SÉMINAIRE DE THÉORIE DES NOMBRES DE BORDEAUX

JEAN FRESNEL

Rang p-adique du groupe des unités d'un corps de nombres

Séminaire de théorie des nombres de Bordeaux (1968-1969), exp. n° 9, p. 1-18

<http://www.numdam.org/item?id=STNB_1968-1969____A9_0>

Séminaire de Théorie des Nombres (J. LESCA)
Année 1968/1969 , n° 9

7 Février 1969

RANG p-ADIQUE DU GROUPE DES UNITES D'UN CORPS DE NOMBRES

par

Jean FRESNEL

-:-:-:-:-:-:-:-

O - INTRODUCTION. Cet exposé a pour but, tout d'abord, de présenter le problème du rang p-adique du groupe des unités, d'un corps de nombres posé pour la première fois par H. W. LEOPOLDT [11]. Nous exposons ensuite la méthode d'AX [3] et de BRUMER [4] qui permet de montrer que le rang p-adique du groupe des unités est égal au nombre de Dirichlet (c'est-à-dire au rang du groupe considéré comme $\mathbb{Z}$-module) dans le cas d'un corps de nombres abélien. Dans un dernier paragraphe nous montrons le lien entre le rang p-adique du groupe des unités et le nombre de Γ-extensions indépendantes d'un corps de nombres. Remarquons enfin que la solution du problème du rang p-adique du groupe des unités d'un corps de nombres permet dans le cas d'une extension abélienne de $\mathbb{Q}$ de déterminer le résidu au point 1 de la fonction Zéta p-adique à l'aide entre autres choses du régulateur p-adique [10] , [1] .

I - DEFINITION DU RANG p-ADIQUE DU GROUPE DES UNITES

Soit $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_k$ les idéaux premiers de l'anneau A au-dessus du nombre premier p. On notera $K_{\mathfrak{P}_i}$ le complété de K pour la valuation $\mathfrak{P}_i$-adique et $P_{\mathfrak{P}_i}$ le groupe des unités principales de $K_{\mathfrak{P}_i}$ (c'est-à-dire le groupe des $x \in K_{\mathfrak{P}_i}$ tels que la valuation $\mathfrak{P}_i$-adique de $x-1$ soit positive). Soit $U_o(K)$ le sous-groupe de U(K) des éléments x de U(K) satisfaisant $x \equiv 1 \bmod \mathfrak{P}_1.\mathfrak{P}_2.\ldots.\mathfrak{P}_k$. On remarquera que $U_o(K)$ est un sous-groupe d'indice fini de U(K). En effet, si $N(\mathfrak{P}_i)$ désigne la norme absolue de $\mathfrak{P}_i$ et si $n = \underset{1\le i\le k}{\text{ppcm}} (N(\mathfrak{P}_i)-1)$ on a $U(K)^n \subset U_o(K)$.

Il est clair que les sous-groupes $P_{\mathfrak{P}_i}$ qui sont complets pour la topologie $\mathfrak{P}_i$-adique peuvent être munis d'une structure de Z_p-module. Plus précisément si $a \in Z_p$ et si $u = 1 + \pi \in P_{\mathfrak{P}_i}$ on pose

$$u^a = \sum_{i=0}^{\infty} \binom{a}{i} \pi^i \quad \text{où} \quad \binom{a}{i} = \frac{a(a-1)\ldots(a-i+1)}{1 \cdot 2 \cdot \ldots \cdot i}.$$

Soit V(K) l'adhérence dans $\prod_i P_{\mathfrak{P}_i}$ (muni de la topologie produit) de l'image de $U_o(K)$ par l'application diagonale. Ainsi V(K) est un sous-Z_p-module du Z_p-module $\prod_{1\le i\le n} P_{\mathfrak{P}_i}$ et le Z_p-rang de V(K) s'appelle le rang p-adique du groupe des unités de K et on le note $r_p(K)$.

