COURS DE L'INSTITUT FOURIER

J. J. PAYAN

Chapitre II

Cours de l'institut Fourier, tome 7 (1972), p. 31-48

<http://www.numdam.org/item?id=CIF_1972__7__31_0>

CHAPITRE II

Le but de ce chapitre est l'étude du groupe des classes ambiges d'une extension cyclique de degré premier impair d'un corps de nombres. Il est directement inspiré du chapitre IV de la thèse de C. CHEVALLEY. On s'est efforcé d'utiliser une présentation relativement moderne et de mettre en évidence pour conclure quelques applications intéressantes : "capitalisation" de certaines classes d'idéaux d'ordre p , théorème d'Iwasawa sur la régularité du p^n-ième corps cyclotomique.

NOTATIONS. Dans ce qui suit on désigne par :

p	un nombre premier impair,
k	un corps de nombres algébriques,
K	une extension cyclique de degré p de k ,
G	le groupe de Galois de K/k ,
σ	un générateur de G (fixé une fois pour toutes),
A_k (resp A_K)	l'anneau des entiers de k (resp de K),
U_k (resp U_K)	le groupe des unités de k (resp de K),
T_k (resp T_K)	le sous-groupe de torsion de U_k (resp de U_K) ,
N ou $N_{K/k}$	l'homomorphisme norme de K^* dans k^*
$U_K^{(N)}$	le sous-groupe de U_K , des unités de norme 1 ,
r_k (resp r_K)	le nombre des places archimédiennes de k , (resp K) diminué d'une unité.

1. LE THEOREME 90 DE HILBERT.

Théorème 1.1.

Soit α un élément non nul de K . Les deux assertions suivantes sont équivalentes :

1) $N_{K/k}(\alpha) = 1$,

2) il existe $\beta \in K^*$ tel que $\alpha = \beta^{1-\sigma}$ $(= \frac{\beta}{\sigma(\beta)})$.

Démonstration : Montrons que 1) implique 2) . Pour cela, considérons l'application $\Phi_\alpha : K \to K$ définie par :

$$\Phi_\alpha(t) = t + \alpha t^{\sigma} + \alpha^{1+\sigma} t^{\sigma^2} + \ldots + \alpha^{1+\sigma+\ldots+\sigma^{p-2}} t^{\sigma^{p-1}} .$$

Il est clair que cette application est k-linéaire. Il résulte du lemme de Dedekind sur les k-automorphismes de K (cf. Samuel [13], p. 47) qu'il existe $t \in K^*$ tel que $\Phi_\alpha(t) \neq 0$. Soit t_o un tel élément de K . Si $\alpha \in U_K^{(N)}$ on a $\alpha(\Phi_\alpha(t_o))^{\sigma} = \Phi_\alpha(t_o)$ c'est-à-dire $\alpha = (\Phi_\alpha(t_o))^{1-\sigma}$.

Le fait que 2) implique 1) résulte de ce que deux éléments de K conjugués sur k ont même norme dans l'extension K/k .

Remarque 1.1.1 : Le théorème ci-dessus est valable pour une extension K/k cyclique de degré quelconque.

Remarque 1 1.2 : L'opération de $\mathbb{Z}[G]$ sur le groupe multiplicatif K^* définie par $\alpha^{\sum_o^{p-1} n_i\sigma^i} = \prod_{i=0}^{p-1} (\alpha^{\sigma_i})^{n_i}$, munit K^* d'une structure de $\mathbb{Z}[G]$-module. De manière analogue, on munit le groupe additif K d'une structure de $k[G]$-module à l'aide de l'opération de G sur K définie par

$$\alpha^{\sum_o^{p-1} \lambda_i\sigma^i} = \sum_{i=0}^{p-1} \lambda_i \alpha^{\sigma^i} \qquad (\lambda_i \in k) .$$

Dans ces conditions, on a une propriété analogue à celle énoncée dans le théorème 1.1, à savoir :

Proposition 1.2.

Soit α un élément de K . Les deux assertions suivantes sont équivalentes :

1) La trace de α dans l'extension K/k est nulle.

2) Il existe $\beta \in K$ tel que $\alpha = \beta - \beta^{\sigma}$.

Démonstration : Il est clair que 2) implique 1) . Prouvons l'implication inverse. Il résulte encore du lemme de Dedekind, qu'il existe dans K un élément θ dont la trace n'est pas nulle. Considérons alors l'élément $\psi_\alpha(\theta) = (\mathrm{Tr}_{K/k}(\theta))^{-1}.(\alpha\theta^{\sigma} + (\alpha+\alpha^{\sigma})\theta^{\sigma^2} + \ldots + (\alpha+\alpha^{\sigma}+\ldots+\alpha^{\sigma^{p-2}})\theta^{\sigma^{p-1}})$. On a alors, si $\mathrm{Tr}_{K/k}(\alpha) = 0$, l'égalité :

$$\alpha + (\psi_\alpha(\theta))^{\sigma} = (\mathrm{Tr}_{K/k}(\theta))^{-1}(\alpha(\theta+\theta^{\sigma}+\ldots+\theta^{\sigma^{p-1}}) + \alpha^{\sigma}\theta^{\sigma^2} + \ldots + (\alpha^{\sigma}+\ldots+\alpha^{\sigma^{p-1}})\theta^{\sigma^p}),$$

c'est-à-dire $\alpha + [\psi_\alpha(\theta)]^{\sigma} = \psi_\alpha(\theta)$, ce qui démontre la propriété.

