ACTA ARITHMETICA
XLV (1985)

Sur la formule du produit pour le symbole de reste normique généralisé

par
JEAN-FRANÇOIS JAULENT

1. Position du problème. Soit L/K une extension abélienne finie de corps de nombres. Si $\mathfrak{p}$ est une place de K, le symbole de reste normique $\left(\frac{\ ,\ L/K}{\mathfrak{p}}\right)$, introduit par Hasse dans [3], est composé de l'injection du groupe multiplicatif de K dans celui de son complété $K_\mathfrak{p}$, de l'application de réciprocité locale $(\ ,\ L_\mathfrak{P}/K_\mathfrak{p})$ associée à l'une quelconque des extensions locales $L_\mathfrak{P}/K_\mathfrak{p}$ au-dessus de L/K, et de l'isomorphisme du groupe de Galois $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$ sur le groupe de décomposition $D_\mathfrak{p}(L/K)$ de la place $\mathfrak{p}$ dans L/K. On sait que les symboles $\left(\frac{\ ,\ L/K}{\mathfrak{p}}\right)$ sont directement reliés au symbole d'Artin global (l'élément $\left(\frac{x,\ L/K}{\mathfrak{p}}\right)$ étant le symbole d'Artin $\left(\frac{L/K}{\mathfrak{a}}\right)$ de l'idéal $\mathfrak{a} = y\mathfrak{p}^{-v_\mathfrak{p}(y)}$, où y est un $\mathfrak{p}$-associé convenable de x) et que la formule du produit $\prod_\mathfrak{p}\left(\frac{\ ,\ L/K}{\mathfrak{p}}\right) = 1$ est essentiellement la seule relation entre les divers symboles $\left(\frac{\ ,\ L/K}{\mathfrak{p}}\right)$ attachés à une même extension.

Supposons maintenant que L/K soit une extension finie quelconque de corps de nombres. Pour chaque place $\mathfrak{p}$ de K, notons $L_\mathfrak{p}$ l'intersection $\bigcap_{\mathfrak{P}|\mathfrak{p}} L_\mathfrak{P}$ des complétés de L au-dessus de $\mathfrak{p}$ (pris dans une même clôture algébrique de $K_\mathfrak{p}$), puis $L_\mathfrak{p}^{ab}$ la sous-extension maximale de $L_\mathfrak{p}$ abélienne sur $K_\mathfrak{p}$. La théorie du corps de classes local nous donne les isomorphismes:

$$\mathrm{Gal}(L_\mathfrak{p}^{ab}/K_\mathfrak{p}) \simeq K_\mathfrak{p}^\times/N_{L_\mathfrak{p}/K_\mathfrak{p}}(L_\mathfrak{p}^\times) = K_\mathfrak{p}^\times/\prod_{\mathfrak{P}|\mathfrak{p}} N_{L_\mathfrak{P}/K_\mathfrak{p}}(L_\mathfrak{P}^\times);$$

et nous disons que l'application $\left(\frac{\ ,\ L/K}{\mathfrak{p}}\right)$ de $K^\times$ dans le groupe de Galois local $D_\mathfrak{p}^{ab}(L/K) = \mathrm{Gal}(L_\mathfrak{p}^{ab}/K_\mathfrak{p})$ donnée par le symbole local de réciprocité est *le symbole de reste normique généralisé*, associé à la place $\mathfrak{p}$ dans l'extension L/K.

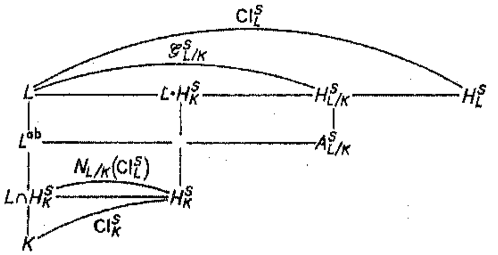
Bien entendu, le symbole généralisé induit le symbole usuel lorsque l'extension est abélienne, de sorte que si L^{ab} désigne la sous-extension maximale de L abélienne sur K, les restrictions à L^{ab} des symboles de Hasse pris dans L/K vérifient la formule du produit $\prod_{\mathfrak{p}}\left(\frac{\;,\,L/K}{\mathfrak{p}}\right)\Big|_{L^{\mathrm{ab}}} = 1$.

