Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 16 (1970)

Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: SUR UNE GÉNÉRALISATION DES SYMBOLES DE LEGENDRE-JACOBI

Autor: Cartier, P.

Kapitel: Symboles généralisés

DOI: https://doi.org/10.5169/seals-43850

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

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

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

1 et n cycles de longueur 2, et par suite sa signature est $(-1)^n$. Autrement dit, on a la formule

$$(13) \qquad \left(\frac{-1}{G}\right) = (-1)^{\frac{1}{2}(|G|-1)}.$$

Nous passons maintenant à une *généralisation du lemme de Gauss-Schering*. On appelle demi-*système* toute partie S de $G^* = G - \{0\}$ qui rencontre chaque cycle de -1 dans G^* en un point et un seul; il revient au même de dire que les ensembles S, S^- et $\{0\}$ forment une partition de G. Par exemple, si G est le groupe additif des entiers modulo b (b est un entier impair et positif), l'ensemble des classes modulo b des entiers compris entre 1 et $(b-1)/2$ est un demi-système. Nous allons établir la formule

$$(14) \qquad \left(\frac{u}{G}\right) = (-1)^{|u(S) \cap S^-|},$$

où u est un automorphisme de G et S un demi-système. La démonstration est analogue à celle de Frobenius [2, page 630].

On a $u(0) = 0$, donc $(\frac{u}{G})$ est aussi la signature de la permutation u^* de G^* induite par u. Posons $S = \{x_1, ..., x_n\}$ et énumérons les éléments de G^* sous la forme

$$x_1, x_2, \ldots, x_{n-1}, x_n, \; -x_n, \; -x_{n-1}, \ldots, \; -x_2, \; -x_1;$$

si x et y sont deux éléments de G^*, la relation $x < y$ signifie que x précède y dans la liste précédente. L'ordre choisi sur G^* est donc tel que $x < y$ entraîne $-x > -y$ et que S se compose des $x \in G^*$ tels que $x < -x$. On appelle inversion de u^* un couple (x, y) d'éléments de G^* tel que $x < y$ et $u(x) > u(y)$. On note I l'ensemble de ces inversions, de sorte qu'on a

$$(15) \qquad \left(\frac{u}{G}\right) = (-1)^{|I|}$$

d'après l'une des définitions usuelles de la signature. Par ailleurs, on a $u(-x) = -u(x)$, et les propriétés de la relation d'ordre sur G^* montrent que l'application $(x, y) \mapsto (-y, -x)$ est une permutation σ d'ordre 2 de I; par conséquent, $|\mathrm{I}|$ a même parité que le nombre m des éléments de I invariants par σ et l'on a donc $(\frac{u}{G}) = (-1)^m$ d'après (15). Or m est le nombre des couples $(x, -x)$ avec $x < -x$ et $u(x) > -u(x)$, c'est-à-dire $x \in S$ et $u(x) \in S^-$; on a donc $n = |u(S) \cap S^-|$, d'où (14).

Nous établissons maintenant *la deuxième formule de multiplicativité.* On note G' un sous-groupe de G et G'' le groupe-quotient G/G'; on se donne aussi un automorphisme u de G laissant stable G'. On note u' l'automorphisme de G' induit par u et u'' l'automorphisme de G'' déduit de u par passage au quotient. Je dis que l'on a

$$(16) \qquad \binom{u}{G} = \binom{u'}{G'}\binom{u''}{G''}.$$

Notons π l'homomorphisme canonique de G sur G'', S' un demi-système dans G' et S'' un demi-système dans G''; on pose $T = \pi^{-1}(S'')$ et $S = S' \cup T$. Il est immédiat que S est un demi-système dans G et que les ensembles $u'(S') \cap S'^-$ et $u(T) \cap T^-$ forment une partition de $u(S) \cap S^-$, d'où

$$(17) \qquad |u(S) \cap S^-| = |u'(S') \cap S'^-| + |u(T) \cap T^-|.$$

Par ailleurs, l'ensemble $u(T) \cap T^-$ est la réunion des classes modulo G' appartenant à $u''(S'') \cap S''^-$; l'ordre d'une telle classe est égal à $|G'|$, et comme $|G'|$ divise le nombre impair $|G|$, il est impair. Ceci montre que $|u(T) \cap T^-|$ a même parité que $|u''(S'') \cap S''^-|$, et la formule (16) résulte alors de (14) et (17).

