ANNALES DE L'INSTITUT FOURIER

ABDELMEJID BAYAD

Loi de réciprocité quadratique dans les corps quadratiques imaginaires

Annales de l'institut Fourier, tome 45, n° 5 (1995), p. 1223-1237

<http://www.numdam.org/item?id=AIF_1995__45_5_1223_0>

Ann. Inst. Fourier, Grenoble
45, 5 (1995), 1223–1237

LOI DE RÉCIPROCITÉ QUADRATIQUE DANS LES CORPS QUADRATIQUES IMAGINAIRES

par Abdelmejid BAYAD

0. Introduction.

Soit p un nombre premier $\neq 2$, et soit S une partie de $\mathbb{F}_p^*$ telle que $\mathbb{F}_p^*$ soit réunion disjointe de S et $-S$. Si $s \in S$ et $a \in \mathbb{F}_p^*$, on a alors

$$as = \varepsilon(a, s)s_a, \quad \text{avec} \quad \varepsilon(a, s) = \pm 1 \quad \text{et} \quad s_a \in S.$$

Le symbole de Legendre $\left(\frac{a}{p}\right)$ est défini comme suit :

$$\left(\frac{a}{p}\right) = \prod_{s \in S} \varepsilon(a, s), \tag{0.1}$$

c'est le lemme de Gauss qui donne cela (*cf.* [7], chap. 1, Appendice). Alors pour tout q premier $\neq 2$ et de p, on a

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}, \tag{0.2}$$

c'est la loi de réciprocité quadratique dans $\mathbb{Q}$, due à Gauss.

Dans ce travail, on part d'une courbe elliptique définie sur un corps quadratique imaginaire et à multiplication complexe par l'anneau des entiers de ce corps et on construit des fonctions elliptiques.

D'autre part, on fait apparaître des formules produits relatives à ces fonctions elliptiques et obtenues grâce à l'arithmétique sur cette courbe.

Mots-clés : Loi de réciprocité quadratique – Formule produit – Courbe elliptique – Multiplication complexe.
Classification math. : 11R04 – 14H52 – 11G15 – 14K22.

Il est à noter que nos formules produits sont à rapprocher de celles obtenues par D.S. Kubert [3], §4 pour la fonction elliptique $\wp$ de Weierstrass utilisée pour montrer la loi de réciprocité cubique d'Eisenstein dans $\mathbb{Q}(\sqrt{-3})$. En outre, dans le cadre des corps quadratiques imaginaires, nos formules produits jouent le même rôle que la formule de multiplication de la fonction sinus, suivante :

$$\sin(mx) = (-1)^{\frac{m-1}{2}} 2^{m-1} \sin(x) \prod_{s\in S} \sin\Big(x + \frac{2\pi s}{m}\Big) \sin\Big(x - \frac{2\pi s}{m}\Big)$$

pour démontrer (0.2).

En conséquence, cet article généralise la loi de réciprocité quadratique de Gauss pour les corps quadratiques imaginaires.

Enfin, ce travail se compose de trois parties. Dans la première partie, on développe notre théorie ci-dessus où le corps quadratique imaginaire est de discriminant différent de -4 et -3, dans la deuxième partie on traite le cas particulier où le corps est $\mathbb{Q}(\sqrt{-1})$. Dans la troisième partie, on traite le cas où le corps quadratique imaginaire est $\mathbb{Q}(\sqrt{-3})$.

Nos principaux résultats sont les théorèmes 1.10, 2.9 et 3.7.

Remerciements.

Je tiens à remercier les membres de l'Institut Fourier qui m'ont permis de réaliser ce travail dans de bonnes conditions; mes remerciements vont tout particulièrement à l'équipe de théorie des nombres et au Professeur Gilles Robert qui a corrigé la version préliminaire de cet article.

1. Loi de réciprocité quadratique dans un corps quadratique imaginaire K différent de $\mathbb{Q}(i)$ et $\mathbb{Q}(j)$.

On note par $\mathbb{Z}\omega_1+\mathbb{Z}\omega_2$ l'anneau des entiers de K, avec $\mathrm{Im}(\omega_2/\omega_1)>0$. Nous associons à $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ la fonction $\wp$ de Weierstrass donnée par :

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\mathbb{Z}\omega_1+\mathbb{Z}\omega_2\\ \omega\neq 0}} \Big[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big]. \tag{1.1}$$

Nous définissons aussi les séries $g_2(\mathbb{Z}\omega_1+\mathbb{Z}\omega_2)$ et $g_3(\mathbb{Z}\omega_1+\mathbb{Z}\omega_3)$ d'Eisenstein par

$$g_2 := g_2(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) = 60 \sum_{\substack{\omega\in\mathbb{Z}\omega_1+\mathbb{Z}\omega_2\\ \omega\neq 0}} \frac{1}{\omega^4}$$

et

$$g_3 := g_3(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) = 140 \sum_{\substack{\omega \in \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \\ \omega \neq 0}} \frac{1}{\omega^6}.$$

D'après (*cf.* [4], chap. 1, §2, th. 5), on a

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

donc le point $\big(\wp(z), \wp'(z)\big)$ appartient à la courbe d'équation

$$Y^2 = 4X^3 - g_2X - g_3, \tag{1.2}$$

son discriminant est $\Delta = g_2^3 - 27g_3^2$.

LEMME 1.3. — *La courbe E définie par :*

$$E : Y^2 = 4X^3 - g_2X - g_3$$

est une courbe elliptique sur une extension algébrique L/K de degré au plus égal à 6.

Preuve. — Tout d'abord, remarquons que les deux fonctions elliptiques suivantes ont le même diviseur :

$$z \longmapsto \wp'(z)^2$$

et

$$z \longmapsto \Big(\wp(z) - \wp\Big(\frac{\omega_1}{2}\Big)\Big)\Big(\wp(z) - \wp\Big(\frac{\omega_2}{2}\Big)\Big)\Big(\wp(z) - \wp\Big(\frac{\omega_1+\omega_2}{2}\Big)\Big).$$

En effet,

$$\begin{aligned} \wp'\Big(-\frac{\omega_1}{2}\Big) &= -\wp'\Big(\frac{\omega_1}{2}\Big) \\ \wp'\Big(-\frac{\omega_2}{2}\Big) &= -\wp'\Big(\frac{\omega_2}{2}\Big) \\ \wp'\Big(-\frac{\omega_1+\omega_2}{2}\Big) &= -\wp'\Big(\frac{\omega_1+\omega_2}{2}\Big) \end{aligned} \tag{1.4}$$

car la fonction $z \longmapsto \wp'(z)$ est impaire.

