THEORIE DES NOMBRES
BESANCON

Années 1981-1982
et 1982-1983

INTRODUCTION AU K_2 DES CORPS DE NOMBRES

Jean-François JAULENT

INTRODUCTION AU K_2 DES CORPS DE NOMBRES

par

Jean-François JAULENT

SOMMAIRE

INTRODUCTION

Nous exposons ici quelques résultats classiques sur le K_2 des corps de nombres algébriques, ainsi que les principales propriétés des divers symboles donnés par le corps de classes d'une part, et la cohomologie galoisienne d'autre part. Nous ne parlons donc pas dans les pages qui suivent des liens importants entre le K_2 et les extensions centrales de groupes linéaires ni même des théorèmes obtenus récemment sur le K_2 des corps les plus généraux. En revanche nous nous sommes efforcés de donner des démonstrations aussi élémentaires que possible de la plupart des résultats présentés. Deux exceptions toutefois : D'abord, il n'était guère possible, dans un exposé qui se veut élémentaire, et centré exclusivement sur l'arithmétique des corps de nombres, de donner un aperçu substanciel de la démonstration du théorème de Garland sur la finitude du noyau modéré. Ensuite, il eût été prétentieux de vouloir améliorer l'étude magistrale de Tate sur les relations entre le K_2 et la cohomologie galoisienne. Nous avons donc préféré amdettre ces deux résultats, pour en développer rigoureusement quelques conséquences. En revanche, nous n'avons pas hésité, le cas échéant, à remettre en question la terminologie usuelle, lorsqu'elle nous a paru criticable. C'est ainsi, par exemple, que les symboles de Hilbert attachés aux places réelles sont généralement comptés parmi les symboles sauvages, alors qu'il est manifeste qu'ils sont, tout au contraire, modérés. Cette divergence de points de vue explique d'ailleurs pourquoi certaines formules obtenues ici diffèrent à l'occasion de celles données par d'autres auteurs. Cela est sans conséquence grave, nous semble-t-il, l'important restant naturellement de savoir de quels groupes on parle. Les démonstrations proposées relèvent dans leur totalité de la théorie classique du corps de classes, et même exclusivement de considérations algébriques, à l'exception de celle du théorème de Moore, empruntée à Chase et Waterhouse, qui fait appel à un argument de densité. Enfin, nous avons réservé à un exposé ultérieur l'étude des liens entre le K_2 et la théorie d'Iwasawa.

Comme tel, nous espérons que ce travail pourra se révéler utile à ceux qui souhaitent prendre connaissance en quelques pages des résultats essentiels sur l'arithmétique des symboles définis sur un corps de nombres. Nous invitons le lecteur intéressé par la genèse des problèmes évoqués ici à se reporter à l'exposé de Bass au séminaire Bourbaki, pour ne pas parler d'autres, plus récents.

1. - SYMBOLES SUR UN CORPS COMMUTATIF.

§ a. - Définition et propriétés élémentaires des symboles.

DEFINITION 1. - Un symbole sur un corps commutatif K, à valeurs dans un groupe abélien G, est une application $\langle\ ,\ \rangle$ de $K^\times \times K^\times$ dans G qui est bilinéaire et prend la valeur 1 sur tous les couples (a, b) qui vérifient $a+b=1$; ce qui peut se résumer par les trois conditions :

(i) $\langle aa', b\rangle = \langle a, b\rangle\langle a', b\rangle \quad , \quad \forall (a, a', b) \in K^\times \times K^\times \times K^\times$;

(ii) $\langle a, bb'\rangle = \langle a, b\rangle\langle a, b'\rangle \quad , \quad \forall (a, b, b') \in K^\times \times K^\times \times K^\times$;

(iii) $\langle a, 1-a\rangle = 1 \quad , \quad \forall a \in K^\times \backslash \{0, 1\}$.

PROPOSITION 2. - Etant donné un symbole $\langle\ ,\ \rangle$ sur un corps commutatif K, on a les trois propriétés :

(iv) $\langle a, -a\rangle = 1 \quad , \quad \forall a \in K^\times$;

(v) $\langle a, a\rangle = \langle a, -1\rangle, \quad \forall a \in K^\times$ (et donc $\langle a, a\rangle^2 = \langle a, 1\rangle = 1$) ;

(vi) $\langle a, b\rangle\langle b, a\rangle = 1, \quad \forall (a, b) \in K^\times \times K^\times$.

En particulier un symbole est une application bilinéaire antisymétrique.

Démonstration. - La propriété (iv) s'obtient en appliquant deux fois la condition (iii), et en utilisant la bilinéarité :

$$\langle a, -a\rangle = \frac{\langle a, -a\rangle}{\langle a, 1-a\rangle} = \langle a, \frac{-a}{1-a}\rangle = \langle a, \left(1-a^{-1}\right)^{-1}\rangle = \langle a^{-1}, 1-a^{-1}\rangle = 1.$$

La propriété (v) en résulte directement : $\langle a, a\rangle = \langle a, -1\rangle\langle a, -a\rangle = \langle a, -1\rangle$. Enfin, la propriété (vi) s'en déduit comme suit :

$$\langle a, b\rangle\langle b, a\rangle = \frac{\langle ab, b\rangle}{\langle b, b\rangle}\,\frac{\langle ab, a\rangle}{\langle a, a\rangle} = \frac{\langle ab, ab\rangle}{\langle b, -1\rangle\langle a, -1\rangle} = \frac{\langle ab, -1\rangle}{\langle ab, -1\rangle} = 1.$$

Remarque. - Soient $n \geq 1$ un entier naturel, et ζ_n une racine n-ième de l'unité dans K. Si n est impair, la condition (v) montre que la quantité $\langle \zeta_n, \zeta_n\rangle$ vaut 1, quel que soit le symbole considéré. Chercher en revanche s'il existe des symboles sur K pour lesquels $\langle -1, -1\rangle$ est distinct de 1, n'est pas toujours évident. Par exemple si K est le corps cyclotomique $\mathbb{Q}[\zeta_n]$ (n naturel impair), de tels symboles existent si et seulement si l'ordre de 2 modulo$^{\times}$ n est pair $\left(\text{cf. } [3], \text{th. } 5.1\right)$.

§ b. - Le groupe $K_2(K)$.

DEFINITION 3. - Par $K_2(K)$ nous entendons ici le quotient $K^{\times} \otimes_{\mathbb{Z}} K^{\times} / \prod_{a+b=1} (a \otimes b)^{\mathbb{Z}}$ du carré tensoriel du groupe multiplicatif de K par le sous-groupe engendré par les éléments de la forme $x \otimes (1-x)$ lorsque x décrit $K = \{0,1\}$. Le groupe $K_2(K)$ est caractérisé par la propriété universelle suivante :

PROPOSITION 4. (Propriété universelle) - Pour chaque symbole $\langle\ ,\ \rangle$ sur un corps commutatif K, à valeurs dans un groupe abélien G, il existe un *unique morphisme de groupe* φ *de* $K_2(K)$ *dans* G, *qui rend commutatif le diagramme :*

$$\begin{tikzcd} K^{\times} \times K^{\times} \arrow[r, "\langle\ ,\ \rangle"] \arrow[d, "\{\ ,\ \}"'] & G \\ K_2(K) \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

L'application canonique de $K^{\times} \times K^{\times}$ dans $K_2(K)$, qui au couple (x,y) associe la classe dans $K_2(K)$ du produit tensoriel $x \otimes y$, est un symbole sur K, appelé symbole universel sur le corps K, et noté $\{\ ,\ \}$.

Démonstration. - C'est clair.

§ c. - Les homomorphismes d'extension et de transfert.

