ANNALES SCIENTIFIQUES DE L'É.N.S.

JACQUES HERBRAND

Une propriété du discriminant des corps algébriques

Annales scientifiques de l'É.N.S. 3e série, tome 49 (1932), p. 105-112
<http://www.numdam.org/item?id=ASENS_1932_3_49__105_0>

© Gauthier-Villars (Éditions scientifiques et médicales Elsevier), 1932, tous droits réservés.

L'accès aux archives de la revue « Annales scientifiques de l'É.N.S. » (http://www.elsevier.com/locate/ansens) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

UNE PROPRIÉTÉ

DU

DISCRIMINANT DES CORPS ALGÉBRIQUES

PAR M. JACQUES HERBRAND [1]

THÉORÈME. — *$\mathfrak{D}$ étant le discriminant par rapport au corps k d'un sur-corps relativement métacyclique* K *de degré relatif* N, *on a* $\mathfrak{D} = \mathfrak{a}^2(\alpha)$, *où α est un nombre tel que :*

a. $\alpha \equiv 1 \pmod{\mathfrak{b}}$, $\mathfrak{b}$ *étant le plus grand idéal divisant* 4 *et premier à* $\mathfrak{D}$.

b. Le conjugué de α dans un corps réel conjugué de k n'est négatif que si le conjugué correspondant de K *est imaginaire et si* $N \equiv 2 \pmod{4}$.

Remarques. — 1. *$\mathfrak{D}$ est divisible au moins par le carré de ceux de ses idéaux premiers qui divisent* 2.

Cette remarque est vraie pour tout sur-corps galoisien et résulte de la formule connue de Hilbert donnant la puissance à laquelle un idéal premier $\mathfrak{p}$ intervient dans le discriminant : cette puissance est

$$\mathfrak{p}^{fg[(e-1)+(p^{R_1}-1)+(p^{R_2}-1)+\ldots]},$$

où ef, e, p^{R_1}, p^{R_2}, ... sont respectivement les degrés des groupes de décomposition, d'inertie et des groupes successifs de ramification, et où $efg = N$. L'exposant de cette puissance ne peut être égal à 1 que si $f = g = 1$, $e = 2$, $p^{R_1} = 1$, mais ceci est impossible si $\mathfrak{p}$ divise 2, car

---

[1] Ce Mémoire était partiellement rédigé au moment de la mort tragique de mon ami Jacques Herbrand. J'ai achevé la rédaction de ce Mémoire d'après les brouillons trouvés dans ses papiers. Claude CHEVALLEY.

alors $p = 2$ et p^{R_1} qui est, comme on sait, la plus haute puissance de p divisant c, est égal à 2.

2. Prenons pour k le corps des nombres rationnels, alors :

a. Ou bien $\mathfrak{D}$ est pair et, d'après la remarque 1, $\mathfrak{D}$ est divisible par 4.

b. Ou bien $\mathfrak{D}$ est impair, alors, d'après le théorème, $\mathfrak{D} = (a)$ où $a \equiv 1 \pmod{4}$, a n'étant négatif que si K est imaginaire et $N \equiv 2 \pmod{4}$.

Nous avons jusqu'ici considéré $\mathfrak{D}$ comme un idéal; mais quand le corps de base est rationnel, on sait que l'on peut considérer le discriminant comme un nombre, à savoir le carré du déterminant

$$|\omega_i^{(j)}| \qquad (i, j = 1, 2, \ldots, N),$$

les ω_i formant une base des entiers, les $|\omega_i^{(j)}|$ étant les conjugués des ω_i. Pour appliquer le résultat précédent, il faut trouver le signe du carré de ce déterminant. Or, si nous prenons pour les ω_i, non plus une base des entiers, mais un système d'entiers indépendants quelconque, $|\omega_i^{(j)}|^2$ est multiplié par le carré d'un entier rationnel, donc son signe ne change pas. Posons donc

$$f = |\omega_i^{(j)}|^2,$$

$\omega_1, \omega_2, \ldots, \omega_N$ étant un système quelconque d'entiers indépendants. Nous allons montrer que f n'est négatif que si K est imaginaire, et $N \equiv 2 \pmod{4}$; nous supposerons K galoisien.

a. Si K est réel, $|\omega_i^{(j)}|$ est réel, donc f positif.

b. Si K est imaginaire, soit $\overline{K}$ le plus grand sous-corps réel de K.