D'autre part, grâce à la périodicité de $z \longmapsto \wp'(z)$ on a alors

$$\begin{aligned} \wp'\Big(-\frac{\omega_1}{2}\Big) &= -\wp'\Big(\frac{\omega_1}{2} + \omega_1\Big) = \wp'\Big(\frac{\omega_1}{2}\Big) \\ \wp'\Big(-\frac{\omega_2}{2}\Big) &= -\wp'\Big(\frac{\omega_2}{2} + \omega_2\Big) = \wp'\Big(\frac{\omega_2}{2}\Big) \end{aligned} \tag{1.5}$$

et

$$\wp'\Big(-\frac{\omega_1+\omega_2}{2}\Big) = -\wp'\Big(\frac{\omega_1+\omega_2}{2} + \omega_1 + \omega_2\Big) = \wp'\Big(\frac{\omega_1+\omega_2}{2}\Big)$$

d'où (1.4) et (1.5) impliquent

$$\wp'\Big(\frac{\omega_1}{2}\Big) = \wp'\Big(\frac{\omega_2}{2}\Big) = \wp'\Big(\frac{\omega_1+\omega_2}{2}\Big) = 0,$$

donc

$$(\wp'^2) = 2\Big(\frac{\omega_1}{2}\Big) + 2\Big(\frac{\omega_2}{2}\Big) + 2\Big(\frac{\omega_1+\omega_2}{2}\Big) - 6(0) \tag{1.6}$$

et l'expression (1.6) n'est rien d'autre que le diviseur de la fonction

$$z \longmapsto \Big(\wp(z) - \wp\Big(\frac{\omega_1}{2}\Big)\Big)\Big(\wp(z) - \wp\Big(\frac{\omega_2}{2}\Big)\Big)\Big(\wp(z) - \wp\Big(\frac{\omega_1+\omega_2}{2}\Big)\Big).$$

Donc ces deux fonctions elliptiques ne diffèrent que d'une constante multiplicative. Cette constante n'est rien d'autre que 4. En effet, cela se déduit des égalités suivantes :

$$\lim_{z\to 0} z^2\wp(z) = 1 \quad \text{et} \quad \lim_{z\to 0} z^3\wp'(z) = -2.$$

Ainsi

$$\wp'(z)^2 = 4\Big(\wp(z) - \wp\Big(\frac{\omega_1}{2}\Big)\Big)\Big(\wp(z) - \wp\Big(\frac{\omega_2}{2}\Big)\Big)\Big(\wp(z) - \wp\Big(\frac{\omega_1+\omega_2}{2}\Big)\Big);$$

comme la valence de $z \longmapsto \wp'(z)$ est 3 (resp. $z \longmapsto \wp(z)$ est 2), alors $\wp\Big(\frac{\omega_1}{2}\Big)$, $\wp\Big(\frac{\omega_2}{2}\Big)$ et $\wp\Big(\frac{\omega_1+\omega_2}{2}\Big)$ sont distincts. Par suite, les racines de $4X^3 - g_2X - g_3$ sont distinctes, ce qui implique que $\Delta = g_2^3 - 27g_3^2 \neq 0$. Alors, la courbe E est une courbe elliptique.

En outre,

$$E : Y^2 = 4\Big(X - \wp\Big(\frac{\omega_1}{2}\Big)\Big)\Big(X - \wp\Big(\frac{\omega_2}{2}\Big)\Big)\Big(X - \wp\Big(\frac{\omega_1+\omega_2}{2}\Big)\Big)$$

de ce fait, on déduit que E est définie sur $K\Big(\wp\Big(\frac{\omega_1}{2}\Big), \wp\Big(\frac{\omega_2}{2}\Big), \wp\Big(\frac{\omega_1+\omega_2}{2}\Big)\Big)$ et d'après la théorie de la multiplication complexe cette extension a un degré au plus égal à 6.

On définit, maintenant, la fonction elliptique f associée au réseau $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ par

$$f(z) = \sqrt{\frac{12\wp(\frac{\omega_2}{2})^2 - g_2}{\wp(\frac{\omega_2}{2}) - \wp(\frac{\omega_1+\omega_2}{2})}}\ \frac{\wp(z) - \wp(\frac{\omega_1+\omega_2}{2})}{\wp'(z)}; \tag{1.7}$$

on a alors le résultat suivant :

THÉORÈME 1.8 (Formule produit).

1) $f(z)f\Big(z + \frac{\omega_1}{2}\Big) = 1.$

2) *On a la formule produit, pour* $v \in \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $(v, 2) = 1$:

$$f(vz) = \xi_v f(z) \prod_{\substack{\alpha\in \mathrm{Ker}\, v\\ \alpha\neq 0}} f(z+\alpha)$$

où $\xi_v = \pm 1$ *et* $\xi_v = v \prod_{\substack{\alpha \in \mathrm{Ker}\, v \\ \alpha \neq 0}} f\Big(\alpha + \dfrac{\omega_1}{2}\Big)$.