Exercice.

Soient a , b , c trois entiers rationnels. A l'aide du théorème 1.1 et de la remarque qui le suit, déterminer l'ensemble des solutions en nombres entiers de l'équation

$$(E) \qquad ax^2 + by^2 + cz^2 = 0 \quad .$$

2. LE THEOREME DE HERBRAND-ARTIN (1930-1932).

Théorème 2.1.

Il existe r_k unités de U_K , $\eta_1, \ldots, \eta_{r_k}$ de norme 1 telles que le groupe

$$V_K = \{\eta_1^{\alpha_1}.\eta_2^{\alpha_2}\ldots\eta_{r_k}^{\alpha_{r_k}}.\eta_o \mid \alpha_1, \ldots, \alpha_{r_k} \in \mathbb{Z}[G] \ , \ \eta_o \in U_k\} \ ,$$

soit d'indice fini dans U_K .

Ce théorème fut démontré pour la première fois par Herbrand [9] . Une démonstration simplifiée en fut ensuite donnée par Artin [1] . Pour la démonstration qui va suivre, nous aurons besoin de quelques propriétés de l'algèbre de groupe $\mathbb{Z}[G]$.

Digressions sur $\mathbb{Z}[G]$.

Remarquons que, en tant que $\mathbb{Z}$-algèbre, $\mathbb{Z}[G]$ est isomorphe à $\mathbb{Z}[X]/(X^p-1)$, où $\mathbb{Z}[X]$ désigne l'anneau des polynômes à une indéterminée et à coefficients dans $\mathbb{Z}$. Si on désigne par $N : \mathbb{Z}[G] \to \mathbb{Z}[G]$ la norme, c'est-à-dire l'application $(a \to (1+\sigma+\ldots+\sigma^{p-1}).a)$, on obtient l'isomorphisme

$$\mathbb{Z}[G]/N\mathbb{Z}[G] \simeq \mathbb{Z}[X]/(X^p-1, X^{p-1}+X^{p-2}+\ldots+1) .$$

Puisque l'idéal $(X^{p-1}+X^{p-2}+\ldots+1)$ divise l'idéal (X^p-1) , on déduit de ce qui précède l'isomorphisme d'anneaux :

$$\mathbb{Z}[G]/N\mathbb{Z}[G] \simeq \mathbb{Z}[\zeta_p] ,$$

où ζ_p est une racine primitive p-ième de l'unité. Or on sait que $\mathbb{Z}[\zeta_p]$ est isomorphe à l'anneau des entiers du p-ième corps cyclotomique. Dans ces conditions, il est clair que $\mathbb{Z}[G]/N\mathbb{Z}[G]$ est muni canoniquement d'une structure d'anneau de Dedekind. En particulier, on sait que $\mathbb{Z}[\zeta_p]$ est principal si p est l'un des nombres $3,5,7,11,13,17,19$.

Démonstration du théorème 2.1 : Remarquons tout d'abord que le groupe $U_K^{(N)} \cap U_k$ est le groupe des racines p-ièmes de l'unité qui appartiennent à k . On a une suite exacte de groupes :

$$1 \to U_K^{(N)}/T_K \cap U_K^{(N)} \to U_K/T_K \to U_k/T_k ;$$

les groupes qui interviennent dans cette suite sont des $\mathbb{Z}$-modules libres de type fini. L'application du théorème de la dimension aux éléments de cette suite permet d'écrire :

$$(1) \qquad rg_{\mathbb{Z}}(U_K^{(N)}/T_K \cap U_K^{(N)}) + rg_{\mathbb{Z}}(N(U_K/T_K)) = rg_{\mathbb{Z}}(U_K/T_K) .$$

On déduit du fait que tout $\mathbb{Z}$-module de type fini est somme directe de

son sous-module de torsion et d'un $\mathbb{Z}$-module libre de rang fini la propriété suivante :

Si A est un $\mathbb{Z}$-module de type fini et si B est un sous $\mathbb{Z}$-module libre de A, A et B ont même rang si et seulement si le module quotient A/B est de torsion.

Ceci étant on sait que U_k^p est un sous-groupe de NU_K et que $U_k^p T_k$ est un sous groupe d'indice p^{r_k-1} de U_k/T_k. On applique la propriété ci-dessus à NU_K/T_k et à U_k/T_k pour obtenir l'égalité :

$$(2) \qquad rg_{\mathbb{Z}}(U_K/T_K) = rg_{\mathbb{Z}}(U_k/T_k) + rg_{\mathbb{Z}}(U_K^{(N)}/U_K^{(N)} \cap T_K) \quad .$$

Par ailleurs, on a :

$$(U_k T_K/T_K) \cap (U_K^{(N)} T_K/T_K) = \{1\} \quad ;$$

ceci implique :

$$rg_{\mathbb{Z}}(U_k U_K^{(N)} T_K/T_K) = rg_{\mathbb{Z}}(U_k T_K/T_K) + rg_{\mathbb{Z}}(U_K^{(N)} T_K/T_K) \quad .$$