On note par r(K) le rang du groupe U(K), on sait d'après le théorème de Dirichlet [13] que r(K)+1 est égal au nombre de valeurs absolues sur K qui prolongent la valeur absolue ordinaire de $\mathbb{Q}$. Il est immédiat que l'on a l'inégalité

$$r_p(K) \le r(K).$$

II - INTERPRETATION DU RANG p-ADIQUE DU GROUPE DES UNITES COMME RANG D'UNE MATRICE

1) Rappel sur le logarithme p-adique. Soit Ω_p un complété d'une clôture algébrique de $\mathbb{Q}_p$ et $x \to |x|$ sa valeur absolue. Soit A_p l'anneau de valuation de Ω_p, $\mathfrak{M}_p$ son idéal de valuation et U_p le groupe des $x \in A_p$ tels que $|x| = 1$. Si F_p est le corps à p éléments, $\overline{F_p}$ une clôture algébrique de F_p, alors $\overline{F_p}$ est le corps des restes de Ω_p. Soit $x \to \overline{x}$, la surjection canonique de A_p sur $\overline{F_p}$ et ω l'application de A_p dans A_p qui induit sur $\overline{F_p}$ une application injective et multiplicative (resprésentant de Teichmuller) ; l'image de ω n'est autre que 0 et le groupe des racines de l'unité de A_p dont l'ordre est premier à p ; d'autre part si $x \in U_p$ on a

$$\left| \frac{x}{\omega(x)} - 1 \right| < 1 .$$

On sait que sur $1+\mathfrak{M}_p$ le logarithme p-adique de u est défini par

$$\log u = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(u-1)^n}{n} ,$$

et plus généralement si $u \in U_p$ on pose

$$\log u = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{\left(\frac{u}{\omega(u)} - 1\right)^n}{n} ,$$

il est alors aisé de vérifier, sachant que ω est une fonction multiplicative que

$$\log uv = \log u + \log v ,$$

quels que soient $u , v \in U_p$.

2) Rappel sur idéaux premiers et valuations. Soit K un corps de nombres, A la clôture intégrale de $\mathbb{Z}$ dans K. Soit p un nombre premier, $\mathbb{Q}_p$ le corps p-adique élémentaire, Ω_p un complété d'une clôture

algébrique de $\mathbb{Q}_p$ et $x \to |x|$ sa valeur absolue. Soit $\sigma_1, \sigma_2, \ldots, \sigma_n$ les n $\mathbb{Q}$-homomorphismes de K dans Ω_p. La correspondance entre $\mathbb{Q}$-homomorphismes et idéaux se fait par

$$\mathfrak{P} = \{ x \in A \mid |\sigma(x)| < 1 \} .$$

Il est clair que $\mathfrak{P}$ est un idéal premier puisque c'est l'image réciproque de l'idéal de valuation de Ω_p.

Si σ est un $\mathbb{Q}$-homomorphisme, notons par $\overline{\sigma(K)}$ l'adhérence de $\sigma(K)$ dans Ω_p. On dira que deux $\mathbb{Q}$-homomorphismes σ et σ' sont équivalentes si le $\mathbb{Q}$-isomorphisme entre $\sigma(K)$ et $\sigma'(K)$ se prolonge en un $\mathbb{Q}_p$-isomorphisme entre $\overline{\sigma(K)}$ et $\overline{\sigma'(K)}$. On voit alors que deux homomorphismes sont équivalents si et seulement si ils définissent le même idéal premier. Par suite les classes d'équivalence d'homomorphismes sont en bijection avec les idéaux premiers de K au-dessus de p. Soit donc $\sigma_1, \sigma_2, \ldots, \sigma_k$ des représentants de ces classes d'équivalence en bijection respectivement avec $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_k$.

Soit $K_{\mathfrak{P}_i}$ le complété de K pour la valuation $\mathfrak{P}_i$-adique considéré comme un sous-corps de Ω_p, σ_i est donc l'homomorphisme injectif de K dans $K_{\mathfrak{P}_i}$. Si $u_1, u_2, \ldots, u_r \in U_o(K)$ et si il existe $a_1, a_2, \ldots, a_r \in Z_p$ tels que

$$(1) \qquad \sigma(u_1)^{a_2} . \sigma(u_2)^{a_2} . \ldots . \sigma(u_r)^{a_r} = 1 \qquad \text{dans } \Omega_p$$

on a aussi

$$\sigma'(u_1)^{a_1} . \sigma'(u_2)^{a_r} . \ldots . \sigma'(u_r)^{a_r} = 1 \qquad \text{pour tout } \sigma' \sim \sigma .$$

Si donc on a l'égalité (1) pour $\sigma = \sigma_i$, $1 \leq i \leq k$, on a donc l'égalité pour tout homomorphisme. Il suit donc de ces remarques préléminaires que si Φ est l'injection de $U_o(K)$ dans $\prod_i P_{\mathfrak{P}_i}$ et si $\Phi(u_1), \ldots, \Phi(u_r)$ sont Z_p liés par

$$\Phi(u_1)^{a_1} \cdot \Phi(u_2)^{a_2} \cdot \ldots \cdot \Phi(u_r)^{a_r} = 1 \quad ,$$

on a

$$\sigma(u_1)^{a_1} \cdot \sigma(u_2)^{a_2} \cdot \ldots \cdot \sigma(u_r)^{a_r} = 1 \quad ,$$

pour tout σ , et par suite

$$a_1 \log \sigma(u_1) + \ldots + a_r \log \sigma(u_r) = 0 \ ,$$

il s'ensuit alors que le rang de la matrice $(\log \sigma_j(u_i))_{\substack{1 \leq j \leq n \\ 1 \leq i \leq r}}$ est inférieur à r .