Considérons une extension finie de corps L/K, et notons $d = [L : K]$ son degré. L'application canonique de $K^{\times} \otimes_{\mathbb{Z}} K^{\times}$ dans $L^{\times} \otimes_{\mathbb{Z}} L^{\times}$ induit par passage au quotient un morphisme naturel de $K_2(K)$ dans $K_2(L)$, appelé homomorphisme d'extension, et noté habituellement $i_{L/K}$.

Il est plus difficile malheureusement de définir directement le morphisme dual (le transfert) qui est aux symboles ce que la norme est aux idéaux. Disons simplement ici qu'il existe également un morphisme naturel de $K_2(L)$ dans $K_2(K)$, noté $Tr_{L/K}$, qui possède les propriétés suivantes :

(vii) $Tr_{L/K} \circ i_{L/K} = d = [L : K]$

(viii) Si l'extension L/K est galoisienne, on a :

$i_{L/K} \circ Tr_{L/K} = \sum_{\sigma \in Gal(L/K)} \sigma$ (pour l'action du groupe de Galois $Gal(L/K)$ sur le groupe $K_2(L)$ induite par celle sur $L^\times$, i.e. $\{a, b\}^\sigma = \{a^\sigma, b^\sigma\}$).

(ix) $\forall (a, B) \in K^\times \times L^\times, \quad Tr_{L/K}\left(\{a, B\}_L\right) = \{a, N_{L/K}(B)\}_K$.

Citons deux applications typiques du transfert :

1. Si $a \in K^\times$ est une puissance n-ième dans L, disons $a = A^n$, on a $\{a, N_{L/K}(B)\}_K = \left(Tr_{L/K}\{A, B\}_L\right)^n$, et $\{a, N_{L/K}(B)\}_K$ est une puissance n-ième dans $K_2(K)$, pour chaque B de $L^\times$.

2. Pour chaque premier p qui ne divise pas d, le p-Sylow $K_2(K)_p$ du groupe $K_2(K)$ s'identifie à son image canonique $i_{L/K}\left(K_2(K)_p\right)$ dans $K_2(L)$, et le transfert $T_{L/K}$ envoie $K_2(L)_p$ sur $K_2(K)_p$. En particulier, l'application $\frac{1}{d}\, i_{L/K} \circ Tr_{L/K}$ est un projecteur sur $K_2(L)_p$, qui a pour image le groupe $i_{L/K}\left(K_2(K)_p\right)$ isomorphe à $K_2(L)_p$.

Disons pour finir que les homomorphismes d'extension et de transfert ont les propriétés fonctorielles qu'on devine :

(x) $i_{M/K} = i_{M/L} \circ i_{L/K}$ & $Tr_{M/K} = Tr_{L/K} \circ Tr_{M/L}$, si $K \subset L \subset M$,

et qu'ils sont naturellement compatibles avec l'action des automorphismes de Galois (relatifs à une clôture algébrique donnée)

(xi) $\left(i_{L/K}(x_K)\right)^\sigma = L_{\sigma(L)/\sigma(K)}\left(x_K^\sigma\right)$ &

$\left(Tr_{L/K}(x_L)\right)^\sigma = Tr_{\sigma(L)/\sigma(K)}\left(x_L^\sigma\right)$.

Pour une définition directe du transfert à partir des propriétés (vii) à (ix), on pourra se reporter à [2].

2.- LES SYMBOLES CLASSIQUES SUR UN CORPS DE NOMBRES.

K désigne désormais un corps de nombres algébriques, c'est-à-dire une extension algébrique finie du corps des rationnels : Nous notons $\mathcal{O}$ l'anneau de ses entiers, et m l'ordre du sous-groupe μ des racines de l'unité dans $K^{\times}$.

§ a.- Les symboles modérés.

Quoique l'usage semble s'être établi jusqu'à aujourd'hui d'appeler symboles modérés les symboles définis à partir des valuations attachées aux seules places finies du corps considéré, nous adoptons ici un point de vue plus vaste et, sommes toutes, plus naturel, puisque les places à l'infini donnent lieu tout aussi bien à une description en termes de valuations (cf. [6]).

Considérons d'abord le cas d'une place finie $\mathfrak{p}$, et notons $\nu_{\mathfrak{p}}$ la valuation associée.

DEFINITION 5.- Pour chaque place finie $\mathfrak{p}$ du corps de nombres K, l'application de $K^{\times} \times K^{\times}$, à valeurs dans le groupe multiplicatif $k_{\mathfrak{p}}^{\times}$ du corps résiduel $k_{\mathfrak{p}} = \mathcal{O}/\mathfrak{p}$, qui à un couple (a, b) d'éléments de $K^{\times}$ associe la classe dans $k_{\mathfrak{p}}^{\times}$ du produit

$$(-1)^{\nu_{\mathfrak{p}}(a)\,\nu_{\mathfrak{p}}(b)}\ \frac{a^{\nu_{\mathfrak{p}}(b)}}{b^{\nu_{\mathfrak{p}}(a)}},$$

est un symbole sur K, appelé symbole modéré associé à la place $\mathfrak{p}$, et noté $(\ ,\ )_{\mathfrak{p}}$.

Démonstration.- La bilinéarité est évidente, ainsi que la propriété (iv). Pour vérifier (iii), nous pouvons donc nous restreindre au cas où a est $\mathfrak{p}$-entier ; il en est alors de même de $(1-a)$. Si a et $(1-a)$ sont tous deux des $\mathfrak{p}$-unités, nous avons trivialement $(a, 1-a)_{\mathfrak{p}} = 1$. Sinon l'un d'eux, par exemple a, est une unité principale ; et il vient encore

$$\left(-1\right)^{\nu_p(a)\,\nu_p(b)}\ \frac{a^{\nu_p(b)}}{b^{\nu_p(a)}} = a^{\nu_p(b)} \equiv 1 \pmod{p}, \text{ comme attendu.}$$

Supposons maintenant que p soit une place à l'infini. Notons K_p le complété de K en p (qui s'identifie à $\mathbb{R}$ ou à $\mathbb{C}$, suivant que p est réelle ou complexe), puis $k_p^\times$ le groupe résiduel $K_p^\times/K_p^{\times 2}$. L'application ν_p de $K^\times$ dans $\{0,1\}$ définie par :

$$\nu_p(x) = 0, \text{ si } x \text{ est un carré dans } K_p^\times,$$

$$\nu_p(x) = 1, \text{ sinon,}$$

est alors une valuation sur K.

<u>DEFINITION 6</u>. - Pour chaque place à l'infini p du corps de nombres K, l'application de $K^\times \times K^\times$ dans le groupe résiduel $k_p^\times = K_p^\times/K_p^{\times 2}$, qui à un couple (a,b) d'éléments de $K^\times$ associe la classe dans $k_p^\times$ du produit

$$\left(-1\right)^{\nu_p(a)\,\nu_p(b)}\ \frac{a^{\nu_p(b)}}{b^{\nu_p(a)}},$$

est un symbole sur K, appelé <u>symbole modéré</u> associé à la place p, et noté $(\ ,\ )_p$.

Le symbole $(\ ,\ )_p$ est trivial lorsque p est complexe ; et si p est une place réelle, la quantité $(a,b)_p$ n'est pas 1 si et seulement si les images de a et de b dans le complété K_p sont toutes deux négatives.

Démonstration. - La bilinéarité étant immédiate, seule reste à vérifier la condition (iii), lorsque p est réelle. Cela étant, si a est positif dans K_p, le produit $\left(-1\right)^{\nu_p(a)\,\nu_p(b)}\ \frac{a^{\nu_p(b)}}{b^{\nu_p(a)}}$, égal à $a^{\nu_p(b)}$, l'est aussi ; de même si b est positif ; et, dans les deux cas, le symbole $(a,b)_p$ vaut 1. Au contraire si a et b sont tous deux négatifs, il en est de même du produit $\left(-1\right)^{\nu_p(a)\,\nu_p(b)}\ \frac{a^{\nu_p(b)}}{b^{\nu_p(a)}}$; mais ce cas est exclu si $(a+b)$ vaut 1.