Mentionnons un cas particulier important de (16); c'est celui où le groupe G est somme directe de deux sous-groupes G' et G'', où u' est un automorphisme de G' et u'' un automorphisme de G'', et où u est l'automorphisme de G qui induit u' sur G' et u'' sur G''. La démonstration s'obtient au moyen de l'isomorphisme bien connu du sous-groupe G'' de G sur le groupe-quotient G/G' qui transforme u'' en l'automorphisme déduit de u par passage au quotient. On peut aussi déduire ce cas du résultat suivant: *soient* X' *et* X'' *deux ensembles finis,* s' *une permutation de* X' *et* s'' *une permutation de* X''; *on pose* $\mathrm{X} = \mathrm{X}' \times \mathrm{X}''$ *et l'on note* s *la permutation* $(\mathrm{x}', \mathrm{x}'') \mapsto (\mathrm{s}'(\mathrm{x}'), \mathrm{s}''(\mathrm{x}''))$ *de* X. *Si* ε (resp. ε', ε'') *est la signature de* s (resp. s', s''), *on a* $\varepsilon = \varepsilon'^{|X''|} . \varepsilon''^{|X'|}$. La démonstration est facile et laissée au lecteur.

2. *Restes quadratiques dans les corps finis.*

Dans tout ce numéro, on note $\mathbf{F}$ *un corps fini, et* q *le nombre de ses éléments, que l'on suppose impair*; il revient au même de supposer que la caractéristique p de $\mathbf{F}$ est différente de 2. On a $q = p^f$, où f est le degré de $\mathbf{F}$ sur le sous-corps $\mathbf{F}_p$ formé des entiers modulo p. Si a est un élément non nul de $\mathbf{F}$, la multiplication par a est un automorphisme du groupe additif $\mathbf{F}^+$ de $\mathbf{F}$, dont la signature sera notée $\left(\frac{a}{\mathbf{F}}\right)$. la formule (12) du n° 4 entraîne alors

$$\left(\frac{ab}{\mathbf{F}}\right) = \left(\frac{a}{\mathbf{F}}\right)\left(\frac{b}{\mathbf{F}}\right) \quad \text{pour } a, b \text{ non nuls dans } \mathbf{F}. \tag{18}$$

Nous établissons maintenant la formule [3]

$$\left(\frac{ab}{\mathbf{F}}\right) = a^{\frac{1}{2}(q-1)} \qquad \text{pour } a \text{ non nul dans } \mathbf{F}. \tag{19}$$

La démonstration est une extension de celle que Gauss a utilisée pour démontrer son lemme. On choisit un demi-système S dans $\mathbf{F}^+$; tout élément non nul de $\mathbf{F}$ s'écrit de manière unique sous la forme $\varepsilon\, x$ avec $\varepsilon \in \{1, -1\}$ et $x \in S$. Il existe donc une permutation u de S et une application ε de S dans $\{1, -1\}$ telles que $ax = \varepsilon(x)\, u(x)$ pour tout $x \in S$; multipliant ces égalités entre elles et tenant compte de la relation $\prod_{x \in S} u(x) = \prod_{x \in S} x$, on trouve après simplification $a^{|S|} = \prod_{x \in S} \varepsilon(x)$. Or, on a $|S| = ½(q-1)$ et l'on a $\varepsilon(x) = -1$ si et seulement si $ax \in S^-$. La formule (14) achève alors la démonstration.

La signification des symboles $\left(\frac{a}{\mathbf{F}}\right)$ est la suivante: *ce nombre est égal à* 1 *ou* -1 *selon que* a *est ou non un carré dans le corps* $\mathbf{F}$. Rappelons que le groupe multiplicatif du corps $\mathbf{F}$ est cyclique d'ordre $q-1$; nous choisirons un générateur z de ce groupe et poserons $q-1 = 2n$. Alors les éléments non nuls de $\mathbf{F}$ peuvent s'énumérer comme suit

$$\begin{gathered} z^0, z^2, \ldots, z^{2(n-1)} \\ z^1, z^3, \ldots, z^{2(n-1)+1}, \end{gathered}$$

la première ligne contenant les carrés et la deuxième les non-carrés. Comme (18) entraîne $\left(\frac{z^{2i}}{\mathbf{F}}\right) = 1$ et $\left(\frac{z^{2i+1}}{\mathbf{F}}\right) = \left(\frac{z}{\mathbf{F}}\right)$, il nous suffira de prouver la relation $\left(\frac{z}{\mathbf{F}}\right) = -1$.

A. *Première démonstration* (Euler): on a $z^n \neq 1$ et $(z^n)^2 = z^{2n} = 1$ car z est d'ordre $2n$; on a donc $z^n = -1$, d'où $\left(\frac{z}{\mathbf{F}}\right) = z^{\frac{1}{2}(q-1)} = z^n = -1$ d'après (19).

