Christian Pitti

Étude des normes dans les extensions à groupe de Klein

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 14, nº 1 (1972-1973), exp. nº 7, p. 1-20
<http://www.numdam.org/item?id=SDPP_1972-1973__14_1_A5_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
14e année, 1972/73, n° 7, 20 p.

27 novembre 1972

ÉTUDE DES NORMES DANS LES EXTENSIONS À GROUPE DE KLEIN

par Christian PITTI

Soient k un corps commutatif de caractéristique différente de 2 , $K=k(\sqrt{a}\ , \sqrt{b})$ une extension biquadratique de k (a , b , ab étant des éléments de k^* non carrés dans k). Nous nous proposons l'étude de l'équation aux normes

(1) $$N_{K/k}(\delta) = A \ , \qquad A \in k^* \ .$$

Lorsque A , a , b sont fixés, (1) est une équation en δ au sujet de laquelle se posent naturellement les trois problèmes suivants :

- existence de solutions,
- détermination d'une solution,
- détermination de toutes les solutions.

Lorsque les deux premiers problèmes sont résolus, le dernier équivaut à la résolution complète de

(1') $$N_{K/k}(\delta') = 1 \ .$$

Des résultats de TATE - SERRE, exposés dans [1], donnent un critère d'existence pour (1) lorsque k est un corps de nombres et A carré dans k .

Lorsque a et b sont fixés, on peut étudier les liens existant entre les groupes N , N_1 , N_2 , N_3 des éléments de k^* , normes des corps respectifs K , $k(\sqrt{a})$, $k(\sqrt{b})$, $k(\sqrt{ab})$. Si k est un corps de nombres, on peut étudier le groupe E des éléments de k^* , normes partout locales dans K .

Des résultats de [1] indiquent que $N = E$ si l'un des degrés locaux est égal à 4 , sinon que N est un sous-groupe d'indice 2 de E .

Nous allons étudier ces différents problèmes par une méthode utilisant essentiellement le théorème de Minkowski relatif aux formes quadratiques.

1. Mise en équations.

Notons σ , τ les automorphismes de K laissant respectivement invariants $\sqrt{b}$ et $\sqrt{a}$. On a

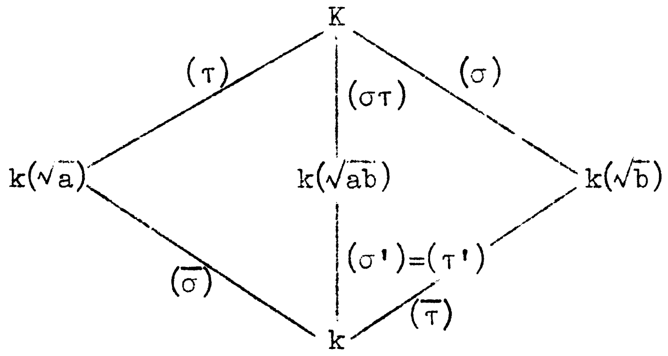
$$\sigma^2 = \tau^2 = 1 \ , \quad \sigma\tau = \tau\sigma \ .$$

Le corps fixe par $\sigma\tau$ est $k(\sqrt{ab})$. Notons

$\bar{\sigma}$, $\bar{\tau}$ les restrictions de σ , τ respectivement à $k(\sqrt{a})$, $k(\sqrt{b})$

σ' , τ' les restrictions de σ , τ à $k(\sqrt{ab})$.

Les différents groupes de Galois sont figurés sur le schéma suivant.



Si (1) admet une solution δ_0 , on a

$$(2) \qquad A = \alpha_0\,\sigma(\alpha_0) = \gamma_0\,\sigma(\gamma_0) \qquad \text{avec} \quad \begin{cases} \alpha_0 = \delta_0\,\tau(\delta_0) \in k(\sqrt{a}) \\ \gamma_0 = \delta_0\,\sigma\tau(\delta_0) \in k(\sqrt{ab}) \end{cases}$$

Inversement, supposons qu'il existe $\alpha_0 \in k(\sqrt{a})$, $\gamma_0 \in k(\sqrt{ab})$ tels que l'on ait (2). Alors

$$(1) \Longleftrightarrow N_{k(\sqrt{a})/k}\Big(\frac{\delta\tau(\delta)}{\alpha_0}\Big) = 1 \Longleftrightarrow \delta\tau(\delta) = \alpha_0\,\frac{\theta'}{\sigma(\theta')}\,, \qquad \theta' \in k(\sqrt{a})$$

$$(1) \Longleftrightarrow N_{k(\sqrt{ab})/k}\Big(\frac{\delta\sigma\tau(\delta)}{\gamma_0}\Big) = 1 \Longleftrightarrow \delta\sigma\tau(\delta) = \gamma_0\,\frac{\psi'}{\sigma(\psi')}\,, \qquad \psi' \in k(\sqrt{ab})$$

On en déduit

$$\sigma(\delta)\ \tau(\delta) = \sigma(\gamma_0)\,\frac{\sigma(\psi')}{\psi'} = \frac{A}{\gamma_0}\,\frac{\sigma(\psi')}{\psi'}$$

puis

$$\frac{\delta}{\sigma(\delta)} = \frac{\alpha_0\,\gamma_0}{A}\,\frac{\theta'\psi'}{\sigma(\theta'\psi')}$$

Or $N_{K/k(\sqrt{b})}((\alpha_0\,\gamma_0)/A) = 1$ d'après (2). Donc

$$(\exists\ u \in K) \qquad \frac{\alpha_0\,\gamma_0}{A} = \frac{u}{\sigma(u)} \qquad (\text{par exemple} \quad u = \frac{\alpha_0\,\gamma_0}{A} + 1)\ .$$

On peut donc écrire

$$\frac{\delta}{u\theta'\psi'} = \sigma\Big(\frac{\delta}{u\theta'\psi'}\Big)$$

soit $\delta = u\theta'\varphi'\psi'$, $\varphi' \in k(\sqrt{b})$, puis

$$(1) \Longleftrightarrow \alpha_0\,\frac{\theta'}{\sigma(\theta')} = \delta\tau(\delta) = u\theta'\varphi'\psi'\tau(u)\ \theta'\tau(\varphi'\psi') \Longleftrightarrow \theta'\sigma(\theta')\ \varphi'\tau(\varphi')\ \psi'\tau(\psi') = \frac{\alpha_0}{u\tau(u)}\ .$$

Le second membre est un élément A_1 de $k(\sqrt{a})$. Montrons qu'il appartient à k , c'est-à-dire qu'il est invariant par σ .

$$\alpha_0\,\sigma(\alpha_0)\,\gamma_0\,\tau(\gamma_0) = A^2 \Rightarrow \frac{\alpha_0\,\gamma_0}{A}\,\frac{\alpha_0\,\tau(\gamma_0)}{A} = \frac{\alpha_0}{\sigma(\alpha_0)} = \frac{u}{\sigma(u)}\,\tau\Big(\frac{u}{\sigma(u)}\Big) \Rightarrow \frac{\alpha_0}{u\tau(u)} = \sigma\Big(\frac{\alpha_0}{u\tau(u)}\Big)\ .$$

Dans le cas où l'on a choisi $u = ((\alpha_0\,\gamma_0)/A) + 1$, on a :

$$A^2\,u\tau(u) = (\alpha_0\,\gamma_0 + A)(\alpha_0\,\sigma(\gamma_0) + A) = \alpha_0(\alpha_0\,A + \sigma(\gamma_0)\,A + A\gamma_0 + A\sigma(\alpha_0))$$

donc

$$\frac{\alpha_0}{u\tau(u)} = \frac{A}{\alpha_0 + \sigma(\alpha_0) + \gamma_0 + \sigma(\gamma_0)}\ .$$

Nous avons démontré le résultat suivant.

THÉORÈME 1. - La résolution de (1) équivaut à celles de

$$(2)\qquad N_{k(\sqrt{a})/k}(\alpha_0) = N_{k(\sqrt{ab})/k}(\gamma_0) = A$$

$$(3)\qquad N_{k(\sqrt{a})/k}(\theta') \, N_{k(\sqrt{b})/k}(\varphi') \, N_{k(\sqrt{ab})/k}(\psi') = A_1 \ , \qquad A_1 \in k$$

avec

$$A_1 = \frac{\alpha_0}{u\tau(u)} \ , \quad \frac{u}{\sigma(u)} = \frac{\alpha_0 \gamma_0}{A} \ .$$

Les solutions de (1) sont données par $\delta = u\theta'\varphi'\psi'$.

Dans le cas particulier où $A = c^2$ $(c \in k)$, on peut choisir $\alpha_0 = \gamma_0 = c$, $u = 1$, et par suite $A_1 = c$.

