=0}^{p-1} \chi_\pi(t)\chi_\pi(1-t) \\ &= \sum_{t=2}^{p-1} \chi_\pi(t)\chi_\pi(1-t) \\ &= \sum_{t=2}^{\frac{p-1}{2}} \chi_\pi(t)\chi_\pi(1-t) + \chi_\pi\left(\frac{p+1}{2}\right)^2 + \sum_{t=\frac{p+3}{2}}^{p-1} \chi_\pi(t)\chi_\pi(1-t). \end{aligned}$$

Le changement d'indice $s = 1 - t$ $(= p + 1 - t)$ donne

$$\sum_{t=\frac{p+3}{2}}^{p-1} \chi_\pi(t)\chi_\pi(1-t) = \sum_{s=2}^{\frac{p-1}{2}} \chi_\pi(1-s)\chi_\pi(s) = \sum_{t=2}^{\frac{p-1}{2}} \chi_\pi(t)\chi_\pi(1-t).$$

Par conséquent,

$$J(\chi_\pi,\chi_\pi)=2\sum_{t=2}^{\frac{p-1}{2}}\chi_\pi(t)\chi_\pi(1-t)+\chi_\pi\left(\frac{p+1}{2}\right)^2.$$

Puisque χ_π est d'ordre 4,

$$\begin{aligned}\chi_\pi\left(\frac{p+1}{2}\right)^2&=(\chi_\pi(2^{-1}))^2=\chi_\pi(2)^{-2}=\chi_\pi(2)^2\\&=\chi_\pi(-i(1+i)^2)^2=(\chi_\pi(-i))^2\chi_\pi^4(1+i)\\&=\chi_\pi((-i)^2)=\chi_\pi(-1).\end{aligned}$$

Réduisons $J(\chi_\pi,\chi_\pi)$ modulo $2+2i$. Puisque $1+i\mid 2$ et que $1-i=-i(1+i)$, les 4 unités de $\mathbb{Z}[i]$ sont congrues à 1 modulo $1+i$. Par conséquent,

$$2\chi_\pi(t)\chi_\pi(1-t)\equiv 2 \pmod{2+2i},$$

et ainsi

$$J(\chi_\pi,\chi_\pi)\equiv 2\,\frac{p-3}{2}+\chi_\pi(-1) \pmod{2+2i}.$$

De plus, puisque $p\equiv 1 \pmod 4$, a fortiori $p\equiv 1 \pmod{2+2i}$, donc

$$J(\chi_\pi,\chi_\pi)\equiv -2+\chi_\pi(-1) \pmod{2+2i}.$$

Enfin

$$\begin{aligned}-\chi_\pi(-1)J(\chi_\pi,\chi_\pi)&\equiv 2\chi_\pi(-1)-\chi_\pi(-1)^2\\&\equiv 2\chi_\pi(-1)-1 \pmod{2+2i}\end{aligned}$$

Or $\chi_\pi(-1)=\pm 1$. Si $\chi_\pi(-1)=1$, alors $2\chi_\pi(-1)-1=1$, et si $\chi_\pi(-1)=-1$, alors $2\chi_\pi(-1)-1=-3\equiv 1 \pmod{2+2i}$. Nous avons prouvé que

$$-\chi_\pi(-1)J(\chi_\pi,\chi_\pi)\equiv 1 \pmod{2+2i},$$

et ainsi $-\chi_\pi(-1)J(\chi_\pi,\chi_\pi)$ est primaire. □

Rappelons ce lemme utile :

Lemme. $1^k+2^k+\ldots+(p-1)^k\equiv\begin{cases}0 \pmod p & si\ p-1\nmid k,\\ -1 \pmod p & si\ p-1\mid k.\end{cases}$

Démonstration. Posons $S(k)=1^k+2^k+\cdots+(p-1)^k$.

Soit g un élément primitif modulo p. Autrement dit $\overline{g}$ est un générateur du groupe $\mathbb{F}_p^*$.

Comme $(\overline{1},\overline{g},\overline{g}^2,\ldots,\overline{g}^{p-2})$ est une permutation de $(\overline{1},\overline{2},\ldots,\overline{p-1})$,

$$\begin{aligned}\overline{S(k)}&=\overline{1}^k+\overline{2}^k+\cdots+\overline{p-1}^k\\&=\sum_{i=0}^{p-2}\overline{g}^{ki}=\begin{cases}\overline{p-1}=-\overline{1} & \text{si}\quad p-1\mid k,\\ \frac{\overline{g}^{(p-1)k}-1}{\overline{g}^k-1}=\overline{0} & \text{si}\quad p-1\nmid k,\end{cases}\end{aligned}$$

puisque $p-1\mid k \iff \overline{g}^k=\overline{1}$.

□

Proposition 118. *Si π est un premier primaire tel que* $\mathrm{N}(\pi) = p \equiv 1 \pmod 4$*, alors*

$$-\chi_\pi(-1)J(\chi_\pi, \chi_\pi) = \pi.$$

Démonstration. Comme il n'existe qu'un seul associé primaire de π (proposition 106), il suffit d'après la proposition précédente de prouver que π et $J(\chi_\pi, \chi_\pi)$ sont associés.

Par définition de χ_π, pour tout $t \in \mathbb{Z}$, $\chi_\pi(t) \equiv t^{\frac{p-1}{4}} \pmod \pi$, et donc

$$J(\chi_\pi, \chi_\pi) \equiv \sum_{t=1}^{p-1} t^{\frac{p-1}{4}}(1-t)^{\frac{p-1}{4}} \pmod \pi.$$

De plus,

$$\begin{aligned}
\sum_{t=1}^{p-1} t^{\frac{p-1}{4}}(1-t)^{\frac{p-1}{4}} &= \sum_{t=1}^{p-1} t^{\frac{p-1}{4}} \sum_{j=0}^{\frac{p-1}{4}} \binom{\frac{p-1}{4}}{j} (-1)^j t^j \\
&= \sum_{j=0}^{\frac{p-1}{4}} (-1)^j \binom{\frac{p-1}{4}}{j} \sum_{t=1}^{p-1} t^{j+\frac{p-1}{4}} \\
&= \sum_{j=0}^{\frac{p-1}{4}} (-1)^j \binom{\frac{p-1}{4}}{j} S\left(j + \frac{p-1}{4}\right),
\end{aligned}$$

où, comme dans le lemme, $S(k) = 1^k + 2^k + \cdots + (p-1)^k$.

Pour les indices j tels que $0 \le j \le \frac{p-1}{4}$, alors $1 \le j + \frac{p-1}{4} < p-1$, donc $S\left(j + \frac{p-1}{4}\right) \equiv 0 \pmod p$, a fortiori $S\left(j + \frac{p-1}{4}\right) \equiv 0 \pmod \pi$. Ainsi

$$J(\chi_\pi, \chi_\pi) \equiv 0 \pmod \pi.$$

La proposition 19 du chapitre "Sommes de Gauss et sommes de Jacobi" montre que $\mathrm{N}(J(\chi_\pi, \chi_\pi)) = p$, donc $J(\chi_\pi, \chi_\pi)$, comme π, est un élément premier de D, et puisque que $\pi \mid J(\chi_\pi, \chi_\pi)$, ils sont associés, ce qui prouve la proposition. □

Proposition 119. *Si π est un premier primaire tel que* $\mathrm{N}(\pi) = p \equiv 1 \pmod 4$*, alors*

$$g(\chi_\pi)^4 = \pi^3\overline{\pi}.$$

Démonstration. Puisque $\chi_\pi(-1) = \pm 1$, les propositions 116 et 118 montrent que

$$\begin{aligned}
g(\chi_\pi)^4 &= pJ(\chi_\pi, \chi_\pi)^2 \\
&= p\pi^2 \\
&= \pi^3\overline{\pi}.
\end{aligned}$$

□

Nous allons maintenant examiner deux cas particuliers de la loi de réciprocité biquadratique.

Proposition 120. *Soit π un premier primaire tel que* $\mathrm{N}(\pi) = p \equiv 1 \pmod 4$*, et soit* $q \equiv 3 \pmod 4$, $q > 0$, *un premier rationnel, premier dans D. Alors*

$$\chi_\pi(-q) = \chi_q(\pi).$$

Notons que $-q$ est un premier primaire, avec $q = 4k-1,\ k \in \mathbb{Z}$.