B. *Deuxième démonstration* (Zolotareff): la multiplication par z dans $\mathbf{F}$ transforme 0 en lui-même et permute circulairement les $2n$ éléments

[3] Dans cette formule, on considère $\left(\frac{a}{\mathbf{F}}\right)$ comme un élément de $\mathbf{F}$, en identifiant les entiers 1 et —1 à leurs images naturelles dans le corps $\mathbf{F}$.

$z^o, z^1, \ldots, z^{2n-1}$, donc c'est une permutation impaire, et $\left(\frac{z}{\mathbf{F}}\right) = -1$ d'après la définition de $\left(\frac{z}{\mathbf{F}}\right)$ comme signature.

Nous considérons maintenant un espace vectoriel V de dimension finie d sur le corps $\mathbf{F}$ et un automorphisme u de V; on note det u le déterminant de u. J'affirme que l'on a

$$\left(\frac{u}{V}\right) = \left(\frac{\det u}{\mathbf{F}}\right). \tag{20}$$

On ne restreint pas la généralité en supposant qu'on a $V = \mathbf{F}^d$. D'après un résultat classique et facile [4], le groupe des automorphismes de V est engendré par les éléments de la forme suivante

$$D_{a_1, \ldots, a_d}(x_1, \ldots, x_d) = (a_1 x_1, \ldots, a_d x_d)$$

$$S_i(x_1, \ldots, x_d) = (x_1, \ldots, x_{i-1}, x_{i+1}, x_i, x_{i+2}, \ldots, x_d)$$

$$T_i(x_1, \ldots, x_d) = (x_1, \ldots, x_{i-1}, x_i + x_{i+1}, x_{i+1}, x_{i+2}, \ldots, x_d),$$

où $a_1, \ldots, a_n$ sont des éléments non nuls de $\mathbf{F}$ et i un entier compris entre 1 et $d-1$. Or, les deux membres de la formule (20) dépendent multiplicativement de u d'après les relations (12) et (18); il suffit donc d'examiner les cas où u est de l'une des formes $D_{a_1,\ldots,a_d}$, S_i et T_i.

a) *Le cas de* $D_{a_1,\ldots,a_d}$: posons $G_1 = \ldots = G_d = \mathbf{F}^+$ et notons u_i l'automorphisme de G_i défini par la multiplication par a_i; on a donc

$$V = G_1 \times \ldots \times G_d \quad \text{et} \quad u(x_1, \ldots, x_d) = (u_1(x_1), \ldots, u_d(x_d))$$

pour $x_1 \in G_1, \ldots, x_d \in G_d$. De la formule (16), on déduit par récurrence sur d la formule $\left(\frac{u}{V}\right) = \left(\frac{u_i}{G_i}\right) \ldots \left(\frac{u_d}{G_d}\right)$; or on a $\left(\frac{n1}{u_i}\right) = \left(\frac{a_i}{\mathbf{F}}\right)$ par définition, et le déterminant de u est $a_1 \ldots a_d$, d'où (20).

b) *Le cas de* S_i: dans ce cas, u échange les coordonnées d'indice i et $i+1$; c'est une permutation d'ordre 2, qui possède q^{d-1} points fixes, et a donc la même parité que $\frac{1}{2}(q^d - q^{d-1}) = \frac{1}{2}(q-1)q^{d-1}$. Comme q est impair, on a donc $\left(\frac{u}{V}\right) = (-1)^{\frac{1}{2}(q-1)} = \left(\frac{-1}{\mathbf{F}}\right)$, et le déterminant de u est égal à -1; on a prouvé (20).

---

[4] Ce résultat équivaut à un lemme classique sur les matrices inversibles: une telle matrice peut être ramenée à la forme diagonale au moyen d'un nombre fini d'applications des transformations du type suivant:

a) permuter deux colonnes;

b) ajouter à une colonne un multiple d'une autre.

c) *Le cas de* T_i: on a alors $u^p = 1$, d'où $(\frac{u}{V})^p = (\frac{u^p}{V}) = 1$; comme p est impair, on a donc $(\frac{u}{V}) = 1$. Par ailleurs, le déterminant de u est 1, d'où (20). Ceci achève la démonstration de (20).

Remarque : on conserve les notations **F** et V précédentes, et l'on note V^* l'ensemble des éléments non nuls de V. Notons aussi $\mathbf{F}^*$ le groupe multiplicatif des éléments non nuls de **F**. Le groupe $\mathbf{F}^*$ agit sans point fixe sur V^* par multiplication, et son action commute à celle du groupe $GL(V)$ des automorphismes de l'espace **F**-vectoriel V.