COROLLAIRE. - La résolution de $N_{K/k}(\delta) = c^2$ équivaut à celle de

$$N_{k(\sqrt{a})/k}(\theta') \, N_{k(\sqrt{b})/k}(\varphi') \, N_{k(\sqrt{ab})/k}(\psi') = c \ .$$

Les solutions sont données par $\delta = \theta'\varphi'\psi'$. On a

$$c^2 \in N \Longleftrightarrow c \in N_1 N_2 N_3 \ .$$

Remarquons que les équations (2) équivalent à l'étude de la représentation de A sur k par les deux formes quadratiques

$$f_1 = X_1^2 - aY_2^2 \ , \quad g_1 = X_1^2 - abY_2^2 \ .$$

On peut également ramener la résolution de (3) à des études de formes quadratiques en posant $\theta'' = \frac{1}{\theta'}$, $\varphi'' = \varphi'$, $\psi'' = \frac{1}{\psi'}$.

(3) $\Longleftrightarrow$ (4) :

$$A_1 N_{k(\sqrt{a})/k}(\theta'') \, N_{k(\sqrt{ab})/k}(\psi'') = N_{k(\sqrt{b})/k}(\varphi'') \Leftrightarrow \begin{cases} N_{k(\sqrt{ab})/k}(\psi'') = n \\ A_1 \, n \, N_{k(\sqrt{a})/k}(\theta'') - N_{k(\sqrt{b})/k}(\varphi'') = 0 \end{cases}$$

ce qui équivaut à la représentation sur k de

0 par la forme quadratique $f = A_1 n(X^2 - aY^2) - Z^2 + bT^2$

n par la forme quadratique $g_1 = L^2 - abM^2$

Montrons que les groupes N , N_1 , N_2 , N_3 , k^{*2} sont liés par les relations suivantes.

THÉORÈME 2. - $Nk^{*2} = N_1 \cap N_2 = N_2 \cap N_3 = N_1 \cap N_3$.

Il suffit, pour raison de symétrie, de démontrer $Nk^{*2} = N_1 \cap N_3$. N et k^{*2} étant inclus dans $N_1 \cap N_3$, il en est de même de Nk^{*2} . Inversement :

$$A \in N_1 \cap N_3 \Rightarrow A = \alpha_0 \, \sigma(\alpha_0) = \gamma_0 \, \sigma(\gamma_0) \ , \qquad \alpha_0 \in k(\sqrt{a}) \ , \ \gamma_0 \in k(\sqrt{ab}) \ .$$

Si on pose

$$\frac{u}{\sigma(u)} = \frac{\alpha_0 \gamma_0}{A} \quad \text{et} \quad A_1 = \frac{\alpha_0}{u\tau(u)} \ ,$$

on sait que $A_1 \in k$,

$$A_1^2 = A_1\,\sigma(A_1) = \frac{\alpha_0\,\sigma(\alpha_0)}{N_{K/k(u)}} = \frac{A}{N_{K/k(u)}}$$

D'où $A = N_{K/k(u)}$, $A_1^2 \in Nk^{*2}$.

COROLLAIRE. - $Nk^{*2}/N \simeq k^*/N_1\,N_2\,N_3$.

Considérons en effet l'homomorphisme $\Phi_1 : x \in k^* \dashrightarrow x^2 \in k^{*2}$.

$$\Phi_1(N_1\,N_2\,N_3) = N \cap k^{*2}$$

d'après le corollaire au théorème 1. Donc $k^{*2}/N \cap k^{*2} \simeq k^*/N_1\,N_2\,N_3$. D'autre part, d'après un résultat de théorie des groupes

$$Nk^{*2}/N \simeq k^{*2}/N \cap k^{*2}$$

Posons $H = k(\sqrt{a})^* \times k(\sqrt{b})^* \times k(\sqrt{ab})^*$. Nous avons vu que les éléments de K ayant pour norme 1 sont donnés par $\varphi''/\theta''\psi''$ avec $(\theta'' , \varphi'' , \psi'') \in H$ et

(4')
$$N_{k(\sqrt{a})/k}(\theta'')\,N_{k(\sqrt{ab})/k}(\psi'') - N_{k(\sqrt{b})/k}(\varphi'') = 0 .$$

On pourrait aussi bien considérer les triplets de H vérifiant

(4")
$$N_{k(\sqrt{a})/k}(\theta'')\,N_{k(\sqrt{ab})/k}(\psi'') + N_{k(\sqrt{b})/k}(\varphi'') = 0 ,$$

en prenant -1 pour racine carrée de 1 .

L'application $\Phi_2 : (\theta'' , \varphi'' , \psi'') \in H \dashrightarrow (\varphi''/\theta''\psi'') \in K^*$ est un homomorphisme pour les structures de groupes multiplicatifs

$$(\theta'' , \varphi'' , \psi'') \in \operatorname{Ker}\Phi_2 \Leftrightarrow \psi'' = \frac{\varphi''}{\theta''} \Rightarrow \frac{\varphi''}{\theta''} \in k(\sqrt{ab}) \Rightarrow \frac{\varphi''}{\theta''} = \sigma\tau\left(\frac{\varphi''}{\theta''}\right) = \frac{\tau(\varphi'')}{\sigma(\theta'')} \Rightarrow \frac{\sigma(\theta'')}{\theta''} = \frac{\tau(\varphi'')}{\varphi''}$$

Le 1er terme est dans $k(\sqrt{a})$, le 2e dans $k(\sqrt{b})$.

La valeur commune est donc un élément π de k . On a

$$\pi^2 = \pi\,\sigma(\pi) = 1 , \text{ donc } \pi = \pm 1 .$$

Si $\pi = 1$, $\sigma(\theta'') = \theta''$ et $\tau(\varphi'') = \varphi''$, soit

$$\theta'' = d_1 \in k^* , \quad \varphi'' = d_2 \in k^* , \quad \psi'' = \frac{d_2}{d_1} .$$

Les triplets obtenus vérifient (4').

Si $\pi = -1$, $\sigma(\theta''\sqrt{a}) = \theta''\sqrt{a}$, $\tau(\varphi''\sqrt{b}) = \varphi''\sqrt{b}$, soit

$$\theta'' = \frac{d_1}{\sqrt{a}} , \quad \varphi'' = \frac{d_2}{\sqrt{b}} , \quad \psi'' = \frac{ad_2}{d_1\sqrt{ab}} \quad \text{avec } d_1 , d_2 \in k^* .$$

Les triplets obtenus vérifient (4"). On déduit de là les résultats suivants.

THÉORÈME 3. - _Si_ $(\theta_0'' , \varphi_0'' , \psi_0'') \in H$, _les triplets_ $(\theta'' , \varphi'' , \psi'')$ _de_ H _tels que_ $(\varphi''/\theta''\psi'') = (\varphi_0''/\theta_0''\,\psi_0'')$ _se répartissent en deux familles définies par_

$$\begin{cases} \left(d_1\,\theta_0'' , d_2\,\varphi_0'' , \dfrac{d_2}{d_1}\,\psi_0''\right) , & d_1 , d_2 \in k^* \\ \text{et} & \\ \left(\dfrac{d_1}{\sqrt{a}}\,\theta_0'' , \dfrac{d_2}{\sqrt{b}}\,\varphi_0'' , \dfrac{ad_2}{d_1\sqrt{ab}}\,\psi_0''\right) , & d_1 , d_2 \in k^* . \end{cases}$$

De plus, si un triplet est solution de (4) pour un certain A_1, il en est ainsi de tous ceux de sa famille. Ceux de l'autre famille vérifient alors l'équation (4) correspondant à $-A_1$.

Nous poserons dans toute la suite

$$G = \{x \mid x \in K^* \text{ et } N_{K/k}(x) = 1\}$$
$$G_1 = \{x \mid x \in K^* \text{ et } N_{K/k(\sqrt{b})}(x) = 1\} = \{\frac{\xi}{\sigma(\xi)}\}_{\xi\in K^*}$$
$$G_2 = \{x \mid x \in K^* \text{ et } N_{K/k(\sqrt{a})}(x) = 1\} = \{\frac{\eta}{\tau(\eta)}\}_{\eta\in K^*}$$
$$G_3 = \{x \mid x \in K^* \text{ et } N_{K/k(\sqrt{ab})}(x) = 1\} = \{\frac{\zeta}{\sigma\tau(\zeta)}\}_{\zeta\in K^*}$$

G_1, G_2, G_3 et $G_1\, G_2\, G_3$ sont des sous-groupes de G. De

$$\frac{\zeta}{\sigma\tau(\zeta)} = \frac{\zeta}{\tau(\zeta)}\, \sigma(\frac{\sigma\tau(\zeta)}{\tau(\zeta)}) ,$$

on déduit $G_3 \subset G_1\, G_2$ et $G_1\, G_2\, G_3 = G_1\, G_2$.