De plus $\frac{\mathrm{N}(-q)-1}{4} = \frac{q^2-1}{4} = \frac{(4k-1)^2-1}{4} = 4k^2-2k$ est pair. Comme $\chi_q(\pi) = \chi_{-q}(\pi)$, cette proposition s'écrit

$$\chi_\pi(-q) = \chi_{-q}(\pi)(-1)^{\frac{\mathrm{N}(-q)-1}{4}\frac{\mathrm{N}(\pi)-1}{4}}.$$

C'est bien un cas particulier de la loi de réciprocité biquadratique.

Démonstration. Comme $q \equiv 3 \pmod 4$,

$$\begin{aligned} g(\chi_\pi)^q &\equiv \sum_{j\in\mathbb{F}_p} \chi_\pi(j)^q \zeta^{qj} \\ &\equiv \sum_{j\in\mathbb{F}_p} \chi_\pi^3(j)\zeta^{qj} \\ &= \sum_{k\in\mathbb{F}_p} \chi_\pi^3(q^{-1}k)\zeta^k \qquad (k = qj) \\ &= \chi_\pi^{-1}(q^{-1}) \sum_{k\in\mathbb{F}_p} \overline{\chi_\pi}(k)\zeta^k \\ &\equiv \chi_\pi(q) g(\overline{\chi_\pi}) \pmod q \end{aligned}$$

Ainsi

$$g(\chi_\pi)^{q+1} \equiv \chi_\pi(q) g(\chi_\pi) g(\overline{\chi_\pi}) \pmod q.$$

La proposition 52 du chapitre "Sommes de Gauss et sommes de Jacobi" montre que $g(\overline{\chi_\pi}) = \chi_\pi(-1)\overline{g(\chi_\pi)}$, et $|g(\chi_\pi)|^2 = p$, donc

$$g(\chi_\pi)^{q+1} \equiv \chi_\pi(-q)p \pmod q.$$

Notons que

$$\pi^q = (a+bi)^q \equiv a^q + b^q i^q \equiv a + bi^3 = a - bi = \overline{\pi} \pmod q,$$

et donc $p = \pi\overline{\pi} \equiv \pi^{q+1} \pmod q$. Ainsi

$$g(\chi_\pi)^{q+1} \equiv \chi_\pi(-q)\pi^{q+1} \pmod q.$$

La proposition 119 permet d'utiliser $g(\chi_\pi)^4 = \pi^3\overline{\pi} \equiv \pi^{q+3} \pmod q$, donc

$$\pi^{\frac{(q+3)(q+1)}{4}} \equiv \chi_\pi(-q)\pi^{q+1} \pmod q,$$

ce qui donne après simplification, puisque q est premier avec π,

$$\pi^{\frac{q^2-1}{4}} \equiv \chi_\pi(-q) \pmod q.$$

Mais, par définition de χ_q,

$$\chi_q(\pi) \equiv \pi^{\frac{q^2-1}{4}} \pmod q,$$

donc

$$\chi_q(\pi) \equiv \chi_\pi(-q) \pmod q.$$

Comme les classes des quatre unités $1, i, i^2, i^3$ sont distinctes dans D/qD, ceci montre que

$$\chi_q(\pi) = \chi_\pi(-q).$$

□

Proposition 121. *Soit π un premier primaire tel que $\mathrm{N}(\pi) = p \equiv 1 \pmod 4$, et soit $q \neq p$ un premier rationnel, $q \equiv 1 \pmod 4, q > 0$. Alors $\chi_\pi(q) = \chi_q(\pi)$.*

(Ici q n'est pas premier dans D, et χ_q est un caractère biquadratique généralisé.)

Démonstration. Puisque $q \equiv 1 \pmod 4$,

$$\begin{aligned} g(\chi_\pi)^q &\equiv \sum_{j\in\mathbb{F}_p} \chi_\pi(j)^q \zeta^{qj} \\ &\equiv \sum_{j\in\mathbb{F}_p} \chi_\pi(j)\zeta^{qj} \\ &\equiv \sum_{k\in\mathbb{F}_p} \chi_\pi(q^{-1}k)\zeta^k \qquad (k = qj) \\ &\equiv \overline{\chi_\pi}(q) g(\chi_\pi) \pmod q. \end{aligned}$$

Par conséquent,

$$g(\chi_\pi)^{q+3} \equiv \overline{\chi_\pi}(q) g^4(\chi_\pi) \pmod q.$$

En utilisant la valeur de $g(\chi_\pi)^4$ donnée par la proposition 116, nous obtenons

$$(\pi^3\overline{\pi})^{\frac{q+3}{4}} \equiv \overline{\chi_\pi}(q)\pi^3\overline{\pi} \pmod q.$$

Puisque $q \wedge p = 1$, alors $q \wedge \pi = 1$ et $q \wedge \overline{\pi} = 1$, et nous pouvons simplifier, pour obtenir

$$(\pi^3)^{\frac{q-1}{4}}(\overline{\pi})^{\frac{q-1}{4}} \equiv \overline{\chi_\pi}(q) \pmod q.$$

Décomposons q sous la forme $q = \lambda\overline{\lambda}$, où λ est premier dans D. Comme $\mathrm{N}(\lambda) = q$, l'égalité précédente implique

$$\chi_\lambda(\pi^3)\chi_\lambda(\overline{\pi}) \equiv \overline{\chi_\pi}(q) \pmod \lambda.$$

Ces deux unités étant congrues modulo λ dans D, elles sont égales (proposition 100). Ainsi

$$\chi_\lambda(\pi^3)\chi_\lambda(\overline{\pi}) = \overline{\chi_\pi}(q).$$

Comme $\chi_\lambda^3 = \chi_\lambda^{-1} = \overline{\chi_\lambda}$,

$$\overline{\chi_\lambda(\pi)}\chi_\lambda(\overline{\pi}) = \overline{\chi_\pi}(q).$$

La proposition 103 donne alors

$$\chi_{\overline{\lambda}}(\overline{\pi})\chi_\lambda(\overline{\pi}) = \overline{\chi_\pi}(q).$$

Par définition du caractère généralisé χ_q,

$$\chi_q(\overline{\pi}) = \overline{\chi_\pi}(q).$$

En prenant les conjugués, et en utilisant à nouveau la proposition 103,

$$\chi_q(\pi) = \chi_\pi(q).$$

□

Proposition 122. *Soit $a \in \mathbb{Z}$ tel que $a \equiv 1 \pmod 4, a \neq 1$, et λ un élément primaire de D tel que $\lambda \wedge a = 1$. Alors*

$$\chi_a(\lambda) = \chi_\lambda(a).$$

Démonstration. La proposition 109 permet de décomposer le primaire λ en produit de premiers primaires $\lambda = \lambda_1 \cdots \lambda_t$, et par définition,

$$\chi_\lambda(a) = \chi_{\lambda_1}(a) \cdots \chi_{\lambda_t}(a).$$

Comme $a \equiv 1 \pmod 4$, a se décompose, quel que soit son signe, sous la forme

$$a = \prod_{i=1}^{r} p_i \prod_{j=1}^{s} (-q_j),$$

où les p_i, q_j vérifient $p_i \equiv 1 \pmod 4,\ q_j \equiv 3 \pmod 4,\ p_i > 0,\ q_j > 0$.

Alors

$$\chi_\lambda(a) = \prod_{k=1}^{t} \left(\prod_{i=1}^{r} \chi_{\lambda_k}(p_i) \prod_{j=1}^{s} \chi_{\lambda_k}(-q_j) \right).$$

La remarque suivant cette proposition 109 montre que chaque premier primaire λ_k est de la forme $\lambda_k = -q$, où $q \equiv 3 \pmod 4$ est un premier rationnel positif, ou bien égal à un premier π tel que $\mathrm{N}(\pi) = \pi\overline{\pi} = p \equiv 1 \pmod 4$.