Réciproquement si le rang de la matrice $(\log \sigma_j(u_i))_{\substack{1 \leq j \leq n \\ 1 \leq i \leq r}}$ est inférieur à r , il existe $a_1, a_2, \ldots, a_r$ appartenant au compositum des $K_{\mathfrak{P}_i}$ tels que

$$a_1 \log \sigma(u_1) + \ldots + a_r \log \sigma(u_r) = 0 \quad \text{quel que soit } \sigma \ .$$

Soit τ un Ω_p-automorphisme de Ω_p , on a

$$\tau(a_1) \log \tau \circ \sigma(u_1) + \ldots + \tau(a_r) \log \tau \circ \sigma(u_r) = 0$$

quel que soit σ , comme $\tau \circ \sigma$ est un homomorphisme de K dans Ω_p , on a

$$\tau(a_1) \log \sigma(u_1) + \ldots + \tau(a_r) \log \sigma(u_r) = 0 \ ,$$

quel que soit σ . Il est clair que si l'on a cette égalité pour tout Ω_p-automorphisme τ de Ω_p . Si T désigne la trace du compositum des $K_{\mathfrak{P}_i}$ sur Ω_p , on a

$$T(a_1) \log \sigma(u_1) + \ldots + T(a_r) \log \sigma(u_r) = 0 \ .$$

Ceci montre alors que $\Phi(u_1)$, $\Phi(u_2)$, ..., $\Phi(u_r)$ sont $\mathbb{Z}_p$ liés
Nous sommes maintenant en mesure de démontrer la proposition suivante.

PROPOSITION [15]. Soit K un corps de nombres de degré n sur $\mathbb{Q}$, soit $(\varepsilon_i)_{1\le i\le r(K)}$ un système d'unités de K tel que le sous-groupe engendré par $(\varepsilon_i)_{1\le i\le r(K)}$ soit d'indice fini dans le groupe U(K) des unités de K. Soit $(\sigma_i)_{1\le i\le n}$ les $\mathbb{Q}$-homomorphismes de K dans Ω_p. Alors le rang de la matrice $(\log \varepsilon_i^{\sigma_j})_{\substack{1\le i\le r(K)\\ 1\le j\le n}}$ est égal au rang p-adique du groupe des unités de K.

Preuve. Les remarques précédentes permettent de montrer que le rang de la matrice $(\log \sigma_j(u_i))_{\substack{1\le i\le r\\ 1\le j\le n}}$ est égal au $\mathbb{Z}_p$-rang du $\mathbb{Z}_p$-module engendré par $\Phi(u_1)$, $\Phi(u_2)$, ..., $\Phi(u_r)$. Il reste alors à constater que si $(\varepsilon_i)_{1\le i\le r(K)}$ et $(\varepsilon'_i)_{1\le i\le r(K)}$ engendrant un sous-groupe d'indice fini de U(K), les matrices

$$(\log \varepsilon_i^{\sigma_j})_{\substack{1\le i\le r(K)\\ 1\le j\le n}} \quad \text{et} \quad (\log \varepsilon'^{\sigma_j}_i)_{\substack{1\le i\le r(K)\\ 1\le j\le n}}$$

ont le même rang.

III - CAS GALOISIEN

Supposons que K soit une extension galoisienne finie de $\mathbb{Q}$ de groupe de Galois G. On sait d'après le théorème de Minkowski [14, 12] qu'il existe une unité ε telle que le système $(\sigma(\varepsilon))_{\sigma\in G}$ engendre un sous-groupe d'indice fini de U(K). La proposition 1 montre alors que le rang de la matrice $(\log(\sigma\tau^{-1}(\varepsilon))_{\sigma,\tau\in G}$ est égal au rang p-adique du groupe des unités.