De l'égalité

$$\frac{\xi\eta}{\sigma(\xi)\ \tau(\eta)} = \Phi_2(\frac{1}{\xi\tau(\xi)} , \eta\sigma(\eta) , \sigma(\xi\eta)\ \tau(\xi\eta)),$$

et du théorème 3, on déduit que tous les triplets de H ayant pour image l'élément $\xi\eta/(\sigma(\xi)\ \tau(\eta))$ sont donnés par

$$(\frac{d_1}{\xi\tau(\xi)} , d_2\ \eta\sigma(\eta) , \frac{d_2}{d_1}\sigma(\xi\eta)\ \tau(\xi\eta)) .$$

Cherchons à caractériser ces triplets par une condition portant sur $N_{k(\sqrt{ab})/k}(\psi'')$.

De l'expression ci-dessus, on déduit

$$N_{k(\sqrt{ab})/k}(\psi'') = \frac{d_2^2}{d_1^2}\, N_{K/k}(\xi\eta) \in k^{*2}\, N$$

donc (théorème 2) :

$$N_{k(\sqrt{ab})/k}(\psi'') \in N_1 \cap N_3$$

soit $\delta \in G_1\, G_2 \Rightarrow N_{k(\sqrt{ab})/k}(\psi'') \in N_1$ lorsque $(\theta'' , \varphi'' , \psi'')$ vérifie (4').

Inversement :

$$N_{k(\sqrt{ab})/k}(\psi'') \in N_1 \iff N_{k(\sqrt{ab})/k}(\psi'') = \lambda^2\, N_{K/k}(\zeta) \qquad \lambda \in k^* , \zeta \in K$$
$$\iff N_{k(\sqrt{ab})/k}(\frac{\psi''}{\lambda\zeta\sigma\tau(\zeta)}) = 1 \iff \psi'' = \lambda\zeta\sigma\tau(\zeta)\ \frac{v}{\sigma(v)} , \qquad v \in k(\sqrt{ab}).$$

Portons dans (4') cette expression,

$$N_{k(\sqrt{a})/k}[\lambda\theta''\zeta\tau(\zeta)] = N_{k(\sqrt{b})/k}(\varphi'') .$$

La valeur commune est dans $N_1 \cap N_2$, donc dans N_3. Écrivons-la $N_{k(\sqrt{ab})/k}(\gamma)$.

On a

$$N_{K/k(\sqrt{b})}[\frac{\lambda\theta''\zeta\tau(\zeta)}{\gamma}] = N_{K/k(\sqrt{a})}(\frac{\varphi''}{\gamma}) = 1$$

soit

$$\theta'' = \frac{\gamma u}{\lambda\sigma(u)\ \zeta\tau(\zeta)} , \quad \varphi'' = \gamma \frac{w}{\tau(w)} \qquad u , w \in K$$

et

$$\frac{\varphi''}{\theta''\psi''} = \frac{\sigma(uv)\ \tau(\zeta)}{uv\sigma\tau(\zeta)} \times \frac{w}{\tau(w)} \in G_1\ G_2 .$$

THÉORÈME 4. - <u>Les éléments de</u> $G_1\ G_2$ <u>sont fournis par les solutions de</u> (4') <u>telles que</u> $N_{k(\sqrt{ab})/k}(\psi'') \in N_1$.

2. Étude des équations (2) et (4) lorsque k est un corps de nombres.

Notons E le groupe des éléments de k^* normes partout locales dans K . Tout élément A de E est norme (pour toute place $\wp$ de k) d'un élément de $k_\wp(\sqrt{a})$ et d'un élément de $k_\wp(\sqrt{ab})$.

D'après le théorème de Hasse, A est norme d'un élément α_0 de $k(\sqrt{a})$ et d'un élément γ_0 de $k(\sqrt{ab})$.

On a donc $E \subset N_1 \cap N_3$.

Montrons maintenant que $Nk^{*2} \subset E$. Vu l'inclusion triviale $N \subset E$, il suffit de montrer que $k^{*2} \subset E$.

Distinguons trois cas :

- si $k_\wp(\sqrt{a} , \sqrt{b}) = k_\wp$, on a $c^2 = N_{k_\wp(\sqrt{a},\sqrt{b})/k_\wp}(c^2)$.
- si $k_\wp(\sqrt{a} , \sqrt{b}) = k_\wp(\sqrt{a})$, on a $c^2 = N_{k_\wp(\sqrt{a},\sqrt{b})/k_\wp}(c)$, il en est de même si $k_\wp(\sqrt{a} , \sqrt{b}) = k_\wp(\sqrt{b})$ ou $k_\wp(\sqrt{a} , \sqrt{b}) = k_\wp(\sqrt{ab})$.
- si $k_\wp(\sqrt{a} , \sqrt{b})$ est une extension biquadratique de $k_\wp$, le corollaire au théorème 1 montre que

$$c^2 = N_{k_\wp(\sqrt{a},\sqrt{b})/k_\wp}(\delta) \Longleftrightarrow c = N_{k_\wp(\sqrt{a})/k_\wp}(\delta_1)\ N_{k_\wp(\sqrt{b})/k_\wp}(\delta_2)\ N_{k_\wp(\sqrt{ab})/k_\wp}(\delta_3)$$

ce qui est en particulier vérifié si c est norme locale pour l'un au moins des 3 corps $k_\wp(\sqrt{a})$, $k_\wp(\sqrt{b})$, $k_\wp(\sqrt{ab})$.

Or ceci résulte de la formule $(ab , c)_\wp = (a , c)_\wp\ (b , c)_\wp$ entre symboles de Hilbert sur $k_\wp$.

Des résultats obtenus et du théorème 2, on déduit le résultat suivant.

THEOREME 5. - $E = Nk^{*2} = N_1 \cap N_2 = N_2 \cap N_3 = N_1 \cap N_3$.

COROLLAIRE. - <u>L'indice de</u> N <u>dans</u> E <u>est égal à l'indice de</u> $N_1\ N_2\ N_3$ <u>dans</u> k^*.

Cela résulte du théorème 5 et du corollaire au théorème 2.

Pour étudier les formes quadratiques f_1 , g_1 , f , nous utiliserons le théorème de Minkowski :

"<u>Une forme quadratique sur</u> k <u>représente un élément</u> B <u>de</u> k <u>si, et seulement</u>

<u>si, elle représente</u> B <u>sur tous les complétés</u> $k_{\wp}$ <u>de</u> k , $\wp$ <u>étant une place quelconque de</u> k ".

On obtient ainsi pour les trois premières formes, les résultats ci-après.

THÉORÈME 6. - f_1 <u>et</u> g_1 <u>représentent</u> A <u>sur</u> $k \Longleftrightarrow (\forall \wp) \quad (a,A)_{\wp} = (b,A)_{\wp} = 1$.

THÉORÈME 7. - g_1 <u>représente</u> n <u>sur</u> $k \Longleftrightarrow (\forall \wp) \quad s_{\wp} = (ab,n)_{\wp} = 1$.

Les résultats relatifs à f sont donnés par le théorème suivant.

THÉORÈME 8. - f <u>représente</u> 0 <u>sur</u> $k \Longleftrightarrow (\forall \wp)$

$$[(a,b \notin k_{\wp}^{*2} \ \underline{\text{et}} \ ab \in k_{\wp}^{*2}) \Rightarrow r_{\wp} = (a,A_1 n)_{\wp} = 1] .$$

Démontrons-le. Sur $k_{\wp}$, f représente $0 \Longleftrightarrow A_1 n \in N_{1,\wp} N_{2,\wp}$, $N_{1,\wp}$ et $N_{2,\wp}$ étant les groupes des éléments de $k_{\wp}^*$ normes des corps respectifs $k_{\wp}(\sqrt{a})$, $k_{\wp}(\sqrt{b})$.

Cette condition est en particulier vérifiée si

$$a \in k_{\wp}^{*2} \text{ , car alors } N_{1,\wp} = k_{\wp}^* ,$$
$$b \in k_{\wp}^{*2} \text{ , car alors } N_{2,\wp} = k_{\wp}^* .$$

Supposons donc a et b non carrés dans $k_{\wp}^*$, et remarquons que

$$N_{1,\wp} = N_{2,\wp} \Leftrightarrow (\forall x \in k_{\wp}^*) \quad (a , x)_{\wp} = (b , x)_{\wp} \Leftrightarrow (\forall x \in k_{\wp}^*) \quad (ab , x)_{\wp} = 1$$
$$\Leftrightarrow ab \in k_{\wp}^{*2} \Leftrightarrow k_{\wp}(\sqrt{a}) = k_{\wp}(\sqrt{b}) .$$

si $ab \in k_{\wp}^{*2}$: f représente $0 \Longleftrightarrow A_1 n \in N_{1,\wp} \Longleftrightarrow (a , A_1 n)_{\wp} = 1$,

si $ab \notin k_{\wp}^{*2}$ et $A_1 n \in N_{1,\wp} \cup N_{2,\wp}$, f représente 0 ,

si $ab \notin k_{\wp}^{*2}$ et $A_1 n \notin N_{1,\wp} \cup N_{2,\wp}$, on a $N_{1,\wp} \neq N_{2,\wp}$.

