ANNALES SCIENTIFIQUES DE L'É.N.S.

FRANÇOISE BERTRANDIAS
JEAN-JACQUES PAYAN

Γ-extensions et invariants cyclotomiques

Annales scientifiques de l'É.N.S. 4^e série, tome 5, n° 4 (1972), p. 517-543
<http://www.numdam.org/item?id=ASENS_1972_4_5_4_517_0>

© Gauthier-Villars (Éditions scientifiques et médicales Elsevier), 1972, 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/

Ann. scient. Éc. Norm. Sup.,
4e série, t. 5, 1972, p. 517 à 543.

Γ-EXTENSIONS ET INVARIANTS CYCLOTOMIQUES

PAR FRANÇOISE BERTRANDIAS ET JEAN-JACQUES PAYAN

K désignera dans la suite un corps commutatif et p un nombre premier impair.

Dans la première partie de notre travail sont présentés certains invariants du corps K à savoir le sous-groupe divisible maximal Z_K et le sous-groupe Y_K des éléments de hauteur infinie du dual X_K du groupe de Galois de la p-extension abélienne maximale de K. Le sous-groupe Z_K décrit les Γ-extensions de K et le sous-groupe Y_K les extensions cycliques de degré p de K qui se plongent dans des p-extensions cycliques de degré arbitrairement grand. Si on suppose que Car $K \neq p$ et que K contient les racines $p^{\text{ièmes}}$ de l'unité, on peut utiliser la théorie de Kummer et mettre en évidence deux sous-groupes Θ_K et Ψ_K de K^* liés respectivement à Z_K et Y_K. Le second est lié au groupe des normes Φ_K de la Γ-extension cyclotomique de K.

Dans la deuxième partie on suppose que K est un corps de nombres; on se sert alors du théorème des normes de Hasse et de la théorie du corps de classes local pour donner une caractérisation globale des invariants Φ_K et Ψ_K définis au chapitre précédent. Cette étude est poussée assez loin dans le cas où un seul idéal premier de K divise p, pour donner des exemples de cas où Z_K et Y_K diffèrent et vérifier la conjecture de Leopoldt sur le rang p-adique des unités dans certains cas nouveaux.

L'étude du groupe des normes Φ_K de la Γ-extension cyclotomique de K est achevée dans le cas où les idéaux premiers de K qui divisent p ont le même corps de décomposition. La détermination de $\dim_{\mathbb{F}_p} \Psi_K/K^{*p}$ s'avère difficile dans le cas où plusieurs idéaux premiers de K divisent p; elle est menée à bien dans l'éventualité où deux idéaux premiers de K divisent p et où le nombre de classes de K n'est pas divisible par p.

Les conversations et échanges de correspondance que nous avons eus avec J.-P. Serre pendant l'élaboration de ce travail, ses suggestions et ses remarques nous ont considérablement facilité la mise au point de nos résultats. Nous tenons à l'en remercier.

1. Application de la théorie de Kummer à l'étude de quelques invariants de la p-extension abélienne maximale de K

1.1. Les groupes X_K, Y_K, Z_K. — On dira qu'une extension L/K est une Γ-extension s'il existe une suite d'extensions K_n de K vérifiant pour tout n, K_n/K cyclique de degré p^n, $K_n \subset K_{n+1}$ et $\bigcup_{n\geq 1} K_n = L$. Gal L/K est isomorphe à Z_p.

Soit G le groupe de Galois de la p-extension abélienne maximale de K, c'est un pro-p-groupe. Posons $X_K = \mathrm{Hom}_{\mathrm{cont}}(G, \mathbf{Q}_p/\mathbf{Z}_p)$, X_K est un p-groupe discret de torsion. Notons respectivement Y_K le sous-groupe des éléments de hauteur infinie et Z_K le sous-groupe divisible maximal de X_K. On sait (voir par exemple [14]) que Z_K est un produit de facteurs isomorphes à $\mathbf{Q}_p/\mathbf{Z}_p$ et que c'est un facteur direct de X_K; il est encore clair que Z_K est un sous-groupe de Y_K.

Les extensions cycliques de degré p^n de K correspondent par dualité et théorie de Galois aux sous-groupes cycliques d'ordre p^n de X_K et les Γ-extensions de K correspondent aux sous-groupes de X_K isomorphes à $\mathbf{Q}_p/\mathbf{Z}_p$.

Les extensions cycliques de degré p de K qui se plongent pour tout n dans une extension cyclique de degré p^n correspondent aux sous-groupes cycliques d'ordre p de Y_K.

Dire que Z_K est produit de s facteurs isomorphes à $\mathbf{Q}_p/\mathbf{Z}_p$ signifie que le nombre maximal de Γ-extensions indépendantes de K est égal à s.

Définition. — *Nous dirons qu'un p-groupe de torsion* A *est de cotype fini si l'ensemble des x de* A *vérifiant $px = 0$ est fini.*

Nous utiliserons le résultat suivant (pour une démonstration voir par exemple [14] ou les exercices de [3]).

Proposition 1.1. — *Soit* A *un p-groupe de torsion de cotype fini; alors* A *est isomorphe à* $(\mathbf{Q}_p/\mathbf{Z}_p)^s \prod_{i=1}^{t} \mathbf{Z}/p^{n_i}\mathbf{Z}$.

EXEMPLES. — (1) Si K est un corps de caractéristique nulle discrètement valué complet à corps résiduel $\overline{K}$ fini, alors X_K est de cotype fini. Cela résulte de ce que K admet un nombre fini d'extensions de degré p. La théorie du corps de classes local montre que si $\operatorname{Car}\overline{K} \neq p$ (resp. $\operatorname{Car}\overline{K} = p$) :

$$X_K \simeq \mathbf{Q}_p/\mathbf{Z}_p \oplus \mathbf{Z}/p^m\mathbf{Z} \qquad [\text{resp. } X_K \simeq (\mathbf{Q}_p/\mathbf{Z}_p)^{[K:\mathbf{Q}_p]+1} \oplus \mathbf{Z}/p^m\mathbf{Z}],$$

où m est l'entier maximal tel que K contienne les racines $(p^m)^{\text{ièmes}}$ de 1. On voit que $Y_K = Z_K \simeq \mathbf{Q}_p/\mathbf{Z}_p$ [resp. $\simeq (\mathbf{Q}_p/\mathbf{Z}_p)^{[K:\mathbf{Q}_p]+1}$].

(2) Si K est un corps de nombres, il existe une infinité d'extensions cycliques de degré p de K; le groupe X_K n'est donc pas de cotype fini.

Établissons alors le résultat suivant :

PROPOSITION 1.2. — *Si* K *est un corps de nombres,* Y_K *est de cotype fini.*

Démonstration. — Cela revient à voir qu'il n'existe qu'un nombre fini d'extensions cycliques de degré p de K se plongeant pour tout n dans une extension cyclique de degré p^n de K. Montrons qu'une extension cyclique K_1/K de degré p vérifiant la propriété précédente est non ramifiée en dehors de p. Soit $\mathfrak{q}$ un idéal premier de K qui ne divise pas p. Si K_1/K est ramifiée en $\mathfrak{q}$, toute p-extension cyclique contenant K_1 est totalement ramifiée en $\mathfrak{q}$. On voit alors que le complété $K_{1,\mathfrak{q}}$ se plonge pour tout n dans une extension cyclique de degré p^n de $K_\mathfrak{q}$ totalement ramifiée ce qui est absurde; en effet, si $n > m$, $K_\mathfrak{q}$ ne possède pas d'extension cyclique de degré p^n totalement ramifiée (théorie du corps de classes local). La théorie du corps de classes global montre qu'il existe un nombre fini au plus d'extensions abéliennes de degré donné non ramifiées en dehors d'un nombre fini de places données, ce qui achève la démonstration.

Il en résulte que Y_K est isomorphe à

$$(\mathbf{Q}_p/\mathbf{Z}_p)^{s_K} \prod_{i=1}^{t_K} \mathbf{Z}/p^{n_i}\mathbf{Z}$$

et que Z_K est isomorphe à $(\mathbf{Q}_p/\mathbf{Z}_p)^{s_K}$. Compte tenu de ce qui a été dit précédemment de la correspondance entre les Γ-extensions de K et les sous-groupes de X_K isomorphes à $\mathbf{Q}_p/\mathbf{Z}_p$, on voit que s_K est le nombre maximal de Γ-extensions indépendantes de K. Rappelons brièvement le lien entre ce nombre et la conjecture de Leopoldt sur le rang p-adique des unités (voir par exemple [2], [4], [12] et [18].

On appelle rang p-adique $r_{K,p}$ des unités de K le rang de la matrice $(\log \tau(\varepsilon_i))_{\tau \in T_K,\, i=1,2,\ldots,r_K}$ où T_K est l'ensemble des $[K:\mathbf{Q}]$ isomorphismes

distincts de K dans une clôture algébrique Ω_p de $\mathbf{Q}_p$, $(\varepsilon_i)_{i=1,2,\ldots,r_K}$ est un système fondamental d'unités de K et log est le logarithme p-adique. La conjecture de Leopoldt [4] est l'égalité $r_{K,p} = r_K$ rang des unités de K, pour tout corps de nombres K. Elle a été démontrée dans certains cas ([2], [4], [12]) et A. Brumer a en particulier prouvé que $r_{K,p} = r_K$ si K est un corps abélien sur $\mathbf{Q}$ ou sur un corps quadratique imaginaire. On voit encore facilement que si la conjecture est vraie pour un corps de nombres K elle est vraie pour tout sous-corps de K.

Grâce à la théorie du corps de classes (*voir* [11], p. 21) on montre que $r_{K,p}$ et s_K sont liés par $s_K = [K : \mathbf{Q}] - r_{K,p}$. La conjecture est donc équivalente à l'égalité

$$s_K = [K : \mathbf{Q}] - r_K$$

ou encore, si K est totalement imaginaire, à

$$s_K = \frac{1}{2}[K : \mathbf{Q}] + 1.$$

1.2. Le groupe Θ_K.

Notations et conventions. — On note μ_{p^i} le groupe des racines $(p^i)^{\text{ièmes}}$ de 1.

On suppose dorénavant que Car $K \neq p$, et que K contient le groupe μ_p. Le cas où K contient $\mu_{p^\infty} = \bigcup_{i \geq 1} \mu_{p^i}$ est relativement simple car X_K est divisible. Nous l'exclurons ici et nous noterons m l'entier positif défini par $K \supset \mu_{p^m}$ et $K \not\supset \mu_{p^{m+1}}$. Pour tout entier $n \geq 1$, nous désignerons par ζ_n une racine primitive $(p^n)^{\text{ième}}$ de 1 normée par $\zeta_n^p = \zeta_{n-1}$; nous poserons $K_n = K(\zeta_n)$ et nous noterons N_n l'application norme de K_n sur K :

$$N_n = N_{K_n/K}.$$

Définition. — *On note* Θ_K *l'ensemble des* α *de* K^* *tels que* $K(\alpha^{p^{-1}})$ *se plonge dans une* Γ-*extension de* K.

Remarques :

(*a*) Θ_K est un sous-groupe multiplicatif de K^* contenant K^{*p};

(*b*) Θ_K/K^{*p} est canoniquement isomorphe (par la théorie de Kummer) au sous-groupe $Z_{K,p}$ des éléments de Z_K annulés par p;

(*c*) On a donc le résultat suivant :

Pour que Z_K soit produit d'un nombre fini de facteurs isomorphes à $\mathbf{Q}_p/\mathbf{Z}_p$ il faut et il suffit que la dimension sur F_p de Θ_K/K^{*p} (notée $\dim_{F_p} \Theta_K/K^{*p}$) soit finie. Dans ce cas $s_K = \dim_{F_p}(\Theta_K/K^{*p})$.