PROPOSITION 2. Si pour tout corps de nombres K galoisien sur $\mathbb{Q}$ on a

$$r(K) = r_p(K) \quad ,$$

alors pour tout corps de nombres L on a

$$r(L) = r_p(L) \quad .$$

Preuve. En effet, soit K la plus petite extension galoisienne contenant L , si $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r(L)}$ engendre un sous-groupe d'indice fini de $U(K)$, il existe alors $\eta_{r(L)+1}, \ldots, \eta_{r(K)}$ tel que $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r(L)}, \eta_{r(L)+1}, \ldots, \eta_{r(K)})$ engendre un sous-groupe d'indice fini de $U(K)$. Il reste alors à utiliser la proposition 1 .

IV - CAS ABELIEN

Nous allons voir que dans le cas abélien le rang de la matrice $(\log \sigma \tau^{-1}(\varepsilon))_{\sigma,\tau \in G}$ s'exprime très simplement en utilisant le dual de G .

PROPOSITION 3 [7]. Soit G un groupe abélien fini, f une application de G dans un corps K , M la matrice

$$M = (f(\sigma \tau^{-1}))_{\sigma,\tau \in G} \quad .$$

Soit $\hat{G}$ le dual du groupe G . La matrice M est semblable à la matrice diagonale dont les éléments sont $\left(\sum_{\sigma \in G} \chi(\sigma) f(\sigma)\right)_{\chi \in \hat{G}}$. En conséquence

$$\det M = \prod_{\chi \in \hat{G}} \left(\sum_{\sigma \in G} \chi(\sigma) f(\sigma) \right) \quad ,$$

de plus

$$rg(M) = \text{nombre de } \chi \in \hat{G} \text{ tels que } \sum_{\sigma \in G} \chi(\sigma) f(\sigma) \neq 0 \quad .$$

Preuve. Le vecteur $(\chi(\sigma_1), \chi(\sigma_2), \ldots, \chi(\sigma_n))$ est un vecteur propre de la matrice M dont la valeur propre associée est $\sum_{\sigma\in G} \chi(\sigma) f(\sigma)$. D'autre part les vecteurs $(\chi(\sigma_1), \ldots, \chi(\sigma_n))$ sont indépendants. En effet

$$n \begin{pmatrix} 1 & & \\ & 1 & \\ & & \ddots \\ & & & 1 \end{pmatrix} = \begin{pmatrix} \chi_1(\sigma_1) & \chi_2(\sigma_1) & \cdots & \chi_n(\sigma_1) \\ \chi_1(\sigma_2) & \chi_2(\sigma_2) & \cdots & \chi_n(\sigma_2) \\ \cdots & \cdots & \cdots & \cdots \\ \chi_1(\sigma_n) & \chi_2(\sigma_n) & \cdots & \chi_n(\sigma_n) \end{pmatrix} \begin{pmatrix} \chi_1^{-1}(\sigma_1) & \chi_1^{-1}(\sigma_2) & \cdots & \chi_1^{-1}(\sigma_n) \\ \chi_2^{-1}(\sigma_1) & \chi_2^{-1}(\sigma_2) & \cdots & \chi_2^{-1}(\sigma_n) \\ \cdots & \cdots & \cdots & \cdots \\ \chi_n^{-1}(\sigma_1) & \chi_n^{-1}(\sigma_2) & \cdots & \chi_n^{-1}(\sigma_n) \end{pmatrix}$$

Nous pouvons maintenant à l'aide de cette proposition déterminer le rang p-adique du groupe des unités d'un corps de nombres abélien.

THEOREME 1 [3],[4],[5]. Soit K un corps de nombres abélien sur $\mathbb{Q}$, alors

$$r_p(K) = r(K) .$$

Preuve. Soit K_o la sous-extension maximale réelle de K, le groupe $U(K_o)$ est d'indice fini dans U(K) (pour plus de précision voir appendice) par suite, on a

$$r_p(K_o) = r_p(K) .$$

Supposons donc que K soit une extension abélienne réelle. Si n est le degré de K sur $\mathbb{Q}$, il s'agit donc de démontrer que le rang de la matrice $(\log \sigma\tau^{-1}(\varepsilon))_{\sigma,\tau\in G}$ est n-1, lorsque ε est une unité de Minkowski.