Etant tous deux d'indice 2 dans $k_{\wp}^*$, aucun des deux n'est inclu dans l'autre. Prenons $n' \in N_{1,\wp} - N_{2,\wp}$

$$A_1 n \notin N_{2,\wp} \text{ et } n' \notin N_{2,\wp} \Rightarrow A_1 nn' \in N_{2,\wp}$$

car $N_{2,\wp}$ est d'indice 2 dans $k_{\wp}^*$

$$n' \in N_{1,\wp} \text{ et } A_1 nn' \in N_{2,\wp} \Rightarrow A_1 nn'^2 \in N_{1,\wp} N_{2,\wp} \Rightarrow A_1 n \in N_{1,\wp} N_{2,\wp}$$

et f représente 0 .

Nous sommes en mesure de démontrer le résultat suivant.

THÉORÈME 9. - <u>Si tous les degrés locaux sont inférieurs ou égaux à</u> 2 , <u>on a</u> $G = G_1 G_2$ (<u>autrement dit</u> : $N_{K/k}(\delta) = 1 \Longleftrightarrow \delta = \xi\eta/(\sigma(\xi)\ \tau(\eta))$, $\xi , \eta \in K^*$).

Rappelons que le degré local en $\wp$ est $[k_{\wp}(\sqrt{a} , \sqrt{b}):k_{\wp}]$. Il est inférieur ou égal à 2 si, et seulement si, a , b ou ab est carré dans $k_{\wp}$.

D'après le théorème 4, il s'agit de montrer que si $\varphi''/\theta''\psi''$ a pour norme 1 , on a $n = N_{k(\sqrt{ab})/k}(\psi'') \in N_1$, c'est-à-dire $(\forall \mathfrak{p})$ $(a , n)_{\mathfrak{p}} = 1$. Cela est réalisé si $a \in k_{\mathfrak{p}}^{*2}$.

Si $b \in k_{\mathfrak{p}}^{*2}$, cela résulte de

$$n \in N_3 \Longleftrightarrow (\forall \mathfrak{p}) \quad (ab , n)_{\mathfrak{p}} = 1 \Longleftrightarrow (\forall \mathfrak{p}) \quad (a , n)_{\mathfrak{p}} = (b , n)_{\mathfrak{p}} .$$

Si $a , b \notin k_{\mathfrak{p}}^{*2}$, on a $ab \in k_{\mathfrak{p}}^{*2}$ d'après l'hypothèse sur les degrés locaux. La condition $(a , n)_{\mathfrak{p}} = 1$ est alors vérifiée d'après le théorème 8.

3. Étude de l'équation (4) lorsque $k = Q$.

Nous supposerons, à partir de maintenant, que k est le corps des rationnels. On peut alors supposer que a et b sont des entiers sans facteurs carrés.

Nous supposerons satisfaites les conditions pour que (2) ait des solutions. On sait alors déterminer effectivement les nombres α_0 , γ_0 , $A_1 = \frac{A}{\alpha_0+\sigma(\alpha_0)+\gamma_0+\sigma(\gamma_0)}$.

On peut de plus supposer $A_1 > 0$ en remplaçant au besoin (α_0 , γ_0) par $(- \alpha_0 , - \gamma_0)$.

Rappelons que (4) s'écrit

$$A_1 \, N_{Q(\sqrt{a})/Q}(\theta'') \, N_{Q(\sqrt{ab})/Q}(\psi'') = N_{Q(\sqrt{b})/Q}(\varphi'')$$

et que les solutions de (1) sont données par

$$\delta = (\frac{\alpha_0 \gamma_0}{A} + 1) \frac{\varphi''}{\theta''\psi''} .$$

Montrons qu'on peut, sans restreindre le problème, supposer $N_{Q(\sqrt{ab})/Q}(\psi'')$ entier sans facteurs carrés.

Soit en effet

$$\delta_0 = (\frac{\alpha_0 \gamma_0}{A} + 1) \frac{\varphi_0''}{\theta_0'' \psi_0''}$$

une solution de (1).

Posons $N_{Q(\sqrt{ab})/Q}(\psi_0'') = q^2 p$, $q \in Q$, p entier sans facteurs carrés. D'après le théorème 3, δ_0 est également obtenu à partir du triplet

$$(q\theta_0'' , \varphi_0'' , \frac{\psi_0''}{q})$$

qui vérifie (4).

On a $N_{Q(\sqrt{ab})/Q}(\frac{\psi_0''}{q}) = p$.

Posons en effet $A_1 = A_1'^2 c$ avec $A_1' \in Q$ et c entier sans facteurs carrés. (4) s'écrit alors

$$c \, N_{Q(\sqrt{a})/Q}(\theta) \, N_{Q(\sqrt{ab})/Q}(\psi) = N_{Q(\sqrt{b})/Q}(\varphi) \tag{5}$$

avec

$$\theta = A_1' \, \theta'' \ , \qquad \varphi = \varphi'' \ , \qquad \psi = \psi'' \ .$$

Les solutions de (1) sont alors données par

$$\delta = \left(\frac{\alpha_0 \, \gamma_0}{A} + 1\right) \frac{\varphi}{A_1' \, \theta \psi} \ .$$

Pour étudier l'équation (5), nous utiliserons les théorèmes 7 et 8.

Nous poserons $d = \operatorname{pgcd}(a \, , \, b)$, $a = da'$, $b = db'$ et

$$\begin{cases} a' = (-1)^{\alpha} \, 2^{\alpha_1} \, p_1 \ldots p_r \\ b' = (-1)^{\beta} \, 2^{\beta_1} \, q_1 \ldots q_s \\ d = 2^{\gamma_1} \, u_1 \ldots u_t \end{cases}$$

$\alpha \, , \, \beta \, , \, \alpha_1 \, , \, \beta_1 \, , \, \gamma_1 \in \{0 \, , \, 1\}$.

Rappelons que, si u et v sont deux entiers et p un premier ne divisant ni u ni v ,

$$(p^{\alpha} \, u \, , \, p^{\beta} \, v)_p = \begin{cases} (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^{\beta} \left(\frac{v}{p}\right)^{\alpha} & \text{pour } p \neq 2 \\ (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)} & \text{pour } p = 2 \end{cases}$$

si on pose

$$\varepsilon(z) \equiv \frac{z-1}{2} \ (2) \ , \quad \omega(z) \equiv \frac{z^2-1}{8} \ (2)$$

$$p^n \, u \text{ est un carré de } Q_p \Longleftrightarrow \begin{cases} n \text{ pair et } \left(\frac{u}{p}\right) = 1 & \text{pour } p \neq 2 \\ n \text{ pair et } u \equiv 1 \ (8) & \text{pour } p = 2 \ . \end{cases}$$

La condition $u \equiv 1 \ (8)$ équivaut à $\varepsilon(u) = \omega(u) = 0$.

1° <u>Représentation de</u> 0 <u>par</u> f <u>sur</u> Q . – On doit avoir, pour $p = 2$,

$$(a \, , \, b \notin Q_2^{*2} \ \text{ et } \ ab \in Q_2^{*2}) \Rightarrow (a \, , \, cn)_2 = 1 \ .$$

Si p divise $a' \, b'$, on a $p | ab$ et $p^2 \nmid ab$, donc $ab \notin Q_p^{*2}$, et f représente 0 .

Si p divise d , on a $a \, , \, b \notin Q_p^{*2}$,

$$ab \in Q_p^{*2} \Longleftrightarrow a' \, b' \in Q_p^{*2} \Longleftrightarrow \left(\frac{a' \, b'}{p}\right) = 1 \Longleftrightarrow \left(\frac{a'}{p}\right) = \left(\frac{b'}{p}\right) \ .$$

Chaque fois que cette condition est vérifiée, on doit avoir

$$r_p = (a \, , \, cn)_p = 1 \ .$$

Si p ne divise pas ab et diffère de 2 :

$$(a \, , \, b \notin Q_p^{*2} \ \text{ et } \ ab \in Q_p^{*2}) \Longleftrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1 \ .$$

Posons

$$\begin{cases} c = p^{v_p(c)} u & \text{avec } p \nmid u \text{ et } v_p(c) \in \{0 , 1\} , \\ n = p^{v_p(n)} v & \text{avec } p \nmid v \text{ et } v_p(n) \in \{0 , 1\} . \end{cases}$$

On a alors

$$r_p = (a , p^{v_p(c)+v_p(n)} uv)_p = (\tfrac{a}{p})^{v_p(c)+v_p(n)} = (-1)^{v_p(c)+v_p(n)}$$

et

$$r_p = 1 \Leftrightarrow v_p(n) = v_p(c) .$$

Autrement dit, les premiers impairs tels que $(a/p) = (b/p) = -1$ doivent être les mêmes pour c et n .