§ b. - Les symboles de Hilbert.

Pour chaque place non complexe $\mathfrak{p}$ de K, désignons par $K_{\mathfrak{p}}$ le complété de K en $\mathfrak{p}$; notons $m_{\mathfrak{p}}$ l'ordre du sous-groupe $\mu_{\mathfrak{p}}$ des racines de l'unité dans $K_{\mathfrak{p}}^{\times}$; et considérons l'application d'Artin $\omega_{\mathfrak{p}}$ relative à une clôture abélienne $\overline{K}_{\mathfrak{p}}^{ab}$ de $K_{\mathfrak{p}}$.

DEFINITION 7. - Pour chaque place non complexe $\mathfrak{p}$ de K, l'identité $\left(\frac{a,b}{\mathfrak{p}}\right) = \sqrt[m_{\mathfrak{p}}]{a}^{\,\left(\omega_{\mathfrak{p}}(b)-1\right)}$, $\forall (a,b) \in K_{\mathfrak{p}}^{\times} \times K_{\mathfrak{p}}^{\times}$ définit un symbole sur $K_{\mathfrak{p}}$, à valeurs dans le groupe $\mu_{\mathfrak{p}}$ des racines de l'unité contenues dans $K_{\mathfrak{p}}^{\times}$. Sa restriction à $K^{\times} \times K^{\times}$ est un symbole sur K, appelé symbole de Hilbert attaché à la place $\mathfrak{p}$, et noté $\left(\frac{\;,\;}{\mathfrak{p}}\right)$.

Démonstration. - Il s'agit de montrer la bilinéarité, ainsi que l'identité $\left(\frac{a,b}{\mathfrak{p}}\right) = 1$ pour $a+b=1$.

(i) La multiplicativité en a est évidente (tout comme le fait que la définition du symbole est indépendante du choix de la racine $m_{\mathfrak{p}}$-ième de a dans $\overline{K}_{\mathfrak{p}}^{ab}$).

(ii) Pour établir la multiplicativité en b, remarquons que si b et b' sont dans $K_{\mathfrak{p}}^{\times}$, nous avons la relation : $\sqrt[m_{\mathfrak{p}}]{a}^{\,\left(\omega_{\mathfrak{p}}(b)-1\right)\left(\omega_{\mathfrak{p}}(b')-1\right)} = 1$, puisque le groupe Gal $\left(\overline{K}_{\mathfrak{p}}^{ab}/K_{\mathfrak{p}}\right)$ opère trivialement sur $\mu_{\mathfrak{p}}$; puis, en développant :

$$\sqrt[m_{\mathfrak{p}}]{a}^{\,\left(\omega_{\mathfrak{p}}(b)-1\right)+\left(\omega_{\mathfrak{p}}(b')-1\right)} = \sqrt[m_{\mathfrak{p}}]{a}^{\,\left(\omega_{\mathfrak{p}}(bb')-1\right)},$$ comme attendu.

(iii) Enfin, pour tout a dans $K_{\mathfrak{p}}$, autre que 0 ou 1, l'élément $(1-a) = \prod_{\zeta \in \mu_{\mathfrak{p}}} \left(1-\zeta \sqrt[m_{\mathfrak{p}}]{a}\right)$ est norme dans l'extension cyclique $K_{\mathfrak{p}}[\sqrt[m_{\mathfrak{p}}]{a}]/K_{\mathfrak{p}}$, donc contenu dans le noyau de la restriction à $K_{\mathfrak{p}}[\sqrt[m_{\mathfrak{p}}]{a}]$ de l'application d'Artin.

On notera que, quand la place $\mathfrak{p}$ est complexe, le complété $K_{\mathfrak{p}}$ est clos, et le corps de classes local ne permet de définir d'autre symbole en $\mathfrak{p}$ que le symbole trivial.

PROPOSITION 8. - L'égalité $\left(\frac{a\,,b}{\mathfrak{p}}\right) = 1$ a lieu si et seulement si b est norme locale en $\mathfrak{p}$ dans l'extension globale $K[\sqrt[m_\mathfrak{p}]{a}]/K$ (ou encore, en vertu de l'antisymétrie, si et seulement si a est norme locale en $\mathfrak{p}$ dans l'extension $K[\sqrt[m_\mathfrak{p}]{b}]/K$).

Démonstration. - Cela résulte directement des propriétés normiques de l'application d'Artin.

THEOREME 9. - Les symboles de Hilbert vérifient la formule du produit :

$$\prod_{\mathfrak{p}} \left(\frac{\,,\,}{\mathfrak{p}}\right)^{m_\mathfrak{p}/m} = 1.$$

Démonstration. - Deux éléments a et b de $K^\times$ étant donnés, l'extension abélienne $K[\sqrt[m]{a}]/K$ est non ramifiée en dehors d'un nombre fini de places (en particulier, pour chaque place finie $\mathfrak{p}$ étrangère à m et à a). Comme b est norme locale en toute place non ramifiée qui ne le divise pas, les symboles $\left(\frac{a\,,b}{\mathfrak{p}}\right)^{m_\mathfrak{p}/m}$ sont presque tous égaux à 1, et la formule du produit a bien un sens. Plus précisément, nous obtenons :

$$\prod_{\mathfrak{p}} \left(\frac{a\,,b}{\mathfrak{p}}\right)^{m_\mathfrak{p}/m} = \sqrt[m]{a}^{\,\sum_{\mathfrak{p}}\left(\omega_\mathfrak{p}(b)-1\right)} = \sqrt[m]{a}^{\,\left(\prod_{\mathfrak{p}}\omega_\mathfrak{p}(b)-1\right)} = \sqrt[m]{a}^{\,\left(\omega(b)-1\right)} = 1,$$

puisque l'application d'Artin globale ω (définie sur le groupe des idèles de K) est triviale sur l'image diagonale de $K^\times$.

§ c. - Comparaison des symboles modérés et des symboles de Hilbert.

Considérons d'abord une place finie $\mathfrak{p}$ de K au-dessus d'un premier donné p. Ecrivons $m_\mathfrak{p} = (N\mathfrak{p}-1)p^{r_\mathfrak{p}} = (p^{f_\mathfrak{p}}-1)p^{r_\mathfrak{p}}$ la factorisation canonique de $m_\mathfrak{p}$, puis $\mu_\mathfrak{p} = \mu_\mathfrak{p}^o \oplus \mu_\mathfrak{p}^1$ celle du groupe des racines de l'unité $\mu_\mathfrak{p}$ comme produit direct du sous-groupe $\mu_\mathfrak{p}^o$, formé des racines d'ordre étranger à $\mathfrak{p}$, et du $\mathfrak{p}$-sous-groupe de Sylow $\mu_\mathfrak{p}^1$. Il est bien connu que $\mu_\mathfrak{p}^1$ est formé des racines principales de l'unité $\left(\mu_\mathfrak{p}^1 = \mu_\mathfrak{p} \cap U_\mathfrak{p}^1\right)$, et que $\mu_\mathfrak{p}^o$ s'identifie, par passage au quotient, au groupe multiplicatif $k_{\mathfrak{p}}^{\times}$ du corps résiduel $k_{\mathfrak{p}} = \mathcal{O}/\mathfrak{p}$ (de sorte que l'ordre de $\mu_{\mathfrak{p}}^{o}$ est bien égal à $(N\mathfrak{p}-1)$).