Démonstration. — Pour démontrer 1) il suffit de remarquer que la fonction $z \mapsto f(z) f\Big(z + \dfrac{\omega_1}{2}\Big)$ est elliptique pour $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ et dont le diviseur est nul, donc c'est une constante et pour finir on détermine cette constante :

$$\begin{aligned}
&\lim_{z \mapsto \frac{\omega_1+\omega_2}{2}} f(z) f\Big(z + \frac{\omega_1}{2}\Big) \\
&= \frac{12\wp\big(\frac{\omega_2}{2}\big)^2 - g_2}{\wp\big(\frac{\omega_2}{2}\big) - \wp\big(\frac{\omega_1+\omega_2}{2}\big)} \cdot \lim_{z \mapsto \frac{\omega_1+\omega_2}{2}} \frac{\Big(\wp(z) - \wp\big(\frac{\omega_1+\omega_2}{2}\big)\Big)\Big(\wp\big(z+\frac{\omega_1}{2}\big) - \wp\big(\frac{\omega_1+\omega_2}{2}\big)\Big)}{\wp'(z)\wp'\big(z+\frac{\omega_1}{2}\big)} \\
&= \frac{12\wp\big(\frac{\omega_2}{2}\big)^2 - g_2}{\wp\big(\frac{\omega_2}{2}\big) - \wp\big(\frac{\omega_1+\omega_2}{2}\big)} \cdot \frac{\frac{1}{2}\wp''\big(\frac{\omega_1+\omega_2}{2}\big)\Big(\wp\big(\frac{\omega_1}{2}\big) - \wp\big(\frac{\omega_1+\omega_2}{2}\big)\Big)}{\wp''\big(\frac{\omega_1+\omega_2}{2}\big)\wp''\big(\frac{\omega_2}{2}\big)} \\
&= \frac{\frac{1}{2}\wp\big(\frac{\omega_2}{2}\big)^2 - g_2}{\wp''\big(\frac{\omega_2}{2}\big)}, \text{ d'après l'équation de la courbe } E \\
&= 1.
\end{aligned}$$

Montrons le 2) du théorème 1.8.

D'une part, on remarque que les deux fonctions $z \mapsto f(vz)$ et $z \mapsto f(z) \prod_{\substack{\alpha \in \mathrm{Ker}\, v \\ \alpha \neq 0}} f(z+\alpha)$ sont elliptiques pour $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ et ont le même diviseur, donc elles diffèrent d'une constante ξ_v. D'autre part, comme $(v, 2) = 1$, il existe $X(v)$, $Y(v)$ éléments de $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ tels que :

$$X(v) \cdot v + 2Y(v) = 1.$$

Ceci implique

$$f\Big(vz + \frac{\omega_1}{2}\Big) = f\Big(v\Big(z + X(v)\frac{\omega_1}{2}\Big)\Big)$$

donc

$$f(v \cdot z) f\Big(v\Big(z + X(v)\frac{\omega_1}{2}\Big)\Big) = 1, \quad \text{d'après le 1) ci-dessus.}$$

Alors

$$\begin{aligned}
1 &= f(v \cdot z) f\Big(v\Big(z + X(v)\frac{\omega_1}{2}\Big)\Big) \\
&= \xi_v^2 f(z) f\Big(z + X(v)\frac{\omega_1}{2}\Big) \prod_{\substack{\alpha \in \mathrm{Ker}\, v \\ \alpha \neq 0}} f(z+\alpha) f\Big(z + X(v)\frac{\omega_1}{2}\Big)
\end{aligned}$$

et comme $\big(X(v),2\big)=1$ et f est elliptique pour $\mathbb{Z}\omega_1+\mathbb{Z}\omega_2$, on obtient

$$1=\xi_v^2 f(z) f\Big(z+\frac{\omega_1}{2}\Big)\prod_{\substack{\alpha\in\mathrm{Ker}\,v\\ \alpha\neq 0}} f(z+\alpha) f\Big(z+\alpha+\frac{\omega_1}{2}\Big);$$

d'après le 1) du théorème 1.8, on a alors :

$$\xi_v^2=1.$$

On sait même plus

$$\xi_v=\lim_{z\mapsto 0}\frac{f(vz)}{f(z)\prod\limits_{\substack{\alpha\in\mathrm{Ker}\,v\\ \alpha\neq 0}} f(z+\alpha)}$$

ce qui donne

$$\xi_v=\frac{v}{\prod\limits_{\substack{\alpha\in\mathrm{Ker}\,v\\ \alpha\neq 0}} f(\alpha)}$$

et d'après le 1) du théorème 1.8, on obtient

$$\xi_v=v\prod_{\substack{\alpha\in\mathrm{Ker}\,v\\ \alpha\neq 0}} f\Big(\alpha+\frac{\omega_1}{2}\Big).$$

Ce qui termine la preuve du théorème 1.8.

DÉFINITION 1.9. — *Pour $\alpha,\beta\in\mathbb{Z}\omega_1+\mathbb{Z}\omega_2$, avec $(\alpha,2)=(\beta,2)=(\alpha,\beta)=1$, on définit le symbole quadratique $\Big(\dfrac{\alpha}{\beta}\Big)_2$ par*

$$\Big(\frac{\alpha}{\beta}\Big)_2=\prod_{\sigma\in S_\beta}\varepsilon(\alpha,\sigma),$$

où $\alpha\sigma=\varepsilon(\alpha,\sigma)\gamma(\sigma)$ avec $\varepsilon(\alpha,\sigma)\in\{-1,1\}$, $\gamma(\sigma)\in S_\beta$ et $\{S_\beta,-S_\beta\}$ est un système complet de représentants de $(\mathbb{Z}\omega_1+\mathbb{Z}\omega_2)/\beta(\mathbb{Z}\omega_1+\mathbb{Z}\omega_2)$.

