Groupe d'étude d'Analyse ultramétrique
(Y. Amice, G. Christol, P. Robba)
8e année, 1980/81, no 36, 14 p. 15 juin 1981

Histoire de la loi de réciprocité quadratique : Gauss et Tate

par Roger Cuculière
Lycée Carnot (Paris)

1. La première démonstration de Gauss revue par Dirichlet.

1.1. Histoire de cette démonstration.

C'est à Legendre que l'on peut reconnaître la paternité de la loi de réciprocité quadratique et du symbole grâce auquel elle s'exprime naturellement (voir [1]). Dès 1785, il avait énoncé ce théorème et en avait ébauché une preuve. Mais celle-ci s'appuyait sur la propriété suivante, que Legendre ne croyait pas difficile à démontrer : toute progression arithmétique, dont le premier terme est premier avec la raison, contient une infinité de nombres premiers. C'est ce que l'on nomme aujourd'hui le "théorème de la progression arithmétique".

Or, cette dernière propriété, d'apparence si simple, n'a été démontrée qu'en 1837 par Lejeune-Dirichlet. De sorte qu'en 1795, lorsque Gauss, agé de 18 ans, s'engage dans l'étude de la théorie des nombres, la loi de réciprocité n'est pas complétement démontrée.

Un an après, c'est chose faite on peut lire cette première démonstration de Gauss dans ses "Recherches arithmétiques", dont elle occupe les articles 131 à 145, pages 96 à 103 de l'édition française (voir [2]), après une vingtaine de pages consacrées à des lemmes et à l'étude de divers cas particuliers de la loi de réciprocité. Il s'agit d'une démonstration longue et difficile, qui avance à l'aide d'un grand nombre de cas et de sous-cas : un texte fort rébarbatif.

Pourtant, cette démonstration présente un grand intérêt et occupe une place à part. Gauss dira par la suite que c'est la seule qui soit "homogène". C'est parce que, concernant une propriété des nombres entiers, elle n'utilise que la méthode spécifique aux nombres entiers : la récurrence.

En effet, lorsque Gauss s'est engagé dans l'étude de la théorie des nombres, il l'a fait sans connaître l'état de cette science, dont il a repris l'étude à la base, par ses seules forces. Cette réflexion originale a produit les "Recherches arithmétiques". C'est pourquoi sa démonstration de la loi de réciprocité ne prolonge pas les efforts infructueux de Legendre, mais procède d'un principe différent, simple dans sa conception, difficile dans son exécution. Mais cet avantage ne va pas sans inconvénient: Gauss se prive également du symbole que Legendre a introduit et qui est particulièrement adapté à ce problème. Mis à même, par la suite, de connaître les apports de ses prédécesseurs, il ne daignera pas y faire emprunt, et sa première démonstration restera en l'état. Gauss en publiera plusieurs autres, très différentes dans leurs principes (voir [1]).

Texte reçu le 5 juin 1981.
Roger CUCULIÈRE, 10 cité Falaise, 75018 PARIS.

En 1857, Lejeune-Dirichlet est revenu sur cette question en montrant que la complexité de cette preuve est fortuite, attendu qu'on la simplifie grandement en utilisant le symbole de Legendre, et plus précisément la généralisation donnée par Jacobi en 1837. Rappelons le contenu de cet article de Dirichlet [3].

1.2. Les prémisses.

On suppose connu le symbole de Legendre, ainsi que les propriétés des résidus -1 et 2, exprimées par

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}, \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8},$$

pour p premier impair.

La première de ces relations équivaut à une propriété de la forme quadratique $x^2 + y^2$, énoncée par Fermat, démontrée par Euler. La seconde provient de même d'une propriété de la forme $x^2 - 2y^2$, énoncée par Fermat, démontrée partiellement par Euler et entièrement par Lagrange ; Gauss en donne aussi, d'ailleurs, une démonstration par récurrence.

On suppose connus également le symbole de Jacobi et ses propriétés :

$$\left(\frac{-1}{P}\right) = (-1)^{(P-1)/2}, \quad \left(\frac{2}{P}\right) = (-1)^{(P^2-1)/8},$$

où P désigne cette fois un nombre entier impair > 1, premier ou non.