Lorsque le groupe $\mu_{\mathfrak{p}}$ se réduit à son sous-groupe $\mu_{\mathfrak{p}}^{o}$, nous disons, suivant la terminologie des corps locaux, que la place $\mathfrak{p}$ est régulière ; nous disons qu'elle est irrégulière sinon, ce qui a lieu chaque fois que le complété $K_{\mathfrak{p}}$ contient une racine primitive p-ième de l'unité ζ_p. La condition sur les degrés qui en résulte $[K:\mathbb{Q}] \geq [K_{\mathfrak{p}} : \mathbb{Q}_p] \geq [\mathbb{Q}_p[\zeta_p]:\mathbb{Q}_p] = (p-1)$ montre ainsi que les places irrégulières sont en nombre fini.

Dans le cas d'une place réelle, enfin, la situation est plus simple : Le groupe $\mu_{\mathfrak{p}}$ se réduit à son sous-groupe $\mu_{\mathfrak{p}}^{o} = \{\pm 1\}$, et s'identifie par conséquent au groupe résiduel $k_{\mathfrak{p}}^{\times}$. En particulier, les places réelles sont toujours régulières.

Revenons maintenant sur le symbole modéré $(\ ,\ )_{\mathfrak{p}}$. Identifiant le groupe résiduel $k_{\mathfrak{p}}^{\times}$ avec son relèvement canonique $\mu_{\mathfrak{p}}^{o}$ dans $\mu_{\mathfrak{p}}$, nous fabriquons ainsi un symbole sur K, à valeurs dans le sous-groupe $\mu_{\mathfrak{p}}^{o}$ de $\mu_{\mathfrak{p}}$, que nous continuons, par abus, à noter $(\ ,\ )_{\mathfrak{p}}$:

<u>DEFINITION 10</u>. - Nous appelons <u>symbole régulier</u> associé à une place non complexe $\mathfrak{p}$ du corps K le relèvement canonique, noté encore $(\ ,\ )_{\mathfrak{p}}$, du symbole modéré dans le sous-groupe régulier $\mu_{\mathfrak{p}}^{o}$ du groupe $\mu_{\mathfrak{p}}$ des racines de l'unité dans le complété $K_{\mathfrak{p}}$.

<u>THEOREME 11</u>. - Pour chaque place finie $\mathfrak{p}$ de K, le symbole régulier $(\ ,\ )_{\mathfrak{p}}$ est la puissance $p^{r_{\mathfrak{p}}}$-ième du symbole de Hilbert $\left(\frac{\ ,\ }{\mathfrak{p}}\right)$; ce qui s'écrit :

$$(a,b)_{\mathfrak{p}} = \left(\frac{a\,,b}{\mathfrak{p}}\right)^{p^{r_{\mathfrak{p}}}}, \qquad \forall (a,b) \in K^{\times} \times K^{\times}.$$

En particulier, le symbole de Hilbert coïncide avec le symbole régulier en chaque place régulière $\mathfrak{p}$ de K.

Démonstration. - Par un argument de bilinéarité, nous pouvons nous restreindre au cas où a et b sont tous deux des uniformisantes locales. Ecrivons donc $b = \pi$ et $a = -u\pi$; nous obtenons $\left(\frac{a\,,\,b}{\mathfrak{p}}\right) = \left(\frac{-u\pi\,,\,\pi}{\mathfrak{p}}\right) = \left(\frac{u\,,\,\pi}{\mathfrak{p}}\right)$, d'après la condition (iv). Ecrivons maintenant $m_{\mathfrak{p}}^{o} = N\mathfrak{p} - 1$; l'extension abélienne $K_{\mathfrak{p}}[\sqrt[m_{\mathfrak{p}}^{o}]{u}]/K_{\mathfrak{p}}$ étant non ramifiée, l'application d'Artin qui lui correspond est donnée par le Frobenius. Il vient donc :

$$\left(\frac{a\,,\,b}{\mathfrak{p}}\right)^{p^{r_{\mathfrak{p}}}} = \left(\frac{u\,,\,\pi}{\mathfrak{p}}\right)^{p^{r_{\mathfrak{p}}}} = \sqrt[m_{\mathfrak{p}}^{o}]{u}^{\left(\omega_{\mathfrak{p}}(\pi)-1\right)} \equiv \sqrt[m_{\mathfrak{p}}^{o}]{u}^{(N\mathfrak{p}-1)} \equiv u \equiv (u\,,\pi)_{\mathfrak{p}} \equiv (a\,,b)_{\mathfrak{p}} (\mathrm{mod}\ \mathfrak{p})$$

comme annoncé.

3.- ETUDE DU K_2 A PARTIR DES SYMBOLES LOCAUX.

§ a.- La suite exacte de Moore.

D'après la propriété universelle de $K_2(K)$, pour chaque place non complexe $\mathfrak{p}$ de K, le symbole de Hilbert $\left(\frac{\ ,\ }{\mathfrak{p}}\right)$ se factorise par un unique morphisme $h_{\mathfrak{p}}$ de $K_2(K)$ dans le groupe $\mu_{\mathfrak{p}}$. La famille des $h_{\mathfrak{p}}$, lorsque $\mathfrak{p}$ décrit les places non complexes de K définit un morphisme h du groupe $K_2(K)$ dans le produit direct $\prod_{\mathfrak{p}\text{ non complexe}} \mu_{\mathfrak{p}}$ des groupes de racines de l'unité locaux. En fait, la formule du produit pour le symbole de Hilbert montre que h prend ses valeurs dans la somme directe $\bigoplus_{\mathfrak{p}\text{ non complexe}} \mu_{\mathfrak{p}}$ des groupes $\mu_{\mathfrak{p}}$ et, plus précisément, dans le sous-groupe $\widetilde{\bigoplus_{\mathfrak{p}}} \mu_{\mathfrak{p}}$ de cette somme, formé des familles $\left(\zeta_{\mathfrak{p}}\right)_{\mathfrak{p}}$ qui vérifient la relation $\prod_{\mathfrak{p}} \zeta_{\mathfrak{p}}^{m_{\mathfrak{p}}/m} = 1$. Le fait que $h\left(K_2(K)\right)$ soit effectivement égal à $\widetilde{\bigoplus_{\mathfrak{p}}} \mu_{\mathfrak{p}}$ constitue le théorème de Moore.

D'un autre côté, on peut montrer par des considérations élémentaires que le noyau $H_2(K) = \mathrm{Ker}\ h$ est un groupe de type fini. L'argument, dû à Tate et Bass, généralise en quelque sorte la première démonstration par

Gauss de la loi de réciprocité quadratique. Mais le fait que $H_2(K)$ soit fini reste un résultat difficile, dû à Garland, qui relève de l'analyse harmonique sur des espaces symétriques (cf. [1], [2], et [10]).