Puisque les groupes U_k/T_k et $U_k T_K/T_K$ d'une part, $U_K^{(N)} T_K/T_K$ et $U_K^{(N)}/U_K^{(N)} \cap T_K$ d'autre part sont isomorphes on a l'égalité

$$(3) \qquad rg_{\mathbb{Z}}(U_k U_K^{(N)} T_K/T_K) = rg_{\mathbb{Z}}(U_K/T_K) \quad .$$

Par ailleurs, il résulte de l'égalité (2) :

$$rg_{\mathbb{Z}}(U_K^{(N)}/U_K^{(N)} \cap T_K) = r_K - r_k = (p-1)r_k \quad .$$

On peut même donner au sujet de ce dernier groupe des renseignements précis :

Lemme 2.1.1.

Le groupe quotient $U_K^{(N)}/U_K^{(N)} \cap T_K$ est muni canoniquement d'une structure de $\mathbb{Z}[\zeta_p]$-module. Ce $\mathbb{Z}[\zeta_p]$-module est de type fini et sans torsion.

Démonstration : Le groupe $U_K^{(N)}$ a une structure de $\mathbb{Z}[G]$-module et il est annulé par la norme. Il a donc une structure de $\mathbb{Z}[\zeta_p]$-module qui confère à $U_K^{(N)}/U_K^{(N)} \cap T_K$ la structure de $\mathbb{Z}[\zeta_p]$-module annoncée. De plus $U_K^{(N)}/U_K^{(N)} \cap T_K$ est un $\mathbb{Z}$-module de type fini sans torsion. Il suffit de montrer

qu'il est sans $\mathbb{Z}[\zeta_p]$-torsion. Soit alors $u \in U_K^{(N)}$ et soit $\alpha \in \mathbb{Z}[\zeta_p]$ tel que $u^\alpha \in T_K$. Soit $\alpha' \in \mathbb{Z}[\zeta_p]$ tel que $N(\alpha) = \alpha\alpha'$. On obtient $(u^\alpha)^{\alpha'} = u^{N(\alpha)} \in T_K$. Puisque $N(\alpha) \in \mathbb{Z}$ et puisque $U_K^{(N)}/U_K^{(N)} \cap T_K$ est sans $\mathbb{Z}$-torsion on a $u \in T_K \cap U_K^{(N)}$, ce qui achève la démonstration.

Pour achever la démonstration du théorème nous aurons besoin de lemmes dont on trouvera les démonstrations dans Bourbaki [4], §4 n°10 :

Lemme 2.1.2.

Soient A un anneau de Dedekind, M un A-module de type fini, T le sous-module de torsion de M. Alors T est facteur direct dans M.

Lemme 2.1.3.

Soient A un anneau de Dedekind, M un A-module sans torsion, de type fini et de rang $n \geq 1$. Il existe alors un idéal $\mathfrak{a}$ de A tel que M soit isomorphe à la somme directe des modules A^{n-1} et $\mathfrak{a}$.

Puisque $\mathbb{Z}[\zeta_p]$ est un anneau de Dedekind, il résulte du lemme 2.1.3 qu'il existe un sous $\mathbb{Z}[\zeta_p]$-module libre V'_K de $U_K^{(N)}$ qui est libre de rang r_k. Dans ces conditions le groupe $V_K = V'_K U_k$ répond aux conditions du théorème.

2.2. Cas particuliers.

Si $k = \mathbb{Q}$ et si $p \leq 19$ on a $U_k = \{\pm 1\}$ et $T_k = T_K = \{\pm 1\}$ car K est formellement réel. Du fait que $\mathbb{Z}[\zeta_p]$ est principal on a :

$$U_K = \{\pm \eta^\alpha \mid \alpha \in \mathbb{Z}[\zeta_p]\} \quad .$$

3. IDEAUX AMBIGES, CLASSES AMBIGES.

Il est bien connu que, si K/k est une extension cyclique de corps de nombres dont le groupe de Galois est $G = \langle \sigma \rangle$, le groupe G opère sur le groupe des idéaux fractionnaires de K. Cette opération induit une opération de G sur le groupe des classes d'idéaux de K. On est alors amené à poser

la définition suivante :

Définition 3.1.

Un idéal fractionnaire $\mathfrak{a}$ de K est dit ambige s'il satisfait à la relation : $\mathfrak{a}^{1-\sigma} = A_K$. De même une classe d'idéaux C de K est dite classe ambige si $C^{1-\sigma}$ est la classe neutre.

Remarque : Une classe d'idéaux qui contient un idéal ambige est une classe ambige. Il se peut qu'une classe ambige ne contienne aucun idéal ambige. A ce sujet voir Payan [12] .

Pour conclure ce cours, on se propose précisément de calculer l'ordre du groupe des classes ambiges de K relativement à k .

Notations complémentaires 3.2.