1.3. Le groupe $K^{*p}\,N_n(K_n^*)$. — Nous allons maintenant établir un résultat qui va jouer un rôle central pour la suite :

Théorème 1. — *Soit α un élément de K^*. Pour que l'extension $K(\alpha^{p^{-1}})$ se plonge dans une extension cyclique de degré p^n de K, il faut et il suffit que α appartienne au groupe $K^{*p}\,N_n(K_n^*)$.*

Remarque. — Par la théorie de Kummer, le groupe $K^{*p}\,N_n(K_n^*)/K^{*p}$ est donc canoniquement isomorphe au groupe des éléments de hauteur $\geqq p^{n-1}$ de $X_{K,p}$ (sous-groupe des éléments de X_K annulés par p).

Démonstration du théorème 1. — Si $1 \leqq n \leqq m$, $K^{*p}\,N_n(K_n^*) = K^*$; le résultat est évident. Supposons donc $m+1 \leqq n$; on a $[K_n : K] = p^{n-m}$. Soit τ le K-automorphisme de K_n tel que $\tau(\zeta_n) = \zeta_n^{1+p^m}$; on sait que τ engendre le groupe cyclique $\mathrm{Gal}(K_n/K)$.

a. Supposons $K(\alpha^{p^{-1}})$ plongé dans une extension cyclique L de degré p^n de K.

On suppose évidemment que α n'appartient pas à K^{*p}. Si L n'est pas linéairement disjointe de K_n sur K, $K(\alpha^{p^{-1}}) = K_{m+1}$, c'est-à-dire $\alpha \in \zeta_m^{\mathbf{Z}}\,K^{*p}$ et donc $\alpha \in K^{*p}\,N_n(K_n^*)$. [En effet $\zeta_m = N_n(\zeta_n)$.]

Si L est linéairement disjointe de K_n, l'extension composée $L' = K_n.L$ est cyclique de degré p^n sur K_n; il existe donc un élément α_n de K_n tel que

$$L' = K_n(\alpha_n^{p^{-n}}) \qquad \text{et} \qquad \alpha_n \in \alpha\,K_n^{*p}.$$

De plus, comme l'extension $K_n(\alpha^{p^{-n}})/K$ est abélienne, on a ([8], [19]) :

$$\alpha_n^{\tau-1-p^m} \in K_n^{*p^n}.$$

Notons ν_n et μ_n les éléments de K_n définis par

$$\alpha_n\,\alpha^{-1} = \nu_n^p \qquad \text{et} \qquad \alpha_n^{\tau-1-p^m} = \alpha^{-p^m}\,\nu_n^{p(\tau-1-p^m)} = \mu_n^{-p^n}.$$

D'où en prenant les normes, on obtient l'égalité

$$\alpha^{p^n} = N_n(\nu_n)^{-p^{m+1}}\,N_n(\mu_n)^{p^n} \tag{1}$$

qui entraîne la propriété annoncée si l'on montre que $N_n(\nu_n)$ est une puissance $(p^{n-m})^{\text{ième}}$ dans K.

Nous aurons besoin du

Lemme 1. — *Soient m et n des entiers vérifiant $n > m \geqq 1$; on peut trouver u_n dans $\mathbf{Z}$ et $f_n(x)$ dans $\mathbf{Z}[x]$ tels que*

$$1 + x + \ldots + x^{p^{n-m}-1} = (x - 1 - p^m)\,f_n(x) + (1 + u_n\,p^m)\,p^{n-m}.$$

Démonstration. — La divisibilité dans $\mathbf{Z}[x]$ montre que le reste de la division de $1 + x + \ldots + x^{p^{n-m-1}}$ par $x - 1 - p^m$ est égal à

$$1 + (1 + p^m) + (1 + p^m)^2 + \ldots + (1 + p^m)^{p^{n-m-1}} = \prod_{i=1}^{p^{n-m-1}} (1 + p^m - \zeta_{n-m}^i)$$

$$= \prod_{j=1}^{n-m} \mathrm{N}_{\mathbf{Q}_j/\mathbf{Q}}(1 + p^m - \zeta_j);$$

comme

$$\mathrm{N}_{\mathbf{Q}_j/\mathbf{Q}}(1 + p^m - \zeta_j) = p\, \mathrm{N}_{\mathbf{Q}_j/\mathbf{Q}}\left(1 + \frac{p^m}{1 - \zeta_j}\right) \equiv p \quad (p^{m+1}),$$

on en déduit :

$$\prod_{j=1}^{n-m} \mathrm{N}_{\mathbf{Q}_j/\mathbf{Q}}(1 + p^m - \zeta_j) \equiv p^{n-m} \quad (p^{m+1}.p^{n-m-1}).$$

L'assertion est démontrée.

De $\nu_n^p = \alpha_n\, \alpha^{-1}$, résulte $\nu_n^{p(\tau-1-p^m)} = \mu_n^{-p^{n+1}}\, \alpha^{p^{m+1}}$, soit $\nu_n^{\tau-1-p^m} = \alpha^{p^m}\, \mu_n^{-p^n}\, \zeta_1^i$. Par ailleurs $\mathrm{N}_n(\nu_n) = \nu_n^{1+\tau+\ldots+\tau^{p^{n-m}-1}}$; compte tenu du lemme on obtient

$$\mathrm{N}_n(\nu_n) = \nu_n^{(\tau-1-p^m) f_n(\tau) + (1+u_n p^m) p^{n-m}},$$

d'où

$$\mathrm{N}_n(\nu_n) = \alpha^{p^m f_n(\tau)}\, \mu_n^{-p^n f_n(\tau)}\, \zeta_1^{i f_n(\tau)}\, \nu_n^{(1+u_n p^m) p^{n-m}};$$

soit encore, compte tenu de $\alpha^{f_n(\tau)} = \alpha^{f_n(1)} = \alpha^{u_n p^{n-m}}$,

$$\mathrm{N}_n(\nu_n) = \alpha^{p^n u_n}\, \nu_n^{(1+u_n p^m) p^{n-m}}\, \mu_n^{-p^n f_n(\tau)} \in \mathrm{K}_n^{*p^{n-m}}$$

donc $\mathrm{N}_n(\nu_n) \in \mathrm{K}_n^{*p^{n-m}} \cap \mathrm{K}^*$ ce qui équivaut à $\mathrm{N}_n(\nu_n) = \zeta_m^j . \rho_n^{p^{n-m}}$ avec $\rho_n \in \mathrm{K}^*$. En reportant dans (1) on obtient $\alpha^{p^n} = \rho_n^{-p^{n+1}}\, \mathrm{N}_n(\mu_n)^{p^n}$. D'où $\alpha = \rho_n^{-p}\, \mathrm{N}_n(\mu_n)$.

b. Réciproquement supposons que $\alpha \in \mathrm{K}^{*p}\, \mathrm{N}_n(\mathrm{K}_n^*)$. Écrivons :

$$\alpha = \rho^p\, \mathrm{N}_n(\mu_n) \qquad (\rho \in \mathrm{K}^*,\ \mu_n \in \mathrm{K}_n^*).$$

Ceci peut s'écrire, en utilisant le lemme 1 du (*a*) :

$$\alpha = \rho^p \left[\mu_n^{1+u_n p^m}\right]^{p^{n-m}} \left[\mu_n^{f_n(\tau)}\right]^{\tau-1-p^m}.$$

D'où

$$\alpha^{p^m} = \left[\mu_n^{1+u_n p^m}\right]^{p^n} \left[\mu_n^{p^m f_n(\tau)}\, \rho^{-p}\right]^{\tau-1-p^m}.$$

Posons

$$\nu_n = \mu_n^{p^{m-1} f_n(\tau)}\, \rho^{-1}, \qquad \alpha_n = \alpha \nu_n^p.$$

On a

$$\alpha_n^{\tau-1-p^m} = \alpha^{-p^m}\, \nu_n^{p(\tau-1-p^m)} = \left[\mu_n^{1+\mu_n p^m}\right]^{p^n} \in \mathrm{K}_n^{*p^n}.$$

L'extension $K_n(\alpha_n^{p^{-n}})/K$ est donc abélienne ([8], [19]); cette extension contient $K(\alpha^{p^{-1}})$. On peut en déduire l'existence d'une extension L cyclique de degré p^n de K contenant $K(\alpha^{p^{-1}})$ grâce au :

LEMME 2. — *Soit* $K(\alpha^{p^{-1}})$ *une extension cyclique de degré p de* K *contenue dans une extension* $K_n(\alpha_n^{p^{-n}})$ *cyclique de degré* p^n *de* K_n, *abélienne sur* K. *Il existe une extension* L *cyclique de degré* p^n *de* K *contenant* $K(\alpha^{p^{-1}})$.

Démonstration. — Si $K(\alpha^{p^{-1}}) \subset K_n$, le résultat est évident. Sinon, considérons le corps $K_\infty = \bigcup_{n \in \mathbf{N}} K_n$ et l'extension $K_\infty(\alpha_n^{p^{-n}})$, qui est une extension abélienne de K.

Soient $G = \mathrm{Gal}(K_\infty(\alpha_n^{p^{-n}})/K)$, σ un K_∞-automorphisme de $K_\infty(\alpha_n^{p^{-n}})$ engendrant le groupe cyclique $\mathrm{Gal}(K_\infty(\alpha_n^{p^{-n}})/K_\infty)$, τ un K-automorphisme de $K_\infty(\alpha_n^{p^{-n}})$ tel que pour tout entier $n \geqq m$: $\tau(\zeta_n) = \zeta_n^{1+p^m}$. On voit que G est un $\mathbf{Z}_p$-module engendré par σ et τ; son sous-module de torsion, $\langle \sigma \rangle$ est donc facteur direct. Il en résulte $G = \langle \sigma \rangle \times \langle \tau \rangle$ (produit direct) ($\langle \sigma \rangle \simeq \mathbf{Z}/p^n\mathbf{Z}$ et $\langle \tau \rangle \simeq \mathbf{Z}_p$).

L'extension intermédiaire $K(\alpha^{p^{-1}})$ est le corps des invariants d'un sous-groupe d'indice p de G, qui ne contient pas σ; c'est donc un sous-groupe de la forme $\langle \sigma^p, \tau\sigma^i \rangle$, où i est un entier $(0 \leqq i < p)$; $K(\alpha^{p^{-1}})$ est donc contenu dans le corps L des invariants du groupe $\langle \tau\sigma^i \rangle$ et on a bien $G/\langle \tau\sigma^i \rangle \simeq \mathbf{Z}/p^n\mathbf{Z}$.

1.4. LE GROUPE Ψ_K. — Si une extension $K(\alpha^{p^{-1}})$ de K est contenue dans une Γ-extension de K elle se plonge pour tout entier n dans une extension cyclique de degré p^n de K. Il est donc naturel d'introduire la définition suivante :

DÉFINITION. — *On note* Ψ_K *l'ensemble des* α *de* K^* *tels que pour tout entier* $n \geqq 1$, $K(\alpha^{p^{-1}})$ *se plonge dans une extension cyclique de degré* p^n *de* K.

REMARQUES :

(*a*) Ψ_K est un sous-groupe de K^* et $\Psi_K \supset K^{*p}$.

(*b*) $\Theta_K \subset \Psi_K$.

(*c*) Ψ_K/K^{*p} est canoniquement isomorphe (par la théorie de Kummer) au sous-groupe $Y_{K,p}$ des éléments de Y_K annulés par p.

(*d*) On a donc le résultat suivant : pour que Y_K soit de cotype fini il faut et il suffit que la dimension sur F_p de Ψ_K/K^{*p} soit finie. Dans ce cas $s_K + t_K = \dim_{F_p} \Psi_K/K^{*p}$.