Enonçons ces deux résultats :

THEOREME 12.- Les symboles de Hilbert induisent un morphisme h du groupe $K_2(K)$ dans la somme directe des groupes de racines de l'unité des complétés de K associés aux places non complexes de ce corps. Le noyau $H_2(K)$ de ce morphisme est un groupe fini, et son conoyau s'identifie, via la formule du produit, au groupe μ des racines de l'unité contenues dans K ; ce qui se traduit par l'exactitude de la suite :

$$1 \longrightarrow H_2(K) \longrightarrow K_2(K) \xrightarrow{h} \bigoplus_{\mathfrak{p} \text{ non complexe}} \mu_{\mathfrak{p}} \longrightarrow \mu \longrightarrow 1.$$

Démonstration du théorème de Moore (cf. [5]).- Il s'agit évidemment d'établir la réciproque de la formule du produit, ce qui peut se faire localement, pour chaque nombre premier ℓ, en montrant que l'image de h contient le ℓ-Sylow de $\widetilde{\bigoplus_{\mathfrak{p}}} \mu_{\mathfrak{p}}$. Fixons donc un nombre premier ℓ, notons S l'ensemble fini constitué des places divisant $\ell\infty$ et des places irrégulières, puis considérons une famille $\zeta = (\zeta_{\mathfrak{p}})_{\mathfrak{p}}$ de racines locales de l'unité d'ordre ℓ-primaire, égales presque toutes à 1, et vérifiant la formule du produit $\prod_{\mathfrak{p}} \zeta_{\mathfrak{p}}^{m_{\mathfrak{p}}/m} = 1$. Nous savons que pour chaque place non complexe $\mathfrak{p}$ de K, la racine $\zeta_{\mathfrak{p}}$ est l'image par le symbole de Hilbert $\left(\frac{a_{\mathfrak{p}}, b_{\mathfrak{p}}}{\mathfrak{p}}\right)$ d'un couple $(a_{\mathfrak{p}}, b_{\mathfrak{p}})$ d'éléments de $K_{\mathfrak{p}}^{\times}$. Le théorème d'approximation simultanée nous permet donc d'écrire $\zeta_{\mathfrak{p}} = \left(\frac{a, b}{\mathfrak{p}}\right)$, avec a et b dans $K^{\times}$, pour chaque $\mathfrak{p}$ de S. Ainsi, comme il est toujours possible d'imposer à $h(\{a, b\})$ d'être d'ordre ℓ-primaire (par exemple en remplaçant a par une puissance convenable a^n), quitte à raisonner sur $\zeta/h(\{a, b\})$ plutôt que sur ζ, nous pouvons désormais supposer que $\zeta_{\mathfrak{p}}$ vaut 1, pour chaque $\mathfrak{p}$ de S.

Cela étant, notons d la ℓ-valuation de l'ordre m de μ et considérons l'extension cyclique ℓ-ramifiée $K[\eta]/K$, engendrée sur K par une racine ℓ^{d+1}-ième primitive de l'unité η. L'idéal $\mathfrak{a} = \prod_{\zeta_{\mathfrak{p}} \neq 1} \mathfrak{p}$ étant non ramifié dans cette extension, le théorème de Čebotarev nous assure l'existence d'une infinité de premiers $\mathfrak{q}$ pour lesquels le symbole d'Artin $(\mathfrak{a}\mathfrak{q}, K[\eta]/K)$ engendre Gal $(K[\eta]/K)$. Choisissons l'un d'eux $\mathfrak{q}$, qui n'appartiennent pas à $\mathcal{S}$. Pour chaque place $\mathfrak{p}$ divisant $\mathfrak{a}$, l'expression du symbole régulier nous permet d'écrire $\zeta_{\mathfrak{p}} = \left(\frac{a_{\mathfrak{p}}, b_{\mathfrak{p}}}{\mathfrak{p}}\right)$ en imposant à $a_{\mathfrak{p}}$ d'être une unité et à $b_{\mathfrak{p}}$ d'être une uniformisante. Invoquant à nouveau le théorème d'approximation simultanée, choisissons a dans $K^{\times}$, vérifiant les congruences :

$$a \equiv 1 \left(\operatorname{mod}^{\times} \mathfrak{q}\right) \qquad \text{et} \qquad a \equiv a_{\mathfrak{p}} \left(\operatorname{mod}^{\times} \mathfrak{p}\right) \quad \forall \mathfrak{p} \mid \mathfrak{a}.$$

Nous obtenons alors $\left(\frac{a, b_{\mathfrak{p}}}{\mathfrak{p}}\right) \equiv a \ (\operatorname{mod} \mathfrak{p})$, pour tout $\mathfrak{p}$ divisant $\mathfrak{a}\mathfrak{q}$, i. e. $\left(\frac{a, b_{\mathfrak{p}}}{\mathfrak{p}}\right) = \left(\frac{a_{\mathfrak{p}}, b_{\mathfrak{p}}}{\mathfrak{p}}\right) = \zeta_{\mathfrak{p}}$.

Désignons maintenant par $\mathcal{S}(a)$ la réunion de $\mathcal{S}$ et de l'ensemble des places divisant a, fixons n assez grand, formons le diviseur $\mathfrak{M} = \prod_{\mathfrak{p} \in \mathcal{S}(a)} \mathfrak{p}^n$, et considérons le groupe de congruences $J_{\mathfrak{M}}/P_{\mathfrak{M}}$. D'après le théorème de Čebotarev, la classe de l'idéal $\mathfrak{a}\mathfrak{q}$ peut être représentée par un idéal premier $\mathfrak{r}$ étranger à $\mathfrak{a}\mathfrak{q}$ (et évidemment à a). Autrement dit nous pouvons écrire $\mathfrak{a}\mathfrak{q}/\mathfrak{r} = (b)$, avec $b \equiv 1 \left(\operatorname{mod}^{\times} \mathfrak{M}\right)$ et $\mathfrak{r}$ premier étranger à $\mathfrak{a}\mathfrak{q}$. Examinons les symboles $\left(\frac{a, b}{\mathfrak{p}}\right)$.

- Pour $\mathfrak{p} \mid \mathfrak{a}\mathfrak{q}$, nous avons $\left(\frac{a, b}{\mathfrak{p}}\right) \equiv a \equiv \left(\frac{a_{\mathfrak{p}}, b_{\mathfrak{p}}}{\mathfrak{p}}\right) (\operatorname{mod} \mathfrak{p})$ i. e. $\left(\frac{a, b}{\mathfrak{p}}\right) = \zeta_{\mathfrak{p}}$.

- Pour $\mathfrak{p} \in \mathcal{S}(a)$, nous avons $\left(\frac{a, b}{\mathfrak{p}}\right) = 1$, car b (qui est congru à 1 modulo $\mathfrak{M}$) est norme locale en $\mathfrak{p}$.

- Pour tous les autres $\mathfrak{p}$, sauf $\mathfrak{r}$ peut-être, $\left(\frac{a, b}{\mathfrak{p}}\right)$ vaut 1, car a et b sont des $\mathfrak{p}$-unités. Mais comme le symbole d'Artin $((b), K[\eta]/K)$ est trivial (puisque b est proche de 1 pour les places au-dessus de ℓ), l'identité $(\mathfrak{r}, K[\eta]/K) = (\mathfrak{a}\mathfrak{q}, K[\eta]/K)$ montre que $\mathfrak{r}$ ne se décompose pas dans l'extension $K[\eta]/K$, i. e. que $\mu_{\mathfrak{r}}$ ne contient pas η. La formule du produit entraîne donc $\left(\frac{a, b}{\mathfrak{r}}\right) = 1$; ce qui achève la démonstration.

Remarques. - 1. La suite exacte de Moore résume les informations sur le K_2 données par le corps de classes. Le noyau hilbertien $H_2(K)$ mesure ainsi le nombre de symboles exotiques définis sur le corps K.

2. De façon générale, le groupe $H_2(K)$ est très mal connu. On sait que $H_2(\mathbb{Q})$ est nul (cf. [9]) et qu'il en est de même pour quelques corps quadratiques imaginaires (cf. [2]). En revanche on connait des résultats plus précis pour la p-partie de $H_2(K)$ pour certains corps (cf. [6]).

§ b. - Noyau modéré et noyau hilbertien.