Le but de cette note est d'établir la réciproque de ce dernier résultat:

Théorème. *Etant donnée une extension finie quelconque de corps de nombres L/K, les familles $(\sigma_{\mathfrak{p}})_{\mathfrak{p}}$ appartenant à la somme directe $\bigoplus_{\mathfrak{p}} D_{\mathfrak{p}}^{\mathrm{ab}}(L/K)$ des groupes de Galois attachés aux extensions abéliennes locales associées à L/K, dont les restrictions à la sous-extension abélienne globale L^{ab} vérifient la formule du produit $\prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}|_{L^{\mathrm{ab}}} = 1$, sont celles provenant par les symboles de reste normique généralisés d'un même élément de $K^{\times}$.*

2. Eléments de théorie des genres. Désignons par S un ensemble fini de places de K, puis, pour chaque corps de nombres F contenant K, notons J_F le groupe des idèles de F, $J_F(S)$ le sous-groupe des idèles unités en dehors de S, et U_F celui des idèles unités. Par l'isomorphisme du corps de classes, le groupe de Galois du *S-corps de classes de Hilbert* H_F^S de F (i.e. de l'extension abélienne maximale de F, qui est non ramifiée et S-décomposée) s'identifie au quotient: $\mathrm{Gal}(H_F^S/F) \simeq J_F/J_F(S)F^{\times}$ (encore isomorphe au groupe Cl_F^S des S-classes d'idéaux du corps F).

Considérons l'extension L/K, et introduisons son *S-corps des genres* $H_{L/K}^S$ (i.e. la sous-extension maximale de H_L^S qui provient par composition avec L d'une extension abélienne sur K), puis sa sous-extension maximale $A_{L/K}^S$ abélienne sur K. Nous obtenons le schéma de corps:



Et le groupe $\mathscr{G}_{L/K}^S \simeq \mathrm{Gal}(H_{L/K}^S/L)$ est, par définition, le *S-quotient des genres attaché à l'extension relative L/K.*

Cela étant, puisque $A_{L/K}^S$ est la sous-extension maximale de H_L^S abélienne sur K, la théorie du corps de classes nous donne l'isomorphisme:

$$\mathrm{Gal}(A_{L/K}^S/K) \simeq J_K/N_{H_{L/K}^S/K}(J_{H_{L/K}^S})K^{\times} = J_K/N_{L/K}(J_L(S))K^{\times},$$

et, par suite, l'identité:

$$\begin{aligned}[A_{L/K}^S:\ H_K^S] &= (J_K(S)K^{\times}:\ N_{L/K}(J_L(S))K^{\times}) \\ &= \frac{(J_K(S):\ N_{L/K}(J_L(S)))}{(K^{\times} \cap J_K(S): K^{\times} \cap N_{L/K}(J_L(S)))} \\ &= \frac{\prod_{\mathfrak{p}\in S}(K_{\mathfrak{p}}^{\times}: N_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(L_{\mathfrak{p}}^{\times}))\prod_{\mathfrak{p}\notin S}(U_{\mathfrak{p}}(K): N_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(U_{\mathfrak{p}}(L)))}{(K(S): K(S) \cap N_{L/K}^{\mathrm{loc}})}\end{aligned}$$

où $U_{\mathfrak{p}}(K)$ et $U_{\mathfrak{p}}(L)$ désignent les groupes d'unités des complétés $K_{\mathfrak{p}}$ et $L_{\mathfrak{p}}$ définis plus haut; $K(S)$ est le groupe des S-unités de K; et $N_{L/K}^{\mathrm{loc}}$ est le sous-groupe des éléments de $K^{\times}$ qui sont normes locales partout dans l'extension L/K (i.e. normes dans chacune des extensions locales $L_{\mathfrak{p}}/K_{\mathfrak{p}}$).