En sus des notations précisées au début de ce chapitre, on utilisera les suivantes :

P_K groupe des idéaux fractionnaires principaux de K ,

P_k groupe des idéaux fractionnaires principaux de k étendus à K ,

F_k groupe des idéaux fractionnaires de k étendus à K ,

h_k ordre du groupe des classes d'idéaux de k ,

$\mathcal{A}_K$ groupe des idéaux fractionnaires ambiges de K ,

$\mathcal{U}$ groupe des classes ambiges de K ,

$\mathcal{U}^*$ groupe des classes des idéaux ambiges de K ,

Δ le groupe $\{\alpha \in K^* \mid \alpha A_K = (\alpha) \in \mathcal{A}_K \cap P_K\}$,

Θ_K le groupe $\{\alpha \in K^* \mid \exists \mathfrak{a},\ \alpha A_K = \mathfrak{a}^{1-\sigma}\}$.

Remarques : Il résulte des notations et des définitions qu'on a :

- $P_k \subset \mathcal{A}_K \cap P_K \subset \mathcal{A}_K$
- $\mathcal{U}^* = \mathcal{A}_K P_K / P_K$ est isomorphe à $\mathcal{A}_K / \mathcal{A}_K \cap P_K$.
- $\Delta = \{\alpha \in K^* \mid \alpha^{1-\sigma} \in \mathcal{U}_K\}$.

Lemme 3.3.1.

Soient $\mathfrak{p}_1,\ldots,\mathfrak{p}_t$ les idéaux premiers de k qui sont ramifiés dans K et soient $\mathfrak{P}_1,\mathfrak{P}_2,\ldots,\mathfrak{P}_t$, les idéaux premiers de K respectivement situés au-dessus de $\mathfrak{p}_1,\ldots,\mathfrak{p}_t$. Soit $\mathfrak{a} \in \mathcal{C}_K$ un idéal ambige de K. Il existe une décomposition unique de $\mathfrak{a}$ sous la forme :

$$\mathfrak{a} = \Big(\prod_{i=1}^{t} \mathfrak{P}_i^{\lambda_i}\Big)\mathfrak{a}_o \qquad (D)$$

avec $\mathfrak{a}_o \in F_k$ et $\lambda_1,\ldots,\lambda_t \in \{0,1,\ldots,p-1\}$.

Réciproquement, tout idéal de K qui se décompose sous la forme (D) est un idéal ambige.

Démonstration : Soit $\mathfrak{a}$ un idéal fractionnaire de K. On peut écrire $\mathfrak{a}$ de façon unique sous la forme $\mathfrak{a} = \mathfrak{a}'\mathfrak{a}_o$ où $\mathfrak{a}_o$ est dans F_k et où $\mathfrak{a}'$ est un idéal entier de K sans facteur appartenant à F_k. Dans ces conditions, l'idéal $\mathfrak{a}'$ n'admet pas de facteur premier inerte. De plus, si un facteur premier de $\mathfrak{a}'$ est l'un des $\mathfrak{P}_i$, celui-ci intervient dans $\mathfrak{a}'$ avec une puissance positive strictement inférieure à p. Enfin, l'idéal $\mathfrak{a}$ est ambige si et seulement si $\mathfrak{a}'$ l'est. Si $\mathfrak{a}'$ est ambige, aucun idéal premier de K qui est décomposé ne divise $\mathfrak{a}'$. Ceci montre l'existence et l'unicité de la décomposition (D) si $\mathfrak{a} \in \mathcal{C}_K$. La dernière assertion du lemme est immédiate.

Corollaire 3.3.2.

On a $[\mathcal{C}_K : F_k] = p^t$.

Proposition 3.3.

Le groupe quotient $\mathcal{C}_K/P_k$ est fini. Son ordre est $h_k.p^t$ où t est le nombre d'idéaux premiers de k qui sont ramifiés dans K.

Démonstration : La suite exacte canonique

$$0 \to F_k \to \mathcal{C}_K \to \mathcal{C}_K/F_k \to 0$$

donne lieu par passage au quotient par P_k à la suite exacte

$$0 \to (F_k/P_k) \to (\mathcal{C}_K/P_k) \to (\mathcal{C}_K/F_k) \to 0 .$$

(Ne pas oublier que P_k est un sous-groupe de F_k et que F_k/P_k est isomorphe au groupe des classes d'idéaux de k). La proposition est alors une conséquence du lemme 3.3.1 et de son corollaire 3.3.2.

Corollaire 3.3.3.

Le groupe $\mathcal{U}^*$ des classes d'idéaux ambiges est fini. Son ordre est :

$$\text{Card } \mathcal{U}^* = \frac{h_k . p^t}{[\mathcal{C}_K \cap P_K : P_k]} .$$

En effet on a $\mathcal{U} = \mathcal{C}_K P_K/P_K$ qui est isomorphe à $\mathcal{C}_K/\mathcal{C}_K \cap P_K$. Puisque $P_k \subset \mathcal{C}_K \cap P_K \subset \mathcal{C}_K$, il résulte de la proposition 3.3 que $[\mathcal{C}_K : \mathcal{C}_K \cap P_K] = [\mathcal{C}_K : P_k][\mathcal{C}_K \cap P_K : P_k]^{-1} = \text{Card } \mathcal{U}$. Donc $\text{Card } \mathcal{U} = h_k . p^t [\mathcal{C}_K \cap P_K : P_k]^{-1}$

Lemme 3.4.1.