Si P et Q sont deux nombres impairs, notons $LRQ(P, Q)$ la relation :

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{(P-1)(Q-1)/4}.$$

La loi de réciprocité quadratique dit que l'on a $LRQ(p, q)$ pour tous les entiers naturels p, q premiers, impairs, distincts : c'est ce que nous voulons démontrer.

Si S est un ensemble de nombres premiers impairs, notons $\mathcal{N}(S)$ l'ensemble des entiers naturels dont tous les diviseurs premiers appartiennent à S.

Voici alors une assertion qui intervient dans la démonstration en question : si l'on a $LRQ(p, q)$ pour toute paire de nombres premiers impairs positifs appartenant à S, alors on a $LRQ(P, Q)$ pour toute paire d'entiers impairs premiers entre eux appartenant à $\mathcal{N}(S)$.

Ceci fait l'objet des sections 133 et 134 des "Recherches Arithmétiques", mais sous une forme peu explicite, faute d'un symbolisme adéquat.

Pour le démontrer, il suffit de constater que si on écrit un entier R forme sous la forme

$$R = \prod_i r_i \quad \text{(facteurs impairs)}$$

Alors :

$$R - 1 = \sum_i (r_i - 1) \pmod 4$$

et par suite $(R-1)/2$ et $\sum_i (r_i - 1)/2$ ont même parité.

1.3. La démonstration.

L'idée de la démonstration est de procéder par récurrence sur les nombres premiers. Considérons la propriété suivante pour un nombre q, premier impair : pour tous les nombres premiers impairs u et v tels que $u < q, v < q, u \neq v$, on a $LRQ(u, v)$.

Elle est vraie pour $q = 7$ parce que l'on a $LRQ(3, 5)$. Nous allons montrer que, si elle est vraie pour un nombre premier impair q, elle est vraie pour le suivant. Et pour cela, nous établirons qu'elle implique $LRQ(p, q)$ pour tout nombre premier impair $p < q$.

Soit donc q vérifiant la propriété ci-dessus, et $p < q$, tous deux premiers impairs. Nous voulons montrer que l'on a $LRQ(p, q)$.

Premier cas : $(p/q) = 1$. Il existe alors un entier rationnel e tel que $e^2 \equiv p \pmod q$. On peut choisir cet entier pair, et vérifiant $0 < e < q$. Il existe un autre entier f tel que $e^2 - p = qf$. On a f impair, et $0 < f < q$.

(a) Si p ne divise pas f, f et p sont premiers entre eux, impairs, et tous leurs diviseurs premiers sont $< q$. D'après l'hypothèse de récurrence et le lemme ci-dessus, on a donc $LRQ(p, f)$ c'est-à-dire

$$\left(\frac{p}{f}\right)\left(\frac{f}{p}\right) = (-1)^{(p-1)(p-1)/4}.$$

Mais on a aussi $(p/f) = 1$ car $p \equiv e^2 \pmod f$. Donc $(f/p) = (-1)^{(p-1)(f-1)/4}$. Or, l'égalité $e^2 - p = qf$ nous indique aussi que $(qf/p) = 1$. D'où il découle

$$\left(\frac{q}{p}\right) = \left(\frac{f}{p}\right)\left(\frac{qf}{p}\right) = (-1)^{(p-1)(f-1)/4}.$$

Il reste à prouver que

$$\frac{(p-1)(f-1)}{4} \equiv \frac{(p-1)(q-1)}{4} \pmod 2,$$

ce qui provient de considérations élémentaires sur les congruences, et il s'avère que l'on a $LRQ(p, q)$ dans ce cas.

(b) Si p divise f, alors il existe f' tel que $f = f'p$, et aussi e' tel que $e = e'p$, d'où $e'^2 p - 1 = qf'$. Par suite, f' est impair, e' est pair, $f' < f$, p et f' sont premiers entre eux. Comme au paragraphe (a),

la relation $LRQ(p, f')$ est vérifiée, et puisque $(p/f') = 1$, on en déduit $(f'/p) = (-1)^{(p-1)(f'-1)/4}$. Or, nous avons cette fois $qf' = -1 \pmod{p}$ d'où $(qf'/p)(-1/p)$, et enfin

$$\left(\frac{q}{p}\right) = \left(\frac{qf'}{p}\right)\left(\frac{f'}{p}\right)(-1)^{(p-1)/2}(-1)^{(p-1)(f'-1)/4} = (-1)^{(p-1)(f'+1)/4}.$$

On termine comme ci-dessus, en montrant que les entiers $((p-1)(f'+1))/4$ et $(p-1)(q-1))/4$ ont même parité.