Généralisant le résultat de [2], nous en déduisons l'expression du *nombre de S-genres*:

Proposition 1. *L'ordre $g_{L/K}^S = [H_{L/K}^S:L]$ du S-quotient des genres est donné par la formule:*

$$g_{L/K}^S = \frac{h_K^S}{[L^{\mathrm{ab}}:K]}\ \frac{\prod_{\mathfrak{p}\in S} d_{\mathfrak{p}}(L/K)\cdot\prod_{\mathfrak{p}\notin S} e_{\mathfrak{p}}(L/K)}{(K(S): K(S)\cap N_{L/K}^{\mathrm{loc}})}.$$

Dans celle-ci $h_K^S = [H_K^S:K]$ est le nombre de S-classes d'idéaux du corps K; $e_{\mathfrak{p}}(L/K)$ est l'indice de ramification de la sous-extension maximale $L_{\mathfrak{p}}^{\mathrm{ab}}$ de $L_{\mathfrak{p}}$ abélienne sur $K_{\mathfrak{p}}$; et $d_{\mathfrak{p}}(L/K) = [L_{\mathfrak{p}}^{\mathrm{ab}}:K_{\mathfrak{p}}]$ est le degré de cette extension.

3. Réciproque de la formule du produit. De l'égalité entre les groupes d'idèles $N_{L/K}(J_L(S))$ et $N_{H_{L/K}^S/K}(J_{H_{L/K}^S}(S))$, nous déduisons le lemme:

Lemme. *Les S-unités qui sont normes locales partout dans l'extension L/K sont exactement celles qui sont normes locales partout dans l'extension $H_{L/K}^S/K$. De plus, les divers indices $d_{\mathfrak{p}}(L/K) = (K_{\mathfrak{p}}^{\times}: N_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(L_{\mathfrak{p}}^{\times}))$, lorsque $\mathfrak{p}$ décrit S, et $e_{\mathfrak{p}}(L/K) = (U_{\mathfrak{p}}(K): N_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}(U_{\mathfrak{p}}(L)))$ s'interprètent encore comme ordres des groupes de décomposition $D_{\mathfrak{p}}$ et d'inertie $I_{\mathfrak{p}}$ de la place $\mathfrak{p}$ dans l'extension abélienne locale associée à $H_{L/K}^S/K$.*

Cela étant:

Proposition 2. *Il existe une suite exacte courte canonique:*

$$1 \to K^{\times}(S)/K^{\times}(S) \cap N_{L/K}^{\mathrm{loc}} \xrightarrow{\mathfrak{h}} \Big(\bigoplus_{\mathfrak{p}\in S} D_{\mathfrak{p}}\Big) \oplus \Big(\bigoplus_{\mathfrak{p}\notin S} I_{\mathfrak{p}}\Big) \xrightarrow{\pi} \mathrm{Gal}(A_{L/K}^S/H_K^S) \to 1.$$

Dans celle-ci, l'application $\mathfrak{h}$ est induite par les symboles de Hasse $\left(\frac{\;,\,H_{L/K}^S/K}{\mathfrak{p}}\right)$, et π est la projection canonique $(\sigma_{\mathfrak{p}})_{\mathfrak{p}} \mapsto \prod_{\mathfrak{p}} \sigma_{\mathfrak{p}}|_{A_{L/K}^S}$ de la somme directe des sous-groupes de décomposition ou d'inertie sur le groupe de Galois de $A_{L/K}^S/H_K^S$.