On a $K = \overline{K}(\sqrt{\alpha})$, pour un α de $\overline{K}$ qu'on peut supposer entier. Soit $\mu_1, \mu_2, \ldots, \mu_{\frac{N}{2}}$ une base des entiers de $\overline{K}$. Prenons pour $\omega_1, \omega_2, \ldots, \omega_N$, le système $\mu_1, \mu_2, \ldots, \mu_{\frac{N}{2}}, \mu_1\sqrt{\alpha}, \mu_2\sqrt{\alpha}, \ldots, \mu_{\frac{N}{2}}\sqrt{\alpha}$. Si l'on calcule $|\omega_i^{(j)}|$ et qu'on élève au carré, on trouve sans peine

$$f = |\mu_i^{(j)}|^4 N(\alpha)^{2N} \qquad \left(i, j = 1, 2, \ldots, \frac{N}{2}\right),$$

l'indice supérieur j indiquant les différents conjugués de $\overline{K}$, $N(\alpha)$ désignant la norme de α prise dans $\overline{K}$ par rapport à k.

$|\mu_i^{(j)}|^2$ étant rationnel, $|\mu_i^{(j)}|^4$ est > 0. α et tous ses conjugués sont négatifs, car K et tous ses conjugués sont imaginaires. Donc, l'expression étudiée n'est négative que si $N \equiv 2 \pmod{4}$.

Nous avons, en résumé, démontré que :

a. Le discriminant d'un corps algébrique galoisien n'est négatif que si ce corps est imaginaire et si son degré est congru à $2 \pmod{4}$.

Il suffit de comparer à ce que nous disions au début de cette remarque pour voir que nous retrouvons dans le cas particulier d'un corps métacyclique le théorème de Stickelberger-Schur.

b. Le discriminant d'un corps algébrique est congru à 0 *ou à* $1 \pmod{4}$.

La démonstration qu'a donnée Schur de ce théorème est infiniment plus simple que tout ce qui précède; mais notre seul but était de montrer qu'en tenant compte de *a.*, c'est un cas particulier de notre théorème.

Il suffit de particulariser ce même théorème pour retrouver, toujours dans le cas des sur-corps métacycliques, le théorème de Hecke :

Le discriminant d'un corps algébrique, par rapport à un sous-corps, est dans le carré d'une classe de ce sous-corps.

Notre théorème fond donc en un seul les théorèmes de Stickelberger-Schur et de Hecke. Mais comme ces deux théorèmes sont vrais pour des sur-corps quelconques, même non galoisiens, il est probable que notre théorème reste vrai quand on supprime l'hypothèse que K est relativement métacyclique.

De plus, comme le théorème de Hecke n'est qu'une conséquence du suivant :

La différente d'un corps algébrique par rapport à un sous-corps est toujours dans le carré d'une classe du sur-corps, il est probable qu'un théorème analogue à celui énoncé au début doit être vrai pour la différente au lieu du discriminant.

Démonstration. — I. Supposons le théorème démontré pour tous les degrés relatifs diviseurs de N.

Soient alors k un corps réel, K un sur-corps métacyclique, de degré relatif non premier, $\overline{K}$ un corps intermédiaire, N le degré de K par rapport à k, n celui de K par rapport à $\overline{K}$.

Soient $\mathfrak{D}_{Kk}$, $\mathfrak{D}_{\overline{K}k}$, $\mathfrak{D}_{K\overline{K}}$, les discriminants relatifs du premier corps en indice par rapport au second; $\mathfrak{b}_{Kk}$, $\mathfrak{b}_{\overline{K}k}$, $\mathfrak{B}_{K\overline{K}}$ les plus grands idéaux des corps k, k, $\overline{K}$, respectivement premiers aux discriminants de mêmes indices et divisant 4.

D'après une formule connue

$$\mathfrak{D}_{Kk} = (\mathfrak{D}_{\overline{K}k})^n N_{\overline{K}k}(\mathfrak{D}_{K\overline{K}}),$$

$N_{\overline{K}k}$ désignant la norme prise dans $\overline{K}$ par rapport à k. D'après l'hypothèse, on a

$$\mathfrak{D}_{\overline{K}k} = \mathfrak{a}^2(\alpha),$$

$\mathfrak{a}$ étant un idéal de k, α un nombre de k tel que $\alpha \equiv 1 \pmod{\mathfrak{b}_{\overline{K}k}}$, et le conjugué de α dans un conjugué réel de k n'est négatif que si le conjugué correspondant de $\overline{K}$ est imaginaire et $\frac{N}{n} \equiv 2 \pmod 4$;

$$\mathfrak{D}_{K\overline{K}} = \mathfrak{A}^2(A),$$

$\mathfrak{A}$ étant un idéal de $\overline{K}$, A un nombre de $\overline{K}$ tel que $A \equiv 1 \pmod{\mathfrak{B}_{K\overline{K}}}$, et le conjugué de A dans un conjugué réel de $\overline{K}$ n'est négatif que si le conjugué correspondant de K est imaginaire et $n \equiv 2 \pmod 4$.