Le théorème 1 admet le corollaire :

COROLLAIRE :

$$\Psi_K = \bigcap_{n>m} K^{*p}\, N_n\,(K_n^*) = \bigcap_{n\geq m} N_{n+1,n}\,(K_{n+1}^*) \qquad (\text{où } N_{n+1,n} = N_{K_{n+1}/K_n}).$$

La première expression de Ψ_K résulte immédiatement du théorème 1; la deuxième se déduit du lemme suivant :

LEMME. — *On a, pour tout entier $n \geq m$, l'égalité*

$$K^{*p}\, N_{n+1}\,(K_{n+1}^*) = K^* \cap N_{n+1,n}\,(K_{n+1}^*).$$

Démonstration. — *a.* Montrons que $K^{*p}\, N_{n+1}\,(K_{n+1}^*) \subset K^* \cap N_{n+1,n}\,(K_{n+1}^*)$ si $n \geq m$. Il suffit de vérifier que $N_{n+1}\,(K_{n+1}^*) \subset N_{n+1,n}\,(K_{n+1}^*)$ pour tout entier $n \geq m$. Soit $\alpha \in N_{n+1}\,(K_{n+1}^*)$; il existe $\beta \in K_{n+1}^*$ tel que

$$\begin{aligned}\alpha &= \beta^{1+\tau+\tau^2+\ldots+\tau^{p^{n-m+1}-1}} \\ &= \beta^{\left[1+\tau+\tau^2+\ldots+\tau^{p^{n-m}-1}\right]\left[1+\tau^{p^{n-m}}+\tau^{2p^{n-m}}+\ldots+\tau^{(p-1)p^{n-m}}\right]} \\ &= N_{n+1,n}\left(\beta^{1+\tau+\ldots+\tau^{p^{n-m}-1}}\right).\end{aligned}$$

(*b*) En sens inverse, montrons que

$$K^* \cap N_{n+1,n}\,(K_{n+1}^*) \subset K^{*p}\, N_{n+1}\,(K_{n+1}^*) \qquad \text{si} \quad n \geq m.$$

Soit α un élément du premier membre, c'est-à-dire

$$\alpha = \beta^{1+\tau^{p^{n-m}}+\tau^{2p^{n-m}}+\ldots+\tau^{(p-1)p^{n-m}}}$$

avec $\alpha \in K^*$, $\beta \in K_{n+1}^*$.

L'égalité $\alpha^\tau = \alpha$ entraîne $N_{n+1,n}\,(\beta^{\tau-1}) = 1$; comme l'extension K_{n+1}/K_n est cyclique, le théorème 90 montre l'existence d'un élément γ de K_{n+1} tel que

$$\beta^{\tau-1} = \gamma^{\tau^{p^{n-m}}-1} = \gamma^{\left[\tau^{p^{n-m}-1}+\ldots+\tau+1\right][\tau-1]}.$$

On en déduit l'existence d'un élément ρ de K^* tel que

$$\beta = \gamma^{\tau^{p^{n-m}-1}+\ldots+\tau+1}\,\rho.$$

Par suite en prenant la norme

$$\alpha = \rho^p\, \gamma^{1+\tau+\tau^2+\ldots+\tau^{p^{n-m+1}-1}} = \rho^p\, N_{n+1}\,(\gamma)$$

et donc $\alpha \in K^{*p}\, N_{n+1}\,(K_{n+1}^*)$.

1.5. Le groupe Φ_K. — On peut toujours écrire

$$\bigcap_{n\geqq m} K^{*p}\, N_n(K_n^*) \supset K^{*p} \bigcap_{n\geqq m} N_n(K_n^*)$$

mais il n'y a pas égalité en général. Ce qui précède montre l'intérêt d'introduire le groupe des normes cyclotomiques de K :

Définition. — *On note* Φ_K *le sous-groupe de* K^* *défini par*

$$\Phi_K = \bigcap_{n\geqq m} N_n(K_n^*).$$

C'est le groupe des normes cyclotomiques.

Remarques :

(*a*) $K^{*p}\,\Phi_K \subset \Psi_K$.

(*b*) Pour tout n on a l'inclusion $N_{n+1,n}(\Phi_{K_{n+1}}) \subset \Phi_{K_n}$.

Dans le cas où l'inclusion de la remarque (*b*) est remplacée par une égalité on peut énoncer :

Proposition 1.3. — *Supposons que pour tout* $n \geqq m$ *on ait*

$$N_{n+1,n}(\Phi_{K_{n+1}}) = \Phi_{K_n};$$

alors $K^{*p}\,\Phi_K \subset \Theta_K$.

Démonstration. — Soit α un élément de Φ_K, il existe une suite $\{\mu_n\}$ telle que pour tout n : $\mu_n \in K_n$, $\alpha = N_n(\mu_n)$ et $\mu_n = N_{n+1,n}(\mu_{n+1})$. Reprenons les notations du lemme 1 du paragraphe 1.3 et posons

$$\nu_n = \mu_n^{p^{m-1} f_n(\tau)}.$$

La démonstration du théorème 1, partie (*b*) montre que $L'_n = K_n((\alpha\nu_n^p)^{1/p^n})$ est abélienne sur K et cyclique de degré p^n sur K_n. Notons $K_\infty = \bigcup_{n\geqq m} K_n$ et $L'_\infty = \bigcup_{n\geqq m} L'_n$. On voit facilement que la suite L'_n est croissante; il suffit en effet de vérifier que $\nu_{n+1}/\nu_n \in K_{n+1}^{*p^{n-1}}$ pour tout $n > m$. On trouve

$$\frac{\nu_{n+1}}{\nu_n} = \left(\frac{\mu_{n+1}^{f_{n+1}(\tau)}}{\mu_{n+1}^{(1+\tau^{p^n}+\ldots+\tau^{(p-1)p^n}) f_n(\tau)}}\right)^{p^{m-1}} = \left(\mu_{n+1}^{\frac{(1+\tau^{p^n}+\ldots+\tau^{(p-1)p^n})(1+\mu_n p^m) - p(1+\mu_{n+1}p^m)}{\tau-1-p^m}}\right)^{p^{n-1}},$$

d'où le résultat.

On peut donc affirmer : ou bien $K(\alpha^{p^{-1}})$ est égale à K_{m+1}, $K(\alpha^{p^{-1}})$ est alors plongée dans la Γ-extension cyclotomique de K; ou bien $K(\alpha^{p^{-1}})$ est linéairement disjointe de K_{m+1} sur K. L'_∞ est alors une Γ-extension de K_∞

abélienne sur K et, contenant $K(\alpha^{p^{n-1}})$. On en déduit par une démontration analogue celle du lemme 2 du paragraphe 1.3 que $\mathrm{Gal}\, L'_\infty/K$ est isomorphe à $\mathbf{Z}_p \oplus \mathbf{Z}_p$ et l'existence d'une Γ-extension L_∞ de K contenant $K(\alpha^{p^{n-1}})$.

EXEMPLE. — Supposons que K est un corps local de caractéristique nulle à corps résiduel fini vérifiant $K \supset \mu_p$. Alors $\Theta_K = \Psi_K = K^{*p}\Phi_K$.

L'égalité $\Psi_K = K^{*p}\Phi_K$ résulte de la compacité locale de K. Celle de Θ_K et de Ψ_K est conséquence de l'égalité $Y_K = Z_K$ (exemple 1 du paragraphe 1.1).

Pour cet exemple, les applications $N_{n+1,n} : \Phi_{K_{n+1}} \to \Phi_{K_n}$ sont surjectives. (Cela se voit encore par des arguments de compacité locale.)

1.6. LES GROUPES $\Theta_K^{(i)}$ ET $\Psi_K^{(i)}$. — Lorsque l'entier m relatif au corps K est > 1, on peut obtenir, par les méthodes des paragraphes 1.3 et 1.4 des groupes isomorphes aux sous-groupes Z_{K,p^i} (resp. Y_{K,p^i}) des éléments de Z_K (resp. Y_K) annulés par p^i, i étant un entier compris entre 1 et m.

DÉFINITIONS :

(*a*) *On note* $\Theta_K^{(i)}$ *l'ensemble des* α *de* K* *tels que* $K(\alpha^{p^{n-i}})$ *se plonge dans une* Γ*-extension de* K;

(*b*) *On note* $\Psi_K^{(i)}$ *l'ensemble des* α *de* K* *tels que, pour tout entier* $n \geq 1$, $K(\alpha^{p^{n-i}})$ *se plonge dans une extension cyclique de degré* p^n *de* K.

REMARQUES :

(*a*) $\Theta_K^{(i)}$ *et* $\Psi_K^{(i)}$ *sont des sous-groupes de* K* *contenant* K^{*p^i};

(*b*) $\Theta_K^{(i)}/K^{*p^i}$ (resp. $\Psi_K^{(i)}/K^{*p^i}$) est canoniquement isomorphe (par la théorie de Kummer) à Z_{K,p^i} (resp. Y_{K,p^i}).

Donnons, sans démonstration, les résultats suivants, qui généralisent ceux des paragraphes 1.3 et 1.4 :

THÉORÈME 1'. — *Soient* α *un élément de* K* *et n un entier* $> m$. *Pour que l'extension* $K(\alpha^{p^{n-i}})$ *se plonge dans une extension cyclique de* K *de degré* p^{n-i} *sur* $K(\alpha^{p^{n-i}})$, *il faut et il suffit que* α *appartienne au groupe* $K^{*p^i} N_n(K_n^*)$.

COROLLAIRE :

$$\Psi_K^{(i)} = \bigcap_{n>m} K^{*p^i} N_n(K_n^*) = \bigcap_{n\geq m} N_{n+i,n}(K_{n+i}^*).$$

2. Cas des corps de nombres

NOTATIONS ET CONVENTIONS. — On suppose dorénavant que K est une extension finie de $\mathbf{Q}$ et on reprend les hypothèses du paragraphe 1 : K contient μ_p et on désigne encore par m l'entier défini par $K \supset \mu_{p^m}$ et $K \not\supset \mu_{p^{m+1}}$. On note $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_g$ les idéaux premiers qui divisent p,

et si $K/\mathbf{Q}$ galoisienne, e et f leur indice de ramification et leur degré absolu, $(p) = (\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_g)^e$. On désignera, dans le cas $K/\mathbf{Q}$ galoisienne, par k_i le corps de décomposition de $\mathfrak{p}_i$ et par k la norme des k_i, à savoir $k = k_1\, k_2 \ldots k_g$.

On dit qu'un élément α de K^* est une p-unité si l'idéal (α) s'écrit $(\alpha) = \mathfrak{p}_1^{n_1}\, \mathfrak{p}_2^{n_2} \ldots \mathfrak{p}_g^{n_g}$ $(n_i \in \mathbf{Z})$. On note P_K le groupe des p-unités de K; il contient le groupe T_K des racines de l'unité de K et on sait que P_K/T_K est un $\mathbf{Z}$-module libre de rang $r_2 + g - 1$, où $[K : \mathbf{Q}] = 2\, r_2$.

Pour toute place finie $\mathfrak{q}$ de K on note $\alpha_\mathfrak{q}$ l'image de α par un plongement de K dans $K_\mathfrak{q}$ complété $\mathfrak{q}$-adique de K.

2.1. Localisation. — Nous utiliserons fréquemment dans ce qui suit les deux théorèmes suivants sur les normes.

Théorème A (Hasse, *cf.* [5]). — *Soient* K *un corps de nombres et* L *une extension cyclique de* K. *Pour que* $\alpha \in K^*$ *soit une norme pour* L/K *il faut et il suffit que pour toute place* $\mathfrak{q}$ *de* K *et toute place* $\mathfrak{Q}$ *de* L *au-dessus de* $\mathfrak{q}$, $\alpha_\mathfrak{q}$ *soit une norme pour* $L\mathfrak{Q}/K_\mathfrak{q}$.

Théorème B (Pour une démonstration voir [6], chap. IX). — *Soient* K *un corps local de caractéristique nulle à corps résiduel fini,* L *une extension abélienne de* K *et* K′ *une extension finie de* K. *Pour que* α *de* K'^* *soit une norme pour l'extension* LK′/K′ *il faut et il suffit que* $N_{K'/K}(\alpha)$ *soit une norme pour l'extension* L/K.