On peut alors énoncer notre premier résultat principal :

THÉORÈME 1.10 (Loi de réciprocité quadratique dans K). — *Soient $\alpha,\beta\in\mathbb{Z}\omega_1+\mathbb{Z}\omega_2$, avec $(\alpha,2)=(\beta,2)=(\alpha,\beta)=1$. On a alors*

$$\Big(\frac{\alpha}{\beta}\Big)_2\Big(\frac{\beta}{\alpha}\Big)_2^{-1}=\xi_\alpha^{\frac{N(\beta)-1}{2}}\xi_\beta^{\frac{N(\alpha)-1}{2}}(-1)^{\frac{N(\alpha)-1}{2}\cdot\frac{N(\beta)-1}{2}}$$

où ξ_α, $\xi_\beta\in\{1,-1\}$ tels que :

$$\xi_\alpha=\alpha\prod_{\substack{\gamma\in\mathrm{Ker}\,\alpha\\ \gamma\neq 0}} f\Big(\gamma+\frac{\omega_1}{2}\Big)\ \text{ et }\ \xi_\beta=\beta\prod_{\substack{\gamma\in\mathrm{Ker}\,\beta\\ \gamma\neq 0}} f\Big(\gamma+\frac{\omega_1}{2}\Big).$$

Démonstration. — En fait, on peut écrire

$$\varepsilon(\alpha,\sigma)=\frac{\alpha\sigma}{\gamma(\sigma)}=\frac{f(\alpha\sigma)}{f(\gamma(\sigma))}$$

car f est impaire. Donc

$$\left(\frac{\alpha}{\beta}\right)_2=\prod_{\sigma\in S_\beta}\frac{f(\alpha\sigma)}{f(\gamma(\sigma))}=\prod_{\sigma\in S_\beta}\frac{f(\alpha\sigma)}{f(\sigma)}$$

et du théorème 1.8, on déduit que

$$\left(\frac{\alpha}{\beta}\right)_2=\xi_\alpha^{\frac{N(\beta)-1}{2}}\prod_{\sigma\in S_\beta}\prod_{\sigma'\in S_\alpha}f(\sigma+\sigma')f(\sigma-\sigma')$$

et

$$\left(\frac{\beta}{\alpha}\right)_2=\xi_\beta^{\frac{N(\alpha)-1}{2}}\prod_{\sigma\in S_\alpha}\prod_{\sigma'\in S_\beta}f(\sigma+\sigma')f(\sigma-\sigma').$$

Par suite, on obtient

$$\left(\frac{\alpha}{\beta}\right)_2\left(\frac{\beta}{\alpha}\right)_2^{-1}=\xi_\alpha^{\frac{N(\beta)-1}{2}}\xi_\beta^{\frac{N(\alpha)-1}{2}}(-1)^{\frac{N(\alpha)-1}{2}\cdot\frac{N(\beta)-1}{2}}$$

où ξ_α et ξ_β sont donnés par le théorème 1.8. Ce qui montre le théorème 1.10.

2. Loi de réciprocité quadratique dans $\mathbb{Q}(\sqrt{-1})$.

L'anneau des entiers de $\mathbb{Q}(\sqrt{-1})$ est l'anneau $\mathbb{Z}[\sqrt{-1}]$. On considère la courbe elliptique E définie sur $\mathbb{Q}(\sqrt{-1})$ par le modèle de Weierstrass

$$E : Y^2 = 4(X^3 - X). \tag{2.1}$$

Cette courbe a multiplication complexe par $\mathbb{Z}[\sqrt{-1}]$, alors E comme variété complexe est isomorphe à $\mathbb{C}/\mathbb{Z}[\sqrt{-1}]$ et cet isomorphisme est donné par :

$$\begin{array}{rcll} \mathbb{C}/\mathbb{Z}[\sqrt{-1}] & \longrightarrow & E(\mathbb{C}) & \\ z & \longmapsto & \big(\wp(z),\wp'(z)\big) & \text{si } z\notin\mathbb{Z}[\sqrt{-1}] \\ z & \longmapsto & 0 & \text{si } z\in\mathbb{Z}[\sqrt{-1}] \end{array} \tag{2.2}$$

où $\wp$ est la fonction de Weierstrass pour le réseau $\mathbb{Z}[\sqrt{-1}]$. Le point M de coordonnées $\big(\wp(z),\wp'(z)\big)$ est dit de paramètre z. D'autre part, la fonction $\wp$ de Weierstrass associée au réseau $\mathbb{Z}[\sqrt{-1}]$ vérifie :

(2.3)

$$\wp(iz)=-\wp(z)\ \text{ et son diviseur est }\ (\wp)=2\Big(\frac{1+i}{2}\Big)-2(0)$$

$$\wp'(iz)=i\wp'(z)\ \text{ et son diviseur est }\ (\wp')=\Big(\frac{1}{2}\Big)+\Big(\frac{i}{2}\Big)+\Big(\frac{i+1}{2}\Big)-3(0).$$

On considère maintenant la fonction elliptique pour le réseau $\mathbb{Z}[\sqrt{-1}]$ définie par

$$f(z) = \frac{\wp(z)\wp'\left(\frac{1+i}{4}\right)}{\wp\left(\frac{1+i}{4}\right)\wp'(z)}. \tag{2.4}$$

On a alors le résultat :

THÉORÈME 2.5 (Formule produit).

1) $f(iz) = if(z)$ *et* $f(z)f\left(z - \frac{1}{2}\right) = i.$

2) *Soit* $v \in \mathbb{Z}[\sqrt{-1}]$, $(v, 2) = 1$, *on a alors la formule produit*

$$f(vz) = \xi_v f(z) \prod_{\substack{\alpha \in \operatorname{Ker} v \\ \alpha \neq 0}} f(z+\alpha)$$

où ξ_v *est la racine* $4^{\text{ème}}$ *de l'unité telle que :* $\xi_v \equiv v \bmod \mathfrak{p}_2^3$ *et où* $\mathfrak{p}_2^2 = 2\mathbb{Z}[\sqrt{-1}]$ *et* Ker v *est le noyau de l'endomorphisme de* E *qui à* $z \mapsto vz$.

Démonstration. — D'après (2.3) et (2.4), il est clair que : $f(iz) = if(z)$. Soit maintenant, la fonction $z \mapsto f(z) \cdot f\left(z - \frac{1}{2}\right)$ qui est elliptique pour le réseau $\mathbb{Z}[\sqrt{-1}]$. D'autre part, son diviseur est donné par

$$\begin{aligned}(f) + \left(f(\cdot - \tfrac{1}{2})\right) &= (0) + \left(\tfrac{1+i}{2}\right) - \left(\tfrac{1}{2}\right) - \left(\tfrac{i}{2}\right) + \left(\tfrac{-1}{2}\right) + \left(\tfrac{i}{2}\right) - (0) - \left(\tfrac{-1+i}{2}\right) \\ &= 0\end{aligned}$$

donc, d'après la théorie des fonctions elliptiques, la fonction qui à $z \mapsto f(z)f\left(z - \frac{1}{2}\right)$ est une constante. En outre, pour $z = \frac{1+i}{4}$ on a

$$f\left(\frac{1+i}{4}\right) \cdot f\left(\frac{1+i}{4} - \frac{1}{2}\right) = 1 \times f\left(\frac{i-1}{4}\right) = f\left(i \cdot \frac{1+i}{4}\right).$$

Ceci est égal à $if\left(\frac{1+i}{4}\right) = i$. D'où $f(z)f\left(z - \frac{1}{2}\right) = i$.