Donc,

$$\mathfrak{D}_{Kk} = \mathfrak{a}^{*2}(\alpha)^n N_{Kk}(A),$$

$\mathfrak{a}^*$ étant un idéal de k.

1° L'idéal $\mathfrak{b}_{Kk}$ divise $\mathfrak{b}_{\overline{K}k}$, puisque $\mathfrak{D}_{\overline{K}k}$ divise $\mathfrak{D}_{Kk}$. Donc,

$$\alpha^n \equiv 1 \pmod{\mathfrak{b}_{Kk}}.$$

D'autre part, $\mathfrak{b}_{Kk}$ divise $\mathfrak{B}_{K\overline{K}}$. En effet, soit $\mathfrak{p}$ un facteur premier de $\mathfrak{b}_{Kk}$, et soit $\mathfrak{P}$ un diviseur premier de $\mathfrak{p}$ dans $\overline{K}$. $\mathfrak{P}$ est premier à $\mathfrak{D}_{Kk}$, donc à $\mathfrak{D}_{K\overline{K}}$. $\mathfrak{P}^e$ étant la contribution de $\mathfrak{P}$ à 4, il en résulte que $\mathfrak{P}^e$ divise $\mathfrak{B}_{K\overline{K}}$. Or, $\Pi\mathfrak{P}^e$ étendu aux diviseurs premiers de $\mathfrak{p}$ dans $\overline{K}$ est la contribution de $\mathfrak{p}$ à 4. D'autre part, $\mathfrak{B}_{K\overline{K}}$ est un idéal invariant par les automor-

phismes de $\overline{K}$ par rapport à k, car il en est ainsi de $\mathfrak{I}_{K\overline{K}}$, K étant galoisien sur k. Donc,

$$N_{\overline{K}k}(A) \equiv 1 \,(\text{mod. } \mathfrak{B}_{K\overline{K}})$$

et, par suite,

$$\alpha^n N_{\overline{K}k}(A) \equiv 1 \,(\text{mod. } \mathfrak{B}_{Kk}).$$

2° Il reste à démontrer l'assertion sur le signe de $\alpha^n N_{\overline{K}k}(A)$ et de ses conjugués. Pour cela, il suffit de faire un tableau des différents cas possibles. $k^{(i)}$ désigne dans ce tableau un conjugué réel de k, $\overline{K}^{(i)}$ et $K^{(i)}$ les conjugués de $\overline{K}$, K qui contiennent $k^{(i)}$. On désigne par $\alpha^{(i)}$ le conjugué de α dans $k^{(i)}$, par $A^{(i)}$ les conjugués de A dans $K^{(i)}$. K étant galoisien sur k, ces conjugués ont tous le même signe si $K^{(i)}$ est réel.

					Signe de $[\alpha^n N_{\overline{K}K}(A)]^{(i)}$.	
$\overline{K}^{(i)}$ réel, $\alpha^{(i)} > 0$	$K^{(i)}$ réel		$A^{(i)} > 0$		+	
	$K^{(i)}$ imaginaire	$n \equiv 2 \pmod 4$	$A^{(i)} < 0$	$\frac{N}{n}$ pair	+	$N \equiv 0$ (4)
				$\frac{N}{n}$ impair	−	$N \equiv 2$ (4)
		$n \equiv 0 \pmod 4$	$A^{(i)} > 0$		+	$N \equiv 0$ (4)
$\overline{K}^{(i)}$ imaginaire, $\frac{N}{n} \equiv 0$ (2), $[N_{\overline{K}k}(A)]^{(i)} > 0$	$K^{(i)}$ imaginaire	$n \equiv 0 \pmod 2$			+	$N \equiv 0$ (4)
		$n \not\equiv 0 \pmod 2$	$\frac{N}{n} \equiv 2$ (4) $\alpha^{(i)} > 0$		−	$N \equiv 2$ (4)
			$\frac{N}{n} \equiv 0$ (4) $\alpha^{(i)} > 0$		+	$N \equiv 0$ (4)

L'examen de ce tableau prouve que $[\alpha^n N_{\overline{K}k}(A)]^{(i)}$ a toujours le signe indiqué par l'énoncé du théorème.