Nous pouvons alors énoncer :

Proposition 2.1. — Φ_K *est le sous-groupe de* P_K *défini par*

$$\Phi_K = \{\, \alpha \in P_K \mid \textit{Pour tout } i = 1, 2, \ldots, g,\ N_{K_{\mathfrak{p}_i}/\mathbf{Q}_p}(\alpha_{\mathfrak{p}_i}) \in p^{\mathbf{Z}} \,\}.$$

Démonstration. — $\Phi_K = \bigcap_{n \geq m} N_n(K_n^*)$; comme K_n/K est cyclique, le théorème de Hasse montre qu'un α de K^* appartient au groupe des normes $N_n(K_n^*)$ si et seulement si pour toute place finie $\mathfrak{q}$ de K, on a $\alpha_\mathfrak{q} \in N_{K_{\mathfrak{q},n}/K_\mathfrak{q}}(K_{\mathfrak{q},n}^*)$. En appliquant le théorème B avec $K = \mathbf{Q}_p$, $L = \mathbf{Q}_p(\zeta_n)$ et $K' = K_\mathfrak{q}$, cela équivaut à

$$N_{K_\mathfrak{q}/\mathbf{Q}_q}(\alpha_\mathfrak{q}) \in N_{\mathbf{Q}_q(\zeta_n)/\mathbf{Q}_q}(\mathbf{Q}_q(\zeta_n)^*)$$

(où q est le nombre premier naturel que divise $\mathfrak{q}$). Par ailleurs,

$$\bigcap_{n \geq m} N_{\mathbf{Q}_q(\zeta_n)/\mathbf{Q}_q}(\mathbf{Q}_q(\zeta_n)^*) = \begin{cases} U_q & \text{si } q \neq p, \\ p^{\mathbf{Z}} & \text{si } q = p. \end{cases}$$

(en désignant par U_q le groupe des unités de $\mathbf{Q}_q$.) D'où la proposition 2.1.

Les quelques notations qui suivent nous seront utiles pour l'étude de Ψ_K. Pour $i = 1, 2, \ldots, g$, on note j_i l'entier défini par $K_{\mathfrak{p}_i} \supset \mu_{p^{m+j_i}}$ et $K_{\mathfrak{p}_i} \not\supset \mu_{p^{m+j_i+1}}$. Pour tout entier n, on notera $U^{(n)}$ le sous-groupe de U_p formé des u vérifiant $u \equiv 1\ (p^n)$.

PROPOSITION 2.2. — *Ψ_K est formé des α de K^* vérifiant*

$$N_{K_{\mathfrak{p}_i}/\mathbf{Q}_p}(\alpha_{\mathfrak{p}_i}) \in p^{\mathbf{Z}} U^{(m+j_i+1)}$$

pour $i = 1, 2, \ldots, g$, et $\alpha_{\mathfrak{q}} \in K_{\mathfrak{q}}^{*p} U_{\mathfrak{q}}$ (où $U_{\mathfrak{q}}$ désigne le groupe des unités de $K_{\mathfrak{q}}$) pour toute place $\mathfrak{q}$ finie ne divisant pas p.

Démonstration. — Le corollaire du théorème 1 (§ 1.4) montre que $\Psi_K = \bigcap_{n \geq m} N_{n+1,n}(K_{n+1}^*)$. Le théorème de Hasse montre qu'un α de K^* appartient à $N_{n+1,n}(K_{n+1}^*)$ si et seulement si pour toute place $\mathfrak{q}$ de K on a

$$\alpha_{\mathfrak{q}} \in N_{K_{\mathfrak{q}}(\zeta_{n+1})/K_{\mathfrak{q}}(\zeta_n)}(K_{\mathfrak{q}}(\zeta_{n+1})^*).$$

Si $\mathfrak{q}$ ne divise pas p, $K_{\mathfrak{q}}(\zeta_{n+1})/K_{\mathfrak{q}}(\zeta_n)$ est non ramifiée, elle est de degré p pour n assez grand, d'où l'énoncé pour ces places.

Pour $\mathfrak{q} = \mathfrak{p}_i$ le théorème B montre que

$$\alpha_{\mathfrak{p}_i} \in N_{K_{\mathfrak{p}_i}(\zeta_{n+1})/K_{\mathfrak{p}_i}(\zeta_n)}(K_{\mathfrak{p}_i}(\zeta_{n+1})^*)$$

équivaut

$$N_{K_{\mathfrak{p}_i}(\zeta_n)/\mathbf{Q}_p}(\alpha_{\mathfrak{p}_i}) \in N_{\mathbf{Q}_p(\zeta_{n+1})/\mathbf{Q}_p}(\mathbf{Q}_p(\zeta_{n+1})^*).$$

On sait (voir par exemple [1]) que le groupe des normes associé à $\mathbf{Q}_p(\zeta_{n+1})/\mathbf{Q}_p$ est égal à $p^{\mathbf{Z}} U^{(n+1)}$. La condition se ramène donc à

$$N_{K_{\mathfrak{p}_i}/\mathbf{Q}_p}(\alpha_{\mathfrak{p}_i})^{p^{n-m-j_i}} \in p^{\mathbf{Z}} U^{(n+1)}$$

(pour un $n < m + j_i$, $\alpha_{\mathfrak{p}_i}$ est évidemment une norme). On constate que si la condition est vérifiée pour $n = m + j_i$, elle l'est pour tous les $n > m + j_i$. D'où le résultat de la proposition 2.2.

REMARQUE. — $j_i > 0$ signifie que $\mathfrak{p}_i$ est décomposée dans K_{m+1}/K. Si p ne divise pas le nombre de classes h_K de K, un des j_i au moins est nul. Si $K/\mathbf{Q}(\zeta_m)$ est galoisienne et si p ne divise pas h_K, tous les j_i sont nuls. Si $K/\mathbf{Q}(\zeta_m)$ est galoisienne de degré premier à p, tous les j_i sont nuls.

2.2. ÉTUDE DE Φ_K. — Pour pouvoir poursuivre plus facilement notre étude à l'aide d'invariants globaux nous supposerons en outre que $K/\mathbf{Q}$ est galoisienne. La proposition 2.1 admet alors le

COROLLAIRE. — *Si* $K/\mathbf{Q}$ *est galoisienne,* Φ_K *est le sous-groupe de* P_K *défini par*

$$\Phi_K = \{ \alpha \in P_K \mid \textit{Pour tout } i = 1, 2, \ldots, g,\ N_{K/k_i}(\alpha) \in p^{\mathbf{Z}} \}.$$

On peut alors être plus précis dans le cas particulier où les $\mathfrak{p}_i$ ont le même corps de décomposition et énoncer :

THÉORÈME 2. — *Si* K *est un corps de nombres contenant* μ_p, *galoisien sur* $\mathbf{Q}$, *et si les* $\mathfrak{p}_i$ *ont un même corps de décomposition* k, *alors* Φ_K/T_K *est un* Z*-module libre de rang* $r_2 - g + 1$ $\left(\text{resp. } r_2 - \frac{g}{2} + 1\right)$ *pour* k *réel* (resp. *imaginaire*), *facteur direct de* P_K/T_K.

Démonstration. — Il est clair que les hypothèses supplémentaires et le corollaire de la proposition 2.2, entraînent $\Phi_K = \{ \alpha \in P_K \mid N_{K/k}(\alpha) \in p^{\mathbf{Z}} \}$; il est clair également que T_K est contenu dans Φ_K. La norme réalise alors une application $\mathbf{Z}$-linéaire de P_K/T_K dans P_k/T_k. L'image de P_K/T_K est d'indice fini dans P_k/T_k. Il suffit pour le voir de remarquer que si $\beta \in P_k$, $\beta^{[K:k]} \in N_{K/k}(P_K)$. Des considérations classiques de rang d'applications $\mathbf{Z}$-linéaires (voir par exemple [3]) entraînent la première assertion. L'isomorphie de P_K/Φ_K avec $N_{K/k}(P_K/T_K)/p^{\mathbf{Z}} \cap N_{K/k}(P_K/T_K)$ montre que Φ_K est un facteur direct de P_K si et seulement si $N_{K/k}(P_K/T_K)/p^{\mathbf{Z}} \cap N_{K/k}(P_K/T_K)$ est sans torsion. Supposons que $x \in N_{K/k}(P_K/T_K)$ et $x^r \in p^{\mathbf{Z}}$ c'est-à-dire $x^r = p^r$. Alors $(x^r) = (\mathfrak{p}_{k,1}\mathfrak{p}_{k,2}\ldots\mathfrak{p}_{k,g})^r$ (on a posé $\mathfrak{p}_{k,i} = \mathfrak{p}_i \cap k$ et utilisé la propriété : k est corps de décomposition des $\mathfrak{p}_i$). Il en résulte $r = \lambda n$ dans Z, donc $x = \varepsilon p^{\lambda}$, où ε est une racine $n^{\text{ième}}$ de l'unité. $k(\zeta_1)$ est une extension cyclique de degré $p - 1$ de k et x est une norme pour $k(\zeta_1)/k$; il en résulte que pour tout $i = 1, 2, \ldots, g$: $x_{\mathfrak{p}_{k,i}}$ est norme pour $\mathbf{Q}_p(\zeta_1)/\mathbf{Q}_p$, p est également norme pour cette extension, il en est donc de même pour $\varepsilon_{\mathfrak{p}_{k,i}}$. Comme la seule racine de l'unité norme pour $\mathbf{Q}_p(\zeta_1)/\mathbf{Q}_p$ est 1, on en déduit $\varepsilon_{\mathfrak{p}_{k,i}} = 1 \Leftrightarrow \varepsilon = 1$ d'où $x = p^{\lambda}$, c'est-à-dire $x \in p^{\mathbf{Z}} \cap N_{K/k}(P_K/T_K)$.

REMARQUES :

(*a*) Dans le cas où $g = 1$ (en supposant toujours que $K/\mathbf{Q}$ est galoisienne) on voit que $\Phi_K = P_K$. Si on suppose en outre que p ne divise pas h_K alors, quel que soit n, p ne divise pas h_{K_n} (voir par exemple [17] et [21]) et les résultats de [21] montrent même que les applications $N_{n+1,n} : \Phi_{K_{n+1}} \to \Phi_{K_n}$ sont surjectives.

(*b*) Dans le cas où $g = 2$ les hypothèses du théorème 2 sont vérifiées (k, extension quadratique de $\mathbf{Q}$). On montre au passage que, si k est imaginaire, le groupe E_K des unités de K est contenu dans Φ_K.

L'éventualité où les k_i sont distincts ne peut se produire que pour $g \geqq 3$. L'exemple suivant semble indiquer que la structure de Φ_K dépend de propriétés de l'algèbre $\mathbf{Z}[\mathrm{Gal}\ K/\mathbf{Q}]$.

PROPOSITION 2.3. — *Soit* K *une extension galoisienne finie de* $\mathbf{Q}$ *vérifiant* $K \supset \mu_p$, *trois idéaux premiers* $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ *divisent* p *et les corps de décomposition respectifs* k_1, k_2, k_3 *de* $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$ *sont distincts. Désignons par* k_0 *l'extension quadratique intermédiaire de* $k/\mathbf{Q}$ $(k = k_1 k_2 k_3)$; *alors* Φ_K/T_K *est un module libre de rang* $r_2 - 2$ *ou* $r_2 - 4$ *suivant que* k_0 *est imaginaire ou pas.*

Démonstration. — Notons d'abord A_k l'ensemble des α de P_k tels que $N_{k/k_i}(\alpha) \in p^{\mathbf{Z}}$ pour $i = 1, 2, \ldots, g$. Alors la transitivité de la norme $(N_{K/k_i} = N_{k/k_i} \circ N_{K/k})$ entraîne $\Phi_K = \{\alpha \in P_K \mid N_{K/k}(\alpha) \in A_k\}$. Pour caractériser A_k dans le cas qui nous intéresse ici $(g = 3)$ notons 1, σ, σ^2 les éléments de $\mathrm{Gal}\ k/k_0$ et 1, τ les éléments de $\mathrm{Gal}\ k/k_1$. On a évidemment $\sigma\tau = \tau\sigma^{-1}$. $A_k = \{\alpha \in P_k \mid \alpha^{1+\tau} = p^{x_1}$ et $\alpha^{1+\sigma\tau\sigma^2} = p^{x_2}\}$; on en déduit que si $\alpha \in A_k$, $\alpha^{-\tau+\sigma\tau\sigma^2} = p^{x_2-x_1}$; en prenant $N_{k/k_0}(\alpha)$ il vient $x_1 = x_2$ et $\alpha^{\sigma-1} = 1$, ce qui entraîne $\alpha \in P_{k_0}^+$, avec $P_{k_0}^+$ formé des éléments de P_{k_0} de norme positive; réciproquement $P_{k_0}^+ \subset A_k$, d'où $A_k = P_{k_0}^+ A_k/T_k$ est donc un $\mathbf{Z}$-module libre de rang 1 ou 2 suivant que k_0 est imaginaire ou pas (un seul idéal premier au-dessus de p dans k_0). La démonstration s'achève alors par des considérations de rang analogues à celles qui ont été utilisées pour le théorème 2.