- Si $\lambda_k = -q, q \equiv 3 \pmod 4$, alors la proposition 104 montre que

  $$\chi_{\lambda_k}(-q_j) = \chi_{-q}(-q_j) = \chi_q(-q_j) = 1, \text{et}$$
  $$\chi_{-q_j}(\lambda_k) = \chi_{-q_j}(-q) = \chi_{q_j}(-q) = 1,$$

  puisque $\lambda \wedge a = 1$, et donc $q \wedge q_j = \lambda_k \wedge q_j = 1$. Par conséquent,

  $$\chi_{\lambda_k}(-q_j) = \chi_{-q_j}(\lambda_k).$$

  De plus, si on écrit $p_i = \pi_i\overline{\pi_i}$, alors

  $$\chi_{\lambda_k}(p_i) = \chi_q(p_i) = \chi_q(\pi_i)\chi_q(\overline{\pi_i}).$$

  Puisque $\pi_i \equiv 1 \pmod 4$, et $p_i \neq q$ est un premier rationnel, la proposition 120 montre que

  $$\chi_q(\pi_i) = \chi_{\pi_i}(-q) = \chi_{\pi_i}(\lambda_k),$$
  $$\chi_q(\overline{\pi_i}) = \chi_{\overline{\pi_i}}(-q) = \chi_{\overline{\pi_i}}(\lambda_k),$$

  par conséquent

  $$\chi_{\lambda_k}(p_i) = \chi_{\pi_i}(\lambda_k)\chi_{\overline{\pi_i}}(\lambda_k) = \chi_{p_i}(\lambda_k).$$

- Si $\lambda_k = \pi$, où $\mathrm{N}(\pi) = \pi\overline{\pi} = p \equiv 1 \pmod 4$, alors, puisque $q_j \equiv 3 \pmod 4$ est un premier rationnel, la proposition 120 donne

  $$\chi_{\lambda_k}(-q_j) = \chi_\pi(-q_j) = \chi_{-q_j}(\pi) = \chi_{-q_j}(\lambda_k).$$

  De plus, puisque $p_i \equiv 1 \pmod 4$ est un premier rationnel, la proposition 121 donne

  $$\chi_{\lambda_k}(p_i) = \chi_\pi(p_i) = \chi_{p_i}(\pi) = \chi_{p_i}(\lambda_k).$$

Pour conclure,

$$\begin{aligned}\chi_\lambda(a) &= \prod_{k=1}^{t}\left(\prod_{i=1}^{r}\chi_{\lambda_k}(p_i)\prod_{j=1}^{s}\chi_{\lambda_k}(-q_j)\right)\\ &= \prod_{k=1}^{t}\left(\prod_{i=1}^{r}\chi_{p_i}(\lambda_k)\prod_{j=1}^{s}\chi_{-q_j}(\lambda_k)\right)\\ &= \prod_{k=1}^{t}\chi_a(\lambda_k)\\ &= \chi_a(\lambda).\end{aligned}$$

□

La restriction $a \neq 1$ conduit à considérer de nombreux cas inutiles dans la démonstration de la réciprocité biquadratique. Pour éviter cet écueil, définissons χ_π dans la cas où π est une unité par $\chi_\pi = \varepsilon$, le caractère trivial. Ainsi

$$\chi_1 = \chi_{-1} = \chi_i = \chi_{-i} = \varepsilon,$$

et χ_π a un sens pour tout π tel que $1 + i \nmid \pi$. Ceci permet de lever l'exception de la proposition 122.

Proposition 123. *Soit $a \in \mathbb{Z}$ tel que $a \equiv 1 \pmod 4$, et λ un élément primaire de D tel que $\lambda \wedge a = 1$. Alors*

$$\chi_a(\lambda) = \chi_\lambda(a).$$

Démonstration. Il ne reste à vérifier que la cas $a = 1$. Alors, puisque $\chi_1 = \varepsilon$, $\chi_1(\lambda) = 1 = \chi_\lambda(1)$. □

Définissons, pour un entier impair n,

$$\varepsilon(n) = (-1)^{\frac{n-1}{2}}.$$

Lemme. *Soient n, m deux entiers impairs. Alors*

(a) Si $n \equiv m \pmod 4$, alors $\varepsilon(n) = \varepsilon(m)$.

(b) $\varepsilon(nm) = \varepsilon(n)\varepsilon(m)$.

(c) $\varepsilon(n)n \equiv 1 \pmod 4$.

Démonstration. Ici n, m sont des entiers impairs.

(a) Si $n \equiv m \pmod 4$, alors $m = n + 4k,\ k \in \mathbb{Z}$, donc

$$\varepsilon(m) = (-1)^{\frac{n+4k-1}{2}} = (-1)^{\frac{n-1}{2}}(-1)^{2k} = (-1)^{\frac{n-1}{2}} = \varepsilon(n).$$

(b) Si on note $n = 2k + 1, m = 2l + 1$, alors

$$\frac{nm-1}{2} = 2kl + k + l \equiv k + l \equiv \frac{n-1}{2} + \frac{m-1}{2} \pmod 2,$$

donc $(-1)^{\frac{nm-1}{2}} = (-1)^{\frac{n-1}{2}}(-1)^{\frac{m-1}{2}}$.

(c) Comme $\varepsilon(n) = 1$ si $n \equiv 1 \pmod 4$, et $\varepsilon(n) = -1$ si $n \equiv -1 \pmod 4$, nous avons pour tout n impair

$$\varepsilon(n)n \equiv 1 \pmod 4.$$

□

Proposition 124. *Soient $\pi = a + bi$ et $\lambda = c + di$ des éléments de D primaires et premiers entre eux. Si $a \wedge b = 1$ et $c \wedge d = 1$, alors*

$$\chi_\lambda(\pi) = \chi_\pi(\lambda)(-1)^{\frac{a-1}{2}\frac{c-1}{2}}.$$

Notons qu'on ne suppose pas que $\mathrm{N}(\pi) \neq \mathrm{N}(\lambda)$, ni que λ, π sont premiers dans D.

Démonstration. Les hypothèses impliquent que $a \wedge \pi = b \wedge \pi = c \wedge \lambda = d \wedge \lambda = 1$. Comme $c\pi \wedge \lambda = 1$, la congruence

$$\begin{aligned} c\pi &= ac + bci \\ &= ac + bd + bi(c + id) \\ &\equiv ac + bd \pmod \lambda, \end{aligned}$$

montre que $(ac + bd) \wedge \lambda = 1$, et symétriquement $(ac + bd) \wedge \pi = 1$.

Notons que $a \wedge \pi = 1$ entraîne l'existence de $u, v \in D$ tels que $ua + v\pi = 1$, donc $\overline{u}\, a + \overline{v}\, \overline{\pi} = 1$, ce qui prouve $a \wedge \overline{\pi} = 1$. Le même raisonnement donne $a \wedge \overline{\pi} = b \wedge \overline{\pi} = c \wedge \overline{\lambda} = d \wedge \overline{\lambda} = 1$, et $(ac + bd) \wedge \overline{\lambda} = (ac + bd) \wedge \overline{\pi} = 1$.

La congruence $c\pi \equiv ac + bd \pmod \lambda$, et la proposition 110(a), montrent que

$$\chi_\lambda(c)\chi_\lambda(\pi) = \chi_\lambda(ac + bd). \tag{4.1}$$

Symétriquement, comme $a\lambda = ac + bd + id\pi \equiv ac + bd \pmod \pi$,

$$\chi_\pi(a)\chi_\pi(\lambda) = \chi_\pi(ac + bd). \tag{4.2}$$

Puisque a et $ac + bd$ sont réels, le passage au conjugué dans l'égalité (4.2) donne, grâce à la proposition 103,

$$\chi_{\overline{\pi}}(a)\overline{\chi_\pi(\lambda)} = \chi_{\overline{\pi}}(ac + bd). \tag{4.3}$$

Le produit de (4.1) et (4.3) s'écrit, grâce à la proposition 110(c),

$$\chi_\lambda(c)\chi_{\overline{\pi}}(a)\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_{\lambda\overline{\pi}}(ac + bd).$$

En utilisant à nouveau la proposition 103,

$$(\chi_\lambda(c)\chi_{\overline{\pi}}(a))^{-1} = \overline{\chi_\lambda(c)\chi_{\overline{\pi}}(a)} = \chi_\pi(a)\chi_{\overline{\lambda}}(c).$$

Nous avons donc prouvé

$$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_\pi(a)\chi_{\overline{\lambda}}(c)\chi_{\lambda\overline{\pi}}(ac + bd). \tag{4.4}$$

Calculons le membre de droite de l'égalité (4.4).