II. Si nous démontrons le théorème par les extensions relativement cycliques de degré premier, il sera évidemment, en vertu de I, démontré pour toute extension métacyclique. Soit donc K un sur-corps cyclique de degré relatif l du corps k.

a. $l \neq 2$. — Dans ce cas, si $\mathfrak{f}$ est le conducteur de K par rapport à k, on a $\mathfrak{I} = \mathfrak{f}^{l-1}$ et $l - 1$ est pair. Donc, $\mathfrak{I}$ est le carré d'un idéal. D'autre part, $K^{(i)}$ est de degré l sur $k^{(i)}$ et ne peut, par suite, être imaginaire que si $k^{(i)}$ est imaginaire. Donc, le théorème est démontré dans ce cas.

b. $l = 2$. — Soit $\tilde{\mathfrak{f}}$ le conducteur de K par rapport à k. On dési-

gnera par $\mathfrak{p}$ les idéaux premiers finis premiers à 2 divisant $\tilde{\mathfrak{f}}$, par $\mathfrak{l}$, $\bar{\mathfrak{l}}$, $\bar{\bar{\mathfrak{l}}}$ des idéaux premiers facteurs de 2, par $\mathfrak{p}_{\infty,i}$ les idéaux premiers à l'infini divisant $\tilde{\mathfrak{f}}$, par $\tilde{\mathfrak{p}}_{\infty,i}$ les autres. L'idéal $\tilde{\mathfrak{f}}$ est de la forme

$$\tilde{\mathfrak{f}} = \Pi \mathfrak{p}_i \Pi \mathfrak{l}_i^{2e_i+1} \Pi \bar{\mathfrak{l}}_i^{2x_i} \Pi \mathfrak{p}_{\infty,i},$$

où l'on désigne par e la contribution d'un idéal $\mathfrak{l}$ à 2 et où $x_i \leqq \bar{e}_i$ (¹). Donc, les idéaux $\bar{\bar{\mathfrak{l}}}$ sont ceux premiers à $\tilde{\mathfrak{f}}$. Soient H le groupe des nombres de k premiers à $\tilde{\mathfrak{f}}$, $H_{\tilde{\mathfrak{m}}}$ pour un idéal généralisé $\tilde{\mathfrak{m}}$, le groupe des restes quadratiques (mod. $\tilde{\mathfrak{m}}$). Donc,

$$H_{\tilde{\mathfrak{f}}} = [H_{\mathfrak{p}_i}, H_{\mathfrak{l}_i^{2e_i+1}}, H_{\bar{\mathfrak{l}}_i^{2x_i}}, H_{\mathfrak{p}_{\infty,i}}].$$

Soit

$$\bar{\bar{H}} = [H_{\mathfrak{l}_i^{2e_i}}, H_{\bar{\mathfrak{l}}_i^{2x_i}}].$$

Désignons par :

a_{i_0} un nombre appartenant à tous les groupes $H_{\mathfrak{p}_i}$, $H_{\mathfrak{l}_i^{2e_i+1}}$, $H_{\mathfrak{l}_i^{2x_i}}$, $H_{\mathfrak{p}_{\infty,i}}$, sauf à $H_{\mathfrak{p}_{i_0}}$;

b_{i_0} un nombre appartenant à tous les groupes $H_{\mathfrak{p}_i}$, $H_{\mathfrak{l}_i^{2e_i+1}}$, $H_{\bar{\mathfrak{l}}_i^{2x_i}}$, $H_{\mathfrak{p}_{\infty,i}}$, sauf à $H_{\mathfrak{l}_{i_0}^{2e_{i_0}+1}}$, mais appartenant à $H_{\mathfrak{l}_{i_0}^{2e_{i_0}}}$;

c_{i_0} un nombre appartenant à tous les groupes $H_{\mathfrak{p}_i}$, $H_{\mathfrak{l}_i^{2e_i+1}}$, $H_{\bar{\mathfrak{l}}_i^{2x_i}}$, $H_{\mathfrak{p}_{\infty,i}}$, sauf à $H_{\mathfrak{p}_{\infty,i_0}}$.