2.3. ÉTUDE DE Ψ_K. — On notera H_K le sous-groupe de K^* formé des α tels que $K(\alpha^{1/p})/K$ soit non ramifiée en dehors de p. La démonstration de la proposition 1.2 nous a prouvé que $\Psi_K \subset H_K$. Nous allons évaluer $\dim_{F_p} H_K/K^{*p}$ à l'aide de certains invariants de K. On en déduira une majoration évidente de $s_K + t_K = \dim_{F_p} \Psi_K/K^{*p}$.

Notons $\mathfrak{H}$ le p-groupe des classes de K et $\mathfrak{H}_0$ le p-sous-groupe de $\mathfrak{H}$ formé des classes d'idéaux engendrées par des idéaux de la forme $\mathfrak{p}_1^{n_1} \ldots \mathfrak{p}_g^{n_g}$ ($n_1, n_2, \ldots, n_g$ entiers relatifs).

Notons r le rang de $\mathfrak{H}/\mathfrak{H}_0$, c'est-à-dire le nombre de facteurs dans une décomposition de $\mathfrak{H}/\mathfrak{H}_0$ en produit de groupes cycliques.

PROPOSITION 2.4 :

$$\dim_{F_p} H_K/K^{*p} = r_2 + g + r.$$

Démonstration. — D'après la théorie de Kummer on peut écrire pour tout α de H : $(\alpha) = \mathfrak{N}^p \mathfrak{B}$ où $\mathfrak{N}$ et $\mathfrak{B}$ sont des idéaux de K avec $\mathfrak{N}$ premier à p et $\mathfrak{B}_\lambda$ produit d'idéaux premiers au-dessus de p. Soit λ dans K^*; on peut écrire de manière unique $(\lambda) = \mathfrak{N}_\lambda \mathfrak{B}_\lambda$ avec $\mathfrak{N}_\lambda$ premier à p, $\mathfrak{B}_\lambda$

produit d'idéaux au-dessus de p. Il en résulte $(\lambda^p \alpha) = (\mathfrak{N}_\lambda \mathfrak{N})^p \mathfrak{B}_\lambda'' \mathfrak{B}$ et $\mathrm{Cl}\,\mathfrak{N}_\lambda \mathfrak{N} = \mathrm{Cl}\,\mathfrak{N} \bmod \mathfrak{H}_0$. On définit aisinsi un homomorphisme de H/K^{*p} dans $\mathfrak{H}/\mathfrak{H}_0$; il est clair que l'image de H/K^{*p} par cet homomorphisme est formé d'éléments de $\mathfrak{H}/\mathfrak{H}_0$ annulés par p. Notons $(\mathfrak{H}/\mathfrak{H}_0)_p$ l'ensemble des éléments de $\mathfrak{H}/\mathfrak{H}_0$ annulés par p. Il est alors facile de voir que la suite

$$0 \to P_K\, K^{*p}/K^{*p} \to H/K^{*p} \to (\mathfrak{H}/\mathfrak{H}_0)_p \to 0$$

est exacte; elle est même scindée puisqu'il s'agit d'espaces vectoriels sur F_p. Le lemme résulte alors des égalités

$$\dim_{F_p} (\mathfrak{H}/\mathfrak{H}_0)_p = r \qquad \text{et} \qquad \dim_{F_p} P_K\, K^{*p}/K^{*p} = r_2 + g.$$

Corollaire :

$$s_K + t_K \leq r_2 + g + r.$$

Les résultats ci-dessus ont été déduits de l'inclusion : $\Psi_K \subset H_K$. Lorsque $r = 0$ on remarque que l'on a de plus : $\Psi_K \subset H_K = P_K\, K^{*p}$. La détermination de $\dim_{F_p} \Psi_K/K^{*p} = \dim_{F_p} (\Psi_K \cap P_K/P_K^p)$ se ramène alors à un problème sur les p-unités. Si p ne divise pas h_K, on obtient le résultat suivant :

Proposition 2.5. — *Si* $K/\mathbb{Q}$ *est galoisienne et si* p *ne divise pas* h_K, $\Psi_K \cap P_K$ *est le sous-groupe de* P_K *formé des* p*-unités qui sont des normes pour* K_{m+1}/K.

Démonstration. — Dans ce cas les j_i sont nuls, la proposition 2.2 montre qu'alors

$$\Psi_K \cap P_K = \{\, \alpha \in P_K \mid \text{Pour tout } i = 1, 2, \ldots, g,\ N_{K\mathfrak{P}_i/\mathbb{Q}}(\alpha) \in p^{\mathbb{Z}}\, U^{(m+1)} \,\};$$

le théorème de Hasse entraîne

$$\Psi_K \cap P_K = N_{m+1}(K_{m+1}^*) \cap P_K.$$

Remarques :

(*a*) Si on suppose simplement que les j_i sont tous nuls on voit facilement que $\Psi_K = H_K \cap N_{m+1}(K_{m+1}^*)$.

(*b*) Les résultats de ce paragraphe 2.3 peuvent se généraliser de la façon suivante, lorsque $m > 1$: $(1 \leq i \leq m)$. On note

$$H_K^{(i)} = \{\, \alpha \in K^* \mid K(\alpha^{p^{m-i}})/K \text{ est non ramifiée en dehors de } p \,\}.$$

On montre $\Psi_K^{(i)} \subset H_K^{(i)}$.

En notant $r^{(i)}(G)$ le p^i-rang d'un p-groupe abélien fini G (c'est-à-dire le nombre de composantes cycliques d'ordre $\geq p^i$ dans une décomposition

de G en produit), on trouve

$$r^{(i)}(\mathrm{H}_{\mathrm{K}}^{(i)}/\mathrm{K}^{*p^i}) = r_2 + g + r^{(i)}(\mathfrak{H}/\mathfrak{H}_0),$$

ce qui généralise la proposition 2.5.

On en déduit l'inégalité

$$s_{\mathrm{K}} \leq r_2 + g + r^{(m)}(\mathfrak{H}/\mathfrak{H}_0).$$

2.4 Le cas $g = 1$. — On note $\mathfrak{p}$ (au lieu de $\mathfrak{p}_1$) l'idéal premier de K qui divise p, et j (au lieu de j_1) l'entier défini au paragraphe 2.1.

Théorème 3. — *Soit* K *un corps de nombres contenant* μ_p *et pour lequel* $g = 1$ *et* $r = 0$ (*notations du paragraphe* 2.3). *Alors la conjecture de Leopoldt est vraie pour le couple* (K, p). *De plus on a les égalités*

$$\Theta_{\mathrm{K}} = \Psi_{\mathrm{K}} = \mathrm{H}_{\mathrm{K}} = \mathrm{P}_{\mathrm{K}}\,\mathrm{K}^{*p}.$$

Démonstration. — La proposition 2.5 entraîne : $\dim_{\mathbf{F}_p}(\mathrm{H}_{\mathrm{K}}/\mathrm{K}^{*p}) = r_2 + 1$. D'où, puisque $\Theta_{\mathrm{K}} \subset \Psi_{\mathrm{K}} \subset \mathrm{H}_{\mathrm{K}}$, l'égalité $\Theta_{\mathrm{K}} = \Psi_{\mathrm{K}} = \mathrm{H}_{\mathrm{K}}$. D'autre part, on a l'inclusion $\mathrm{P}_{\mathrm{K}}\mathrm{K}^{*p} \subset \mathrm{H}_{\mathrm{K}}$; l'égalité résulte de l'égalité des dimensions sur $\mathbf{F}_p$.

Remarques.

(*a*) Lorsque $m > 1$, le théorème 3 a la généralisation suivante [*cf.* remarque (*b*), § 2.3] : soit K un corps de nombres tel que $g = 1$ et $r^{(m)}(\mathfrak{H}/\mathfrak{H}_0) = 0$. La conjecture de Leopoldt est vraie pour le couple (K, p) et on a

$$r^{(m)}(\Theta_{\mathrm{K}}^{(m)}/\mathrm{K}^{*p^m}) = r^{(m)}(\Psi_{\mathrm{K}}^{(m)}/\mathrm{K}^{*p^m}) = r^{(m)}(\mathrm{H}_{\mathrm{K}}^{(m)}/\mathrm{K}^{*p^m}) = r_2 + 1.$$

(*b*) G. Gras et M. Waldschmidt ont obtenu des démonstrations indépendantes de la conjecture de Leopoldt pour un corps K vérifiant des conditions analogues à celles du théorème 3.

Exemple. — Le théorème 3 donne de nouveaux exemples de corps où la conjecture de Leopoldt est vérifiée. C'est ainsi que le corps $\mathrm{K} = \mathbf{Q}(\zeta_1,\ 1 + p_1(1 - \zeta_1)^{1/p})$, avec $p = 5$, vérifie les hypothèses du théorème 3 sans satisfaire aux conditions de Brumer.

On peut avoir égalité des groupes Ψ_{K} et H_{K} avec d'autres hypothèses :

Proposition 2.6. — *Soit* K *un corps de nombres contenant* μ_p, *galoisien sur* $\mathbf{Q}$, *et pour lequel* $g = 1$ *et* $j = 0$. *On a l'égalité* $\Psi_{\mathrm{K}} = \mathrm{H}_{\mathrm{K}}$.

Démonstration. — Soit $\alpha \in \mathrm{H}_{\mathrm{K}}$, écrivons encore $(\alpha) = \mathfrak{N}^p\mathfrak{B}$ avec $\mathfrak{N}$ premier à p et $\mathfrak{B}$ est une puissance de $\mathfrak{p}$. Prenons la norme relativement

à $\mathbf{Q}(\zeta_m)$; on obtient $(N_{K/\mathbf{Q}(\zeta_m)}(\alpha)) = \mathfrak{N}'^p (1-\zeta_m)^x$ avec $\mathfrak{N}'$ idéal de $\mathbf{Q}(\zeta_m)$ premier avec p. Prenons alors la norme relativement à $\mathbf{Q}$,

$$N_{K/\mathbf{Q}}(\alpha) = p^x \left[N_{\mathbf{Q}(\zeta_m)/\mathbf{Q}}\, \mathfrak{N}'\right]^p.$$

On sait (voir par exemple [6], chap. VII) que $N_{\mathbf{Q}(\zeta_m)/\mathbf{Q}}\, \mathfrak{N}' \equiv 1\ (p^m)$ compte tenu de $N_{K/\mathbf{Q}}(\alpha) = N_{K_\mathfrak{p}/\mathbf{Q}_p}(\alpha_\mathfrak{p})$ on obtient $N_{K_\mathfrak{p}/\mathbf{Q}}(\alpha_\mathfrak{p}) \in p^{\mathbf{Z}}\, U^{(m+1)}$ d'où le résultat annoncé d'après la proposition 2.2.

EXEMPLES DE CORPS K VÉRIFIANT $\Theta_K \neq \Psi_K$.

— (1) Soit

$$K = \mathbf{Q}(\sqrt{-3}, \sqrt{83}) \text{ et } p = 3 \quad \text{(exemple dû à J.-P. Serre).}$$

On voit que $g = 1$, $\mathfrak{H}_0 = \{1\}$, $r = 1$ et $j = 0$.

Les résultats précédents montrent que $\Psi_K = H_K$ et $\dim_{\mathbf{F}_3} H_K/H^{*3} = 4$. Comme $K/\mathbf{Q}$ est abélienne, on sait (*cf.* [4]) que $\dim_{\mathbf{F}_3} \Theta_K/K^{*3} = 3$. D'où $\Theta_K \neq \Psi_K$. Un calcul direct montre que $\Theta_K = P_K K^{*3}$.