Pour chaque facteur du membre de droite de l'égalité (4.4), utilisons l'égalité suivante, vraie pour tout entier impair x, puisque $\varepsilon(x)^2 = 1$,

$$\chi_\alpha(x) = \chi_\alpha(\varepsilon(x))\chi_\alpha(\varepsilon(x)x) \qquad (x \in \{a, c, ac + bd\}).$$

En appliquant cette méthode, puisque $\varepsilon(a)a \equiv 1 \pmod 4$, et $\pi \wedge a = 1$, la proposition 123 montre que (même si a est une unité)

$$\begin{aligned}\chi_\pi(a) &= \chi_\pi(\varepsilon(a))\chi_\pi(\varepsilon(a)a)\\ &= \chi_\pi(\varepsilon(a))\chi_{\varepsilon(a)a}(\pi)\\ &= \chi_\pi(\varepsilon(a))\chi_a(\pi),\end{aligned}$$

la dernière égalité vient du fait que a et $\varepsilon(a)a$ étant associés, ils définissent le même caractère.

Dans le cas où $\varepsilon(a) = -1$, la proposition 112 donne

$$\chi_\pi(\varepsilon(a)) = \chi_\pi(-1) = (-1)^{\frac{a-1}{2}} = \varepsilon(a)^{\frac{a-1}{2}},$$

et l'égalité $\chi_\pi(\varepsilon(a)) = \varepsilon(a)^{\frac{a-1}{2}}$ est trivialement vraie si $\varepsilon(a) = 1$. Par conséquent,

$$\chi_\pi(a) = \varepsilon(a)^{\frac{a-1}{2}}\chi_a(\pi).$$

En procédant de même pour les trois facteurs du membre de droite de l'égalité (4.4), puisque $\overline{\lambda} \wedge c = 1$, et $\lambda\overline{\pi} \wedge (ac + bd) = 1$, nous obtenons les trois égalités

$$\chi_\pi(a) = \varepsilon(a)^{\frac{a-1}{2}}\chi_a(\pi), \tag{4.5}$$

$$\chi_{\overline{\lambda}}(c) = \varepsilon(c)^{\frac{c-1}{2}}\chi_c(\overline{\lambda}) \tag{4.6}$$

$$\chi_{\lambda\overline{\pi}}(ac + bd) = \varepsilon(ac + bd)^{\frac{ac+bd-1}{2}}\chi_{ac+bd}(\lambda\overline{\pi}). \tag{4.7}$$

Le produit de ces trois égalités donne

$$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = P\ \chi_a(\pi)\chi_c(\overline{\lambda})\chi_{ac+bd}(\lambda\overline{\pi}),$$

où

$$P = \varepsilon(a)^{\frac{a-1}{2}}\varepsilon(c)^{\frac{c-1}{2}}\varepsilon(ac + bd)^{\frac{ac+bd-1}{2}}.$$

Puisque $ac + bd \equiv ac \pmod 4$, le lemme donne

$$\begin{aligned}P &= \varepsilon(a)^{\frac{a-1}{2}}\varepsilon(c)^{\frac{c-1}{2}}\varepsilon(ac)^{\frac{ac-1}{2}}\\ &= \varepsilon(a)^{\frac{a-1}{2}}\varepsilon(c)^{\frac{c-1}{2}}\varepsilon(ac)^{\frac{a-1}{2}}\varepsilon(ac)^{\frac{c-1}{2}}\\ &= \varepsilon(a)^{\frac{a-1}{2}}\varepsilon(c)^{\frac{c-1}{2}}\varepsilon(a)^{\frac{a-1}{2}}\varepsilon(c)^{\frac{a-1}{2}}\varepsilon(a)^{\frac{c-1}{2}}\varepsilon(c)^{\frac{c-1}{2}}\\ &= \varepsilon(c)^{\frac{a-1}{2}}\varepsilon(a)^{\frac{c-1}{2}}\\ &= (-1)^{\frac{c-1}{2}\frac{a-1}{2}}(-1)^{\frac{a-1}{2}\frac{c-1}{2}}\\ &= 1.\end{aligned}$$

Ainsi

$$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_a(\pi)\chi_c(\overline{\lambda})\chi_{ac+bd}(\lambda\overline{\pi}).$$

Justifions les égalités suivantes, donnant les trois facteurs du membre de droite.

$$\chi_a(\pi) = \chi_a(a + bi) = \chi_a(bi) = \chi_a(i), \tag{4.8a}$$

$$\chi_c(\overline{\lambda}) = \chi_c(c - di) = \chi_c(-di) = \chi_c(i), \tag{4.8b}$$

$$\chi_{ac+bd}(\lambda\overline{\pi}) = \chi_{ac+bd}(ac + bd + (ad - bc)i) = \chi_{ac+bd}((ad - bc)i) = \chi_{ac+bd}(i). \tag{4.8c}$$

En effet, si a, c et $ac+bd$ ne sont pas des unités, ce sont des entiers impairs, vérifiant $a \wedge b = 1, c \wedge d = 1$: la proposition 113 montre qu'alors $\chi_c(-d) = \chi_a(b) = 1$. Ceci reste vrai si a est une unité, puisqu'alors $\chi_a = \varepsilon$, ou si c est une unité.

Il reste à vérifier que $(ad-bc)\wedge(ac+bd) = 1$. Si un premier μ de D vérifie $\mu \mid ad-bc$ et $\mu \mid ac+bd$, alors $\mu \mid \lambda\overline{\pi} = ac+bd+(ad-bc)i$, donc μ divise λ ou $\overline{\pi}$. Ceci est impossible, car nous avons prouvé au début de cette démonstration que $(ac+bd)\wedge\lambda = (ac+bd)\wedge\overline{\pi} = 1$. Ainsi $ad-bc$ et $ac+bd$ sont premiers entre eux dans D, donc aussi dans $\mathbb{Z}$. Par conséquent, la proposition 113 montre que $\chi_{ac+bd}(ad-bc) = 1$ (même si $ac+bd$ est une unité), et les égalités (4.8a),(4.8b),(4.8c) sont justifiées.

En multipliant ces trois égalités (4.8a),(4.8b),(4.8c), nous obtenons

$$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_{(ac+bd)ac}(i) \tag{4.9}$$

Comme a, c sont impairs, et b, d pairs, $(ac+bd)ac \equiv (ac)^2 \equiv 1 \pmod 4$. La proposition 114 donne alors (même si $(ac+bd)ac = 1$)

$$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = (-1)^{\frac{(ac+bd)ac-1}{4}}.$$

Comme vu au début du paragraphe 5, π et λ étant primaires, la proposition 105 montre qu'il existe des entiers m, n, s, t tels que

$$a = 2m+1, b = 2n, \qquad c = 2s+1, d = 2t,$$

tels que $m = \frac{a-1}{2}, n = \frac{b}{2}$ ont même parité, et $s = \frac{s-1}{2}, t = \frac{d}{2}$ ont même parité.

La réduction modulo 8 de $(ac+bd)ac-1$ donne

$$\begin{aligned}(ac+bd)ac-1 &= [(2m+1)(2s+1)+4nt](2m+1)(2s+1)-1\\ &= (4ms+4nt+2m+2s+1)(4ms+2m+2s+1)-1\\ &\equiv 4ms+(4m^2+4ms+2m)+(4ms+4s^2+2s)+(4ms+4nt+2m+2s)\\ &\equiv 4m^2+4m+4s^2+4m+4s+4nt \pmod 8,\end{aligned}$$

donc la réduction modulo 2 de l'exposant donne

$$\begin{aligned}\frac{(ac+bd)ac-1}{4} &\equiv m(m+1)+s(s+1)+nt\\ &\equiv nt\\ &\equiv ms \pmod 2,\end{aligned}$$

puisque m, n d'une part, t, s d'autre part, ont même parité. Ainsi

$$(-1)^{\frac{(ac+bd)ac-1}{4}} = (-1)^{\frac{a-1}{2}\frac{c-1}{2}},$$

et nous avons prouvé dans ce cas que

$$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = (-1)^{\frac{a-1}{2}\frac{c-1}{2}}.$$

ce qui est équivalent à la formule de l'énoncé, puisque $\overline{\chi_\pi(\lambda)} = \chi_\pi(\lambda)^{-1}$.

□

Nous pouvons maintenant prouver la loi de réciprocité biquadratique.

Proposition 125. Loi de Réciprocité Biquadratique.
Si λ, π sont des éléments primaires de $\mathbb{Z}[i]$, alors

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{\frac{\mathrm{N}(\lambda)-1}{4}\frac{\mathrm{N}(\pi)-1}{4}}.$$

Démonstration. Si λ et π ne sont pas premiers entre eux, alors $\chi_\pi(\lambda) = \chi_\lambda(\pi) = 0$. Nous pouvons donc supposer $\lambda \wedge \pi = 1$.