Deuxième cas : $\left(\frac{p}{q}\right) = -1$ et $q \equiv 3 \pmod{4}$. Pour pouvoir user d'un raisonnement analogue au précédent, il faut disposer de nombres qui **soient** résidus quadratiques. On écrit donc

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

D'où découle l'existence de e tel que $e^2 \equiv -p \pmod{q}$ et de f tel que $e^2 + p = qf$, et la suite se déroule à peu près comme au premier cas.

Troisième cas : $\left(\frac{p}{q}\right) = -1$ et $q \equiv 1 \pmod{4}$. Ici, l'on doit faire intervenir un lemme :
Pour tout nombre premier $q \equiv 1 \pmod{4}$ *il existe un nombre premier impair* $p' < q$ *tel que* $\left(\frac{q}{p'}\right) = -1$.

Si l'on avait $(p'/q) = 1$, on pourrait appliquer à p' les considérations du "premier cas" ci-dessus, et l'on aurait $LRQ(p', q)$, d'où $(q/p') = -1$, ce qui n'est pas. Par suite, p' et q vérifient $(p'/q) = -1$, et donc $(pp'/q) = 1$. C'est dire qu'il existe deux entiers e et f tels que $e^2 - pp' = qf$, etc.

Voici en résumé le schéma de la démonstration, comprenant la liste des cas à envisager :

$$\left(\frac{p}{q}\right) = 1, \quad e^2 - p = qf \begin{cases} \nearrow p \nmid f \\ \searrow p \mid f \end{cases}$$

$$\left(\frac{p}{q}\right) = -1, q \equiv 3 \pmod 4, \left(\frac{-p}{q}\right) = 1,$$

$$e^2 + p = qf \begin{cases} \nearrow p \nmid f \\ \searrow p \mid f \end{cases}$$

$$\left(\frac{p}{q}\right) = -1, q \equiv 1 \pmod 4, \left(\frac{q}{p'}\right) = -1, \left(\frac{pp'}{q}\right) = 1,$$

$$e^2 - pp' = qf \begin{cases} \nearrow p \nmid f, p' \nmid f \\ \nearrow p \mid f, p' \nmid f \\ \nearrow p \nmid f, p' \mid f \\ \searrow p \mid f, p' \mid f \end{cases}$$

1.4. Le lemme.

Ce lemme invoqué au troisième cas a été démontré par Gauss au cours des articles 125 à 129 des "Recherches arithmétiques" :

"si q est premier, si $q \equiv 1 \pmod 4$, alors il existe p' premier impair, tel que $p' < q$ et $(q/p') = -1$. (En d'autres termes : tout nombre premier q de la forme $4k+1$ est non-résidu de certains nombres premiers plus petits que lui.)"

Gauss distingue encore deux cas : $q = 8k + 5$, ou $q = 8k + 1$.

(a) Si $q = 8k + 5$, on a $q - 2 \equiv 3 \pmod 8$ donc l'un des facteurs premiers de $q - 2$ est de la forme $8k \pm 3$ Si l'on note p' ce facteur, on a $q \equiv 2 \pmod{p'}$ et par suite

$$\left(\frac{q}{p'}\right) = \left(\frac{2}{p'}\right) = (-1)^{(p'^2-1)/8}.$$

Or, si $p = 8k \pm 3$, alors $(p'^2 - 1)/8$ est impair.

C. Q. F. D.

Remarquons que l'on pouvait éviter d'utiliser le caractère quadratique de 2, en notant que $q + 1 = 2(4k + 3)$, et en appelant p' un diviseur premier de $4k + 3$, tel que $p' = 4h + 3$, car il en existe

nécessairement. Il est clair qu'alors $(q/p')(-1/p') = -1$.

(b) Si $q = 8k + 1$, soit m la partie entière de $\sqrt{q}$. Raisonnons par l'absurde et supposons que tout p' premier impair tel que $p' \leq 2m + 1$ vérifie $(q/p') = 1$.