On a $[\mathcal{C}_K \cap P_K : P_k] = [U_K^{(N)} : U_K^{1-\sigma}]$

Démonstration : Tout d'abord, il résulte de la définition du groupe Δ qu'on a l'isomorphisme de groupes

$$\mathcal{C}_K \cap P_K \simeq \Delta/U_K .$$

Considérons alors les suites exactes de groupes :

$$1 \to U_K \to \Delta \to \Delta/U_K \to 1$$

$$1 \to U_K \to k^*U_K \to k^*U_K/U_K \to 1 .$$

De ces deux suites exactes et du fait que le groupe k^*U_K/U_K est isomorphe au groupe P_k on déduit le diagramme commutatif :

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & U_K & \to & k^*U_K & \to & P_k & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & U_K & \to & \Delta & \to & \mathcal{C}_K \cap P_K & \to & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & \to & \Delta/k^*U_K & \to & (\mathcal{C}_K \cap P_K)/P_k & \to & 1
\end{array}$$

(Forme affaiblie du diagramme du serpent, Bourbaki [3], §1, n°4). En particulier, on a l'égalité :

$$[\mathfrak{a}_K \cap P_K : P_k] = [\Delta : k^* U_K] \quad .$$

L'utilisation du même procédé avec les suites exactes de groupes :

$$1 \to k^* \to \Delta \xrightarrow{1-\sigma} \Delta^{1-\sigma} \to 1$$

$$1 \to k^* \to k^* U_K \xrightarrow{1-\sigma} U_K^{1-\sigma} \to 1$$

donne l'égalité :

$$[\Delta : k^* U_K] = [\Delta^{1-\sigma} : U_K^{1-\sigma}] \ .$$

Enfin, remarquons que $\Delta^{1-\sigma}$ est un sous-groupe de $U_K^{(N)}$; il résulte du théorème 90 de Hilbert (voir §1) que $U_K^{(N)} \subset U_K \cap (K^*)^{1-\sigma} = \Delta^{1-\sigma}$. Le regroupement de tous ces résultats partiels donne l'égalité :

$$[\mathfrak{a}_K \cap P_K : P_k] = [U_K^{(N)} : U_K^{1-\sigma}] \quad .$$

Théorème 3.4.

Le groupe des classes ambiges $\mathcal{U}$ *est d'ordre*

$$\text{Card } \mathcal{U} = \frac{h_k \times p^{t-1}}{[U_k : U_k \cap NK^*]} \quad .$$

La démonstration de ce théorème repose sur les quelques lemmes qui suivent :

Lemme 3.4.2.

Compte tenu des notations de (3.2) *on a l'égalité* :

$$[\mathcal{U} : \mathcal{U}^*] = [\Theta_K : U_K (K^*)^{1-\sigma}] \quad .$$

Démonstration : Tout d'abord il est clair que si :

$$\Theta_K = \{\alpha \in K^* \mid \text{il existe } \mathfrak{a} \text{ avec } \alpha A_K = \mathfrak{a}^{1-\sigma}\}$$

on a $U_K . (K^*)^{1-\sigma}$ sous-groupe de Θ_K . Soit $\mathfrak{a}_K^o$ le groupe des idéaux fractionnaires de K qui appartiennent à des classes ambiges. En particulier on a

$\mathcal{U}$ égal au groupe quotient $\mathfrak{a}_K^o/P_K$. On considère l'homomorphisme de Θ_K dans $(\mathfrak{a}_K^o)^{1-\sigma}$ qui à tout α associe αA_K et on examine les deux diagrammes commutatifs suivants :

$$\begin{array}{ccccccccc} 1 & \to & U_K & \to & U_K.(K^*)^{1-\sigma} & \to & P_K^{1-\sigma} & \to & 1 \\ & & \text{id.}\downarrow & & j\downarrow & & j\downarrow & & \\ 1 & \to & U_K & \to & \Theta_K & \to & (\mathfrak{a}_K^o)^{1-\sigma} & \to & 1 \end{array} \qquad (I)$$

$$\begin{array}{ccccccccc} 1 & \to & \mathfrak{a}_K \cap P_K & \to & P_K & \xrightarrow{1-\sigma} & P_K^{1-\sigma} & \to & 1 \\ & & j\downarrow & & j\downarrow & & j\downarrow & & \\ 1 & \to & \mathfrak{a}_K & \to & \mathfrak{a}_K^o & \xrightarrow{1-\sigma} & (\mathfrak{a}_K^o)^{1-\sigma} & \to & 1 \end{array} \qquad (II) \quad .$$

Le lemme du serpent appliqué à (I) donne immédiatement l'isomorphisme

$$\Theta_K/U_K(K^*)^{1-\sigma} \simeq (\mathfrak{a}_K^o)^{1-\sigma}/P_K^{1-\sigma} \quad .$$

Le lemme du serpent appliqué à (II) donne la suite exacte :

$$1 \to \mathcal{U}^* \to \mathcal{U} \to (\mathfrak{a}_K^o)^{1-\sigma}/P_K^{1-\sigma} \to 1 \ .$$

En particulier, on obtient :

$$[\mathcal{U}:\mathcal{U}^*] = [(\mathfrak{a}_K^o)^{1-\sigma}:P_K^{1-\sigma}] = [\Theta_K:U_K(K^*)^{1-\sigma}] \quad .$$

Lemme 3.4.3.