En factorisant par le pgcd des parties réelles et imaginaires de π, λ, on peut écrire

$$\pi = m(a+bi), \lambda = n(c+di), \text{ où } a \wedge b = 1, c \wedge d = 1.$$

Puisque les élément primaires π, λ ne sont pas divisibles par 2, m, n sont impairs. Quitte à remplacer m par $-m($ et $a+bi$ par $-a-bi)$, on peut supposer $m \equiv 1 \pmod 4$, et aussi $n \equiv 1 \pmod 4$.

Nous savons que $n \equiv 1 \pmod 4$, et aussi que $a+bi \wedge n = 1$, puisque $\pi \wedge \lambda = 1$. La proposition 122 montre alors que $\chi_{a+bi}(n) = \chi_n(a+bi)$, et symétriquement, $\chi_{c+di}(m) = \chi_m(c+di)$. De plus, la proposition 113 montre que $\chi_m(n) = \chi_n(m) = 1$, et ceci reste vrai si $m = 1$, ou si $n = 1$, puisque $\chi_1 = \varepsilon$.

Comme $\pi \equiv 1 \pmod{(1+i)^3}$, et $m \equiv 1 \pmod{(1+i)^3}$ (puisque $(1+i)^3 = -2(1+i)$ divise 4), l'égalité $\pi = m(a+bi)$ montre que $a+bi \equiv 1 \pmod{(1+i)^3}$, donc $a+bi$ est primaire, et de même $c+di$ est primaire. Alors, en utilisant les propositions 123 et 124,

$$\begin{aligned}
\chi_\lambda(\pi) &= \chi_\lambda(m)\chi_\lambda(a+bi) \\
&= \chi_m(\lambda)\chi_n(a+bi)\chi_{c+di}(a+bi) \\
&= \chi_m(\lambda)\chi_{a+bi}(n)\chi_{a+bi}(c+di)(-1)^{\frac{a-1}{2}\frac{c-1}{2}} \\
&= \chi_m(\lambda)\chi_{a+bi}(\lambda)(-1)^{\frac{a-1}{2}\frac{c-1}{2}} \\
&= \chi_\pi(\lambda)(-1)^{\frac{a-1}{2}\frac{c-1}{2}}.
\end{aligned}$$

Notons le primaire $a+bi$ sous la forme $a+bi = 2k+1+2li$, où $k = \frac{a-1}{2} \equiv l = \frac{b}{2} \pmod 2$.

Puisque $m \equiv 1 \pmod 4$, $m^2 \equiv 1 \pmod 8$.

$$\begin{aligned}
\mathrm{N}(\pi) - 1 &= m^2[(2k+1)^2 + 4l^2) - 1 \\
&= m^2(4k^2 + 4k + 4l^2 + 1) - 1 \\
&\equiv 4(k^2 + k + l^2) \pmod 8,
\end{aligned}$$

et puisque $k \equiv l \equiv \frac{a-1}{2} \pmod 2$,

$$\begin{aligned}
\frac{\mathrm{N}(\pi)-1}{4} &\equiv k^2 + k + l^2 \\
&\equiv \frac{a-1}{2} \pmod 2,
\end{aligned}$$

si bien que

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{\frac{\mathrm{N}(\lambda)-1}{4}\frac{\mathrm{N}(\pi)-1}{4}}.$$

□

4.6 Résidus biquadratiques entiers.

Si $p \equiv 3 \pmod 4$, la proposition 24 du chapitre "Sommes de Gauss et sommes de Jacobi" montre que pour tout $\alpha \in \mathbb{F}_p^*$ qui est un carré de $\mathbb{F}_p$, l'équation $x^4 = \alpha$ admet deux solutions dans $\mathbb{F}_p$, puisque $d = (p-1) \wedge 4 = 2$.

Par exemple, pour $p = 19$, l'équation $x^4 = 5$ équivaut à $x^2 = 9$ ou $x^2 = -9$. La première équation a deux solutions 3 et -3, mais la deuxième n'en a pas, puisque $\left(\frac{-9}{19}\right) = \left(\frac{-1}{19}\right)\left(\frac{9}{19}\right) = \left(\frac{-1}{19}\right) = -1$.

Supposons maintenant que $p \equiv 1 \pmod 4$. Alors $d = 4 \wedge (p-1) = 4$, et cette même proposition prouve que $x^4 = \alpha$ admet une solution dans $\mathbb{F}_p$ si et seulement si $\alpha^{\frac{p-1}{4}} = 1$, et dans ce cas, elle en admet quatre.

Comme $p \equiv 1 \pmod 4$, $p = \pi\overline{\pi}$, où π est premier dans D.

Soit $a \in \mathbb{Z}$. Supposons que la congruence $x^4 \equiv a \pmod p$ admet une solution dans $\mathbb{Z}$. Alors $x^4 \equiv a \pmod \pi$, et la proposition 102 montre que $\chi_\pi(\alpha) = 1$.

Réciproquement, si $\chi_\pi(\alpha) = 1$, alors cette même proposition montre l'existence de $\alpha \in D$ tel que $\alpha^4 \equiv a \pmod \pi$. De plus, $D/\pi D \simeq \mathbb{F}_p$, et il existe un représentant $x \in \{0, 1, \cdots, p-1\}$ de α modulo π. Ainsi $x^4 \equiv a \pmod \pi$, où $x \in \mathbb{Z}$.

Comme $\pi \mid x^4 - a$, alors $p = \mathrm{N}(\pi) \mid (x^4 - a)^2$, et p est un premier rationnel, donc $p \mid x^4 - a$, soit $x^4 \equiv a \pmod p$.

Nous avons ainsi prouvé cette proposition :

Proposition 126. *Soit $a \in \mathbb{Z}$, et $p \equiv 1 \pmod 4$ est un premier rationnel. Alors $p = \mathrm{N}(\pi)$, où π est premier dans D, et*

$$\exists x \in \mathbb{Z},\ x^4 \equiv a \pmod p \iff \chi_\pi(a) = 1 \iff \exists \alpha \in D,\ \alpha^4 \equiv a \pmod \pi.$$

4.7 Loi supplémentaire à la loi de réciprocité biquadratique.

Chaque élément premier de $\mathbb{Z}[i]$ qui n'est pas divisible par $1+i$ est associé à un premier primaire λ, et la loi de réciprocité biquadratique permet d'évaluer $\chi_\pi(\lambda)$. Il reste à connaître le caractère biquadratique des unités, et de $1+i$.

Pour les unités, la définition donne

$\chi_\pi(i) = i^{\frac{p-1}{4}}$ si $\mathrm{N}(\pi) = p$ est un premier rationnel congru à 1 modulo 4.

$\chi_{-q}(i) = \chi_q(i) = i^{\frac{q^2-1}{4}}$ si $q > 0$ est un premier rationnel congru à 3 modulo 4.

Nous pouvons donner une formule commune simple, qui fera partie de la loi supplémentaire.

Proposition 127. *Si $\pi = a + bi$ est un premier primaire, alors*

$$\chi_\pi(i) = i^{\frac{-a+1}{2}}.$$

Démonstration. Soit $\pi = a + bi$ un premier primaire de $\mathbb{Z}[i]$.

- Si $\pi = -q$, où $q \equiv 3 \pmod 4, q > 0$, est un premier rationnel, alors $a = -q, b = 0$. Notons $-q = a = 4k + 1,\ k \in \mathbb{Z}$. Alors

$$\begin{aligned} \frac{q^2-1}{4} &= 4k^2 + 2k \\ &\equiv 2k = \frac{a-1}{2} \pmod 4. \end{aligned}$$

Donc

$$\chi_{-q}(i) = \chi_q(i) = i^{\frac{q^2-1}{4}} = i^{\frac{a-1}{2}} = \left(\frac{1}{i}\right)^{\frac{-a+1}{2}} = (-i)^{\frac{-a+1}{2}} = (-1)^{\frac{-a+1}{2}} i^{\frac{-a+1}{2}} = i^{\frac{-a+1}{2}},$$

puisque $(-1)^{\frac{-a+1}{2}} = (-1)^{-2k} = 1$.