En effet, l'application π est surjective par maximalité du S-corps de classes de Hilbert H_K^S; et $\mathfrak{h}$ est injective d'après ce qui précède; l'inclusion $\operatorname{Im}\mathfrak{h} \subset \operatorname{Ker}\pi$ traduit la formule du produit; et l'exactitude de la suite, qui en constitue donc une première réciproque, résulte du calcul du nombre de S-genres effectué plus haut.

Introduisons de même les groupes de Galois $D_\mathfrak{p}^{ab}(L/K)$ des extensions abéliennes locales $L_\mathfrak{p}^{ab}/K_\mathfrak{p}$ associées à L/K, puis leurs sous-groupes d'inertie $I_\mathfrak{p}^{ab}(L/K)$ (d'ordres respectifs $d_\mathfrak{p}(L/K)$ et $e_\mathfrak{p}(L/K)$), et notons $\Gamma_{L/K}^S$ le sous-groupe de la somme directe $\bigoplus_\mathfrak{p} D_\mathfrak{p}^{ab}(L/K)$ formé des familles $(\sigma_\mathfrak{p})_\mathfrak{p}$ qui vérifient la formule du produit $\prod_\mathfrak{p} \sigma_\mathfrak{p}|_{L^{ab}} = 1$ et les conditions $\sigma_\mathfrak{p} \in I_\mathfrak{p}^{ab}(L/K)$ pour $\mathfrak{p} \notin S$. Désignons enfin par $\mathfrak{h}_{L/K}$ le composé des symboles de Hasse dans L/K. Nous obtenons immédiatement:

$$|\Gamma_{L/K}^S| = \frac{\prod_{\mathfrak{p}\in S} d_\mathfrak{p}(L/K) \cdot \prod_{\mathfrak{p}\notin S} e_\mathfrak{p}(L/K)}{[L^{ab}: L \cap H_K^S]},$$

puis, d'après le lemme précédent:

(i) $$\left(\Gamma_{L/K}^S : \mathfrak{h}_{L/K}(K(S))\right) = [H_{L/K}^S : LH_K^S].$$

D'un autre côté, puisque le sous-groupe d'idèles du corps L qui fixe LH_K^S est le noyau

$$J_L^* = \{\mathfrak{x} \in J_L \mid N_{L/K}(\mathfrak{x}) \in J_K(S)\, K^\times\}$$

de la norme arithmétique, et que celui qui fixe le S-corps des genres $H_{L/K}^S$ est le *S-genre principal*

$$\bar{J}_L = \{\mathfrak{x} \in J_L \mid N_{L/K}(\mathfrak{x}) \in N_{L/K}(J_L(S))\, K^\times\},$$

l'isomorphisme de réciprocité du corps de classes nous donne:

(ii) $$\operatorname{Gal}(H_{L/K}^S/LH_K^S) \simeq J_L^*/\bar{J}_L \simeq N_{L/K}^S/K^\times(S)\, N_{L/K}^{loc},$$

où $N_{L/K}^S = K^\times \cap (J_K(S)\, N_{L/K}(J_L))$ est contenu dans le groupe des éléments de $K^\times$ qui sont normes locales pour les places non ramifiées n'appartenant pas à S.

Rassemblant (i) et (ii) nous concluons de l'égalité des ordres que l'injection du groupe $N_{L/K}^S/K(S)\, N_{L/K}^{loc}$ dans le quotient $\Gamma_{L/K}^S/\mathfrak{h}_{L/K}(K(S))$, donnée par le composé des symboles de Hasse $\mathfrak{h}_{L/K}$, est un isomorphisme, ce qui constitue le résultat attendu, tout élément de $\Gamma_{L/K}^S$ étant bien l'image par $\mathfrak{h}_{L/K}$ d'un élément de $N_{L/K}^S$:

PROPOSITION 3. *Le symbole de Hasse généralisé donne lieu à une suite exacte courte*:

$$1 \to N_{L/K}^S/N_{L/K}^{loc} \to \Big(\bigoplus_{\mathfrak{p}\in S} D_\mathfrak{p}^{ab}(L/K)\Big) \oplus \Big(\bigoplus_{\mathfrak{p}\notin S} I_\mathfrak{p}^{ab}(L/K)\Big) \to \operatorname{Gal}(L^{ab}/L \cap H_K^S) \to 1.$$

Le théorème s'en déduit aisément, tout élément de la somme directe $\bigoplus_\mathfrak{p} D_\mathfrak{p}^{ab}(L/K)$ étant contenu dans une somme finie $\bigoplus_{\mathfrak{p}\in S} D_\mathfrak{p}^{ab}(L/K)$.

4. Lien avec le théorème de Moore. K étant un corps de nombres (de degré fini sur $\mathbf{Q}$), supposons donnée, pour chaque place $\mathfrak{p}$ non complexe d'un ensemble fini S, une racine de l'unité $\zeta_\mathfrak{p}$ dans le complété $K_\mathfrak{p}$. Notons μ_K le groupe des racines de l'unité du corps K, puis m son ordre et $m_\mathfrak{p}$ celui du groupe $\mu_{K_\mathfrak{p}}$ des racines de l'unité locales, n enfin un multiple commun à ceux des $m_\mathfrak{p}$ associés aux places de S, et, de façon générale, $n \wedge m_\mathfrak{p}$ le plus grand diviseur commun de n et $m_\mathfrak{p}$.

Par le théorème d'approximation simultanée, nous pouvons choisir un a dans K dont l'image dans le quotient $K_\mathfrak{p}^\times/\mu_{K_\mathfrak{p}} K_\mathfrak{p}^{\times}$ soit exactement d'ordre $m_\mathfrak{p}$ (par exemple, en imposant à a d'être une uniformisante locale), et ce pour chaque $\mathfrak{p}$ de l'ensemble fini S. Prenons un tel a et formons l'extension $L = K[\sqrt[n]{a}]$: sa sous-extension abélienne maximale L^{ab} est de degré m, et pour tout $\mathfrak{p}$ de S la sous-extension maximale $L_\mathfrak{p}^{ab}$ de $K_\mathfrak{p}[\sqrt[n]{a}]$ abélienne sur $K_\mathfrak{p}$ est de degré $m_\mathfrak{p}$. Si donc $\sigma_\mathfrak{p}$ désigne l'élément du groupe de Galois $D_\mathfrak{p}^{ab}(L/K) = \operatorname{Gal}(K_\mathfrak{p}[\sqrt[m_\mathfrak{p}]{a}]/K_\mathfrak{p})$ défini par $\sigma_\mathfrak{p} = 1$ pour $\mathfrak{p} \notin S$, et

$$\sqrt[m_\mathfrak{p}]{a}^{(\sigma_\mathfrak{p}-1)} = \zeta_\mathfrak{p}, \quad \text{pour } \mathfrak{p} \in S,$$

la relation

$$\prod_\mathfrak{p} \zeta_\mathfrak{p}^{m_\mathfrak{p}/m} = \sqrt[m]{a}^{\sum_\mathfrak{p}(\sigma_\mathfrak{p}-1)} = \sqrt[m]{a}^{(\prod_\mathfrak{p}\sigma_\mathfrak{p}-1)}$$

et le théorème établi plus haut nous montrent que la formule du produit $\prod_\mathfrak{p} \zeta_\mathfrak{p}^{m_\mathfrak{p}/m} = 1$ est la condition pour que les $\sigma_\mathfrak{p}$ soient les symboles de Hasse dans l'extension L/K d'un élément b de $K^\times$ qui est norme locale en dehors de S. Lorsqu'elle est vérifiée, nous avons ainsi:

$$\sigma_\mathfrak{p} = \left(\frac{b,\ K[\sqrt[n]{a}]/K}{\mathfrak{p}}\right), \quad \text{pour chaque place } \mathfrak{p},$$