Par suite, en utilisant la proposition 3, il suffit de démontrer que

$$\sum_{\sigma\in G} \chi(\sigma) \log \sigma(\varepsilon) \neq 0 \qquad \text{pour} \qquad \chi \neq 1 .$$

La famille $(\log \sigma(\varepsilon))_{\sigma \neq \varepsilon}$ est un système $\mathbb{Q}$-indépendant puisque ε est une unité de Minkowski. Un théorème [4] sur la linéaire indépendance des logarithmes de nombres algébriques montre que ce système est $\bar{\mathbb{Q}}$-indépendant ($\bar{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$). Ainsi

$$\sum_{\sigma \neq e} (\chi(\sigma)-1) \log \sigma(\varepsilon) \neq 0 \qquad \text{si} \quad \chi \neq 1 .$$

Comme la norme ε est ± 1 , on a

$$\sum_{\sigma \in G} \log \sigma(\varepsilon) = 0 .$$

Il en résulte que

$$\sum_{\sigma \in G} \chi(\sigma) \log \sigma(\varepsilon) \neq 0 .$$

Remarque. Si l'on savait que des logarithmes de nombres algébriques qui sont linéairement $\mathbb{Q}$-indépendants sont alors algébriquement indépendants sur $\mathbb{Q}$, on pourrait alors montrer que

$$r_p(K) = r(K) ,$$

quel que soit le corps de nombres K [16] (cf. remarque 3, p. 02).

V - NOMBRE DE Γ-EXTENSIONS INDEPENDANTES D'UN CORPS DE NOMBRES

1) Γ-extension

Définition 1 [8], [9], [15]. Soit K un corps, on appelle Γ-extension de K toute extension L de K telle que Gal(L/K) soit isomorphe algébriquement et topologiquement à $\mathbb{Z}_p$ (groupe additif des entiers p-adiques).

Puisque les seuls sous-groupes fermés d'indice fini de $\mathbb{Z}_p$ sont les $p^n \mathbb{Z}_p$ il existe une seule suite croissante de corps $(K_i)_{i \in \mathbb{N}}$ de degré

fini sur K tels que

$$K = K_o \subset K_1 \subset K_2 \subset \ldots \subset K_i \subset \ldots \subset L \quad ,$$

avec

$$\mathrm{Gal}(K_n/K) \simeq \mathbb{Z}/p^n\mathbb{Z} \qquad L = \bigcup_{i \in \mathbb{N}} K_i \quad .$$

Exemples. Soit P_n l'extension cyclotomique de $\mathbb{Q}$ engendrée par les racines p^{n+1} ième de l'unité, soit $P = \bigcup_{n \in \mathbb{N}} P_n$, alors P est une Γ-extension de P_o.

Soit $\mathbb{Q}_n$ l'unique extension cyclique de $\mathbb{Q}$ de degré p^n contenue dans P_n, alors $L = \bigcup_n \mathbb{Q}_n$ est une Γ-extension de $\mathbb{Q}$.

Soit L une Γ-extension de K, soit K' une extension finie de K. Alors $K'L$ est une Γ-extension de K'. Ceci montre que toute extension finie de $\mathbb{Q}$ admet une Γ-extension.

2) Ramification dans les Γ-extensions [9], [15]

Définition 2. Soit K une extension finie de $\mathbb{Q}$. L une Γ-extension de K, (K_i) la suite des sous-corps de L extension finie de K. Un diviseur premier de K (fini ou infini) est dit non ramifié dans L s'il est non ramifié dans K_i pour tout $i \geq 0$.

PROPOSITION 4. Soit K une extension finie de $\mathbb{Q}$, L une Γ-extension de K. Soit $\mathfrak{P}$ un diviseur premier infini de K, alors $\mathfrak{P}$ est non ramifié dans L.

Preuve. Si p est impair c'est évident. Si $p = 2$ et si $\mathfrak{P}$ est ramifié dans K_i il l'est dans K_n pour $n \geq i$, la sous-extension réelle maximale de K_n est donc K_{n-1} et $\mathfrak{P}$ n'est pas ramifié dans K_{n-1}, ce qui entraîne une contradiction.

PROPOSITION 5. Soit K une extension finie de $\mathbb{Q}$, L une Γ-extension de K avec $\mathrm{Gal}(L|K) \simeq Z_p$. Soit $\mathfrak{P}$ un premier ramifié dans L, alors $\mathfrak{P}|p$.

Preuve. Soit n le plus grand entier tel que $\mathfrak{P}$ soit non ramifié dans K_n. Soit $\mathfrak{q}$ un premier de K_n divisant $\mathfrak{P}$. Soit $m > n$, d'après la théorie de la ramification d'Hilbert, K_n est le corps d'inertie de $\mathfrak{P}$ et l'idéal $\mathfrak{q}$ est complètement ramifié dans K_m. Si $\mathfrak{P} \nmid p$, alors la ramification est douce et par suite l'indice de ramification de $\mathfrak{q}$ dans l'extension K_m de K_n est p^{m-n} et l'on a $p^{m-n} \mid [N_{K_m|\mathbb{Q}}(\mathfrak{q})-1]$. Ainsi lorsque m tend vers l'infini cette division est impossible et par suite $\mathfrak{P}|p$.

