loi de réciprocité quadratique et le lemme de Gauss-Schering

SUR UNE GÉNÉRALISATION DES SYMBOLES DE LEGENDRE-JACOBI

par P. CARTIER (Strasbourg)

INTRODUCTION

Un théorème assez peu connu (Zolotareff, Frobenius) donne une interprétation des symboles de Legendre-Jacobi au moyen de la signature de permutations convenables. Cette interprétation suggère une généralisation de ces symboles, à laquelle nous consacrons dans ces pages une étude élémentaire. Les propriétés des symboles généralisés redonnent facilement les principaux résultats classiques de Legendre, Gauss et Jacobi et nous permettront d'étendre le théorème de Zolotareff-Frobenius au cas des corps de nombres algébriques. On peut utiliser les résultats de cette Note pour donner un exposé rapide des propriétés des symboles de Legendre-Jacobi, exposé qui différerait très peu de celui de Frobenius dans [2].

PREMIÈRE PARTIE
LA LOI DE RÉCIPROCITÉ QUADRATIQUE ET LE LEMME DE GAUSS-SCHERING

1. *Résumé des résultats classiques* (Legendre, Gauss, Jacobi).

Soient a et b deux entiers, avec $b > 0$. On dit que a est *reste quadratique modulo* b s'il existe deux entiers x et y tels que $x^2 = a + by$, autrement dit, si la classe de a est un carré dans l'anneau des entiers modulo b. Gauss note $a\ R\ b$ cette relation et $a\ N\ b$ sa négation. Soient p et q deux nombres premiers, distincts de 2 et distincts entre eux. La loi de réciprocité quadratique, conjecturée par Euler, démontrée partiellement par Legendre, et établie par Gauss en 1796, affirme qu'il n'y a que les quatre possibilités suivantes:

$$\left.\begin{matrix} p\ R\ q \text{ et } q\ R\ p \\ p\ N\ q \text{ et } q\ N\ p \end{matrix}\right\} \text{ si } p \textit{ ou } q \text{ est congru à 1 modulo 4,}$$

$$\left.\begin{matrix} p\ R\ q \text{ et } q\ N\ p \\ p\ N\ q \text{ et } q\ R\ p \end{matrix}\right\} \text{ si } p \textit{ et } q \text{ sont congrus à 3 modulo 4.}$$

Le symbole de Legendre $\left(\frac{a}{p}\right)$ est défini pour un nombre premier $p \neq 2$ et un entier a non divisible par p; il vaut 1 ou -1 selon que a est reste

quadratique modulo p ou non. L'introduction de ce symbole permet de condenser la loi de réciprocité en la formule

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

Jacobi a généralisé les symboles de Legendre de la manière suivante: soit b un entier positif impair, de la forme $p_1 \ldots p_h$ où les nombres premiers $p_1, \ldots, p_h$ sont nécessairement distincts de 2; si a est un entier étranger à b, il n'est divisible par aucun des nombres premiers $p_1, \ldots, p_h$ et l'on définit le symbole de Jacobi $\left(\frac{a}{b}\right)$ comme le nombre $\left(\frac{a}{p_1}\right) \ldots \left(\frac{a}{p_h}\right)$. On a $\left(\frac{a}{b}\right) = 1$ si a est reste quadratique modulo b, mais la réciproque n'est pas vraie, et la signification des symboles de Jacobi est moins évidente que pour ceux de Legendre.

Voici les principales propriétés des symboles de Jacobi:

A. *Propriétés de multiplicativité et de congruence.*

(I) Si b est impair et positif et a, a' étrangers à b, on a $\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$.

(II) Si b est impair et positif, a et a' étrangers à b et si $a \equiv a'$ mod. b, on a $\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$.

(III) Si b et b' sont impairs et positifs, et a étranger à b et b', on a $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$.

(IV) Si b et b' sont impairs et positifs, a étranger à b et b', a congru à 0 ou 1 modulo 4, et si $b \equiv b'$ mod. $|a|$, on a $\left(\frac{a}{b}\right) = \left(\frac{a}{b'}\right)$.