Avec les mêmes notations que plus haut on a :

$$N\Theta_K = U_k \cap NK^* \quad .$$

Démonstration : Soit $\alpha \in \Theta_K$. Il existe $\mathfrak{a}$, idéal fractionnaire de K qui satisfait à la relation $\mathfrak{a}^{1-\sigma} = \alpha A_K$. Par application de la norme on obtient $N(\alpha A_K) = (N\mathfrak{a})^{1-\sigma} = A_k$. Par conséquent, on a $N\alpha \in U_k$.

Réciproquement, soit $\alpha \in K^*$ tel que $N_{K/k}(\alpha) \in U_k$. Il est clair que $N(\alpha A_K) = A_k$. On vérifie facilement que les seuls idéaux premiers de K qui

interviennent dans la décomposition de αA_K sont des idéaux décomposés. Soit donc $\mathfrak{p}$ un idéal premier de k qui intervient dans αA_K . On peut écrire $\mathfrak{p} = \mathfrak{P}_1 \ldots \mathfrak{P}_p$ et

$$\alpha A_K = (\prod_1^p \mathfrak{P}_j^{a_j}).\mathfrak{a}(\mathfrak{p}) \quad ; \quad (a_j \in \mathbb{Z} \ , \ (\mathfrak{a}(\mathfrak{p}),\mathfrak{p}) = A_K) \ .$$

Puisque l'idéal αA_K est de norme 1 , on a $\sum_1^p a_j = 0$. On peut supposer que σ agit sur les $\mathfrak{P}_j$ de telle sorte que $\mathfrak{P}_p^\sigma = \mathfrak{P}_1$ et $\mathfrak{P}_j^\sigma = \mathfrak{P}_{j+1}$ si $1 \leq j < p$. Dans ces conditions il existe des entiers rationnels $b_1, \ldots, b_p$ tels que $b_p - b_1 = a_p$ et $b_j - b_{j'+1} = a_j$ et on a

$$(\prod_{j=1}^p \mathfrak{P}_j^{a_j}) = (\prod_{j=1}^p \mathfrak{P}_j^{b_j})^{1-\sigma} \ .$$

On en conclut l'existence d'un idéal fractionnaire $\mathfrak{a}$ de K tel que $\alpha A_K = \mathfrak{a}^{1-\sigma}$, c'est-à-dire que $\alpha \in \Theta_K$. Le lemme est démontré.

Lemme 3.4.5.

Toujours avec les mêmes notations on a l'égalité :

$$[\mathcal{U}:\mathcal{U}^*] = [N\Theta_K : NU_K] \ .$$

Démonstration : Il suffit d'appliquer le lemme du serpent au diagramme commutatif suivant construit à l'aide du théorème 90 :

$$\begin{array}{ccccccccc} 1 & \to & (K^*)^{1-\sigma} & \to & U_K(K^*)^{1-\sigma} & \overset{N}{\to} & NU_K & \to & 1 \\ & & \text{id.} \downarrow & & j \downarrow & & j \downarrow & & \\ 1 & \to & (K^*)^{1-\sigma} & \to & \Theta_K & \to & N\Theta_K & \to & 1 \end{array} \quad ;$$

on obtient $[N\Theta_K : NU_K] = [\Theta_K : U_K(K^*)^{1-\sigma}]$, et on applique le lemme 3.4.2.

Corollaire 3.4.6.

Les deux assertions suivantes sont équivalentes :

a) Toute unité de k qui est une norme est une norme d'unité ;

b) Toute classe ambige est classe d'un idéal ambige.

Corollaire 3.4.7.

L'ordre du groupe $\mathcal{U}$ des classes ambiges satisfait à la relation

$$\text{Card } \mathcal{U} = \frac{h_k p^t}{[U_k : U_k \cap NK^*]} \cdot \frac{[U_k : NU_K]}{[U_K^{(N)} : U_K^{1-\sigma}]} \cdot$$

Démonstration : Tout d'abord la formule écrite a un sens car U_k/NU_K est un groupe fini du fait que U_k/U_k^p est fini -(U_k est un Z-module libre de type fini)- et du fait que U_k^p est un sous-groupe de NU_K . Pour le reste, on regroupe les résultats obtenus de (3.3.3) à (3.4.6).

Lemme 3.4.8. (Lemme de Herbrand).

Soit G' un sous-groupe d'indice fini d'un groupe G . Soient $g_1 : G \to G$ et $g_2 : G \to G$ deux endomorphismes de noyaux respectifs H_1 et H_2 et tels que $g_1 \circ g_2(G) = g_2 \circ g_1(G) = \{1\}$. On suppose que G' est stable par g_1 et par g_2 et que les indices $[G' \cap H_1 : g_2 G']$ et $[G' \cap H_2 : g_2 G']$ sont finis. Dans ces conditions il en est de même des indices $[H_1 : g_2 G]$ et $[H_2 : g_1 G]$ et on a l'égalité :

$$\frac{[H_1 : g_2 G]}{[H_2 : g_1 G]} = \frac{[G' \cap H_1 : g_2 G']}{[G' \cap H_2 : g_1 G']} \cdot$$