(2) Soit $K = \mathbf{Q}(\zeta_m)$ et p un nombre premier irrégulier. Les résultats précédents montrent que $\Psi_K = H_K$ et $\dim_{\mathbf{F}_p} H_K/K^{*p} = r_2 + 1 + r$. L'extension $K/\mathbf{Q}$ étant abélienne, $\dim_{\mathbf{F}_p} \Theta_K/K^{*p} = r_2 + 1$. D'où $\Theta_K \neq \Psi_K$. On peut se demander si $\Theta_K = P_K K^{*p}$; la réponse est donnée, dans le cas p proprement irrégulier, par le résultat suivant :

PROPOSITION 2.7. — *Soit* $K = \mathbf{Q}(\zeta_m)$ *et soit* p *un nombre premier régulier ou proprement irrégulier. On a l'égalité* $\Theta_K = P_K K^{*p}$.

Démonstration. — Si p est régulier, l'égalité est démontrée dans le théorème 3. Si p est proprement irrégulier, on sait (voir par exemple [13]) que les applications $N_{n+1,n} : \Phi_{K_{n+1}} \to \Phi_{K_n}$ sont surjectives. La proposition 1.3 montre que $\Phi_K K^{*p} \subset \Theta_K$; comme $\Phi_K = P_K$ [remarque (*a*), § 2.2], on a $P_K K^{*p} \subset \Theta_K$. Or l'extension $K/\mathbf{Q}$ étant abélienne $\dim_{\mathbf{F}_p} \Theta_K/K^{*p} = r_2 + 1$ ([4]). Comme $\dim_{\mathbf{F}_p} P_K K^{*p}/K^{*p} = r_2 + 1$, on a $P_K K^{*p} = \Theta_K$.

2.5. LE CAS $g = 2$ ET p NE DIVISE PAS h_K. — On suppose encore K galoisienne sur $\mathbf{Q}$ et on note $\mathfrak{p}$ et $\mathfrak{p}'$ (au lieu de $\mathfrak{p}_1$ et $\mathfrak{p}_2$) les idéaux premiers de K au-dessus de $\mathfrak{p}$. Pour toute extension intermédiaire L de K/Q on pose $\mathfrak{p}_L = \mathfrak{p} \cap L$ et on désigne par E_L le groupe des unités de L. On note η_k (resp. η_k') un générateur de l'idéal principal $\mathfrak{p}_k^{h_k}$ (resp. $\mathfrak{p}_k'^{h_k}$), où h_k est le nombre de classes d'idéaux de k. Enfin C désignera le p-corps de classes de k, c'est-à-dire la p-extension abélienne non ramifiée maximale de k.

2.5.1. Le résultat suivant concernant la structure de K nous servira considérablement.

THÉORÈME 4. — *Soit* K *un corps de nombres vérifiant les hypothèses ci-dessus, alors* $\mathfrak{p}$ *et* $\mathfrak{p}'$ *admettent le même* p-corps *d'inertie* T *et* T = C. *En outre, si* k *est imaginaire,* $m = 1$.

Démonstration. — Notons provisoirement $T_{\mathfrak{p}}$ et $T_{\mathfrak{p}'}$ les p-corps d'inertie respectifs de $\mathfrak{p}$ et $\mathfrak{p}'$ pour l'extension K/k, c'est-à-dire les p-extensions intermédiaires maximales où $\mathfrak{p}_k$ et $\mathfrak{p}'_k$ sont inertes. $K/T_{\mathfrak{p}}$ est résoluble et la définition de $T_{\mathfrak{p}}$ entraîne que $K/T_{\mathfrak{p}}$ est une tour d'extensions intermédiaires cycliques, les étages de degré p étant ramifiés en $\mathfrak{p}$, il en résulte que si p divisait $h_{T_{\mathfrak{p}}}$ il diviserait également h_K (voir par exemple [21]), ce qui est exclu par hypothèse. Il en résulte $C \subset T_{\mathfrak{p}} \cap T_{\mathfrak{p}'}$, (sinon on en déduirait par composition l'existence d'une p-extension abélienne non ramifiée et non triviale de $T_{\mathfrak{p}}$).

Montrons d'abord que $m = 1$ si k est imaginaire. Notons Λ l'extension intermédiaire de k_2/k de degré p sur k. Considérons l'extension cyclique $C\Lambda/C$; les unités de C sont des normes car leur norme relativement à k

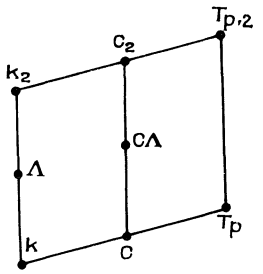

Fig. 1

est une norme pour Λ/k. La formule donnant le nombre $a_{C\Lambda/C}$ des classes ambiges pour $C\Lambda/C$ (voir par exemple [6], chap. IV) s'écrit alors : $a_{C\Lambda/C} = h_C \dfrac{p^2}{p} = p h_C$. Par suite, p divise $h_{C\Lambda}$ donc divise h_{C_2} (le degré de $C_2/C\Lambda$ est premier à p) et divise alors $h_{T_{\mathfrak{p}',2}}$ (car ou bien $T_{\mathfrak{p}',2} = C_2$ ou bien $T_{\mathfrak{p}',2}/C_2$ ramifiée). Cette dernière propriété est incompatible avec $K \supset \mu_{p^2}$ (qui équivaut à $K \supset T_{\mathfrak{p}',2}$) puisque p ne divise pas h_K.

Revenons maintenant à la démonstration de l'égalité $T_{\mathfrak{p}} = T_{\mathfrak{p}'} = C$. Si $T_{\mathfrak{p}}$ diffère de C il existe une extension intermédiaire L de $T_{\mathfrak{p}}/C$ avec $[L : C] = p$ [et aussi L' intermédiaire de $T_{\mathfrak{p}'}/C$ avec $(L' : C] = p$]. Comme $T_{\mathfrak{p}}/k$ est cyclique il en est de même pour L/k (et aussi pour L'/k).

Posons alors $[C : k] = p^\nu$, la formule donnant le nombre $a_{L/K}$ de classes ambiges pour L/k s'écrit :

$$a_{L/k} = h_k \frac{p^t}{p^{\nu+1}[E_k : E_k \cap N_{L/k}(L^*)]},$$

où i est le nombre d'idéaux premiers de k ramifiés dans L/k (c'est-à-dire dans L/C). Si on pose $h_k = h'_k . p^\nu$ avec h'_k premier à p cette formule s'écrit :

$$a_{L/k} = h'_k \frac{p^{i-1}}{[E_k : E_k \cap N_{L/k}(L^*)]}.$$

Si k est imaginaire, E_k est d'ordre premier à p et i est nécessairement égal à 1. Si k est réel, $E_k \cap N_{L/k}(L^*)$ contient E_k^p; en effet C/k étant non ramifiée, $E_k \subset N_{C/k} C^*$ (*voir* [21]); il en résulte que la participation de p à l'indice figurant au dénominateur est 1 ou p. Ce qui entraîne $i = 1$ ou $i = 2$.

Nous utiliserons le

LEMME 1. — *Soit L/k une extension cyclique de degré p de corps de nombres, et soit $\mathfrak{q}$ un idéal premier de k ne divisant pas p et qui se ramifie dans L. Posons $N_{K/\mathbb{Q}}(\mathfrak{q}) = q^f$ avec q premier; alors p divise $q^f - 1$.*

Démonstration. — En localisant en $\mathfrak{q}$, on voit que $L_\mathfrak{q}/k_\mathfrak{q}$ est cyclique et que l'indice de ramification de $\mathfrak{q}$ est égal à p. La théorie du corps de classes local montre que le sous-groupe de $U_\mathfrak{q}$ formé des unités normes pour $L_\mathfrak{q}/k_\mathfrak{q}$ est d'indice p. Il en résulte bien p divise $q^f - 1$.

Nous allons maintenant travailler dans l'extension L_1/k_1. On sait (*voir* [6], chap. IX) que les unités u de k_1 vérifiant $N_{k_1/k}(u)$ est une norme pour L/k sont des normes pour L_1/k_1 (*voir* [6], chap. IX). Les racines de l'unité de k_1 ont une norme relativement à k égale à 1, ce sont donc des normes

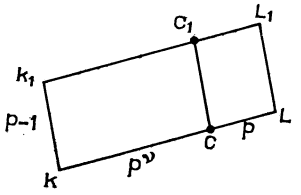

Fig. 2

pour L_1/k_1. En considérant l'application $\mathbf{Z}$-linéaire $N_{k_1/k} : E_{k_1}/T_{k_1} \to E_k$ on voit qu'on peut trouver, si k est réel, un système d'unités fondamentales de E_{k_1} tel que $p - 3$ d'entre elles soient de norme 1 relativement à k. Ce qui entraîne $[E_{k_1} : E_{k_1} \cap N_{L_1/k_1}(L_1^*)] = 1$ ou p. Si k est imaginaire :

$$N_{k_1/k}(E_{k_1}) = 1 \qquad \text{et} \qquad [E_{k_1} : E_{k_1} \cap N_{L_1/k_1}(L_1^*)] = 1.$$

Soit j le nombre d'idéaux premiers de k, ramifiés dans L_1/k_1. La formule donnant le nombre de classes ambiges de L_1/k_1 s'écrit :

$$a_{L_1/k_1} = h_{k_1} \frac{p^j}{p^{\nu+1}[E_{k_1} : E_{k_1} \cap N_{L_1/k_1}(L_1^*)]}$$
$$= h'_{k_1} \frac{p^{j-1}}{[E_{k_1} : E_{k_1} \cap N_{L_1/k_1}(L_1^*)]},$$

où on a posé $h_{k_1} = p^\nu h'_{k_1}$ (h'_{k_1} entier).

Les idéaux premiers de k_1 ramifiés dans L_1/k_1 sont les diviseurs dans k_1 des idéaux de k ramifiés dans L/k.

Si $i = 2$ et si les idéaux $\mathfrak{q}_1$ et $\mathfrak{q}_2$ de k qui se ramifient dans L/k ne divisent pas p, chacun possède $p - 1$ diviseurs idéaux premiers dans k_1 (d'après le lemme 1, p divise $q^f - 1$); d'où $j = 2(p-1)$, $j - 1 = 2p - 3$ et il en résulterait p^{2p-4} divise a_{L_1/k_1} donc h_L, ce que l'hypothèse $p \nmid h_K$ exclut.

Si $i = 2$ et si un des idéaux qui se ramifient dans L/k divise p alors $j = p$, $j - 1 = p - 1$ et p^{p-2} divise a_{L_1/k_1} ce qui donne la même contradiction.

Si $i = 1$, la formule donnant $a_{L/k}$ montre que p ne divise pas $[E_k : E_k \cap N_{L/k}(L^*)]$ d'où résulte $[E_{k_1} : E_{k_1} \cap N_{L_1/k_1}(L_1^*)] = 1$. Si l'idéal de k qui se ramifie dans L/k est distinct de $\mathfrak{p}'_k$, on a $j = p - 1, j - 1 = p - 2$ et p divise a_{L_1/k_1} ce qui est exclu .