Considérons maintenant les symboles modérés $(\ ,\ )_{\mathfrak{p}}$. Pour chaque place non complexe $\mathfrak{p}$ du corps K, il existe, tout comme pour les symboles de Hilbert, un unique morphisme $m_{\mathfrak{p}}$ de $K_2(K)$ dans le groupe résiduel $K_{\mathfrak{p}}^{\times}$, qui factorise le symbole $(\ ,\ )_{\mathfrak{p}}$. La donnée de l'ensemble des $m_{\mathfrak{p}}$ définit ainsi un morphisme m du groupe $K_2(K)$ dans la somme directe $\bigoplus_{\mathfrak{p}} k_{\mathfrak{p}}^{\times}$ des groupes résiduels $k_{\mathfrak{p}}^{\times}$. Nous allons voir que ce dernier morphisme est surjectif.

PROPOSITION 13. - Les symboles modérés induisent un morphisme surjectif du groupe $K_2(K)$ sur la somme directe $\oplus\, k_{\mathfrak{p}}^{\times}$ des groupes résiduels associés aux places non complexes de K ; ce qui se traduit par l'exactitude de la suite :

$$1 \longrightarrow R_2(K) \longrightarrow K_2(K) \xrightarrow{m} \bigoplus_{\mathfrak{p}\text{ non complexe}} k_{\mathfrak{p}}^{\times} \longrightarrow 1.$$

Le noyau $R_2(K)$ de ce morphisme est un sur-groupe fini de $H_2(K)$, appelé noyau modéré.

Démonstration. - La proposition est une conséquence facile du théorème précédent : D'une part, les symboles modérés se factorisent par les symboles de Hilbert (d'après le théorème 10) et le noyau hilbertien $H_2(K)$ est donc contenu dans le noyau modéré $R_2(K)$. Comme, d'autre part, le symbole $\left(\frac{\ ,\ }{\mathfrak{p}}\right)$ est régulier pour presque tout $\mathfrak{p}$, l'indice $\left(R_2(K) : H_2(K)\right)$ est bien fini, et tout le problème revient à vérifier que m est surjectif. Pour ce faire, écrivons

$m = \prod_p p^{n_p}$ l'ordre de μ, et désignons par $\mathcal{S}$ l'ensemble (contenant les diviseurs de m) des places irrégulières. La formule du produit envoie $\bigoplus_{p \in \mathcal{S}} \mu_p^1$ sur μ, et la proposition résulte donc du diagramme commutatif exact :

$$\begin{tikzcd}
1 \arrow[r] & H_2(K) \arrow[r] \arrow[d, hook] & K_2(K) \arrow[r, "h"] \arrow[d, equal] & \left(\bigoplus_p \mu_p^{o}\right) \oplus \arrow[d, "\wr\ \times p^{r_p}"] & \left(\bigoplus_{p \in \mathcal{S}} \mu_p^1\right) \arrow[r] \arrow[d, two heads, "\times m_p/m"] & \mu \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & R_2(K) \arrow[r] & K_2(K) \arrow[r, "m"] & \left(\bigoplus_p k_p^\times\right) \oplus & \mu \arrow[r, "="] & \mu \arrow[r] & 1
\end{tikzcd}$$

<u>COROLLAIRE 14</u>. - Les symboles de Hilbert et la formule du produit conduisent à la suite exacte courte canonique, où tous les termes sont finis :

$$1 \longrightarrow R_2(K)/H_2(K) \longrightarrow \bigoplus_{p \text{ irrégulier}} \mu_p^1 \longrightarrow \mu \longrightarrow 1.$$

En particulier, l'indice du noyau hilbertien dans le noyau modéré est donné par la formule :

$$\left(R_2(K) : H_2(K)\right) = \frac{1}{|\mu|} \prod_{p \text{ irrégulier}} |\mu_p^1| = \frac{1}{m} \prod_{p \mid m_p} p^{r_p}.$$

4. - DESCRIPTION COHOMOLOGIQUE DU K_2

Nous exposons dans cette section les importants résultats de Tate qui ramènent l'étude du K_2 d'un corps de nombres à des questions de cohomologie galoisienne. L'existence de [12] nous a dispensé de donner la plupart des démonstrations.

§ a. - *Définition du symbole cohomologique.*

Désignons par $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$, puis, pour chaque naturel n, notons μ_n le groupe des racines n-ièmes de l'unité dans $\overline{\mathbb{Q}}$. L'action du groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ sur chacun des termes de la suite exacte courte

$$1 \longrightarrow \mu_n \longrightarrow \overline{\mathbb{Q}}^{\times} \xrightarrow{\times n} \overline{\mathbb{Q}}^{\times} \longrightarrow 1$$

donne naissance à la suite exacte de cohomologie :

$$1 \longrightarrow \mu_n \cap K^{\times} \longrightarrow K^{\times} \xrightarrow{\times n} K^{\times} \longrightarrow H^1(K, \mu_n) \longrightarrow \ldots$$

Notant δ_n l'application de $K^{\times}$ dans $H^1(K, \mu_n)$ ainsi obtenue, et formant le cup-produit $\delta_n . \delta_n$, nous définissons une application bilinéaire antisymétrique $(\ ,\ )_n$ de $K^{\times} \times K^{\times}$ dans $H^2(K, \mu_n \otimes \mu_n)$. Nous allons voir que cette application est un symbole.

<u>DEFINITION 15</u>. - Pour chaque naturel $n \geq 1$, l'application $(\ ,\ )_n$ définie par l'identité

$$(a, b)_n = \delta_n a . \delta_n b \qquad \forall (a, b) \in K^{\times} \times K^{\times},$$

est un symbole sur K à valeurs dans $H^2(K, \mu_n \otimes \mu_n)$, appelé <u>symbole cohomologique de niveau n</u>.

Démonstration. - Il s'agit évidemment de vérifier l'identité $(a, 1-a)_n = 1$, pour tout $a \in K \setminus \{0, 1\}$. Or c'est là une conséquence facile de l'existence du transfert cohomologique : L'élément a étant donné, écrivons $X^n - a = \prod_i P_i(X)$ la décomposition irréductible dans $K[X]$ du polynôme $(X^n - a)$; pour chaque indice i, notons a_i une racine de P_i dans $\overline{\mathbb{Q}}$, et posons $K_i = K[a_i]$. Nous obtenons $(1-a) = \prod_i P_i(1) = \prod_i N_{K_i/K}(1-a_i)$; d'où :

$$(a, 1-a)_n^K = \prod_i \left(a, N_{K_i/K}(1-a_i)\right)_n^K = \prod_i \mathrm{Tr}_{K_i/K}(a, 1-a_i)_n^{K_i} =$$

$$= \prod_i \mathrm{Tr}_{K_i/K}(a_i^n, 1-a_i)_n^{K_i} = \left(\prod_i \mathrm{Tr}_{K_i/K}(a_i, 1-a_i)_n^{K_i}\right)^n = 1,$$

comme attendu, le groupe $H^2(K, \mu_n \otimes \mu_n)$ étant annulé par n.

On a, en fait, le résultat plus fort :

PROPOSITION 16. - L'identité $(a,b)_n = 1$ a lieu si et seulement si b est norme dans l'extension K_a/K, où K_a désigne l'algèbre $K[X]/(X^n - a)$ (ou encore si et seulement si a est norme dans l'extension K_b/K).