Montrons le 2) du théorème 2.5.

On compare les diviseurs des fonctions elliptiques se trouvant de chaque côté de l'égalité 2) du théorème 2.5, on remarque que $z \mapsto f(vz)$ et $z \mapsto f(z) \prod_{\substack{\alpha \in \operatorname{Ker} v \\ \alpha \neq 0}} f(z+\alpha)$ ont le même diviseur.

Plus important, le 1) du théorème 2.5 implique que

$$\begin{aligned} f\left(\frac{i+1}{4} + \alpha\right) f\left(\frac{i+1}{4} - i\alpha\right) &= -i \cdot f\left(\frac{i+1}{4} + \alpha\right) f\left(i \cdot \frac{1+i}{4} + \alpha\right) \\ &= -i \cdot f\left(\frac{i+1}{4} + \alpha\right) f\left(\frac{1+i}{4} + \alpha - \frac{1}{2}\right) \\ &= 1 \end{aligned}$$

donc, on arrange le produit $\prod_{\alpha\in\operatorname{Ker} v} f\Big(\frac{1+i}{4}+\alpha\Big)$ comme suit :

$$\prod_{\alpha\in\operatorname{Ker} v} f\Big(\frac{1+i}{4}+\alpha\Big) = f\Big(\frac{1+i}{4}\Big)\cdot\prod_{\alpha\in S_v} f\Big(\frac{1+i}{4}+\alpha\Big)f\Big(\frac{1+i}{4}-i\alpha\Big) \cdot\prod_{\alpha\in -S_v} f\Big(\frac{1+i}{4}+\alpha\Big)f\Big(\frac{1+i}{4}-i\alpha\Big) \tag{2.6}$$

et où S_v est un système de représentants modulo v tels que : $\{0, S_v, -S_v, iS_v, -iS_v\}$ forme un système complet de représentants de $\mathbb{Z}[\sqrt{-1}]/v\mathbb{Z}[-1]$.

Alors

$$\begin{aligned}\prod_{\alpha\in\operatorname{Ker} v} f\Big(\frac{1+i}{4}+\alpha\Big) &= \prod_{\alpha\in Sv} -if\Big(\frac{i+1}{4}+\alpha\Big)f\Big(i\frac{i+1}{4}+\alpha\Big)\\ &\quad\cdot\prod_{\alpha\in -Sv} -if\Big(\frac{i+1}{4}+\alpha\Big)f\Big(\frac{i+1}{4}i+\alpha\Big)\\ &= \prod_{\alpha\in Sv} -if\Big(\frac{i+1}{4}+\alpha\Big)f\Big(\frac{i+1}{4}+\alpha-\frac{1}{2}\Big)\\ &\quad\cdot\prod_{\alpha\in -Sv} -if\Big(\frac{i+1}{4}+\alpha\Big)f\Big(\frac{i+1}{4}i+\alpha-\frac{1}{2}\Big)\\ &= 1.\end{aligned}$$

On obtient

$$f(vz) = f\Big(v\cdot\frac{1+i}{4}\Big)f(z)\prod_{\substack{\alpha\in\operatorname{Ker} v\\ \alpha\neq 0}} f(z+\alpha)$$

et

$$\begin{aligned}f\Big(v\cdot\frac{1+i}{4}\Big) &= f\Big(\xi_v\cdot\frac{1+i}{4}+(v-\xi_v)\cdot\frac{1+i}{4}\Big)\\ &= f\Big(\xi_v\cdot\frac{1+i}{4}\Big) = \xi_v,\quad \text{car } (v-\xi_v)\frac{1+i}{4}\in\mathbb{Z}[\sqrt{-1}]\end{aligned}$$

ce qui termine la démonstration du théorème 2.5.

COROLLAIRE 2.7. — *Soit $v\in\mathbb{Z}[\sqrt{-1}]$, $(v,2)=1$, on a alors*

$$f(vz) = \xi_v f(z)\prod_{\substack{\alpha\in\operatorname{Ker} v\\ \alpha\neq 0}} f(z+\alpha) \quad \text{où}\quad \xi_v = \begin{cases} 1 & \text{si } v\equiv 1 \bmod \mathfrak{p}_2^3\\ -1 & \text{si } v\equiv -1 \bmod \mathfrak{p}_2^3\\ i & \text{si } v\equiv i \bmod \mathfrak{p}_2^3\\ -i & \text{si } v\equiv -i \bmod \mathfrak{p}_2^3.\end{cases}$$

DÉFINITION 2.8. — *Soient $\alpha,\beta\in\mathbb{Z}[\sqrt{-1}]$ tels que*

$$(\alpha,2) = (\beta,2) = (\alpha,\beta) = 1.$$

On définit le symbole quadratique $\left(\frac{\alpha}{\beta}\right)_2$ *comme suit :*

$$\left(\frac{\alpha}{\beta}\right)_2 := \prod_{\sigma \in S_\beta \cup iS_\beta} \frac{f(\alpha\sigma)}{f(\sigma)},$$

où $\{0, S_\beta, -S_\beta, iS_\beta, -iS_\beta\}$ *forme un système complet de représentants de* $\mathbb{Z}[\sqrt{-1}]/\beta\mathbb{Z}[\sqrt{-1}]$.

Cette définition est une formulation analytique du lemme de Gauss généralisé ([6]).