COROLLAIRE 1. Soit L une Γ-extension de K. Il existe au moins un premier $\mathfrak{P}$ de K ramifié dans L et au plus un nombre fini.

Preuve. La deuxième partie du corollaire est la proposition précédente et la première partie est une conséquence du fait que l'extension abélienne maximale non ramifiée de K (corps de classes de Hilbert) est une extension de degré fini (égal à l'ordre du groupe des classes d'idéaux de K).

3) Théorie du corps de classes pour les Γ-extensions

Soit K une extension finie de $\mathbb{Q}$, L une Γ-extension de K, avec $L = \bigcup_n K_n$ et

$$\mathrm{Gal}(K_n|K) = Z/p^n Z \quad , \quad \text{on a alors}$$

$$\mathrm{Gal}(L|K) = \varprojlim \mathrm{Gal}(K_n|K) = Z_p .$$

Notons par ψ_n l'application d'Artin $\psi_{K_n|K}$ du groupe J des idèles de K sur le groupe Gal $(K_n|K)$ [6] (cf. Tate, Global class field theory). Soit d'autre part ψ la limite projective des application ψ_n. Ainsi ψ est un homomorphisme continu de J dans $\varprojlim \text{Gal}(K_n|K) = \text{Gal}(L|K) \simeq Z_p$. L'application ψ est surjective ([6], [2]) et ainsi $J / \text{Ker}\ \psi \simeq Z_p$. Réciproquement si N est un sous-groupe fermé de J contenant K^* tel que J/N soit isomorphe (algébriquement et topologiquement) à Z_p alors la surjection canonique $J \to J/N$ est l'application d'Artin d'une Γ-extension (théorème d'existence). On peut préciser cette bijection entre les Γ-extensions et les sous-groupes de J. Soit

$$H = \{(a_{\mathfrak{P}}) \in J \mid a_{\mathfrak{P}} = 1 \quad \text{pour } \mathfrak{P}|p \quad \text{et} \quad a_{\mathfrak{P}} \in U_{\mathfrak{P}} \quad \text{pour } \mathfrak{P} \text{ fini}\}$$

($U_{\mathfrak{P}}$ désigne le groupe des unités $\mathfrak{P}$-adiques).

PROPOSITION 6. Il y a une correspondance bijective entre les Γ-extensions de K et les sous-groupes N de J contenant $K^* H$ tels que $J/N \simeq \mathbb{Z}_p$. L'application d'Artin de la Γ-extension définie par N est la surjection canonique $J \to J/N$.

4) Nombre de Γ-extensions indépendantes d'un corps de nombres [9]

Soit K une extension finie de $\mathbb{Q}$, K^{ab} la clôture abélienne de K et $G = \text{Gal}(K^{ab}|K)$ le groupe de Galois topologique de K^{ab} sur K. D'après la théorie de Galois il y a bijection entre les Γ-extensions de K et les homomorphismes continus de G sur $\mathbb{Z}_p$. Le groupe $A = \text{Hom}_{\text{cont}}(G, Z_p)$ des homomorphismes continus de G dans $\mathbb{Z}_p$ est canoniquement muni d'une structure de $\mathbb{Z}_p$-module.

Par définition 3, le nombre de Γ-extensions idépendantes de K est le rang du Z_p-module A.

PROPOSITION 7. Soit $\overline{K^*H}$ l'adhérence de K^*H et $J' = J/\overline{K^*H}$. Alors le $\mathbb{Z}_p$-module $\mathrm{Hom}_{cont}(G, \mathbb{Z}_p)$ est isomorphe à $\mathrm{Hom}_{cont}(J', \mathbb{Z}_p)$.

Preuve. Cet isomorphisme est défini par l'application $\varphi \to \psi \circ \varphi$ où ψ est l'application d'Artin de J sur G. Il suffit ensuite de remarquer que $\mathrm{Ker}\,\psi \subset K^*H$ puisque $\ker \psi$ est la composante connexe de J.

Nous sommes donc ramenés à calculer le rang sur Z_p de J'. On a la suite exacte :

$$1 \longrightarrow \prod_{\mathfrak{P}|p} U_{\mathfrak{P}} / \bar{E}' \longrightarrow J' \longrightarrow \bar{I} \longrightarrow 1$$

$\bar{I}$ est le groupe des classes d'idéaux de K, $\bar{E}'$ est l'adhérence dans $\prod_{\mathfrak{P}|p} U_{\mathfrak{P}}$ de l'image du groupe des unités de K, par l'application diagonale.