- Supposons maintenant que $\mathrm{N}(\pi) = p$, où $p \equiv 1 \pmod 4$ est un premier rationnel. $\pi = a + bi$ étant primaire, alors a est impair, et b pair, et

$$\pi = 2m + 1 + 2ni, \qquad \text{où } m = \frac{a-1}{2} \equiv n = \frac{b}{2} \pmod 2.$$

Comme $m \equiv n \pmod 2$, $m^2 \equiv n^2 \pmod 4$. Alors $p = \pi\overline{\pi} = (2m+1)^2 + (2n)^2$, donc

$$\frac{p-1}{4} = m^2 + n^2 + m \equiv 2m^2 + m = 4\frac{m(m+1)}{2} - m \equiv -m \pmod 4.$$

Par conséquent

$$\chi_\pi(i) = i^{\frac{\mathrm{N}(\pi)-1}{4}} = i^{\frac{p-1}{4}} = i^{-m} = i^{\frac{-a+1}{2}}.$$

L'égalité $\chi_\pi(i) = i^{\frac{-a+1}{2}}$. a donc été vérifiée pour tous les premiers primaires π.

□

Nous aurons besoin de la valeur de $\chi_a(i)$ pour un entier impair a. En généralisant la proposition 114, nous obtenons

Proposition 128. *Si a est un entier impair, alors*

$$\chi_a(i) = (-1)^{\frac{a^2-1}{8}}.$$

Démonstration. Si $a \equiv 1 \pmod 4$, la proposition 114 donne $\chi_a(i) = (-1)^{\frac{a-1}{4}}$. Notons $a = 4A + 1,\ A \in \mathbb{Z}$. Alors

$$(-1)^{\frac{a^2-1}{8}} = (-1)^{2A^2+A} = (-1)^A = (-1)^{\frac{a-1}{4}} = \chi_a(i).$$

Si $a \equiv -1 \pmod 4$, alors $\chi_a(i) = \chi_{-a}(i) = (-1)^{\frac{-a-1}{4}}$ par la même proposition. Notons $a = 4A - 1,\ A \in \mathbb{Z}$. Alors

$$(-1)^{\frac{a^2-1}{8}} = (-1)^{2A^2-A} = (-1)^{-A} = (-1)^{\frac{-a-1}{4}} = \chi_a(i).$$

Dans les deux cas,

$$\chi_a(i) = i^{\frac{a^2-1}{8}}.$$

Si $a = \pm 1$ est une unité, alors $(-1)^{\frac{a^2-1}{8}} = (-1)^0 = 1 = \chi_a(i)$. □

Il reste le calcul de $\chi_\pi(1+i)$. Commençons par le calcul de $\chi_q(1+i)$.

Proposition 129. *Si $q \equiv 3 \pmod 4,\ q > 0$, est un premier rationnel, alors*

$$\chi_q(1+i) = i^{\frac{-q-1}{4}}.$$

Démonstration. Notons $q = 4k+3, k \in \mathbb{N}$.

Comme $(1+i)^2 = 2i$, alors $(1+i)^{q-1} = (2i)^{\frac{q-1}{2}}$. De plus,

$$2^{\frac{q-1}{2}} \equiv \left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = (-1)^{\frac{(4k+3)^2-1}{8}} = (-1)^{2k^2+3k+1} = (-1)^{k+1} \pmod{q},$$

et $i^{\frac{q-1}{2}} = i^{2k+1} = (-1)^k i$, si bien que

$$(1+i)^{q-1} \equiv -i \pmod{q}.$$

Comme $\mathrm{N}(q) = q^2$,

$$\chi_q(1+i) \equiv (1+i)^{\frac{q^2-1}{4}} = \left[(1+i)^{q-1}\right]^{\frac{q+1}{4}} \equiv (-i)^{\frac{q+1}{4}} \pmod{q},$$

et ainsi

$$\chi_q(1+i) = (-i)^{\frac{q+1}{4}} = i^{\frac{-q-1}{4}}.$$

□

Proposition 130. *Soit p un premier rationnel , $p \equiv 1 \pmod 4$. Alors*

$$\chi_p(1+i) = i^{\frac{p-1}{4}}.$$

Démonstration. Soit $p = \pi\overline{\pi}, \pi \in \mathbb{Z}[i]$ une décomposition de p. Alors

$$\begin{aligned}
\chi_p(1+i) &= \chi_\pi(1+i)\chi_{\bar\pi}(1+i) \\
&= \chi_\pi(1+i)\overline{\chi_\pi(1-i)} \qquad \text{(proposition 111)} \\
&= \frac{\chi_\pi(1+i)}{\chi_\pi(1-i)} = \chi_\pi(i) \qquad \text{(puisque } (1-i)i = 1+i\text{)} \\
&= i^{\frac{p-1}{4}}.
\end{aligned}$$

□

Généralisons les propositions 129 et 130 à un entier quelconque.

Proposition 131. *Soit $n \in \mathbb{Z}$ un entier, $n \equiv 1 \pmod 4$. Alors*

$$\chi_n(1+i) = i^{\frac{n-1}{4}}.$$

Démonstration. Soit $n \in \mathbb{Z}, n \equiv 1 \pmod 4$.

Si $n = 1$, alors $\chi_1(1+i) = 1 = i^{\frac{n-1}{4}}$. Supposons maintenant que $n \neq 1$.

Si $n > 0$, $n = q_1 q_2 \cdots q_k p_1 p_2 \cdots p_l$, où les p_i, q_i sont des premiers rationnels positifs vérifiant $q_i \equiv -1 \pmod 4, p_i \equiv 1 \pmod 4$, avec k pair, puisque $n \equiv 1 \pmod 4$.

Si $n < 0$, $n = -q_1 q_2 \cdots q_k p_1 p_2 \cdots p_l$, avec k impair.

Dans les deux cas,

$$n = (-q_1)(-q_2)\cdots(-q_k)p_1 p_2 \cdots p_l,$$

si bien que nous pouvons écrire

$$n = s_1 s_2 \cdots s_m, \qquad \text{where } s_i = -q_i, 1 \le i \le k, s_i = p_{i-k},\ k+1 \le i \le k+l = m,$$

où $s_i \equiv 1 \pmod 4$ pour $1 \leq i \leq N$. Alors

$$\begin{aligned}\chi_n(1+i) &= \chi_{-q_1}(1+i)\cdots\chi_{-q_k}(1+i)\chi_{p_1}(1+i)\cdots\chi_{p_l}(1+i)\\ &= i^{\frac{-q_1-1}{4}}\cdots i^{\frac{-q_k-1}{4}} i^{\frac{p_1-1}{4}}\cdots i^{\frac{p_l-1}{4}}\\ &= i^{\frac{s_1-1}{4}}\cdots i^{\frac{s_m-1}{4}}\\ &= i^{\sum_{i=1}^{m}\frac{s_i-1}{4}}\\ &= i^{\frac{n-1}{4}},\end{aligned}$$

où la dernière égalité résulte du lemme précédant la proposition 114.

Ainsi $\chi_n(1+i) = i^{\frac{n-1}{4}}$.

□

Proposition 132. *Soit $\pi = a + bi$ un premier primaire de $\mathbb{Z}[i]$, tel que $\mathrm{N}(\pi) = p \equiv 1 \pmod 4$, où p est un premier rationnel. Alors*

(a) $a \equiv (-1)^{\frac{p-1}{4}} \pmod 4$,

(b) $b \equiv (-1)^{\frac{p-1}{4}} - 1 \pmod 4$.

Démonstration.

(a) L'hypothèse faite sur π s'écrit

$$p = \pi\bar{\pi} = a^2 + b^2 \equiv 1 \pmod 4.$$

Comme dans la preuve de la proposition 127, écrivons π sous la forme

$$\pi = 2m + 1 + 2ni, \qquad \text{où } m = \frac{a-1}{2} \equiv n = \frac{b}{2} \pmod 2.$$

Comme $m \equiv n \pmod 2$, $m^2 \equiv n^2 \pmod 4$. Alors $p = \pi\overline{\pi} = (2m+1)^2 + (2n)^2$, donc

$$\frac{p-1}{4} = m^2 + n^2 + m \equiv 2m^2 + m = 4\frac{m(m+1)}{2} - m \equiv -m \pmod 4.$$

Ainsi $(-1)^{\frac{p-1}{4}} = (-1)^m$.