B. *Loi de réciprocité et compléments.*

(V) Si a et b sont impairs et positifs, et a étranger à b, on a $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$.

(VI) Si b est impair et positif, on a $\left(\frac{-1}{b}\right) = (-1)^{\frac{1}{2}(b-1)}$.

(VII) Si b est impair et positif, on a $\left(\frac{2}{b}\right) = 1$ ou -1 selon que b est congru modulo 8 à ± 1 ou à ± 3.

C. *Restes quadratiques.*

(VIII) Pour tout nombre premier $p \neq 2$, on a $\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)}$ mod. p.

(IX) Si $p \neq 2$ est premier, l'entier $\left(\frac{a}{p}\right)$ est égal à 1 ou -1 selon que a est ou non reste quadratique modulo p.

On peut étendre la définition des symboles de Jacobi en posant $(\frac{a}{-b}) = (\frac{a}{b})$ pour b positif impair et a étranger à b. Notons $\sigma(x)$ le signe d'un nombre x non nul, égal à $x/|x|$; on a alors l'expression la plus générale de la loi de réciprocité sous la forme

$$(2) \qquad \left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2} + \frac{\sigma(a)-1}{2}\cdot\frac{\sigma(b)-1}{2}},$$

où a et b sont deux entiers impairs de signe quelconque, avec a étranger à b. Nous laissons au lecteur le soin de modifier les propriétés (I) à (IV) pour couvrir ce cas plus général.

Les propriétés (III) et (IX) ci-dessus ne font que traduire la construction des symboles de Jacobi et en donnent donc une caractérisation axiomatique. Notons la généralisation suivante de (VI):

(VI′) Si b est impair et positif et a étranger à b, on a $(\frac{-a}{b}) = (-1)^{\frac{1}{2}(b-1)}(\frac{a}{b})$.

Une démonstration facile par récurrence sur le maximum de $|a|$ et b montre que les groupes de propriétés (II) + (IV) + (VI′) et (II) + (V) + (VI′) fournissent deux caractérisations axiomatiques des symboles de Jacobi.

En principe, la théorie des symboles de Jacobi ne contient rien de plus que celle des symboles de Legendre; en particulier, la loi générale de réciprocité (2) est une conséquence facile de (1). Mais le calcul effectif d'un symbole de Legendre par la formule de réciprocité oblige à de nombreuses factorisations en nombres premiers, et l'on sait que celles-ci sont ennuyeuses et longues pour des nombres un peu grands. Le lecteur pourra s'exercer à montrer par cette méthode que le symbole de Legendre $S = (\frac{-1148}{523})$ vaut -1, c'est-à-dire que la congruence $x^2 \equiv -1148$ mod. 523 n'a pas de solution (523 est premier). Voici à titre de comparaison le calcul par les symboles de Jacobi. On a $523 \equiv 3$ mod. 8, d'où $(\frac{2}{523}) = -1$ par (VII); on a $-1148 \equiv -102$ mod. 523, d'où $S = (\frac{-102}{523}) = (\frac{2}{523})(\frac{-51}{523}) = -(\frac{-51}{523})$ par (II) et (I). Comme on a $-51 \equiv 1$ mod. 4 et $523 \equiv 13$ mod. 51, on a $(\frac{-51}{523}) = (\frac{-51}{13})$ par (IV). Enfin, on a $-51 \equiv 1$ mod. 13 et donc $(\frac{-51}{13}) = (\frac{1}{13}) = 1$ par (II), d'où $S = -1$.

2. *Démonstrations de la loi de réciprocité par le lemme de Gauss.*

On sait que Gauss n'a pas donné moins de six (et même sept) démonstrations de la loi de réciprocité [3]. Nous nous intéressons ici à la troisième (1808) et à la cinquième (1818); elles reposent toutes deux sur le lemme de Gauss (1808) qui s'énonce comme suit: *étant donnés un nombre premier* p $\neq 2$ *et un entier* a *non divisible par* p, *notons* n *le nombre*

des entiers x *compris entre* 1 *et* (p−1)/2 *et tels que* −ax *soit congru modulo* p *à un entier compris entre* 1 *et* (p−1)/2; *on a alors* $(\frac{a}{p}) = (-1)^n$.