donc, en particulier,

$$\zeta_\mathfrak{p} = \left(\frac{a,\ b}{\mathfrak{p}}\right)_{m_\mathfrak{p}}, \text{ pour } \mathfrak{p} \in S, \quad \text{et} \quad \left(\frac{a,\ b}{\mathfrak{p}}\right)_{m_\mathfrak{p}}^{m_\mathfrak{p}/m_\mathfrak{p} \wedge n} = 1, \text{ pour } \mathfrak{p} \notin S,$$

ce qui établit l'exactitude de la suite induite par les symboles de Hilbert:

$$K^\times \otimes_\mathbf{Z} K^\times \to \bigoplus_{\mathfrak{p}\ \text{non complexe}} \mu_{K_\mathfrak{p}}/\mu_{K_\mathfrak{p}}^n \to \mu_K/\mu_K^n \to 1,$$

pour l'entier n choisi, donc, finalement, pour tout n. Cela suffit à montrer qu'il n'y a pas d'autre loi de réciprocité pour le symbole de Hilbert, que la formule du produit $\prod_\mathfrak{p} \left(\frac{,}{\mathfrak{p}}\right)^{m_\mathfrak{p}/m} = 1$.

References

[1] S. U. Chase and W. C. Waterhouse, *Moore's theorem on uniqueness of reciprocity laws*, Invent. Math. 16 (1972), p. 267–270.
[2] Y. Furuta, *The genus field and genus number in algebraic number fields*, Nagoya Math. J. 29 (1967), p. 281–285.
[3] H. Hasse, *Neue Begründung und Verallgemeinerung der Theorie des Normenrestsymbols*, J. Reine Angew. Math. 162 (1931), p. 134–144.

UNIVERSITÉ DE FRANCHE-COMTÉ
FACULTÉ DES SCIENCES-MATHÉMATIQUES
25030 Besançon Cedex

Reçu le 6.12.1983 (1388)

ACTA ARITHMETICA
XLV (1985)

On the evaluation of the Legendre symbol $\left(\frac{A+B\sqrt{m}}{p}\right)$

by

KENNETH S. WILLIAMS*, KENNETH HARDY** (Ottawa, Ont., Canada)
and CHRISTIAN FRIESEN*** (Fredericton, N. B., Canada)

1. Introduction. Let m be a positive squarefree integer which is either of the form

$$m = p_1 p_2 \ldots p_r \equiv 1 \pmod 4 \quad (r \geqslant 1) \tag{1.1}$$

or of the form

$$m = 2p_1 p_2 \ldots p_r \equiv 2 \pmod 8 \quad (r \geqslant 0), \tag{1.2}$$

where $p_1, \ldots, p_r$ are primes congruent to 1 modulo 4. Let (A, B, C) be a triple of positive integers such that

$$A^2 = m(B^2+C^2). \tag{1.3}$$

(The form of m guarantees that there are infinitely many such triples (A, B, C).) From (1.3) we see that the greatest common divisor of B and C must divide A and so can be divided out of the equation (1.3). Hence we may assume that

$$(A, B) = (A, C) = (B, C) = 1. \tag{1.4}$$

Let p be an odd prime, not dividing ABC, which is such that

$$\begin{cases} \left(\frac{p_i}{p}\right) = 1 & (i = 1, \ldots, r), \quad \text{if} \quad m \equiv 1 \pmod 4, \\ \left(\frac{2}{p}\right) = \left(\frac{p_i}{p}\right) = 1 & (i = 1, \ldots, r), \quad \text{if} \quad m \equiv 2 \pmod 8, \end{cases} \tag{1.5}$$

---

* Research supported by Natural Sciences and Engineering Research Council Canada Grant No. A-7233.
** Research supported by Natural Sciences and Engineering Research Council Canada Grant No. A-8049.
*** Research supported by a Natural Sciences and Engineering Research Council Canada Undergraduate Summer Research Award.