On est maintenant en mesure d'énoncer notre deuxième résultat :

THÉORÈME 2.9 (Loi de réciprocité quadratique dans $\mathbb{Q}(\sqrt{-1})$). *Soient* $\alpha, \beta \in \mathbb{Z}[\sqrt{-1}]$, $(\alpha, 2) = (\beta, 2) = (\alpha, \beta) = 2$. *Alors on a*

$$\left(\frac{\alpha}{\beta}\right)_2 \cdot \left(\frac{\beta}{\alpha}\right)_2^{-1} = \xi_\alpha^{\frac{N(\beta)-1}{2}} \xi_\beta^{-\frac{N(\alpha)-1}{2}} (-1)^{\frac{N(\alpha)-1}{2} \cdot \frac{N(\beta)-1}{2}}$$

où $N(\alpha)$ *est la norme de* α *dans* $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ *et* ξ_α *et* ξ_β *sont donnés par le corollaire 2.7.*

Démonstration. — D'après la définition 2.8 et le théorème 2.5, on a

$$\begin{aligned}
\left(\frac{\alpha}{\beta}\right)_2 &= \prod_{\alpha \in S_\beta \cup iS_\beta} \frac{f(\sigma\alpha)}{f(\sigma)} \\
&= \prod_{\alpha \in S_\beta \cup iS_\beta} \xi_\alpha \prod_{\substack{\sigma' \in \operatorname{Ker} \alpha \\ \sigma' \neq 0}} f(\sigma + \sigma') \\
&= \xi_\alpha^{\frac{N(\beta)-1}{2}} \prod_{\sigma \in S_\beta \cup iS_\beta} \prod_{\sigma' \in S_\alpha \cup iS_\alpha} f(\sigma + \sigma') f(\sigma - i\sigma')
\end{aligned}$$

d'autre part,

$$\begin{aligned}
\left(\frac{\beta}{\alpha}\right)_2 &= \xi_\beta^{\frac{N(\alpha)-1}{2}} \prod_{\sigma \in S_\alpha \cup iS_\alpha} \prod_{\substack{\sigma' \in \operatorname{Ker} \beta \\ \sigma' \neq 0}} f(\sigma + \sigma') \\
&= \xi_\beta^{\frac{N(\alpha)-1}{2}} \prod_{\sigma \in S_\alpha \cup iS_\alpha} \prod_{\sigma' \in S_\beta \cup iS_\beta} f(\sigma + \sigma') f(\sigma - \sigma').
\end{aligned}$$

En échangeant σ et σ' on obtient

$$\left(\frac{\beta}{\alpha}\right)_2^{-1} = \xi_\beta^{\frac{N(\alpha)-1}{2}} \prod_{\sigma \in S_\beta \cup iS_\beta} \prod_{\sigma' \in S_\alpha \cup iS_\alpha} f(\sigma + \sigma') f(\sigma' - \sigma)$$

donc

$$\left(\frac{\alpha}{\beta}\right)_2\left(\frac{\beta}{\alpha}\right)_2^{-1}=\xi_\alpha^{\frac{N(\beta)-1}{2}}\xi_\beta^{-\frac{N(\alpha)-1}{2}}\prod_{\sigma\in S_\beta\cup iS_\beta}\prod_{\sigma'\in S_\alpha\cup iS_\alpha}\frac{f(\sigma-\sigma')}{f(\sigma'-\sigma)}$$
$$=\xi_\alpha^{\frac{N(\beta)-1}{2}}\xi_\beta^{-\frac{N(\alpha)-1}{2}}\prod_{\sigma\in S_\beta\cup iS_\beta}\prod_{\sigma'\in S_\alpha\cup iS_\alpha}-1$$

ce qui donne bien

$$\boxed{\left(\frac{\alpha}{\beta}\right)_2\left(\frac{\beta}{\alpha}\right)_2^{-1}=\xi_\alpha^{\frac{N(\beta)-1}{2}}\xi_\beta^{-\frac{N(\alpha)-1}{2}}(-1)^{\frac{N(\beta)-1}{2}\cdot\frac{N(\alpha)-1}{2}}.}$$

3. Loi de réciprocité quadratique dans $\mathbb{Q}(\sqrt{-3})$.

L'anneau des entiers de $\mathbb{Q}(\sqrt{-3})$ est l'anneau $\mathbb{Z}[j]$, $j=\dfrac{1+\sqrt{-3}}{2}$. On considère la courbe elliptique E dont le modèle de Weierstrass est donné par

$$E : Y^2 = 4(X^3-1). \tag{3.1}$$

Cette courbe elliptique a multiplication complexe par $\mathbb{Z}[j]$ et E en tant que variété complexe, est isomorphe à $\mathbb{C}/\mathbb{Z}[j]$ et cet isomorphisme est donné par :

$$\begin{array}{rcll}\mathbb{C}/\mathbb{Z}[j] & \longrightarrow & E(\mathbb{C}) & \\ z & \longmapsto & (\wp(z),\wp'(z)) & \text{si } z\notin\mathbb{Z}[j] \\ z & \longmapsto & 0 & \text{si } z\in\mathbb{Z}[j].\end{array} \tag{3.2}$$

Cette fois-ci la fonction $\wp$ est la fonction de Weierstrass associée au réseau $\mathbb{Z}[j]$. Maintenant, on considère la fonction g elliptique pour le réseau $\mathbb{Z}[j]$ définie par

$$g(z)=2\sqrt{\wp\left(\frac{1}{2}\right)(j-1)}\ \frac{\wp(z)-\wp(j^2/2)}{\wp'(z)}. \tag{3.3}$$

Cette fonction a pour diviseur

$$(0)+\left(\frac{j^2}{2}\right)-\left(\frac{1}{2}\right)-\left(\frac{j}{2}\right).$$

Cela se déduit aisément du lemme suivant :

LEMME 3.4. — *Les diviseurs de $\wp$ et $\wp'$ sont donnés par*

$$(\wp)=\left(\frac{j-1}{3}\right)+\left(\frac{j^2-1}{3}\right)-2(0)$$
$$(\wp')=\left(\frac{1}{2}\right)+\left(\frac{j}{2}\right)+\left(\frac{j^2}{2}\right)-3(0).$$