Dans une Note antérieure (*Sur une généralisation du transfert en théorie des groupes*, ce même journal, pp. 49-57), nous avons étudié la situation générale suivante: X est un ensemble fini, G et A sont deux groupes agissant sur X; on suppose que A est commutatif et agit sans point fixe sur X, et que les actions de G et A commutent. On a défini un homomorphisme Φ_A de G dans A par la construction suivante: on choisit un ensemble $S \subset X$ tel que tout élément de X s'écrive de manière unique sous la forme $a \,.\, s$ avec $a \in A$ et $s \in S$; pour tout $g \in G$, il existe une permutation σ de S et une application α de S dans A telles que $g\,(s) = \alpha\,(s)\,.\,\sigma(s)$ pour tout $s \in S$; on a alors $\Phi_A(g) = \prod_{s \in S} \alpha\,(s)$, ce produit ne dépendant pas du choix de S. Si A' est un sous-groupe de A, on peut définir de manière analogue un homomorphisme $\Phi_{A'}$ de G dans A', et l'on vérifie facilement que l'on a (*) $\Phi_{A'}\,(g) = \Phi_A\,(g)^{|A/A'|}$ pour tout $g \in G$.

Lorsque l'on a $X = V^*$, $G = GL(V)$ et $A = \mathbf{F}^*$, on a $\Phi_{\mathbf{F}^*}\,(g) = \det g$ pour tout $g \in GL(V)$. Il suffit de vérifier cette assertion lorsque g est de l'une des formes $D_{a_1,\ldots,a_n}$, S_i et T_i; la vérification est élémentaire dans chaque cas.

Prenons pour A' le sous-groupe $\{1, -1\}$ de $\mathbf{F}^*$. Le lemme de Gauss-Schering généralisé entraîne $(\frac{g}{V}) = \Phi_{A'}\,(g)$ pour tout $g \in GL(V)$, d'où

$$\begin{pmatrix} g \\ V \end{pmatrix} = \Phi_A(g)^{|\mathbf{F}^*/A'|} = (\det g)^{\frac{1}{2}(q-1)} = \begin{pmatrix} \det u \\ \mathbf{F} \end{pmatrix},$$

d'après (*). On a redémontré la formule (20).

Nous prenons cette fois pour A' le groupe multiplicatif $\mathbf{F}'^*$ d'un sous-corps $\mathbf{F}'$ de **F**, à q' éléments. Soit g un automorphisme de l'espace **F**-vectoriel V; on peut considérer V comme un $\mathbf{F}'$-espace vectoriel V' et g comme un automorphisme g' de V'. La propriété (*) ci-dessus entraîne alors $\det g' = (\det g)^{(q-1)/(q'-1)}$. On notera que la norme d'un élément a de **F** par rapport à $\mathbf{F}'$ est $a^{(q-1)/(q'-1)}$, donc $\det g'$ est la norme de $\det g$. Ce dernier résultat ne suppose pas **F** fini, il est valable pour un espace vectoriel V de dimension finie sur un corps **F** de degré fini sur un sous-corps $\mathbf{F}'$.

3. *Retour sur les symboles de Jacobi.*

Nous résumons d'abord les résultats des deux derniers numéros. On note G un groupe commutatif, d'ordre fini impair, et **F** un corps fini de caractéristique $\neq 2$.

A. *Propriétés de multiplicativité.*

A_1) Si u et v sont des automorphismes de G, on a $\left(\frac{uv}{G}\right) = \left(\frac{u}{G}\right)\left(\frac{v}{G}\right)$.

A_2) Soient G' un sous-groupe de G, u un automorphisme de G tel que $u(G') = G'$, u' et u'' les automorphismes de G' et $G'' = G/G'$ respectivement déduits de u. On a $\left(\frac{u}{G}\right) = \left(\frac{u'}{G'}\right)\left(\frac{u''}{G''}\right)$.

A_3) On suppose que le groupe G est somme directe des sous-groupes $G_1, \ldots, G_n$; pour $1 \leqq i \leqq n$, soit u_i un automorphisme de G_i, et soit u l'automorphisme de G induisant u_1 dans $G_1, \ldots, u_n$ dans G_n. On a $\left(\frac{u}{G}\right) = \left(\frac{u_1}{G_1}\right) \cdots \left(\frac{u_n}{G_n}\right)$.

B. *Lemme de Gauss généralisé.*

B_1) Soit S une partie de G ne contenant pas 0, et telle que pour tout $x \in G$, on ait soit $x \in S$, soit $-x \in S$ (mais non les deux). Soient u un automorphisme de G et m le nombre des éléments x de S tels que $-u(x) \in S$. On a alors $\left(\frac{u}{G}\right) = (-1)^m$.

B_2) On a $\left(\frac{-1}{G}\right) = (-1)^{\frac{1}{2}(|G|-1)}$.