Les propriétés des résidus, suivant des modules composés (voir par exemple [2], soit section 4, n° 100 à 103), permettent d'affirmer que q esr résidu de $(2m+1)! = M$: il existe k tel que $k^2 \equiv q \pmod{M}$ D'où la congruence :

$$(k^2 - 1^2)(k^2 - 2^2) \dots (k^2 - m^2) \equiv (q - 1^2)(q - 2^2) \dots (q - m^2) \pmod{M}.$$

Or, le nombre

$$k(k^2 - 1^2)(k^2 - 2^2) \dots (k^2 - m^2) = (k - m)(k - m + 1) \dots (k - 1)k(k + 1) \dots (k + m - 1)(k + m)$$

est le produit de $2m + 1$ entiers consécutifs : il est donc multiple de $(2m + 1)! = M$. Mais l'entier M est premier avec q, donc avec k. Il divise donc le premier membre de la congruence ci-dessus, et aussi, dès lors, son second membre $(q - 1^2)(q - 2^2) \dots (q - m^2)$.

Mais ceci est impossible car la définition de m implique que $(m + 1)^2 > q$, et par suite

$$M = (m + 1)((m + 1)^2 - 1^2)((m + 1)^2 - 2^2) \dots ((m + 1)^2 - m^2) > (q - 1^2)(q - 2^2) \dots (q - m^2).$$

Notre hypothèse ci-dessus se révèle fausse : il est ainsi prouvé qu'il existe $p' < 2\sqrt{q} + 1$ tel que $(q/p') = -1$. On termine en remarquant que l'inégalité $2\sqrt{q} + 1 < q$ est vérifiée dès que $q \geq 11$.

1.5. Remarque.

La démonstration de ce lemme utilise la propriété suivante :

Le produit de n entiers consécutifs, par exemple $A = a(a+1) \dots (a+n-1)$, est toujours divisible par $n!$. Ceci est très clair, parce que le quotient de ces deux nombres est égal à C^n_{a+n-1} : Gauss indique justement (n° 127) que cette proposition est "connue par la théorie des nombres figurés", nous dirons par la Combinatoire. Mais, toujours à l'affût de démonstrations "homogènes", il éprouve le besoin de produire une preuve purement arithmétique, donnant l'expression de $v_p(n!)$, et montrant que $v_p(A) \geq v_p(n!)$ pour tout nombre premier p. C'est ce p que reprend Milnor dans [4], p. 105.

1.6. Conclusion.

Ayant ainsi mis en lumière la simplicité du principe de cette démonstration, nous pouvons, après Dirichlet, affirmer son intérêt méthodologique qui vient s'ajouter à son intérêt historique. C'est ainsi que, pendant plus d'un siècle, on a vu la "Première démonstration de Gauss".

Mais John Tate a montré de plus qu'on pouvait la reconsidérer dans le cadre de la K-théorie : c'est ce que nous allons voir.

2. Symboles et K-théorie.

2.1. Symboles de Steinberg

Soit F un corps commutatif, et $F^* = F - \{0\}$.

Définition. Un symbole de Steinberg est une application c de $K^* \times K^*$ dans un groupe abélien A, bimultiplicative, et qui vérifie

$$c(x, 1-x) = 1 \text{ si } x \neq 0 \text{ et } x \neq 1.$$

Un tel symbole vérifie nécessairement

$$c(1,x) = c(x,1) = 1\ ; \qquad c(x, 1-x^{-1}) = 1\ ; \qquad c(x,-x) = 1;$$

$$c(x,x) = c(-1,x) = c(x,-1), \quad \text{élément de carré 1;}$$

Enfin

$$c(y,x) = (c(x,y))^{-1} \qquad ([4], p.94).$$

2.2. Symbole de Hilbert, ou symbole des restes normiques quadratique.

On considère $F = \mathbb{Q}_p$, p premier fini, ou $F = R = \mathbb{Q}_\infty$ et A= {-1, 1}.

On note $\left(\frac{a,b}{p}\right) = 1$ s'il existe des éléments (x,y,z) de F non tous nuls tels que $ax^2 + by^2 - z^2 = 0$ (ou s'il existe u et v éléments de F tels que $ax^2 + by^2 = 1$), et l'on note $\left(\frac{a,b}{p}\right) = -1$ dans le cas contraire.

Ce symbole vérifie tout d'abord les propriétés :

$$\left(\frac{a,b}{p}\right) = \left(\frac{b,a}{p}\right)\ ;\ \left(\frac{a,1-a}{p}\right) = 1\ ;\ \left(\frac{a,-a}{p}\right) = 1$$

$$\text{et } \left(\frac{a,c^2}{p}\right) = 1 \text{ pour tout } a.$$

Lorsque b n'est pas un carré dans F, on a $\left(\frac{a,b}{p}\right) = 1$ si, et seulement si, a appartient au groupe des normes $N(F(\sqrt{b})^*)$.