En outre,

$$\wp(jz) = j\wp(z) \quad et \quad \wp'(jz) = \wp'(z).$$

Démonstration. — On sait que

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in \mathbf{Z}[j] \\ \omega \neq 0}} \Big(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big)$$

donc

$$\wp(jz) = \frac{1}{j^2 z^2} + \sum_{\substack{\omega \in \mathbf{Z}[j] \\ \omega \neq 0}} \Big(\frac{1}{(jz-\omega)^2} - \frac{1}{\omega^2}\Big),$$

on change ω en $j\omega$, on obtient

$$\wp(jz) = \frac{1}{j^2 z^2} + \sum_{\substack{\omega \in \mathbf{Z}[j] \\ \omega \neq 0}} \frac{1}{j^2}\Big(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big) = j\wp(z),$$

car la multiplication par j laisse stable $\mathbb{Z}[j]$. De cela, on déduit que les zéros de $\wp(z)$ sont $\mathrm{Ker}(j-1) \setminus \{0\}$. De plus, en dérivant les deux côtés des égalités $\wp(jz) = j\wp(z)$ et $\wp(-z) = \wp(z)$ on obtient

$$\wp'(jz) = \wp'(z) \quad \text{et} \quad \wp'(-z) = -\wp'(z).$$

De ce fait, on déduit que si z_0 est un zéro de $\wp'(z)$ alors z_0, jz_0, j^2z_0 et $-z_0$, $-jz_0$, $-j^2z_0$ le sont. Or z_0 ne peut être égal à 0 car 0 est un pôle triple pour $\wp'(z)$. D'où z_0, jz_0 et j^2z_0 sont distincts et comme la valence de $\wp'$ est égale à 3, on a forcément $z_0 = -z_0$, ce qui donne

$$(\wp') = \Big(\frac{1}{2}\Big) + \Big(\frac{j}{2}\Big) + \Big(\frac{j^2}{2}\Big) - 3(0).$$

On a alors le résultat suivant :

THÉORÈME 3.5 (Formule produit).

1) *$g(-jz) = -jg(z)$ et $g(z)g\Big(z + \dfrac{1}{2}\Big) = 1$.*

2) *On a la formule produit, pour $v \in \mathbb{Z}[j]$, $(v, 2) = 1$:*

$$g(vz) = \xi_v g(z) \prod_{\substack{\alpha \in \mathrm{Ker}\, v \\ \alpha \neq 0}} g(z+\alpha), \quad avec \quad \xi_v = \pm 1$$

déterminé par $\xi_v = v \displaystyle\prod_{\alpha \in \mathrm{Ker}\, v} g\Big(\alpha + \frac{1}{2}\Big)$.

Démonstration. — Comme la fonction $\wp$ est paire et $\wp'$ est impaire, on a $g(-z) = -g(z)$. D'autre part, la fonction $z \mapsto g(z)g\Big(z + \dfrac{1}{2}\Big)$ est elliptique pour le réseau $\mathbb{Z}[j]$ dont le diviseur est nul, donc c'est une fonction constante. Déterminons cette constante :

$$\begin{aligned}
&\lim_{z\mapsto\frac{j^2}{2}} g(z)g\Big(z+\frac{1}{2}\Big)\\
&\quad= 4(j-1)\wp\Big(\frac{1}{2}\Big)^2 \lim_{z\mapsto\frac{j^2}{2}} \frac{\wp(z)-\wp\big(\frac{j^2}{2}\big)}{\wp'(z)\wp'\big(z+\frac{1}{2}\big)}(j-j^2)\\
&\quad= -4(j-1)^2 j\wp\Big(\frac{1}{2}\Big)^2 \lim_{z\mapsto\frac{j^2}{2}} \frac{\frac{1}{2}\wp''\big(\frac{j^2}{2}\big)\big(z-\frac{j^2}{2}\big)^2+o\Big(\big(z-\frac{j^2}{2}\big)^2\Big)}{\wp''\big(\frac{j^2}{2}\big)\wp''\big(\frac{j}{2}\big)\big(z-\frac{j^2}{2}\big)^2+o\Big(\big(z-\frac{j^2}{2}\big)^2\Big)}\\
&\quad= -\frac{2(j-1)^2 j\wp\big(\frac{1}{2}\big)^2}{\wp''\big(\frac{1}{2}\big)} = -\frac{2(j-1)^2 j\wp\big(\frac{1}{2}\big)^2}{6j^2\wp\big(\frac{1}{2}\big)^2} = -\frac{1}{3}(j^2-j)^2\\
&\quad= 1.
\end{aligned}$$

D'où 1).

Montrons maintenant le 2).

Les deux fonctions $z \mapsto g(vz)$ et $z \mapsto g(z) \prod_{\substack{\alpha\in\mathrm{Ker}\, v\\ \alpha\neq 0}} g(z+\alpha)$ sont elliptiques pour $\mathbb{Z}[j]$ et ont le même diviseur, donc elles diffèrent à une constante multiplicative dépendant de v, ξ_v. Le calcul de la constante se fait comme suit :

d'une part

$$\begin{aligned}
g(vz)g\Big(v\Big(z+\frac{1}{2}\Big)\Big) &= g(vz)g\Big(vz+\frac{v}{2}\Big)\\
&= g(vz)g\Big(vz+\frac{1}{2}\Big)\\
&= 1,
\end{aligned}$$

d'autre part,

$$g(vz)g\Big(vz+\frac{1}{2}\Big) = \xi_v^2 g(z)g\Big(z+\frac{1}{2}\Big) \prod_{\substack{\alpha\in\mathrm{Ker}\, v\\ \alpha\neq 0}} g(z+\alpha)g\Big(z+\alpha+\frac{1}{2}\Big)$$

d'après 1), cela donne

$$g(vz)g\Big(v\Big(z+\frac{1}{2}\Big)\Big) = \xi_v^2$$

d'où

$$\xi_v^2 = 1.$$

Aussi

$$\xi_v = \lim_{z\mapsto 0} \frac{g(vz)}{g(z)\prod\limits_{\substack{\alpha\in\mathrm{Ker}\,v\\ \alpha\neq 0}} g(z+\alpha)} = \frac{v}{\prod\limits_{\substack{\alpha\in\mathrm{Ker}\,v\\ \alpha\neq 0}} g(\alpha)}$$

et d'après 1) du théorème 3.5, on a

$$\xi_v = v \prod_{\substack{\alpha\in\mathrm{Ker}\,v\\ \alpha\neq 0}} g\Big(\alpha+\frac{1}{2}\Big).$$

Ceci termine la démonstration du théorème 3.5.