C. *Corps finis et restes quadratiques.*

C_1) On a $\left(\frac{a}{\mathbf{F}}\right) = a^{\frac{1}{2}(|\mathbf{F}|-1)}$ pour tout $a \neq 0$ dans **F**.

C_2) On a $\left(\frac{a}{\mathbf{F}}\right) = 1$ ou -1 selon que a est ou non un carré dans **F**.

C_3) Soient V un espace vectoriel de dimension finie sur **F**, et u un automorphisme de V. On a $\left(\frac{u}{V}\right) = \left(\frac{\det u}{\mathbf{F}}\right)$.

Convenons maintenant de *définir* les symboles de Jacobi par $\left(\frac{a}{b}\right) = \left(\frac{u_a}{\mathbf{Z}_b}\right)$: on note b un entier impair et positif, $\mathbf{Z}_b$ le groupe additif des entiers modulo b, a un entier étranger à a, et u_a la multiplication par a dans $\mathbf{Z}_b$. En particulier, si p est un nombre premier différent de 2, $\mathbf{F}_p$ le corps des entiers modulo p et a un entier non divisible par p, on a $\left(\frac{a}{p}\right) = \left(\frac{\bar{a}}{\mathbf{F}_p}\right)$ où $\bar{a}$ est la classe de a modulo p. Les propriétés (I), (II), (VI), (VIII) et (IX) des symboles de Jacobi résultent alors immédiatement des propriétés des symboles $(\frac{u}{G})$; on a montré au n° 2 de la première partie comment déduire la loi de réciprocité (V) du lemme de Gauss-Schering. Il reste à examiner (III), (IV) et (VII).

Ad (III): notons b' et b'' deux entiers impairs et positifs, et a un entier étranger à b' et b''. On pose $G = \mathbf{Z}_{b'b''}$ et l'on définit l'automorphisme u de G par $u(x) = ax$. Soit G' le sous-groupe cyclique d'ordre b' de G engendré par la classe modulo $b'b''$ de b''; le groupe quotient $G'' = G/G'$ est cyclique d'ordre b''. Comme on a $u(G') = G'$, on peut appliquer (A_2); on a évidemment $(\frac{u}{G}) = (\frac{a}{b'b''})$, $(\frac{u'}{G'}) = (\frac{a}{b'})$ et $(\frac{u''}{G''}) = (\frac{a}{b''})$, d'où $(\frac{a}{b'b''}) = (\frac{a}{b'})(\frac{a}{b''})$ ([5]).

Ad (VII): soit $b = 2b' + 1$ un nombre impair et positif. Représentons chaque classe modulo b par le plus petit entier positif qu'elle contient. L'automorphisme u de $\mathbf{Z}_b$ défini par $u(x) = 2x$ est alors la permutation

$$u = \begin{pmatrix} 1 & 2 & \ldots & b' & b'+1 & b'+2 & \ldots & 2b' \\ 2 & 4 & \ldots & 2b' & 1 & 3 & \ldots & 2b'-1 \end{pmatrix}$$

dont le nombre d'inversions est égal à

$$1 + 2 + \ldots + (b'-1) + b' = \tfrac{1}{2}b'(b'+1) = (b^2-1)/8,$$

d'où $(\frac{2}{b}) = (-1)^{(b^2-1)/8}$; ceci établit (VII) ([6]).

Ad (IV): soient b et b' deux entiers impairs et positifs, et a un entier étranger à b et b'. Supposons d'abord $a \equiv 1$ mod. 4 et $b \equiv b'$ mod. $|a|$. La loi de réciprocité entraîne $(\frac{a}{b}) = (\frac{b}{|a|})$ et $(\frac{a}{b'}) = (\frac{b'}{|a|})$, et comme on a évidemment $(\frac{b}{|a|}) = (\frac{b'}{|a|})$, on a prouvé $(\frac{a}{b}) = (\frac{a}{b'})$. Supposons maintenant qu'on ait $b \equiv b'$ mod. $4\,|a|$ et prouvons la formule $(\frac{a}{b}) = (\frac{a}{b'})$. Or, on a $(\frac{xy}{b}) = (\frac{x}{b})(\frac{y}{b})$ et pour tout entier impair x, l'un des nombres x et $-x$ est congru à 1 modulo 4. Il suffit donc d'examiner les cas $a \equiv 1$ mod. 4 (qui vient d'être traité), $a = -1$ (qui résulte de (VI)) et $a = 2$ (qui résulte de (VII)).