Nous allons donner une version simplifiée des deux démonstrations de Gauss. Les notations sont les suivantes: p et q sont deux nombres premiers, distincts de 2 et distincts entre eux; on pose $p = 2p' + 1$ et $q = 2q' + 1$, et l'on note R l'ensemble des couples d'entiers (x, y) avec $1 \leqq x \leqq p'$ et $1 \leqq y \leqq q'$; enfin, on note $|X|$ le nombre d'éléments d'un ensemble fini X.

Voici d'abord la troisième démonstration de Gauss, dans la présentation «géométrique» d'Eisenstein. On note $[t]$ la partie entière d'un nombre réel t, c'est-à-dire le plus grand entier majoré par t. Supposons que a soit entier et t non entier; on établit immédiatement la formule

$$[a-t] = a - [t] - 1. \tag{3}$$

Notons Y l'ensemble des entiers y compris entre 1 et $2q'$ et τ la permutation de Y qui transforme y en $q - y$; pour tout $y \in Y$, on pose $F(y) = (-1)^{[py/q]}$. Comme p est impair, la formule (3) où l'on fait $a = p$ et $t = py/q$ [1] donne

$$F(\tau(y)) = F(y) \qquad \text{pour tout } y \text{ dans } Y. \tag{4}$$

Or, tous les cycles de la permutation τ sont d'ordre deux, et le produit $\prod_{y \in S} F(y)$ a donc la même valeur pour toutes les parties S de Y rencontrant chaque cycle de τ en un point et un seul. On peut prendre pour S l'ensemble $\{1, 2, ..., q'\}$ ou l'ensemble $\{2, 4, ..., 2q'\}$, d'où la formule

$$\prod_{y=1}^{q'} F(y) = \prod_{y=1}^{q'} F(2y). \tag{5}$$

Soit y un entier compris entre 1 et q'; il existe un unique entier v compris entre $-q'$ et q' et congru à py modulo q; on peut donc poser $py = qu + v$, où u et v sont entiers et $|v| \leqq q'$. Comme q ne divise pas py [1], on a $v \neq 0$, et il est immédiat que $[2py/q]$ est égal à $2u$ ou $2u-1$ selon que l'on a $v > 0$ ou $v < 0$. Autrement dit, on a $F(2y) = 1$ si $v > 0$ et $F(2y) = -1$ si $v < 0$. Le lemme de Gauss entraîne alors la formule

$$\left(\frac{p}{q}\right) = \prod_{y=1}^{q'} F(2y). \tag{6}$$

Enfin, soit P l'ensemble des couples (x, y) appartenant à R et tels que $py > qx$; il est immédiat qu'on a $|P| = \sum_{y=1}^{q'} [py/q]$, d'où, par définition de F, la formule

$$(7) \qquad (-1)^{|P|} = \prod_{y=1}^{q'} F(y).$$

Les formules (5), (6) et (7) donnent $\left(\frac{p}{q}\right) = (-1)^{|P|}$. En échangeant les rôles de p et q, on trouve $\left(\frac{q}{p}\right) = (-1)^{|Q|}$ où Q se compose des couples (x, y) appartenant à R et tels que $py < qx$. Pour tout (x, y) dans R, on a $px \neq qy$ [1]; par suite, les ensembles P et Q forment une partition de R, d'où $|P| + |Q| = |R| = p'q'$; on a donc prouvé la formule de réciprocité $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{p'q'}$.