Si m est pair, alors $a \equiv 1 = (-1)^m \pmod 4$, et si m est impair, alors $a \equiv -1 = (-1)^m \pmod 4$. Dans les deux cas,

$$a \equiv (-1)^{\frac{p-1}{4}} \pmod 4.$$

(b) Dans chacun de ces cas, $b \equiv a - 1 \pmod 4$, donc

$$b \equiv (-1)^{\frac{p-1}{4}} - 1 \pmod 4.$$

□

En d'autres termes, pour tous les premiers primaires $\pi = a + bi$ tels que $\mathrm{N}(\pi) = p$,

$$\begin{aligned}p \equiv 1 \pmod 8 &\iff \pi \equiv 1 \pmod 4,\\ p \equiv 5 \pmod 8 &\iff \pi \equiv 3 + 2i \pmod 4.\end{aligned}$$

Proposition 133. *Soit $\pi = a + bi$ un premier primaire de $\mathbb{Z}[i]$, tel que $\mathrm{N}(\pi) = p \equiv 1 \pmod 4$, où p est un premier rationnel. Alors*

$$\chi_\pi(a(-1)^{\frac{p-1}{4}}) = (-1)^{\frac{a^2-1}{8}}.$$

Démonstration. La proposition 132(a) montre que $a \equiv (-1)^{\frac{p-1}{4}} \pmod 4$, donc $a(-1)^{\frac{p-1}{4}} \equiv 1 \pmod 4$. Par conséquent $a(-1)^{\frac{p-1}{4}}$ est soit une unité, soit un élément primaire.

Si a est une unité, $a = \pm 1$, alors $a(-1)^{\frac{p-1}{4}} = 1$ et dans ce cas $\chi_\pi(a(-1)^{\frac{p-1}{4}}) = 1 = (-1)^{\frac{a^2-1}{8}}$, et la conclusion est vérifiée. Nous pouvons supposer maintenant que a n'est pas une unité.

Comme $a(-1)^{\frac{p-1}{4}} \equiv 1 \pmod 4$, la loi de réciprocité biquadratique (proposition 125) donne

$$\begin{aligned}
\chi_\pi(a(-1)^{\frac{p-1}{4}}) &= \chi_{a(-1)^{\frac{p-1}{4}}}(\pi) \\
&= \chi_a(\pi) \qquad (a \text{ et } a(-1)^{\frac{p-1}{4}} \text{ sont associés }) \\
&= \chi_a(a + bi) \\
&= \chi_a(bi) \\
&= \chi_a(b)\chi_a(i).
\end{aligned}$$

Comme $a \wedge b = 1$ (puisque $p = a^2 + b^2$), $\chi_a(b) = 1$ (proposition 113), et la proposition 128 donne $\chi_a(i) = (-1)^{\frac{a^2-1}{8}}$. Ainsi

$$\chi_\pi(a(-1)^{\frac{p-1}{4}}) = (-1)^{\frac{a^2-1}{8}}.$$

□

Proposition 134. *Soit $\pi = a + bi$ un premier primaire de $\mathbb{Z}[i]$, tel que $\mathrm{N}(\pi) = p \equiv 1 \pmod 4$, où p est un premier rationnel. Alors*

(a) Si $\pi \equiv 1 \pmod 4$, alors $\chi_\pi(a) = i^{\frac{a-1}{2}}$.

(b) Si $\pi \equiv 3 + 2i \pmod 4$, alors $\chi_\pi(a) = -i^{\frac{-a-1}{2}}$.

Démonstration. Comme $p = \mathrm{N}(\pi) = a^2 + b^2$, ici $a \wedge b = 1$. La proposition 133 donne

$$\chi_\pi(a(-1)^{\frac{p-1}{4}}) = (-1)^{\frac{a^2-1}{8}}.$$

Comme $\chi_\pi(-1) = (-1)^{(a-1)/2}$ (proposition 112),

$$\chi_\pi(a) = (-1)^{\frac{a-1}{2}\frac{p-1}{4}}(-1)^{\frac{a^2-1}{8}},$$

où $p = \mathrm{N}(\pi) = a^2 + b^2$.

(a) Supposons que $\pi \equiv 1 \pmod 4$. Ici $a \equiv 1 \pmod 4, b \equiv 0 \pmod 4$, soit $a = 4A + 1, b = 4B,\ A, B \in \mathbb{Z}$. Alors

$$(-1)^{\frac{p-1}{4}} = (-1)^{\frac{a^2-1}{4}+\frac{b^2}{4}} = (-1)^{4A^2+2A+4B^2} = 1,$$

et ainsi $(-1)^{\frac{a-1}{2}\frac{p-1}{4}} = 1$.

$$\chi_\pi(a) = (-1)^{\frac{a^2-1}{8}} = (-1)^{2A^2+A} = (-1)^A = (-1)^{\frac{a-1}{4}} = i^{\frac{a-1}{2}}.$$

Conclusion : si $\pi \equiv 1 \pmod 4$, $\chi_\pi(a) = i^{\frac{a-1}{2}}$.

(b) Supposons maintenant que $\pi \equiv 3+2i \pmod 4$.
Alors $a \equiv 3 \pmod 4, b \equiv 2 \pmod 4, a = 4A+3, b = 4B+2,\ A, B \in \mathbb{Z}$.
Comme dans la partie (a),

$$\chi_\pi(a) = (-1)^{\frac{a-1}{2}\frac{p-1}{4}}(-1)^{\frac{a^2-1}{8}},$$

où

$$p - 1 = a^2 + b^2 - 1 = 16A^2 + 24A + 16B^2 + 16B + 12 \equiv 4 \pmod 8,$$

si bien que $\frac{p-1}{4} \equiv 1 \pmod 2$, et ainsi $(-1)^{\frac{p-1}{4}} = -1$.

$$(-1)^{\frac{a-1}{2}\frac{p-1}{4}} = (-1)^{\frac{a-1}{2}} = (-1)^{2A+1} = -1,$$

$$\frac{a^2-1}{8} = 2A^2 + 3A + 1,$$

$$(-1)^{\frac{a^2-1}{8}} = (-1)^{3A+1} = (-1)^{A+1} = (-1)^{\frac{a+1}{4}}.$$

Par conséquent,

$$\chi_\pi(a) = -(-1)^{\frac{a+1}{4}} = -i^{\frac{a+1}{2}}.$$

De plus,

$$\frac{a+1}{2} \equiv \frac{-a-1}{2}\ [4] \iff a+1 \equiv -a-1\ [8] \iff 2a \equiv -2\ [8] \iff a \equiv 3\ [4],$$

par conséquent $i^{\frac{a+1}{2}} = i^{\frac{-a-1}{2}}$.
Conclusion : si $\pi \equiv 3+2i \pmod 4$, $\chi_\pi(a) = -i^{\frac{-a-1}{2}}$.

□

Proposition 135. *Soit $\pi = a + bi$ un premier primaire de $\mathbb{Z}[i]$, tel que $\mathrm{N}(\pi) = p \equiv 1 \pmod 4$, où p est un premier rationnel. Alors*

$$\chi_\pi(a)\chi_\pi(1+i) = i^{\frac{3(a+b-1)}{4}}.$$

Démonstration. Soit $\pi = a+bi$ un premier primaire. Comme $a(1+i) = a+b+i(a+bi)$, $a(1+i) \equiv a+b \mod \pi$, si bien que

$$\chi_\pi(a)\chi_\pi(1+i) = \chi_\pi(a+b).$$

Puisque $\pi = a+bi$ est primaire, $a+b \equiv 1 \pmod 4$.
Si $a+b=1$, alors $\chi_\pi(a)\chi_\pi(1+i) = \chi_\pi(a+b) = 1 = i^{3(a+b-1)/4}$.
Sinon, la loi de réciprocité biquadratique (proposition 125) donne

$$\chi_\pi(a+b) = \chi_{a+b}(\pi).$$

De plus, $b \equiv -a \pmod{a+b}$, donc $\pi = a+bi \equiv a(1-i) \equiv -ia(1+i) \pmod{a+b}$.
Par conséquent,

$$\chi_{a+b}(\pi) = \chi_{a+b}(-1)\chi_{a+b}(i)\chi_{a+b}(a)\chi_{a+b}(1+i).$$

Comme $a+b \equiv 1 \pmod 4$ est primaire, la proposition 112 donne $\chi_{a+b}(-1) = (-1)^{\frac{a+b-1}{2}} = 1$, et la proposition 114 donne $\chi_{a+b}(i) = (-1)^{\frac{a+b-1}{4}}$.

De plus $a \wedge b = 1$, puisque $p = a^2 + b^2$. Donc $(a+b) \wedge a = 1$, et par conséquent $\chi_{a+b}(a) = 1$ (proposition 113).