Soient alors

c' le produit des diviseurs premiers impairs de c tels que $(\frac{a}{p}) = (\frac{b}{p}) = -1$

c_1 , c_2 les produits des diviseurs premiers impairs de c et n tels que $(a/p) = 1$ ou $(b/p) = 1$.

On aura

$$c = c'c_1 \, 2^{\lambda} \prod_{i=1}^{r} p_i^{\mu_i} \prod_{j=1}^{s} q_j^{\nu_j} \prod_{K=1}^{t} u_K^{\rho_K} ,$$

$$n = (-1)^{\gamma} c'c_2 \, 2^{\lambda'} \prod_{i=1}^{r} p_i^{\mu'_i} \prod_{j=1}^{s} q_j^{\nu'_j} \prod_{K=1}^{t} u_K^{\rho'_K} .$$

La représentation sur $\underset{\sim}{R}$ exige de plus que γ soit nul lorsque a et b sont négatifs. Remarquons que les inconnues γ , λ' , μ'_i , ν'_j , ρ'_K valent 0 ou 1 , et que c_2 est un entier naturel sans facteurs carrés.

2° Représentation de n par g_1 sur Q . - La représentation sur $\underset{\sim}{R}$ exige que γ soit nul lorsque $ab < 0$. On doit avoir $(ab , n)_2 = (a'b' , n)_2 = 1$,

$$(\forall\, i) , (\forall\, j) \qquad s_{p_i} = s_{q_j} = 1$$

Si $p = u_K$, $s_{u_K} = (a'b'/u_K)^{\rho'_K}$.

Dans le cas où $(a'b'/u_K) = 1$, on a $s_{u_K} = 1$. Sinon $s_{u_K} = 1 \Leftrightarrow \rho'_K = 0 \Leftrightarrow u_K \nmid n$.

Si p ne divise pas ab , plusieurs cas sont à envisager

$$(p \nmid c' \text{ et } p \nmid c_2) \Rightarrow s_p = 1 ,$$

$$p | c' \Rightarrow s_p = (\tfrac{a}{p})(\tfrac{b}{p}) = (-1)^2 = 1 \quad \text{d'après la définition de } c' .$$

Si $p | c_2$,

$$s_p = 1 \Leftrightarrow (\tfrac{a}{p}) = (\tfrac{b}{p}) = 1 \quad \text{d'après la définition de } c_2 ,$$

$$\Leftrightarrow (a , n)_p = (b , n)_p = 1 .$$

Cela implique

$$\prod_{p|c_2}(ab\ ,\ n)_p = \prod_{p|c_2}(a\ ,\ n)_p$$

Explicitons ces deux conditions.

D'après la formule du produit, on a :

$$\prod_{p|c_2}(ab,n)_p = \prod_{p|c'}(ab,c')_p \prod_{i=1}^{r}(ab,n)_{p_i} \prod_{j=1}^{s}(ab,n)_{q_j} \prod_{K=1}^{t}(ab,n)_{u_K}(ab,n)_2\,(ab,n)_\infty$$

et cela vaut 1 d'après les autres équations et compte tenu de ce que

$$(ab\ ,\ c')_p = (\frac{ab}{p}) = (-1)^2 = 1\ .$$

On a de même

$$\prod_{p|c_2}(a\ ,\ n)_p = \prod_{p|c'}(a\ ,\ n)_p \prod_{i=1}^{r}(a\ ,\ n)_{p_i} \prod_{K=1}^{t}(a\ ,\ n)_{u_K}\ (a\ ,\ n)_2\ (a\ ,\ n)_\infty$$

Or $\prod_{p|c'}(a\ ,\ c')_p = (-1)^R$, R étant le nombre de premiers divisant c'

$$(a\ ,\ n)_{p_i} = (b\ ,\ n)_{p_i} = (\frac{b}{p_i})^{\mu'_i}$$

$$(a\ ,\ n)_{q_j} = (\frac{a}{q_j})^{\nu'_j}$$

$$(a\ ,\ n)_{u_K} = \begin{cases}(a\ ,\ c)_{u_K} & \text{pour } K = 1\ ,\ \dots\ ,\ t_1\\ (\frac{n}{u_K}) & \text{pour } K = t_1+1\ ,\ \dots\ ,\ t\end{cases}$$

en supposant

$$(\frac{a'b'}{u_K}) = \begin{cases}1 & \text{pour } K = 1\ ,\ \dots\ ,\ t_1\\ -1 & \text{pour } K = t_1+1\ ,\ \dots\ ,\ t\end{cases}$$

et $t_1 = 0$ si $(a'b'/u_K) = -1$ quel que soit K .

Compte tenu de ces valeurs, on obtient la condition

$$(a\ ,\ n)_2 \prod_{i=1}^{r}(\frac{b}{p_i})^{\mu'_i} \prod_{j=1}^{s}(\frac{a}{q_j})^{\nu'_j} \prod_{K=t_1+1}^{t}(\frac{n}{u_K}) = (-1)^R \prod_{K=1}^{t_1}(a\ ,\ c)_{u_K}\ .$$

Récrivons le système des équations du problème en posant

$$\begin{cases} n = c'c_2\ 2^{\lambda'}\ n_1\\ n_1 = (-1)^\gamma \prod_{i=1}^{r} p_i^{\mu'_i} \prod_{j=1}^{s} q_j^{\nu'_j} \prod_{K=1}^{t_1} u_K^{\rho'_K}\ .\end{cases}$$

THÉORÈME 10. - <u>L'équation</u> (5) <u>équivaut au système</u> (S) <u>suivant</u> :

$$
(S')\begin{cases}
\gamma\alpha = \gamma\beta = 0 \\
(ab\ ,\ 2^{\lambda'}\ c_2)_2 = (ab\ ,\ c'n_1)_2 \\
(a\ ,\ b \notin Q_2^{*2}\ \text{ et }\ ab \in Q_2^{*2}) \Rightarrow (a\ ,\ 2^{\lambda'}\ c_2)_2 = (a\ ,\ cc'n_1)_2 \\
(a\ ,\ 2^{\lambda'}\ c_2)_2\ {}_{i=1}^{r}(\frac{b}{p_i})^{\mu'_i} \prod_{j=1}^{s}(\frac{a}{q_j})^{\nu'_j} \prod_{K=t_1+1}^{t}(\frac{2^{\lambda'}\ c_2}{u_K}) \\
\qquad\qquad = (-\ 1)^R \prod_{K=1}^{t_1}(a\ ,\ c)_{u_K}\ (a\ ,\ c'n_1)_2 \prod_{K=t_1+1}^{t}(\frac{c'n_1}{u_K}) \\
(\forall\ i)\quad (\frac{c_2}{p_i}) = (ab\ ,\ 2^{\lambda'}\ c'n_1)_{p_i} \\
(\forall\ j)\quad (\frac{c_2}{q_j}) = (ab\ ,\ 2^{\lambda'}\ cn_1)_{q_j} \\
(\frac{c_2}{u_K}) = (a\ ,\ cc'\ 2^{\lambda'}\ n_1)_{u_K} \quad \text{pour}\ K = 1\ ,\ \dots\ ,\ t_1\ .
\end{cases}
$$

$$(S'')\quad p \mid c_2 \Rightarrow (\frac{a}{p}) = (\frac{b}{p}) = 1\ .$$

On voit qu'on peut considérer (S') comme un système (Σ) par rapport aux inconnues <u>auxiliaires</u> γ , λ' , $\varepsilon(c_2)$, $\omega(c_2)$, μ'_i , ν'_j , ρ'_K , (c_2/p_i) , (c_2/q_j) , (c_2/u_K) . La détermination effective de c_2 se fait ensuite en utilisant (S'').

Les inconnues auxiliaires ne prenant chacune que 2 valeurs, on peut, par un nombre fini d'essais, déterminer si (Σ) possède ou non des solutions.

S'il n'y a pas de solutions, l'équation (1) n'en a pas non plus. Sinon la connaissance de γ , μ'_i , ν'_j , ρ'_K entraîne celle de n_1 . De plus, on peut alors trouver un premier c_2 correspondant aux valeurs trouvées pour $\varepsilon(c_2)$, $\omega(c_2)$, (c_2/p_i) , (c_2/q_j) , (c_2/u_K) .

Un tel premier doit être congru à certains entiers suivant les modules 8 , p_i , q_j , u_K , ces entiers étant

- impairs pour le module 8 ,
- égaux à un résidu quadratique lorsque le symbole de Legendre vaut 1 ,
- égaux à un non-résidu quadratique lorsque le symbole de Legendre vaut $-\ 1$.