Démonstration : On a l'égalité

$$\begin{aligned} [G:G'] &= [G:H_2G'].[H_2G':G'] \\ &= [G:H_2G'].[H_2:G' \cap H_2] \ . \end{aligned}$$

De plus, on a la suite exacte : $1 \to H_2G' \to G \to g_2G/g_2G' \to 1$ qui donne lieu à l'égalité $[G:H_2G'] = [g_2G:g_2G']$. Par hypothèse, on a $g_1G' \subset H_2 \cap G'$ et on peut écrire :

$$[H_2:H_2 \cap G'].[H_2 \cap G':g_1G'] = [H_2:g_1G'] \ .$$

Alors : $[G:G'].[G' \cap H_2 : g_1G'] = [g_2G:g_2G'][H_2:g_1G']$

$$= [H_2:g_1G][g_1G:g_1G'][g_2G:g_2G'] \ .$$

Puisque g_1 et g_2 jouent des rôles analogues on a la formule

$$[G:G'].[G'\cap H_1:g_2G'] = [H_1:g_2G][g_2G:g_2G'][g_1G:g_1G'] \quad .$$

La formule du lemme est alors donnée par division membre à membre de ces égalités.

Fin de la démonstration du théorème 3.4 : Reprenons les notations du §2 concernant le théorème de Herbrand-Artin. Au cours de la démonstration de ce théorème on a mis en évidence le sous-groupe V'_K de $U_K^{(N)}$, qui est muni d'une structure de $\mathbb{Z}[\zeta_p]$-module libre de rang r_k et le groupe $V_K = V'_K.U_k$. En plus, on considère le groupe W_k des racines de l'unité appartenant à k, ${}^pW_k$ le sous-groupe des racines p-ièmes de l'unité appartenant à k. Remarquons que ${}^pW_k = {}^pW_K$ car on a $[K:k] = p$. Remarquons encore que $V'_K \cap U_k = 1$ et par suite que $(V'_K)^{1-\sigma}$ est sans $\mathbb{Z}$-torsion.

Dans ces conditions, on applique le lemme (3.4.8) à la situation suivante :

G est le groupe U_K, G' est le groupe V_K ;
g_1 est l'endomorphisme $x \to x^{1-\sigma}$;
g_2 est l'endomorphisme norme ;
H_1 est alors U_k tandis que H_2 est $U_K^{(N)}$;
$g_1(V_K) = (V'_K)^{1-\sigma}$ et $g_2(V_K) = U_k^p$;

Puisque $[U_K^{(N)}:U_K^{1-\sigma}]$ et $[U_k:NU_K]$ sont finis, il en est de même de $[U_k:U_k^p]$ et $[V_K^{(N)}:(V'_K)^{1-\sigma}]$, où on désigne par $V_K^{(N)}$ le groupe $V_K \cap U_K^{(N)}$. On obtient la relation :

$$\frac{[U_k:U_k^p]}{[V_K^{(N)}:(V'_K)^{1-\sigma}]} = \frac{[U_k:NU_K]}{[U_K^{(N)}:U_K^{1-\sigma}]} \quad .$$

D'une part, il est clair qu'on a : $U_k \simeq W_k \times \mathbb{Z}^{r_k-1}$, et par suite que :

$$[U_k:U_k^p] = [W_k:W_k^p] \times p^{r_k-1} \quad .$$

D'autre part, on a l'isomorphisme ${}^pW_k \times V'_K \simeq V_K^{(N)}$. Dans ces conditions,

et puisque $V_K'^{1-\sigma}$ est sans $\mathbb{Z}$-torsion on peut écrire :

$$\frac{[U_k:NU_K]}{[U_K^{(N)}:U_K^{1-\sigma}]} = \frac{[W_k:W_k^p].p^{r_k-1}}{[{}^pW_k:1].[V_K':(V_K')^{1-\sigma}]} .$$

On sait que W_k/W_k^p est cyclique et d'exposant p. Dans ces conditions, on a $[W_k:W_k^p] = [{}^pW_k:1] \in \{1,p\}$. Enfin, puisque V_K' est un $\mathbb{Z}[\zeta_p]$-module libre de rang r_k, on a l'isomorphisme de $\mathbb{Z}[\zeta_p]$-modules

$$V_K'/V_K'^{1-\sigma} \simeq [\mathbb{Z}[\zeta_p]/(1-\zeta_p)]^{r_k} \simeq (\mathbb{Z}/p\mathbb{Z})^{r_k} .$$

Il en résulte :

$$\frac{[U_k:NU_K]}{[U_K^{(N)}:U_K^{1-\sigma}]} = \frac{1}{p} .$$

On utilise alors le corollaire (3.4.7) et on obtient :

$$\boxed{\text{Card } \mathcal{U} = \frac{h_k p^{t-1}}{[U_k:U_k \cap NK^*]}} .$$

4. QUELQUES APPLICATIONS.

4.1. Le corps de base k est principal et $U_k = \{-1,+1\}$.

(Par exemple $k = \mathbb{Q}$ ou $k = \mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})\ldots$)