Il reste à examiner l'éventualité où $\mathfrak{p}'_k$ serait le seul idéal de k ramifié dans L/k. Le corps k possède au plus une extension L abélienne non ramifiée en dehors de $\mathfrak{p}'_k$ de degré $p^{\nu+1}$ sur k et telle que l'indice de ramification $e_{\mathfrak{p}'_k}$ soit égal à p. Cette extension contient évidemment C. Pour le voir, remarquons que le groupe $U_{\mathfrak{p}'_k}$ des unités de $k_{\mathfrak{p}'_k}$ est isomorphe à $\mathbf{Z}/(p-1)\mathbf{Z} \oplus \mathbf{Z}_p$, il possède un seul sous-groupe d'indice p, à savoir $U^*_{\mathfrak{p}'_k} = V.U^{(2)}_{\mathfrak{p}'_k}$ où V désigne le groupe des racines de l'unité de $\mathbf{Q}_p$ et $U^{(2)}_{\mathfrak{p}'_k}$ le groupe des unités qui sont congrues à 1 modulo p^2. La théorie du corps de classes montre que L existe ou non suivant que l'indice

$$\left[k^* \prod_{\mathfrak{q}} k^*_{\infty_i} \times \prod_{\mathfrak{q}} U_{\mathfrak{q}} : k^* \prod_{\mathfrak{q}} k^*_{\infty_i} \times U^*_{\mathfrak{p}'_k} \times \prod_{\mathfrak{q} \neq \mathfrak{q}'_k} U_{\mathfrak{q}}\right]$$

est égal à p ou à 1. On voit facilement que cet indice est égal à p si toutes les unités de k sont dans $U^*_{\mathfrak{p}'_k}$ et à 1 dans le cas contraire.

Si k est imaginaire, $E_k \subset U^*_{\mathfrak{p}'_k}$ et L existe. Posons $L' = \tau L$ (où τ désigne un $\mathbf{Q}$-isomorphisme de L dont la restriction à k n'est pas l'identité). Si $K \supset L$ alors $K \supset LL'$ et on voit encore par la théorie du corps de classes global que LL' contient l'extension Λ cyclique de degré p de k vérifiant $\Lambda \subset k_2$.

Il en résulte $K \supset k_2$ ce qui contredit la propriété $m = 1$, d'où la validité du théorème pour k imaginaire.

Il nous reste à examiner l'éventualité k réel. Le lemme suivant prouve que l'unité fondamentale ε de k n'appartient pas à $U^*_{\mathfrak{p}'_k}$; il n'existe donc pas d'extension L où $\mathfrak{p}'_k$ est le seul idéal ramifié, ce qui démontre le théorème pour k réel.

LEMME 2. — *Soient k un corps quadratique réel, ε une unité fondamentale de k, C le p-corps de classes de k et $C_1 = C(\zeta_1)$. On suppose que p est divisible par deux idéaux premiers $\mathfrak{p}_k$ et $\mathfrak{p}'_k$ dans k et que p ne divise pas h_{C_1}, alors $\varepsilon^{p-1} \equiv 1 \bmod \mathfrak{p}'_k$ et $\varepsilon^{p-1} \not\equiv 1 \bmod \mathfrak{p}'^2_k$.*

Démonstration. — Si $\varepsilon^{p-1} \equiv 1\ (\mathfrak{p}_k^2)$ on a dans C_1, $\varepsilon^{p-1} \equiv 1\ (\mathfrak{p}_{C_1}^{2(p-1)})$. La théorie de Kummer montre (*voir* [7], I, § 11) que ou bien ε est une puissance $p^{\text{ième}}$ dans C_1, ou bien l'extension $C_1\left(\varepsilon^{\frac{p-1}{p}}\right)/C_1$ est de degré p non ramifiée. La première éventualité est à exclure car $k_1(\varepsilon^{p-1})/k_1$ n'est pas abélienne (voir par exemple [8] ou [19]). Comme p ne divise pas h_{C_1}, la seconde est exclue, d'où le lemme.

REMARQUE. — On a vu au cours de la démonstration du théorème 3 que p pouvait diviser h_k (voir les exemples donnés un peu plus loin). Nous savons que dans ce cas le p-groupe des classes de k est cyclique (puisque C/k est cyclique) et même que $\mathrm{Cl}\,\mathfrak{p}_k$ engendre ce p-groupe puisque $\mathfrak{p}_k$ est inerte dans C/k (voir par exemple [6], chap. VI, théorème A).

2.5.2. Nous sommes alors en mesure d'énoncer :

THÉORÈME 5. — *Soit K un corps de nombres vérifiant :*

(a) K/Q galoisienne et $K \supset \mu_p$;

(b) p ne divise pas h_K;

(c) deux idéaux premiers $\mathfrak{p}$ et $\mathfrak{p}'$ de K divisent p;

(d) le corps de décomposition k de $\mathfrak{p}$ et $\mathfrak{p}'$ est imaginaire.

Alors,

$$\dim_{F_p} \Psi_K/K^{*p} = \begin{cases} r_2 + 1 & \text{si } \eta^{p-1} \not\equiv 1\ (\mathfrak{p}'^2_k), \\ r_2 + 2 & \text{si } \eta^{p-1} \equiv 1\ (\mathfrak{p}'^2_k). \end{cases}$$

(η désigne toujours un générateur de $\mathfrak{p}_k^{h_k}$.)

Démonstration. — On sait grâce à la proposition 2.6 que

$$\dim_{F_p} \Psi_K/K^{*p} = \dim_{F_p} (P_K \cap N_{K_2/K}(K_2^*)/P_K^{*p}) \qquad (k \text{ imaginaire entraîne } m = 1).$$

La remarque (*b*) du paragraphe 2.2 montre que $E_K \subset N_{K_2/K}(K_2^*)$; on aura donc $\dim_{F_p} \Psi_K/K^{*p} = r_2 + 1$ suivant qu'il existe ou non une p-unité

de K qui n'est pas une norme pour K_2/K. Cela équivaut comme on le voit facilement à $\gamma_{|K}$ (où $\gamma_{|K}$ est un générateur de $\mathfrak{p}^{h_K}$) n'est pas une norme pour K_2/K. En utilisant les notations du théorème 4, on voit que

$$N_{K/k}(\mathfrak{p}_K) = \mathfrak{p}_k^{p^\nu f_0} \quad \text{avec} \quad p^\nu = [C : k] \quad \text{et} \quad f = p^\nu f_0 \text{ degré de } \mathfrak{p}.$$

Ce qui entraîne $N_{K/k}(\mathfrak{p}_K^{h'_k}) = \mathfrak{p}_k^{f_0 h_k}$ d'où $N_{K/k}(\gamma_{|K}^{h'_k}) = u\,\gamma_{|}^{f_0 h_K}$, u étant une unité de k et $f_0 h_K$ un entier premier à p. Désignons encore par Λ l'extension intermédiaire de k_2/k de degré p sur k. $\gamma_{|K}$ est une norme pour K_2/K si et seulement si $N_{K/k}(\gamma_{|K})$ est une norme pour Λ/k; c'est une conséquence du théorème de Hasse et du théorème B. Nous connaissons bien par ailleurs les éléments α de k premiers à $\mathfrak{p}'_k$ normes pour Λ/k; ils vérifient $\alpha^{p-1} \equiv 1\ (\mathfrak{p}_k'^2)$, d'où le théorème.

Corollaire. — *Si sous les hypothèses du théorème* 5, $\gamma_{|}^{p-1} \not\equiv 1\ (\mathfrak{p}_k'^2)$ *alors* $Y_K = Z_K$ *et la conjecture de Leopoldt est vraie pour le couple* (p, K).

2.5.3. Le résultat suivant concerne le cas où k est réel; il est moins satisfaisant.

Proposition 2.8. — *Soit* K *un corps de nombres vérifiant :*

(*a*) $K/\mathbb{Q}$ *est galoisienne* $K \supset \mu_{p^m}$ *et* $K \not\supset \mu_{p^{m+1}}$;

(*b*) p *ne divise pas* h_K;

(*c*) *deux idéaux premiers* $\mathfrak{p}$ *et* $\mathfrak{p}'$ *de* K *divisent* p;

(*d*) *le corps de décomposition* k *de* $\mathfrak{p}$ *et* $\mathfrak{p}'$ *est réel*;

(*e*) p^m *ne divise pas l'indice de ramification* e *de* $\mathfrak{p}$ *et* $\mathfrak{p}'$.

Alors, $\dim \Psi_K/K^{*p} = r_2 + 1$ *et la conjecture de Leopoldt est vérifiée pour le couple* (p, K).

Démonstration. — La proposition 2.2 montre que le groupe

$$E_K \cap N_{K_{m+1}/K}(K^*_{m+1})$$

est formé des unités u de K vérifiant $N_{K/k}(u) \equiv 1\ (\mathfrak{p}_k^{m+1})$. Il contient donc en particulier les unités de norme 1 relativement à k. Montrons que ces dernières forment un groupe produit de T_K par un Z-module libre de rang $r_2 - 2$ facteur direct de E_K; autrement dit on peut trouver un système $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r_2-1})$ d'unités fondamentales de K telles que $N_{K/k}(\varepsilon_1) = \varepsilon_k^x$ (ε_k unité fondamentale de k, x entier $\neq 0$) et $T_K \times \varepsilon_2^Z \times \varepsilon_3^Z \ldots \varepsilon_{r_2-1}^Z$ est le sous-groupe des unités de K de norme 1 relativement à k.

En effet, on sait que $T_K \subset \Phi_K$, d'où $N_{K/k}(T_K) = 1$. Par ailleurs, $E_k \supset N_{K/k} E_K \supset E_k^{r_2}$, $N_{K/k}(E_K)$ est donc un sous-groupe de E_k d'indice fini; donc $N_{K/k}(E_K)$ est isomorphe à Z. On en déduit que le noyau de $N_{K/k}$

dans E_K/T_K est un Z-module libre de rang $r_2 - 2$ qui est facteur direct de E_K/T_K (puisque le quotient est sans torsion). D'où le résultat annoncé. Il en résulte $[E_K : E_K \cap N_{K_{m+1}/K} K^*_{m+1}] = 1$ ou p. Si l'indice est égal à p, il existe une unité de K, ε_1 qui n'est pas une norme pour K_{m+1}/K, d'où

$$\dim_{F_p} (\Psi_K/K^{*p}) = r_2 + 1.$$

Nous allons montrer que c'est le cas si le corps K vérifie les hypothèses de la proposition.

Supposons en effet que $N_{K/k_1}(\varepsilon_1) \equiv 1 (\mathfrak{p}_k^{m+1})$, nous avons vu au lemme 2 du paragraphe 2.5.1 que $\varepsilon_k^{p-1} \not\equiv 1 (\mathfrak{p}_k^2)$, cela entraîne, en utilisant la structure du groupe des unités distinguées de $\mathbf{Q}_p$, $N_{K/k}(\varepsilon_1) = \varepsilon_k^x$ avec p^m divise x. On aurait donc en posant $x = x_0 p^m$:

$$N_{K/k}(E_K) \subset E_k^{x_0 p^m}.$$

Posons $e_0 = [K : T_m]$ où T est le corps d'inertie de $\mathfrak{p}_k$ et $T_m = T(\zeta_m)$; la condition (e) entraîne e_0 premier à p. Soit $f_0 = [T : C]$; le théorème 4 montre que f_0 est premier à p. Il en résulte $N_{K/C}(E_K) \supset E_C^{e_0 f_0 p^{m-1}}$. Comme C/k est non ramifiée on sait (*voir* [21]) que $E_k = N_{C/k}(E_C)$, d'où

$$N_{K/k}(E_K) \supset E_k^{e_0 f_0 p^{m-1}}.$$

Si $N_{K/k}(E_K) \subset E_k^{x_0 p^m}$, on a l'inclusion $E_k^{e_0 f_0 p^{m-1}} \subset E_k^{x_0 p^m}$, qui est impossible puisque $e_0 f_0$ est premier à p.

REMARQUE. — Il est vraisemblable que (e) n'est pas une conséquence de (a), (b), (c) et (d). Cependant si $K/\mathbf{Q}$ est abélienne et si (a), (b), (c) et (d) sont vérifiées il est clair que (e) est vérifiée. En effet, si $K/\mathbf{Q}$ est abélienne, il ne peut y avoir d'extension intermédiaire L de K/C_m avec $[L : C_m] = p$. Si L/C_m est non ramifiée en dehors de p on montre en utilisant la structure de J_k et le lemme 2 du paragraphe 2.5.1 que $L = C_{m+1}$ ce qui est exclu. Si L/C_m est ramifiée en dehors de p, il y a au moins trois idéaux premiers de C_m ramifiés dans L/C_m et on montre, en utilisant encore la formule donnant le nombre de p-classes ambiges, soit dans L/k si elle est cyclique, soit dans L'/k si $L = C_m L'$, que p divise h_L ce qui est exclu par (b).