Les entiers 8 , p_i , q_j , u_K étant premiers entre eux 2 à 2 , ce système de congruences admet des solutions dans $\underset{\sim}{N}$ d'après le théorème chinois.

Soit x_0 l'une de ces solutions ; tous les entiers congrus à x_0 modulo

$$8 \prod_{i=1}^{r} p_i \prod_{j=1}^{s} q_j \prod_{K=1}^{t} u_K$$

sont aussi solutions.

x_0 étant premier avec le module, le théorème de Dirichlet affirme l'existence de premiers parmi ces solutions.

Le calcul, fait page 11, montre alors que

$$(a , n)_{c_2} = (ab , n)_{c_2} = 1$$

ce qui signifie que c_2 est solution de (S").

On aboutit ainsi au théorème suivant.

THÉORÈME 11. - (S) a des solutions si, et seulement si, (Σ) en a.

A toute solution de (Σ) (par rapport aux inconnues auxiliaires) correspondent des solutions de (S) avec c_2 premier.

Il en résulte que les problèmes de l'existence d'une solution de (S) et de la détermination de l'une d'entre elles équivalent aux mêmes problèmes relativement à (Σ). L'étude de (Σ) se fait aisément du fait que chaque inconnue auxiliaire ne peut prendre que deux valeurs.

On cherche les ensembles de valeurs de ces inconnues vérifiant (Σ). Si l'on en trouve aucun, (S) n'a pas de solution, et il en est de même de l'équation (1).

Sinon on considère un tel ensemble. Il lui correspond, d'après le théorème 11, au moins une solution de (S) avec c_2 premier. On obtient ainsi une valeur n_0 pour l'entier n.

Il reste à trouver $(\theta_0 , \varphi_0 , \psi_0) \in H$ tel que

$$\begin{cases} N_{Q(\sqrt{ab})/Q}(\psi_0) = n_0 , \\ cn_0 \, N_{Q(\sqrt{a})/Q}(\theta_0) - N_{Q(\sqrt{b})/Q}(\varphi_0) = 0 . \end{cases}$$

On est ramené à la recherche d'une représentation de n_0 par une forme quadratique à deux variables, et de 0 par une forme à quatre variables.

Cela fournit une solution particulière Δ de (1).

Posant $\delta = \Delta\delta'$, on voit que

$$(1) \qquad N_{K/Q}(\delta) = A \Longleftrightarrow (1') \qquad N_{K/Q}(\delta') = 1 .$$

Nous verrons, dans le paragraphe 5, comment l'on peut effectivement obtenir toutes les solutions de (1'). Nous allons auparavant étudier de plus près le problème de l'existence de solutions de (5).

4. Degrés locaux et existence de solutions de (5).

1° Etude des degrés locaux. - Rappelons que, si p est premier, le degré local en p est, par définition, $\pi_p = [Q_p(\sqrt{a}, \sqrt{b}) : Q_p]$, et que $\pi_p \in \{1 , 2 , 4\}$.

Il en résulte que

$$\pi_p \leq 2 \Longleftrightarrow (a \in Q_p^{*2} , \text{ ou } b \in Q_p^{*2} , \text{ ou } ab \in Q_p^{*2}) .$$

Si $p = 2$ et $\pi_2 \leq 2$, on peut supposer, par raison de symétrie, $a \in Q_2^{*2}$ c'est-à dire $a \equiv 1 \pmod 8$.

Si p est impair et ne divise pas ab , on a :

$$\pi_p \leqslant 2 \Longleftrightarrow [(\frac{a}{p}) = 1 \quad \text{ou} \quad (\frac{b}{p}) = 1 \quad \text{ou} \quad (\frac{ab}{p}) = 1] .$$

ce qui est toujours vérifié du fait que $(ab/p) = (a/p)(b/p)$.

$$\pi_{p_i} \leqslant 2 \Longleftrightarrow (\frac{b}{p_i}) = 1 \quad \text{puisque} \quad a , ab \notin Q_{p_i}^{*2} ,$$

$$\pi_{q_j} \leqslant 2 \Longleftrightarrow (\frac{a}{q_j}) = 1 \quad \text{puisque} \quad b , ab \notin Q_{q_j}^{*2} .$$

Enfin, si $p = u_K$, on a $a , b \notin Q_{u_K}^{*2}$, donc

$$\pi_{u_K} \leqslant 2 \Longleftrightarrow ab \in Q_{u_K}^{*2} \Longleftrightarrow a'b' \in Q_{u_K}^{*2} \Longleftrightarrow (\frac{a'b'}{u_K}) = 1 .$$

2° <u>Étude du cas où l'un au moins des degrés locaux est égal à</u> 4 . - Montrons que (Σ) possède alors toujours des solutions.

Si $\pi_2 = 4$, nous choisirons $n_1 = 1$ (c'est-à-dire $\gamma = \mu_i' = \nu_j' = \rho_K' = 0$) .

Nous déterminerons λ' , $\varepsilon(c_2)$, $\omega(c_2)$ par les équations

$$\begin{cases} (a'b' , 2^{\lambda'} c_2)_2 = (ab , c')_2 , \\ (a , 2^{\lambda'} c_2)_2 = (-1)^R \prod_{K=1}^{t_1} (a , c)_{u_K} (a , c')_2 . \end{cases}$$

Cela est possible, car les premiers membres de ces équations s'écrivent

$$\varepsilon(\frac{a'b'}{2^{\alpha_1+\beta_1}})\ \varepsilon(c_2) + \lambda' \omega(\frac{a'b'}{2^{\alpha_1+\beta_1}}) + (\alpha_1 + \beta_1)\ \omega(c_2) \equiv \dots$$

$$\varepsilon(\frac{a}{2^{\alpha_1+\gamma_1}})\ \varepsilon(c_2) + \lambda' \omega(\frac{a}{2^{\alpha_1+\gamma_1}}) + (\alpha_1 + \gamma_1)\ \omega(c_2) \equiv \dots$$

et on constate que, dans l'hypothèse $\pi_2 = 4$, il existe toujours un déterminant d'ordre 2 non nul.

On prendra enfin $(c_2/u_K) = ((2^{\lambda'} c')/u_K)$ pour $K = t_1 + 1 , \dots , t$. Les autres inconnues (c_2/p_i) , (c_2/q_j) , (c_2/u_K) pour $K = 1 , \dots , t_1$ sont données par les dernières équations de (Σ) .

Supposons maintenant $\pi_2 \leqslant 2$. On peut alors supposer $a \in Q_2^{*2}$.

Distinguons deux cas selon que $t_1 \neq t$ ou $t_1 = t$.

Si l'on a $t_1 \neq t$, on peut prendre $n_1 = 1$, déterminer λ' , $\varepsilon(c_2)$, $\omega(c_2)$ par

$$(b , 2^{\lambda'} c_2)_2 = (b , c')_2$$

et choisir

$$(\frac{c_2}{u_t}) = (-1)^R \prod_{K=1}^{t_1} (a , c)_{u_K} \prod_{K=t_1+1}^{t} (\frac{2^{\lambda'} c'}{u_K}) \qquad (\frac{c_2}{u_K}) = 1 \quad \text{pour} \quad t_1+1 \leqslant K \leqslant t-1 .$$

Si $t_1 = t$ et $\pi_{p_{i_0}} = 4$, on prend $\mu_i' = 0$ pour $i \neq i_0$, $\nu_j' = \rho_K' = 0$, et on détermine μ_{i_0}' , λ' , $\varepsilon(c_2)$, $\omega(c_2)$ par

$$(-1)^{\mu'_{i_0}} = (-1)^R \prod_{K=1}^{t} (a\ ,\ c)_{u_K}\ ,$$

$$(b\ ,\ 2^{\lambda'}\ c_2)_2 = (b\ ,\ c')_2\ .$$

On fait un raisonnement analogue lorsque $t_1 = t$ et $\pi_{q_{j_0}} = 4$.

On aboutit donc au résultat suivant.

THÉORÈME 12. - Si l'un au moins des degrés locaux est égal à 4 , $N_1\ N_2\ N_3 = Q^*$.

COROLLAIRE. - Sous les mêmes hypothèses, toute norme locale est norme globale $(E = N)$.

Ce dernier point résulte du théorème 12 et du corollaire au théorème 5.

3° Étude du cas où tous les degrés locaux sont inférieurs ou égaux à 2 . - On a alors

$$(\forall\ i)\ (\forall\ j)\ (\forall\ K) \qquad \left(\frac{b}{p_i}\right) = \left(\frac{a}{q_j}\right) = \left(\frac{a'b'}{u_K}\right) = 1 \quad (\text{donc } t_1 = t\ )$$

et on peut remplacer $\pi_2 \leqslant 2$ par $a \in Q_2^{*2}$.