Nous exposons maintenant la cinquième démonstration de Gauss sous la forme très transparente due à Frobenius [2]. On a utilisé précédemment le fait que $py - qx$ est non nul pour tout couple (x, y) appartenant à R. Les inégalités suivantes

$$\begin{aligned} R_1&: \quad py - qx < -q/2 \\ R_2&: -q/2 < py - qx < 0 \\ R_3&: \quad 0 < py - qx < p/2 \\ R_4&: \quad p/2 < py - qx \end{aligned}$$

définissent donc une partition de l'ensemble R en quatre parties notées encore $R_1, \ldots, R_4$. Pour y donné compris entre 1 et q', l'inégalité R_2 ne peut avoir lieu que pour une valeur au plus de x et l'on a alors $1 \leqq x \leqq p'$; on a donc $\left(\frac{p}{q}\right) = (-1)^{|R_2|}$ par le lemme de Gauss. On établit de même la relation $\left(\frac{q}{p}\right) = (-1)^{|R_3|}$. Enfin, l'application $(x, y) \mapsto (p'+1-x, q'+1-y)$ est une bijection de R_1 sur R_4, d'où $|R_1| = |R_4|$. On a alors

$$p'q' = |R| = |R_1| + |R_2| + |R_3| + |R_4| \equiv |R_2| + |R_3| \mod 2,$$

d'où immédiatement la formule de réciprocité $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{p'q'}$.

3. *Démonstration du lemme de Gauss-Schering.*

Les démonstrations précédentes n'utilisent que le lemme de Gauss pour calculer $\left(\frac{a}{p}\right)$ et le résultat suivant: si x et y sont des entiers tels que $1 \leqq x \leqq p'$ et $1 \leqq y \leqq q'$, on a $py \neq qx$. Or, ce dernier fait ne nécessite pas que p et q soient premiers, mais simplement qu'ils soient étrangers (lemme d'Euclide). Les deux démonstrations de Gauss établissent donc la loi de réciprocité (V) pour les symboles de Jacobi, pourvu que l'on prouve la généralisation suivante du lemme de Gauss: *soient* b *un entier impair et positif et* a *un*

[1] Si x est un entier et y un entier compris entre 1 et q', on a $py \neq qx$: en effet, q est premier et ne divise pas le nombre premier $p \neq q$, ni le nombre $y < q$, donc il ne divise pas py.

entier étranger à b; *on a* $\left(\frac{a}{b}\right) = (-1)^{|A|}$ *où* A *est l'ensemble des entiers x compris entre* 1 *et* (b−1)/2 *et tels que* −ax *soit congru modulo* b *à un entier compris entre* 1 *et* (b−1)/2. C'est ce qu'a démontré Schering (éditeur des œuvres de Gauss) en 1876; nous allons donner un exposé simplifié de sa méthode [5].

Pour tout diviseur m de b, soit A_m l'ensemble défini de manière analogue à A, au remplacement près de b par m; on note aussi B_m l'ensemble des entiers compris entre 1 et $(m-1)/2$ et étrangers à m. On montre facilement que tout élément de A s'écrit de manière unique sous la forme $\frac{b}{m}.x$ où m est un diviseur de b et x un élément de $A_m \cap B_m$;
posant $\eta(a, m) = |A_m \cap B_m|$, on a donc

$$|A| = \sum_{m|b} \eta(a, m). \tag{8}$$

L'argument suivant est une extension de celui par lequel Gauss établit son lemme. Soit m un diviseur de b. Il existe une permutation u de B_m et une fonction ε sur B_m à valeurs dans $\{1, -1\}$ caractérisées par la congruence

$$ax \equiv \varepsilon(x) \,.\, u(x) \quad \text{mod. } m \quad \text{pour tout } x \in B_m. \tag{9}$$

Or, $|B_m|$ est égal à $\frac{1}{2}\varphi(m)$, où $\varphi(m)$ est l'indicateur d'Euler bien connu; comme u est une permutation de B_m, on a $\prod_{x \in B_m} x = \prod_{x \in B_m} u(x)$; enfin, on a $\varepsilon(x) = -1$ si et seulement si x appartient à $A_m \cap B_m$. Multipliant les congruences (9), on obtient après simplification [2]

$$a^{\frac{1}{2}\varphi(m)} \equiv (-1)^{\eta(a, m)} \quad \text{mod. } m. \tag{10}$$