La valeur de $\left(\frac{a,b}{p}\right)$ ne dépend que de la classe de a et de b modulo $(F^*)^2$: il suffit de le calculer lorsque a et b décrivent un ensemble de représentants de $F^*/(f^*)^2$. On peut alors distinguer trois cas :

(a) Si p est un nombre premier impair, alors l'extension $\mathbb{Q}_p(\sqrt{b})$ est modérement ramifiée, et le groupe $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ a quatre éléments. Les éléments a et b de $\mathbb{Q}_p^*$ se mettent de manière unique sous

la forme

$$a = p^\alpha a',\ b = p^\beta b' \quad \text{avec} \quad \alpha \in \mathbb{Z},\ \ \beta \in \mathbb{Z},\ \ a' \in \mathbb{Z}_p^*,\ \ b' \in \mathbb{Z}_p^*,$$

et l'on a

$$\alpha = v_p(a),\ \ \beta = v_p(b).$$

On en déduit :

$$\left(\frac{a,b}{p}\right) = (-1)^{\alpha\beta(p-1)/2} \left(\frac{\overline{a}'}{p}\right)^\beta \left(\frac{\overline{b}'}{p}\right)^\alpha,$$

où $\overline{a}'$ et $\overline{b}'$ désignent les images de a' et b' par le morphisme de réduction modulo $p : z \mapsto \overline{z}$, de $\mathbb{Z}_p^*$ dans $(\mathbb{Z}/p\mathbb{Z})^*$ (voir [5], p. 39).

(b) Si p = 2, le groupe $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ est d'ordre 8, avec pour générateurs $\{-1, 2, 5\}$. Tout élément a de $\mathbb{Q}_2^*$ se met de manière unique sous la forme :

$$a = (-1)^i 2^j 5^k a',$$

avec $i = 0$ ou 1, $j = v_2(a) \in \mathbb{Z}$, $k = 0$ ou 1, $a' \in 1 + 8\mathbb{Z}_2 \subset (\mathbb{Q}_2^*)^2$. Soit, de même, $b = (-1)^I 2^J 5^K 5b'$. Alors, on a

$$\left(\frac{a,b}{2}\right) = (-1)^{iI+jK+kJ}.$$

Remarquons que, si l'on pose $a = 2^j u$, alors i et k sont égaux respectivement aux classes modulo 2 de $\dfrac{u-1}{2}$ et $\dfrac{u^2-1}{8}$ ([5], p. 39).

(c) Si $p = \infty$, alors on a :

$$\left(\frac{a,b}{\infty}\right) = 1 \text{ si } a > 0 \text{ ou } b > 0, \ \text{ et } \ \left(\frac{a,b}{\infty}\right) = -1 \text{ si } a < 0 \text{ et } b < 0.$$

La bimultiplication de ce symbole en résulte, et c'est donc un symbole de Steinberg.

2.3. La formule du produit.

Tous les symboles $\left(\dfrac{x,y}{p}\right)$, ainsi que $\left(\dfrac{x,y}{\infty}\right)$, sont définis sur $\mathbb{Q}^*$. Si p et q sont des entiers naturels premiers impairs, on a $\left(\dfrac{p,q}{p}\right) = \left(\dfrac{q}{p}\right)$; $\left(\dfrac{p,q}{r}\right) = 1$ si r est premier impair, $r \neq p$, $r \neq q$; $(p, q/\infty) = 1$; et enfin $\left(\dfrac{p,q}{2}\right) = (-1)^{(p-1)(q-1)/4}$. Da sorte que, si l'on désigne par V l'ensemble des nombres premiers auxquels on adjoint ∞, on a :

$$\prod_{v \in V} \left(\frac{p,q}{v}\right) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}.$$

Ainsi, la relation $LRQ(p,q)$ équivaut à $\prod_{v\in V}\left(\frac{p,q}{v}\right)=1$. En fait, la loi de réciprocité, jointe aux propriétés des résidus -1 et 2 équivaut à la formule du produit, de Hilbert :

$$\prod_{v\in V}\left(\frac{a,b}{v}\right)=1$$

quels que soient a et b rationnels non nuls ([5], p. 44, et [7], p. 313).