La 4e équation de (Σ) implique alors $\prod_{K=1}^{t}(a\ ,\ c)_{u_K} = (-1)^R$. Si cette condition est satisfaite, on a une solution de (Σ) en choisissant $n_1 = 1$, et en déterminant λ' , $\varepsilon(c_2)$, $\omega(c_2)$ par l'équation

$$(b\ ,\ 2^{\lambda'}\ c_2)_2 = (b\ ,\ c')_2\ .$$

Si l'on se souvient de la définition de c à partir de A_1 (début du § 3), on peut énoncer le théorème suivant.

THÉORÈME 13. - Lorsque tous les degrés locaux sont inférieurs ou égaux à 2 , un rationnel P/Q appartient à $N_1\ N_2\ N_3$ si, et seulement si,

$$\prod_{K=1}^{t}\left(a\ ,\ \frac{P}{Q}\right)_{u_K} = (-1)^R\ ,$$

R étant le nombre de diviseurs premiers impairs de PQ tels que $(a/p)=(b/p)=-1$.

Cet énoncé suppose que l'on soit dans le cas $a \in Q_2^{*2}$.

En particulier, si a et b sont premiers entre eux, cette condition s'écrit simplement " R pair".

Remarque. - Ce critère d'existence est la traduction, pour $k = Q$, de celui de [1], p. 360, à savoir $\prod_{p\in S_2}(a\ ,\ c)_p = 1$, S_2 étant l'ensemble des premiers qui se décomposent dans $Q(\sqrt{b})$.

On déduit du théorème 13 le résultat suivant, qui figure dans [1] pour un corps global quelconque.

THÉORÈME 14. - Lorsque tous les degrés locaux sont inférieurs ou égaux à 2 , N

<u>est un sous-groupe d'indice</u> 2 <u>de</u> E .

Il suffit, d'après le corollaire au théorème 5, de montrer que

$$\begin{cases} N_1 N_2 N_3 \neq Q^* , \\ (\frac{P_1}{Q_1} , \frac{P_2}{Q_2} \notin N_1 N_2 N_3) \Rightarrow \frac{P_1 P_2}{Q_1 Q_2} \in N_1 N_2 N_3 . \end{cases}$$

Le deuxième point résulte immédiatement du théorème 13. Quant au premier, il s'agit de démontrer l'existence d'entiers c tels que

$$\prod_{K=1}^{t} (a , c)_{u_K} = (-1)^{R+1} .$$

Si a et b sont premiers entre eux, il suffit de choisir c tel que R soit impair.

Si $d \neq 1$, on peut supposer $i \neq 0$ (sinon on se ramènerait au cas précédent en remplaçant b par ab/d^2).

Choisissons alors c premier tel que :

$$\begin{cases} \varepsilon(c) = 0 , \\ (\frac{c}{p_1}) = (\frac{c}{u_1}) = -1 , \\ (\frac{c}{p_i}) = (\frac{c}{u_K}) = 1 \quad \text{pour} \quad i \neq 1 , K \neq 1 . \end{cases}$$

On aura

$$(\frac{a}{c}) = (-1)^{\alpha\varepsilon(c)} \prod_{i=1}^{r} (\frac{p_i}{c}) \prod_{K=1}^{t} (\frac{u_K}{c}) = \prod_{i=1}^{r} (\frac{c}{p_i}) \prod_{K=1}^{t} (\frac{c}{u_K}) = 1 ,$$

donc $R = 0$ et $\prod_{K=1}^{t} (a , c)_{u_K} = (c/u_1) = -1$.

5. <u>Détermination des éléments de</u> K <u>de norme</u> 1 <u>sur</u> Q .

Ce sont les solutions de (1') $N_{K/Q}(\delta') = 1$.

Appliquons la méthode du § 3 avec $c = 1$

$$\delta' \in G \Longleftrightarrow \begin{cases} \delta' = \frac{\varphi}{\theta\psi} , \\ N_{Q(\sqrt{a})/Q}(\theta) \, N_{Q(\sqrt{ab})/Q}(\psi) = N_{Q(\sqrt{b})/Q}(\varphi) . \end{cases}$$

Cette deuxième équation peut aussi s'écrire

$$N_{Q(\sqrt{ab})/Q}(\psi) \in N_1 N_2 .$$

Nous avons vu (théorème 3) que ψ est défini modulo Q^* . On définit donc une application F de G sur $(N_1 N_2 \cap N_3)/Q^{*2}$ en posant

$$F(\delta') = N_{Q(\sqrt{ab})/Q}(\psi) \, Q^{*2} \quad \text{si} \quad \delta' = \frac{\varphi}{\theta\psi} .$$

F est un homomorphisme multiplicatif.

Soit, d'autre part, $x \in N_1 N_2 \cap N_3$, n_x l'entier sans facteurs carrés (unique) tel que $n_x \in xQ^{*2}$.

Nous avons vu dans le § 3 que n_x ne possède pas de diviseur premier vérifiant $(a/p) = (b/p) = -1$. Écrivons

$$n_x = (-1)^{\gamma}\, c_2\, 2^{\lambda'} \prod_{i=1}^{r} p_i^{\mu_i'} \prod_{j=1}^{s} q_j^{\nu_j'} \prod_{K=1}^{t} u_K^{\rho_K'}$$

où γ , λ' , μ_i' , ν_j' , ρ_K' sont à valeurs 0 ou 1 , et où c_2 est un entier sans facteurs carrés tel que

$$p \mid c_2 \Rightarrow [(\tfrac{a}{p}) = 1 \quad \text{ou} \quad (\tfrac{b}{p}) = 1] .$$

Nous définirons une application ϕ de $(N_1 N_2 \cap N_3)/Q^{*2}$, dans $P=\{-1,+1\}^{2(r+s+t+2)}$ par

$$\phi(xQ^{*2}) = ((-1)^{\gamma},(-1)^{\lambda'},(-1)^{\frac{\varepsilon(c_2)}{2}},(-1)^{\frac{\omega(c_2)}{2}},(-1)^{\mu_1'},\dots,(-1)^{\rho_t'},(\frac{c_2}{p_1}),\dots,(\frac{c_2}{u_t}))$$

ϕ est un homomorphisme multiplicatif.

$\phi_0 F$ est donc un homomorphisme multiplicatif de G dans P .

Montrons que $\operatorname{Ker} \phi \circ F \subset G_1 G_2$ c'est-à-dire que (théorème 4)

$$\left.\begin{array}{ll} \gamma = \lambda' = \varepsilon(c_2) = \omega(c_2) = 0 & \\ (\forall\, i)\ (\forall\, j)\ (\forall\, K) & \mu_i' = \nu_j' = \rho_K' = 0 \\ (\forall\, i)\ (\forall\, j)\ (\forall\, K) & (\frac{c_2}{p_i}) = (\frac{c_2}{q_j}) = (\frac{c_2}{u_K}) = 1 \end{array}\right\} \Rightarrow N_{Q(\sqrt{ab})/Q}(\psi) \in N_1 .$$

On a alors, avec les notations précédentes, $n = c_2$. c_2 étant positif est représenté sur $\underset{\sim}{R}$ par $X^2 - aY^2$. Il reste à vérifier que :

$$(p \neq 2 \quad \text{et} \quad p \mid ac_2) \Rightarrow (a\, ,\, c_2)_p = 1 .$$

Si p divise c_2 , $(a\, ,\, c_2)_p = (a/p) = 1$ d'après (S"),

Si $p = p_i$, $(a\, ,\, c_2)_{p_i} = (c_2/p_i) = 1$,

Si $p = u_K$, $(a\, ,\, c_2)_{u_K} = (c_2/u_K) = 1$.

D'après des résultats de théorie des groupes

$$G/G_1 G_2 \simeq \frac{G/\operatorname{Ker} \phi \circ F}{G_1 G_2/\operatorname{Ker} \phi \circ F} \simeq (\phi \circ F)(G)/(\phi \circ F)(G_1 G_2)$$

Mais

$$F(G) = (N_1 N_2 \cap N_3)/Q^{*2} ,$$

$$F(G_1 G_2) = (N_1 \cap N_3)/Q^{*2} .$$

On a donc le résultat suivant.

THÉORÈME 15. - $G/G_1 G_2$ est isomorphe à $\phi((N_1 N_2 \cap N_3)/Q^{*2})/\phi((N_1 \cap N_3)/Q^{*2})$.

COROLLAIRE. - L'indice de $G_1 G_2$ dans G est une puissance de 2 .

Cela résulte de ce qu'il en est ainsi de card P .

On aura un ensemble de représentants de $G/G_1 G_2$ en prenant des images inverses par $\phi \circ F$ d'un ensemble de représentants de $(\phi \circ F)(G)/(\phi \circ F)(G_1 G_2)$.