On a $\bar{I}$ = groupe fini

$$\prod_{\mathfrak{P}|p} U_{\mathfrak{P}} = (\text{groupe fini}) \oplus \mathbb{Z}_p^n \qquad \text{où} \qquad n = [K;\mathbb{Q}]$$

$$\bar{E}' = (\text{groupe fini}) \oplus \mathbb{Z}_p^s \qquad 1 \le s \le r_1 + r_2 - 1$$

(r_1 est le nombre de valeurs absolues réelles et r est le nombre de valeurs absolues complexes de K). Par suite on a

$$J' \simeq (\text{groupe fini}) \oplus \mathbb{Z}_p^{n-s} .$$

PROPOSITION 8 [9]. Le nombre de Γ-extensions indépendantes d'un corps de nombres K est $n-r_p(K)$ où n est le degré de K sur $\mathbb{Q}$ et $r_p(K)$ est le rang p-adique du groupe des unités de K.

On a donc l'inégalité

$$r_2+1 \leq \text{nombre de } \Gamma\text{-extensions indépendantes} \leq n-1 .$$

En particulier si K est une extension abélienne (non réelle) de $\mathbb{Q}$ le théorème 1 montre que le nombre de Γ-extensions indépendantes est r_2+1.

VI - APPENDICE. RELATION ENTRE LES UNITES D'UN CORPS ABELIEN ET CELLES DU SOUS-CORPS REEL MAXIMAL

Soit K une extension abélienne de $\mathbb{Q}$, K_o le sous-corps réel maximal. Si l'on note par σ la restriction à K de l'automorphisme de conjugaison complexe, K_o est le sous-corps des invariants de K par σ. Soit E le groupe des unités de K, W le groupe des racines de l'unité de K et E_o le groupe des unités de K_o. Nous allons démontrer que l'ordre du groupe quotient $E/_{W E_o}$ est 1 ou 2.

PROPOSITION 9. Un entier algébrique dont toutes les valeurs absolues archimédiennes sont 1 est une racine de l'unité.

Preuve. Les entiers algébriques d'un corps de nombres dont toutes les valeurs absolues archimédiennes sont 1 forment un groupe multiplicatif. D'autre part, ce groupe est fini puisque ses éléments sont racines de polynômes à coefficients entiers et bornés.

PROPOSITION 10. Soit K une extension abélienne de $\mathbb{Q}$. Notons par σ la restriction à K de l'automorphisme de conjugaison complexe. Soit a un entier algébrique non nul de K, alors $a^{1-\sigma}$ est une racine de l'unité.

Preuve. Notons $|\ .\ |$ la valeur absolue complexe. Soit τ un automorphisme quelconque du groupe de Galois de K sur $\mathbb{Q}$. On a

$$\tau\left(\frac{a}{\sigma(a)}\right) = \frac{\tau(a)}{\sigma(\tau(a))} \qquad \text{(commutativité)}$$

et ainsi $$\left|\tau\left(\frac{a}{\sigma(a)}\right)\right| = 1$$

Par suite tous les conjugués de $a^{1-\sigma}$ sont de valeur absolue complexe 1 et $a^{1-\sigma}$ est une racine de l'unité (proposition 9).

Remarque. Si l'extension K n'est pas abélienne, la proposition est fausse. Il suffit par exemple de remarquer que

$$\frac{j\sqrt[3]{2} - 1}{j^2\sqrt[3]{2} - 1} \neq 1\ ,\ -1\ ,\ j\ ,\ j^2\ ,$$ où j est une racine primitive cubique de l'unité.

PROPOSITION 11. Soit $\eta \in E$, alors il existe $\eta' \in E$ tel que

$$\eta \equiv \eta' \mod W E_o \quad \text{et} \quad \eta'^2 = \zeta\,\varepsilon \quad \text{avec} \quad \varepsilon \in E_o$$

et ζ est une racine primitive 2^k ième de l'unité avec $k \geq 2$.

Preuve. Soit $\eta \in E$, alors $\eta^2 = (\eta.\sigma(\eta))\ .\ \frac{\eta}{\sigma(\eta)}$, $\eta.\sigma(\eta) \in E_o$ et d'après la proposition 10, $\eta/\sigma(\eta)$ est une racine de l'unité. Cette racine de l'unité est produit d'une racine primitive 2^k ième de l'unité ζ et d'une racine primitive ξ, $m^{\text{ième}}$ de l'unité avec $(m, 2) = 1$. Par suite

$$\left(\frac{\eta}{\xi^{\frac{m+1}{2}}}\right)^2 = (\eta.\sigma(\eta))\,\zeta \ .$$

Si $k = 0$ ou 1, $\zeta \in E_o$ et la proposition est démontrée en prenant

$$\eta' = \eta \Big/ \xi^{\frac{m+1}{2}} \ .$$

THEOREME 2. Soit K une extension abélienne de $\mathbb{Q}$, K_o le sous-corps maximal réel. Soit E le groupe des unités de K, W le groupe des racines de l'unité de K, E_o le groupe des unités de K_o. Alors le groupe quotient $E/_{W E_o}$ est d'ordre 1 ou 2.