---

[5] Le raisonnement qui établit (A_2) peut s'utiliser dans la théorie classique de la manière suivante. On suppose les symboles de Jacobi définis à partir de ceux de Legendre, et le lemme de Gauss démontré. On admet aussi que dans l'énoncé du lemme de Schering, on peut remplacer l'ensemble des entiers 1, 2, ..., b' par n'importe quel demi-système modulo b (ce que Gauss et Schering savaient). Le raisonnement de (A_2) montre alors que si le lemme de Schering est vrai pour b_1 et b_2, il est vrai pour $b = b_1 b_1$. Par récurrence sur b, on se ramène donc au cas où b est premier, c'est-à-dire au lemme de Gauss. Cette démonstration du lemme de Schering est nettement plus simple que celle de cet auteur.

[6] Une autre méthode est la suivante: des deux nombres impairs b et $b + 2$, l'un est congru à 1 modulo 4, d'où $(\frac{b+2}{b}) = (\frac{b}{b+2})$ par la loi de réciprocité. On en déduit $(\frac{2}{b}) = (\frac{-2}{b+2}) = (\frac{-1}{b+2})(\frac{2}{b+2}) = (-1)^{\frac{1}{2}(b+1)}(\frac{2}{b+2})$, d'où $(\frac{2}{b}) = (-1)^{(b^2-1)/8}$ par récurrence sur b.

4. *Extension aux corps de nombres algébriques.*

On note A l'anneau des entiers d'un corps de nombres algébriques, de degré fini sur le corps des nombres rationnels. On note $\mathfrak{a}$, $\mathfrak{b}$, ... des indéaux de A; si $\mathfrak{a}$ est un idéal, on note $\mathrm{N}(\mathfrak{a})$ le nombre des éléments de l'anneau quotient $A/\mathfrak{a}$. On note $\mathfrak{p}$ un idéal premier de A tel que $\mathrm{N}(\mathfrak{p})$ soit impair.

A. *Symboles de restes quadratiques.*

Soient $\mathfrak{a}$ un idéal tel que $\mathrm{N}(\mathfrak{a})$ soit impair et x un élément de A. On dit que x est étranger à $\mathfrak{a}$ si l'on a $A = Ax + \mathfrak{a}$, c'est-à-dire si la classe $\bar{x}$ de x modulo $\mathfrak{a}$ est un élément inversible de l'anneau $A/\mathfrak{a}$. S'il en est ainsi, la multiplication par $\bar{x}$ définit une permutation de l'ensemble fini $A/\mathfrak{a}$, dont la signature sera notée $\left(\frac{x}{\mathfrak{a}}\right)$. Les propriétés des symboles $\left(\frac{u}{G}\right)$ entraînent immédiatement les règles suivantes:

$$\left(\frac{xy}{\mathfrak{a}}\right) = \left(\frac{x}{\mathfrak{a}}\right)\left(\frac{y}{\mathfrak{a}}\right) \tag{21}$$

$$\left(\frac{x}{\mathfrak{a}\mathfrak{b}}\right) = \left(\frac{x}{\mathfrak{a}}\right)\left(\frac{x}{\mathfrak{b}}\right) \tag{22}$$

$$\left(\frac{x}{\mathfrak{p}}\right) \equiv x^{\frac{1}{2}(N(\mathfrak{p})-1)} \qquad \text{mod. } \mathfrak{p} \tag{23}$$

$$\left(\frac{x}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{s'il existe } y \text{ dans } A \text{ avec } y^2 \equiv x \text{ mod. } \mathfrak{p}, \\ -1 & \text{dans les autres cas.} \end{cases} \tag{24}$$

La démonstration de (22) utilise l'isomorphisme des groupes $A/\mathfrak{a}$ et $\mathfrak{b}/\mathfrak{a}\mathfrak{b}$.

Les règles (22) et (24) donnent une caractérisation des symboles $\left(\frac{x}{\mathfrak{a}}\right)$, qui coïncident donc avec les symboles de restes quadratiques usuels (Hilbert, Hecke). Nous avons ainsi étendu au cas des corps de nombres algébriques le théorème de Zolotareff-Frobenius.

B. *Déterminants généralisés* ([7]).

Notons M un A-module de type fini, annulé par une puissance de l'idéal premier $\mathfrak{p}$ et $\mathbf{F}$ le corps fini $A/\mathfrak{p}$. Nous associerons à tout endomorphisme u de M un élément $D(u)$ de $\mathbf{F}$, qui doit être considéré comme un déterminant

[7] A l'exception de la formule $\left(\frac{u}{M}\right) = \left(\frac{D(u)}{\mathbf{F}}\right)$ les résultats qui suivent sont valables sous les hypothèses plus générales: A est un anneau commutatif, $\mathfrak{p}$ est un idéal maximal de A engendré par un nombre fini d'éléments, M est un A-module de type fini.

généralisé de u. Pour tout entier positif i, le A-module $M_i = \mathfrak{p}^i M / \mathfrak{p}^{i+1} M$ est annulé par $\mathfrak{p}$, donc peut être considéré comme un espace vectoriel sur $\mathbf{F}$, dont la dimension est finie. Comme u laisse stable chacun des sous-modules $\mathfrak{p}^i M$ de M, il définit un endomorphisme u_i de M_i, dont le déterminant sera noté $D_i(u)$. D'après les hypothèses faites, il existe un entier $N \geqslant 0$ tel que $M_i = 0$ pour $i \geqslant N$. On posera $D(u) = \prod_{i=0}^{N-1} D_i(u)$(définition indépendante de N).