Supposons $m \neq 1$ et soit p un diviseur premier de m; on pose $m = p^f.m'$ avec m' non divisible par p et $f \geqslant 1$. Or, on a $\frac{1}{2}\varphi(m) = \frac{p-1}{2} \cdot p^{f-1}.\varphi(m')$, p est impair et $\varphi(m')$ est pair si $m' \neq 1$; la congruence (10) entraîne une congruence analogue modulo p, et l'on a $a^{\frac{1}{2}(p-1)} \equiv \left(\frac{a}{p}\right)$ mod. p par le lemme d'Euler (cf. (VIII)). De tout ceci, on déduit

$$(-1)^{\eta(a, m)} = \begin{cases} \left(\frac{a}{p}\right) & \text{si } m = p^f \text{ avec } p \text{ premier et } f \geqslant 1, \\ 1 & \text{dans les autres cas.} \end{cases} \tag{11}$$

---

[2] Le résultat le plus général de ce type est le suivant: soient G un groupe *commutatif* fini et G' un sous-groupe de G; l'homomorphisme de transfert de G dans G' transforme tout $a \in G$ en $a^{|G/G'|}$. Ici, G est le groupe multiplicatif des éléments inversibles de l'anneau des entiers modulo m, et $G' = \{1, -1\}$.

Posons alors $b = p_1^{f_1} \dots p_r^{f_r}$, les nombres premiers $p_1, \dots, p_r$ étant distincts et les exposants $f_1, \dots, f_r$ strictement positifs. De (8) et (11), on déduit sans peine

$$(-1)^{|A|} = \left(\frac{a}{p_1}\right)^{f_1} \dots \left(\frac{a}{p_r}\right)^{f_r} = \left(\frac{a}{b}\right),$$

c'est-à-dire le résultat de Schering.

Deuxième partie

Symboles généralisés

Il est assez tentant de renverser l'ordre des démonstrations précédentes et de *définir* le symbole de Jacobi par le lemme de Gauss-Schering; les raisonnements de la première partie montrent comment établir la loi de réciprocité (V) à partir de cette définition, et il ne serait pas difficile d'obtenir avec cette définition les propriétés (I) à (IX) des symboles de Jacobi. Un tel exposé serait assez artificiel, mais il se présente heureusement une possibilité bien plus satisfaisante. Notons $\mathbf{Z}_b$ le groupe additif des entiers modulo b et u_a l'automorphisme de $\mathbf{Z}_b$ défini par la multiplication par a; par des raison-o nements élémentaires exposés plus bas, on montre que le lemme de Gauss-Schering équivaut au résultat suivant: $\left(\frac{a}{b}\right)$ *est la signature de la permutation* u_a *de l'ensemble fini* $\mathbf{Z}_b$. Ce théorème a été prouvé par Zolotareff [6] en 1872 pour le cas où b est premier, et généralisé immédiatement par Frobenius [2]; il suggère immédiatement la définition suivante des symboles $\left(\frac{u}{G}\right)$.

4. *Etudes des symboles* $\left(\frac{u}{G}\right)$.

Soit G un groupe commutatif fini, d'ordre impair $2n + 1$, dont l'opération est notée additivement. Pour toute partie X de G, on note X^- l'ensemble des éléments $-x$ de G, pour x parcourant X. Pour tout automorphisme u de G, on note $\left(\frac{u}{G}\right)$ la signature de la permutation u de l'ensemble fini G. La multiplicativité des signatures entraîne immédiatement

$$\left(\frac{uv}{G}\right) = \left(\frac{u}{G}\right)\left(\frac{v}{G}\right) \tag{12}$$

pour deux automorphismes u et v de G.

L'application $x \mapsto -x$ est un automorphisme de G que l'on notera simplement -1. Pour tout $x \in G$, on a $(2n+1).x = 0$, et l'on ne peut donc avoir $x = -x$ que lorsque $x = 0$. Il s'ensuit que -1 a un cycle de longueur