Nous considérerons à cet effet (S') comme un système (Σ_1) par rapport aux inconnues <u>secondaires</u>

$(-1)^{\gamma}$, $(-1)^{\lambda'}$, $(-1)^{\varepsilon(c_2)}$, $(-1)^{\omega(c_2)}$, $(-1)^{\mu'_1}$,..., $(-1)^{\rho'_t}$, $(\frac{c_2}{p_1})$,..., $(\frac{c_2}{u_t})$

D'après le théorème 11, les éléments de $(\phi \circ F)(G)$ sont les éléments de P formés à partir d'inconnues secondaires vérifiant (Σ_1) .

Les éléments de $(\phi \circ F)(G_1\ G_2)$ sont ceux pour lesquels on a de plus $n \in N_1$, n ayant été déterminé à partir des valeurs obtenues.

$$n \in N_1 \Longleftrightarrow \begin{cases} a < 0 \Rightarrow n > 0 , \\ (p \neq 2 \quad \text{et} \quad p | an) \Rightarrow (a , n)_p = 1 . \end{cases}$$

Les éléments de $(\phi \circ F)(G_1\ G_2)$ sont ceux de $(\phi \circ F)(G)$ qui vérifient de plus le système (σ) suivant

$$\begin{cases} (\forall\ i) \quad (b , n)_{p_i} = 1 , \\ (\forall\ j) \quad (a , n)_{q_j} = 1 , \\ (\forall\ K) \quad (\frac{a'b'}{u_K}) = -1 = (a , n)_{u_K} = 1 . \end{cases}$$

(σ) peut encore s'écrire (avec les définitions données plus haut de t_1 et n_1)

$$\begin{cases} (\forall\ i) \quad (\frac{b}{p_i})^{\mu'_i} = 1 , \\ (\forall\ j) \quad (\frac{a}{q_j})^{\nu'_j} = 1 , \\ (\frac{c_2}{u_K}) = (\frac{2^{\lambda'}\ n_1}{u_K}) \quad \text{pour} \quad K = t_1 + 1 , \ldots , t . \end{cases}$$

On peut considérer (σ) comme un système (σ_1) relatif aux inconnues secondaires.

Les éléments de $(\phi \circ F)(G_1\ G_2)$ sont les éléments de P formés à partir d'inconnues secondaires vérifiant à la fois (Σ_1) et (σ_1) .

THÉORÈME 16. - <u>Les éléments de norme</u> 1 <u>de</u> K <u>sont obtenus à l'aide d'un nombre fini de formules</u> $\delta = \delta_i(\xi\eta/(\sigma(\xi)\ \tau(\eta)))$; $\xi , \eta \in K$ <u>et les</u> δ_i <u>étant des solutions particulières connues de</u> (1'). <u>De plus, chaque solution n'est obtenue ainsi qu'une seule fois.</u>

6. <u>Calcul de l'indice de</u> $G_1\ G_2$ <u>dans</u> G <u>en fonction du nombre de degrés locaux égaux à</u> 4 .

Il résulte de l'étude du paragraphe 5 que cet indice est 2^T , T étant le nombre des inconnues secondaires qui jouent le rôle d'indéterminées dans la résolution de (Σ_1) et qui sont déterminées par (σ_1) .

Nous avons vu (théorème 9) que G est égal à $G_1 G_2$ si tous les degrés locaux sont inférieurs ou égaux à 2.

Il nous reste à étudier le cas où l'un au moins des degrés locaux est égal à 4.

Réécrivons le système (S') pour $c = 1$:

$$\begin{cases} \gamma\alpha = \gamma\beta = 0 \\ (ab\ ,\ 2^{\lambda'}\ c_2)_2 = (ab\ ,\ n_1)_2 \\ (a\ ,\ b \notin Q_2^{*2} \text{ et } ab \in Q_2^{*2}) \Rightarrow (a\ ,\ 2^{\lambda'}\ c_2)_2 = (a\ ,\ n_1)_2 \\ (a\ ,\ 2^{\lambda'}\ c_2)_2 \prod_{i=1}^{r} (\frac{b}{p_i})^{\mu'_i} \prod_{j=1}^{s} (\frac{a}{q_j})^{\nu'_j} \prod_{K=t_1+1}^{t} (\frac{2^{\lambda'}\ c_2}{u_K}) = (a\ ,\ n_1)_2 \prod_{K=t_1+1}^{t} (\frac{n_1}{u_K}) \\ (\forall\ i)\quad (\frac{c_2}{p_i}) = (ab\ ,\ 2^{\lambda'}\ n_1)_{p_i} \\ (\forall\ j)\quad (\frac{c_2}{q_j}) = (ab\ ,\ 2^{\lambda'}\ n_1)_{q_j} \\ (\frac{c_2}{u_K}) = (a\ ,\ 2^{\lambda'}\ n_1)_{u_K} \quad \text{pour } K = 1\ ,\ \dots\ t_1\ . \end{cases}$$

Si $\pi_2 = 4$ (c'est-à-dire a, b, $ab \notin Q_2^{*2}$), on a vu dans le § 4 qu'on peut calculer deux des trois inconnues $(-1)^{\lambda'}$, $(-1)^{\varepsilon(c_2)}$, $(-1)^{\omega(c_2)}$ par les 2e et 4e équations, les autres étant indéterminées.

Les inconnues indéterminées pour (Σ_1) sont :

la 3e des inconnues ci-dessus,

$(-1)^{\gamma}$ (lorsque $\alpha = \beta = 0$),

$(-1)^{\mu'_i}$ pour $i = 1\ ,\ \dots\ ,\ r$,

$(-1)^{\nu'_j}$ pour $j = 1\ ,\ \dots\ ,\ s$,

$(-1)^{\rho'_K}$ pour $K = 1\ ,\ \dots\ ,\ t_1$,

(c_2/u_K) pour $K = t_1 + 1\ ,\ \dots\ ,\ t$.

D'autre part,

> (σ) détermine $(\frac{c_2}{u_K})$ pour $K = t_1 + 1\ ,\ \dots\ ,\ t$,
>
> (σ) détermine μ'_i si et seulement si $(\frac{b}{p_i}) = -1$ $\quad(\pi_{p_i} = 4)$,
>
> (σ) détermine ν'_j si et seulement si $(\frac{a}{q_j}) = -1$ $\quad(\pi_{q_j} = 4)$.

On voit donc que T est égal au nombre N' de degrés locaux π_p égaux à 4 pour $p \neq 2$.

Si $\pi_2 \leqslant 2$, on peut supposer par exemple $a \in Q_2^{*2}$.

La deuxième équation fournit l'une des inconnues $(-1)^{\lambda'}$, $(-1)^{\varepsilon(c_2)}$, $(-1)^{\omega(c_2)}$ les autres étant indéterminées.

Si $t_1 \neq t$ (c'est-à-dire s'il existe K tel que $\pi_{u_K} = 4$), la 4e équation fournit (c_2/u_K) .

Sont alors indéterminées pour (Σ_1) :

deux des trois inconnues ci-dessus,

$(-1)^{\gamma}$ (lorsque $\alpha = \beta = 0$) ,

$(-1)^{\mu'_i}$ pour $i = 1 , \ldots , r$,

$(-1)^{\nu'_j}$ pour $j = 1 , \ldots , s$,

$(-1)^{\rho'_K}$ pour $K = 1 , \ldots , t_1$,

(c_2/u_K) pour $K = t_1 + 1 , \ldots , t - 1$.

On a donc $T = N' - 1$.

Si $a \in Q_2^{*2}$ et $t_1 = t$, la 4e équation fournit

$$(-1)^{\mu'_{i_0}} \quad \text{si } \pi_{p_{i_0}} = 4$$
$$(-1)^{\nu'_{j_0}} \quad \text{si } \pi_{q_{j_0}} = 4$$

On trouve ici encore $T = N' - 1$.

On peut grouper ces résultats dans un seul énoncé.

THÉORÈME 17. - L'indice de $G_1 G_2$ dans G est égal à $2^{\pi - 1}$, π étant le nombre de degrés locaux égaux à 4 , si $\pi \neq 0$.

COROLLAIRE. - Pour que G soit égal à $G_1 G_2$, il faut et il suffit qu'il y ait au plus un degré local égal à 4 .

Cela résulte des théorèmes 9 et 17.

BIBLIOGRAPHIE

[1] CASSELS (J. W. S.) and FRÖHLICH (A.) [Editors]. - Algebraic number theory. Proceedings of an instructional conference organized by the London mathematical Society [1965. Brighton]. - London and New York, Academic Press, 1967.

(Texte définitif reçu le 3 mai 1973)

Christian PITTI
La Caravelle
Chemin de Cambaud
83140 SIX FOURS LA PLAGE