2.4. Symbole de Steinberg associé à une valuation.

Soit F un corps valué commutatif, avec valuation discrète v. Soit $\bigwedge$ l'anneau de valuation $\{x/v(x)\geq 0\}$, et $\mathcal{P}$ son idéal premier $\{x/v(x)>0\}$ Le corps résiduel est $\bigwedge/\mathcal{P}$. Si x et y sont des éléments non nuls de F alors l'élément de F : $(-1)^{v(x)v(y)}(x^{v(y)}/y^{v(y)})$ a une valuation nulle. C'est donc un élément de $\bigwedge$ non nul modulo $\mathcal{P}$. On note $d_y(x,y)$ sa classe mod $\mathcal{P}$, et l'on définit ainsi une application d_v de $F^*\times F^*$ dans $(\bigwedge/\mathcal{P})^*$, qui est le groupe multiplicatif du corps résiduel. On montre par le calcul qu'il s'agit d'un symbole de Steinberg ([4], p. 98).

En particulier, si $F=\mathbb{Q}_p$ avec p premier impair et v la valuation p-adique $d_{v_p}(x,y)=(x,y)_p$, symbole de Steinberg avec, pour groupe d'arrivée, $(\mathbb{Z}_p/p\mathbb{Z}_p)^*$ isomorphe au groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$, que nous noterons A_p ([4], p. 99).

Il existe une relation simple entre le symbole $(a,b)_p$ associé à la valuation p-adique et le symbole de Hilbert $\left(\frac{a,b}{p}\right)$.

En comparant les formules des n° 2.2 (a) et 2.4, on voit que

$$\left(\frac{x,y}{p}\right)=((x,y)_p)^{(p-1)/2}.$$

Si $p=2$, la définition ci-dessus conduit à un symbole trivial, l'application $\mathbb{Q}_2^*\to\{1\}$. Dans ce cas, on pose simplement $(a,b)_2=\left(\frac{a,b}{2}\right)$, à valeurs dans le groupe multiplicatif $\{-1,1\}$, que nous noterons A_2.

2.5. Les symboles de Steinberg et le K_2 d'un corps.

Si F est un corps commutatif, on pose par définition

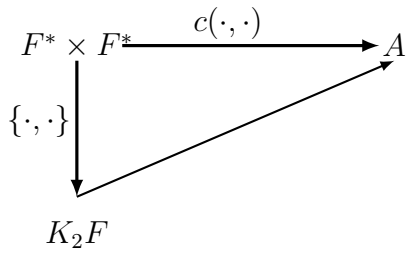
$$K_2F=H_2(SL_\infty(F),\mathbb{Z})\qquad([6],p.202).$$

Le lien entre K-théorie et symboles de Steinberg est assuré par le théorème suivant.

Théorème. (Matsumoto, 1969). *Le groupe abélien K_2F est défini par les générateurs $\{x,y\}$, où $x\in F^*$ et $y\in F^*$ vérifient les relations :*

$$\begin{array}{l}\{x,1-x\}=1\ \text{ si }\ x\neq 0\ \text{ et }\ x\neq 1\ ;\\ \{x_1x_2,y\}=\{x_1,y\}\{x_2,y\};\\ \{x,y_1y_2\}=\{x,y_1\}\{x,y_2\}\qquad([4],p.93).\end{array}$$

Il en résulte que tout symbole de Steinberg c sur F^* se factorise à travers K_2F.



Autrement dit, il existe un unique morphisme $\varphi : K_2F \to A$ tel que, pour tout $x \in F^*$ et tout $y \in F^*$,

$$c(x,y) = \varphi(\{x,y\}).$$

Le groupe K_2F apparaît ainsi comme la solution d'un problème universel.

2.6. Structure de K_2

Le théorème de Tate (1970) affirme que $K_2\mathbb{Q} \approx \bigcup_{p \text{ premier}} A_p$, l'isomorphisme étant donné par la correspondance :

$$\{x,y\} \mapsto \prod_p (x,y)_p,$$

car les $(x,y)_p$ sont presque tous égaux à 1. On peut trouver cet énoncé dans [6], p. 202, et sa démonstration dans [4], p. 100. Comme le fait remarquer son auteur, elle se fonde sur le même argument que la "Première démonstration de Gauss" décrite ci-dessus : toutes deux usent d'une récurrence sur les nombres premiers.