THEOREME 17. - Le morphisme t_n du groupe $K_2(K)$ dans $H^2(K, \mu_n \otimes \mu_n)$, qui factorise le symbole cohomologique $(\ ,\ )_n$, est surjectif, et son noyau est $K_2(K)^n$. Autrement dit, t_n induit un isomorphisme :

$$K_2(K)/K_2(K)^n \simeq H^2(K, \mu_n \otimes \mu_n).$$

Tate a montré que l'application naturelle $H^2(K, \mu_n \otimes \mu_n) \longrightarrow \bigoplus_{p \text{ non complexe}} H^2(K_p, \mu_n \otimes \mu_n)$ est injective si n n'est pas divisible par 8 et, dans ce dernier cas que son noyau est au plus d'ordre 2. Il résulte alors du théorème précédent qu'on a :

COROLLAIRE 18. - Pour chaque naturel $n \geq 1$ non divisible par 8, le noyau hilbertien $H_2(K)$ est contenu dans $K_2(K)^n$. En particulier, on a alors la suite exacte courte :

$$1 \longrightarrow K_2(K)/K_2(K)^n \longrightarrow \bigoplus_p \mu_p/\mu_p^n \longrightarrow \mu/\mu^n \longrightarrow 1.$$

Et, pour chaque premier impair p, le p-sous-groupe de Sylow du noyau hilbertien $H_2(K)$ est l'ensemble des éléments de hauteur infinie du p-Sylow de $K_2(K)$.

§ b. - Le symbole universel de Tate.

Introduisons le module de Tate $\mathbb{T}$, défini comme la limite projective des groupes de racines de l'unité : $\mathbb{T} = \varprojlim_n \mu_n$ (En tant que groupe abstrait, le module $\mathbb{T}$ s'identifie au complété profini $\hat{\mathbb{Z}}$ de l'anneau $\mathbb{Z}$). Le théorème suivant ramène toute question sur le K_2 à un problème de cohomologie galoisienne :

THEOREME 19. - L'application de $K^\times \times K^\times$ dans le groupe $H^2(K, \mathbb{T} \otimes_{\hat{\mathbb{Z}}} \mathbb{T})$, définie par passage à la limite projective à partir des symboles $(\ ,\ )_n$, est un symbole sur K, appelé symbole cohomologique universel, et noté $(\ ,\ )$. L'homomorphisme t du groupe $K_2(K)$ dans $H^2(K, \mathbb{T} \otimes_{\hat{\mathbb{Z}}} \mathbb{T})$ qui factorise ce symbole est une bijection de $K_2(K)$ sur le sous-groupe de torsion $H^2_{tor}(K, \mathbb{T} \otimes_{\hat{\mathbb{Z}}} \mathbb{T})$ du groupe de cohomologie $H^2(K, \mathbb{T} \otimes_{\hat{\mathbb{Z}}} \mathbb{T})$.

Enfin, le groupe $H^2_{tor}(K, \mathbb{T} \otimes_{\hat{\mathbb{Z}}} \mathbb{T})$ s'identifie au quotient $H^1(K, \mu \otimes \mu)/H^1_{div}(K, \mu \otimes \mu)$ du groupe de cohomologie $H^1(K, \mu \otimes \mu)$, où $\mu = \bigcup_{n \geq 1} \mu_n$ est le dual du module de Tate, par son sous-module divisible maximal. En tant que groupe abstrait, le module $H^1_{div}(K, \mu \otimes \mu)$ est somme directe de c_K exemplaires de $\mathbb{Q}/\mathbb{Z}$, l'entier c_K étant le nombre de places complexes du corps K.

COROLLAIRE 20. - Lorsque le corps K contient une racine n-ième primitive de l'unité ζ_n, tout élément d'ordre n de $K_2(K)$ est de la forme $\{\zeta_n, x\}$, pour un x de $K^\times$.

Démonstration. - Cela résulte de la commutativité du diagramme

$$\begin{tikzcd}
\mu_n \otimes K^\times \arrow[r] \arrow[d, "\wr"] & K_2(K) \arrow[r, "\times n"] \arrow[d, hook] & K_2(K) \arrow[r] \arrow[d, hook] & K_2(K)/K_2(K)^n \arrow[d, "\wr"] \\
H^1(K, \mu_n \otimes \mu_n) \arrow[r] & H^2(K, \mathbb{T} \otimes_{\hat{\mathbb{Z}}} \mathbb{T}) \arrow[r, "\times n"] & H^2(K, \mathbb{T} \otimes_{\hat{\mathbb{Z}}} \mathbb{T}) \arrow[r] & H^2(K, \mu_n \otimes \mu_n)
\end{tikzcd}$$

où la ligne du bas est une partie de la suite exacte de cohomologie engendrée par la suite exacte courte :

$$1 \longrightarrow \mathbb{T} \otimes_{\hat{\mathbb{Z}}} \mathbb{T} \xrightarrow{\times n} \mathbb{T} \otimes_{\hat{\mathbb{Z}}} \mathbb{T} \longrightarrow \mu_n \otimes \mu_n \longrightarrow 1.$$

COROLLAIRE 21. - Soient $n \geq 1$ un entier naturel non divisible par 8, et S un ensemble fini de places non complexes de K, contenant les places finies qui divisent n. Si le corps K contient les racines n-ièmes de l'unité, il existe une suite exacte courte canonique :

$$1 \longrightarrow \mu_n \otimes \mathcal{C}\ell^{\mathcal{S}} \longrightarrow R_2^{\mathcal{S}}(K)/R_2^{\mathcal{S}}(K)^n \xrightarrow{h} \widetilde{\bigoplus_{\mathfrak{p} \in \mathcal{S}}} \mu_{\mathfrak{p}}/\mu_{\mathfrak{p}}^n \longrightarrow 1,$$

où $\mathcal{C}\ell^{\mathcal{S}}$ est le groupe des $\mathcal{S}$-classes de diviseurs du corps ; $R_2^{\mathcal{S}}(K)$ est le noyau de l'application : $K_2(K) \longrightarrow \bigoplus_{\mathfrak{p} \notin \mathcal{S}} k_{\mathfrak{p}}^{\times}$; et $\widetilde{\bigoplus_{\mathfrak{p} \in \mathcal{S}}} \mu_{\mathfrak{p}}/\mu_{\mathfrak{p}}^n$ désigne le sous-groupe de la somme directe des quotients d'exposant n des groupes de racines de l'unité des complétés de K pour les places de $\mathcal{S}$, formé des familles $(\bar{\zeta}_{\mathfrak{p}})_{\mathfrak{p} \in \mathcal{S}}$ qui vérifient la formule du produit (dans μ/μ^n).

Démonstration. - Partons de la suite exacte courte

$1 \longrightarrow R_2^{\mathcal{S}}(K) \longrightarrow K_2(K) \xrightarrow{m_{\mathcal{S}}} \bigoplus_{\mathfrak{p} \notin \mathcal{S}} k_{\mathfrak{p}}^{\times} \longrightarrow 1$, qui définit $R_2^{\mathcal{S}}(K)$. Elevant à la puissance n, nous pouvons former, via le lemme du serpent, le diagramme commutatif exact :

$$\begin{tikzcd}
K_2(K)^{(n)} \arrow[r] & \bigoplus_{\mathfrak{p} \notin \mathcal{S}} k_{\mathfrak{p}}^{\times} \arrow[r] & R_2^{\mathcal{S}}(K)/R_2^{\mathcal{S}}(K)^n \arrow[r] & K_2(K)/K_2(K)^n \arrow[r] \arrow[d, "\wr"] & \bigoplus_{\mathfrak{p} \notin \mathcal{S}} k_{\mathfrak{p}}^{\times}/k_{\mathfrak{p}}^{\times n} \arrow[d, "\wr"] \\
\mu_n \otimes K^{\times} \arrow[r] \arrow[u] & \mu_n \otimes D_{\mathcal{S}} \arrow[u, "\wr"] & & \widetilde{\bigoplus_{\mathfrak{p}}} \mu_{\mathfrak{p}}/\mu_{\mathfrak{p}}^n \arrow[r] & \bigoplus_{\mathfrak{p} \notin \mathcal{S}} \mu_{\mathfrak{p}}/\mu_{\mathfrak{p}}^n
\end{tikzcd}$$

Dans celui-ci, la surjection $\mu_n \otimes K^{\times} \longrightarrow K_2(K)^{(n)}$ est donnée par le corollaire 20 ; l'isomorphisme $K_2(K)/K_2(K)^n \simeq \widetilde{\bigoplus_{\mathfrak{p}}} \mu_{\mathfrak{p}}/\mu_{\mathfrak{p}}^n$ résulte du corollaire 18 ; et $D_{\mathcal{S}}$ désigne le groupe des diviseurs de K qui sont étrangers aux places de $\mathcal{S}$ (Rappelons que le groupe des diviseurs d'un corps de nombres est le groupe abélien engendré par les places non complexes de ce corps, avec les relations $\mathfrak{p}^2 = 1$, pour chaque place réelle $\mathfrak{p}$; et que le groupe des classes de diviseurs s'identifie avec le groupe des classes d'idéaux au sens ordinaire lorsque $\mathcal{S}$ contient les places réelles, avec le groupe des classes d'idéaux au sens restreint lorsque $\mathcal{S}$ n'en contient aucune).