Lorsque M est annulé par $\mathfrak{p}$, on peut le considérer comme un espace vectoriel sur $\mathbf{F}$, et l'on a $D(u) = \det u$ dans ce cas. Il est clair que si u et v sont deux endomorphismes de M, on a $D(uv) = D(u) \,.\, D(v)$, et enfin si $D(u)$ est non nul si et seulement u est un automorphisme de M. Les propriétés (A_2) et (C_3) du n° 3 et une récurrence immédiate sur N entraînent la formule $\left(\frac{u}{M}\right) = \left(\frac{D(u)}{\mathbf{F}}\right)$ pour tout automorphisme u de M.

On peut établir pour les déterminants généralisés une propriété analogue à la propriété de multiplicativité (A_2): si u est un automorphisme de M, M' un sous-module de M tel que $u(M') = M'$, u' (resp. u'') l'automorphisme de M' (resp. M/M') déduit de u, on a $D(u) = D(u') \,.\, D(u'')$. En bref, la démonstration est la suivante. On traite d'abord le cas où M est annulé par $\mathfrak{p}$, ce qui ramène à une propriété connue des déterminants: si T est une matrice partitionnée en $\left(\begin{smallmatrix} U & V \\ O & W \end{smallmatrix}\right)$, on a $\det T = \det U \,.\, \det W$. Appelons sous-groupe stable de M tout sous-module de M stable par u. On peut prolonger la suite $(M, \mathfrak{p}M, \ldots, \mathfrak{p}^N M)$ de sous-groupes stables en une suite de Jordan-Hölder $(P_o, P_1, \ldots, P_r)$. Chaque module $Q_j = P_j / P_{j+1}$ (pour $0 \leqq j < r$) est annulé par $\mathfrak{p}$, et si v_j est l'automorphisme de Q_j déduit de u, on a $D(u) = \prod_{j=0}^{r-1} \det v_j$ par le cas déjà étudié. Il existe par ailleurs un entier s tel que $0 \leqq s \leqq r$ et une suite de Jordan-Hölder $(P_0', P_1', \ldots, P_r')$ de sous-groupes stables de M, telle que $P_s' = M'$. D'après le théorème de Jordan-Hölder, on a $\prod_{j=0}^{r-1} \det v_j = \prod_{j=0}^{r-1} \det v_j'$ si v_j' est l'automorphisme de $Q_j' = P_j' / P_{j+1}'$ déduit de u. On a donc $D(u) = \prod_{j=0}^{r-1} \det v_j'$; comme $(P_0'/M', P_1'/M', \ldots, P_s'/M')$ est une suite de Jordan-Hölder de M/M' et de même $(P_s', P_{s+1}', \ldots, P_r')$ pour M', on a $D(u'') = \prod_{j=0}^{s-1} \det v_j'$ et $D(u') = \prod_{j=s}^{r-1} \det v_j'$. Ceci établit la formule $D(u) = D(u') \,.\, D(u'')$.

5. *Calcul des symboles* $\left(\frac{u}{G}\right)$.

On note G un groupe commutatif fini d'ordre impair et u un automorphisme de G. On sait que G est somme directe de sous-groupes cycliques $G_1, \ldots, G_n$; notons d_i l'ordre et x_i un générateur de G_i. Il est loisible de supposer que d_i divise d_{i+1} pour $1 \leqq i \leqq n-1$; on définit les entiers $e_i = d_i/d_{i-1}$ pour $1 \leqq i \leqq n$, avec la convention $d_o = 1$. Par ailleurs, on choisit des entiers u_{ij} tels que $u(x_i) = \sum_{j=1}^{n} u_{ij} \cdot x_j$ pour $1 \leqq i \leqq n$ et l'on note D_i le déterminant de la matrice

$$\begin{pmatrix} u_{ii} & u_{i,\,i+1} & \cdots & u_{in} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ u_{ni} & u_{n,\,i+1} & \cdots & u_{nn} \end{pmatrix}.$$

Nous allons établir la formule

$$\left(\frac{u}{G}\right) = \left(\frac{D_1}{e_1}\right) \cdots \left(\frac{D_n}{e_n}\right). \tag{25}$$