Mais il y a plus. Au-delà de cette simple analogie, Tate a pu déduire de ces considérations une nouvelle démonstration de la loi de réciprocité.

3. Démonstration de Tate de la loi de réciprocité.

3.1. Une formule de produit.

Les théorèmes de Matsumoto et de Tate conduisent au corollaire suivant :

Théorème. *Pour tout symbole de Steinberg $\mathbb{Q}^* \times \mathbb{Q}^* \to A$, il existe une seule famille d'homomorphismes $\varphi : A_p \to A$ telle que*

$$c(x,y) = \prod_p \varphi_p((x,y)_p).$$

En effet, d'après le théorème de Matsumoto, il existe un seul homomorphisme $\varphi : K_2\mathbb{Q} \to A$ tel que $c(x,y) = \varphi(\{x,y\})$; si l'on assimile $K_2\mathbb{Q}$ à $\bigcup_p A_p$ et que l'on note i_p l'injection canonique

$A_p \to K_2\mathbb{Q}$, on obtient

$$\varphi_p = \varphi \circ i_p.$$

Si nous appliquons ce théorème au symbole de Hilbert $\left(\frac{x,y}{\infty}\right)$, à valeurs dans $A_2 = \{-1, 1\}$, nous constatons qu'il existe une famille unique d'endomorphismes $\varphi_p : A_p \to A_2$ tels que

$$\left(\frac{x,y}{\infty}\right) = \prod_p \varphi_p((x,y)_p).$$

Mais, si p est impair, le groupe A_p est cyclique, et il n'y a que deux homomorphismes $A_p \to A_2$: $z \to 1$ et $z \to z^{(p-1)/2}$. Il existe donc ε_p, égal à 0 ou 1, tel que $\varphi_p(z) = z^{\varepsilon_p(p-1)/2}$ pour tout $z \in A_p$. Il en résulte que

$$\varphi_p((x,y)_p) = (((x,y)_p)^{(p-1)/2})^{\varepsilon_p} = \left(\frac{x,y}{p}\right)^{\varepsilon_p}.$$

Si maintenant $p = 2$, il n'y a encore que deux homomorphismes de A_2 dans $A_2 : z \to z^{\varepsilon_2}$ où ε_2 est égal à 0 ou à 1, et l'on a

$$\varphi_2((x,y)_2) = ((x,y)_2)^{\varepsilon_2} = \left(\frac{x,y}{2}\right)^{\varepsilon_2}.$$

D'où la formule du produit :

$$\left(\frac{x,y}{\infty}\right) = \prod_p \left(\frac{x,y}{p}\right)^{\varepsilon_p} \quad \text{où les } \varepsilon_p \text{ valent 0 ou 1.}$$

Comme nous l'avons vu au n° 2.3, démontrer la loi de réciprocité, c'est démontrer que les ε_p sont tous égaux à 1.

3.2. La démonstration.

(a) Détermination de ε_2. On prend $x = y = -1$, et il vient

$$\left(\frac{-1,-1}{\infty}\right) = -1, \quad \left(\frac{-1,-1}{p}\right) = 1$$

pour p premier impair (car toute équation $ax^2 + by^2 = c$ a des racines dans $\mathbb{Z}/p\mathbb{Z}$ si $ab \not\equiv 0$). Par suite, on a $(-1, -1/2)^{\varepsilon_2} = -1$, d'où $\varepsilon_2 = 1$ et $(-1, -1/2) = -1$. Cette dernière affirmation pourrait se vérifier directement par exemple en partant du fait que -1 n'est pas somme de deux carrés dans $\mathbb{Z}/8\mathbb{Z}$.

(b) Détermination de ε_p pour $p = 8k + 5$. Soit $x = 2, y = p$. Pour q premier, $q \neq p, q \neq 2$, on a $(2, p/q) = 1$, d'où

$$\left(\frac{2,p}{\infty}\right) = \left(\frac{2,p}{2}\right)^{\varepsilon_2} \left(\frac{2,p}{p}\right)^{\varepsilon_p}.$$

Or, on a $\dfrac{2,p}{\infty} = 1$. Pour déterminer $\dfrac{2,p}{2}$, on écrit :

$$2 = (-1)^0.2^1.5^0.1 \text{ et } p = (-1)^0.2^0.5^1.\frac{5p}{25}$$

et on applique la formule vue au n° 2.2 (b): il vient $\left(\frac{2,p}{2}\right) = -1$ d'où $(2,p/p)^{\varepsilon_p} = -1$, ce qui implique $(2,p/p) = -1$ et $\varepsilon_p = 1$.