2.5.4. EXEMPLES. — Nous utiliserons à plusieurs reprises le résultat suivant (rappelé dans [15]) : si k est un corps de nombres dont le p-groupe des classes est cyclique d'ordre p, la p-tour des corps de classes de k est de longueur 1. Cela revient à dire que si C est le p-corps de classes de k, p ne divise pas h_C.

Nous allons essayer de construire des exemples illustrant le théorème 5. Il est naturel de commencer par $p = 3$. On prend donc $k = \mathbf{Q}(\sqrt{m})$ (m désigne ici un entier « quadratfrei ») avec $m < 0$ et $\left(\frac{m}{3}\right) = 1$, on écrit encore $(3) = \mathfrak{p}_k \mathfrak{p}'_k$ et on supposera que si 3 divise h_k, $\mathrm{Cl}\,\mathfrak{p}_k$ engendre le 3-groupe des classes de k supposé d'ordre 3. Remarquons d'abord que si 3 divise $h_{\mathbf{Q}(\sqrt{-3m})}$, le 3-groupe des classes de $\mathbf{Q}(\sqrt{-3}, \sqrt{m})$ n'est pas cyclique et que le résultat de [15] ne s'appliquera pas. En effet, le 3-groupe des classes de $\mathbf{Q}(\sqrt{-3}, \sqrt{m})$ est produit direct des 3-groupes des classes de $\mathbf{Q}(\sqrt{m})$ et $\mathbf{Q}(\sqrt{-3m})$ (*voir* par exemple [16]) et le théorème de dualité de Scholz-Leopoldt montre que si 3 divise $h_{\mathbf{Q}(\sqrt{-3m})}$, alors 3 divise $h_{\mathbf{Q}(\sqrt{m})}$.

Les tables numériques donnent de nombreuses valeurs de m « favorables ».

Exemple 1 :

(*a*) $m = -2, -5, -11, -14, -17, -35$ avec 3 ne divise pas h_k, on prendra $\mathrm{K} = \mathbf{Q}(\sqrt{-3}, \sqrt{m})$.

(*b*) $m = -23, -26, -38, -53, -59$. Le 3-groupe des classes de k est cyclique d'ordre 3 et engendré par $\mathrm{Cl}\,\mathfrak{p}_k$ et 3 ne divise pas $h_{\mathbf{Q}(\sqrt{-3m})}$. On prendra alors pour K le 3-corps de classes de $\mathbf{Q}(\sqrt{-3}, \sqrt{m})$.

Les exemples (*a*) donnent tous $\eta_1^2 \not\equiv 1\ (\mathfrak{p}_k'^2)$. Les exemples (*b*) donnent tous également $\eta_1^2 \not\equiv 1\ (\mathfrak{p}_k'^2)$. Cette dernière propriété est une conséquence de la remarque suivante :

Remarque. — Si $p = 3$, si $\mathrm{Cl}\,\mathfrak{p}_k$ engendre le 3-groupe des classes de $\mathbf{Q}(\sqrt{m})$ supposé non trivial, on voit en considérant l'extension $\mathbf{Q}(\sqrt{-3}, \sqrt{m})(\eta_1^{1/3})$ que 3 divise $h_{\mathbf{Q}(\sqrt{-3m})}$ si et seulement si $\eta_1^2 \equiv 1\ (\mathfrak{p}_k'^2)$. Cela prouve que si $\eta_1^2 \equiv 1\ (\mathfrak{p}_k'^2)$ le 3-groupe des classes de $\mathbf{Q}(\sqrt{-3}, \sqrt{m})$ n'est pas cyclique. (Exemple $m = -107$.)

Pour les exemples 1, la conjecture de Leopoldt est vraie, ce que le résultat de Brumer donnait déjà puisque K est abélienne sur k; le théorème 5 nous montre qu'en plus $\mathrm{Y_K} = \mathrm{Z_K}$.

C'est à l'aide de $p = 5$ que nous allons exhiber un exemple de K vérifiant les hypothèses du théorème 5 avec $\eta_1^{p-1} \equiv 1\ (\mathfrak{p}_k'^2)$.

Exemple 2 :

$$p = 5, \qquad k = \mathbf{Q}(\sqrt{-11}), \qquad \mathrm{K} = k(\zeta_1).$$

On obtient facilement

$$\eta_1 = \frac{3 + \sqrt{-11}}{2}, \qquad \eta_1^4 = \frac{-49 - 3\sqrt{-11}}{2} \equiv 1\ (\mathfrak{p}_k'^2).$$

Il est clair que $g = 2$ car $\mathfrak{p}_k$ et $\mathfrak{p}_k'^2$ se ramifient totalement dans K/k. Il reste à prouver que 5 ne divise pas h_K. Cela revient à prouver grâce aux résultats de [10] que 5 ne divise pas h_{K_0} (K_0, sous-corps réel maximal de K). On voit facilement que K_0 est cyclique de degré 4 sur $\mathbf{Q}$ et que son dicriminant est égal à $5^3.11^2$; en appliquant alors les majorations de Minkowski (voir par exemple [9]) on obtient le résultat désiré.

Comme K est abélien sur $\mathbf{Q}$ on sait que $s_K = r_2 + 1$, le théorème 5 nous prouve que $t_K = 1$, c'est le premier exemple de corps K avec p qui ne divise pas h_K et Y_K distinct de Z_K.

Nous donnons enfin un dernier exemple vérifiant les hypothèses de la proposition 2.9 et pour lequel la conjecture de Leopoldt est vraie sans que les hypothèses de Brumer soient vérifiées.

EXEMPLE 3. — Prenons $p = 3$ et $K = \mathbf{Q}(\sqrt{-1}, \sqrt{7}, \sqrt[4]{\alpha})$ avec $\alpha = -3(2+\sqrt{7})^2$. On voit facilement que $K = \mathbf{Q}(\sqrt{7}).N$, où $N = \mathbf{Q}(\sqrt{-3}, \sqrt{-7}, \sqrt{6+4\sqrt{-3}})$. On montre que $N/\mathbf{Q}$ est galoisienne à groupe de Galois diédral d'ordre 8 et que les seuls idéaux premiers qui s'y ramifient sont 2, 3 et 7. Posons $\mathbf{Q}(\sqrt{-3}, \sqrt{-7}) = K_0$, il est clair que K/K_0 est biquadratique non-cyclique et que les extensions intermédiaires non triviales sont N,

$$K_0(\sqrt{7}) = K_0' \qquad \text{et} \qquad K_0\left(\sqrt{-6-4\sqrt{-3}}\right) = \hat{N}.$$

L'hypothèse (a) de la proposition 2.9 est vérifiée avec $m = 1$ ainsi que l'hypothèse (e). Pour vérifier les hypothèses (c) et (d) on remarque d'abord que $g = 2$ et que le corps de décomposition des idéaux premiers au-dessus de 3 est $\mathbf{Q}(\sqrt{7})$.

Pour vérifier (b) nous avons besoin du lemme suivant dont la démonstration ne présente pas de difficulté.

LEMME. — *Soit* L *une extension galoisienne d'un corps de nombres* L_0 *avec* Gal L/L_0 *isomorphe au « vierergruppe ». Désignons par* L_1, L_2, L_3 *les extensions quadratiques intermédiaires de* L/L_0. *Pour que* h_L *soit divisible par un nombre premier p impair il faut et il suffit que p divise l'un des* h_{L_i}, $i = 1, 2$ ou 3.

En appliquant plusieurs fois ce lemme à K/K_0, K_0', $N/\mathbf{Q}(\sqrt{-3})$ et $\hat{N}/\mathbf{Q}(\sqrt{-3})$ on voit que (b) sera vérifiée si et seulement si 3 ne divise pas les nombres de classes des corps $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{3})$, $\mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{7})$, $\mathbf{Q}(\sqrt{-7})$, $\mathbf{Q}(\sqrt{21})$, $\mathbf{Q}(\sqrt{-21})$, $\mathbf{Q}(\sqrt{-3}, \sqrt{6+4\sqrt{-3}})$ et

$\mathbf{Q}\left(\sqrt{-3}, \sqrt{-6-4\sqrt{-3}}\right)$. Pour les corps quadratiques on le vérifie facilement à l'aide de tables. Pour les deux corps biquadratiques (qui ne sont pas galoisiens sur $\mathbf{Q}$ et dont le discriminant vaut $3^3.7.8^2$) on utilise les majorations de Minkowski (voir par exemple [9], § 30).

Il semble bien que les méthodes du paragraphe 1 n'aient pas encore donné tout ce qui était possible d'en tirer. Nous avons exprimé qu'une extension cyclique de degré p d'un K, envisagé dans cette partie, se plongeait pour tout n dans une extension cyclique de degré p^n. Il resterait à donner une condition explicite « d'emboîtement » de ces extensions pour caractériser les extensions cycliques de degré p qui se plongent dans une Γ-extension.

BIBLIOGRAPHIE

[1] E. Artin, *Algebraic numbers and algebraic functions*, Gordon and Breach, 1967.

[2] J. Ax, *On the units of an algebraic number field* (*Illinois J. Math.*, vol. 9, 1967, p. 584-589).

[3] N. Bourbaki, *Algèbre*. Chap. VII : *Modules sur les anneaux principaux*, 2e éd., Hermann, Paris, 1964.

[4] A. Brumer, *On the units of algebraic number fields* (*Mathematika*, vol. 14, 1967, p. 121-124).

[5] J. W. S. Cassels et A. Fröhlich, *Algebraic number theory*, Academic Press, 1967.

[6] C. Chevalley, *Sur la théorie du corps de classes dans les corps finis et dans les corps locaux* (*J. Fac. Sc. Tokyo*, 1933, p. 365-476).

[7] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Physica Verlag, 1965.

[8] H. Hasse, *Invariante Kennzeichnung relativ abelscher Zahlkörper* (*Abh. d. D. Akad. d. Wiss. zu Berlin*, 1947, p. 1-56).

[9] H. Hasse, *Zahlentheorie*, Akademie-Verlag, Berlin, 1963.

[10] H. Hasse, *Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.

[11] K. Iwasawa, Notes d'un Séminaire à Princeton, 1966.

[12] K. Iwasawa et C. C. Sims, *Computations of invariants in the theory of cyclotomic fields* (*J. Math. Soc. Japan*, vol. 18, 1966, p. 86-98).

[13] K. Iwasawa, *Some Modules in local cyclotomic fields*, Coll. C. N. R. S., Clermont-Ferrand, 1964.

[14] I. Kaplansky, *Infinite Abelian Groups*, Ann. Arbor, 1968.

[15] H. Kisilevsky, *Some results related to Hilbert's theorem* 94 (*Journal of Number Theory*, vol. 2, 1970, p. 199-206.

[16] T. Kubota, *Über den bizyklischen biquadratischen Zahlkörper* (*Nagoya Math. J.*, 1953, p. 65 à 85).

[17] S. N. Kuroda, *Über die Klassenzahl eines relativ zyklischer Zahlkörpers vom Primzahlgrad* (*Proceedings of Japan Acad.*, vol. 40, 1964).

[18] H. W. LEOPOLDT, *Zur Arithmetik in abelscher Zahlkörper* (*J. reine u. angew. Math.*, vol. 209, 1962, p. 54-71).

[19] J. J. PAYAN, *Critère de décomposition d'une extension de Kummer...* (*Ann. scient. Éc. Norm. Sup.*, 4e série, t. 1, 1968, p. 445-458).

[20] J.-P. SERRE, *Corps locaux*, Hermann, Paris, 1962.

[21] H. YOKOI, *On the class number of a relatively cyclic number field* (*Nagoya Math. J.*, 1966-1967, p. 31-44).

(Manuscrit reçu le 4 novembre 1971.)

Françoise BERTRANDIAS,
Jean-Jacques PAYAN,
Institut de Mathématiques pures,
B. P. n° 116,
38400 Saint-Martin-d'Hères.