La proposition 131 donne $\chi_{a+b}(1+i) = i^{\frac{a+b-1}{4}}$, si bien que

$$\begin{aligned}\chi_{a+b}(\pi) &= \chi_{a+b}(-1)\chi_{a+b}(i)\chi_{a+b}(a)\chi_{a+b}(1+i)\\ &= (-1)^{\frac{a+b-1}{4}} i^{\frac{a+b-1}{4}}\\ &= i^{\frac{a+b-1}{2}} i^{\frac{a+b-1}{4}}\\ &= i^{\frac{3(a+b-1)}{4}}.\end{aligned}$$

Dans tous les cas,

$$\chi_\pi(a)\chi_\pi(1+i) = i^{\frac{3(a+b-1)}{4}}.$$

□

Nous pouvons maintenant donner le caractère biquadratique de $1+i$.

Proposition 136. Supplément à la loi de réciprocité biquadratique.
Si $\pi = a + bi$ est un premier primaire de $\mathbb{Z}[i]$, alors

(a) $\chi_\pi(i) = i^{\frac{-a+1}{2}}$.

(b) $\chi_\pi(1+i) = i^{\frac{a-b-b^2-1}{4}}$.

Démonstration. Soit $\pi = a + ib$ un premier primaire de $\mathbb{Z}[i]$. La partie (a) est l'objet de la proposition 127. Passons à la partie (b).

- Si $b = 0$, alors $\pi = a \in \mathbb{Z}$. Comme π est primaire, $\pi = -q, q \equiv 3 \pmod 4$, où q est un premier rationnel positif, donc $a = -q, b = 0$.
  La proposition 129 donne alors,

  $$\chi_\pi(1+i) = \chi_{-q}(1+i) = i^{\frac{-q-1}{4}} = i^{\frac{a-b-b^2-1}{4}}.$$

  Si $b \neq 0$, alors π n'est pas associé à un premier rationnel $q \equiv 3 \pmod 4$ (puisque le seul associé primaire de q est $-q$). La classification des premiers de $\mathbb{Z}[i]$ montre que π vérifie $\mathrm{N}(\pi) = p$, où $p \equiv 1 \pmod 4$ est un premier rationnel. La proposition 135 donne alors

  $$\chi_\pi(a)\chi_\pi(1+i) = i^{\frac{3(a+b-1)}{4}}.$$

- Si $\pi \equiv 1 \pmod 4$, alors $a \equiv 1 \pmod 4, b \equiv 0 \pmod 4$, donc

  $$a = 4A + 1, b = 4B,\ A, B \in \mathbb{Z}.$$

  En appliquant la proposition 134(a),

  $$\chi_\pi(a) = i^{\frac{a-1}{2}}, \qquad \chi_\pi(a)^{-1} = (-i)^{\frac{a-1}{2}} = i^{\frac{a-1}{2}}.$$

  Par conséquent,

  $$\begin{aligned}\chi_\pi(1+i) &= i^{3\frac{a+b-1}{4} - 2\frac{a-1}{4}}\\ &= i^{\frac{a+3b-1}{4}}\\ &= i^{\frac{a-b-b^2-1}{4}},\end{aligned}$$

puisque $\left(\frac{a+3b-1}{4}\right) - \left(\frac{a-b-b^2-1}{4}\right) = b + \frac{b^2}{4} = 4B + 4B^2 \equiv 0 \pmod 4$.

- Si $\pi \equiv 3 + 2i \pmod 4$, alors $a \equiv 3 \pmod 4, b \equiv 2 \pmod 4$, soit

$$a = 4A - 1, b = 4B + 2,\ A, B \in \mathbb{Z}.$$

Dans ce cas, la proposition 134(b) donne

$$\chi_\pi(a) = -i^{\frac{-a-1}{2}}, \qquad \chi_\pi(a)^{-1} = -i^{\frac{a+1}{2}} = i^{\frac{a-3}{2}},$$

donc

$$\chi_\pi(1+i) = i^{\frac{3a+3b-3+2a-6}{4}} = i^{\frac{5a+3b-9}{4}}.$$

De plus,

$$\begin{aligned}\frac{1}{4}[(a-b-b^2-1)-(5a+3b-9)] &= \frac{1}{4}(-4a-4b-b^2+8)\\ &= -a-b+2-\frac{b^2}{4}\\ &= -4A+1-4B-2+2-(2B+1)^2\\ &\equiv 0 \pmod 4,\end{aligned}$$

donc $\chi_\pi(1+i) = i^{\frac{a-b-b^2-1}{4}}$.

Dans tous les cas

$$\chi_\pi(1+i) = i^{\frac{a-b-b^2-1}{4}}.$$

□

4.8 Caractère biquadratique de 2.

Proposition 137. *Si $\pi = a + bi$ est un premier primaire de $\mathbb{Z}[i]$, alors*

$$\chi_\pi(2) = i^{\frac{ab}{2}}.$$

Démonstration. Puisque $2 = i^3(1+i)^2$, le supplément à la loi de réciprocité biquadratique (proposition 136) donne

$$\begin{aligned}\chi_\pi(2) &= \chi_\pi(i)^3\chi_\pi(1+i)^2\\ &= i^{\frac{3(-a+1)}{2}} i^{\frac{a-b-b^2-1}{2}}\\ &= i^{1-a-(b+1)\frac{b}{2}}\end{aligned}$$

Comme π est primaire, $a \equiv b+1 \equiv -b+1 \pmod 4$, donc

$$\begin{aligned}1-a-(b+1)\frac{b}{2} &\equiv -b-(b+1)\frac{b}{2}\\ &\equiv \frac{b}{2}(-b-3)\\ &\equiv \frac{b}{2}(-b+1)\\ &\equiv \frac{ab}{2} \pmod 4,\end{aligned}$$

donc $\chi_\pi(2) = i^{\frac{ab}{2}}$. □

Notons que, puisque a est impair, $i^a = \pm i$, donc $\chi_\pi(2) = (\pm i)^{\frac{b}{2}}$, si bien que $\chi_\pi(2) = 1$ équivaut à $8 \mid b$. Ceci donne l'idée de la proposition suivante.

Proposition 138. *Si p est un nombre premier, p se décompose sous la forme $p = A^2 + 64B^2$ si et seulement si $p \equiv 1 \pmod 4$ et si la congruence $x^4 \equiv 2 \pmod p$ admet une solution dans $\mathbb{Z}$.*

$$\exists (A, B) \in \mathbb{Z}^2,\ p = A^2 + 64B^2 \iff (p \equiv 1 \pmod 4 \text{ et } \exists x \in \mathbb{Z},\ x^4 \equiv 2 \pmod p).$$

Démonstration. ($\Rightarrow$) Si $p = A^2 + 64b^2 = A^2 + (8B)^2$, alors le nombre premier p est somme de deux carrés, et $p \neq 2$, donc $p \equiv 1 \pmod 4$. Comme $p = A^2 + 64b^2$, A est impair. Posons $b = 8B$. Si $A \equiv 1 \pmod 4$, posons $a = A$, et si $A \equiv -1 \pmod 4$, posons $a = -A$. Alors $\pi = a + bi$ vérifie $\mathrm{N}(\pi) = a^2 + b^2 = p$, et $a \equiv 1 \pmod 4, b \equiv 0 \pmod 4$, donc π est un premier primaire.

Le caractère biquadratique de 2 (proposition 137) donne

$$\chi_\pi(2) = i^{\frac{ab}{2}} = i^{4aB} = 1.$$

Par conséquent, il existe $x \in \mathbb{Z}$ tel que $x^4 \equiv 2 \pmod p$ (proposition 125).

($\Leftarrow$) Réciproquement, supposons que $p \equiv 1 \pmod 4$ et que 2 est un résidu biquadratique modulo p. Comme $p \equiv 1 \pmod 4$, p se décompose sous la forme $p = \pi\overline{\pi}$, où π est un premier primaire. Puisque $2 \equiv x^4 \pmod p$, alors $2 \equiv x^4 \pmod \pi$, et donc $\chi_\pi(2) = 1$. La proposition 137 montre que

$$1 = \chi_\pi(2) = i^{\frac{ab}{2}}.$$

Puisque a est impair, ceci montre que b est un multiple de 8, donc $p = A^2 + 64B^2$, où $A = a, B = b/8$. □