(c) Détermination de ε_p pour $p = 8k-5$. Même déroulement qu'au (b), mais ici on écrit $p = (-1)^1.2^0.5^1.\frac{-p}{5}$ et on en déduit $(2,p/2) = -1$, etc.

(d) Cas où $p = 8k-1$. On prend $x = -1, y = p$, et l'on a $\left(\frac{-1,p}{2}\right) = -1$ etc.

3.3. Cas où $p = 8k+1$.

Dans les cas précédents, nous nous sommes efforcés de trouver des valeurs de a et b telles que $\left(\frac{a,b}{p}\right) = -1$, ce qui correspond à la nécessité, rencontrée dans la "Première démonstration", de prendre p' tel que $\left(\frac{p'}{q}\right) = -1$ (voir n° 1.3).

Mais, de la même manière, ce dernier cas offre des résistances à cette recherche. TATE le dit en ces termes: "I then tried to prove the law of reciprocity using the result on $K_2\mathbb{Q}$, and was surprised to find that there was still a non-trivial lemma needed"[1].

Ce lemme, c'est celui que nous avons exposé plus haut (n° 1.4): il existe $p' < p$ tel que $(p/p') = -1$, ce qui implique $(p,p'/p') = -1$. Dès lors, notre théorème se démontre encore par récurrence sur les nombres premiers: supposons que $\varepsilon_q = 1$ pour tous les nombres premiers $q < p$. Notre dernière "formule de produit" s'écrit alors :

$$\left(\frac{p,p'}{\infty}\right) = \left(\frac{p,p'}{2}\right)\left(\frac{p,p'}{p'}\right)\left(\frac{p,p'}{p}\right)^{\varepsilon_p}.$$

Or, il est clair que $\left(\frac{p,p'}{\infty}\right) = \left(\frac{p,p'}{2}\right) = 1$, et $\left(\frac{p,p'}{p'}\right) = -1$. D'où il découle encore que

$$\left(\frac{p,p'}{p}\right) = -1 \qquad \text{et} \qquad \varepsilon_p = 1.$$

C. Q. F. D.

[1] "Je tentai alors de prouver la loi de réciprocité en utilisant le résultat concernent $K_2\mathbb{Q}$, et je fus surpris de constater qu'un lemme non trivial était encore nécessaire".

Bibliographie

[1] Cuculière R. Histoire d'un théorème d'arithmétique : la loi de réciprocité quadratique, Publication de l'IREM, Paris-Nord, Université Paris-XII, 1930.

[2] Gauss C. F. Disquisitiones arithmeticae, Werke, Band I. Göttingen, 1870. Traduction française de Poullet-Delisle, Paris, 1807. Réédition Librairie Blanchard, 1979. Traduction anglaise de A. Clarke, Yale University Press, 1956.

[3] Lejeune-Dirichlet G. Über den ersten der von Gauss gegebenen Boweise des Reciprocitätsgesetzes in der Theorie der quadratischen Roste. J. für reine und angw. Math., t. 47, 1854, p. 139-150. Werke, Band II, p. 121-138. Berlin, 1897. Reprint Chelsea, 1969. Traduction française de Houel : Sur la première démonstration donnée par Gauss de la loi de réciprocité dans la théorie des résidus quadratiques, J. Math. pures et appl., 2e série, t. 4, 1859, p. 401-420.

[4] Milnor J. Introduction to algebraic K-theory, Princeton, Princeton University Press and University of Tokyo Press, 1971 (Annals of Mathematics Studies, 72).

[5] Serre J.-P. Cours d'arithmétique. Paris, Presses universitaires de France, 1970 (Collection SUP, "Le Mathématicien", 2).

[6] Tate J. Symbols in arithmetic, Actes du Congrès international des Mathématiciens [1970, Nice], Vol 1, p. 201-211. Paris, Gauthier. Villars, 1971.

[7] Tate J. The general reciprocity law, Mathematical developments arising from Hilbert problems, p. 311-322. Providence, American mathematical Society, 1976 (Proceedings of Symposia in pure Mathematics, 28, Part 2).