Traitons d'abord le cas où $d_1 = \ldots = d_n = d$. On a alors $e_1 = d$ et $e_i = 1$ pour $2 \leqq i \leqq n$, de sorte que la formule à prouver s'écrit $\left(\frac{u}{G}\right) = \left(\frac{D}{d}\right)$ où D est le déterminant de la matrice $U = (u_{ij})_{1 \leqq i,j \leqq n}$. Il existe des nombres premiers $p_1, \ldots, p_h$ non nécessairement distincts, tels que $d = p_1 \ldots p_h$. On pose $H_1 = G/p_1G$, $H_2 = p_1G/p_1p_2G, \ldots, H_h = p_1p_2 \ldots p_{h-1}G/p_1p_2 \ldots p_{h-1}p_hG$. Alors H_j est un espace vectoriel de dimension n sur le corps $\mathbf{F}_{p_j}$ à p_j éléments; à u est associé un automorphisme u_j de H_j, admettant la réduction de U modulo p_j pour matrice par rapport à une base convenable de H_j. D'après (C_3), on a $\left(\frac{u_j}{H_j}\right) = \left(\frac{D}{p_j}\right)$, et la propriété de multiplicativité (A_2) entraîne alors $\left(\frac{u}{G}\right) = \left(\frac{u_1}{H_1}\right) \cdots \left(\frac{u_h}{H_h}\right) = \left(\frac{D}{p_1}\right) \cdots \left(\frac{D}{p_h}\right) = \left(\frac{D}{d}\right)$.

Le cas général se traite par récurrence sur n. Si l'on n'est pas dans le cas précédent, il existe un entier r compris entre 1 et $n-1$ et tel que $d_1 = \ldots = d_r$ et $d_r \neq d_{r+1}$. Posons $d = d_1$ et notons D le déterminant de U. Posons aussi $G' = dG$ et $G'' = G/G'$; il est clair que u laisse G' stable, donc définit des automorphismes u' et u'' de G' et G'' respectivement. Or le groupe G' est somme directe des sous-groupes cycliques engendrés respectivement par les éléments $x'_{r+1} = dx_{r+1}, \ldots, x' = dx_n$, x_i est d'ordre

d_i/d et l'on a $u'(x_i') = \sum_{j=r+1}^{n} u_{ij} \,.\, x_j'$ pour $r+1 \leqq i \leqq n$. L'hypothèse de récurrence entraîne alors

$$(26) \qquad \begin{pmatrix} u' \\ G' \end{pmatrix} = \begin{pmatrix} D_{r+1} \\ e_{r+1} \end{pmatrix} \cdots \begin{pmatrix} D_r \\ e_r \end{pmatrix}.$$

Par ailleurs, le groupe G'' est somme directe des sous-groupes cycliques engendrés respectivement par $x_1'' = x_1 + G', \ldots, x_r'' = x_r + G'$, et ces éléments sont tous d'ordre d. D'après l'alinéa précédent, on a donc $\binom{u''}{G''} = \binom{D}{d}$; or, on a $e_1 = d$ et $e_2 = \ldots = e_r = 1$, et aussi $D_1 = D$, d'où

$$(27) \qquad \begin{pmatrix} u'' \\ G'' \end{pmatrix} = \begin{pmatrix} D_1 \\ e_1 \end{pmatrix} \cdots \begin{pmatrix} D_r \\ e_r \end{pmatrix}.$$

D'après la propriété (A_2), on a $\binom{u}{G} = \binom{u'}{G'}\binom{u''}{G''}$ et la formule à démontrer résulte de (26) et (27).

BIBLIOGRAPHIE

[1] Eisenstein, G. Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste, *Journ. für reine u. ang. Math.*, 28 (1844), p. 246-248.

[2] Frobenius, F. *Gesammelte Abhandlungen*, tome III, pages 628 à 647, Springer, Heidelberg, 1968.

[3] Gauss, C. F. *Untersuchungen uber höhere Arithmetik (Disquisitiones arithmeticae)*, pages 457-462 et 496-501, Chelsea, New-York, 1965.

[4] Lejeune-Dirichlet, P. et R. Dedekind, *Vorlesungen über Zahlentheorie*, pages 75 à 112, Chelsea, New-York, 1968.

[5] Schering, E. Zur Theorie der quadratischen Reste, *Acta Mathematica*, 1 (1882), p. 153-170.

[6] Zolotareff, M. Nouvelle démonstration de la loi de réciprocité de Legendre, *Nouv. Ann.*, 11 (1872), p. 354-362.

Institut de recherche mathématique avancée
Rue René-Descartes, 67
Strasbourg

(Reçu le 1er novembre 1969)