DÉFINITION 3.6. — *Pour $\alpha,\beta\in\mathbb{Z}[j]$, $(\alpha,2)=(\beta,2)=(\alpha,\beta)=1$. On définit le symbole quadratique $\left(\frac{\alpha}{\beta}\right)_2$ par*

$$\left(\frac{\alpha}{\beta}\right)_2 = \prod_{\sigma\in S_\beta} \varepsilon(\alpha,\sigma) \quad \text{où} \quad \alpha\sigma = \varepsilon(\alpha,\sigma)\gamma(\sigma)$$

avec $\varepsilon(\alpha,\sigma)\in\{-1,1\}$, $\gamma(\sigma)\in S_\beta$ et $\{S_\beta,-S_\beta\}$ est un système complet des représentants de $\mathbb{Z}[j]/\beta\mathbb{Z}[j]\smallsetminus\{0\}$.

On peut donc énoncer notre troisième résultat principal :

THÉORÈME 3.7 (Loi de réciprocité quadratique dans $\mathbb{Q}(j)$). — *Soient $\alpha,\beta\in\mathbb{Z}[j]$, $(\alpha,\beta)=(\alpha,2)=(\beta,2)=1$. On a alors*

$$\left(\frac{\alpha}{\beta}\right)_2\left(\frac{\beta}{\alpha}\right)_2^{-1} = \xi_\alpha^{\frac{N(\beta)-1}{2}}\xi_\beta^{\frac{N(\alpha)-1}{2}}(-1)^{\frac{N(\alpha)-1}{2}\frac{N(\beta)-1}{2}}$$

où $N(\alpha)$ désigne la norme de α dans $\mathbb{Q}(j)/\mathbb{Q}$ et $\xi_\alpha = \alpha \prod\limits_{\substack{\gamma\in\mathrm{Ker}\,\alpha\\ \gamma\neq 0}} g\Big(\gamma+\frac{1}{2}\Big)$, de même $\xi_\beta = \beta \prod\limits_{\substack{\gamma\in\mathrm{Ker}\,\beta\\ \gamma\neq 0}} g\Big(\gamma+\frac{1}{2}\Big)$, avec ξ_α, $\xi_\beta\in\{-1,1\}$.

Démonstration. — La preuve de ce résultat est similaire à celle du théorème 1.10. En effet, on peut écrire $\varepsilon(\alpha,\sigma) = \dfrac{\alpha\sigma}{\gamma(\sigma)}$. D'autre part, $g(\alpha\sigma) = g\big(\varepsilon(\alpha,\sigma)\gamma(\sigma)\big) = \varepsilon(\alpha,\sigma)g(\gamma(\sigma))$ car g est impaire; d'où

$$\varepsilon(\alpha,\sigma) = \frac{\alpha\sigma}{\gamma(\sigma)} = \frac{g(\alpha\sigma)}{g(\gamma(\sigma))}.$$

Alors

$$\left(\frac{\alpha}{\beta}\right)_2 = \prod_{\sigma\in S_\beta}\frac{g(\alpha\sigma)}{g(\gamma(\sigma))} = \prod_{\sigma\in S_\beta}\frac{g(\alpha\sigma)}{g(\sigma)}$$

on déduit du théorème 3.5 que

$$\left(\frac{\alpha}{\beta}\right)_2 = \xi_\alpha^{\frac{N(\beta)-1}{2}} \prod_{\sigma\in S_\beta} \prod_{\sigma'\in S_\alpha} g(\sigma+\sigma')g(\sigma-\sigma');$$

de même

$$\left(\frac{\beta}{\alpha}\right)_2 = \xi_\beta^{\frac{N(\alpha)-1}{2}} \prod_{\sigma'\in S_\alpha} \prod_{\sigma\in S_\beta} g(\sigma'+\sigma)g(\sigma'-\sigma).$$

Cela implique

$$\left(\frac{\alpha}{\beta}\right)_2 \left(\frac{\beta}{\alpha}\right)_2^{-1} = \xi_\beta^{\frac{N(\alpha)-1}{2}} \xi_\alpha^{\frac{N(\beta)-1}{2}} (-1)^{\frac{N(\alpha)-1}{2}\frac{N(\beta)-1}{2}},$$

où ξ_α et ξ_β sont donnés par le théorème 3.5; d'où le théorème 3.7.

BIBLIOGRAPHIE

[1] R. FUETER, Vorlesungen über die singulären Moduln und die complexe Multiplikation der elliptischen Funktionnen, Teubner, Leipzig, I (1924), II (1927).

[2] H. HASSE, Zetafunktion und L-Funktion zu einem arithmetischen Funktionenkörper vom Fermatschen Typus, Abh. Deutsch. Akad. der Wiss. zu Berlin, Klase f. Math. u. Allg. Naturw., Jahrg., 1954, Heft4.

[3] D.S. KUBERT, Product formulae on elliptic curves, Invent. Math., 117 (1994), 227–273.

[4] S. LANG, Elliptic functions, Reading MA, Addison-Wesley, 1973.

[5] T. KUBOTA, Reciprocities in Gauss' and Eisenstein's number fields, J. für reine und angew. Math., 208 (1961), 35–50.

[6] H. REICHARDT, Eine Bemerkung zur theorie der Jacobischen symbols, Math. Nachr., 19 (1958), 171–175.

[7] J.-P. SERRE, Cours d'arithmétique, PUF, 970.

Manuscrit reçu le 16 janvier 1995,
accepté le 13 juin 1995.

Abdelmejid BAYAD,
Institut Fourier
Université de Grenoble I
URA 188 du CNRS
BP 74
38402 St Martin d'Hères (France).