Tout nombre de H se met et d'une seule manière sous la forme $\Pi a_i^{x_i} \Pi b_i^{y_i} \Pi c_i^{z_i} \omega$, les x_i, y_i, z_i étant des exposants égaux à 0 ou à 1 et ω un nombre de $H_{\tilde{\mathfrak{f}}}$.

Soit G le groupe des nombres α de H tels que (α) soit un idéal du groupe pour lequel K est corps de classes. Le groupe G ne contient aucun des nombres a_i, b_i, c_i et est d'indice 2 dans H (²). Par suite, la condition nécessaire et suffisante pour le nombre $\Pi a_i^{x_i} . \Pi b_i^{y_i} . \Pi c_i^{z_i} \omega$, ω étant dans $H_{\mathfrak{f}}$, soit dans G est que

$$\Sigma x_i + \Sigma y_i + \Sigma z_i \equiv 0 \qquad (\text{mod. } 2).$$

Ceci posé, considérons les nombres β tels que

$$(\beta, \mathfrak{f}) = 1, \qquad \beta \underset{2}{\equiv} 1 \quad (\text{mod. } \mathfrak{l}_i^{2e_i}), \qquad \beta \underset{2}{\equiv} 1 \quad (\text{mod. } \bar{\mathfrak{l}}_i^{2e_i}), \qquad (\beta) = \mathfrak{a}^2.$$

(¹) *Voir* Hasse, *Klassenkönpertheorie*, 2ᵉ partie.

(²) Sauf si $\tilde{\mathfrak{f}} = (1)$. Mais, dans ce cas, le théorème est trivial.

Les (β) étant carrés d'idéaux sont dans G. D'autre part,

$$\left(\frac{\beta}{\mathfrak{f}}\right)=\Pi\left(\frac{\beta}{\mathfrak{p}_i}\right)\Pi\left(\frac{\beta}{\mathfrak{l}_i^{2e_i+1}}\right)\Pi\left(\frac{\beta}{\bar{\mathfrak{l}}_i^{2r_i}}\right).$$

Soit $\beta=\Pi a_i^{x_i}\Pi b_i^{y_i}\Pi c_i^{z_i}\omega$, ω étant dans $H_{\tilde{\mathfrak{f}}}$. On a

$$\left(\frac{\beta}{\mathfrak{f}}\right)=\Pi\left(\frac{a_i}{\mathfrak{p}_i}\right)^{x_i}\Pi\left(\frac{b_i}{\mathfrak{l}_i^{2e_i+1}}\right)^{y_i}=(-1)^{\Sigma x_i+\Sigma y_i}.$$

D'où, puisque

$$\Sigma x_i+\Sigma y_i+\Sigma z_i\equiv 0 \qquad (\text{mod.}\,2), \qquad \left(\frac{\beta}{\mathfrak{f}}\right)=(-1)^{\Sigma z_i}.$$

Or, nous poserons

$$\tilde{\mathfrak{b}}=\Pi\bar{\bar{\mathfrak{l}}}_i^{2e_i+1}\Pi\mathfrak{p}_{\infty,i}\Pi\bar{\mathfrak{p}}_{\infty,i}, \qquad \mathfrak{b}=\Pi\bar{\bar{\mathfrak{l}}}_i^{2e_i+1}$$

et nous remarquerons que les corps $k(\sqrt{\beta})$ sont les corps dont le conducteur divise $\tilde{\mathfrak{b}}$. En effet, le conducteur de tout corps $k(\sqrt{\beta})$ divise $\tilde{\mathfrak{b}}$; si, d'autre part, le conducteur d'un corps $k(\sqrt{\beta'})$ divise $\tilde{\mathfrak{b}}$, (β') est le carré d'un idéal que l'on peut supposer, en multipliant β' par le carré d'un nombre de k, premier à $\tilde{\mathfrak{f}}$. De plus,

$$\beta'\underset{2}{\equiv}1 \qquad (\text{mod}\,\Pi\mathfrak{l}_i^{2e_i}\Pi\bar{\mathfrak{l}}_i^{2e_i}).$$

Or, soient :

$\mathfrak{A}$, le groupe des idéaux de k premiers à $\mathfrak{b}$;

$\mathcal{H}$, le groupe des idéaux de la forme $\mathfrak{a}^2(\alpha)$, $\mathfrak{a}$ et α étant dans $\mathfrak{A}$;