5.- APPENDICE - L'ANNEAU DE MILNOR D'UN CORPS DE NOMBRES.

DEFINITION 22.- L'anneau de Milnor d'un corps commutatif K est le quotient $K_*(K)$ de l'algèbre tensorielle $T(K^\times) = \bigoplus_{n\in\mathbb{N}} T^n(K^\times)$, construite sur son $\mathbb{Z}$-module multiplicatif $K^\times$, par l'idéal bilatère gradué I engendré par les éléments de la forme $x \otimes (1-x)$ lorsque x décrit $K \setminus \{0,1\}$. L'anneau $K_*(K) = \bigoplus_{n\in\mathbb{N}} K_n(K)$ est un anneau gradué anticommutatif, dont on note $*$ la loi de composition.

En particulier, on a $K_o(K) = \mathbb{Z}$ et $K_1(K) = K^\times$.

PROPOSITION 23.- Dans l'anneau de Milnor d'un corps commutatif K, les propriétés suivantes sont vérifiées :

$$\left.\begin{array}{ll}(i)' & (aa')*b = (a*b).(a'*b) \\ (ii)' & a*(bb') = (a*b).(a*b')\end{array}\right\} \text{(distributivité)}$$

(iii)' $a*(1-a) = 1$

(iv)' $a*(-a) = 1$

(v)' $a*a = a*(-1)$ $\left(\text{et donc } (a*a)^2 = 1\right)$

(vi)' $(a*b).(b*a) = 1$ (anticommutativité)

(vii)' $a_1*a_2*\ldots*a_n = 1$, pour $a_1+a_2+\ldots+a_n = 0$ ou 1.

Démonstration.- L'idéal gradué I étant engendré par ses éléments de degré 2, on a, comme annoncé dans la définition : $K_o(K) = T^o(K^\times) = \mathbb{Z}$, et $K_1(K) = T^1(K^\times) = K^\times$; ce qui permet d'identifier le groupe multiplicatif de K avec son image canonique $K_1(K)$ dans l'anneau de Milnor. Cela étant, les propriétés (i)' à (vi)' ne sont rien d'autre que la traduction dans $K_*(K)$ des propriétés (i) à (vi), écrites pour le symbole universel $\{\ ,\ \}$, telles qu'elles sont exposées dans la section 1 § a, l'antisymétrie du symbole $\{\ ,\ \}$ correspondant à l'anticommutativité de l'anneau $K_*(K)$. Quant à la propriété (vii)', elle s'obtient directement à partir de (iii)' et (iv)' :

$$a_1 * \ldots * a_{n-1} * \left(1 - a_1 - \ldots - a_{n-1}\right) =$$
$$= \left[a_1 * \ldots * a_{n-1} * \left(1 - a_1\right)\right]\left[a_1 * \ldots * a_{n-1} * \left(-a_2\right)\right] \ldots$$
$$\ldots \left[a_1 * \ldots * a_{n-1} * \left(-a_{n-1}\right)\right] = 1$$

$$a_1 * \ldots * a_{n-1} * \left(-a_1 - \ldots - a_{n-1}\right) =$$
$$= \left[a_1 * \ldots * a_{n-1} * \left(-a_1\right)\right]\left[a_1 * \ldots * a_{n-1} * \left(-a_2\right)\right] \ldots$$
$$\ldots \left[a_1 * \ldots * a_{n-1} * \left(-a_{n-1}\right)\right] = 1.$$

<u>THEOREME ET DEFINITION 24</u>. - Etant donnée une application n-linéaire f sur $K^\times \times \ldots \times K^\times$, à valeurs dans un groupe abélien G, qui prend la valeur unité sur chaque n-uplet $\left(a_1, \ldots, a_n\right)$ vérifiant $a_i + a_{i+1} = 1$, pour un i de $\{1, 2, \ldots, n-1\}$, il existe un unique morphisme $\tilde{f}$ de $K_n(K)$ dans G tel que l'on ait :

$$f\left(a_1, \ldots, a_n\right) = \tilde{f}\left(a_1 * \ldots * a_n\right), \qquad \forall \left(a_1, \ldots, a_n\right) \in K^\times \times \ldots \times K^\times.$$

Une telle application f est appelée un <u>n-symbole</u>.

Démonstration. - Cela résulte immédiatement de la propriété universelle de l'algèbre tensorielle.

Le théorème suivant, dû à Bass et Tate, montre que, pour un corps de nombres, les groupes $K_n(K)$ de degré $n \geq 3$ sont essentiellement bien connus :

<u>THEOREME 25</u>. - Si K est un corps de nombres algébriques, pour chaque naturel $n \geq 3$, le groupe $K_n(K)$ est isomorphe au produit de r copies de $\mathbb{Z}/2\mathbb{Z}$, où r désigne le nombre de places réelles de K.

Pour une démonstration de ce dernier résultat, on pourra se reporter à [2].

BIBLIOGRAPHIE

[1] H. BASS.- K_2 des corps globaux (d'après Tate, Garland,...). Séminaire Bourbaki (1970/71) exp n°394.

[2] H. BASS & J. TATE (avec un appendice de J. TATE).- The Milnor ring of a global field. Algebraic K-Theory II. Lecture Notes in Math. 342 (1973).

[3] J. CARROLL.- On the 2-primary part of $K_2\mathcal{O}$ and on $\mathbb{Z}_2$-extensions for imaginary quadratic fields. Ph. D. Thesis, Cambridge, Mass. (1973).

[4] J.W.S. CASSELS & A. FRÖHLICH.- Algebraic Number Theory. Academic Press, London & New-York (1967).

[5] S.U. CHASE & W.C. WATERHOUSE.- Moore's theorem on uniqueness of reciprocity laws. Inv. Math. 16 (1972) 267-270.

[6] G. GRAS.- Remarks on K_2 of number fields. (preprint).

[7] J.-F. JAULENT.- Sur la formule du produit pour le symbole de reste normique généralisé.

[8] J.-P. SERRE.- Corps locaux. Hermann, Paris (1968).

[9] J. TATE.- Sur la première démonstration par Gauss de la loi de réciprocité (rédigé par J.-R. JOLY). Colloque de Mathématiques Pures, Grenoble (1968).

[10] J. TATE.- Symbols in arithmetic.
Actes Congrès Inter. Math. 1 (1970) 201-211.

[11] J. TATE.- Letter from Tate to Iwasawa on a relation between K_2 and Galois cohomology.
Algebraic K-Theory II. Lecture Notes in Math. 342 (1973).

[12] J. TATE.- Relations between K_2 and Galois cohomology.
Inv. Math. 36 (1976) 257-274.

Jean-François JAULENT
Université de Franche-Comté
Faculté des Sciences - Mathématiques
(E.R.A. n° 070654)
25030 BESANCON CEDEX