Preuve. Il s'agit de montrer que si η et $\eta' \in E$ et si $\eta \notin W E_o$ et $\eta' \notin W E_o$, que $\eta \equiv \eta' \bmod W E_o$. Nous allons considérer pour cela trois possibilités et ensuite conclure.

a) $\eta^2 = \varepsilon \in E_o$ et $\eta'^2 = \varepsilon' \in E_o$. Alors $K = K_o(\eta)$ et $\eta/_{\eta'} \in K_o$ ce qui prouve que

$$\eta \equiv \eta' \bmod W E_o \ .$$

b) $\eta^2 = \varepsilon \in E_o$, $\eta'^2 = \zeta \varepsilon'$, $\varepsilon' \in E_o$, ζ est une racine primitive $2^{k\,\text{ième}}$ de l'unité avec $k \geq 2$. Alors $K = K_o(i)$ et $\eta \in W E_o$.

c) $\eta^2 = \zeta \varepsilon$, $\eta'^2 = \zeta' \varepsilon'$, avec $\varepsilon \in E_o$, $\varepsilon' \in E_o$ et ζ et ζ' sont respectivement des racines primitives $2^{k\,\text{ième}}$ et $2^{k'\,\text{ième}}$ de l'unité avec $k, k' \geq 2$. Alors $K = K_o(i)$, si $k = k'$ d'après b) on a $\eta/_{\eta'} \in W E_o$. Si $k > k'$ il suit de b) que $\eta' \Big/ \zeta^{2^{k-k'-1}} \in W E_o$.

En utilisant finalement la proposition 11, le théorème est démontré.

BIBLIOGRAPHIE

[1] AMICE Y. et FRESNEL J. - Fonctions Zéta p-adique et formule des résidus pour le nombre de classes d'idéaux. Acta arithmética (à paraître).

[2] ARTIN E. , TATE J. - Class fields theory.

[3] AX J. - On the units of an algebraic number field Illinois Jl. of math. (1965).

[4] BRUMER A. - On the units of algebraic number field Mathematika vol. 14, part. 2, dec. 1967, n° 28, pp. 121-124.

[5] BRUMER A. - Le régulateur p-adique de Léopoldt. Journées arithmétiques de Grenoble, mai 1967, fasc. 1.

[6] CASSELS - FROLICH. - Algebraic number theory. Academic press, 1967.

[7] HASSE H. - Uber die Klassenzahl Abelscher Zahlkörper. Berlin - Academie Verlag, 1952.

[8] IWASAWA K. - On Γ-extensions of algebraic number fields - Bull. Amer. Math. Soc. t. 65, 1959.

[9] IWASAWA K. - Cours donné à Princeton fin 1966

[10] KUBOTA T. und LEOPOLDT H. W. - Eine p-adishe theorie der Zetawerte , I Einführung der p-adischer Dirichletschen, L. Funktionen. Journal für die reine und ang Math. t. 214/125 (1964) 328-339.

[11] LEOPOLDT H. W. - Zur Arithmetik in abelshen Zahlkörper. Journal für die reine und ang. Math. Band 209, Hept 1/2 (1962).

[12] MARTINET J. - Le théorème de Herbrand sur les unités. Séminaire de Théorie des Nombres de Bordeaux, 1968-1969, exposé n° 10.

[13] O'MEARA O. T. - Quadratics forms, Springer Verlag, Berlin 1963.

[14] MINKOWSKI H. - Zur theorie der Einheiten in den algebraishe Zahlkörpern. Göttingen Nachrichten, 1900, p. 90.

[15] SERRE J. P. - Classes de corps cyclotomiques. Sem. Bourbaki, 1958/59, fasc. 1, exp. 174.

[16] SERRE J. P. - Travaux de Baker. Sem. Bourbaki, 1969/70, fasc. 1, exp. 368.

[17] ROUSSEAU B. - Sur les unités d'un corps de nombres algébriques. Séminaire de Théorie des Nombres de Bordeaux, 1968-1969, exposé n° 11.

-:-:-:-:-