$\mathcal{H}_{\tilde{\mathfrak{m}}}$, le groupe des idéaux de la forme $\mathfrak{a}^2(\gamma)$, $\mathfrak{a}$ étant dans $\mathfrak{A}$

$$\gamma\equiv 1 \qquad (\text{mod}\,\tilde{\mathfrak{m}});$$

et soit enfin

$$\bar{\mathcal{H}}=\mathcal{H}_{\mathfrak{b}\Pi\mathfrak{p}_{\infty,i}}.$$

Soit $\mathcal{G}$ un sous-groupe d'indice 2 de $\mathfrak{A}$ contenant $\mathcal{H}_{\tilde{\mathfrak{b}}}$, et soit $k(\sqrt{\beta})$ le corps de classes pour $\mathcal{G}$. La condition nécessaire et suffisante pour que $\mathfrak{f}$ soit dans $\mathcal{G}$ est $\left(\frac{\beta}{\mathfrak{f}}\right)=1$, c'est-à-dire si l'on pose

$$\beta=\Pi a_i^{x_i}\Pi b_i^{y_i}\Pi c_i^{z_i}\omega,$$

ω dans $H_{\tilde{\mathfrak{f}}}$, $\Sigma z_i\equiv 0\,(\text{mod.}\,2)$. Mais les $z_i\neq 0$ correspondent à des idéaux $\mathfrak{p}_{\infty,i}$ qui sont dans le conducteur de $\mathcal{G}$. Donc, la condition nécessaire et suffisante pour que $\mathfrak{f}$ soit dans $\mathcal{G}$ est que le nombre des idéaux $\mathfrak{p}_{\infty,i}$ divisant le conducteur de $\mathcal{G}$ soit pair.

Soit, d'autre part, β_{j_0} un nombre $\equiv 1$

$$\left(\text{mod. } \mathfrak{b}\Pi\tilde{\mathfrak{p}}_{\infty,i}\prod_{j\neq j_0}\mathfrak{p}_{\infty,j}\right),$$

mais $\not\equiv 1 \,(\text{mod. } \mathfrak{p}_{\infty,j_0})$. Considérons l'idéal $\frac{\mathfrak{f}}{\Pi_j(\beta_j)}$. Le groupe $\mathfrak{A}/\mathcal{H}_{\tilde{\mathfrak{b}}}$ est de type $(2, 2, \ldots, 2)$. Soit $\mathcal{G}$ un sous-groupe d'indice 2 de $\mathfrak{A}$ contenant $\mathcal{H}_{\tilde{\mathfrak{b}}}$. Si le conducteur de $\mathcal{G}$ ne contient pas $\mathfrak{p}_{\infty,j_0}$, (β_{j_0}) est dans $\mathcal{G}$, car β_{j_0} est congru à 1 modulo le conducteur de $\mathcal{G}$. Si le conducteur de $\mathcal{G}$ contient $\mathfrak{p}_{\infty,j_0}$, (β_{j_0}) n'appartient pas à $\mathcal{G}$. En effet, soit $\tilde{\mathfrak{n}}$ ce conducteur et soit

$$\tilde{\mathfrak{n}} = \tilde{\mathfrak{n}}_1 \mathfrak{p}_{\infty,j_0}.$$

Tout nombre $\equiv 1 \,(\text{mod. } \tilde{\mathfrak{n}}_1)$ est ou bien congru à $1 \,(\text{mod. } \tilde{\mathfrak{n}})$ ou bien produit d'un nombre $\equiv 1 \,(\text{mod. } \tilde{\mathfrak{n}})$ par β_{j_0}. Si β_{j_0} était dans $\mathcal{G}$, tout idéal représentable par un nombre $\equiv 1 \,(\text{mod. } \tilde{\mathfrak{n}}_1)$ serait dans $\mathcal{G}$, ce qui n'est pas. Donc $\Pi_j(\beta_j)$ appartient ou non à $\mathcal{G}$ suivant que le nombre des $\mathfrak{p}_{\infty,j}$ qui divisent le conducteur de $\mathcal{G}$ est pair ou impair. Donc $\frac{\mathfrak{f}}{\Pi_j(\beta_j)}$ appartient toujours à $\mathcal{G}$. Comme $\mathfrak{A}/\mathcal{H}_{\tilde{\mathfrak{b}}}$ est de type $(2, 2, \ldots, 2)$, l'idéal en question appartient à $\mathcal{H}_{\tilde{\mathfrak{b}}}$, ce qui démontre le théorème.