Dans ce cas on a pour tout nombre premier impair p les égalités $U_k = U_k \cap NK^*$ et évidemment $h_k = 1$, et par suite Card $\mathcal{U} = p^{t-1}$. De plus, on a : $[\mathcal{U}:\mathcal{U}^*] = [N\Theta_K:NU_K] = 1$. Il s'ensuit que toute classe ambige est classe d'un idéal ambige (corollaire 3.4.6). Or les seuls idéaux premiers ambiges qui peuvent ne pas être principaux sont les idéaux premiers ramifiés. Soient $\mathfrak{P}_1,\ldots,\mathfrak{P}_t$ les idéaux premiers de K qui sont ramifiés et

pour tout $i \in \{1,\ldots,t\}$, soit $\gamma_i = Cl(\mathfrak{P}_i)$. Le groupe engendré par la famille $\{\gamma_i\}_{i\leq t}$ est d'exposant p ; il est muni canoniquement d'une structure de $\mathbb{F}_p$-espace vectoriel dont la dimension est $t-1$ puisque Card $\mathcal{U} = p^{t-1}$. On en conclut qu'il existe t entiers rationnels $n_1,\ldots,n_t$ non tous congrus à 0 modulo p tels que l'idéal $\prod_{i=1}^{t} \mathfrak{P}_i^{n_i}$ soit principal.

En particulier, si $t = 1$, le seul idéal premier de K qui est ramifié est principal. Dans le cas $k = \mathbb{Q}$, on peut montrer directement que si $K/\mathbb{Q}$ est non ramifiée en dehors du nombre premier q et cyclique de degré $p \neq q$, alors q est congru à 1 modulo p , K est un sous-corps du q-ième corps cyclotomique $\mathbb{Q}^{(q)}$ et si $qA_K = \mathfrak{q}^p$ on a $\mathfrak{q} = N_{\mathbb{Q}(q)/K}((1-\zeta_q))$. (A ce sujet cf. M.J. FERTON [6]).

4.2. Cas d'une extension non ramifiée.

Dans ce cas $t = 0$ et p divise h_k . On trouvera une illustration de ce phénomène dans Ushida [14].

Il se peut que p divise h_k sans que p^2 divise h_k . Dans ces conditions il existe dans k un idéal non principal $\mathfrak{a}$ dont la puissance p-ième est un idéal principal. Si K/k est une extension non ramifiée cyclique de degré p , alors $\mathfrak{a}A_K$ est principal dans K! (On trouvera une illustration de ce phénomène dans le Zahlbericht de Hilbert [10] ou dans l'exposé de G. GRAS [7]).

4.3. Cas où $t = 1$ et $(h_k, p) = 1$.

Dans ce cas, p ne divise pas Card $\mathcal{U}$. On peut montrer alors que p ne divise pas le nombre de classe h_K de K . (Voir l'exposé de F. BERTRANDIAS [2]). On obtient comme cas particulier une conséquence inattendue : -(théorème dû à Iwasawa-1959)- si p est un nombre premier régulier, c'est-à-dire si p ne divise pas le nombre de classes du p-ième corps cyclotomique $\mathbb{Q}^{(p)}$, alors quel que soit $n \geq 1$, p ne divise pas le nombre de classes de $\mathbb{Q}^{(p^n)}$!

Remarque : Si $\mathfrak{a}$ est un idéal non principal de k qui devient principal dans l'extension cyclique de degré p K/k , alors $\mathfrak{a}^p$ est principal dans k . Il suffit de considérer $N_{K/k}(\mathfrak{a}A_K)$.

BIBLIOGRAPHIE

[1] - E. ARTIN - "Uber Einheiten relativ Galoisscher Zahlkorper". Journal de Crelle 167 (1932).

[2] - F. BERTRANDIAS - "Sur le genre des corps abéliens réels". Séminaire de théorie des Nombres de Grenoble - 1971-72.

[3] - N. BOURBAKI - "Algèbre commutative, chapitre 1 : modules plats". Hermann.

[4] - N. BOURBAKI - "Algèbre commutative, chapitre 7 : diviseurs". Hermann.

[5] - C. CHEVALLEY - "Sur la théorie du corps de classes dans les corps finis et les corps locaux (Thèse)". Journal of the Faculty of Science, Tokyo 1933.

[6] - M.J. FERTON - "Théorème de Kronecker-Weber". Séminaire de Théorie des Nombres, Grenoble 1971.

[7] - G. GRAS - "Le théorème 94 de Hilbert". Séminaire de Théorie des Nombres, Grenoble 1971.

[8] - G. GRAS - "Etude du groupe des unités d'un anneau d'entiers algébriques dans le cas galoisien cyclique". Séminaire de Théorie des Nombres, Grenoble 1969.

[9] - J. HERBRAND - "Nouvelle démonstration et généralisation d'un théorème de Minkowski". C.R.A.S. (1930), p. 1282.

[10] - D. HILBERT - "Théorie des corps de Nombres algébriques".

[11] - J. MARTINET - "Le théorème de Herbrandt sur les unités". Séminaire de Théorie des Nombres, Bordeaux 1968-69.

[12] - J.J. PAYAN - "Extension non ramifiées non résolubles". Séminaire de Théorie des Nombres, Grenoble 1972.

[13] - SAMUEL - "Introduction à la théorie algébrique des nombres". Hermann.

[14] - USHIDA - "Unramified extensions of quadratic number fields I et II". Tôhhu Math. Jour. 22 (1970).
